HAL open science

La Résolvante de Lagrange et ses Applications

Annick Valibouze

To cite this version:

Annick Valibouze. La Résolvante de Lagrange et ses Applications. 2008. hal-00376921

HAL Id: hal-00376921

https://hal.science/hal-00376921v1

Preprint submitted on 24 Apr 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

LA RÉSOLVANTE DE LAGRANGE ET SES APPLICATIONS

ANNICK VALIBOUZE

Résumé

Dans cet article, les changements de représentations d'un groupe sont utilisés pour décrire son action en tant que groupe de Galois d'un polynôme sur les racines des facteurs simples d'une quelconque de ses résolvantes de Lagrange. Ainsi est déterminé le groupe de Galois de la résolvante mais aussi celui de chacun de ses facteurs. Nous exposons ensuite différentes applications. En particulier, par ce biais, sont retrouvés des résultats classiques de la théorie de Galois constructive.

Abstract

This paper describes the action of the Galois group of a univariate polynomial on the factors of any of its resolvents.

Introduction

En introduisant la résolvante J.L. Lagrange (voir [13]) unifia les résultats obtenus par ses prédécesseur pour résoudre les équations jusqu'au quatrième degré. Avec ses résolvantes, prélude aux célèbres sommes de Gauss, il introduisit les groupes de permutations dans la résolution des équations algébriques. L'idée de J.L. Lagrange est de faire agir un sous-groupe L du groupe symétrique sur un polynôme r de plusieurs variables et d'observer ce qui se passe quand ces variables se spécialisent en les solutions de l'équation. Plus tard, E. Galois identifia le groupe de l'équation comme celui échangeant les racines du polynôme minimal d'un élément primitif du corps des solutions de l'équation ; il fit agir ce groupe sur les spécialisations ; cette façon d'étudier le groupe de l'équation, appelé aujourd'hui Groupe de Galois, restreint le champs d'investigations lorsqu'il s'agit de le déterminer. En effet, si une permutation n'appartient pas au groupe de Galois, l'action n'est pas définie (voir Paragraphe 2) et, a priori, seule l'identité appartient de façon certaine au groupe de Galois. Par la suite, les travaux d'E. Artin permirent d'énoncer la correspondance galoisienne. Si ce point de vue apporte une vision théorique fructueuse et utile, il reste difficile de mener des calculs dans le corps des racines avec un groupe de k-automorphismes non identifiés a priori.

Pour la détermination du groupe de Galois d'un polynôme et de son corps des racines, le point de vue de J.L. Lagrange est le plus fructueux. Le polynôme r sur

Date: April 24, 2009.

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

Key words and phrases. Groupe de Galois, Résolvantes, Matrices de Partitions et de Groupes.

lequel agissent les permutations de L est un invariant (précisément un invariant L-primitif) d'un sous-groupe H de L. Par conséquent, il est possible de s'affranchir du polynôme r pour ne réaliser que des pré-calculs groupistiques.

Dans cet article, cette démarche groupistique est poussée jusqu'au point de prédéterminer les groupes de Galois des résolvantes (et donc de leurs facteurs) d'un polynôme d'une variable par de simples changements de représentations du groupe de Galois de ce polynôme. Il aboutit aux matrices de groupes (déterminées différemment dans [18]).

Ce travail s'inscrit dans la suite des travaux d'E.H. Berwick (voir [4]), de Foulkes (voir [9]) et de ceux, plus récents, de J. Mc Kay et G. Butler (voir [5]) et de bien d'autres. Il reprend et complète l'article [1] aboutissant aux matrices dites de partitions (détermination des degrés des facteurs des résolvantes).

Cet article décrit clairement la composante résolvante de la théorie de Galois constructive. Seule la définition classique de la résolvante est considérée car ne sont abordés ni son aspect calculatoire ni celui de la détermination du groupe de Galois obtenue simultanément au calcul du corps de décomposition du polynôme (voir [7], [19] et [20]). Via le livre de N. Tchebotarev (voir [17]), le lecteur pourra pousser plus avant l'étude de la théorie de Galois constructive du point de vue des idéaux poursuivant ainsi celui de J.L. Lagrange.

Afin que cet article soit abordable par les non spécialistes, les trois premiers paragraphes sont dévolus à une introduction rapide à la théorie de Galois unifiant différentes approches : idéal des relations, groupe de Galois en tant que groupe de permutations et en tant que groupe des k-automorphismes du corps des racines, correspondance galoisienne. Certaines nouvelles démonstrations de théorèmes connus y sont proposées. Les matrices de groupes sont définies au quatrième paragraphe. Les paragraphes 5 à 9 sont consacrés à la résolvante, son groupe de Galois, les groupes de Galois de ses facteurs, le corps de ses racines. Le dixième paragraphe illustre les résultats avec des résolvantes connues. Le dernier paragraphe est consacré aux applications.

Données et notations préliminaires

Nous fixons n variables $x_1, x_2, \ldots, x_n$ algébriquement indépendantes. Soit $\alpha_1, \ldots, \alpha_n$ une numérotation des n racines d'un polynôme f de degré n à coefficients dans un corps parfait k. Posons $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$.

Le corps des racines du polynôme f est noté $k(\underline{\alpha})$. Ce corps est la plus petite extension algébrique de k dans lequel le polynôme f se factorise entièrement en facteurs linéaires ; ce qui fait qu'il s'appelle aussi corps de décomposition de f.

Le groupe des permutations d'un ensemble E est noté S_E et si E est l'ensemble $\{1, 2, \ldots, n\}$ alors S_E est le groupe symétrique de degré n, noté aussi S_n. Ce groupe agit naturellement sur les polynômes de $k[x_1, \ldots, x_n]$ par permutations des indices des variables : $\sigma.p = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ pour $p \in k[x_1, \ldots, x_n]$ et $\sigma \in S_n$.

1. Idéal des relations, groupe de Galois et corps des racines

L'*idéal* $\mathfrak{M}$ *des* $\underline{\alpha}$*-relations (sur* k*)* est défini par :

$$\mathfrak{M} = \{r \in k[x_1, \ldots, x_n] \ \mid \ r(\underline{\alpha}) = 0\}$$

et considérons l'anneau quotient :

$$K_{\underline{\alpha}} = k[x_1, \ldots, x_n]/\mathfrak{M} \quad .$$

Nous constatons que $\mathfrak{M}$ est défini en observant l'évaluation d'un polynôme r en les racines du polynôme f. C'est donc le point de vue de J.L. Lagrange qui s'applique.

Le *groupe de Galois* G *de* $\underline{\alpha}$ *sur* k se définit comme le sous-groupe du groupe symétrique S_n stabilisant globalement l'idéal $\mathfrak{M}$:

$$G = \{\sigma \in S_n \ \mid \ \sigma.\mathfrak{M} = \mathfrak{M}\} \ .$$

où $\sigma.\mathfrak{M}$ est l'ensemble des permutés $\sigma.r$ où r parcourt $\mathfrak{M}$.

Remarque 1. Ici, nous touchons le point clef qui donne la préférence au point de vue de J.L. Lagrange. Sans erreurs et sans connaître G a priori, il est possible de faire agir toute permutation du groupe symétrique S_n car il s'agit de polynômes génériques sur lesquels l'action est définie. En effet, nommons $\alpha_1 = 1, \alpha_2 = j$ et $\alpha_3 = j^2$ les racines du polynôme $x^3 - 1$ et choisissons la permutation $\sigma = (1, 2)$. Nous avons l' $\underline{\alpha}$-relation $x_2^2 - x_3$ inexistante pour un polynôme générique. A quoi correspondrait $\sigma.(\alpha_2^2)$?, à $\alpha_1^2 = 1$ ou bien à $\sigma.\alpha_3 = \alpha_3$? L'action n'est donc pas définie si σ n'appartient pas à G qui est précisément le plus grand sous-ensemble de S_n pour lequel l'action ait un sens.

Par le k-morphisme d'évaluation de l'anneau $k[x_1, \ldots, x_n]$ dans le corps $k(\underline{\alpha})$ qui à x_i associe α_i, de noyau $\mathfrak{M}$, l'anneau quotient $K_{\underline{\alpha}}$ est isomorphe au corps $k(\underline{\alpha})$.

La dimension $\dim_k(k(\underline{\alpha}))$ du corps $k(\underline{\alpha})$ en tant que k-espace vectoriel, appelée aussi degré de l'extension $k(\underline{\alpha})/k$, satisfait l'identité :

$$\dim_k(k(\underline{\alpha})) = \mathrm{Card}(G) \quad . \tag{1}$$

En effet, le k-isomorphisme entre les corps $K_{\underline{\alpha}}$ et $k(\underline{\alpha})$ induit l'égalité :

$$\dim_k(k(\underline{\alpha})) = \dim_k(K_{\underline{\alpha}}) \quad .$$

Or la dimension $\dim_k(K_{\underline{\alpha}})$ est identique au cardinal de la variété V de $\mathfrak{M}$ puisque cet idéal est radical (il est maximal puisque $k(\underline{\alpha})$ est un corps). La variété V est l'ensemble des $(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ où σ parcourt G (voir [19]). Comme les racines de f sont distinctes deux-à-deux, le cardinal de V est identique à celui du groupe de Galois G.

2. Groupe de Galois et groupe des k-automorphismes

Soit E une k-algèbre. Un k-endomorphisme de E (en tant que k-algèbre) est une application ϕ de E dans E telle que si $e_1, e_2 \in E$ et $\lambda \in k$ alors $\phi(\lambda) = \lambda$, $\phi(e_1 e_2) = \phi(e_1)\phi(e_2)$ et $\phi(e_1 + e_2) = \phi(e_1) + \phi(e_2)$. Si ϕ est surjectif alors ϕ est un k-automorphisme. L'ensemble de k-automorphismes de E est le groupe noté $\mathrm{Aut}_k(E)$.

Chaque k-endomorphisme de $k(\underline{\alpha})$ laissant invariants les coefficients de f, il est induit par une permutation de ses racines. Donc tout k-endomorphisme de $k(\underline{\alpha})$ est un k-automorphisme et nous pouvons définir une représentation, dite *associée à* $\underline{\alpha}$, du groupe $Aut_k(k(\underline{\alpha}))$ dans S_n :

$$\begin{array}{ccc} Aut_k(k(\underline{\alpha})) & \longrightarrow & S_n \\ \phi & \mapsto & \sigma_\phi : \alpha_{\sigma_\phi(i)} = \phi(\alpha_i) \end{array} \quad .$$

Notons $\mathcal{F}$ le k-isomorphisme du corps $K_{\underline{\alpha}}$ dans le corps $k(\underline{\alpha})$ qui à p associe $p(\underline{\alpha})$.

Lemme 2. *Soit $\sigma \in G$. Soit le k-endomorphisme de permutations $\mathcal{G}_\sigma$ de $K_{\underline{\alpha}}$ qui à p associe $\sigma.p$. Alors $\mathcal{G}_\sigma$ est un k-automorphisme. Par conséquent, l'application*

$$\phi_\sigma = \mathcal{F}\mathcal{G}_\sigma\mathcal{F}^{-1}$$

est un k-automorphisme de $k(\alpha_1, \ldots, \alpha_n)$ satisfaisant

$$\phi_\sigma(i) = \alpha_{\sigma(i)}$$

pour tout $i \in [\![1, n]\!]$.

