Résolvantes produits en théorie de Galois

Annick Valibouze

RÉSOLVANTES PRODUITS EN THÉORIE DE GALOIS

1. Introduction

La résolvante est l'outil fondamental introduit par Lagrange afin d'unifier les méthodes de résolution par radicaux jusqu'en degré 4 et de fournir un outil pour les degrés supérieurs. En particulier, Lagrange envisageait de montrer qu'à partir du degré 5, il n'existe pas de résolvante dont le degré abaisse celui de tout polynôme comme jusqu'en degré 4. La conséquence qu'il espérait en tirer était, qu'à partir du degré 5, toute équation n'est pas résoluble par radicaux.

Dans sa thèse, Soicher ([8]) étudie l'action du groupe de Galois d'un polynôme p d'une variable sur les r-ensembles et les r-séquences de ses racines (voir également [7]). Cette étude consiste à factoriser certaines résolvantes linéaires du polynôme p. Ces factorisations induisent des partitions propres au groupe de Galois de p : la partition induite par la factorisation de la résolvantes d'un polynômes ne dépend que de son groupe de Galois. L.E. Soicher a su montrer que trois types de résolvantes suffisent à déterminer le groupe de Galois d'un polynôme degré inférieur ou égal à 7. Ces trois types de résolvantes sont tous linéaires, et deux d'entre eux sont symétriques (i.e. la fonction transformant le polynôme est symétrique). Les degrés des facteurs irréductibles des résolvantes linéaires symétriques, dites *sommes*, (i.e. dont le polynôme de transformation est une somme de variables) sont induits par l'action du groupe de Galois de p sur les r-ensembles. Mais toute résolvante symétrique possède la même propriété puisque l'action ne dépend que du stabilisateur du polynôme de transformation (voir [2] et [1]). Or, comme nous allons le montrer, les résolvantes les plus faciles et rapides à calculer sont les résolvantes produits (i.e. symétriques induites par un produit). Après avoir décrit comment les calculer, nous comparerons avec les temps de L.E. Soicher pour les résolvantes sommes. Pour les calculs, nous utilisons la bibliothèque `Symmetries` disponible sous le système de calcul formel libre `Maxima` (voir [10]).

2. Définitions et Notations

Pour simplifier, nous prendrons le corps des rationnels $\mathbb{Q}$ comme corps de base. Dans tout l'article nous étudierons un polynôme irréductible p de $\mathbb{Q}[x]$ et de degré n.

Soit S_n le groupe symétrique de degré n. L'action de S_n sur $\{1, \ldots, n\}$ induit naturellement une action sur tout polynôme de n variables $x_1, \ldots, x_n$ par permutation des indices.

Soit f une fonction de n variables $x_1, \ldots, x_n$, et H un sous-groupe de S_n, nous notons $H.f$ l'ensemble $\{\sigma.f | \sigma \in H\}$ et nous l'appelons l'*orbite* de f sous l'action de H. De la même

manière, si H agit sur un ensemble E et e est un élément de cet ensemble, nous noterons $H.e$ l'orbite de e dans E sous l'action de H.

Pour tout n-uplet $\boldsymbol{i} \in \mathbb{N}^n$, nous posons

$$\boldsymbol{x}^{\boldsymbol{i}} = x_1^{i_1} \cdots x_n^{i_1} \quad .$$

Nous adopterons les notation de I.G. Macdonald sur les fonctions symétriques ([6]). Soit A un alphabet. Pour tout $k \in \mathbb{N}$, la k-ième *fonction symétrique élémentaire* sur A est $e_k(A) = \sum_{m \in S_n.a_1 \cdots a_k} m$, avec $e_0(A) = 1$, et la k-ième *fonction puissance* sur A est $p_k(A) = \sum_{a \in A} a^k$. Par exemple,

$$e_2(\{x_1, x_2, x_3\}) = x_1x_2 + x_2x_3 + x_2x_3 \quad \text{et} \quad p_2(\{x_1, x_2, x_3\}) = x_1^2 + x_2^2 + x_3^2 \quad .$$

Nous rappelons les formules de Girard-Newton ([4]) : pour tout alphabet A et pour tout entier $m > 0$, il vient :

$$p_m(A) - e_1(A)p_{m-1}(A) + e_2(A)p_{m-2}(A) + \cdots + (-1)^m m\, e_m(A) = 0. \tag{1}$$

Ainsi il est aisé d'obtenir les fonctions puissance à partir des fonctions symétriques élémentaires et réciproquement. Si A est

Définition 2.1. (Résolvante de Lagrange) Soit f un polynôme de $\mathbb{Q}[x_1, \ldots, x_n]$. Soient $\alpha_1, \ldots, \alpha_n$ les racines d'un polynôme p de $\mathbb{Q}[x]$ de degré n. La *résolvante (absolue) de p par f* est le polynôme :

$$R_{f,p} = \prod_{h \in S_n.f} (x - h(\alpha_1, \ldots, \alpha_n)).$$

Par le théorème fondamental des fonctions symétriques, les coefficients de la résolvante $R_{f,p}$ appartiennent à $\mathbb{Q}$ puisqu'ils sont symétriques en les racines de p.

