RÉSOLVANTES DE LAGRANGE

JEAN-MARIE ARNAUDIES, ANNICK VALIBOUZE *

Septembre 1993

Abstract. This paper is devoted to a sharp investigation of the notion of Lagrange's resolvents and his connections with Galois Theory.

1. Représentations par permutations

En théorie de Galois explicite, on est amené à représenter un même groupe de Galois abstrait $\mathrm{Gal}(E/K)$ dans des groupes de permutations des racines de divers polynômes $f \in K[x]$ dont les degrés peuvent varier. En effet on a besoin de calculer beaucoup de résolvantes en contrôlant au maximun leur corps de racines (voir Théorème 4.6 par exemple). Il nous a donc paru utile de rappeler quelques faits connus concernant les représentations par permutations d'un groupe fini (cf. [W. Burnside]).

Notation. Soit $\mathcal{C}$ une classe de conjugaison de sous-groupes d'un groupe fini G ; nous noterons $I_{\mathcal{C}} = \bigcap_{H\in\mathcal{C}} H$. On a : $I_{\mathcal{C}} \lhd G$, et pour tout $H \in \mathcal{C}$, le groupe $I_{\mathcal{C}}$ est le plus grand sous-groupe distingué de G inclus dans H. On dira que $\mathcal{C}$ est *réduite* ssi $I_{\mathcal{C}} = \{e_G\}$.

Soit G un groupe fini et E un ensemble fini non vide. Un morphisme de groupe $\Psi : G \to \mathfrak{S}_E$ est appelé une *représentation de G par permutations*, ou encore *symétrique de degré* $N = \mathrm{card}(E)$. Une telle représentation est dite *fidèle* ssi $\mathrm{Ker}(\Psi) = \{e_G\}$, et *transitive* ssi le G-ensemble E défini par Ψ n'a qu'une orbite. On a $\mathrm{Ker}(\Psi) = \bigcap_{x\in E} \mathrm{Stab}_G(x)$, et il est clair que si Ψ est transitive alors l'ensemble $\{\mathrm{Stab}_G(x)\}_{x\in E}$ est une classe de conjugaison de sous-groupes de G. Deux représentations $\Psi : G \to \mathfrak{S}_E$ et $\Phi : G \to \mathfrak{S}_F$ seront dites *équivalentes* ssi il existe une bijection $\Theta : E \to F$ telle que $\Psi(g) = \Theta^{-1} \circ \Phi(g) \circ \Theta$ pour tout $g \in G$. S'il en est ainsi, on a $\mathrm{Ker}(\Psi) = \mathrm{Ker}(\Phi)$, et $\{\mathrm{Stab}_{G,\Psi}(x)\}_{x\in E} = \{\mathrm{Stab}_{G,\Phi}(x)\}_{x\in F}$. Donc, deux représentations équivalentes sont fidèles (resp. transitives) en même temps. Toute représentation par permutations de degré N de G est équivalente à au moins une représentation $G \to \mathfrak{S}_N$.

* Avec le soutien du GDR de Calcul Formel MEDICIS, du GDR-PRC Math-Info, du Centre de Calcul Formel de l'Ecole Polytechnique, et de CEC, ESPRIT BRA contrat 6846 POSSO

1.1. Représentations par permutations transitives. Soit $\Psi : G \to \mathfrak{S}_E$ une représentation transitive de G. La classe de conjugaison $\mathcal{C}_\Psi = \{\mathrm{Stab}_G(x)\}_{x\in E}$ de sous-groupes de G sera dite *associée* à Ψ. Elle est réduite ssi Ψ est fidèle. Pour tout choix de $x_0 \in E$, en notant $H_0 = \mathrm{Stab}_G(x_0)$, la bijection Θ de E dans l'ensemble $(G/H_0)_g$ des classes à gauche de G mod H_0 définie par $\Theta(x) = \{g \in G \,|\, \Psi(g)(x_0) = x\}$ établit une équivalence de représentations $\Phi : G \to \mathfrak{S}_{(G/H_0)_g}$ définie par les translations à gauche de G. Le résultat suivant est élémentaire :

Théorème 1.1. Fixons un groupe fini G et un entier $N \geq 1$. Soit E un ensemble de cardinal N. En faisant correspondre, à chaque classe d'équivalence Γ de représentations transitives $G \to \mathfrak{S}_E$, la classe de conjugaison $\mathcal{C}(\Gamma)$ de sous-groupes de G associée à toutes les $\Psi \in \Gamma$, on obtient une bijection de Γ sur l'ensemble des classes de conjugaison de sous-groupes de G formées de sous-groupes d'indice N. Dans cette bijection, les classes réduites correspondent aux représentations fidèles, et la classe $\{\{e_G\}\}$ correspond aux représentations régulières.

Soient $\mathcal{C}$ et $\mathcal{C}'$ deux classes de conjugaison de sous-groupes de G. Nous écrirons $\mathcal{C} \preceq \mathcal{C}'$ ssi il existe $H \in \mathcal{C}$ et $H' \in \mathcal{C}'$ tels que $H \subset H'$; ce qui équivaut à dire que $\forall H \in \mathcal{C}\,, \exists H' \in \mathcal{C}' \,|\, H \subset H'$. La relation $\preceq$ est une relation d'ordre. Si $\mathcal{C} \preceq \mathcal{C}'$, on a $I_{\mathcal{C}} \subset I'_{\mathcal{C}}$.

Pour que $\mathcal{C} \neq \{G\}$ soit maximal parmi les classes autres que $\{G\}$, il faut et il suffit qu'il existe $H \in \mathcal{C}$ qui soit maximal parmi les sous-groupes distincts de G. Alors tout $H \in \mathcal{C}$ est maximal. Cela arrive ssi $\mathcal{C}$ correspond à des représentations *primitives*.

Supposons $\mathcal{C} \neq \mathcal{C}' \neq \{G\}$ et $\mathcal{C} \preceq \mathcal{C}'$. Soient $H \in \mathcal{C}$ et $H' \in \mathcal{C}'$ tels que $H \subset H'$. Posons $e = [H' : H]$, $N = [G : H]$, $N' = [G : H']$ d'où $N = eN'$. Pour toute classe $C' \in (G/H')_g$ soit $B_{C'}$ l'ensemble des $C \in (G/H)_g$ contenus dans C'. L'ensemble $\mathcal{B} = \{B_{C'}\}_{C'\in(G/H')_g}$ est une partition de $(G/H)_g$ en blocs de primitivité pour l'action de G par translations à gauche. Cette action induit donc sur $\mathcal{B}$ une action à gauche qui s'identifie à celle de G sur $(G/H')_g$ par translation à gauche (par exemple une telle identification s'obtient à partir de la bijection $C' \mapsto B_{C'}$).

Si C est donné non maximal, il y a une bijection naturelle entre les sous-groupes H' de G tels que $H \subset H' \neq G$, $H \neq H'$ et les systèmes d'imprimitivité du G-ensemble $(G/H)_g$ défini par les translations à gauches. Si H'_1 et H'_2 sont deux tels H', de même indice N' dans G, les actions par translations à gauche induites sur les blocs d'imprimitivité correspondant respectivement à H'_1 et H'_2 sont équivalentes ssi H'_1 et H'_2 sont conjugués dans G.

1.2. Représentations par permutations quelconques. Soit $\mathcal{E}$ l'ensemble des classes de conjugaison de sous-groupes de G ; à chaque $\mathcal{C} \in \mathcal{E}$, nous associerons son *degré* (noté $\deg(\mathcal{C})$) qui est par définition l'entier égal à $[G : H]$ pour tout $H \in \mathcal{C}$, et sont *poids*, noté $\pi(\mathcal{C})$, égal par définition à $\mathrm{card}(G)/\deg(\mathcal{C})$. Ci-après, nous ordonnerons $\mathcal{E}$ en une suite $(\mathcal{C}_1, \ldots, \mathcal{C}_s)$ telle que $\pi(\mathcal{C}_1) = 1 \leq \pi(\mathcal{C}_2) \leq \cdots \leq \pi(\mathcal{C}_s) = \mathrm{card}(G)$, de sorte que $\mathcal{C}_1 = \{\{e_G\}\}$ et $\mathcal{C}_s = \{G\}$. Observons que $\mathcal{C}_i \preceq \mathcal{C}_j \Rightarrow i \leq j$.

Soit $\mathcal{C} \in \mathcal{E}$ et $\mathcal{C}' \in \mathcal{E}$; si $H \in \mathcal{C}$, le nombre de points H-fixes dans une représentation donnée ρ' de G associée à $\mathcal{C}'$ est le nombre des $H' \in \mathcal{C}'$ tels que $H \subset H'$. Il

ne dépend que du couple $(\mathcal{C},\mathcal{C}')$, c'est un entier ≥ 0, qui est > 0 ssi $\mathcal{C} \preceq \mathcal{C}'$ (et $= 1$ ssi $\mathcal{C} = \mathcal{C}'$). Nous l'appellerons *nombre d'incidence* de $(\mathcal{C},\mathcal{C}')$ et nous le noterons $J(\mathcal{C},\mathcal{C}')$. La matrice $[m_{i,j}] = [J(\mathcal{C}_i,\mathcal{C}_j)]_{(i,j)\in[1,s]^2}$, notée $J(G)$, sera appelée la *matrice d'incidence de* G. D'après ce qu'on à vu, elle est trigonale supérieure, à coefficients dans $\mathbb{N}$ et à diagonale > 0 donc en particulier inversible.

Soit Ψ une représentation de G par permutations. Soit ω une G-orbite correspondante, de cardinal noté N. Par restriction, ρ définit une représentation transitive $G \to \mathfrak{S}_\omega$, qui est donc équivalente à l'une de celles définies par les $\mathcal{C}_i$ de degré N. Notons $\nu_i(\rho)$ le nombre de telles orbites ω qui conduisent ainsi à $\mathcal{C}_i$. Il est clair que $\nu_i(\rho)$ reste invariant si on remplace ρ par une représentation équivalente. On peut donc associer à ρ l'élément $U(\rho) = \sum_{1\leq i\leq s} \nu_i(\rho)\,\mathcal{C}_i$ du $\mathbb{Z}$-module libre $\mathcal{L}_G = \bigoplus_{i=1}^s \mathbb{Z}\mathcal{C}_i$ de base $(\mathcal{C}_1,\dots,\mathcal{C}_s)$. L'application U est donc constante sur chaque classe d'équivalence de représentations de G, et on a :

$$\deg(\rho) = \sum_{i=1}^{s} \nu_i(\rho)\deg(\mathcal{C}_i) \qquad ; \tag{1}$$

on a alors (voir [W. Burnside])

Théorème 1.2. Avec les notations ci-dessus, l'application $U : \rho \mapsto \sum_{1\leq i\leq s} \nu_i(\rho)\,\mathcal{C}_i$ définit une bijection entre l'ensemble des classes d'équivalence de représentations de G par permutations de degré n ($n \in \mathbb{N}^*$), et l'ensemble des éléments $\sum_{1\leq i\leq s} \nu_i\,\mathcal{C}_i$ de $\mathcal{L}_G$ tels que $\nu_i \in \mathbb{N}$ pour tout i et $\sum_{1\leq i\leq s} \nu_i \deg(\mathcal{C}_i) = n$.

Supposons connue la matrice d'incidence $J(G)$; soit ρ une représentation de degré n de G par permutations ; posons $U(\rho) = \sum_{1\leq i\leq s} \nu_i(\rho)\,\mathcal{C}_i$; le nombre de points fixes de $\rho(H)$ est $\sum_{1\leq i\leq s} \nu_i(\rho) J(H,\mathcal{C}_i)$. En particulier, le nombre de points fixes m_j commun à tous les $\rho(H)$ pour $H \in \mathcal{C}_i$ est $\sum_{1\leq i\leq s} \nu_i(\rho) J(\mathcal{C}_j,\mathcal{C}_i) = \sum_{i=j}^s J(\mathcal{C}_j,\mathcal{C}_i)$. Supposons connus les m_j, les ν_i sont alors donnés par le système de Cramer trigonal suivant :

$$\sum_{i=j}^{s} \nu_i(\rho) J(\mathcal{C}_j,\mathcal{C}_i) = m_j \qquad (1 \leq j \leq s). \tag{2}$$

1.3. Produit tensoriel de représentations par permutations. Soit $\rho : G \to \mathfrak{S}_E$ et $\theta : G \to \mathfrak{S}_F$ deux représentations de G par permutations, de degrés respectifs m et n. Notons $(e_\alpha)_{\alpha\in E}$ et $(f_\beta)_{\beta\in F}$ les bases respectives canoniques des $\mathbb{Q}$-espaces vectoriels $V = \mathbb{Q}^E$ et $W = \mathbb{Q}^F$; elles définissent les plongements naturels de $\mathfrak{S}_E$ et $\mathfrak{S}_F$ respectivement dans $\mathrm{GL}_{\mathbb{Q}}(V)$ et $\mathrm{GL}_{\mathbb{Q}}(W)$, plongements que nous noterons u et v.