Démonstration. Car, par définition, la condition $\sigma \in G$ est équivalente à $\sigma.\mathfrak{M} = \mathfrak{M}$. □

Lemme 3. *Le groupe G est la représentation de $Aut_k(k(\alpha_1, \ldots, \alpha_n))$ dans S_n associée à $\underline{\alpha}$ et l'image réciproque de $\sigma \in G$ par cette représentation est le k-automorphisme ϕ_σ.*
Soient $p \in k(\underline{\alpha})$ et $P = \mathcal{F}^{-1}(p)$ appartenant à $K_{\underline{\alpha}}$. Alors pour tout $\sigma \in G$:

$$\phi_\sigma(p) = (\sigma.P)(\alpha_1, \ldots, \alpha_n) \quad .$$

Démonstration. Soient $\phi \in Aut_k(k(\alpha_1, \ldots, \alpha_n))$ et $R \in k[x_1, \ldots, x_n]$ tel que $r = R(\alpha_1, \ldots, \alpha_n) = 0$. Posons $\sigma = \sigma_\phi$. Nous avons

$$(\sigma.R)(\alpha_1, \ldots, \alpha_n) = R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = R(\phi(\alpha_1), \ldots, \phi(\alpha_n)) = \phi(r) = 0$$

car ϕ est un k-automorphisme. Donc $\sigma \in G$. □

Notation 4. D'après les deux lemmes précédents et ayant fixé la numérotation des racines de f, pour tout $\beta \in k(\alpha_1, \ldots, \alpha_n)$ et tout $\sigma \in G$, nous pouvons poser :

$$\beta^\sigma = \phi_\sigma(\beta) \quad .$$

Remarque 5. En appliquant la notation 4, G est le plus grand sous-groupe de S_n assurant que pour tout $\sigma \in G$ et $\gamma \in k(\underline{\alpha})$ si $\gamma = 0$ alors $\gamma^\sigma = 0$. La notation 4 n'a de sens que pour $\sigma \in G$. En revanche, pour $P \in k[x_1, \ldots, x_n]$ et $\sigma \in S_n$, la notation $(\sigma.P)(\underline{\alpha})$ en a un (voir Remarque 1).

Convention 6. Lorsque nous voudrons désigner une représentation symétrique quelconque de $Aut_k(k(\alpha_1, \ldots, \alpha_n))$ dans S_n, nous l'appellerons *groupe de Galois de f sur k* et nous la noterons $\mathrm{Gal}_k(f)$.

Note Le groupe $\mathrm{Aut}_k(k(\underline{\alpha}))$ est aussi communément appelé le groupe de Galois de l'extension $k(\underline{\alpha})/k$. Par abus de langage, le groupe G (et donc aussi $\mathrm{Gal}_k(f)$) est souvent appelé le groupe de Galois de cette extension.

3. La correspondance galoisienne

Le polynôme minimal sur k de tout β appartenant à $k(\alpha_1, \ldots, \alpha_n)$ est donné par :

$$Min_{\beta,k} = \prod_{\gamma \in \{\beta^g \mid g \in G\}} (x - \gamma) \tag{2}$$

Cette identité est démontrable par de l'algèbre linéaire sur le k-espace vectoriel $K_{\underline{\alpha}}$ (voir [19]).

D'après le théorème de l'élément primitif de J.L. Lagrange (voir Note 31), il existe $v \in k(\underline{\alpha})$ tel que

$$k(\underline{\alpha}) = k(v) \quad .$$

Cet élément s'exprime sous la forme

$$v = V(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

où $V \in k[x_1, \ldots, x_n]$. Le degré du polynôme minimal de v sur k est d, l'ordre du groupe de Galois G (puisque, d'après l'identité (1), c'est le degré de l'extension $k(\underline{\alpha})/k$).

Note 7. L'idéal $\mathfrak{M}$ est calculable à partir de l'idéal $\mathfrak{J}$ des relations symétriques (voir [2]) :

$$\mathfrak{M} = \mathfrak{J} \ + \ \langle Min_{v,k}(V) \rangle \qquad .$$

Mais cela nécessiterait d'abord d'obtenir $\mathrm{Min}_{v,k}$ par le calcul et la factorisation du polynôme

$$R_V = \prod_{\sigma \in S_n} (x - (\sigma.V)(\underline{\alpha}))$$

de degré $n!$ et d'ensuite de calculer l'ensemble triangulaire engendrant $\mathfrak{M}$. Ce dernier calcul peut s'avérer très complexe si l'ordre du groupe de Galois est élevé. Le lecteur pourra consulter les articles [7], [14], [19] et [20] présentant des méthodes plus efficaces pour le calcul de $\mathfrak{M}$.

Note L'historique résolvante dite de Galois est le polynôme

$$\mathrm{Min}_{v,k} = \prod_{g \in G} (x - v^g)$$

ou bien tout autre facteur sur $k[x]$ du polynôme R_V (c'est selon selon les auteurs). E. Galois définit le groupe de l'équation comme celui échangeant les racines de $\mathrm{Min}_{v,k}$. L'approche proposée ici est de le définir comme le groupe stabilisant l'idéal des relations et d'aboutir ensuite à la formule (2). Le théorème qui suit est connu sous le nom de *Théorème de Galois.*

Théorème 8. *([10]) Soit $\beta \in k(\underline{\alpha})$. Pour que β appartienne à k il faut et il suffit que $\beta^g = \beta$ pour tout $g \in G$.*

Démonstration. Soit $P \in k[x]$ de degré au plus $d-1$ tel que $\beta = P(v)$. Le polynôme

$$W(x) = P(x) - \beta$$

de degré strictement inférieur à d appartient à $k(\underline{\alpha})[x]$. De plus, pour chaque $g \in G$, l'identité $\beta^g = \beta$ est équivalente à $W(v^g) = 0$ (voir Notation 4).
Si $\beta^g = \beta$ pour tout $g \in G$ alors les d racines distinctes du polynôme minimal de v sur k sont aussi racines de W de degré $d-1$. Le polynôme W est donc nul et par suite $\beta = P(0) \in k$. Inversement, si $\beta \in k$ alors $W(V) = P(V) - \beta$ appartient à l'idéal des relations $\mathfrak{M}$ car $V(\underline{\alpha}) = v$. Donc, par définition de G, $W(v^g) = 0$ pour tout $g \in G$. Ce qui termine la démonstration. □

Note La dernière partie de cette démonstration est un bon reflet de la différence entre l'approche lagrangienne que nous adoptons et l'approche galoisienne. Comme E. Galois, introduisons le groupe $\mathcal{G}$ échangeant les racines du polynôme $\mathrm{Min}_{v,k}$. Pour montrer que $W(v^g) = 0$ pour tout $g \in \mathcal{G}$, il y a deux solutions. La première consiste à remarquer que W possède une racine en commun avec $\mathrm{Min}_{v,k}$ et de déduire de l'irréductibilité de ce dernier que W possède toutes ses racines v^σ, $\sigma \in \mathcal{G}$; ce qui nécessite la démonstration d'un lemme préalable. La seconde est de chercher à faire agir $\mathcal{G}$ sur $P(v) - \beta = 0$. C'est ce que font de nombreux auteurs avec beaucoup de contorsions, voir avec des erreurs ; cette deuxième solution fonctionne parce que $\mathcal{G} = G$ (voir Remarque 5).

Une extension de k est dite *galoisienne* si elle est le corps des racines d'un polynôme de $k[x]$.

Notation 9. Soit H un sous-groupe du groupe de Galois G. La notation $k(\underline{\alpha})^H$ désigne le sous-corps de $k(\underline{\alpha})$ formé de ses éléments β tels que $\beta^\sigma \in k(\underline{\alpha})^H$ pour tout $\sigma \in H$ (i.e. invariants par toute permutation de H).

Le théorème 8 s'exprime sous la forme :

$$k = k(\underline{\alpha})^G \quad .$$

L'identité $k(\underline{\alpha}) = k(\underline{\alpha})^{I_n}$, où I_n est le sous-groupe identité de S_n, conduit à s'interroger sur le lien existant entre les sous-groupes de G et les corps intermédiaires entre k et $k(\underline{\alpha})$. C'est la correspondance galoisienne qui y répond. Elle s'exprime en les

points suivants :

1. Si K est un corps intermédiaire entre k et $k(\underline{\alpha})$ alors il existe un sous-groupe de G tel que $K = k(\underline{\alpha})^H$.

2. Si H est un sous-groupe de G alors il existe un sous-corps K de $k(\underline{\alpha})$ tel que $K = k(\underline{\alpha})^H$.

3. Dans chacun de ces cas, d'après le Lemme d'Artin, l'extension $k(\underline{\alpha})$ de K est galoisienne et le groupe H est le groupe de Galois de $\underline{\alpha}$ sur K ; l'extension $k(\underline{\alpha})$ de K est donc de degré l'ordre du groupe H et l'extension K de k est de degré l'indice de H dans G ; si, de plus, H est un sous-groupe distingué de G alors l'extension K/k est galoisienne et le groupe quotient G/H est isomorphe au groupe des k-automorphismes de K.

Proposition 10. *Soient $H_1 \subset H_2$ deux sous-groupes de G et $\beta \in k(\underline{\alpha})$. L'égalité*

$$Stab_{H_2}(\beta) = H_1$$

est satisfaite si et seulement si β est un élément primitif du corps $k(\underline{\alpha})^{H_1}$ sur le corps $k(\underline{\alpha})^{H_2}$ et dans ce cas

$$Min_{\beta,k} = \prod_{\sigma \in H_2/H_1} (x - \beta^\sigma) \qquad .$$

Démonstration. Comme l'impliquent les deux assertions de la proposition, nous avons $\beta \in k(\underline{\alpha})^{H_1}$. Le polynôme minimal de β sur $k(\underline{\alpha})^{H_2}$ est de degré au plus d, l'indice de H_1 dans H_2 (i.e. le degré de l'extension). H_2 étant le groupe de Galois de f sur $k(\underline{\alpha})^{H_2}$, les racines de ce polynôme sont les β^σ où σ parcourt H_2.
Si $\mathrm{Stab}_{H_2}(\beta) = H_1$, il existe exactement d racines distinctes : celles obtenues en parcourant H_2/H_1. Le polynôme minimal de β étant de même degré que l'extension considérée, β est un élément primitif de cette extension. Inversement s'il existait $\sigma \in H_2 \backslash H_1$ tel que $\beta^\sigma = \beta$ alors le polynôme minimal de β serait de degré strictement inférieur à d ; ce qui contredirait la primitivité de β. □

4. Matrices des groupes et des partitions

Soit L un sous-groupe de S_n et G et H deux sous-groupes de L. Nous notons e l'indice de H dans L. Nous faisons agir G à gauche sur L/H, les classes à gauche de L modulo H. Nous définissons ainsi une représentation (naturelle) par permutations de G dans le groupe $S_{L/H}$:

$$\begin{array}{rccc} \Psi : & G & \longrightarrow & S_{L/H} \\ & g & \mapsto & \sigma_g \end{array}$$

telle que, pour $C, C' \in L/H$, $\sigma_g.C = C'$ si $gC = C'$. Par $\mathcal{O}$, nous désignons l'ensemble des orbites pour cette représentation.