Le polynôme f est appelé le *polynôme de transformation* associé à la résolvante. Si ce polynôme est linéaire alors la résolvante est dite *linéaire*. Soit r un entier de $[\![1, n]\!]$. Si le polynôme f est d'arité r et symétrique en ses r variables alors la résolvante est dite *symétrique*. La résolvante $R_{x_1+\ldots+x_r,p}$ est appelée une *résolvante somme* et $R_{x_1 \cdots x_r,p}$ est appelée une *résolvante produit*.

Exemple 2.2. Posons $p = (x - a)(x - b)(x - c)$. Alors le polynôme

$$R_{x_1+x_2,p} = (x - (a + b))(x - (a + c))(y - (b + c))$$

est la résolvante de p par f. Cette résolvante est à la fois linéaire et symétrique ; c'est une résolvante somme. La résolvante $R_{x_1x_2,p} = (x - ab)(x - ac)(y - bc)$ est une résolvante produit.

3. Résolvantes symétriques et action sur les r-ensemble

Nous noterons G le groupe de Galois de p sur $\mathbb{Q}$. Un *r-ensemble* est un sous-ensemble de $\{1,\dots,n\}$ de r éléments. Soit f un polynôme symétrique de r variables ($r \leq n$). Si H est un sous-groupe de S_n, l'action de H sur l'orbite $S_n.f$ est équivalente à celle de H sur les r-ensembles de $\{1,\dots,n\}$. Ainsi la factorisation de $R_{f,p}$ est déterminée par la partition engendrée par les cardinaux $|G.\{i_1,\dots,i_r\}|$ où les ensembles $\{i_1,\dots i_r\}$ parcourent les r-ensembles de $\{1,\dots,n\}$ de cardinal r. Ces partitions sont appelées les *partitions des longueurs d'orbites*. Dans sa thèse L. Soicher donne les tables des partitions des longueurs d'orbites jusqu'en degré 8 et calcule les groupes de Galois jusqu'en degré 7. Ces tables avaient été calculées par G. Butler et J. McKay (voir [3]). L. Soicher n'évoque que les résolvantes sommes, bien que toute résolvante symétrique satisfasse cette propopriété de factorisation. La raison semble provenir du fait qu'il propose un algorithme pour les résolvantes linéaires. Nous allons voir que dans le cas des résolvantes symétriques, il est préférable de calculer des résolvantes produits.

4. Résolvantes produits

Nous nous posons le problème de calculer une résolvante produit. Pour cela nous proposons un algorithme simple utilisant le fait que les coefficients d'un polynôme d'une variable sont, à un signe près, les fonctions symétriques élémentaires de ses racines. Nous allons calculer les fonctions puissances des racines de la résolvante produit à partir des fonctions puissances des racines du polynôme p.

4.1. **Propriété de base pour les algorithmes.**

Nous proposons trois méthodes : la première avec les résultants et les formules de Girard-Newton, la seconde uniquement avec les formules de Girard-Newton et la troisième avec la fonction de `SYM` calculant un polynôme symétrique à partir des fonctions symétriques élémentaires. Les deux premières méthodes permettent d'obtenir simultanément toutes les résolvantes produits d'un même polynôme. Nous verrons qu'il est préférable d'utiliser :

- la troisième méthode pour le calcul d'une seule résolvante,
- la seconde pour calculer simultanément toutes les résolvantes produits d'un polynôme.