Considérons la base $(a_{\alpha,\beta}) = e_\alpha \otimes f_\beta$ ($(\alpha,\beta) \in E \times F$) du $\mathbb{Q}$-espace vectoriel $V \bigotimes_{\mathbb{Q}} W$. Pour $(\sigma,\tau) \in \mathfrak{S}_E \times \mathfrak{S}_F$, il est clair que $u(\sigma) \otimes u(\tau)$ correspond à une permutation des $a_{\alpha,\beta}$, i.e. à un élément de $\mathfrak{S}_{E\times F}$ que nous noterons $\sigma \star \tau$. Soit $\rho\star\theta : G \to \mathfrak{S}_{E\times F}$, $g \mapsto \rho(g)\star\theta(g)$: c'est une représentation de G par permutations, dont la classe d'équivalence ne dépend que de celles de ρ et θ. En particulier,

supposant $U(\rho)=\mathcal{C}_i$ et $U(\theta)=\mathcal{C}_j$, $U(\rho\star\theta)$ de dépend que de $(\mathcal{C}_i,\mathcal{C}_j)$, et sera noté $\mathcal{C}_i\otimes\mathcal{C}_j$ et sera appelé *produit tensoriel de* $\mathcal{C}_i$ *et* $\mathcal{C}_j$. On a donc des entiers $(a_{i,j,l})_{1\leq l\leq s}$ tels que $\mathcal{C}_i\otimes\mathcal{C}_j=\sum_{l=1}^{s}a_{i,j,l}\,\mathcal{C}_l$, et qui vérifient

$$\sum_{l=1}^{s}a_{i,j,l}\deg(\mathcal{C}_l)=\deg(\mathcal{C}_i)\deg(\mathcal{C}_j)=d_i\,d_j \qquad , \tag{3}$$

(en notant $d_k=\deg(\mathcal{C}_k)$ pour $1\leq k\leq s$).

Dans le cas général, soit $U(\rho)=\sum_{i=1}^{s}\nu_i(\rho)\,\mathcal{C}_i$ et $U(\theta)=\sum_{i=1}^{s}\nu_i(\theta)\,\mathcal{C}_i$. Fixons arbitrairement pour chaque i une représentation ρ_i de G telle que $U(\rho_i)=\mathcal{C}_i$; alors ρ et θ sont respectivement équivalentes à $\bigoplus_{i=1}^{s}\nu_i(\rho)\rho_i$ et $\bigoplus_{i=1}^{s}\nu_i(\theta)\rho_i$. D'où :

$$\rho\star\theta = \bigoplus_{1\leq i\leq s,1\leq j\leq s}\nu_i(\rho)\,\nu_j(\theta)\rho_i\star\rho_j \qquad , \text{ et} \tag{4}$$

$$\begin{aligned} U(\rho\star\theta) &= \sum_{1\leq i\leq s,1\leq j\leq s}\nu_i(\rho)\,\nu_j(\theta)U(\rho_i\star\rho_j) \\ &= \sum_{l=1}^{s}\Big(\sum_{1\leq i\leq s,1\leq j\leq s}\nu_i(\rho)\nu_j(\theta)\,a_{i,j,l}\Big)\,\mathcal{C}_l \qquad . \end{aligned} \tag{5}$$

Munissons $\mathcal{L}_G$ de la structure de $\mathbb{Z}$-algèbre obtenue en prolongeant par $\mathbb{Z}$-linéarité les relations $\mathcal{C}_i\otimes\mathcal{C}_j=\sum_{l=1}^{s}a_{i,j,l}\,\mathcal{C}_l$, et notons $\otimes$ le produit dans cette algèbre.

On a donc :

$$U(\rho\star\theta)=U(\rho)\otimes U(\theta) \qquad . \tag{6}$$

La $\mathbb{Z}$-algèbre de $\mathcal{L}_G$ est associative et admet un élément unité, qui est $\mathcal{C}_s$.

Il est clair que pout tout sous-groupe H de G, le nombre de points fixes de $(\Psi\star\Theta)(H)$ est $m_\Psi(H)\times m_\Theta(H)$, en notant $m_\Psi(H)$ (resp. $m_\Theta(H)$) le nombre de points fixes de $\Psi(H)$ (resp. $\Theta(H)$). En particulier :

$$m_{\Psi_i\star\Psi_j}(H)=m_{\Psi_i}(H)m_{\Psi_j}(H) \qquad ;$$

donc en prenant $H\in\mathcal{C}_l$:

$$m_{\Psi_i\star\Psi_j}(H)=J(\mathcal{C}_l,\mathcal{C}_i)\times J(\mathcal{C}_l,\mathcal{C}_j) \qquad ;$$

mais

$$m_{\Psi_i\star\Psi_j}(H)=\sum_{r=1}^{s}a_{i,j,r}m_{\Psi_r}(H)=\sum_{r=1}^{s}a_{i,j,r}J(\mathcal{C}_l,\mathcal{C}_r) \qquad ;$$

donc pour $1\leq l\leq s$, $1\leq i\leq s$, $1\leq j\leq s$:

$$\sum_{r=1}^{s} a_{i,j,r} J(\mathcal{C}_l, \mathcal{C}_r) = J(\mathcal{C}_l, \mathcal{C}_i) \times J(\mathcal{C}_l, \mathcal{C}_j) \qquad , \tag{7}$$

et cette relation détermine les constantes $a_{i,j,r}$ puisque pour chaque (i,j), il s'agit d'un système de Cramer en les inconnues $(a_{i,j,r})_{1\leq r\leq s}$. La $\mathbb{Z}$-algèbre $\mathcal{L}_G$ est essentiellement celle appelée par certains auteurs, *Algèbre de Burnside*, son produit $\otimes$ étant appelé le *produit tensoriel*.

1.4. Représentations fidèles. Soit $\Psi : G \to \mathfrak{S}_n$ une représentation symétrique de degré n de G. Posant $U(\Psi) = \sum_{i=1}^{s} \nu_i \mathcal{C}_i$, nous appellerons *support* de Ψ et noterons $\mathrm{Supp}(\Psi)$, l'ensemble $\{i \in [1,s] \,|\, \nu_i \geq 1\}$. On a : $\mathrm{Ker}(\Psi) = \bigcap_{i\in \mathrm{Supp}(\Psi)} I_{\mathcal{C}_i}$. Donc Ψ est fidèle ssi $\bigcap_{i\in \mathrm{Supp}(\Psi)} I_{\mathcal{C}_i} = \{e_G\}$.

Dans toute la suite, nous noterons k un corps commutatif et $\hat{k}$ une de ses clôtures algébriques fixée une fois pour toutes.

2. Représentations et corps des racines

2.1. Soit $f \in k[X]$, normalisé (unitaire), de degré $n \geq 1$, séparable. Notons E_f sa k-algèbre des racines dans $\hat{k}$. On considère une numérotation des racines $\rho_1, \ldots, \rho_n$ de f dans $\hat{k}$, i.e. $f = \prod_{i=1}^{n}(X - \rho_i)$ et $E_f = k[\rho_1, \ldots, \rho_n]$. On a une représentation symétrique de degré n :

$$\mathrm{Gal}(E_f/k) \to \mathfrak{S}_n \ , \ \sigma \mapsto s_\sigma \ , \ \text{ où } \sigma(\rho_i) = \rho_{s_\sigma(i)} \qquad , \tag{8}$$

associée à l'action naturelle du groupe $\mathrm{Gal}(E_f/k)$ sur $\mathcal{R}_f = \{\rho_1, \ldots, \rho_n\}$. La représentation (8) est fidèle, et elle est transitive ssi f est irréductible.

Si $t \in \mathfrak{S}_n$, posons $\rho'_i = \rho_{t^{-1}(i)}$; la représentation (8) associée à l'ordination $(\rho'_1, \ldots, \rho'_n)$ de $\mathcal{R}_f$ est donnée par

$$\sigma \mapsto s'_\sigma = t\, s_\sigma\, t^{-1} \qquad ; \tag{9}$$

donc un changement de numérotation de $\mathcal{R}_f$ change la représentation de (8) en une représentation équivalente.

Soient $P_1, \ldots, P_r$ les facteurs irréductibles normalisés de f et soient $n_i = \deg(P_i)$, où $n_1 \geq \cdots \geq n_r$. Le groupe $\mathrm{Gal}(E_f/k)$ opère transitivement sur $\mathcal{R}_{P_i}$; soit C_i la classe de conjugaison de sous-groupes de $\mathrm{Gal}(E_f/k)$ correspondant à cette représentation ; alors la classe d'équivalence de la représentation (8) est $\sum_{i=1}^{r} C_i$; puisque cette représentation (8) est fidèle, on a donc $\bigcap_{i=1}^{r} I_{C_i} = \{\mathrm{Id}_{E_f}\}$.

2.2. Inversement, soit E une extension finie galoisienne de k, avec $E \subset \hat{k}$. Cherchons si une représentation symétrique donnée

$$S \ : \ \mathrm{Gal}(E/k) \to \mathfrak{S}_n \qquad , \tag{10}$$

fidèle et degré n, peut être définie sous la forme (8). Supposons k infini.

Soient $\omega_1, \ldots, \omega_r$ les orbites de $[1,n]$ pour la représentation (10) ; posons $n_i = \mathrm{card}(\omega_i)$, supposons les ω_i ordonnés pour que $n_1 \geq \cdots \geq n_r$, et $\omega_1 = [1, n_1]$, $\omega_2 = [n_1+1, n_1+n_2], \ldots$ etc. Soit a_i un élément fixé quelconque de ω_i ; notons $G_i = \mathrm{Stab}_{\mathrm{Gal}(E/k)}(a_i)$ et Ω_i le corps des invariants de G_i dans E.

Choisissons un élément ξ_i de Ω_i qui soit k-primitif, et soit P_i son polynôme minimal sur k. On a $\deg(P_i) = [\Omega_i : k] = [\mathrm{Gal}(E/k) : G_i] = n_i$, et les racines de P_i dans $\hat{k}$ sont les $\xi_{i,j} = \tau_{i,j}(\xi_i)$ $(1 \leq j \leq n_i)$, où $\{\tau_{i,j}\}_{1 \leq j \leq n_i}$ désigne une transversale quelconque de $\mathrm{Gal}(E/k)$ mod G_i. Puisque k est infini, on peut choisir les ξ_i pour que les ensembles $\{\xi_{i,j}\}_{1 \leq j \leq n_i} = \mathcal{R}_{P_i}$ soient disjoints. Posons alors

$$f = \prod_{1 \leq i \leq r} P_i \qquad , \ (f \in k[x])$$

c'est un polynôme séparable. Soit C_i la classe de conjugaison du groupe G_i dans $\mathrm{Gal}(E/k)$. Alors I_{C_i} est le sous-groupe des $\sigma \in \mathrm{Gal}(E/k)$ qui induisent l'identité sur ω_i. Donc $\bigcap_{i=1}^{r} I_{C_i} = \{\mathrm{Id}_E\}$ car la représentation (10) est fidèle. Cela signifie que le sous-groupe des $\sigma \in \mathrm{Gal}(E/k)$ tels que $\sigma(\xi_{i,j}) = \xi_{i,j}$ pour tous i et j est $\{\mathrm{Id}_E\}$, donc $E = k((\xi_{i,j})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n_i}})$, i.e. E est une k-algèbre des racines de f.

Numérotons les racines de f dans l'ordre $\xi_{1,1}, \ldots, \xi_{1,n_1}, \xi_{2,1}, \ldots, \xi_{r,1}, \ldots, \xi_{r,n_r}$. Il est alors clair que la représentation (10) n'est autre que celle associée à cette numérotation pour f. On a donc prouvé :

Proposition 2.1. Si le corps k est infini, toute représentation symétrique fidèle de degré n du groupe de Galois $\mathrm{Gal}(E/k)$ d'une extension finie galoisienne E de k peut être définie d'au moins une manière sous la forme (8) avec f séparable, $f \in k[x]$.

Remarque 1. Cette Proposition est à rapprocher du Théorème 4.6 qui permet de construire de tels polynômes f à partir de la connaissance de l'un d'eux.

Sur l'ensemble des polynômes $f \in k[x]$, normalisés, de degré $n \geq 1$, et séparables, on obtient une relation d'équivalence dont les classes sont les ensembles de polynômes ayant même k-algèbre des racines dans $\hat{k}$ et définissant des représentations équivalentes.

