CORPS DE DÉCOMPOSITION DE GROUPE DE GALOIS PSL(2,7)

A. VALIBOUZE

Résumé

Dans cet article, nous proposons une méthode très efficace pour le calcul du corps de décomposition d'un polynôme de degré 7 de groupe de Galois PSL(2,7). La méthode proposée est généralisable.

Abstract

In this paper, we propose a new and efficient method for the computation of the splitting field of an univariate polynomial of Galois group PSL(2,7). This method can be generalized.

1. Introduction

Cet article présente une nouvelle méthode vérifiant que le groupe de Galois d'un polynôme de degré 7 est PSL(2,7) tout en calculant rapidement son corps de décomposition. Ce travail fait parti de travaux expérimentaux réalisés par l'auteur en 2001 et 2002 sur de nombreux groupes finis. Le résultat sur PSL(2,7) nous a paru assez édifiant pour mériter d'être présenté indépendamment.

Nous nous donnons un polynôme f de degré 7 en une variable sur un corps parfait k.

Le groupe symétrique de degré n sera noté S_n. Les groupes $7T_i$ sont les sous-groupes transitifs de S_7 de la nomenclature de G. Butler and J. McKay (voir [1]) et tabulés dans le logiciel de calcul symbolique Magma (voir [2]). L'exposant $+$ signifie que le groupe est pair. Dans cette nomenclature, le groupe PSL(2,7) est le groupe $7T_5$. Le groupe des k-automorphismes du corps de décomposition de f sera représenté dans S_n par un groupe $7T_i$ noté $\mathrm{Gal}_k(f)$.

2. Factorisation dans les extensions

L'idée est de factoriser le polynôme dans les extensions algébriques afin d'en extraire des informations sur son groupe de Galois. Jusqu'à présent, de ces factorisations n'étaient utilisés que les facteurs irréductibles pour être identifiés comme des relations et, lorsque cela à un sens, être factorisés à nouveau dans des extensions supérieures (voir [3] et [4]). Cette méthode

Date: 17 janvier 2005.

2000 *Mathematics Subject Classification.* Primary 12F10 ; Secondary 12Y05, 11Y40.

Key words and phrases. Splitting field, Galois ideal, Galois group.

de factorisation “à l’aveugle” aboutit au calcul du corps de décomposition mais avec un coût bien plus supérieur que ce qui est proposé ici.

Les sous-groupes 2-transitifs de S_7 sont $7T_4, 7T_5, 7T_6^+$ et $7T_7 = S_7$. Il est bien connu que $\mathrm{Gal}_k(f)$ est 2-transitif si et seulement si $g = f/(x-\alpha)$ est irréductible sur $k(\alpha)$ où α est une racine de f. Dès la première extension nous pouvons donc déterminer que l’un de ces groupes est ou non le groupe de Galois de f sur k. Nous avons le lemme plus précis suivant :

Lemme 2.1. *Soit α une racine de f. Si $\mathrm{Gal}_k(f)$ est 2-transitif, selon que $F = \mathrm{Gal}_k(f)$ soit respectivement $7T_4, 7T_5, 7T_6^+$ ou $7T_7 = S_7$, le groupe $\mathrm{Gal}_{k(\alpha)}(g) = \mathrm{Stab}(F, 1)$ est respectivement (dans S_7) le groupe $S_1 \times 6T_1$, $S_1 \times 6T_7^+$, $S_1 \times 6T_{15}^+$ et $S_1 \times 6T_{16}$.*

Démonstration. Par hypothèse, chaque groupe T parmi $7T_4, 7T_5, 7T_6^+$ et $7T_7 = S_7$ vérifient que le groupe $\mathrm{Stab}(T, 1)$ a une action transitive sur $\{2, \ldots, 7\}$. Le résultat est obtenu en faisant agir $\mathrm{Stab}(T, 1)$ sur l’unique orbite $\{2, \ldots, 7\}$. C’est un cas particulier du calcul des groupes de Galois des facteurs d’une résolvante dans le cas où la résolvante est le polynôme g lui-même (voir [5]). □

Ainsi, dès la première factorisation de f dans $k(\alpha)$ (i.e. $f = (x-\alpha)g$), nous disposons d’informations sur son groupe de Galois. Supposons donc que $\mathrm{Gal}_k(f)$ soit 2-transitif et posons $G = \mathit{Stab}(F, 1)$, le groupe de Galois de g sur $k(\alpha)$. Soit β une racine de g. Nous avons le lemme suivant :