Les deux premières méthodes sont basées sur le lemme suivant :

Lemme 4.1. *Soit A un alphabet. Notons A^r l'alphabet $\{a^r : a \in A\}$ avec $r \in \mathbb{N}$ ($|A| = |A^r|$) et A^{*k} l'alphabet $\{a_1a_2\cdots a_k : a_i$ distincts dans $A\}$ avec $k = 0,\dots,|A|$. La k-ième fonction symétrique élémentaire sur A^r est la r-ième fonction puissance sur A^{*k}.*

Démonstration. En effet,

$$p_r(A^{*k}) = \sum_{b\in A^{*k}} b^r = \sum_{a_1\cdots a_k\in A^{*k}} a_1^r\cdots a_k^r = e_k(A^r).$$

□

En termes de résolvantes, le lemme se traduit par la proposition suivante qui exprime que les coefficients des résolvantes produits sont déductibles, via les relations de Girard-Newton, des coefficients des résolvantes de Tchirnhaus par des fonctions de transformation de la forme x_1^r :

Propriété 4.2. *Soit p un polynôme d'une variable de degré n. Pour tout $r \in \mathbb{N}$ et tout $k = 0, \ldots, n$, la k-ième fonction symétrique élémentaire des racines de la résolvante $R_{x_1^r,p}$ est la r-ième fonction puissance des racines de la résolvante $R_{x_1\cdots x_k,p}$.*

Preuve. Soit A l'ensemble des racines du polynôme p. La k-ième fonction symétrique élémentaire des racines de $R_{x_1^r,p}$ est $e_k(A^r)$ tandis que la r-ième fonction puissance des racines de $R_{x_1\cdots x_k,p}$ est $p_r(A^{*k})$. Le lemme 4.1 permet de conclure. ♢

Remarque 1. Si n est le degré du polynôme p, le degré de $R_{x_1\cdots x_k,p}$ est $\begin{pmatrix} n \\ k \end{pmatrix}$ puisqu'il s'agit de choisir k éléments non ordonnés parmi n et de les sommer. Le degré maximun d'une résolvante $R_{x_1\cdots x_k,p}$ pour $k = 1, \ldots, n$ est donc

$$rmax = \begin{pmatrix} n \\ k_0 \end{pmatrix}$$

où $k_0 = ent(n/2)$, la partie entière de $n/2$. Il est donc suffisant de calculer les résolvantes $R_{x_1^r,p}$ pour $r \leq rmax$.

4.2. **Les algorithmes.**

Notre objectif est le calcul des résolvantes produits $R_{x_1\cdots x_k,p}$. Afin de simplifier la présentation, nous supposons le polynôme p unitaire.

Le shéma suivant est celui de Lagrange pour le calcul des résolvantes absolues (voir [5]) :

`Algorithme : RésolvanteProduit`

Entrées : p `un polynôme d'une variable et de degré` n
f `un polynôme en` n `variables`
Sortie : `la résolvante` $R_{f,p}$
Corps :
`1) Calculer les fonctions puissances des racines de` $R_{f,p}$.
`2) En déduire la résolvante` $R_{f,p}$.

Le point 2) est résolu par les formules de Girard-Newton. Nous utiliserons dans nos algorithmes la fonction `pui2ele(m,[c,p1,p2,...,pm])` qui calcule les `m` premières fonctions symétriques élémentaires à partir des `m` premières fonctions puissance d'un alphabet de cardinal `c`.

Pour résoudre le point 1), d'après la proposition 4.2, nous devons calculer les k-ième fonctions symétriques élémentaires des racines des résolvantes $R_{x_1^r,p}$ pour $r = 1, \ldots, \left(\begin{array}{c} n \\ k \end{array} \right)$.

4.2.1. *Avec les résultants.*

Nous notons $Res(p, q, x)$ le résultant en x de deux polynômes p et q. Par définition du résultant, ayant supposé p unitaire, les résolvantes de Tchrinhaus se calculent ainsi :

$$R_{f(x_1),p} = Res(p(x_1), x - f(x_1), x_1) \tag{2}$$

Par conséquent, en appliquant cette formule à $f(x_1) = x_1^r$, la partie 1) de l'algorithme général `RésolvanteProduit` peut se réaliser ainsi :

`Algorithme : RésolvanteProduit Option Résultant`

Entrée : p `un polynôme`
Sortie : `les listes pui[k] des fonctions puissances des racines des résolvantes` $R_{x_1 \cdots x_k,p}$ `pour k=0 à n`

Corps :

```
n:deg(p)
rmax : binomial(n,quotient(n,2))
POUR r:0 A rmax FAIRE
        pol[r] : resultant(p,y-x**r,x)
POUR k:0 A n FAIRE
        pui[k] : []
        POUR r:rmax A 0 FAIRE
                    pui[k]:cons((-1)**k*coeff(pol[r],y,n-k),pui[k])
```

Dans cet algorithme, la résolvante $R_{x_1^r,p}$ est le polynôme `pol[`r`]` ($r = 1, \ldots, rmax$).