2.3. Soit E une extension galoisienne finie de k $(E \subset \hat{k})$.

Notant $N = [E : k]$, considérons une représentation symétrique fidèle et transitive

$$\mathrm{Gal}(E/k) \to \mathfrak{S}_N \qquad . \tag{11}$$

Soit ξ un élément primitif fixé de E sur k. Notons $G = \mathrm{Gal}(E/k) = \{\sigma_1, \ldots, \sigma_N\}$, où $\sigma_1 = \mathrm{Id}_E$, et posons $\xi_i = \sigma_i(\xi)$. On peut supposer la numérotation (σ_i) choisie

pour que $\sigma_i.1 = i$ dans la représentation (11). Il est alors clair que cette représentation n'est autre que la représentation régulière à gauche de G définie par la numérotation (σ_i). Donc la classe d'équivalence de la représentation régulière à gauche de G est définie par le polynôme k-minimal de n'importe quel élément primitif de E/k.

3. La matrice des partitions associée à un groupe fini

Le problème le plus naturel de la théorie de Galois explicite est de calculer le groupe de Galois sur K d'un polynôme donné $f \in K[x]$. La littérature disponible sur ce sujet développe la méthode suivante : à partir de " fonctions " aussi simples que possible, on calcule des " résolvantes " de f. On dresse des tables de ces résolvantes et de leur groupe associé (voir [E.H. Berwick,1929] page 11 pour la méthode jusqu'alors employée). Quand on peut relever assez d'incompatibilités dans ces tables, qui ne peuvent être que partielles, on en déduit le groupe de Galois cherché. On pourra suivre la progression de cette idée de Lagrange à Soicher (voir [L. Soicher] ou [J. McKay, L. Soicher]) en passant par Cayley, Jordan, Kronecker, Netto, Berwick, Foulkes et d'autres (voir la bibliographie jointe).

L'idée de base du présent article est d'inverser la démarche. L'étude des auteurs cités nous a convaincus que les tables partielles en question sont en fait des parties de tables purement groupistiques. Nous avons donc défini ces tables de façon globale, abstraite et indépendante, et nous en avons calculé un grand nombre grâce à des logiciels de calculs sur les groupes. De ces tables nous avons déduit les résolvantes qu'il faut calculer et non l'inverse.

Nos tables permettent de travailler sur des polynômes séparables arbitraires et non seulement sur des polynômes irréductibles. Notre méthode s'applique aussi aux " résolvantes relatives " dont on se contentait jusqu'ici de tester la linéarité de l'un de leurs facteurs.

3.1. Partitions d'un entier ≥ 1. Soit $n \in \mathbb{N}^\star$. rappelons qu'on appelle *partition* de n toute suite $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ telle que $\sum_{i=1}^n i\alpha_i = n$. Le *support* d'une telle partition est par définition l'ensemble $\{i \in [1,n] \mid \alpha_i \geq 1\}$; l'entier α_i est appelé *multiplicité* de i dans la partition, et le cardinal du support est appelé le *nombre de composants* dans la partition. Une partition ϖ de n est déterminée de manière unique par la suite strictement croissante $(d_1, \ldots, d_r)$ des termes de son support et par la suite $\nu_1 = \alpha_{d_1}, \ldots, \nu_r = \alpha_{d_r}$ des multiplicités des composants. On notera

$$\varpi = [(\nu_1, d_1), \ldots, (\nu_r, d_r)] \tag{12}$$

étant entendu que $1 \leq d_1 < \cdots < d_r \leq n$, $r \geq 1$ et $\nu_i \geq 1$ pour tout i.

3.2. Soit maintenant G un groupe fini, de cardinal N, et $\mathcal{C}$ une classe de conjugaison de sous-groupes de G, de degré $e = e_{\mathcal{C}}$. A tout couple $(H, \mathcal{C})$, où H désigne un sous groupe de G, on va associer une partition de e.

Pour cela, fixons $H_1 \in \mathcal{C}$, soit $C_1 = H_1, C_2, \ldots, C_e$ les classes à gauche de G mod H_1, et faisons opérer H à gauche sur $\mathcal{H}_1 = \{C_1, \ldots, C_e\}$ par translations à gauche.

Soit α_i le nombre de H-orbites de cardinal i dans $\mathcal{H}_1$, alors $(\alpha_1, \dots, \alpha_e)$ est une partition de e.

Lemme 1. La partition $(\alpha_1, \dots, \alpha_e)$ de e définie ci-dessus ne dépend que de $\mathcal{C}$ et non du choix de $H_1 \in \mathcal{C}$.

Démonstration. Soit $\{g_1, \dots, g_e\}$ une transversale de $G \bmod H_1$, avec $g_1 = 1_G$, et $C_i = g_i H_1$. Posons $H_i = g_i H_1 g_i^{-1}$; on a $\mathrm{Stab}_H(C_i) = H \cap H_i$. Le cardinal de la H-orbite de C_i est donc $[H : H \cap H_i]$.

Si ω est une H-orbite dans $\mathcal{H}_1$, en notant $d_\omega = \mathrm{card}(\omega)$, dans la suite d'entiers $([H : H \cap H_i])_{1 \le i \le e}$, on trouve donc d_ω fois l'entier d_ω, une fois pour chaque i tel que $C_i \in \omega$. Donc la partition $(\alpha_1, \dots, \alpha_e)$ s'obtient ainsi : pour chaque entier j, $1 \le j \le e$, $\alpha_j = N_j/j$, où $N_j = \mathrm{card}\{i \in [1,e] \mid [H : H \cap H_i] = j\}$.

Soit maintenant $H'_1 = \sigma H_1 \sigma^{-1} \in \mathcal{C}$, où $\sigma \in G$. L'ensemble $\mathcal{H}'_1$ des classes à gauche de $G \bmod H'_1$ est $\{g'_i H'_1\}_{1 \le i \le e}$, où $g'_i = \sigma g_i \sigma^{-1}$. La partition $(\alpha'_1, \dots, \alpha'_e)$ construite comme ci-dessus à partir de H'_1 est donc définie par $\alpha'_j = N'_j/j$, où $N'_j = \mathrm{card}\{i \in [1,e] \mid [H : H \cap H'_i] = j\}$ et $H'_i = g'_i H'_1 {g'_i}^{-1} = \sigma g_i H_1 g_i^{-1} \sigma^{-1} = \sigma H_i \sigma^{-1}$ pour tout i. Notons t_σ l'élément de $\mathfrak{S}_e$ tel que $H'_i = H_{t_\sigma(i)}$ pour tout i ; il est clair que les ensembles $\{i \in [1,e] \mid [H : H \cap H_{t_\sigma(i)} = j\}$ et $\{i \in [1,e] \mid [H : H \cap H_i] = j\}$ sont égaux, d'où $N_j = N'_j$ pour tout j, d'où $(\alpha'_1, \dots, \alpha'_e) = (\alpha_1, \dots, \alpha_e)$. □

Remarque 2. Il existe une variante de cette démonstration en utilisant les classes doubles modulo H.

D'après le Lemme 1, la partition $(\alpha_1, \dots, \alpha_e)$ de $e = e_{\mathcal{C}}$ construite ci-dessus ne dépend que du couple $(H, \mathcal{C})$. Nous l'appellerons *partition associée* à $(H, \mathcal{C})$ et la noterons $\varpi(H, \mathcal{C})$.

Lemme 2. Soit H un sous-groupe de G et $\mathcal{C}$ une classe de conjugaison de sous-groupes de G. La partition $\varpi(H, \mathcal{C})$ ne dépend que de la classe de conjugaison de H et de $\mathcal{C}$.

Démonstration. Reprenons les notations de la preuve du Lemme 1. Soit $H' = \sigma H \sigma^{-1}$; on a $[H' : H' \cap H'_i] = [H : H \cap H_i]$ puisque $x \mapsto \sigma x \sigma^{-1}$ est un automorphisme de G. Donc pour tout $j \in [1,e]$, $\mathrm{card}\{i \mid [H : H \cap H_i] = j\} = \mathrm{card}\{i \mid [H' : H' \cap H'_i] = j\}$. □

Finalement soit $\mathcal{E}$ l'ensemble des classes de conjugaison de sous-groupes de G. Pour $\mathcal{C} \in \mathcal{E}$ et $\mathcal{D} \in \mathcal{E}$, posons $\varpi(\mathcal{C}, \mathcal{D})$ égale à la valeur commune des $\varpi(H, \mathcal{D})$. Cette partition $\varpi(\mathcal{C}, \mathcal{D})$ sera dite *associée* à $\mathcal{C}, \mathcal{D}$.

Ordonnons $\mathcal{E}$ en une suite $\mathcal{C}_1, \dots, \mathcal{C}_s$ par degrés décroissants, de sorte que $\mathcal{C}_1 = \{\{e_G\}\}$ et $\mathcal{C}_s = \{G\}$. On obtient une matrice carrée :

$$\mathcal{P} = [\varpi(\mathcal{C}_i, \mathcal{C}_j)]_{1 \le i,j \le s} \quad , \tag{13}$$

que nous appellerons *matrice des partitions* définie par G.

Pour calculer chaque coefficient $\varpi(\mathcal{C}_i, \mathcal{C}_j)$ de la matrice $\mathcal{P}$, choisissons des éléments H_i et H_j dans les classes $\mathcal{C}_i$ et $\mathcal{C}_j$ respectivement. Soit $e_j = [G : H_j]$, et

soit $\{\gamma_m\}_{1\le m\le e_j}$ une transversale à gauche de $G \bmod H_j$, avec $\gamma_1 = 1_G$. Alors $\varpi(\mathcal{C}_i, \mathcal{C}_j) = (\alpha_1, \dots, \alpha_{e_j})$, où pour tout $l \in [1, e_j]$:

$$\alpha_l = \frac{1}{l}\,\mathrm{card}\{m \in [1, e_j] \mid [H_i : \gamma_m\, H_j\, \gamma_m^{-1} \cap H_i] = l\} \qquad . \tag{14}$$

Notons que, posant

$$\varpi(\mathcal{C}_i, \mathcal{C}_j) = [(\nu_{i,j,1}, d_{i,j,1}), \dots, (\nu_{i,j,r_{i,j}}, d_{i,j,r_{i,j}})] \qquad ,$$

($1 \le d_{i,j,1} < \cdots < d_{i,j,r_{i,j}} \le e_j$, $\nu_{i,j,l} \ge 1$), alors il est clair d'après (14) que les éléments $d_{i,j,l}$ du support de $\varpi(\mathcal{C}_i, \mathcal{C}_j)$ sont des diviseurs de $\mathrm{card}(H_i) = N/[G : H_i]$.

Voici maintenant le théorème fondamental qui va être à la base de tous les calculs explicites ultérieurs de groupes de Galois :

Théorème 3.1. Les lignes de la matrice $\mathcal{P}$ définie par (13) sont distinctes. Par suite il y a une bijection naturelle entre l'ensemble de ces lignes et l'ensemble $\mathcal{E} = \{\mathcal{C}_1, \dots, \mathcal{C}_s\}$.

Démonstration. Choisssons dans chaque classe $\mathcal{C}_i$ un élément H_i. Fixons i et j, avec $1 \le j < i \le s$. Calculons la matrice $\mathcal{P}$ par la formule (14). Pour la partition $\varpi(\mathcal{C}_j, \mathcal{C}_j)$, on a $d_{j,j,1} = [H_j : H_j \cap H_j] = 1$, avec multiplicité $\nu_{j,j,1} = [\mathcal{N}_G(H_j) : H_j]$, où $\mathcal{N}_G(H_j)$ désigne le normalisateur de H_j dans G. Pour la partition $\varpi(\mathcal{C}_i, \mathcal{C}_j)$, aucun des $\gamma_m\, H_j\, \gamma_m^{-1}$ ne peut être égal à H_i, car $\mathcal{C}_i \ne \mathcal{C}_j$, ni contenir H_i, car $e_j \ge e_i$; donc lorsque m décrit $[1, e_j]$, les indices $[H_i : \gamma_m\, H_j\, \gamma_m^{-1} \cap H_i]$ sont tous > 1. Donc $d_{i,j,1} > 1$, d'où $\varpi(\mathcal{C}_i, \mathcal{C}_j) \ne \varpi(\mathcal{C}_j, \mathcal{C}_j)$ et les lignes d'indices i et j sont bien distinctes. □

Lorsque $G = \mathfrak{S}_n$, nous avons calculé la matrice des partitions complète pour $n \in \{4, 5, 6, 7\}$ (pour $n = 7$, il y a 96 classes de conjugaisons et le tableau occupe 50 pages d'impression en Latex, contre 2 si les lignes retenues ne concernent que les 7 classes de sous-groupes transitifs $\mathfrak{S}_7$). Pour $n = 8$, nous avons calculé les $\varpi(\mathcal{C}_i, \mathcal{C}_j)$ pour les 50 indices i tels que $\mathcal{C}_i$ soit une classe de sous-groupes transitifs de $\mathfrak{S}_8$, et pour 110 classes $\mathcal{C}_j$ sur les 296, excluant ainsi celles dont le degré dépasse 672 (i.e. celles qui donneraient des polynômes de degré ≥ 672 à factoriser).