Note 11. Soient $g, g' \in G$. L'identité $\Psi(g) = \Psi(g')$ est satisfaite si et seulement si $g' \in gJ$ où

$$J = \bigcap_{\sigma \in L} H^\sigma$$

est un sous-groupe normal de L. Le groupe G est m-isomorphe au groupe $\Psi(G)$ où m est l'ordre du groupe $N = J \cap G$. Le groupe G/N est simplement isomorphe à $\Psi(G)$. Si $H \notin \{S_n, A_n, V_4, D_4\}$ alors N est le groupe identité.

Notation 12. La notation

$$P_L(G, H) \quad ,$$

ou plus simplement $P(G, H)$, désignera la partition $1^{m_1}, 2^{m_2}, ..., e^{m_e}$ où, pour $i \in [\![1, e]\!]$, l'entier m_i est le nombre d'orbites de cardinal i (nous retirons les i^0 de $P(G, H)$ et posons $i = i^1$) par action de $\Psi(G)$ sur L/H. Nous avons $e = m_1 + 2m_2 + \cdots + em_e$, le poids de la partition, et nous posons $m = m_1 + \cdots + m_e$ sa longueur qui est le nombre d'orbites (i.e. le cardinal de $\mathcal{O}$).

Exemples 13. Ces exemples seront poursuivis pour illustrer les résultats essentiels.

1. Pour $L = S_4$, $G = D_4 = \langle (1, 2, 3, 4), (1, 3) \rangle$, un groupe diédral dans S_4 et $H = A_4$, le groupe alterné, nous avons

$$S_4/A_4 = \{A_4, (3, 4)A_4\} \quad , \mathcal{O} = \{\{A_4, (3, 4)A_4\}\} \text{ et } P_{S_4}(D_4, A_4) = 2 \ .$$

2. Pour $L = S_4$, $G = D_4$ et $H = S_2 \times S_2$, nous avons $P_{S_4}(D_4, H) = 2, 4$ avec

$$\mathcal{O} = \{\{(2, 3)H, (1, 2, 4, 3)H\}, \{H, (1, 2, 3)H, (1, 3)(2, 4)H, (2, 4, 3)H\}\} \quad .$$

3. Pour $L = M_5 = \langle (1, 2, 3, 4, 5), (1, 2, 4, 3) \rangle$, le groupe méta-cyclique de degré 5, $G = C_5 = \langle (1, 2, 3, 4, 5) \rangle$ et $H = D_5 = \langle (1, 2, 3, 4, 5), (2, 5)(3, 4) \rangle$, nous avons

$$\mathcal{O} = \{\{D_5\}, \{(2, 3, 5, 4)D_5\}\} \quad \text{ et } \quad P_{M_5}(C_5, D_5) = 1^2 \quad .$$

De même, soient $H_1 = Id_5$, $H_2 = \langle (2, 5)(3, 4) \rangle$, $H_3 = \langle (2, 5)(3, 4), (2, 3, 5, 4) \rangle$, $H_4 = C_5$, $H_5 = D_5$ et $H_6 = M_5$ des représentants des six classes de conjugaisons dans M_5. La matrice $\mathfrak{P} = (P(H_i, H_j))_{1 \leq i,j \leq 6}$ est la suivante :

$$\mathfrak{P} = \begin{pmatrix} 1^{20} & 1^{10} & 1^5 & 1^4 & 1^2 & 1 \\ 2^{10} & 1^2, 2^4 & 1, 2^2 & 2^2 & 1^2 & 1 \\ 4^5 & 2, 4^2 & 1, 4 & 4 & 2 & 1 \\ 5^4 & 5^2 & 5 & 1^4 & 2 & 1 \\ 10^2 & 5^2 & 5 & 2^2 & 1^2 & 1 \\ 20 & 10 & 5 & 4 & 2 & 1 \end{pmatrix} \quad .$$

Les partitions d'une même colonne j ont comme poids l'indice de H_j dans le groupe M_5. Nous verrons plus loin que cette matrice ne dépend pas des représentants choisis pour chaque classe de conjugaison.

La représentation Ψ de G dans $S_{L/H}$ est équivalente à une représentation symétrique Ψ_{sym} de G dans S_e induite par un ordre sur les e classes de L/H :

$$\Psi_{sym} \ : \ G \longrightarrow S_{L/H} \longrightarrow S_e$$

Convention 14. Afin de simplifier la présentation, nous choisissons d'ordonner les classes de L/H de telle manière que les classes d'une même orbite soient consécutives et que les classes d'une orbites de cardinal c soient ordonnées avant celles des orbites de cardinal supérieur à c (ce n'est pas un ordre total).

Le produit direct de groupes symétriques $S_1^{m_1} \times S_2^{m_2} \times \cdots \times S_e^{m_e}$ est usuellement noté $S_{1^{m_1},2^{m_2},\ldots,e^{m_e}}$. Avec la convention que nous avons choisie, la représentation symétrique $\Psi_{sym}(G)$ de G dans S_e est un sous-groupe de $S_{P(G,H)}$.

Notation-Définition 15. Soit $j \in [\![1, m]\!]$. Notons p_j le cardinal de la j-ième orbite O. Le groupe noté

$$\Psi(G)_j$$

est une représentation symétrique transitive de G dans S_{p_j} induite par une représentation de G par action à gauche sur l'orbite O. La notation

$$Gr_L(G, H) \quad ,$$

ou plus simplement $Gr(G, H)$, désignera la suite $\Psi(G)_1, \ldots, \Psi(G)_m$.

Remarque 16. Pour $j \in [\![1, m]\!]$,

$$\Psi(G)_j$$

est aussi le sous-groupe de S_{p_j} obtenu par l'action du groupe de permutations $\Psi_{sym}(G)$ sur l'ensemble des p_j entiers $\{p_1 + \cdots + p_{j-1} + 1, \ldots, p_1 + p_2 + \cdots + p_j\}$ (en posant $p_0 = 0$).

Reprenons nos exemples, en choisissant chaque fois un ordre sur les orbites.

Exemples 17.
1. (suite). Nous avons $Gr_{S_4}(D_4, A_4) = S_2$ car $P_{S_4}(D_4, A_4) = 2$.

2. (suite). Nous avons $P_{S_4}(D_4, S_2 \times S_2) = 2, 4$. L'action de D_4 sur l'orbite de cardinal 4 montre que $Gr_{S_4}(D_4, S_2 \times S_2) = S_2, D_4$.

3. (suite) Nous avons $Gr_{M_5}(C_5, D_5) = S_1, S_1 = S_1^2$ car $P_{M_5}(C_5, D_5) = 1^2$.

Note La démonstration de la proposition suivant adapte celle de la proposition 10 de [1] portant sur la partition $P_L(G, H)$.

Proposition 18. *La suite $Gr_L(G, H)$ ne dépend que des classes de conjugaison de G et H dans L.*

Démonstration. Posons $G^\tau = \tau G \tau^{-1}$ et $H^\tau = \tau H \tau^{-1}$, $\tau \in L$. Nous avons la bijection naturelle : $\begin{array}{rccc} h: & L/H & \longrightarrow & L/H^\tau \\ & C & \mapsto & C\tau^{-1} \end{array}$.

Soit Ψ' la représentation de G dans S_{L/H^τ}. La suite $Gr_L(G,H)$ ne dépend que de la classe de conjugaison de H dans L car les représentations Ψ et Ψ' sont équivalentes. En effet, pour tout $C \in L/H$, $g \in G$, en posant $C' = gC = \Psi(g).C$, nous avons

$$h^{-1}o\Psi'(g)oh(C) = h^{-1}o\Psi'(g)(C\tau^{-1}) = h^{-1}(gC\tau^{-1}) = h^{-1}(C'\tau^{-1}) = C' = \Psi(g).C \quad .$$

Montrons l'indépendance du choix de G dans sa classe d'équivalence. Soit I_τ l'automorphisme de conjugaison de L dans L qui à σ associe σ^τ. L'ensemble L/H^τ est formé des classes à gauche $I_\tau(\sigma H) = I_\tau(\sigma)I_\tau(H)$ où σH parcourt L/H (i.e. I_τ induit une bijection de L/H sur L/H^τ). De même, pour $g \in G$ et $C \in L/H$, nous avons $I_\tau(gC) = I_\tau(g)I_\tau(C)$. Donc, en ordonnant correctement les classes à gauche, l'action de G sur L/H est identique à celle de G^τ sur L/H^τ. Plus précisément, en notant Θ la représentation de G dans L/H^τ, nous avons $\Theta = I_\tau \Psi I_\tau^{-1}$. D'où $Gr(G,H) = Gr(G^\tau, H^\tau) = Gr(G^\tau, H)$, d'après la première partie de cette démonstration. Donc l'indépendance du choix de G est démontrée. □

Soient $H_1, \ldots, H_r$ des représentants des classes de conjugaisons de L. Les matrices

$$\mathfrak{P} = (P_L(H_i, H_j))_{1 \le i,j \le r} \quad \text{et} \quad \mathfrak{G} = (Gr_L(H_i, H_j))_{1 \le i,j \le r}$$

sont respectivement appelées la *matrice des partitions relative à* L et la *matrice des groupes relative à* L.

Proposition 19.
1. La partition $P_L(G,H)$ est de la forme $1^m \ldots$ avec $m \ge 1$ si et seulement si G est un sous-groupe d'un conjugué de H dans L ;
2. $P_L(G, I_n) = \mathrm{Card}(H)^c$ où c est l'indice de G dans L ;
3. $P_L(G,H) = [L : H]$ ssi $L = GH$ (par ex., $G = L$) ;
4. $P_L(I_n, H) = 1^e$.

