Résolvantes, groupe de Galois et Idéaux galoisiens

Annick Valibouze

RÉSOLVANTES, GROUPE DE GALOIS ET IDÉAUX GALOISIENS

ANNICK VALIBOUZE

1. Introduction

Depuis qu'elle fut introduite par J. L. lagrange, la résolvante d'un polynôme est devenue un outil central pour étudier son groupe de Galois, sa résolution par radicaux et ses idéaux galoisiens. Souvent, les résultats ne portent que sur les facteurs sans multiplicité dans la résolvante. Par exemple, dans [15] est énoncé le théorème de l'élément primitif des idéaux galoisiens avec une méthode de calcul utilisant un facteur simple d'une résolvante. En revanche, il est possible d'obtenir dynamiquement un élément primitif d'un idéal galoisien à partir de facteurs non simples (voir [6]). C'est à l'étude générale des résolvantes non nécessairement séparables qu'est consacré cet article.

2. Données et Notations

2.1. **Données.**

- k un corps , $\overline{k}$ une clôture algébrique de k
- $x_1, \ldots, x_n, x$ variables indépendantes sur k
- f polynôme en x de degré n à coefficients dans k
- $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$ le n-uplet formé des racines supposées distinctes de f dans $\overline{k}$:

$$f = a_n \prod_{i=1}^{n} (x - \alpha_i) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

Date: October 2, 2009.
2000 *Mathematics Subject Classification.* Primary 12F10; Secondary 12Y05, 11Y40.
Key words and phrases. Groupe de Galois, Résolvantes, Matrices de Partitions et de Groupes.

2.2. **Notations et rappels généraux.**

Nous reprenons les notations classiques sur les idéaux galoisiens.

Nous notons $\mathfrak{M} = \{P \in k[\boldsymbol{x}] \mid P(\boldsymbol{\alpha}) = 0\}$ l'idéal maximal des $\boldsymbol{\alpha}$-relations et G son groupe de décomposition (i.e. $G.\mathfrak{M} = \mathfrak{M}$, G max) ; G est le groupe de Galois de $\boldsymbol{\alpha}$ sur k.

Nous fixons un sous-groupe L de $\mathfrak{S}_n$, le groupe symétrique de degré n, tel que G soit un sous-groupe de L et donc, en posant

$$I := I^L_{\boldsymbol{\alpha}} = \{P \in k[\boldsymbol{x}] \mid \forall \sigma \in L \ (\sigma.P)(\boldsymbol{\alpha}) = 0\} \quad ,$$

nous avons

$$I \subset \mathfrak{M} \quad .$$

Nous fixons H un sous-groupe de L et $\Theta \in k[x_1, \ldots, x_n]$ un H-invariant L-primitif.

Proposition 1. *Pour tout $\sigma \in L$, le polynôme $\sigma.\Theta$ est H^σ-invariant L-primitif.*

Rappelons que L se décompose en l'union disjointe de ses classes à gauche modulo H :

$$L = \sigma_1 H + \ldots + \sigma_e H$$

et que L/H désigne un système $\{\sigma_1, \ldots, \sigma_e\}$ de représentants de ces classes que nous noterons $(\sigma_i H)$ afin de les identifier comme des éléments de l'ensemble des classes à gauche modulo H.

3. Les G-orbites

Une G-orbite (à gauche) $G\sigma$ de σ dans L/H est l'ensemble formé des $\tau \in L/H$ tels qu'il existe $g \in G$ satisfaisant $g\sigma = \tau$; on a $g\sigma = \tau$ dans L/H si et seulement si $g\sigma H = \tau H$; donc la G-orbite $G(\sigma H)$ de (σH) dans les classes à gauche de L modulo H est formée des classes distinctes (τH) où τ parcourt la G-orbite $G\sigma$ dans L/H.

De la même manière, la G-orbite $G.\Theta$ de Θ est l'ensemble des $g.\Theta$ où g parcourt G.

Soit $\sigma \in L$. A chaque élément $\tau.\Theta$ de la G-orbite de $\sigma.\Theta$ faisons correspondre l'élément (τH) de la G-orbite $G(\sigma H)$.

En nous appuyant sur cette correspondance, nous constatons

(1) que la représentation symétrique de l'action de G sur l'orbite $G.\Theta$ est identique à celle de G sur l'orbite $G(\sigma H)$;

(2) qu'il existe une correspondance biunivoque (triviale) entre l'ensemble des G-orbites de la L-orbite de Θ et celui des G-orbites de L/H et que deux orbites en correspondance sont elles-mêmes en correspondance biunivoque sur leurs éléments. Nous dirons que la correspondance est *doublement biunivoque*.