Pour $n = \{9, 10, 11\}$, nous avons calculé les $\varpi(\mathcal{C}_i, \mathcal{C}_j)$ pour les indices i tels que $\mathcal{C}_i$ soit une classe de sous-groupes de $\mathfrak{S}_n$, et pour les classes $\mathcal{C}_j$ qui nous ont paru dignes d'intérêt compte tenu des matrices déjà obtenues en degré < 9 : pour ces 3 tables, nous avons utilisé la nomenclature des sous-groupes transitifs de $\mathfrak{S}_n$ pour $n \le 11$ donnée par [G. Butler, J. McKay].

Le calcul de tables partielles pour $n \in \{12, 13, 14, 15\}$ est en cours.

Par exemple, il apparait qu'en degré 9, il existe une unique classe de sous-groupes transitifs de $\mathfrak{A}_9$, dont la partition avec la classe de $\mathfrak{A}_8 \times \{\mathrm{Id}\}$ soit (18). En d'autres termes, il sera extrêmement rapide d'identifier un polynôme de degré 9 ayant un des groupes de cette classe comme groupe de Galois.

Lorsque $G \neq \mathfrak{S}_n$, cas qu'il faut envisager pour exploiter les résolvantes relatives (cf. Théorème 6.11 ci-après), les calculs de tables sont bien évidemment plus faciles que dans le cas des groupes $\mathfrak{S}_n$ (il y a moins de groupes et les partitions sont plus courtes, cf. Remarque 12 page 27)

Tous ces calculs ont été exécutés à l'aide du logiciel [`G.A.P`] (=Groups, Algorithms and Programming).

4. La notion de résolvante de Lagrange

Nous donnons ici la définition de la résolvante de Lagrange *générique* (terme qui traduit l'ancienne expression " fonction en forme " par opposition à "fonction en valeur ", qui en sont les diverses spécialisations), et nous verrons dans les paragraphes ultérieurs des propriétés que l'on peut tirer de ses spécialisations. Elle est, entre autres, l'outil technique permettant d'identifier la classe de conjugaison du groupe de Galois d'un polynôme donné.

On considère n indéterminées $x_1, \ldots, x_n$ sur $\hat{k}$. On note $\mathcal{F}$ le corps $k(x_1, \ldots, x_n)$, $\mathcal{A}$ l'anneau $k[x_1, \ldots, x_n]$, $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires des x_i ($\sigma_i \in \mathcal{A}$), $\mathcal{S}$ l'anneau $k[\sigma_1, \ldots, \sigma_n]$ et $\mathcal{K}$ le corps $k(\sigma_1, \ldots, \sigma_n)$ des fractions de $\mathcal{S}$.

On sait que $\mathcal{F}$ est une extension galoisienne de $\mathcal{K}$, qui est une $\mathcal{K}$-algèbre des racines de $F(T) = T^n - \sigma_1 T^{n-1} + \cdots + (-1)^n \sigma_n = \prod_{i=1}^{n} (T - x_i) \in \mathcal{S}[T]$; que la représentation par permutations $\mathrm{Gal}(\mathcal{F}/\mathcal{K}) \to \mathfrak{S}_n$ associée à la numérotation $(x_i)_{1 \leq i \leq n}$ est un isomorphisme de groupes ; et que $\mathcal{A}$ est la clôture intégrale de $\mathcal{S}$ dans $\mathcal{F}$.

Ci-après nous identifierons les groupes $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$ et $\mathfrak{S}_n$ à l'aide de la représentation ci-dessus.

Pour tout sous-groupe H de $\mathfrak{S}_n$, nous noterons $\mathrm{Inv}(H)$ le corps des invariants de H dans $\mathcal{F}$; donc $\mathcal{F}$ est une extension galoisienne de $\mathrm{Inv}(H)$, et $H = \mathrm{Gal}(\mathcal{F}/\mathrm{Inv}(H))$. La clôture intégrale $\mathcal{A}_H$ de $\mathcal{S}$ dans $\mathrm{Inv}(H)$ est $\mathcal{A} \cap \mathrm{Inv}(H)$. L'anneau $\mathcal{A}_H$ est intégralement clos, noethérien et c'est une k-algèbre de type fini. Puisque $\mathcal{S}$ est noethérien et intégralement clos, on en déduit que $\mathcal{A}_H$ est un $\mathcal{S}$-module de type fini. En d'autres termes, $\sigma_1, \ldots, \sigma_n$ est un *système homogène de paramètres* au sens de Stanley (voir [R.P. Stanley]) pour la k-algèbre $\mathcal{A}_H$. On voit aussi que $\mathrm{Inv}(H)$ est le corps des fractions de $\mathcal{A}_H$; en fait, on a mieux : $\mathcal{A}_H[\frac{1}{\mathcal{S}}] = \mathrm{Inv}(H)$, car si $x = \frac{\alpha}{\beta} \in \mathrm{Inv}(H)$ avec $\alpha \in \mathcal{A}$ et $\beta \in \mathcal{A} \backslash \{0\}$, il est clair que $x = \frac{a}{b}$, avec $b = \prod_{\sigma \in \mathfrak{S}_n} \sigma(\beta) \in \mathcal{S} \backslash \{0\}$ et $a = \alpha \prod_{\sigma \in \mathfrak{S}_n \,,\, \sigma \neq \mathrm{Id}} \sigma(\beta) \in \mathcal{A}_H$.

Théorème 4.1. Supposons k de caractéristique 0. Soit H un sous-groupe de $\mathfrak{S}_n$. Alors $\mathcal{A}_H = \mathcal{A} \cap \mathrm{Inv}(H)$ est un $\mathcal{S}$-module libre de type fini, dont le rang est $e = [\mathfrak{S}_n : H]$.

Démonstration. Le fait que $\mathcal{A}_H$ est un $\mathcal{S}$-module libre de type fini découle de ce que $(\sigma_1, \ldots, \sigma_n)$ est un système homogène de paramètres de $\mathcal{A}_H$. (voir [R.P. Stanley]).

Le rang r de ce module est évidemment $r = \dim_{|\mathcal{K}}(\mathcal{K} \bigotimes_{\mathcal{S}} \mathcal{A}_H)$. Mais on a vu que $\mathrm{Inv}(H) = \mathcal{A}_H[\frac{1}{\mathcal{S}}] \cong \mathcal{K} \bigotimes_{\mathcal{S}} \mathcal{A}_H$. Donc d'après la théorie de Galois, on a bien $r = \dim_{\mathcal{K}}(\mathrm{Inv}(H)) = [\mathfrak{S}_n : H]$ □

On peut construire concrètement une base du $\mathcal{S}$-module $\mathcal{A}_H$ de la manière suivante : notons $\mathfrak{I}_H$ l'idéal de $\mathcal{A}_H$ engendré par $\sigma_1, \dots, \sigma_n$. On sait (voir [R.P. Stanley]) que des éléments homogènes $\eta_1, \dots, \eta_e$ de $\mathcal{A}_H$ formeront une base de $\mathcal{S}$-module ssi leurs images dans $\mathcal{A}_H/\mathcal{J}_H$ forment une base de k-espace vectoriel de $\mathcal{A}_H/\mathcal{J}_H$. Soient $(\mathfrak{I}_H)_m$ et $(\mathcal{A}_H)_m$ les composantes homogènes de degré m de $\mathfrak{I}_H$ et $\mathcal{A}_H$; soit $\mathfrak{I}$ l'idéal de $\mathcal{A}$ engendré par $(\sigma_1, \dots, \sigma_n)$ et $\mathfrak{I}_m$ la composante homogène de degré m. On sait que $\dim_k(\mathcal{A}/\mathfrak{I}) = n! = \sum_{m\geq 0} \dim_k(\mathcal{A}_m/\mathfrak{I}_m) = \dim_{\mathcal{S}}(\mathcal{A})$, la famille $(P_\alpha)_{\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n, \alpha_1<1,\dots,\alpha_n<n} = (x_1^{\alpha_1}\cdots x_n^{\alpha_n})_{\alpha_1<1,\dots,\alpha_n<n}$ étant une base de $\mathcal{A}$ comme $\mathcal{S}$-module et de $\mathcal{A}/\mathfrak{I}$ comme k-espace vectoriel. Supposons toujours la caractéristique de k nulle. Posons :

$$\hat{P}_\alpha = \frac{1}{\mathrm{card}(H)} \sum_{h\in H} h \star P_\alpha \qquad ;$$

alors $(\hat{P}_\alpha)_{\alpha_1<1,\dots,\alpha_n<n}$ engendre $\mathcal{A}_H$ comme $\mathcal{S}$-module, donc engendre $\mathcal{A}_H/\mathfrak{I}_H$ comme k-espace vectoriel. De plus, $(\mathfrak{I}_H)_m = (\mathcal{A}_H)_m \cap \mathfrak{I}_m$, donc $(\mathfrak{I}_H)_m$ est engendré par les éléments homogènes de degré m du type $\sum_\alpha \eta_\alpha \hat{P}_\alpha$, où $\eta_\alpha \in k[\sigma_1, \dots, \sigma_n]$ est un polynôme sans terme constant en les σ_i, tandis que $(\mathcal{A}_H)_m$ est engendré par les $\sum_\alpha \eta_\alpha \hat{P}_\alpha$, où $\eta_\alpha \in k[\sigma_1, \dots, \sigma_n]$ est un polynôme homogène en les x_i tel que $\deg(\eta_\alpha P_\alpha) = m$ (voir [R.P. Stanley]).

Existence d'éléments primitifs homogènes

Soit toujours H un sous-groupe de $\mathfrak{S}_n$. Le corps $\mathrm{Inv}(H)$ est le corps des fractions de $\mathcal{A}_H$. Plus précisément, comme nous l'avons vu juste avant le Théorème 4.1, on a : $\mathrm{Inv}(H) \cong \mathcal{K} \bigotimes_{\mathcal{S}} \mathcal{A}_H$. Comme $\mathrm{Inv}(H)$ est séparable sur $\mathcal{K}$, il admet des éléments $\mathcal{K}$-primitifs. Donc il existe des éléments $\Psi \in \mathcal{A}_H$ qui sont $\mathcal{K}$-primitifs pour le corps $\mathrm{Inv}(H)$. En fait il existe toujours de tels éléments qui soient homogènes, pourvu que k soit infini. En effet, soit $\Psi \in \mathcal{A}_H$ élément $\mathcal{K}$-primitif de degré d ; soit λ une indéterminée sur $\mathcal{K}$, notons Ψ_λ l'homogénéisé de Ψ par $\lambda\sigma_1$:

$$\Psi_\lambda = (\lambda\sigma_1)^d \Psi(\frac{x_1}{\lambda\sigma_1}, \dots, \frac{x_n}{\lambda\sigma_1}) \qquad .$$

Soit $(t_i)_{1\leq i\leq e}$ une transversale à gauche de $\mathfrak{S}_n$ mod H. Notons $\mathcal{D}(\lambda)$ le x-discriminant de $P_\lambda(x) = \prod_{1\leq i\leq e}(x - t_i \star \Psi_\lambda)$. Alors $\mathcal{D}(\lambda) \in \mathcal{S}[\lambda]$ et puisque Ψ est $\mathcal{K}$-primitif, on a $\mathcal{D}(\frac{1}{\sigma_1}) \neq 0$, car $P_{\frac{1}{\sigma_1}}(x) = \mathcal{L}_\Psi$ est le polynôme minimal de Ψ sur $\mathcal{K}$. Donc $\mathcal{D}(\lambda) \neq 0$. Le corps k étant infini, on a $\tilde{\lambda} \in k$ tel que $\mathcal{D}(\tilde{\lambda}) \neq 0$, d'où alors $\Theta = \Psi_{\tilde{\lambda}}$ est encore $\mathcal{K}$-primitif, est homogène de degré d et $\mathcal{L}_\Theta = P_{\tilde{\lambda}}(x)$ est le polynôme minimal de Θ sur $\mathcal{K}$. (Les notations $\mathcal{L}_\Psi$ et $\mathcal{L}_\Theta$ sont celles introduites ci-dessous.)