Lemme 2.2. *Selon que G soit respectivement $S_1 \times 6T_1$, $S_1 \times 6T_7^+$, $S_1 \times 6T_{15}^+$ ou $S_1 \times 6T_{16}$, les degrés des facteurs irréductibles de $g/(x-\beta)$ sur $k(\alpha)(\beta)$ sont respectivement 1^5 (i.e. que des facteurs linéaires), $1, 4$ (1 facteur linéaire et un de degré 4), 5 ou 5.*

Démonstration. Pour les groupes 2-transitifs $6T_{15}^+$ et $6T_{16}$ nous avons forcément 5. Pour le groupe $S_1 \times 6T_1$ d’ordre 6, g se factorise nécessairement complètement dans l’extension $k[x]/ < g(x) >$ de degré 6 sur k. Pour $6T_7^+$, le calcul des cardinaux des orbites de l’action de $\mathrm{Stab}(6T_7, 1)$ sur $\{3, \ldots, 7\}$ donne 1 et 4. □

Nous en déduisons que :

Proposition 2.3. *Soient α et β deux racines distinctes de f. Nous avons $\mathrm{Gal}_k(f) = 7T_5$ si et seulement si $g = f/(x-\alpha)$ est irréductible sur $k(\alpha)$ et que $g/(x-\beta)$ se factorise sur $k(\alpha, \beta)$ en un facteur h linéaire et un facteur l irréductible de degré 4.*

3. Calcul du corps de décomposition

Dans cette partie, nous supposons que sont calculés :

(1) $\mathrm{Gal}_k(f) = 7T_5$

(2) le facteur linéaire $h(\alpha, \beta, x)$ et le facteur de degré 4 $l(\alpha, \beta, x)$ de $f(x)/(x-\alpha)(x-\beta)$ sur $k(\alpha, \beta)$ (voir Proposition 2.3).

Les méthodes pour que la condition (1) soit satisfaite sont nombreuses (voir, par exemple, [6]). Nous pouvons utiliser les résultats du paragraphe précédent qui fournissent aussi les facteurs h et l de g. Si $\mathrm{Gal}_k(f)$ est déterminé, il est possible d'obtenir h et l avec des calculs p-adiques puisque les degrés en chaque variable sont connus (voir [7]). En 1999, dans une communication privée, K. Yokoyama proposa de calculer directement le corps de décomposition de f avec des calculs p-adiques en formant la matrice des coefficients de l'idéal maximal cherché. Pour borner sa matrice, il utilisait la formule de [8] qui fournit les degrés des monômes initiaux de l'ensemble triangulaire engendrant l'idéal. Encore une fois, la méthode proposée ici est plus efficace car elle dispense de calculer bon nombre de ces coefficients (seules certaines relations seront à calculer).

Soient $\alpha_1, \ldots, \alpha_7$ des racines distinctes de f. Posons $\underline{\alpha} = (\alpha_1, \ldots, \alpha_7)$. L'idéal

$$\mathfrak{M} = \{r \in k[x_1, \ldots, x_7] \mid r(\alpha_1, \ldots, \alpha_7) = 0\}$$

est un idéal maximal dans $k[x_1, ..., x_7]$ car noyau du morphisme surjectif d'évaluation entre l'anneau $k[x_1, ..., x_7]$ et le corps de décomposition $K = k(\alpha_1, \ldots, \alpha_7)$ de f. Cet idéal est appelé l'*idéal des $\underline{\alpha}$-relations.* Il est engendré par un ensemble triangulaire de polynômes

$$r_1(x_1), r_2(x_1, x_2), \ldots, r_7(x_1, \ldots, x_7)$$

où chaque polynôme r_i est unitaire de degré d_i en x_i. Le groupe de décomposition $\mathrm{Dec}(\mathfrak{M})$ de cet idéal (i.e. l'ensemble des permutations de S_7 qui laissent $\mathfrak{M}$ invariant) est un conjugué de $\mathrm{Gal}_k(f)$. Il s'appelle le *groupe de Galois de $\underline{\alpha}$ sur k*. Il est isomorphe au groupe des k-automorphismes de K. Son ordre 168 est le produit $d_1 \cdots d_7$ (voir [9] pour tout ce qui précède).
Pour calculer le corps K, nous devons donc déterminer un tel idéal $\mathfrak{M}$ par un ensemble triangulaire l'engendrant.
Le lemme suivant découle des résultats de [9] mais sa démonstration directe n'est pas compliquée.