Démonstration. 1. Si G est un sous-groupe d'un conjugué H' de H dans L alors $\Psi(G).H' = \{H'\}$. D'où $P_L(G,H) = P_L(G,H') = 1^m \ldots$ avec $m \ge 1$. Inversement, supposons qu'il existe $C = \tau H$ une classe de L/H telle que $\Psi(G).C = \{C\}$ (i.e. $P(G,H)$ possède au moins une part égale à 1) ; pour tout $\sigma \in G$, nous avons $\sigma\tau H = \tau H$; ce qui est équivalent à $\sigma \in \tau H \tau^{-1}$.
2. Le groupe I_n est d'indice $e = \mathrm{Card}(L)$ dans L. Pour toute classe $C = \tau I_n = \{\tau\}$ de L/I_n, le cardinal de l'orbite $\Psi(G).C$ est donc identique à celui de G. Comme la partition $P(G, I_n)$ est de poids e, le résultat est démontré.
3. C'est lorsqu'il n'y a qu'une seule orbite.
4. Car $\Psi(I_n).C = C$ pour toute classe C de L/H. □

Proposition 20. *([1]) Les lignes de la matrice des partitions (et donc aussi des groupes) sont distinctes deux à deux.*

Démonstration. Montrons que les lignes qui correspondent à G et H sont distinctes si ces deux groupes ne sont pas L-conjugués. Nous ferons référence aux assertions 1. et 2. de la proposition 19. Si G n'est pas un sous-groupe d'un conjugué de H alors

$P(G,H) \neq P(H,H)$, d'après 1.. Si G est un sous-groupe propre d'un conjugué de H alors, d'après 2., $P(G,I_n) \neq P(H,I_n)$. Si les lignes correspondant à G et H sont identiques alors $P(G,H) = P(H,H)$ et $P(G,I_n) = P(H,I_n)$ et, par conséquent, G est un conjugué de H dans L. □

Exemple 21. Pour $L = M_5$ et en reprenant les notations de l'exemple 13, nous obtenons :

$$\mathfrak{G} = \begin{pmatrix} S_1^{20} & S_1^{10} & S_1^5 & S_1^4 & S_1^2 & S_1 \\ S_2^{10} & S_1^2, S_2^4 & S_1, S_2^2 & S_2^2 & S_1^2 & S_1 \\ \mathcal{H}_3^5 & S_2, \mathcal{H}_3^2 & S_1, \mathcal{H}_3 & \mathcal{H}_3 & S_2 & S_1 \\ H_4^4 & H_4^2 & H_4 & S_1^4 & S_1^2 & S_1 \\ \mathcal{H}_5^2 & H_5^2 & H_5 & S_2^2 & S_1^2 & S_1 \\ H_6^{(20)} & H_6^{(10)} & H_6 & \mathcal{H}_3 & S_2 & S_1 \end{pmatrix}$$

où
- $\mathcal{H}_3$ est le sous-groupe cyclique de S_4 engendré par $(1,4)(2,3)$ et $(1,2,4,3)$; on a $S_1 \times \mathcal{H}_3 = H_3$,
- $\mathcal{H}_5 = \langle (1,2,4,7,10)(3,6,9,8,5), (1,3)(2,5)(4,8)(6,10)(7,9) \rangle$ est la représentation régulière symétrique de H_5 (dans S_{10}),
- $H_6^{(10)} = \langle (1,2,4,7,10)(3,6,5,9,8), (1,3,7,6)(2,5,4,8)(9,10) \rangle$ est une représentation symétrique de H_6 dans S_{10},
- $H_6^{(20)} = \langle (1,2,4,7,10)(3,6,9,8,5), (1,3)(2,5)(4,8)(6,10)(7,9) \rangle$ est la représentation symétrique régulière de H_6 dans S_{20}.

Note Tandis qu'E.H Berwick et H.O. Foulkes construisent des sous-matrices de $\mathfrak{P}$ pour $L = S_n$ ($n = 5, 6$ et 7), G et H parcourant les sous-groupes transitifs de S_n, G. Butler et J. McKay prennent pour L les groupes symétriques jusqu'au degré 11, pour G les sous-groupes transitifs de S_n et pour H des groupes de la forme $U \times S_m$ où U est ou bien le groupe identité ou bien le groupe symétrique de degré $n - m$. Dans ce qui est proposé ici, tous les groupes sont considérés et nous ne calculons pas seulement $\mathfrak{P}$ mais aussi $\mathfrak{G}$. Néanmoins, tous ces travaux s'inscrivent dans la même démarche.

5. Résolvante Générique

Pour $P \in k[x_1, \ldots, x_n]$, l'orbite de P sous l'action de L est l'ensemble $L.P$ suivant :

$$L.P = \{\sigma.P \mid \sigma \in L\} \quad .$$

La *résolvante L-relative générique par P* est le polynôme :

$$\mathcal{R}(\underline{x}, x) = \prod_{Q \in L.P} (x - Q) \quad .$$

Supposons que H soit le sous-groupe de L stabilisant P dans L :

$$H = \{\sigma \in L \mid \sigma.P = P\} \quad (i.e.\ \mathrm{Stab}_L(P) = H) \quad .$$

Le polynôme P est alors appelé un *H-invariant L-primitif.* La proposition 26 justifiera cette terminologie.

La proposition suivante est considérée comme classique.

Proposition 22.
1. L'orbite $L.P$ est constituée des e polynômes distincts $\sigma.P$ où $\overline{\sigma}$ parcourt L/H.
2. Pour tout $\sigma \in L$, le polynôme $\sigma.P$ est un H^σ-invariant L-primitif.

Démonstration. Soient $\tau, \sigma \in L$.
1. Nous avons $\tau.P = \sigma.P$ si et seulement si $\sigma^{-1}\tau.P = P$; ce qui est équivalent à $\tau \in \sigma H$.
2. De la même manière, nous avons $\tau.(\sigma.P) = \sigma.P$ si et seulement si $\tau \in \sigma H \sigma^{-1}$. $\square$

L'application

$$\begin{array}{rccc} h_1 : & L/H & \longrightarrow & L.P \\ & \sigma H & \mapsto & \sigma.P \end{array}$$

est une bijection entre L/H et l'ensemble des racines de $\mathcal{R}$. La représentation naturelle Ψ_1 de G dans $S_{L.P}$ est équivalente à sa représentation Ψ dans $S_{L/H}$:

$$\Psi = h_1^{-1}\Psi_1 h_1 \quad .$$

En effet, pour tout $\tau \in G$ et $C = \sigma H \in L/H$ si $\tau C = C' = \sigma' H$ alors $\tau.(\sigma.P) = \sigma'.P$.

Convention 23. Nous ordonnons l'orbite $L.P$ de telle sorte que le i-ième élément noté P_i soit l'image par h_1 de la i-ième orbite C_i de L/H.

La représentation symétrique de G dans S_e induite par Ψ_1 est identique à sa représentation Ψ_{sym} induite par Ψ (voir Paragraphe 4) :

$$\begin{array}{rccl} \Psi_{sym} : & G & \longrightarrow & S_e \\ & \tau & \mapsto & \sigma : \sigma(i) = j \text{ si } \tau C_i = C_j \text{ (i.e. } \tau.P_i = P_j) \end{array} \quad .$$

D'après la proposition 22, nous pouvons définir l'orbite $(L/H).P$ et nous avons :

$$\mathcal{R} = \prod_{\overline{\sigma} \in L/H} (x - \sigma.P) = \prod_{Q \in (L/H).P} (x - Q) \quad .$$

Remarque 24. Soit G est un sous-groupe de L. Par la théorie de Galois classique, nous constatons que l'action à gauche de G sur les classes de L/H fournit les degrés et groupes de Galois des facteurs de $\mathcal{R}$ sur le corps $K(x_1, \ldots, x_n)^G$. Il s'agit donc des listes $P_L(G, H)$ et $\mathrm{Gr}_L(G, H)$.

Exemples 25.
1. (suite) Le Vandermond $P = \prod_{1 \le i < j \le 4}(x_i - x_j)$ est un A_4-invariant S_4-primitif. Comme $(3, 4).P = -P$, nous avons

$$\mathcal{R} = x^2 - P^2 = x^2 - \prod_{1 \le i \le j \le 4} (x_i - x_j) = x^2 - \Delta$$

où Δ est le discriminant du polynôme $(x-x_1)(x-x_2)(x-x_3)(x-x_4)$.

2. (suite) Les polynômes $P = x_1 + x_2$ et $Q = x_1x_2$ sont des S_{2^2}-invariants S_4-primitifs. En se basant sur l'orbite $\mathcal{O}$, il vient

$$(S_4/S_{2^2}).P = \{x_1+x_3, x_2+x_4, x_1+x_2, x_2+x_3, x_3+x_4, x_1+x_4\} \quad .$$

3. (suite) Le polynôme $P = x_4x_5 + x_3x_4 + x_2x_3 + x_1x_5 + x_1x_2$ est un D_5-invariant M_5-primitif et

$$\mathcal{R} = (x-P)(x-(2,3,5,4).P) = (x-P)(x-(x_2x_4+x_5x_2+x_3x_5+x_1x_4+x_1x_3)) \quad .$$

Étudions la résolvante $\mathcal{R}$ comme un polynôme de $k(x_1,\ldots,x_n)[x]$. Notons K le corps

$$k(x_1,\ldots,x_n)^{S_n} = k(\sigma_1,\ldots,\sigma_n),$$

où

$$\sigma_1 = \sum x_i, \ldots, \sigma_i = \sum x_1x_2\cdots x_i, \ldots, \sigma_n = x_1x_2\cdots x_n$$

sont les fonctions symétriques élémentaires de $x_1, x_2, \ldots, x_n$.

Proposition 26. *Le polynôme P est un élément primitif du corps $K(x_1,\ldots,x_n)^H$ sur le corps $\mathcal{K} = K(x_1,\ldots,x_n)^L$ et la résolvante $\mathcal{R}$ est son polynôme minimal sur le corps $\mathcal{K}$.*

Démonstration. Montrons d'abord que $\mathcal{R}$ est le polynôme minimal de P.
Les coefficients de $\mathcal{R}$ étant des fonctions symétriques des éléments de $L.P$, ils sont invariants par L et appartiennent donc au corps $\mathcal{K}$. Montrons que $\mathcal{R}$ est irréductible sur $\mathcal{K}$. Supposons que h soit le facteur unitaire de $\mathcal{R}$ et irréductible sur le corps $\mathcal{K}$ tel que $h(P) = 0$. Donc h est invariant par l'action de L sur $x_1,\ldots,x_n$. D'où, pour tout $\sigma \in L$, $\sigma.P$ est une racine de h ; ce qui impose à h d'être un multiple de $\mathcal{R}$. Par conséquent, $\mathcal{R} = h$ et $\mathcal{R}$ étant irréductible sur $\mathcal{K}$, elle est le polynôme minimal de P.
Nous en déduisons la primitivité de P : d'après la proposition 22, le degré de la résolvante $\mathcal{R}$ est e. Donc le polynôme minimal de P a pour degré le cardinal de L/H, qui, d'après la correspondance galoisienne, est le degré de l'extension $K(x_1,\ldots,x_n)^H$ du corps $\mathcal{K}$. □

Théorème 27. *Posons $\mathcal{K} = K(x_1,\ldots,x_n)^L$. Soit le sous-groupe normal de L donné par*

$$J = \bigcap_{\sigma\in L} H^\sigma \quad .$$

Alors

1. le corps des racines $P_1,\ldots,P_e$ de la résolvante générique $\mathcal{R}$ est

$$\mathcal{K}(P_1,\ldots,P_e) = \mathcal{K}(x_1,\ldots,x_n)^J \quad ;$$

2. toute représentation symétrique dans S_e du groupe L/J est une représentation symétrique et transitive dans S_e du groupe de Galois de $\mathcal{R}$ sur $\mathcal{K}$.