Ainsi, dans tout ce qui suit certains résultats peuvent être reformulés en choisissant indifféremment les G-orbites dans $L.\Theta$ ou bien dans L/H.

Nous allons voir que c'est en étudiant les G-orbites des évaluations en $\boldsymbol{\alpha}$ des éléments de $L.\Theta$ qu'il est possible d'obtenir de nombreuses informations galoisiennes. En faisant varier H et L, ces informations sont suffisantes pour pouvoir calculer le groupe de Galois G ($L = \mathfrak{S}_n$ suffit) et le corps des racines de f. Lorsque les G-orbites liées aux évaluations sont en correspondance doublement biunivoque avec celles de $L.\Theta$, en vertu de ce que nous venons de voir, elles le seront aussi avec les G-orbites de L/H (c'est le cas des résolvantes séparables). Ce cas à donné lieu à de nombreux résultats. L'objet de cet article porte sur le cas général.

Matrice des partitions (voir [1])

Soit $\mathcal{P}(G, H)$ la partition de $e = [L : H]$ formée par les cardinaux des G-orbites de L/H. Elle ne dépend que des classes de conjugaison respectives de G et H dans L. La matrice des partitions est formée des éléments $\mathcal{P}(G, H)$, où G et H parcourent les représentants des classes de conjugaisons de sous-groupes de L. Ses lignes sont deux-à-deux distinctes.

Matrice des groupes (voir [14])

Soit $\mathcal{G}r(G, H)$ la liste des groupes formée par les actions à gauche de G sur les différentes G-orbites de L/H ; la liste des degrés de ces groupes étant, à une permutation près, identique à $\mathcal{P}(G, H)$. $\mathcal{G}r(G, H)$ ne dépend que des classes de conjugaison respectives de G et H dans L. La matrice des groupes est formée des éléments $\mathcal{G}r(G, H)$, où G et H parcourent les représentants des classes de conjugaisons de sous-groupes de L.

4. La résolvante

La résolvante L-relative de $\boldsymbol{\alpha}$ par Θ (ou bien la résolvante I-relative par Θ) est le polynôme

$$R = \prod_{\Psi \in L.\Theta} (x - \Psi(\boldsymbol{\alpha})) \quad .$$

Une telle résolvante est aussi appelée une *H-résolvante L-relative*. Si $L = \mathfrak{S}_n$, la résolvante ne dépend plus de l'ordre des racines, elle est dite *absolue* ; ce sont les résolvantes absolues qui furent tout d'abord introduites par Lagrange.

La résolvante R montée à la puissance $\#H$ s'identifie au polynôme caractéristique de l'endomorphisme multiplicatif induit par Θ dans l'anneau quotient R/I et nous pouvons l'exprimer également sous la forme :

$$R = \prod_{\sigma \in L/H} (x - (\sigma.\Theta)(\boldsymbol{\alpha})) \quad .$$

Les G-orbites de L/H constituent une partition de L/H (par action à gauche) ; elles induisent une relation d'équivalence sur L/H : deux permutations de L/H sont équivalentes si elles appartiennent à la même G-orbite. Notons $\overline{\sigma}$ la classe d'équivalence $G\sigma$ de σ. Pour $\sigma \in L/H$, considérons le facteur $R_{\overline{\sigma}}$ de R associé à la G-orbite de σ dans L/H :

$$R_{\overline{\sigma}} := \prod_{\tau \in G\sigma} (x - \tau.\Theta(\boldsymbol{\alpha})) \; ;$$

ou exprimé autrement (voir le paragraphe sur les G-orbites)

$$R_{\overline{\sigma}} = \prod_{\Psi \in G.(\sigma.\Theta)} (x - \Psi(\alpha)) \quad ,$$