Définition 4.2. Dans les conditions ci-dessus, tout élément $\Psi \in \mathrm{Inv}(H)$ qui est $\mathcal{K}$-primitif et qui appartient à $\mathcal{A}_H$ est appelé un *résolvant* de H. Un tel résolvant est dit *homogène* ssi c'est un polynôme homogène des x_i. Le polynôme $\mathcal{K}$-minimal d'un tel résolvant Ψ sera appelé *résolvante de Lagrange* de H associées à Ψ et noté $\mathcal{L}_\Psi$: on a donc $\mathcal{L}_\Psi \in \mathcal{S}[x]$.

D'après la théorie de Galois, étant donné $\Psi \in \mathcal{A}$, si on pose $H = \mathrm{Stab}_{\mathfrak{S}_n}(\Psi)$, alors Ψ est un résolvant de H.

Remarque 3. Il existe un algorithme parallélisable (voir [A. Valibouze1] page 99) permettant de calculer le polynôme minimal d'un nombre algébrique obtenus par une relation algébrique entre les racines de polynômes d'une variable donnés. Cet algorithme s'optimise grâce au Théorème de l'arité (voir [A. Valibouze2] ou [A. Valibouze1]). Cet algorithme était utilisé par Lagrange (voir par exemple [J.L. Lagrange, tome VIII] page 236, le calcul d'une résolvante produit) pour calculer des résolvantes particulières ; c'est pourquoi nous proposons de l'appeler *Algorithme de Lagrange*. Dans [A. Valibouze4] un nouvel algorithme utilise une base standard de l'idéal de relations symétriques afin de calculer efficacement des résolvantes avec des résultants. Dans [F. Lehobey] l'auteur décrit également une méthode efficace pour calculer des résolvantes avec des résultants et étudie la factorisation des polynômes appliquée aux résolvantes. LL'auteur réalisé ses implantations en `AXIOM`. Un module [A. Valibouze5] de calculs de résolvantes est fourni avec la dernière version du système de calcul formel [MAXIMA]. Il existe d'autres méthodes permettant de calculer de résolvantes ; entre autres dans [L. Soicher] (avec des résultants), [K. Girstmair] (par interpolation), [D. Casperson, J. McKay] (avec des séries génératrices), [E.H. Berwick,1915] (avec des invariants).

Théorème 4.3. (Lagrange) Soit H un sous-groupe de $\mathfrak{S}_n$ et Ψ un résolvant de H. Notons Δ_Ψ le discriminant de la résolvante de Lagrange $\mathcal{L}_\Psi$. On a :

$$\mathcal{A}_H \subset \frac{1}{\Delta_\Psi}\mathcal{S}[\Psi] \qquad .$$

Démonstration. (d'après Lagrange) Soit $e = [\mathfrak{S}_n : H]$ et $\{t_i\}_{1\leq i\leq e}$ une transversale de $\mathfrak{S}_n \bmod H$, avec $t_1 = \mathrm{Id}_{\mathfrak{S}_n}$. Posons $\Psi_i = t_i \star \Psi$ (donc $\Psi = \Psi_1$), d'où $\mathcal{L}_\Psi = \prod_{i=1}^{e}(x - \Psi_i) = x^e - C_1 x^{e-1} + \cdots + (-1)^e C_e$ ($\mathcal{L}_\Psi \in \mathcal{S}[x]$). (Notons que $\mathcal{L}_\Psi$ est théoriquement calculable à l'aide du théorème fondamental sur les fonctions symétriques.)

Fixons $g \in \mathcal{A}_H$, soit $g_j = t_j \star g$. Posons, pour $0 \leq m \leq e-1$:

$$h_m = \sum_{j=1}^{e} g_j \Psi_j^m \qquad = \sum_{j=1}^{e} t_j \star (g\Psi^m). \tag{15}$$

Il est clair que $h_m \in \mathcal{S}$ (et h_m est théoriquement calculable). On considère (15) comme un système de Cramer en les g_j. La résolution donne :

$$g_1 = \frac{1}{\delta_\Psi}\mathcal{D} \qquad , \text{ où} \tag{16}$$

$$\mathcal{D} = \begin{vmatrix} h_0 & 1 & \cdots & 1 \\ h_1 & \Psi_2 & \cdots & \Psi_e \\ \vdots & \vdots & & \vdots \\ h_{e-1} & \Psi_2^{e-1} & \cdots & \Psi_e^{e-1} \end{vmatrix}$$

et $\delta_\Psi = \mathrm{Vand}(\Psi_1, \dots, \Psi_e) = \prod_{1 \le i < j \le e}(\Psi_j - \Psi_i)$, donc $\delta_\Phi^2 = \Delta_\Psi \in \mathcal{S}$, et (16) équivaut à

$$g = \frac{1}{\Delta_\Psi}\mathcal{E} \text{ , où } \mathcal{E} = \delta_\Psi \mathcal{D} \qquad . \tag{17}$$

On prouve ensuite que $\mathcal{E} \in \mathcal{S}[\Psi]$. Pour cela, notons que $\mathcal{E} = E(\Psi_2, \dots, \Psi_e)$ avec $E \in \mathcal{S}[\Psi][T_2, \dots, T_e]$ et E symétrique en $T_2, \dots, T_e$ (c'est évident sur δ_Ψ et sur $\mathcal{D}$).

D'après le théorème fondamental des fonctions symétriques, $E(\Psi_2, \dots, \Psi_e) = F(S_1, \dots, S_{e-1})$, où $F \in \mathcal{S}[\Psi][Y_1, \dots, Y_{e-1}]$ et où les S_i sont les fonctions symétriques élémentaires en $\Psi_2, \dots, \Psi_e$. Mais $(x - \Psi_2)\dots(x - \Psi_e) = \frac{\mathcal{L}_\Psi(x)}{x - \Psi} = x^{e-1} + (\Psi - C_1)x^{e-2} + \cdots \in \mathcal{S}[\Psi][x]$. Donc $S_j \in \mathcal{S}[\Psi]$ pour tout j. D'où $E(\Psi_2, \dots, \Psi_e) = \mathcal{E} = F(S_1, \dots, S_{e-1}) \in \mathcal{S}[\Psi]$. Donc d'après (17) : $g \in \frac{1}{\Delta_\Psi}\mathcal{S}[\Psi]$ □

Remarque 4. *Analyse de la démonstration du Théorème* 4.3 : Cette démonstration est en substance celle donnée par Lagrange dans ses Réflexions sur la résolution des équations algébriques. Il est intéressant de la situer par rapport à la théorie moderne des corps ; pour cela, conservons-en toutes les notations. Le corps $\mathrm{Inv}(H)$ est une extension finie séparable de $\mathcal{K}$, dont $\mathcal{B} = (1, \Psi, \Psi^2, \dots, \Psi^{e-1})$ est une $\mathcal{K}$-base. Notons $p(x) = \mathcal{L}_{\Psi,f}(x)$ et soit $\frac{p(x)}{x - \Psi} = \alpha_0 + \alpha_1 x + \cdots + \alpha_{e-1}x^{e-1}$. Soit Tr la trace de $\mathrm{Inv}(H)$ relativement à $\mathcal{K}$. Selon les conventions habituelles, pour toute partie M de $\mathrm{Inv}(H)$, notons M^* l'ensemble $\{\xi \in \mathrm{Inv}(H) \mid \mathrm{Tr}(\xi M) \subset \mathcal{S}\}$. D'après le Théorème d'Euler bien connu, la base complémentaire de $\mathcal{B}$ dans $\mathrm{Inv}(H)$ est $(\alpha_i/p'(\Psi))_{1 \le i \le e-1}$, c'est-à-dire qu'on a : $\mathrm{Tr}(\Psi^j \alpha_i/p'(\Psi)) = \delta_{i,j}$ $(0 \le i \le e-1,\ 0 \le j \le e-1,\ \delta_{i,j} =$ symbole de Knonecker), d'où l'on déduit classiquement (puisque $\mathcal{A}_H$ est la clôture intégrale de $\mathcal{S}$ dans $\mathrm{Inv}(H)$) :

$$\mathcal{S}[\Psi] \subset \mathcal{A}_H \subset \mathcal{A}_H^* \subset \mathcal{S}[\Psi]^* = \frac{1}{p'(\Psi)}\mathcal{S}[\Psi] \qquad .$$

Posons $\eta = p'(\Psi)$; soit u l'élément de $\mathrm{Hom}_\mathcal{K}(\mathrm{Inv}(H))$ défini par la multiplication par η. Les relations ci-dessus montrent que $u(\mathcal{A}_H) \subset \mathcal{S}[\Psi]$. Comme $p(x) \in \mathcal{S}[x]$, la matrice de u dans la base $\mathcal{B}$ est à coefficients dans $\mathcal{S}$. Les formules de Cramer permettent donc à partir de : $u(\mathcal{A}_H) \subset \mathcal{S}[\Psi]$, de déduire que $\det(u)\mathcal{A}_H \subset \mathcal{S}[\Psi]$. Mais en notant $\mathcal{N}$ la norme de $\mathrm{Inv}(H)$ relative à $\mathcal{K}$, on a : $\det(u) = \mathcal{N}(\eta) = (1-)^{e(e-1)/2}\Delta_\Psi$, ce qui redémontre que $\Delta_\Psi \mathcal{A}_H \subset \mathcal{S}[\Psi]$.

Nous voyons donc que Lagrange, par son raisonnement direct, réussit à se passer de l'intermédiaire $u(\mathcal{A}_H) \subset \mathcal{S}[\Psi]$.

Spécialisation d'une résolvante

Dans ce sous-paragraphe, nous fixons un polynôme $f \in k[x]$, de degré $n \geq 1$, séparable, normalisé, et nous notons E la k-algèbre de ses racines dans $\hat{k}$. On numérote une fois pour toutes l'ensemble $\mathcal{R}_f$ des racines dans $\hat{k}$: $\mathcal{R}_f = \{\rho_1, \dots, \rho_n\}$. Revenons aux notations et hypothèses de la Définition 4.2. Posons :

$$f = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n \quad ; \tag{18}$$

Définition 4.4. Soit Ψ un résolvant du sous-groupe H de $\mathfrak{S}_n$. On appellera (H, Ψ)-*résolvante (de Lagrange) de* f, et on notera $\mathcal{L}_{\Psi,f}$, le polynôme obtenu en substituant les c_i de (18) aux σ_i dans $\mathcal{L}_\Psi$. On dira que Ψ est f-*séparable* ssi la résolvante $\mathcal{L}_{\Psi,f}$ est séparable.

Les résolvantes les plus commodes à utiliser sont les résolvantes séparables. On a :

Théorème 4.5. Supposons le corps k infini. Soit A un sous-anneau de k dont k soit le corps des fractions. Il existe un résolvant $\Psi \in A[x_1, \dots, x_n]$ de H tel que $\mathcal{L}_{\Psi,f}$ soit séparable, et on peut choisir Ψ homogène.

Démonstration. Soit $\mathcal{H}$ l'ensemble des classes à gauche de $\mathfrak{S}_n$ mod H. Prenons n indéterminées $U_1, \dots, U_n$. Puisque les ρ_i sont distincts, lorsque s décrit $\mathfrak{S}_n$, les $n!$ polynômes $(\sum_{i=1}^n U_i \rho_{s(i)}) - 1 \in k[U_1, \dots U_n]$ sont deux à deux premiers entre eux. Donc si, pour $C \in \mathcal{H}$, on définit $\varphi_C \in k[U_1, \dots U_n]$ par

$$\varphi_C = \prod_{s \in C} [(\sum_{i=1}^n U_i \rho_{s(i)}) - 1] \quad , \tag{19}$$

les φ_C $(C \in \mathcal{H})$ sont aussi deux à deux premiers entre eux, et a fortiori distincts. Comme A est infini, on peut donc trouver $(u_1, \dots, u_n) \in A^n$ tel que les éléments $(\varphi_C(u_1, \dots, u_n))_{C \in \mathcal{H}}$ soient distincts. Pour un tel choix de $(u_1, \dots, u_n)$ posons :

$$\Psi = \prod_{s \in H} [(\sum_{i=1}^n u_i x_{s(i)}) - 1] \quad ; \tag{20}$$

on a : $\Psi \in \mathrm{Inv}(H) \cap A[x_1, \dots, x_n]$. Les conjugués de Ψ dans l'extension $\mathcal{F}$ de $\mathcal{K}$ sont les $\Psi_C = \prod_{s \in C} [(\sum_{i=1}^n u_i x_{s(i)}) - 1]$, $C \in \mathcal{H}$. (Ainsi $\Psi = \Psi_H$). D'après le choix des u_i, ces conjugués sont distincts, donc Ψ est un résolvant de H. Il est clair que

$$\mathcal{L}_{\Psi,f}(x) = \prod_{C \in \mathcal{H}} (x - \Psi_C(\rho_1, \dots, \rho_n)) \quad , \tag{21}$$

donc $\mathcal{L}_{\Psi,f}$ est séparable.