Démonstration. D'après la proposition 26, nous avons

$$\mathcal{K}(P_1,\ldots,P_e) = \bigcup_{\sigma\in L} \mathcal{K}(\sigma.P) = \bigcup_{\sigma\in L} \mathcal{K}(x_1,\ldots,x_n)^{H^\sigma} = \mathcal{K}(x_1,\ldots,x_n)^J \quad .$$

car, pour tout $\sigma \in L$, le polynôme $\sigma.P$ est un H^σ-invariant L-primitif (voir Proposition 22) et $\mathcal{R}$ est également la résolvante par $\sigma.P$. La représentation est transitive puisque $\mathcal{R}$ est irréductible sur $\mathcal{K}$. □

Lorsque $L = S_n$ et G est un sous-groupe transitif de S_n, le théorème 27 induit les résultats suivants :

- si $H = S_n$ alors $P \in K$ est un polynôme symétrique en $x_1,\ldots,x_n$, $e = 1$, $J = S_n$; S_1 est le groupe de Galois sur K de la résolvante $\mathcal{R} = x - P$;
- si $H = A_n$ alors $e = 2$, $J = A_n$ et S_2, la représentation symétrique dans dans S_e du groupe S_n/A_n, est le groupe de Galois sur K de la résolvante $\mathcal{R}$; nous avons
$$K(P_1,P_2) = K(P_1) \quad ;$$
comme A_n-invariant S_n-primitif P, nous pouvons prendre le Vandermond
$$\delta = \prod_{1\le i<j\le n} (x_i - x_j) \quad ; \quad \text{d'où} \quad \mathcal{R} = x^2 - \delta^2$$
où δ^2 est le discriminant du polynôme générique $\prod_{i=1}^n (x - x_i)$;
- si $n = 4$ et $H = V_4 = \langle (1,4)(2,3),(1,2)(3,4)\rangle$ alors $e = 6$, $J = V_4$ et le groupe de Galois sur K de la résolvante $\mathcal{R}$ de degré 6 est isomorphe au groupe S_4/V_4 d'ordre 6 ; une représentation symétrique dans S_6 de ce groupe est le groupe $\langle (1,2)(3,5)(4,6),(1,3)(2,4)(5,6)\rangle$; on peut prendre $P_1 = (x_1 - x_2)(x_3 - x_4)$ et on a :
$$K(P_1,P_2,\ldots,P_6) = K(P_1) = K(x_1,x_2,x_3,x_4)^{V_4} \quad ;$$
- si $n = 4$ et $H = D_4$ alors $e = 3$, $J = V_4$ et
$$K(P_1,P_2,P_3) = K(x_1,x_2,x_3,x_4)^{V_4} = K(P_i,P_j)$$
pour tout $i \neq j$; le groupe de Galois sur K de la résolvante $\mathcal{R}$ de degré 3 est isomorphe au groupe S_4/V_4 d'ordre 6 ; S_3 est une représentation symétrique de ce groupe ; on peut prendre $P = x_1x_3 + x_2x_4$;
- dans tous les autres cas, J est le groupe identité et S_n est isomorphe au groupe de Galois sur K de la résolvante $\mathcal{R}$; nous avons alors
$$K(P_1,P_2,\ldots,P_e) = K(x_1,\ldots,x_n) \quad .$$

6. Spécialisation de la résolvante générique

Rappelons que $f = (x - \alpha_1)\cdots(x - \alpha_n)$ est un polynôme de $k[x]$ et que $\underline{\alpha} = (\alpha_1,\ldots,\alpha_n)$. Nous conservons les notations du paragraphe précédent. En particulier, H est le sous-groupe de L stabilisant l'invariant P :

$$\mathrm{Stab}_L(P) = H \quad .$$

Nous supposons que G est le groupe de Galois de $\underline{\alpha}$ sur k.

La *résolvante L-relative de $\underline{\alpha}$ par P* est le polynôme d'une variable :

$$R(x) = \mathcal{R}(\underline{\alpha}, x) = \prod_{\overline{\sigma} \in L/H} (x - (\sigma.P)(\alpha_1, \ldots, \alpha_n)) \quad .$$

Ce polynôme est aussi appelé une *H-résolvante L-relative de $\underline{\alpha}$*.

Note Lorsque $L = S_n$, la résolvante ne dépend pas de la numérotation des racines de f et elle peut s'appeler la *résolvante (absolue) de f par P* ou une *H-résolvante (absolue) de f*. J.L. Lagrange a introduit la résolvante absolue. Afin de déterminer le groupe de Galois par descente dans le graphe d'inclusions des sous-groupes de S_n, R.P. Stauduhar utilise les résolvantes relatives avec $G \subset L$ (voir [16]) .

En toute généralité, les coefficients de la résolvante R appartiennent au corps $k(\underline{\alpha})^{G \cap L}$. Le polynôme minimal de $P(\underline{\alpha})$ sur ce corps est donc un facteur de la résolvante R. La proposition suivante énonce un cas d'égalité.

Proposition 28. *Posons $\beta = P(\underline{\alpha})$ et prenons pour L un sous-groupe de G. La résolvante R est le polynôme minimal de β sur le corps $k(\underline{\alpha})^L$ (i.e. elle est irréductible sur ce corps) si et seulement si β est une racine simple de R. Dans ce cas, β est un élément $k(\underline{\alpha})^L$-primitif du corps $k(\underline{\alpha})^H$.*

Démonstration. C'est une reformulation de la proposition 10 car les deux assertions sont équivalentes à $\mathrm{Stab}_L(\beta) = H$. □

Remarque 29. Dans tout ce qui suit, on peut remplacer le corps k par toute extension de k et G par le groupe de Galois de $\underline{\alpha}$ sur ce corps. Ceci vaut, en particulier, pour toute extension intermédiaire entre k et $k(\underline{\alpha})$.

Hypothèse Forts de la remarque précédente, nous supposons désormais que G est un sous-groupe de L (i.e. $k = k(\underline{\alpha})^{G \cap L}$).

Par le Théorème de Galois, la résolvante $R(x)$ est à coefficients dans k puisque ceux de $\mathcal{R}(\underline{x}, x)$ sont invariants par L. En particulier, si R est une résolvante absolue, ses coefficients sont des fonctions symétriques des racines de f ; il existe de nombreuses méthodes pour les calculer (indépendemment de G) ; certaines sont évoquées dans les articles de la bibliographie. Le lecteur y trouvera aussi des méthodes pour calculer des résolvantes L-relatives.

Théorème 30. *([1]) Supposons que f soit sans racine multiple et que le corps k soit infini. Il existe une H-résolvante L-relative de $\underline{\alpha}$ sur k qui soit sans racine multiple. Le polynôme H-invariant L-primitif associé à cette résolvante est alors dit L-séparable pour $\underline{\alpha}$.*

Démonstration. Toute résolvante L-relative de $\underline{\alpha}$ par P étant un facteur sur k de la résolvante de f par P, nous pouvons supposer que $L = S_n$.
Tout d'abord, montrons le théorème pour le groupe $H = I_n$. Soient $t_1, \ldots, t_n$ des indéterminées et le polynôme

$$V_{\underline{t}} = t_1 x_1 + \ldots + t_n x_n \quad .$$

Pour toute permutation σ de S_n distincte de l'identité, nous avons

$$V_{\underline{t}}(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \neq V_{\underline{t}}(\alpha_1, \ldots, \alpha_n) \quad .$$

Le corps k étant infini, il existe des valeurs $\tilde{t_1}, \ldots, \tilde{t_n}$ de k telles que

$$V(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \neq V(\alpha_1, \ldots, \alpha_n) \quad .$$

où $V = V_{\tilde{t_1}, \ldots, \tilde{t_n}}$ est un polynôme de $k[x_1, \ldots, x_n]$ (il n'existe qu'un nombre fini de valeurs pour lesquelles il y a égalité). La résolvante R de f par V est donc une I_n-résolvante de f sans racine multiple.
Soient $\tau_1 H, \ldots \tau_e H$, $\tau_1 = id$, les classes à gauche de L modulo H. Pour $i \in [\![1, e]\!]$, posons

$$R_i = \prod_{\tau \in \tau_i H} (x - \tau.V) \quad .$$

Les polynômes $r_i = R_i(\alpha_1, \ldots, \alpha_n)$ sont des facteurs de la I_n-résolvante séparable R : $R = r_1 r_2 \ldots r_e$. Donc si $i \neq 1$ alors $r_1(x) \neq r_i(x)$. Le polynôme $r_1 - r_i$ ne pouvant posséder plus de racines que son degré, il existe une infinité de $u \in k$ tels que $r_1(u) \neq r_i(u)$. Pour $u \in k$ bien choisi, le polynôme $R_1(u)$ est un H-invariant S_n-primitif et le polynôme $\prod_{i=1}^{e}(x - r_i(u))$, résolvante de f par $R_1(u)$, est sans racine multiple. □

Note 31. Dans la démonstration précédente, lorsque k est infini, v est l'élément primitif de $k_1 = k(\underline{\alpha})$ sur k dont nous avons supposé l'existence au paragraphe 3. Lorsque k est fini, il suffit de prendre un générateur du groupe fini monogène k_1^*. De plus, si H est un sous-groupe de G alors r_i est un élément k-primitif du corps $\mathrm{Inv}(H) = k(\underline{\alpha})^H$ lorsque le corps k est infini. De même, lorsque k est fini, $\mathrm{Inv}(H)^*$ est un groupe fini monogène. Ceci constitue une démonstration du théorème de l'élément primitif.

Note Il existe des résolvantes génériques qui restent séparables quelques soient les valeurs distinctes en lesquelles elles sont spécialisées. C'est le cas de la A_n-résolvante $x^2 - \delta^2$ et de la M_5-résolvante dite de Cayley (voir [6]).

Exemples 32. Les polynômes proviennent de la base de données du logiciel Magma.

1. (suite) Le polynôme $f = x^4 - x^3 - 3x^2 + x + 1$ possède D_4 comme groupe de Galois sur $\mathbb{Q}$ et $R = x^2 - 725$ où 725 est le discriminant de f.

2. (suite) Gardons $f = x^4 - x^3 - 3x^2 + x + 1$. La résolvante par P est le polynôme

$$R_1 = x^6 - 3x^5 - 3x^4 + 11x^3 - 2x^2 - 4x + 1$$

et celle par Q est le polynôme

$$R_2 = x^6 + 3x^5 - 2x^4 - 8x^3 - 2x^2 + 3x + 1 \quad .$$

3. (suite) Le polynôme $f = x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$ possède C_5 comme groupe de Galois sur $\mathbb{Q}$. Si C_5 est le groupe de Galois de $\underline{\alpha} = (\alpha_1, \ldots, \alpha_5)$ sur $\mathbb{Q}$, l'idéal $\mathfrak{M}$ des $\underline{\alpha}$-relations est engendré par les 5 polynômes

$$x_1^5 - x_1^4 - 4x_1^3 + 3x_1^2 + 3x_1 - 1, x_2 - x_1^3 + 3x_1, x_3 + x_1^2 - 2,$$
$$x_4 - x_1^4 + x_1^3 + 3x_1^2 - 2x_1 - 1, x_5 + x_1^4 - 4x_1^2 + 2 \quad .$$

Ces polynômes résultent de la factorisation de f sur $\mathbb{Q}(\alpha_1)$ et sont ordonnés de telle sorte que C_5 soit le groupe de décomposition de $\mathfrak{M}$ (i.e. $C_5.\mathfrak{M} = \mathfrak{M}$). Les évaluations des coefficients de $\mathcal{R}$ modulo $\mathfrak{M}$ donnent :

$$R = (x+2)^2 \quad .$$

7. Groupe de Galois de la résolvante

Le degré des résolvantes $\mathcal{R}$ et R est e, l'indice de H dans L. Choisissons un ordonnancement $\beta_1, \ldots, \beta_e$ des racines de R (que nous préciserons ultérieurement) et posons $\underline{\beta} = (\beta_1, \ldots, \beta_e)$. Nous pouvons définir une représentation par permutations :

$$\begin{array}{rccl} \Theta : & G & \longrightarrow & S_{\{\beta_1,\ldots,\beta_e\}} \\ & g & \mapsto & \Theta(g) : \Theta(g).\beta_i = \beta_i^g \end{array} \quad .$$

En effet, pour $g \in G$, d'une part, l'action β_i^g est bien définie et d'autre part β_i^g est bien une racine de R puisque c'est une racine du polynôme minimal de β_i sur k qui est un facteur de R.