Le degré du facteur $R_{\overline{\sigma}}$ associé à σ dans L/H est donné par :

$$\deg(R_{\overline{\sigma}}) = \#\{g(\sigma H) \;\mid g \in G\} = [G : G \cap H^\sigma] \tag{1}$$

et nous avons

$$R = \prod R_{\overline{\sigma}} \tag{2}$$

où la somme est étendue aux classes d'équivalences distinctes induites par les G-orbites de L/H. Nous posons :

$$R_\sigma := R_{\overline{\sigma}} \quad .$$

Introduire les facteurs R_σ de la résolvante remplace la comparaison de R à une résolvante séparable lorsque R ne l'est pas (méthode de Lagrange dans [11] qui ne disposant pas des groupes ne pouvait étudier les G-orbites). Lorsqu'une résolvante est séparable, chaque facteur $R_{\overline{\sigma}}$ l'est également ; ce qui signifie, par la théorie de Galois classique (voire [8]), que $R_{\overline{\sigma}}$ est irréductible sur k et qu'à chaque élément de la G-orbite $G\sigma$ de σ dans L/H correspond un et un unique élément de la G-orbite de $\sigma.\Theta(\alpha)$. C'est à partir de cette constatation, qu'à partir de la matrice des partitions, un algorithme de détermination du groupe de Galois ne tenant compte que des degrés des facteurs simples des résolvantes absolues (fonctionnant aussi des résolvantes L-relatives) a pu être élaboré (voir [1]). Auparavant de nombreuses méthodes partielles furent élaborées qui permirent de déterminer les groupes de Galois jusqu'au degré 7 avec des résolvantes absolues ([3], [7], [12], [4]). La méthode de [12] déterminant de groupe de Galois jusqu'au degré 7 disponible dans le logiciel MAPLE y a été implantée par L. Soicher . La méthode de R.P. Stauduhar, basée sur le corollaire 3, construit une chaîne descendante de groupes minimisée par le groupe de Galois (voir [13]). Pour être appliquée, elle nécessite des calculs de résolvantes relatives ne relevant plus seulement du théorème fondamental des fonctions symétriques suffisant au calcul d'une résolvante absolue. Y. Eichenlaub l'a implantée jusqu'au degré 11 par dans le logiciel GP/PARI en faisant appel à des approximations numériques des racines comme le préconisait R.P. Stauduhar.

Résolvantes universelles

Ce sont des résolvantes qui sont séparables quelque soit le polynôme séparable f. Il en existe 2 bien connues. Celle de Cayley associée à l'un des six groupes métacycliques principaux de $\mathfrak{S}_5$ et celle par le déterminant Vandermonde δ associée au groupe alterné. Elles ont toutes deux la propriété que le discriminant de la résolvante est divisible par une puissance de celui, non nul, du polynôme f et que le quotient de la division ne peut être nul (voir [5] et [2] pour la résolvante de Cayley). Ceci constitue une condition nécessaire et suffisante pour que la résolvante soit universelle. Pour illustrer les résolvantes universelles, choisissons la résolvante (absolue) de f par $\delta = \prod_{1\leq i<j\leq n}(x_i - x_j)$:

$$R = (x^2 - \delta^2(\boldsymbol{\alpha})) = (x - \delta(\boldsymbol{\alpha}))(x + \delta(\boldsymbol{\alpha})).$$

On voit immédiatement que si les racines de f sont distinctes, nous n'aurons jamais $\delta(\boldsymbol{\alpha}) = -\delta(\boldsymbol{\alpha})$. Afin de mettre en lumière ce qui est énoncé plus haut, considérons le discriminant $4\delta^2(\boldsymbol{\alpha})$ de R ; étant donné que $\delta^2(\boldsymbol{\alpha})$ est à une constante près le discriminant de f, celui de R ne peut s'annuler qu'avec celui de f.

Si la question de l'existence d'une résolvante universelle n'est pas encore tranchée pour chaque groupe H, il existe néanmoins une infinité d'H-invariants L-primitifs séparables (i.e. la résolvante est sans racine multiple) (voir [1]).

5. Résolvantes et groupes de Galois

Dans [2], se trouvent de nombreux résultats portant sur les racines de multiplicité supérieure à 1 dans la résolvante. Le théorème suivant (un peu reformulé) en est l'un d'eux :

Théorème 2 ([2], Théorème 6.10)**.** *Supposons que $\theta = \Theta(\boldsymbol{\alpha})$ soit une racine simple (i.e. de son polynôme minimal sur k) de multiplicité $m \geq 1$ de R, la résolvante L-relative de $\boldsymbol{\alpha}$ par Θ, avec $H = Stab_L(\Theta) \subset L$ et $G = Gal_k(\boldsymbol{\alpha}) \subset L$. Soit*

$$\mathcal{T} := \{\Psi \in L.\Theta \ \mid \ \Psi(\boldsymbol{\alpha}) = \theta\}.$$

Notons

$$M = Stab_L(\mathcal{T}).$$

i) Alors

$$\mathrm{Gal}(k(\boldsymbol{\alpha})/k(\theta)) = Stab_G(\theta) = G \cap M,$$

$G \cap H \subset G \cap M$ *,* $[G : G \cap H] = m[k(\theta) : k]$ *et* $[k(\theta) : k] = [G : G \cap M]$.

ii) En particulier, si θ est une racine simple de R alors $M = H$.