Pour obtenir un résolvant homogène, raisonnons comme nous l'avons fait précédemment. Soit λ une indéterminée sur $\mathcal{F}$. Posons $(\Psi_C)_\lambda$ l'homogénéisé de Ψ_C par $\lambda\sigma_1$, et :

$$\mathcal{P}_\lambda(x) = \prod_{C\in\mathcal{H}} (x - (\Psi_C)_\lambda) \; ;$$

soit $\mathcal{D}(\lambda)$ le x-discriminant de $\mathcal{P}_\lambda(x)$, et soit $D(\lambda) \in A[\lambda]$ obtenu en spécialisant les σ_i en les c_i dans $\mathcal{D}(\lambda)$. On a $D(\frac{1}{\sigma_1}) \neq 0$, car $D(\frac{1}{\sigma_1})$ est le discriminant de $P_{\frac{1}{\sigma_1}}(x) = \mathcal{L}_{\Psi,f}(x)$. Puisque A est infini, on peut trouver $\tilde{\lambda} \in A$ tel que $D(\tilde{\lambda}) \neq 0$, car $D(\lambda) \neq 0$ d'après ce qu'on vient de voir. Posons, après avoir fixé un tel $\tilde{\lambda}$:

$$\Theta = \Psi_{\tilde{\lambda}} \qquad .$$

Alors $\Theta \in \mathrm{Inv}(H) \cap A[x_1, \ldots, x_n]$; Θ est homogène de degré $\deg(\Psi)$ (=card(H)) en les x_i. Les conjugués de Θ dans l'extension $\mathcal{F}$ de $\mathcal{K}$ sont les $\Theta_C = (\Psi_C)_{\tilde{\lambda}}$.

Soit $\theta_C \in k$ obtenu en substituant $\rho_1, \ldots, \rho_n$ à $x_1, \ldots, x_n$ dans Θ_C. On a : $\mathcal{L}_{\Theta,f}(x) = \prod_{C\in\mathcal{H}}(x - \theta_C)$, et le discriminant de $\mathcal{L}_{\Theta,f}$ est $D(\tilde{\lambda}) \neq 0$, donc d'une part les $(\Theta_C)_{C\in\mathcal{H}}$ sont nécessairement tous distincts, ce qui prouve que Θ est un résolvant de H, et d'autre part le polynôme $\mathcal{L}_{\Theta,f}$ est séparable, i.e. ce résolvant est séparable □

Théorème 4.6. Supposons k infini. Soit A un sous-anneau de k dont k soit le corps des fractions. Soit Ψ un résolvant d'un sous-groupe H de $\mathfrak{S}_n$ tel que : $\mathcal{L}_{\Psi,f}$ est séparable, $n \geq 5$, et $H \notin \{\mathfrak{A}_n, \mathfrak{S}_n\}$, où $\mathfrak{A}_n$ est le groupe alterné. Alors la k-algèbre des racines de $\mathcal{L}_{\Psi,f}$ dans $\hat{k}$ est E, celle de f.

Démonstration. Soient $\Psi_1, \ldots, \Psi_e$ les conjugués de Ψ dans l'extension $\mathcal{F}$ de $\mathcal{K}$, avec $\Psi = \Psi_1$. Posons $\tilde{\Psi}_i = \Psi_i(\rho_1, \ldots, \rho_n)$. Choisissons $a_1, a_2, \ldots, a_e$ éléments de A (où $e = [\mathfrak{S}_n : H]$) tels que les éléments $\lambda_s = \sum_{i=1}^e a_i \tilde{\Psi}_{s(i)}$ $(s \in \mathfrak{S}_e)$ soient tous distincts (c'est possible puisque d'après l'hypothèse les $\tilde{\Psi}_i$ sont distincts). L'action de $\mathfrak{S}_n = \mathrm{Gal}(\mathcal{F}/\mathcal{K})$ sur $\{\Psi_1, \ldots, \Psi_e\}$ est transitive, de plus comme par hypothèse $n \geq 5$, les seuls groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{A}_n, \mathfrak{S}_n$ et $\{1\}$ et comme on a $e \geq 3$, cette action est donc fidèle, ce qui revient à dire que :

$$\mathcal{K}[\Psi_1, \ldots, \Psi_e] = \mathcal{F} \qquad ; \tag{22}$$

on a une représentation naturelle de $\mathfrak{S}_n$ par permutations de $\{\Psi_1, \ldots, \Psi_e\}$, qui est fidèle et transitive, et qui associe à toute $\varphi \in \mathfrak{S}_n$, l'unique $s_\varphi \in \mathfrak{S}_e$ tel que $\varphi(\Psi_i) = \Psi_{s_\varphi(i)}$ pour tout i (voir § 2). Notons Γ_n le sous-groupe de $\mathfrak{S}_e$ image de cette représentation, alors Γ_n est l'image naturelle dans $\mathfrak{S}_e$ de $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$, i.e. de la $\mathcal{K}$-algèbre des racines dans $\mathcal{F}$ du polynôme $\mathcal{L}_\Psi$. Puisque les éléments $(\sum_{i=1}^e a_i \Psi_{s(i)})_{s\in\Gamma_n}$ de $\mathcal{F}$ sont distincts, on voit que $\Phi = \sum_{i=1}^e a_i \Psi_i$ est élément primitif de $\mathcal{F}$ sur $\mathcal{K}$. D'après le Théorème 4.3, appliqué avec $H = \{1\}$, et avec le résolvant Φ de ce H, on a (puisque $\mathcal{A}_{\{1\}} = \mathcal{A}$) : $\mathcal{A} \subset \frac{1}{\Delta_\Phi}\mathcal{S}[\Phi]$, où Δ_Φ est le x-discriminant du polynôme

$$\prod_{s\in\Gamma_n}(x-\sum_{i=1}^{e}a_i\Psi_{s(i)}) \qquad ;$$

puisque $\mathcal{S}[\Phi]\subset\mathcal{S}[\Psi_1,\dots,\Psi_e]$, on en déduit :

$$\left\{\begin{array}{l}\mathcal{A}\subset\frac{1}{\Delta_\Phi}\mathcal{S}[\Psi_1,\dots,\Psi_e] \quad \text{c'est à dire :}\\ \Delta_\Phi\mathcal{A}\subset\mathcal{S}[\Psi_1,\dots,\Psi_e]\end{array}\right. ; \tag{23}$$

$$\text{Posons } \tilde{\Delta}_\Phi=\Delta_\Phi(\rho_1,\dots,\rho_n)=\epsilon\prod_{s,t\in\Gamma_n,s\neq t}(\lambda_s-\lambda_t)$$

(où $\epsilon=(-1)^{n!(n!-1)/2}$). Par le choix même de Φ, on a $\tilde{\Delta}_\Phi\neq 0$. En spécialisant les deux membres de (23), on obtient donc $E=\tilde{\Delta}_\Phi k[\rho_1,\dots,\rho_n]\subset k[\tilde{\Psi}_1,\dots,\tilde{\Psi}_e]\subset E$, d'où $E=(=k[\rho_1,\dots,\rho_n])=k[\tilde{\Psi}_1,\dots,\tilde{\Psi}_e]$ □

Remarque 5. Ce Théorème 4.6 améliore le résultat donné par [L.E. Dickson] pages 190 et suivantes ; les groupes notés G et Γ dans cette référence sont respectivement $\mathrm{Gal}(f/k)$ et $\mathrm{Gal}(\mathcal{L}_{\Psi,f}/k)$, et Dickson dit que " G est simplement ou multiplement isomorphe à Γ, et donc que $\mathrm{card}(G)\geq\mathrm{card}(\Gamma)$. ".

Remarque 6. Sous les hypothèses du Théorème 4.6, Soit $P_1P_2\dots P_r$ une décomposition dans $k[x]$ en facteurs irréductibles normalisés de $\mathcal{L}_{\Psi,f}(x)$. Si $\mathrm{Gal}(E/k)$ est simple, on a $\mathrm{Gal}(P_i/k)\cong\mathrm{Gal}(E/k)$ pour tout i tel que $\deg(P_i)>1$. Sinon, on obtient une tour normale de sous-groupes de $\mathrm{Gal}(E/k)$:

$$\{1\}\to\mathrm{Gal}(K_1/k)\to\cdots\to\mathrm{Gal}(K_{r-1}/k)\to\mathrm{Gal}(K_r/k)=\mathrm{Gal}(E/k) \qquad ,$$

où K_i désigne le corps des racines de $P_1P_2\dots P_i$ dans E $(1\leq i\leq r)$. Cette tour donne évidemment, pour $1\leq i\leq r$:

$$\mathrm{Gal}(K_i/k)\cong\mathrm{Gal}(K_{i+1}/k)/\mathrm{Gal}(K_{i+1}/K_i)$$

$(\mathrm{Gal}(K_{i+1}/K_i)=\mathrm{Gal}(P_{i+1}/K_i))$, i.e. $\mathrm{Gal}(K_{i+1}/k)$ est une extension de $\mathrm{Gal}(K_i/k)$ par $\mathrm{Gal}(P_{i+1}/K_i)$.

Remarque 7. Le Théorème 4.6 est très utile pour construire des polynômes particuliers de groupe de Galois donné. On en verra plus loin quelques exemples.

5. Résolvantes et idéaux de $k[x_1, \dots, x_n]$

Reprenons les notations du §4. Nous utiliserons ci-dessous la terminologie et les résultats de [J.M. Arnaudiès] relatifs aux variétés de dimension zéro. (Rappelons que selon cette terminologie, le mot variété désigne des ensembles de points.) Donc nous supposerons ici que k est de caractéristique nulle. Nous noterons : $\hat{\mathcal{A}} = \hat{k} \bigotimes_k \mathcal{A}$; $\mathfrak{I}$ l'idéal de $\mathcal{A}$ engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n\}$ dit *idéal des relations symétriques* ; $\hat{\mathfrak{I}} = \hat{k} \bigotimes \mathfrak{I}$ l'idéal de $\hat{\mathcal{A}}$ engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n\}$; $\mathcal{W}$ la variété de dimension zéro définie par $\hat{\mathfrak{I}}$ dans $\hat{k}^n$; $\Gamma = \mathrm{Gal}(E/k)$; $N = \mathrm{card}(\Gamma)$. Dans [A. Mach, A. Valibouze] on trouvera une formule close donnant une base standard de l'idéal $\mathfrak{I}$ relativement à l'ordre lexicographique.

On a une représentation par permutations fidèle $R : \Gamma \to \mathfrak{S}_n$ qui associe, à tout élément $u \in \Gamma$, la permutation $s_u \in \mathfrak{S}_n$ telle que $u(\rho_i) = \rho_{s_u(i)}$ pour tout $i \in [1, n]$. Nous conviendrons d'identifier Γ à un sous-groupe de $\mathfrak{S}_n$ à l'aide de R. Cette identification sera systématiquement utilisée par la suite. Notons ici que pour tout $g \in \mathcal{A}$ et tout $s \in \Gamma$, on a :

$$(s(g))(\rho_1, \dots, \rho_n) = s(g(\rho_1, \dots, \rho_n)) \qquad , \tag{24}$$

relation dans laquelle au membre de gauche s est considéré comme élément de $\mathfrak{S}_n = \mathrm{Gal}(\mathcal{F}/\mathcal{K})$, et au membre de droite comme élément de $\Gamma = \mathrm{Gal}(E/k)$.

La variété $\mathcal{W}$

Il est clair que $\mathcal{W} = \{(\rho_{s(1)}, \dots, \rho_{s(n)})\}_{s \in \mathfrak{S}_n}$; la forme fondamentale $\Psi_{\mathcal{W}}(T, U)$ est $\prod_{s \in \mathfrak{S}_n}(T - \sum_{i=1}^n U_i \rho_{s(i)})$; sa décomposition en facteurs irréductibles de $k[T, U]$ est $\Psi_{\mathcal{W}}(T, U) = \prod_{C \in \mathcal{H}} P_C$, où $\mathcal{H} = (\mathfrak{S}_n/\Gamma)_d$ et où, pour tout $C \in \mathcal{H}$, on a posé $P_C = \prod_{s \in C}(T - \sum_{i=1}^n U_i \rho_{s(i)})$.