Note 33. Le sous-groupe $\Theta(G)$ de G n'est pas nécessairement simplement isomorphe à G. En effet, supposons que $g, g' \in G$ satisfont $\beta_i^g = \beta_i^{g'}$ et que les β_i soient distincts deux-à-deux. Alors $g' \in gJ$ où J est le sous-groupe normal

$$\cap_{\sigma \in L} H^\sigma$$

de L. Le groupe G est m-isomorphe au groupe $\Theta(G)$ où m est l'ordre du groupe $N = J \cap G$. Le groupe G/N est simplement isomorphe à $\Theta(G)$ (Faire le lien avec la note 11). Dans la littérature ancienne, nous retrouvons cette remarque sous diverses formes (voir, par exemple, [15])

Si la résolvante R n'a aucune racine double, la représentation symétrique du groupe $\Theta(G)$:

$$\begin{array}{ccl} \Theta(G) & \longrightarrow & S_e \\ \tau & \mapsto & \sigma : \sigma(i) = j \text{ si } \tau.\beta_i = \beta_j \end{array}$$

est bien définie ; nous définissons ainsi une représentation symétrique de G dans S_e :

$$\begin{array}{rccl} \Theta_{sym} : & G & \longrightarrow & S_e \\ & g & \mapsto & \sigma_g : \sigma_g(i) = j \text{ si } \beta_i^g = \beta_j \end{array} \quad .$$

Convention 34. La représentation symétrique $\Psi_{sym}(G)$ de G dans S_e est induite par un ordonnancement des classes de L/H (voir Convention 14). Nous décidons que si $\beta_j = \sigma.P(\underline{\alpha})$ alors la j-ième classe est σH et qu'ainsi $\beta_j = P_j(\alpha_1, \ldots, \alpha_n)$, où P_j est le j-ième polynôme de l'ordonnancement choisi pour l'orbite $L.P$.

Théorème 35. *Supposons le corps k infini. Si la résolvante $R = (x-\beta_1)\ldots(x-\beta_e)$ est sans racine multiple alors la représentation symétrique $\Theta_{sym}(G)$ de G dans S_e est le groupe de Galois de $\underline{\beta}$ sur k.*

Démonstration. Notons $G_{\underline{\beta}}$ le groupe de Galois de $\underline{\beta}$ sur k. Montrons tout d'abord que $\Theta_{sym}(G) \subset G_{\underline{\beta}}$. Soient $y_1, \ldots, y_e$ des variables. Soit $g \in G$ et $p(y_1, \ldots, y_e)$ un polynôme $G_{\underline{\beta}}$-invariant S_n-primitif tel que pour tout $\sigma \notin G_{\underline{\beta}}$

$$p(\beta_1, \ldots, \beta_e) \neq (\sigma.p)(\beta_1, \ldots, \beta_e) \quad .$$

Comme k est infini, un tel polynôme existe (Voir Théorème 30). Nous avons $p(\beta_1, \ldots, \beta_e) \in k$ car p est invariant par le groupe de Galois de $\underline{\beta}$ sur k. Posons $q = p - p(\beta_1, \ldots, \beta_e)$ et $Q = q(P_1(x_1, \ldots, x_n), \ldots, P_e(x_1, \ldots, x_n))$. Nous avons $0 = q(\beta_1, \ldots, \beta_e) = Q(\alpha_1, \ldots, \alpha_n)$. Par définition du groupe de Galois de $\underline{\alpha}$ sur k, nous avons $(g.Q)(\alpha_1, \ldots, \alpha_n) = 0$. Donc

$$\begin{aligned} 0 = (g.Q)(\alpha_1, \ldots, \alpha_n) &= Q(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \\ &= q(g.P_1(\alpha_1, \ldots, \alpha_n), \ldots, g.P_e(\alpha_1, \ldots, \alpha_n)) \\ &= q(\beta_1^g, \ldots, \beta_e^g) \\ &= (\Theta_{sym}(g).q)(\beta_1, \ldots, \beta_e) \quad . \end{aligned}$$

Seules les permutations de $G_{\underline{\beta}}$ dans S_e envoient la $\underline{\beta}$-relation q sur une autre $\underline{\beta}$-relation. Donc $\Theta_{sym}(G)$ est un sous-groupe de $G_{\underline{\beta}}$.

Pour montrer l'inclusion inverse, choisissons un polynôme $p(y_1, \ldots, y_e)$ qui soit un I_e-invariant S_e-primitif et tel que pour toute permutation $\sigma \in S_n$ distincte de l'identité $\sigma.p(\beta_1, \ldots, \beta_e) \neq p(\beta_1, \ldots, \beta_e)$. Comme k est infini, un tel polynôme existe (Voir Théorème 30). Comme $p(\underline{\beta})$ est un élément k-primitif de $k(\underline{\beta})$, son polynôme minimal sur k est :

$$M = \prod_{\sigma \in G_{\underline{\beta}}} (x - (\sigma.p)(\beta_1, \ldots, \beta_e)) \quad .$$

C'est, en fait, la résolvante de Galois de la résolvante R. Nous avons donc également, par la théorie de Galois et en posant $\gamma = p(\beta_1, \ldots, \beta_e) \in k(\alpha_1, \ldots, \alpha_n)$, :

$$M = \prod_{\theta \in \{\gamma^g | g \in G\}} (x - \theta) \quad .$$

En procédant comme dans la première partie de cette démonstration, nous obtenons que pour tout $\sigma \in G_{\underline{\beta}}$ il existe $g \in G$ tel que

$$(\sigma.p)(\beta_1, \ldots, \beta_e) = \gamma^g = (\Theta_{sym}(g).p)(\beta_1, \ldots, \beta_e) \quad .$$

Comme $\sigma^{-1} \in G_{\underline{\beta}}$, nous pouvons écrire :

$$(\sigma^{-1}\Theta_{sym}(g).p)(\beta_1, \ldots, \beta_e) = p(\beta_1, \ldots, \beta_e) \quad ;$$

ce qui, par le choix de p, impose que $\Theta_{sym}(g) = \sigma$. D'où $G_{\underline{\beta}} \subset \Theta_{sym}(G)$ et le théorème est démontré. □

Note Dans la première partie de la démonstration précédente, il est possible d'utiliser une variante montrant que le groupe $\Theta_{sym}(G)$ envoie toute $\underline{\beta}$-relation sur une autre $\underline{\beta}$-relation. Nous avons choisi de prendre une relation particulière possédant les propriétés nécessaires et suffisantes à la description de l'idéal des $\underline{\beta}$-relations engendré

par les modules de Cauchy de la résolvante (i.e. des relations symétriques) et par la $\underline{\beta}$-relation q (voir Note 7).

Note Tout ceci est cohérent car, étant donné $\gamma \in k(\beta_1, \ldots, \beta_e) \subset k(\alpha_1, \ldots, \alpha_n)$, les permutations $\sigma \in G_\beta$ et $g \in G$ de la démonstration précédente satisfont :

$$\gamma^\sigma = \gamma^g$$

si la représentation du groupe $Aut_k(k(\beta_1, \ldots, \beta_e))$ dans S_e est celle associée à $\underline{\beta}$.

Si les racines de R sont distinctes deux-à-deux (i.e. R est séparable), l'application

$$\begin{array}{rccc} h_2 : & L.P & \longrightarrow & \{\beta_1, \ldots, \beta_e\} \\ & Q & \mapsto & Q(\alpha_1, \ldots, \alpha_n) \end{array} \quad .$$

est une bijection entre les racines de $\mathcal{R}$ et celles de R, l'application $h = h_2 o h_1$ est alors une bijection de L/H dans $\{\beta_1, \ldots, \beta_e\}$ et

$$\Theta = h \Psi h^{-1} \quad .$$

Les représentation Θ et Ψ étant ainsi équivalentes, les représentations Θ_{sym} et Ψ_{sym} de G dans S_e sont identiques. On en déduit le théorème suivant qui pré-détermine le groupe de Galois de R uniquement à partir de G, H et L.

Théorème 36. *Si la résolvante R est sans racine multiple alors la représentation symétrique $\Psi_{sym}(G)$ de G dans S_e est le groupe de Galois de $\underline{\beta}$ sur k ; i.e. c'est le groupe de Galois de R sur k.*

Dans le cas où le groupe de Galois de f est inconnu et celui le R l'est partiellement, ce corollaire permet de savoir si G n'est pas identique à certains sous-groupes de S_n. En effet, l'ensemble des groupes $\Psi_{sym}(G')$ où G' parcourt S_n est pré-calculable (voir Paragraphe 1). Une information partielle du groupe de Galois de R est, par exemple, celle des groupes de Galois de ses facteurs sur k. C'est à cette information qu'est consacré le paragraphe suivant.

8. Groupes de Galois des facteurs de R et détermination de G

Les orbites de $\Psi(G)$ sont en bijection avec celles de $\Theta(G)$. Le groupe G étant le groupe de Galois de $\underline{\alpha}$ sur k, l'ensemble des orbites de $\Theta(G)$ est en bijection avec l'ensemble des facteurs irréductibles (pas nécessairement simples) sur k de la résolvante R : si $R(\beta) = 0$ alors

$$\Theta(G).\beta \mapsto \prod_{\gamma \in \Theta(G).\beta} (x - \gamma) = \mathrm{M}in_{\beta,k} \quad .$$

Soit $\beta = (\sigma.P)(\alpha_1, \ldots, \alpha_n)$ une racine de la résolvante R, $C = \sigma H$ et $g_1 = id, \ldots, g_c$ des permutations de G telles que :
- $\Psi(G).C = \{C = g_1 C, \ldots, g_c C\}$
- si C est la j-ième classe de L/H (voir Convention 14) alors $g_i C$ est la $j+i-1$-ième classe ; c'est-à-dire que $\beta^{g_i} = P_{j+i-1}(\alpha_1, \ldots, \alpha_n)$.

Dans ce paragraphe et le suivant, nous considérerons le polynôme

$$F = \prod_{i=1}^{c} (x - \beta^{g_i})$$

de $k[x]$. Ce polynôme est une puissance du polynôme minimal de β sur k. S'il est sans racine multiple alors il est irréductible sur k.

Théorème 37. *Supposons que $\Psi(G).C$ soit la s-ième orbite de $\Psi(G)$.*
Si le polynôme F est sans racine multiple alors :
- le groupe de Galois de $(\beta, \beta^{g_2}, \ldots, \beta^{g_c})$ sur k est $\Psi(G)_s$, le s-ième élément de la suite $Gr_L(G,H)$, et
- le degré c de F est la s-ième part de la partition $P_L(G,H)$.
Le groupe $\Psi(G)_s$ est donc une représentation symétrique dans S_c du groupe de Galois de F sur k.