Voici le corollaire de ce théorème conçut par Stauduhar pour la détermination du groupe de Galois :

Corollaire 3. *(i) Si $\theta = \Theta(\boldsymbol{\alpha})$ est une racine simple sur k de la résolvante R de $\boldsymbol{\alpha}$ par Θ alors $G = \mathrm{Gal}_k(\boldsymbol{\alpha})$ est un sous-groupe du groupe $H = \mathrm{Stab}_L(\Theta)$.*
(ii) Si la résolvante R possède un facteur linéaire simple dans k alors le groupe de Galois de $\boldsymbol{\alpha}$ sur k est un sous-groupe d'un conjugué de H dans L.

Exemple 4. La résolvante par le déterminant de Vandermonde étant universelle, si le discriminant de f est un carré dans k alors le groupe de Galois G est pair car il est un sous-groupe du groupe alterné qui est distingué dans $\mathfrak{S}_n$.

Remarque 5. Supposons que $\mathcal{T} = \{\sigma_1.\Theta, \ldots, \sigma_m.\Theta\}$. Alors M s'exprime aussi sous la forme :

$$M = \mathrm{Stab}_L(\sigma_1 H + \cdots + \sigma_1 H) \tag{3}$$

(les classes à gauche étant nécessairement disjointes). En effet, pour tout $l, \sigma, \tau \in L$, l'égalité $l\sigma.\Theta = \tau.\Theta$ est équivalente à $l\sigma\tau^{-1}(\tau.\Theta) = \tau.\Theta$; comme $\tau.\Theta$ est un H^τ-invariant L-primitif (voir Proposition 1), l'égalité $l\sigma.\Theta = \tau.\Theta$ est donc équivalente à $l\sigma\tau^{-1} \in H^\tau = \tau H \tau^{-1}$; c'est-à-dire $l\sigma \in \tau H$.

Nous voyons ici qu'il est possible de reformuler les théorèmes de diverses façons puisqu'il y a une correspondance bijective entre les orbites portant sur les classes à gauche σH de H (ou bien les orbites dans L/H) et celles portant sur les $\sigma.\Theta$.

Théorème 6. *Soit h un facteur de R k-irréductible et séparable (i.e. toutes ses racines sont simples) sur k de la résolvante R et soit $m \geq 1$ sa multiplicité dans R. Alors il existe s permutations $\sigma_1, \ldots, \sigma_s$ de L/H telles que pour $i \neq j$ la G-orbite de σ_i dans L/H est disjointe de celle de σ_j (i.e. $\overline{\sigma_i} \neq \overline{\sigma_j}$ si $i \neq j$) et telles que*

$$h^m = R_{\sigma_1} \cdots R_{\sigma_s} \quad .$$

Corollaire 7. *Sous les hypothèses du théorème précédent, il existe $m_1, \ldots, m_s$ des entiers strictement positifs tels que*

$$m = m_1 + \cdots + m_s \quad ;$$

et pour $i = 1, \ldots, s$
(i)

$$R_{\sigma_i} = h^{m_i} \quad .$$

(ii) la G-orbite de $\sigma_i.\Theta$ est de cardinal $deg(h).m_i$.
(iii) l'action du groupe de $\mathrm{Gal}_k(h)$ sur $\{1, \ldots, d = \deg(h)\}$ est une représentation symétrique de l'action (à gauche) de G sur l'ensemble $\{\tau_1, \ldots, \tau_d\}$ des permutations dans L/H appartenant à la G-orbite de σ_i telles que $\tau_1.\Theta(\boldsymbol{\alpha}), \ldots, \tau_d.\Theta(\boldsymbol{\alpha})$ sont les d racines distinctes de h.