4.2.2. *Avec les manipulations de fonctions symétriques.*

C'est ce point de vue qui a été privilégié dans la bibliothèque `Symmetries` de `Maxima` qui comporte deux possibilités : la première avec la fonction `resolvante_produit_sym`, associée à l'algorithme `RésolvanteProduit Option Toutes`, qui calcule simultanément toutes

les résolvantes produits d'un polynôme et la seconde avec la fonctions `prodrac` ou la fonction `resolvante` flaguée avec `produit`, associée à l'algorithme `RésolvanteProduit Option Une`, qui calcule une seule résolvante produit.

Comme avec les résultants nous supposons disposer de la fonction `pui2ele` calculant les fonctions symétriques élémentaires à partir des fonctions puissances. Nous supposons également disposer de la fonction `ele2pui(m,[c,e1,e2,...,ec])` calculant les `m` premières fonctions puissances à partir des `m` premières fonctions symétriques élémentaires d'un alphabet de cardinal `c`. Ces deux fonctions sont disponibles dans `Maxima`.

Pour l'algorithme `Option Toutes`, au lieu de calculer les résolvantes $R_{x_1^r,p}$ avec des résultants, nous calculerons les fonctions puissances $p_i(A^r)$ de ses racines puisque, comme le montre la suite d'identités:

$$p_i(A^r) = \sum_{b \in A^r} a^{ir} = \sum_{a \in A} a^i r = p_{ir}(A),$$

elles sont des fonctions puissances du polynôme p. La plus grande valeur utile pour r est $rmax$ associée à l'entier $k = kmax$, la partie entière supérieure de $n/2$ (n est le degré de p). Ainsi nous n'aurons besoin de ne calculer que les fonctions puissances de 1 à $kmax$ des racines de la résolvante $R_{x_1^{rmax},p}$. C'est ainsi que nous devrons calculer les fonctions puissances des racines de p jusqu'au produit $rmax.kmax$. Ceci nous amène au programme suivant :

```
Algorithme :  RésolvanteProduit Option Toutes
Entrée :  p un polynôme
Sorties :  les listes pui[k] des fonctions puissances
           des racines des résolvantes R_{x_1...x_k,p} pour k=0 à n
Corps :
n:deg(p)
kmax :  if oddp(n) then 1+quotient(n,2) else quotient(n,2)
A[0]:makelist(binomial(n,r),r,0,n),
A[1] :cons(n,makelist(coeff(p,x,n-i)*(-1)**i,i,1,n)),
pi:ele2pui(binomial(n,kmax)*kmax,A[1]),
Pour i:1 A quotient(n,2) FAIRE
     POUR r:binomial(n,i-1)+1 A binomial(n,i) FAIRE
          A[r] :  pui2ele(n-i, makelist(part(pi,r*k+1), k,0,n-i))
Pour k:1 A n FAIRE
     bin :  binomial(n,k)
     pui[k] :  makelist(part(A[k],k+1),r,0,bin).
```

Dans cet algorithme, la fonction `part` extrait un élément d'une liste et la fonction `makelist` construit une liste. Les fonctions symétriques élémentaires des racines du polynôme $R_{x_1^r,p}$ utiles pour le calcul des résolvantes $R_{x_1 \cdots x_k,p}$ sont dans la liste `A[r]`.

Pour l'`Option Une`, l'objectif étant de ne calculer qu'une seule résolvante $R_{x_1\cdots x_k,p}$, nous utilisons l'identité

$$p_r(A^{(k)}) = \sum a_1^r a_2^r \dots a_k^r, \tag{3}$$

où la somme est étendue à toute l'orbite du monôme $a_1^r a_2^r \dots a_k^r$ sous l'action du groupe symétrique S_n. Cette somme symétrique est exprimable en fonction des fonctions symétriques élémentaires des racines de p. La bibliothèque `Symmetries` de `Maxima` est de nouveau utilisable pour implanter cette option puisqu'elle implante le théorème fondamental des fonctions symétriques (voir [9]).

5. Comparaisons de temps

Les calculs sont effectués sur une SPARC 1+ (4-65). Tous les calculs sont effectués sous `Maxima`.

Donnons-nous le polynôme $p = x^7 - 14x^5 + 56x^3 - 56X + 22$. Le calcul de toutes les résolvantes produit prend 18.5 secondes avec l'option l'option `Résultant`, 7 secondes avec l'option `Toutes` et 15 secondes avec l'option `Une`. En revanche, le calcul de $R_{x_1x_2x_3,p}$ prend 4 secondes avec l'option `Une` et c'est la résolvante produit la plus longue à calculer.

En conclusion, si l'on désire obtenir toutes les résolvantes produits d'un polynôme, il faut utiliser l'option `Toutes` n'utilisant essentiellement que les formules de Girard-Newton, mais si l'on désire n'en calculer qu'une il est préférable d'utiliser l'otion `Une`.