Démonstration. Nous avons $\beta^{g_i} = (g_i\sigma.P)(\alpha_1, \ldots, \alpha_n)$ pour $i = 1, \ldots, c$. Si F est sans racine multiple, l'ensemble des racines de F est en bijection avec l'orbite $\Psi(G).C$. La démonstration se termine avec la définition de $Gr_L(G,H)$ (voir Notation-Définition 15). □

Remarque 38. Soit F un facteur irréductible simple sur k de degré c de la résolvante R. Alors, en choisissant β tel que $F(\beta) = 0$, les conditions du théorème sont satisfaites et le groupe de Galois de F sur k est l'un des groupes de degré c de la suite $Gr_L(G,H)$ (à un isomorphisme près).

Note Il est intéressant de constater que si la résolvante est sans racine double, elle est irréductible si et seulement si il n'y a qu'une seule orbite pour $\Psi(G)$. C'est-à-dire lorsque $L = GH$ (voir 3. Proposition 19). Il ne faut pas en être étonné. Lorsqu'on considère l'idéal de Galois défini par $\underline{\alpha}$ et le groupe H alors le plus grand ensemble de permutations définissant aussi cet idéal est GH (qui n'est pas nécessairement un groupe).

Le corollaire suivant est utilisé par R.P. Stauduhar dans sa descente des sous-groupes. Il peut aussi être déduit du théorème 47.

Corollaire 39. *Si $\beta = (\sigma.P)(\underline{\alpha})$ est une racine simple sur k de la résolvante R alors G est un sous-groupe du conjugué H^σ de H dans L.*

Remarque 40. Si G est le groupe de Galois de $\underline{\alpha}$ sur k alors $G^{\sigma^{-1}}$ est celui de $\sigma.\underline{\alpha}$ sur k. Pour $\sigma \in L$, la résolvante L-relative de $\underline{\alpha}$ par P et celle de $\sigma.\underline{\alpha}$ sont identiques. Donc, si $G \subset H^\sigma$ alors $G^{\sigma^{-1}} \subset H$. Il suffit d'échanger $\underline{\alpha}$ et $\sigma.\underline{\alpha}$ pour que dans le corollaire précédent le groupe de Galois soit inclus dans le groupe H. Lorsque le groupe H est distingué dans L alors G est un sous-groupe de H. Nous retrouvons ainsi la propriété bien connue que le groupe de Galois est pair si son discriminant est un carré dans k.

Corollaire 41. *Si la résolvante R est séparable alors la suite $Gr_L(G,H)$ est à une permutation près la liste des groupes de Galois sur k des facteurs irréductibles de R sur k et $P_L(G,H)$ est celle de leurs degrés.*

Théorème 42. *([1]) Supposons que le corps k soit infini. Il est toujours possible de déterminer le groupe de Galois G avec des résolvantes.*

Démonstration. Car les lignes de la matrice $\mathfrak{P}$ sont distinctes deux-à-deux et qu'il existe toujours des résolvantes séparables. □

Examinons le cas des racines multiples..

Théorème 43. *Nous distinguons 2 cas de multiplicité :*
i) Si β est de multiplicité exactement m dans F alors m divise c et

$$F = F_0^m$$

où F_0 est irréductible sur k.
ii) Si β est aussi une racine de R/F alors F^2 divise R ; plus précisément, β est une racine du facteur F de R/F associé à une orbite de $\Psi(G)$ distincte de $\Psi(G).C$ mais de même cardinalité.

Remarque 44. Dans le cas ii), le théorème 37 restant valide, ce cas ne peut se produire que si le groupe $\Psi(G)_s$ apparaît deux fois dans $Gr_L(G, H)$.

Démonstration. Soient P_1 et P_2 deux racines distinctes de la résolvante générique $\mathcal{R}$. Si $P_1(\underline{\alpha}) = P_2(\underline{\alpha})$ alors pour tout $g \in G$ $g.P_1$ et $g.P_2$ sont deux racines distinctes de $\mathcal{R}$ telles que $g.P_1(\underline{\alpha}) = g.P_2(\underline{\alpha})$. Supposons que $\sigma.P = P_1$ (i.e. $\beta = P_1(\underline{\alpha})$).
Montrons i). Si P_1 et P_2 sont dans la même G-orbite (i.e. $G.P_1 = G.P_2$) alors $P_1(\underline{\alpha})$ et $P_2(\underline{\alpha})$ sont deux racines de F de même que $g.P_1(\underline{\alpha})$ et $g.P_2(\underline{\alpha})$. Donc si $\beta = P_1(\underline{\alpha})$ est de multiplicité m dans F alors toute autre racine de F (i.e. $g.P_1(\underline{\alpha})$, avec $g \in G$) est aussi de multiplicité m.
Montrons ii). Supposons que β soit une racine commune à F et à R/F. On a $P_1(\underline{\alpha}) = P_2(\underline{\alpha})$ avec P_1 et P_2 dans deux G-orbites distinctes. Donc toutes les valeurs des deux G-orbites s'identifient deux-à-deux. D'où le résultat. □

Corollaire 45.
i) Si le degré de F est un nombre premier alors F est soit irréductible sur k soit une puissance d'un facteur linéaire sur k.
ii) Si $GL = L$ et que $e = [L : H]$ est premier alors la résolvante R est soit irréductible sur k, soit une puissance une puissance d'un facteur linéaire sur k.

Exemples 46. Nous supposons que f n'a que des racines simples.
1. (suite) La résolvante $x^2 - \Delta$ par A_4 est nécessairement sans racine multiple car le discriminant Δ de f est non nul. Le discriminant 725 de f se factorise en $5^2.29$ qui n'est pas un carré dans $\mathbb{Q}$. La résolvante R est irréductible sur $\mathbb{Q}$. Son groupe de Galois est nécessairement S_2. Nous avions $Gr_{S_4}(D_4, A_4) = S_2$ qui annonçait ce résultat.

2. (suite) La factorisation de la résolvante par P est

$$R_1 = (x^2 - x - 1)(x^4 - 2x^3 - 4x^2 + 5x - 1)$$

et celle par Q est :

$$R_2 = (x+1)^2(x^4+x^3-5x^2+x+1) \quad .$$

D'après l'exemple 17, $Gr_{S_4}(D_4, S_2 \times S_2) = S_2, D_4$. Donc D_4 est le groupe de Galois sur $\mathbb{Q}$ de chacun des facteurs de degré 4 de R_1 et R_2. Le polynôme $x^2 - x - 1$ étant simple, son groupe de Galois S_2 était également prévisible. Le facteur $(x+1)^2$ de R_2 provient d'une orbite de cardinal 2. C'est le cas i) du théorème 43.

3. (suite) La résolvante $R = (x+2)^2$ possède une racine double. Mais nous savons que chaque facteur correspond à chacune des orbites $\{D_5\}$ et $\{(2,3,5,4)D_5\}$ car le groupe de Galois est C_5. C'est le cas ii) du théorème 43.

9. Corps des racines de la résolvante R

Étudions les racines de la résolvante. Nous allons constater que de spécialiser x_i en α_i, pour $i = 1, \ldots, n$, revient à intersecter les groupes avec le groupe de Galois G de f sur k. Nous savons déjà que le corps $k(x_1, \ldots, x_n)^{S_n}$ se spécialise en le corps $k = k(\underline{\alpha})^{S_n \cap G}$ car les fonctions symétriques des racines de f appartiennent à k. Plus généralement, comme $G \subset L$, le corps $\mathcal{K} = K(x_1, \ldots, x_n)^L$ se spécialise en $k = k(\underline{\alpha})^G = k(\underline{\alpha})^{L \cap G}$.

Théorème 47. *Si le polynôme F est sans racine multiple alors sa racine $\beta = (\sigma.P)(\alpha_1, \ldots, \alpha_n)$ est un élément k-primitif du corps $k(\underline{\alpha})^{G \cap H^\sigma}$ et F est son polynôme minimal sur k. Par conséquent, le corps $k(\underline{\alpha})^{G \cap H}$ s'identifie à l'ensemble des $P(\underline{\alpha})$ où P parcourt $K(x_1, \ldots, x_n)^H$.*

Démonstration. Soit $g \in G$. Les égalités $\beta^\sigma = \beta$ et $g\sigma.P = \sigma.P$ sont équivalentes puisque F est sans racine multiple et que ses racines sont les spécialisations en $\underline{\alpha}$ de la G-orbite de $\sigma.P$. Comme $\sigma.P$ est un H^σ-invariant L-primitif et que G est un sous-groupe de L, $\beta^g = \beta$ est donc équivalent à $g \in H^\sigma$. Soit U le sous-groupe de G tel que $k(\beta) = K(\underline{\alpha})^U$. Si $K(\underline{\alpha})^U$ était strictement inclus dans le corps $k(\underline{\alpha})^{G \cap H^\sigma}$ alors il existerait $\tau \in U$ tel que $\tau \notin H^\sigma$ et $\beta^\tau = \beta$; ce qui est impossible. D'où $U = H^\sigma$. □

Note En rapprochant les théorèmes 30 et 47, on trouve une méthode pour calculer un élément k-primitif de tout sous-corps du corps des racines de f.

Corollaire 48. *Si $G \cap H^\sigma$ est le groupe identité et que F est sans racine multiple alors β est un élément k-primitif du corps $k(\underline{\alpha})$ et F est son polynôme minimal sur k.*

Corollaire 49. *Si le polynôme F est sans racine multiple alors son groupe de Galois sur k est isomorphe au groupe $G/G \cap M$ où*

$$M = \bigcap_{g \in G} H^{g\sigma} \quad .$$

En particulier, si $G \cap M$ est le groupe identité alors G est isomorphe au groupe de Galois de F sur k et le corps des racines de F est identique à celui de f.

Démonstration. L'ensemble des racines de F est formé des β^g où g parcourt G. Nous avons donc

$$\begin{aligned} k(\beta^{g_1}, \beta^{g_2}, \ldots, \beta^{g_c}) &= \bigcup_{g \in G} k(\beta^g) \\ &= \bigcup_{g \in G} k(\underline{\alpha})^{G \cap H^{g\sigma}} \end{aligned}$$

car les racines de F sont distinctes (voir Théorème 47). Donc le corps des racines de F est identique au corps $k(\underline{\alpha})^{G \cap M}$. Par conséquent, le sous-groupe normal $G \cap M$ de G est le groupe de Galois de $k(\underline{\alpha})$ sur le corps des racines de F. □

De la même manière, nous obtenons le corollaire suivant qu'il faut rapprocher du théorème 27 et des notes 11 et 33. Nous le trouvons dans

Corollaire 50. *Si la résolvante R est sans racine multiple alors son groupe de Galois sur k est isomorphe au groupe $G/G \cap J$ où*

$$J = \bigcap_{\sigma \in L} H^\sigma \quad .$$

En particulier, si $G \cap J$ est le groupe identité alors G est le groupe de Galois de R sur k et le corps des racines de R est identique à celui de f :

$$k(\underline{\alpha}) = k(\underline{\beta})$$

et le groupe de Galois de f sur k est isomorphe à celui de R sur k.