En particulier, si h est un facteur simple de R alors $s = m = 1$, il existe un unique $\overline{\sigma}$ tel que $h = R_{\overline{\sigma}}$, la G-orbite de (σH) est de cardinal $\deg(h)$ et le groupe de Galois de h sur k est une représentation symétrique de l'action (à gauche) de G sur l'orbite $G(\sigma H)$.

Corollaire 8. *Soit la partition $\mathcal{P}(G, H) = (p_1, \ldots, p_r)$ associée à G et H dans la matrice des partitions de L. Si h est un facteur séparable de degré d et de multiplicité $m \geq 1$ dans une H-résolvante L-relative alors il existe s entiers distincts $i_1, \ldots, i_s$ dans $[\![1, r]\!]$ tels que*

$$md = p_{i_1} + \cdots + p_{i_s} \quad \textit{avec, pour } j = 1, \ldots, s, \quad p_{i_j} = m_j d$$

où les m_i sont les s entiers > 0 du corollaire 7.

En particulier, si h est un facteur simple de R alors $s = 1$, $m_1 = 1$, $\deg(h) = p_{i_1}$.

Comme les lignes de la matrice de partitions sont deux-à-deux distinctes et qu'il existe toujours des H-résolvantes séparables, le cas particulier de ce corollaire induit le théorème suivant :

Théorème 9. *([1]) Pour tout groupe L contenant le groupe de Galois d'un polynôme, il est toujours possible de déterminer le groupe de Galois de ce polynôme avec les degrés des facteurs de ses résolvantes L-relatives et la matrice des partitions. En particulier, on peut prendre $L = \mathfrak{S}_n$.*

Remarque 10. Le *(iii)* du corollaire 7 est doublement exploitable :
(1) pour déterminer rapidement le groupe de Galois de f avec les groupes de Galois des ses facteurs et pas seulement leur degré ; la matrice des partitions est remplacée par celle des groupes ;
(2) pour calculer des polynômes de groupe de Galois donné (problème de Galois inverse) (voir et [14], [9] et [10]) : si le groupe de Galois de f est connu, ceux des facteurs de ses résolvantes le sont également ; ces facteurs sont les nouveaux polynômes construits.

Remarque 11. Il est possible de généraliser en n'imposant pas que le polynôme h du théorème soit k-irréductible tout en restant sans racine multiple. En ce cas, il faudra faire agir (à gauche) G sur la réunion des G-orbites concernées par ses racines pour déterminer son groupe de Galois. Ceci est utilisable avec le (2) de la remarque précédente pour calculer des polynômes réductibles de groupe de Galois donné. Par exemple, le groupe de Galois de la résolvante est, si elle est séparable, la représentation symétrique de l'action de G sur L/H.

Les groupes de Galois des facteurs (irréductibles ou non) de R sur k sont aussi déterminables à partir du théorème 2. Prenons pour h un facteur de R sur k sans racine multiple et associons à chacune de ses racines β l'ensemble M du théorème que nous notons M_β. Notons $\boldsymbol{\beta}$ un uplet constitué des racines distinctes de h. Comme, si H_1 et H_2 sont des sous-groupes du groupe de Galois de f sur k, nous avons :

$$k(\boldsymbol{\alpha})^{H_1} \cup k(\boldsymbol{\alpha})^{H_2} = k(\boldsymbol{\alpha})^{H_1 \cap H_2} \quad ,$$

le théorème 2 possède pour corollaire :

Corollaire 12. *Sous les hypothèses du théorème 2 et avec les notations ci-dessus, en posant*

$$V = \bigcap_{\beta | h(\beta)=0} M_\beta \quad ,$$

nous avons

$$\mathrm{Gal}(k(\boldsymbol{\alpha})/k(\boldsymbol{\beta})) = G \cap V \quad .$$

Ce qui signifie que le groupe de Galois de h sur k est isomorphe à $G/G \cap V$.

Le cas séparable (i.e. h est de multiplicité 1 dans R) a été étudié dans [1] et [14]. En particulier, en prenant $h = R$, nous obtenons :

Théorème 13. *([1]) Fixons $L = S_n$ et supposons que $H \notin \{S_n, A_n, D_4, V_4\}$. Si la résolvante R est sans racine multiple alors $k(\boldsymbol{\alpha}) = k(\boldsymbol{\beta})$.*

Exemple 14. Prenons $L = S_4$, $H = C_4$, le groupe cyclique, et $G = D_4$, le groupe diédral, $f = x^4 - 2$ et

$$\Theta = x_2x_4^2 + x_3x_2^2 + x_4x_1^2 + x_1x_3^2 \quad .$$

La résolvante se factorise ainsi sur $\mathbb{Q}$:

$$R = x^2(x^4 + 512).$$

Mettons-nous dans l'hypothèse où G est inconnu. Seuls le sont L, H, Θ et R. Il existe une G-orbite de cardinal 4 correspondant au facteur simple $x^4 + 512$. D'après la matrice des partitions de $\mathfrak{S}_4$ (donnée dans [1]), le polynôme f étant irréductible sur $\mathbb{Q}$, le groupe de Galois ne peut être que C_4 ou D_4.