Lemme 3.1. *Soit $\mathfrak{M}$ un idéal maximal de relations. Alors*

(1) *l'ensemble des idéaux maximaux de relations est formé des $\sigma.\mathfrak{M}$ où σ parcourt S_n.*

(2) *chaque idéal $\sigma.\mathfrak{M}$ est l'idéal des $\sigma^{-1}.\underline{\alpha}$-relations de groupe de décomposition* $\mathrm{Dec}(\sigma.\mathfrak{M}) = \mathrm{Dec}(\mathfrak{M})^\sigma$ *($= \sigma\,\mathrm{Dec}(\mathfrak{M})\sigma^{-1}$).*

Proposition 3.2. *Un sous-groupe H de S_n est le groupe de décomposition d'un idéal maximal $\langle r_1, r_2, \ldots, r_7\rangle$ de relations tel que $r_1 = f$,$r_2 = g$, $r_3 = h$ et $r_4 = l$ si et seulement si H est un conjugué de $7T_5$ vérifiant :*

(1) $\mathrm{Stab}(H, 1) \subset S_1 \times S_6$ *et*

(2) $\mathit{Stab}(\mathrm{Stab}(H, 1), 2) \subset S_1 \times S_1 \times S_1 \times S_4$.

Démonstration. Soit $\mathfrak{M}$ un idéal maximal de relations tel que $r_1 = f$, $r_2 = g$, $r_3 = h$ et $r_4 = l$. Tout d'abord, le groupe $\mathrm{Dec}(\mathfrak{M})$ est un conjugué de $7T_5$ (voir Lemme 3.1). Nous savons que $\sigma \in \mathrm{Dec}(\mathfrak{M})$ si et seulement si pour toute relation $r \in \mathfrak{M}$, $r(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(7)}) = 0$. Ceci est donc, en particulier, vérifié pour les relations r_1, r_2, r_3, r_4. Si $\sigma \in \mathrm{Dec}(\mathfrak{M})$ tel que $\sigma(1) = 1$ alors $0 = r_2(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}) = r_2(\alpha_1, \alpha_{\sigma(2)}) = g(\alpha_1, \alpha_{\sigma(2)})$. Donc $\mathrm{Dec}(\mathfrak{M})$ satisfait (1) car les racines de $g(\alpha_1, x)$ sont $\alpha_2, \ldots, \alpha_7$. Si, de plus, $\sigma(2) = 2$, alors $0 = r_i(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, , \alpha_{\sigma(i)}) = r_i(\alpha_1, \alpha_2, \alpha_{\sigma(i)})$, pour $i = 3, 4$. Nous avons $\sigma(3) = 3$ car α_3 est l'unique racine de $h(\alpha_1, \alpha_2, x)$ est α_3 et $\sigma(4) \in E = \{\alpha_4, \alpha_5, \alpha_6, \alpha_7\}$ car les éléments de E sont les racines de $l(\alpha_1, \alpha_2, x)$. Donc $\mathrm{Dec}(\mathfrak{M})$ satisfait (2).
Réciproquement si H est un conjugué de $7T_5$ alors il est le groupe de décomposition d'un idéal maximal $\mathfrak{M}$ (voir Lemme 3.1). Soit $\{r_1, \ldots, r_7\}$ l'ensemble triangulaire engendrant $\mathfrak{M}$ s'annulant en $\alpha_1, \ldots, \alpha_7$. Si H satisfait les conditions (1) et (2) alors, d'après [8], les degrés respectifs de $r_1, \ldots, r_7$ en $x_1, \ldots x_7$ sont 7,6,1,4,1,1 et 1 (c'est un simple calcul de stabilisateurs). Comme $\mathfrak{M}$ est maximal, nécessairement r_1 est irréductible sur k, r_2 sur $k(\alpha_1)$, r_3 et r_4 sur $k(\alpha_1, \alpha_2)$. Avec les résultats du paragraphe 2, nous avons donc $r_1 = f$, $r_2 = g$ (le seul polynôme de degré 6 sur $k(\alpha_1)$), $r_3 = h$ (le seul polynôme linéaire sur $k(\alpha_1, \alpha_2)$) et $r_4 = l$ (le seul polynôme de degré 4 sur $k(\alpha_1, \alpha_2)$). □

Comme dans la proposition précédente, choisissons que les racines $\alpha_1, \ldots, \alpha_7$ telles qu'on puisse poser $r_1 = f$, $r_2 = g$, $r_3 = h$ et $r_4 = l$. La somme des racines est opposée au coefficient λ de x^6 dans f. Nous pouvons donc poser $r_7 = x_1 + \cdots + x_7 + \lambda$. Comme l'annonce le théorème suivant, nous disposons déjà de toutes les informations pour pré-calculer les relations r_5 et r_6 respectivement linéaires en x_5 et x_6 (voir démonstration de la proposition).