Pour calculer la résolvante $R_{x_1+x_2+x_3,p}$, L.E. Soicher met 10 secondes sur un CDC Cyber. Or l'information est la même que celle obtenue avec le calcul de $R_{x_1x_2x_3,p}$ qui ne prend que 4 secondes.

6. Exemple

Donnons-nous le polynôme $p(x) = x^6 - 3x^5 + 6x^4 - 7x^3 + 2x^2 + x - 4$. L'action du groupe de Galois de p sur les r-ensembles se déduit des factorisation des 5 résolvantes $R_{x_1\cdots x_k,p}$ où

$k = 1, 2, 3, 4, 5$. Ces résolvantes factorisées sur $\mathbb{Q}$ sont :

$$\begin{aligned}
R_{x_1,p} &= p \\
R_{x_1x_2,p} &= (x^3 - 3x^2 - x + 4)(x^{12} - 3x^{11} + 11x^{10} - 16x^9 + 21x^8 - 72x^7 + 124x^6 \\
&\quad -252x^5 + 219x^4 - 152x^3 + 512x^2 + 192x + 256) \\
R_{x_1x_2x_3,p} &= (x^8 - x^7 - 11x^6 - 19x^5 + 101x^4 + 76x^3 - 176x^2 + 64x + 256) \\
&\quad (x^{12} - 6x^{11} + 16x^{10} - 39x^9 - 19x^8 - 75x^7 - 315x^6 + 300x^5 \\
&\quad -304x^4 + 2496x^3 + 4096x^2 + 6144x + 4096) \\
R_{x_1x_2x_3x_4,p} &= (x^3 + x^2 - 12x - 16)(x^{12} - 3x^{11} + 32x^{10} + 38x^9 + 219x^8 + 1008x^7 \\
&\quad +1984x^6 + 4608x^5 + 5376x^4 + 16384x^3 + 45056x^2 + 49152x + 65536) \\
R_{x_1x_2x_3x_4x_5,p} &= x^6 + x^5 - 8x^4 - 112x^3 - 384x^2 - 768x - 1024
\end{aligned}$$

Les actions du groupe de Galois sur les 1-ensembles, 2-ensembles et 3-ensembles induisent respectivement les partitions de longueur d'orbite (6), (3, 12) et (8, 12). Le groupe de Galois est donc transitif, puisque p est irréductible sur $\mathbb{Q}$. Le seul sous-groupe transitif de S_6 agissant ainsi sur les 2-ensembles et 3-ensembles est le groupe $6T3$ engendré par les permutations $(1, 2, 3)(1, 4)(2, 5)(3, 6)$ et (1,4)(2,5)(3,6)(1,5,2,4)(3,6)(1,5,2,4)(3,6) (voir [8]).

References

[1] J.-M. Arnaudiès and A. Valibouze. Lagrange resolvents. *J. Pure Appl. Algebra*, 117/118:23–40, 1997.

[2] J.M. Arnaudiès and A. Valibouze. Résolvantes de lagrange. Technical Report 93.61, LITP, 1993.

[3] G. Butler and J. McKay. The transitive groups of degree up to eleven. *Comm. Algebra*, 11(8):863–911, 1983.

[4] Girard. Invention nouvelle en algèbre. *Amsterdam*, 1629.

[5] J.-L. Lagrange. *Oeuvres, Tome VIII, Notes sur la théorie des équations algébriques, Note X*. Publiées sous les auspices du ministère de l'instruction publique, 1808.

[6] I.G. Macdonald. *Symmetric Functions and Hall Polynomials, second ed.* Oxford: Clarendon Press. ISBN 0-19-850450-0 (paperback, 1998), 1995.

[7] J. McKay and L. Soicher. Computing Galois groups over the rationals. *J. Number Theory*, 20(3):273–281, 1985.

[8] L.E. Soicher. *The computation of the Galois groups*. PhD thesis, Thesis, Department of computer science, Concordia University, Montreal, Quebec, Canada, 1981.

[9] A. Valibouze. Fonctions symétriques et changements de bases. In *Proceeding of EUROCAL '87 (Leipzig, RDA)*, pages 323–332. Springer-Verlag, 1987.

[10] A. Valibouze. Symbolic computation with symmetric polynomials, an extension to Macsyma. In *Computers and Mathematics (MIT, USA, June 13-17, 1989)*, pages 308–320. Springer-Verlag, New York Berlin, 1989.
(Voir "Symmetries" dans `http://maxima.sourceforge.net/docs.shtml`).