Le groupe de Galois de $x^4 + 512$ étant identique à celui de f, la non séparabilité du facteur $h(x) = x$ ne permet pas de conclure sur G.

Sans perte de généralité, nous pouvons choisir pour C_4 un bon conjugué tel que $D_4 = C_4 + \sigma C_4$; par exemple $C_4 =< (1, 2, 3, 4) >$ et $\sigma = (1, 3)$. Le polynôme h^2 est la résolvante D_4-relative de $\boldsymbol{\alpha}$ par Θ.

Nous avons $m = 2$. Ou bien il existe une G-orbite de cardinale 2 et en ce cas $s = 1$, $m = m_1$ et $G = D_4$ ou bien il existe deux G-orbites de cardinal 1 et en ce cas $s = 2$, $m_1 = m_2 = 1$ et $G = C_4$. Dans le premier cas, la non séparabilité du facteur h provient de la D_4-orbite $\{C_4, \sigma C_4\}$, dans le second, elle provient des deux C_4-orbites distinctes $\{C_4\}$ et $\{\sigma C_4\}$.

Pour déterminer que D_4 est le groupe de Galois de x^4-2 sur $\mathbb{Q}$, il existe de nombreuses possibilités : remplacer G par $\mathrm{Stab}_G(1)$ et considérer f dans $k(\alpha_1)$, réaliser une transformation de Tchirnhaus (i.e. calculer une résolvante par $H = S_1 \times S_{n-1}$ de même groupe de Galois que f), changer de groupe test H, changer d'invariant ... La poursuite de cet exemple dans le paragraphe suivant en est une.

Soit $\tau \in L$. La G-orbite de τH est associée à h si $\tau.\Theta(\boldsymbol{\alpha})$ est une racine de h. Dans ce cas, à toute classe de la G-orbite, on peut associer une racine de h et toute racine de h est donnée par au moins une classe de la G-orbite ; c'est-à-dire qu'il existe alors une application surjective entre la G-orbite et les racines de h. Si cette application est injective alors on peut appliquer à h et à la G-orbite concernée tous les résultats relavant des facteurs simples des résolvantes puisque h est la résolvante G-relative

de $\boldsymbol{\alpha}$ par Θ (i.e. celle obtenue avec $\mathfrak{M}$ à la place de I). Dans le cas contraire, nous disposons ici de nouveaux théorèmes pour extraire de la résolvante des informations sur sur le groupe de Galois et sur les relations entre les racines de f, étudiées dans le prochain paragraphe.

6. Résolvantes et idéaux galoisiens

Définition 15. Soient deux idéaux galoisiens I et J. Un polynôme P de $k[x_1, \ldots, x_n]$ est un *élément I-primitif* de J si

$$J = I + \ < P > \quad .$$

Théorème 16. *([15]) Soit K un sous-ensemble de $\mathfrak{S}_n$ tel que $I^L_{\boldsymbol{\alpha}} \subset I^K_{\boldsymbol{\alpha}} \subset \mathfrak{M}$. Un polynôme P est un élément $I^L_{\boldsymbol{\alpha}}$-primitif de l'idéal $I^K_{\boldsymbol{\alpha}}$ si et seulement si :*

$$GK = \{\sigma \in L \ \mid \ (\sigma.P)(\boldsymbol{\alpha}) = 0\} \quad .$$

Rappelons que GK est le plus grand ensemble définissant $J = I^K_{\boldsymbol{\alpha}}$; c'est l'injecteur de J dans $\mathfrak{M}$.