Théorème 3.3. *Soit f un polynôme univarié de groupe de Galois $7T_5$ sur k. Soit $H = \langle \sigma = (1,4,3,5,6,7,2), (2,5)(3,4) \rangle$ un des conjugués de $7T_5$ satisfaisant les conditions (1) et (2) de la proposition 3.2. Alors H est le groupe de décomposition de l'idéal maximal engendré par l'ensemble triangulaire :*

$$\{ \quad f(x_1), g(x_1, g_2), h(x_1, x_2, x_3), l(x_1, x_2, x_4), \\ h(x_4, x_1, x_5), h(x_3, x_1, x_6), h(x_5, x_4, x_7) \quad \} \quad .$$

où, pour α et β deux racines distinctes de f, $g(\alpha, x) = f/(x-\alpha)$ est irréductible de degré 6 sur $k(\alpha)$, $h(\alpha, \beta, x)$ est le facteur linéaire de $g/(x-\beta)$ sur $k(\alpha, \beta)$ et $l(\alpha, \beta, x)$ est le facteur irréductible de degré 4 de $g/(x-\beta)$ sur $k(\alpha, \beta)$.

Démonstration. D'après la proposition 3.2, H est le groupe de décomposition d'un idéal maximal $\mathfrak{M}$ et $f(x_1), g(x_1, g_2), h(x_1, x_2, x_3), l(x_1, x_2, x_4)$ appartiennent à l'ensemble triangulaire l'engendrant. Donc les trois relations $h(x_4, x_1, x_5) = \sigma.h(x_1, x_2, x_3)$, $h(x_3, x_1, x_6) = \sigma^2.h(x_1, x_2, x_3)$ et

$h(x_5, x_4, x_7) = \sigma^3.h(x_1, x_2, x_3)$ appartiennent aussi à $\mathfrak{M}$. Comme elles sont linéaires en x_5, x_6 et x_7 respectivement, nous obtenons le résultat. $\square$

4. Comparaisons

En utilisant la méthode "à l'aveugle" de factorisation dans les extensions pour calculer les relations r_5 et r_6, il faut factoriser le polynôme $l(\alpha_1, \alpha_2, x)$ dans l'extension $k(\alpha_1, \alpha_2, x)/ < l(x) >$ de degré 168 sur k.

En utilisant les calculs p-adiques, K. Yokoyama cherchait les polynômes r_5 et r_6. De plus, nous savons que, pour $i = 3, 4,$:
- $r_i \in k[x_1, x_2, x_i]$ avec $deg_{x_1}(r_i) < deg_{x_1}(r_1) = 7$, $deg_{x_2}(r_i) < deg_{x_2}(r_2) = 6$
- $deg_{x_3}(r_3) = 1$, $deg_{x_3}(r_4) = 0$ et $deg_{x_4}(r_4) = 4$.

Ainsi, si $\mathrm{Gal}_k(f)$ est connu, les polynômes r_3 et r_4 pourront être obtenus par des calculs p-adiques sans avoir à calculer des coefficients superflus.

Conclusion La méthode décrite dans cet article est applicable dans tout système de calcul formel. Elle s'avère naturellement plus efficace que les autres méthodes connues à ce jour. Pour être généralisée, elle demande une étude approfondie et trop compliquée pour être développée ici.

Références

[1] G. Butler and J. McKay. The transitive groups of degree up to eleven. *Comm. Algebra*, 11(8) :863–911, 1983.
[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4) :235–265, 1997. Computational algebra and number theory (London, 1993).
[3] N. Tchebotarev. *Gründzüge des Galois'shen Theorie.* P. Noordhoff, 1950.
[4] H. Anai, M. Noro, and K. Yokoyama. Computation of the splitting fields and the Galois groups of polynomials. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, volume 143 of *Progr. Math.*, pages 29–50. Birkhäuser, Basel, 1996.
[5] A. Valibouze. Computation of the galois groups of the resolvent factors for the direct and inverse galois problem. *LNCS*, 948 :456–468, 1995.
[6] L. Soicher and J. McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3) :273–281, 1985.
[7] K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118 :617–636, 1997. Algorithms for algebra (Eindhoven, 1996).
[8] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6) :635–651, 2000. Algorithmic methods in Galois theory.
[9] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin*, 6(4) :507–535, 1999.

L.I.P.6, Université Pierre et Marie Curie, 4, place Jussieu, F-75252 Paris Cedex 05
E-mail address: Annick.Valibouze@lip6.fr