Les composantes k-irréductibles de $\mathcal{W}$ sont donc les ensembles

$$\mathcal{T}_C = \{(\rho_{s(1)}, \dots, \rho_{s(n)})\}_{s \in C} \qquad , (C \in \mathcal{H}) \ ;$$

nous poserons $\mathcal{V} = \mathcal{T}_\Gamma$ et $\Psi = P_\Gamma$. On sait que le k-espace vectoriel $\mathcal{A}/\mathfrak{I}$ (resp. $\hat{k}$-espace vectoriel $\hat{\mathcal{A}}/\hat{\mathfrak{I}}$) est engendré par les représentants des $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ pour $\alpha_1 < 1, \dots, \alpha_n < n$ (c'est une conséquence facile des formules de Girard-Newton, ou d'une base standard de $\mathfrak{I}$ donnée dans [A. Mach, A. Valibouze]). Comme d'autre part, $\dim_{\hat{k}}(\hat{\mathcal{A}}/\sqrt{\hat{\mathfrak{I}}}) = \mathrm{card}(\mathcal{W}) = n! \leq \dim_{\hat{k}}(\hat{\mathcal{A}}/\hat{\mathfrak{I}}) \leq n!$, on en déduit les formules bien connues :

$$\hat{\mathfrak{I}} = \sqrt{\hat{\mathfrak{I}}} \ , \ \mathfrak{I} = \sqrt{\mathfrak{I}} \ , \ \dim_k(\mathcal{A}/\mathfrak{I}) = \dim_{\hat{k}}(\hat{\mathcal{A}}/\hat{\mathfrak{I}}) = n! \ ; \tag{25}$$

de plus le U-résultant de $\mathfrak{I}$ est $\Psi_{\mathcal{W}}(T, U)$.

Le groupe de Galois de $\mathcal{W}$ sur k est Γ, car le corps de rupture de $\mathcal{W}$ sur k est E, qui est aussi le corps de rupture sur k de chaque variété $\mathcal{T}_C$, $C \in \mathcal{H}$. Pour chaque $C \in \mathcal{H}$, l'idéal $\mathfrak{M}_C = \{g \in \mathcal{A} \mid g = 0 \text{ sur } \mathcal{T}_C\}$ de $\mathcal{A}$ est maximal, et définit la variété

$\mathcal{T}_C$, et on a $E \cong \mathcal{A}/\mathfrak{M}_C$. Les $\mathfrak{M}_C$ sont les idéaux premiers associés à $\mathfrak{I}$ dans $\mathcal{A}$, et on a :

$$\mathfrak{I} = \bigcap_{C \in \mathcal{H}} \mathfrak{M}_C \qquad . \tag{26}$$

Nous poserons $\mathfrak{N} = \mathfrak{M}_\Gamma$. (Donc $\mathfrak{N} = \{g \in \mathcal{A} \mid g(\rho_1, \dots, \rho_n) = 0\}$ dit *idéal des relations entre les racines de* f.) On voit comme ci-dessus que pour chaque $C \in \mathcal{H}$, le U-résultant de $\mathfrak{M}_C$ est P_C, la forme fondamentale de $\mathcal{T}_C$.

On sait trouver une base standard de l'idéal $\mathfrak{N}$ relative à l'ordre lexicographique. Elle s'obtient en factorisant f dans des extensions successives de k, ce qui est assez coûteux. (voir [N. Tchebotarev] et [A. Mach, A. Valibouze]). Nous allons ci-dessous définir des systèmes générateurs à $n+1$ éléments pour chaque idéal $\mathfrak{M}_C$. Bien entendu, il suffit pour cela d'envisager la génération de l'idéal $\mathfrak{N}$.

Théorème 5.1. Soit $g \in \mathfrak{N} \backslash (\bigcup_{C \in \mathcal{H}, C \neq \Gamma} \mathfrak{M}_C)$; alors l'idéal $\mathfrak{N}$ de $\mathcal{A}$ est engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n, g\}$.

Démonstration. Notons $\mathfrak{a}$ l'idéal de $\mathcal{A}$ engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n, g\}$. Les hypothèses entraînent $\mathcal{V}(\mathfrak{a}) = \mathcal{V} = \mathcal{V}(\mathfrak{N})$, d'où :

$$\mathfrak{I} \subset \mathfrak{a} \subset \sqrt{\mathfrak{a}} = \mathfrak{N} \qquad ;$$

pour tout $l \in \mathbb{N}$, les idéaux $\mathfrak{N}^l$ et $J = \bigcap_{C \in \mathcal{H}\,,\, C \neq \Gamma} \mathfrak{M}_C$ de $\mathcal{A}$ sont comaximaux. Choisissons $l \in \mathbb{N}$ de façon que $\mathfrak{N}^l \subset \mathfrak{a}$, ce qui est possible car $\mathfrak{N} = \sqrt{\mathfrak{a}}$ et car $\mathcal{A}$ est noethérien. Soit alors $u \in \mathfrak{N}^l$ et $v \in J$ tels que $u + v = 1$. Pour tout $x \in \mathfrak{N}$, on a : $x = xu + xv$; or : $xu \in \mathfrak{N}^l \subset \mathfrak{a}$, et $xv \in \mathfrak{N}\, J \subset \mathfrak{N} \cap J = \mathfrak{I} \subset \mathfrak{a}$, d'où $x \in \mathfrak{a}$. Donc $\mathfrak{N} = \mathfrak{a}$ □

Commentaires sur le Théorème 5.1

Ce théorème est implicitement latent dans toute la littérature ancienne sur la théorie de Galois.

Application du Théorème 5.1 aux résolvantes

Théorème 5.2. Soit Θ un résolvant d'un sous-groupe H de $\mathfrak{S}_n$, posons $\theta = \Theta(\rho_1, \dots, \rho_n)$.

a) Si $\Gamma \subset H$, alors $\theta \in k$;

b) si $\theta \in k$ et si θ est racine simple de la résolvante $\mathcal{L}_{\Theta,f}$, alors $\Gamma \subset H$;

c) si $\Gamma \subset H$ et si θ est racine simple de $\mathcal{L}_{\Theta,f}$, alors $\Gamma = H$ ssi l'idéal $\mathfrak{N}$ est engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n, \Theta - \theta\}$.

Démonstration. Notons $g \mapsto \tilde{g}$ le morphisme de k-algèbre $\mathcal{A} \to E$, $g \mapsto g(\rho_1, \dots, \rho_n)$. Pour tout $s \in \Gamma$, on a $\widetilde{s.g} = s(\tilde{g})$ (cf. (24)).

a) supposons $\Gamma \subset H$. Alors pour $s \in \Gamma$, on a : $s(\theta) = s(\tilde{\Theta}) = \widetilde{s.\Theta} = \tilde{\Theta} = \theta$; donc θ est Γ-invariant, d'où $\theta \in k$.

b) Soient $\Theta_1 = \Theta, \Theta_2, \dots, \Theta_\nu$ les conjugués de Θ distincts dans l'extension $\mathcal{F}$ de $\mathcal{K}$. Notons $\theta_i = \tilde{\Theta}_i$. On a : $\mathcal{L}_{\Theta,f}(x) = \prod_{i=1}^{\nu}(x - \theta_i)$, et par hypothèse $\theta_i \neq \theta_1 = \theta$ si $i \geq 2$. Soient alors $s \in \Gamma$ et $j \in [1, \nu]$ tels que $\Theta_j = s.\Theta$; on a : $\theta_j = \widetilde{\Theta_j} = \widetilde{s.\Theta} = s(\tilde{\Theta}) = s(\theta) = \theta \neq \theta_i$ pour $i \geq 2$ et donc $j = 1$; c'est-à-dire $s \in H$; d'où $\Gamma \subset H$.

c) D'après les hypothèses, on a $\theta \in k$. d'après le Théorème 5.1, pour que l'idéal $\mathfrak{N}$ soit engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n, \Theta - \theta\}$, il faut et il suffit que $\Theta - \theta$ prenne une valeur non nulle sur les composantes $(\mathcal{T}_C)_{C \neq \Gamma}$ de $\mathcal{W}$, autrement dit que $\Theta(\rho_{s(1)}, \dots, \rho_{s(n)}) \neq \theta$ pour $s \in \mathfrak{S}_n \backslash \Gamma$. Mais pour tout $s \in \mathfrak{S}_n$, $\Theta(\rho_{s(1)}, \dots, \rho_{s(n)}) = (s.\Theta)(\rho_1, \dots, \rho_n)$. Puisque θ est racine simple de $\mathcal{L}_{\Theta,f}$, le raisonnement vu en b) prouve que $(s.\Theta)(\rho_1, \dots, \rho_n) = \theta$ ssi $s \in H$. Donc la condition " $\mathfrak{N}$ est engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n, \Theta - \theta\}$ " équivaut à " $s \in \mathfrak{S}_n \backslash \Gamma$ implique $s \notin H$ ", c'est-à-dire à $H \subset \Gamma$. Comme on a déjà $\Gamma \subset H$, en fin de compte cette condition équivaut à : $\Gamma = H$ □

En abandonnant la contrainte " $\theta \in k$ ", on peut affiner le Théorème 5.2 :

Théorème 5.3. Soit Θ un résolvant d'un sous-groupe H de $\mathfrak{S}_n$. Posons $\theta = \Theta(\rho_1, \dots, \rho_n)$, notons $\Theta_1, \dots, \Theta_\nu$ les conjugués de $\theta = \Theta_1$ distincts dans l'extension $\mathcal{F}$ de $\mathcal{K}$, soit $C_i = \{s \in \mathfrak{S}_n \mid s.\Theta_1 = \Theta_i\}$ $(1 \leq i \leq \nu)$. Supposons que θ soit une racine simple de la résolvante $\mathcal{L}_{\Theta,f}$; soit h le facteur normalisé irréductible dans $k[x]$ de $\mathcal{L}_{\Theta,f}$ qui s'annule en θ. Supposons la numérotation (Θ_i) choisie pour que $h(x) = (x - \widetilde{\Theta_1}) \cdots (x - \widetilde{\Theta_r})$ $(1 \leq r \leq \nu)$, notons $S = \mathrm{Stab}_{\mathfrak{S}_n}(\{\Theta_1, \dots, \Theta_r\})$. Alors :

a) La Γ-orbite de Θ dans $\mathcal{F}$ est $\mathcal{O} = \{\Theta_1, \dots, \Theta_r\}$.
b) On a $\Gamma \subset S \subset \bigcup_{i=1}^{r} C_i$, et $[S : \Gamma] = [S \cap H : \Gamma \cap H]$.
c) On a : $\Gamma = S = \bigcup_{i=1}^{r} C_i$ ssi l'idéal $\mathfrak{N}$ est engendré par $\mathcal{G} = \{\sigma_1 - c_1, \dots, \sigma_n - c_n, h(\Theta)\}$.