Le théorème suivant décrit comment construire et décrire un nouvel idéal galoisien à partir d'un facteur de R de l'idéal I :

Théorème 17. *Soit H un sous-groupe d'un sur-groupe L du groupe de Galois G de $\boldsymbol{\alpha}$ sur k. Soient Θ un H-invariant L-primitif et R la résolvante de $\boldsymbol{\alpha}$ par Θ.*

Soit un facteur h de R qui soit séparable (i.e. ses racines sont simples) et irréductible sur k. Notons m sa multiplicité dans R. Soient les s permutations $\sigma_1, \ldots, \sigma_s$ du Théorème 6 qui satisfont $\overline{\sigma_i} \neq \overline{\sigma_j}$ pour $i \neq j$ et

$$h^m = R_{\overline{\sigma_1}} \cdots R_{\overline{\sigma_s}} \quad .$$

Posons

$$U := \sigma_1 H + \cdots + \sigma_s H.$$

Alors $h(\Theta)$ est un élément $I^L_{\boldsymbol{\alpha}}$-primitif de l'idéal $I^U_{\boldsymbol{\alpha}}$:

$$I^U_{\boldsymbol{\alpha}} = I^L_{\boldsymbol{\alpha}} + \ < h(\Theta) > \quad .$$

Nous pouvons exprimer ce théorème sous cette autre forme :

Théorème 18. *Supposons que θ soit une racine simple d'un facteur k-irréductible h de la résolvante R. Soit T l'ensemble des éléments de L/H en relation avec les multiplicités de θ dans R :*

$$T := \{\sigma \in L/H \ \mid \ (\sigma.\Theta)(\boldsymbol{\alpha}) = \theta\}.$$

Alors $h(\Theta)$ est un élément $I_{\boldsymbol{\alpha}}^L$-primitif de l'idéal $I_{\boldsymbol{\alpha}}^{\bigcup_{\sigma\in T}\sigma H}$:

$$I_{\boldsymbol{\alpha}}^{\bigcup_{\sigma\in T}\sigma H} = I_{\boldsymbol{\alpha}}^L + \ < h(\Theta) > \quad .$$

Remarque 19. Les ensembles T du théorème 18 et $\mathcal{T}$ du théorème 2 sont en bijection : à $\sigma \in T$ on associe $\sigma.\Theta \in \mathcal{T}$.

Remarque 20. Dans chacun de ces théorèmes, nous avons retiré des classes à gauche de L modulo H pour définir le nouvel idéal : dans le premier, nous n'avons gardé qu'un représentant dans chaque G-orbite et dans le second nous avons pris toutes les permutations d'une même G-orbite donnant lieu à la même racine. Ceci est possible puisque, pour tout ensemble S de permutations, on a

$$I_{\boldsymbol{\alpha}}^S = I_{\boldsymbol{\alpha}}^{GS} \quad ;$$

ce qui signifie qu'on peut remplacer $\sigma_i H$ par $G\sigma_i H$. Soient donc U et T donnés respectivement par les théorèmes 17 et 18. On a

$$GU = G\sigma_1 H + \cdots + G\sigma_s H = \bigcup_{\sigma\in T} G\sigma H = G \bigcup_{\sigma\in T} \sigma H$$

Le nouvel idéal s'exprime alors sous les différentes formes suivantes :

$$I_{\boldsymbol{\alpha}}^U = I_{\boldsymbol{\alpha}}^{\bigcup_{i=1}^s G\sigma_i H} = I_{\boldsymbol{\alpha}}^{\bigcup_{\sigma\in T}\sigma H} \quad .$$

Rappelons que si $E_1, \ldots E_r$ sont des ensembles de permutations alors (voir [15]) :

$$I_{\alpha}^{\bigcup_{i=1}^r E_i} = \bigcap_{i=1}^n I_{\boldsymbol{\alpha}}^{E_i} \quad .$$

Remarque 21. Dans cette vision algébriste, il n'est pas nécessaire de renuméroter les racines de f comme pour les calculs numériques. Il suffit de considérer un n-uplet $\boldsymbol{\alpha}$ de racines de f qui satisfait les conditions. Il est néanmoins possible de réaliser les calculs en identifiant les racines : il suffit de les ordonner afin que le n-uplet choisit satisfasse les bonnes conditions.

Remarque 22. Dans tout cet article, nous avons supposé que L est un groupe contenant le groupe de Galois G. Si ce n'est pas le cas, il est toujours possible de construire à partir de I un idéal galoisien J :

$$I \subset J \subset \mathfrak{M}$$

tel que l'injecteur de J soit un groupe et qui, par conséquent, contient le groupe de Galois G (voir [16]). Cette remarque s'applique également à l'idéal I_α^U construit à partir du théorème 17.