Dans le corollaire suivant, nous excluons les cas dans lesquels N n'est pas le groupe identité (voir les exemples du paragraphe 10).

Corollaire 51. *([1]) Supposons que $L = S_n$. Supposons que $H \notin \{S_n, A_n\}$ et que, de plus, si $n = 4$ alors $H \notin \{D_4, V_4\}$. Alors $k(\underline{\alpha}) = k(\underline{\beta})$.*

10. Exemples de résolvantes connues

Ici, nous retrouvons des résultats classiques.

1. Supposons que le polynôme f est irréductible et que son degré n est 4. Soit $P = x_1x_3 + x_2x_4$ un D_4-invariant S_4-primitif. La résolvante R de degré $e = 3$ est connue sous le nom de *résolvante cubique.* Supposons que R n'ait pas de racine double. Nous avons

$$J = V_4 \quad .$$

Il y a cinq possibilités pour le groupe de Galois G :
- $G = S_4$; $G \cap J = V_4$;
S_4/V_4 est d'ordre 6 ; donc R est irréductible sur k de groupe de Galois S_3 ;
- $G = A_4$; $G \cap J = V_4$;
A_4/V_4 est d'ordre 3 ; donc R est irréductible sur k de groupe de Galois A_3 ;
- $G = V_4$; $G \cap J = V_4$;

V_4/V_4 est le groupe identité ; donc R se factorise en 3 facteurs linéaires sur k ;
- $G = D_4$; $G \cap J = V_4$ et $G \cap H = D_4$;
D_4/V_4 est d'ordre 2 ; donc le groupe de Galois de R est S_2 ; comme $G/G \cap H$ est le groupe identité, la racine $P(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ de R appartient à k ; R se factorise sur k en un facteur linéaire et un de degré 2 ;
- $G = C_4$; $G \cap J = \langle (1,3)(2,4) \rangle$;
$C_4/(G \cap J)$ est d'ordre 2 ; donc R se factorise sur k en un facteur de degré 2 et un facteur linéaire de racine $P(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

2. Soit $P \in k[x_1]$. La résolvante de f par P est appelée une *résolvante de Tchirnhaus*. C'est le polynôme de degré $e = n$:

$$R = \prod_{i=1}^{n} (x - P(\alpha_i)) \quad .$$

Cette résolvante est sans racine multiple si $P(\alpha_i) \neq P(\alpha_j)$ pour $i \neq j$. Le groupe H est le groupe $S_1 \times S_{n-1}$. Le groupe $J = \cap_{\sigma \in S_n} H^\sigma$ est le groupe identité. Si la résolvante est sans racine multiple alors son groupe de Galois est identique à celui de f. En particulier, si $P = x_1$ alors $R = f$ et $Gr_L(G, H)$ est la liste des groupes de Galois des facteurs irréductibles de f sur k.

3. Soit $V = t_1 x_1 + \cdots + t_n x_n$, $t_i \in k$ distincts deux-à-deux, un I_n-invariant S_n-primitif. Ici $H = I_n$ et $G \cap H^\sigma = I_n$ pour tout $\sigma \in S_n$. La résolvante de f par P est un polynôme de degré $n!$ appelé *résolvante de Galois de f*. Supposons que F soit un facteur simple de cette résolvante et que β en soit un racine. Alors, d'après le théorème 47, β est un élément k-primitif du corps $k(\alpha_1, \ldots, \alpha_n)$ des racines de f. Le polynôme F a pour degré l'ordre du groupe de Galois de f sur k et il s'exprime ainsi :

$$F = \prod_{g \in G} (x - \beta^g) \quad .$$

Le groupe de Galois de F sur k est isomorphe à G, le groupe de Galois de $\underline{\alpha}$ sur k. Dans la littérature, la résolvante de Galois désigne parfois toute résolvante G-relative de $\underline{\alpha}$ par V qui ne possède pas de racine multiple; c'est-à-dire le polynôme F.

4. Si le polynôme f est unitaire sans racine multiple, une A_n-résolvante de f est le polynôme séparable $x^2 - \Delta(f)$, où $\Delta(f)$ est le discriminant de f. Le groupe de Galois G de $\underline{\alpha}$ sur k est pair si et seulement si le discriminant de f est un carré sur k (voir Remarque 40).

5. Soit $H = M_5$, le groupe métacyclique de degré 5. La résolvante de f par P est un polynôme de degré 6. Si elle est sans racine multiple, le corps des racines de cette résolvante est identique à celui de f. Supposons que f soit irréductible sur k et que la résolvante n'ait pas de racine multiple. Si $G = S_5$, la résolvante est irréductible. Si $G = A_5$ alors la résolvante possède un facteur irréductible de degré $[A_5 : A_5 \cap M_5] = 60/10 = 6$; donc elle est irréductible. Sinon, pour une numérotation adéquate des racines de f, le groupe G est l'un des groupes M_5, D_5

ou C_5 et la résolvante possède un facteur linéaire sur k (et un de degré 5, si on étudie cas par cas le degré de l'extension que doit diviser l'ordre du groupe G). Pour que G soit un groupe résoluble et que f soit résoluble par radicaux il faut et il suffit que G soit un sous-groupe de M_5. Le polynôme

$$P = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1$$

est un M_5-invariant S_5-primitif. La résolvante R de f par P est connue sous le nom de *résolvante de Cayley* (pour son expression, voir [6] et [2]). Cette résolvante est sans racine multiple si f l'est également. Elle permet donc toujours de tester si un polynôme irréductible de degré 5 est ou non résoluble par radicaux.

Commentaires.

1. Dans les exemples précédents, des résultats du paragraphe 9 sont appliqués pour déterminer les groupes ou degrés des facteurs de R. La matrice des groupes fournit les mêmes informations.

2. Pour $G = S_4$ ou $G = A_4$, en déterminant le groupe de Galois d'un polynôme de degré 3, facteur irréductible de R, nous déterminons celui du polynôme f de degré $n = 4$. Cette chute du degré est un des avantages que présente la matrice des groupes face à celle des partitions. Cette situation n'est pas rare. Elle devient très avantageuse lorsque le degré n s'élève (voir [18] pour le degré 8).

11. Applications des résolvantes et des matrices de groupes

En se restreignant aux résolvantes absolues, il est toujours possible d'identifier le groupe de Galois d'un polynôme non nécessairement irréductible. Les calculs des résolvantes sont réalisés avec des manipulations de fonctions symétriques. Le problème est que les degrés des résolvantes absolues nécessaires à discriminer les groupes s'élèvent rapidement en fonction du degré n du polynôme.

Il faut alors pouvoir calculer des résolvantes relatives. R.P. Stauduhar propose de le faire avec des méthodes numériques. Les résolvantes elles-mêmes offrent un moyen de calculer des résolvantes relatives (voir [3] et [19]) ; une autre méthode est proposée dans [2]. Les résolvantes relatives étant des facteurs de résolvantes absolues, le problème de la croissance des degrés est ainsi contrôlé. Cette méthodologie a pour avantage de calculer simultanément l'idéal $\mathfrak{M}$ (i.e. le corps des racines).Toujours dans l'idée de calculer l'idéal $\mathfrak{M}$, dans [14] les auteurs travaillent sur les facteurs du polynôme f dans ses extensions $k(\alpha_1, \ldots, \alpha_i)$. Les matrices de groupes sont encore utilisables dans ce cadre. En particulier, f étant une résolvante sa factorisation donne des informations sur le groupe de Galois G.

Les matrices de groupes sont utilisable en sens inverse pour calculer un polynôme de degré c dont le groupe de Galois $\mathcal{G}$ apparaît dans $G_L(G, H)$: supposons que f est donné avec son groupe G ; on calcule une H-résolvante L-relative de f dont le facteur associé à l'orbite induisant $\mathcal{G}$ dans $G_L(G, H)$ est sans racine multiple. Ce facteur est le polynôme cherché. Cette méthode proposée dans [18] a été appliquée dans [11] avec $m = 12$. Elle est aussi utilisable pour calculer des polynômes dans des extensions de k.

Les matrices de partitions offrent une aide à la factorisation dans les extensions. Comme nous l'avons noté plus haut, le polynôme f est une H-résolvante avec $H = S_1 \times S_{n-1}$. Supposons qu'on cherche à factoriser un polynôme de $k[x]$ dans une extension k' de k. Pour tout groupe de Galois possible G de f sur k, on détermine, en fonction de G, le groupe de Galois $\mathcal{G}$ qu'aurait f dans l'extension k'. Par exemple, pour $k' = k(\alpha_1)$, $\mathcal{G} =$Stab$(G, 1)$. Alors $P(\mathcal{G}, H)$ est la liste des degrés possibles des facteurs irréductibles de f sur k'. Il est alors possible d'établir une table excluant des types de factorisations de f dans k'.

Enfin, J.L. Lagrange a introduit les résolvantes pour généraliser la résolution par radicaux. Il avait également introduit la fameuse résolvante de Vandermond-Lagrange dont l'invariant est

$$x_1 + \epsilon x_2 + \cdots + \epsilon^{n-1} x_n \quad .$$

Ses résolvantes ont été utilisées plus de deux siècles plus tard dans la résolution par radicaux des polynômes résolubles de degré 5 (voir [8]) et de degré 6 (voir [12]). Dans ce dernier article, l'auteur appelle "Galois resolvent" ce qui en fait est la résolvante de Lagrange. Il utilise la même méthode que dans [2] (voir aussi [1]) pour déterminer une sous-matrice de la matrice des partitions relative à S_6 (i.e. il calcule les cardinaux des orbites).

References

[1] J.-M. Arnaudiès and A. Valibouze. Lagrange resolvents. *J. Pure Appl. Algebra*, 117/118:23–40, 1997. Algorithms for algebra (Eindhoven, 1996).

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

[3] 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.

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

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

[6] 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.

[7] L. Ducos. Construction de corps de décomposition grâce aux facteurs de résolvantes. *Comm. Algebra*, 28(2):903–924, 2000.

[8] D. S. Dummit. Solving solvable quintics. *Math. Comp.*, 57(195):387–401, 1991.

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

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

[11] 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.

[12] Thomas R. Hagedorn. General formulas for solving solvable sextic equations. *J. Algebra*, 233(2):704–757, 2000.

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

[14] S. Orange, G. Renault, and A. Valibouze. Calcul efficace de corps de décomposition. Publication interne LIP6 2003.005, 2003. http://www.lip6.fr/reports/lip6.2003.004.html.

[15] J. Pierpont. Galois' theory of algebraic equations - part I. Rational resolvents. *Annals of Mathematics*, pages 113–143, 1899.

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

[17] N. Tchebotarev. *Gründzüge des Galois'shen Theorie*. P. Noordhoff, 1950.

[18] 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.

[19] 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. (Rapport LIP6 du 10/09/1997 : http://www.lip6.fr/fr/production/publications-rapports.php).

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

L.I.P.6, Université Pierre et Marie Curie, 4, place Jussieu, F-75252 Paris Cedex 05

E-mail address: annick.valibouze@upmc.fr