On peut se demander dans quelle mesure la résolvante n'apporte rien (i.e. $I = J$). Si R est séparable et irréductible sur k ou si

$$R = (x - \theta)^m$$

avec $\theta \in k$ (ce qui est nécessaire lorsque k est un corps parfait) alors $L = GU$ et $I = J$. En toute généralité, $J = I$ si et seulement si $GU = L$ puisque GU est l'injecteur de J dans $\mathfrak{M} = I_{\boldsymbol{\alpha}}$ (le plus grand ensemble définissant J avec $\boldsymbol{\alpha}$).

Notre théorème est particulièrement intéressant lorsque le groupe de Galois G contient le groupe test H comme le montre l'exemple qui termine notre présentation :

Exemple 23. Reprenons l'exemple 14 avec $L = \mathfrak{S}_4$.
L'idéal $I := I_{\boldsymbol{\alpha}}^{\mathfrak{S}_4}$ est engendré par les modules de Cauchy de f :

$$< x_4+x_3+x_2+x_1, x_3^2+x_2x_3+x_1x_3+x_2^2+x_1x_2+x_1^2, x_2^3+x_1x_2^2+x_1^2x_2+x_1^3, x_1^4-2 > \quad .$$

Le théorème 18 nous dit comment construire l'idéal galoisien $J = I_{\boldsymbol{\alpha}}^{D_4}$:

$$J = I + < h(\Theta) >= I + < \Theta >=< x_4 + x_3, x_3^2 + x_1^2, x_2 + x_1, x_1^4 - 2 > \quad .$$

En effet, si $G = D_4$ alors $J = I_{\boldsymbol{\alpha}}^{C_4}$ donc $J = I_{\boldsymbol{\alpha}}^{D_4}$ (puisque $\mathrm{Inj}(J, \mathfrak{M}) = GC_4 = D_4$) et si $G = C_4$ alors $J = I_{\boldsymbol{\alpha}}^{C_4 + \sigma C_4} = I_{\boldsymbol{\alpha}}^{D_4}$.

Sur cet exemple, il existe de nombreuses façons de conclure. Par exemple, comme $x_3^2 + x_1^2$ est irréductible sur $k[x_1]/f(x_1)$, il n'existe pas de relation linéaire en α_3 sur $k(\alpha_1, \alpha_2)$. Donc $J = \mathfrak{M}$ et $G = D_4$.

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] E.H. Berwick. On soluble sextic equations. *Proc. London Math. Soc.a*, 29:1–28, 1929.

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

[5] A. Cayley. On a new auxiliary equation in the theory of equation of the fifth order. *Philosophical Transactions of the Royal Society of London*, CLL, 1861.

[6] G.M. Diaz-Toca. Galois theory, splitting fields and computer algebra. *J. Symb. Comput.*, 41(11):1174–1186, 2006.

[7] H.O. Foulkes. The resolvents of an equation of seventh degree. *Quart. J. Math. Oxfor*, 2(1):9–19, 1931.

[8] E. Galois. *Oeuvres Mathématiques, éditées par la SMF*. Gauthier-Villars, Paris, 1897.

[9] I. Gil-Delessale and A. Valibouze. Galois inverse problem for some subgroups of degree 12. Publication interne 96-13, Equipe Max du LIX (Lab. d'Info. de l'Ecole Polytechnique), 1996. http://www.lix.polytechnique.fr/ max/publications.

[10] J. Klüners and G. Malle. Explicit Galois realization of transitive groups of degree up to 15. *J. Symbolic Comput.*, 30(6):675–716, 2000. Algorithmic methods in Galois theory.

[11] J.-L. Lagrange. Réflexions sur la résolution algébrique des équations. *Prussian Academy*, 1770.

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

[13] R.P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.

[14] A. Valibouze. Computation of the Galois groups of the resolvent factors for the direct and inverse Galois problems. In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Comput. Sci.*, pages 456–468. Springer, Berlin, 1995.

[15] 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. (Version longue du rapport LIP6 1997/014).

[16] A. Valibouze. Classes doubles, idéaux de Galois et résolvantes. *Rev. Roum. de Math. Pures et Appl.*, 2005. à paraître.

LIP6, UPMC, 4, place Jussieu, 75252 Paris Cedex 05

E-mail address: annick.valibouze@upmc.fr www-spiral.lip6.fr/~avb/