Démonstration. a) Si $s \in \Gamma$, on a : $h(\widetilde{s.\Theta}) = h(s(\tilde{\Theta})) = s(h(\tilde{\Theta}) = s(0) = 0$ (car $h \in k[x]$), donc $s.\Theta \in \{\Theta_1, \dots, \Theta_r\}$, car du fait que h est un facteur simple de $\mathcal{L}_{\Theta,f}$, les seuls indices $j \in [1, \nu]$ tels que $\widetilde{\Theta_j} \in \{\widetilde{\Theta_1}, \dots, \widetilde{\Theta_r}\}$ sont $1, 2, \dots, r$. Donc la Γ-orbite de Θ dans $\mathcal{F}$ est contenue dans $\mathcal{O}$. Si $i \in [1, r]$, on a un $\gamma \in \Gamma$ tel que $\gamma.\tilde{\Theta} = \widetilde{\Theta_i}$ puisque h est irréductible dans $k[x]$. Alors $\widetilde{\gamma\Theta} = \gamma(\tilde{\Theta}) = \widetilde{\Theta_i}$, ce qui force $\gamma.\Theta = \Theta_i$ pour les mêmes raisons que ci-dessus. Donc $\mathcal{O}$ est bien la Γ-orbite de Θ dans $\mathcal{F}$.

b) L'inclusion $S \subset \bigcup_{i=1}^{r} C_i$ est claire. Montrons que $\Gamma \subset S$; soit $s \in \Gamma$ on a $s(\{\widetilde{\Theta_1}, \dots, \widetilde{\Theta_r}\}) = \{\widetilde{\Theta_1}, \dots, \widetilde{\Theta_r}\}$ car $h \in k[x]$. Donc si $i \in [1, r]$, du fait (dû à ce que $s \in \Gamma$) que $s(\widetilde{\Theta_i}) = \widetilde{s.\Theta_i}$, on déduit que $\widetilde{s.\Theta_i} \in \{\widetilde{\Theta_1}, \dots, \widetilde{\Theta_r}\}$ par le même argument qu'en a), d'où $s(\Theta_i) \in \{\Theta_1, \dots, \Theta_r\}$, d'où $s \in S$. Ce qui prouve bien que $\Gamma \subset S$. Enfin $\mathcal{O}$ est la S-orbite de Θ, et $\mathrm{Stab}_S(\Theta) = S \cap H$, $\mathrm{Stab}_\Gamma(\Theta) = \Gamma \cap H$, d'où $r = [\Gamma : \Gamma \cap H] = [S : S \cap H]$, d'où $[S : \Gamma] = [S \cap H : \Gamma \cap H]$.

c) Il est clair que $h(\Theta)$ est nul sur $\mathcal{T}_\Gamma$. D'après le Théorème 5.1, pour que l'idéal $\mathfrak{N}$ soit engendré par $\mathcal{G}$, il faut et il suffit que $h(\Theta)$ ne s'annule sur aucun ensemble $\mathcal{T}_C$ pour $C \neq \Gamma$, c'est-à-dire que l'on ait $h(\Theta(\rho_{s(1)}, \dots, \rho_{s(n)})) \neq 0$ pour tout $s \in \mathfrak{S}_n \backslash \Gamma$, ce qui s'écrit : $h(\widetilde{s.\Theta}) \neq 0$ pour tout $s \in \mathfrak{S}_n \backslash \Gamma$. Mais comme h est facteur simple de

$\mathcal{L}_{\Theta,f}$, les seuls $s \in \mathfrak{S}_n$ tels que $h(\widetilde{s.\Theta}) = 0$ sont ceux qui vérifient $s.\Theta \in \{\Theta_1, \dots, \Theta_r\}$, i.e. les éléments de $\bigcup_{i=1}^r C_i$. Donc $\mathfrak{N}$ est engendré par $\mathcal{G}$ ssi $s \in \mathfrak{S}_n \backslash \Gamma$ puisque $s \notin \bigcup_{i=1}^r C_i$, c'est-à-dire ssi $\bigcup_{i=1}^r C_i \subset \Gamma$, et d'après b) cette condition équivaut bien à : $\Gamma = S = \bigcup_{i=1}^r C_i$ □

Sous les hypothèses du Théorème 5.3, il n'y a aucune raison que l'ensemble $\mathcal{E} = \bigcup_{i=1}^r C_i$ soit un sous-groupe de $\mathfrak{S}_n$. Toutefois , si $\mathcal{E}$ est contenu dans le normalisateur $\mathcal{N}$ de Γ dans $\mathfrak{S}_n$, alors $\mathcal{E} = S$. En effet dans ce cas, soit $s \in C_i$ $(1 \leq i \leq r)$ et soit $\gamma \in \Gamma$. On a donc $\gamma s = s\gamma'$ avec $\gamma' \in \Gamma$. En appliquant γ aux coefficients de $P = \prod_{j=1}^r (x - \widetilde{s.\Theta_j})$, on obtient (puisque $\gamma \in \Gamma$) $\prod_{j=1}^r (x - \gamma.\widetilde{s.\Theta_j}) \prod_{j=1}^r (x - \widetilde{(\gamma s).\Theta_j}) = \prod_{j=1}^r (x - \widetilde{(s\gamma').\Theta_j}) = \prod_{j=1}^r (x - \widetilde{s(\gamma'.\Theta_j)}) =$ (du fait que $\gamma' \in \Gamma \in S$)$= \prod_{l=1}^r (x - \widetilde{s.\Theta_l}) = P$. Cela prouve que $P \in k[x]$, mais comme $\deg(P) = r$ et que $P(\widetilde{\Theta_i}) = P(\widetilde{s.\Theta}) = 0$, cela force $P = h$, donc $\{\widetilde{s.\Theta_j}\}_{1 \leq j \leq r} = \{\widetilde{\Theta_j}\}_{1 \leq j \leq r}$, d'où $s \in S$ puisque h est facteur simple de la résolvante $\mathcal{L}_{\Theta,f}$.

6. Résolvantes de Lagrange et groupes de Galois

Dans ce paragraphe, on reprend les notations en vigueur aux §§3 à 5 et les hypothèses des §§3 et 4. En particulier, E désigne la k-algèbre des racines dans $\hat{k}$ de $f(x) = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n \in k[x]$, et $g \mapsto \tilde{g}$ désigne le morphisme de spécialisation $\mathcal{A} \to \hat{k}$, $g \mapsto g(\rho_1, \dots, \rho_n)$. Rappelons que le groupe $\Gamma = \mathrm{Gal}(E/k)$, par son action sur $\{\rho_1, \dots, \rho_n\}$, est identifié à un sous-groupe de $\mathfrak{S}_n = \mathrm{Gal}(\mathcal{F}/\mathcal{K})$. Dans tout ce qui suit, on ne fera aucune hypothèse a priori sur le corps k.

Théorème 6.1. Soit Θ un résolvant d'un sous-groupe H de $\mathfrak{S}_n$; posons $\theta = \tilde{\Theta}$. Si θ est racine simple de $\mathcal{L}_{\Theta,f}$, alors $\mathrm{Stab}_\Gamma(\theta) = \Gamma \cap H$, autrement dit $\mathrm{Gal}(E/k(\theta)) = \Gamma \cap H$.

Démonstration. Pour tout $g \in \Gamma$ et $P \in \mathcal{A}$, on a $\widetilde{g.P} = g(\tilde{P})$ (cf. (24), §5). Si $g \in \Gamma \cap H$, on en déduit : $\widetilde{g.\Theta} = \tilde{\Theta} = \theta = g(\tilde{\Theta}) = g(\theta)$. Donc, $\Gamma \cap H \subset \mathrm{Stab}_\Gamma(\theta)$. Si $g \in \Gamma \backslash H$, alors $\Theta' = g.\Theta$ est un conjugué de Θ dans $\mathcal{F}$ sur $\mathcal{K}$ distinct de Θ. Donc puisque θ est racine simple de $\mathcal{L}_{\Theta,f}(x) = \prod(x - \tilde{\Psi})$, où le produit est étendu aux Ψ conjugués de Θ dans $\mathcal{F}$ sur $\mathcal{K}$, on a $\theta' = \tilde{\Theta}' \neq \theta$, d'où $\theta' = \widetilde{\Theta'} = \widetilde{g.\Theta} = g(\tilde{\Theta}) = g(\theta) \neq \theta$, i.e. $g \notin \mathrm{Stab}_\Gamma(\theta)$. En définitive, $\mathrm{Stab}_\Gamma(\theta) = \Gamma \cap H$ □

Corollaire 6.2. Dans les conditions du théorème 6.1, le degré du polynôme minimal de θ sur k est $[\Gamma : \Gamma \cap H]$.

Théorème 6.3. Soit Θ un résolvant d'un groupe H de $\mathfrak{S}_n$; posons $\theta = \tilde{\Theta}$. Supposons que θ soit une racine de multiplicité ν de $\mathcal{L}_{\Theta,f}(x)$. Ecrivons $\mathcal{L}_\Theta = \prod_{i=1}^e (x - \Theta_i)$ avec $\Theta_1 = \Theta$, $\widetilde{\Theta_i} = \theta$ pour $i \leq \nu$ et $\widetilde{\Theta_i} \neq \theta$ pour $i > \nu$. Notons $L = \mathrm{Stab}_{\mathfrak{S}_n}(\{\Theta_1, \dots, \Theta_\nu\})$. On a : $\mathrm{Gal}(E/k(\theta)) = \mathrm{Stab}_\Gamma(\theta) = \Gamma \cap L$; de plus , $\Gamma \cap H \subset \Gamma \cap L$, et $[\Gamma : \Gamma \cap H] \leq \nu\, [k(\theta) : k]$.

Démonstration. Fixons l'indice i ($1 \leq i \leq \nu$). Si $g \in \Gamma$, on a $g \in \mathrm{Stab}_\Gamma(\theta)$ ssi $g(\widetilde{\Theta_i}) = \widetilde{\Theta_i}$, c'est-à-dire ssi $\widetilde{g.\Theta_i} = \theta$, ce qui signifie : $g.\Theta_i \in \{\Theta_1, \ldots, \Theta_\nu\}$. C'est vrai avec tout $i \leq \nu$, d'où $\mathrm{Gal}(E/k(\theta)) = \mathrm{Stab}_\Gamma(\theta) = \Gamma \cap L$. En particulier si $g.\Theta_1 = \Theta_1$, i.e. si $g \in H$, alors $g \in L$, d'où $\Gamma \cap H \subset \Gamma \cap L$. En faisant opérer $\Gamma \cap L$ sur $\{\Theta_1, \ldots, \Theta_\nu\}$, on voit que le stabilisateur de Θ_1 dans $\Gamma \cap L$ est $\Gamma \cap H$ à cause de ce qui précède. D'où $[\Gamma \cap L : \Gamma \cap H] = \mathrm{card}(\mathrm{Orb}_{\Gamma\cap L}(\Theta)) \leq \mathrm{card}(\mathrm{Orb}_L(\Theta)) = \nu$; d'autre part, $[\Gamma : \Gamma \cap L] = [k(\theta) : k]$, d'où enfin $[\Gamma : \Gamma \cap H] = [\Gamma : \Gamma \cap L]\,[\Gamma \cap L : \Gamma \cap H] \leq [k(\theta) : k]\,\nu$ □

De la démonstration ci-dessus, il se dégage immédiatement :

Corollaire 6.4. Avec les notations et hypothèses du Théorème 6.1, on a :

$$[k(\theta) : k] = [\Gamma : \Gamma \cap L] \qquad ;$$

en particulier, on a : $\theta \in k$ ssi $\Gamma \subset L$.

Ce dernier corollaire résout la question des conditions imposées au groupe de Galois Γ par l'existence de relations algébriques entre les racines de f. De façon précise, supposons connu un élément $\Psi \in k[x_1, \ldots, x_n]$ tel que $\Psi(\rho_1, \ldots, \rho_n) = 0$. Formons la résolvante $\mathcal{L}_{\Psi,f}(x) = \prod_{i=1}^m (x - \widetilde{\Psi}_i)$, où $\mathcal{L}_\Psi = \prod_{i=1}^m (x - \Psi_i)$, $\Psi_1 = \Psi$, $m = [\mathfrak{S}_n : \mathrm{Stab}_{\mathfrak{S}_n}(\Psi)]$. Soit J l'ensemble des $i \in [1, m]$ tels que $\widetilde{\Psi}_i = 0$. Alors d'après le corollaire du Théorème 6.3, on voit que $\Gamma \subset \mathrm{Stab}_{\mathfrak{S}_n}(\{\Psi_j\}_{j\in J})$. En particulier si 0 est racine simple de $\mathcal{L}_{\Psi,f}$, on a : $\Gamma \subset \mathrm{Stab}_{\mathfrak{S}_n}(\Psi)$.

Conservons toujours les notations du Théorème 6.3. Désignons par $C_1, \ldots, C_e$ les classes à gauche de $\mathfrak{S}_n \bmod H$, ordonnées de façon que pour tout i, on ait $C_i = \{\sigma \in \mathfrak{S}_n \mid \sigma.\Theta = \Theta_i\}$. Alors : pour $i \leq \nu$, $C_i \cap \Gamma \subset L$, et si $i > \nu$, $C_i \cap \Gamma \cap L = \emptyset$, donc

$$\Gamma \cap L = \bigcup_{i=1}^{\nu} (C_i \cap \Gamma) \qquad .$$

Poursuivons notre analyse du Théorème 6.3 en introduisant un deuxième résolvant Ψ de H. Notons Ψ_i la valeur commune des $\sigma.\Psi$ pour $\sigma \in C_i$ ($1 \leq i \leq e$). Deux facteurs normalisés F et G de $\mathcal{L}_{\Theta,f}$ et $\mathcal{L}_{\Psi,f}$ respectivement seront dits *parallèles* ssi on a une même partie J de $[1, e]$ telle que : $F(x) = \prod_{j\in J}(x - \widetilde{\Theta_j})$, et $G(x) = \prod_{j\in J}(x - \widetilde{\Psi_j})$. S'il en est ainsi, et si l'une des deux résolvante est f-séparable, J est alors unique.

Dans ce qui suit, nous supposerons que Ψ est f-séparable, et nous nous proposons d'étudier le facteur de $\mathcal{L}_{\Psi,f}$ parallèle à un facteur multiple de $\mathcal{L}_{\Theta,f}$ dans $k[x]$.

Notons h l'élément irréductible dans $k[x]$ et normalisé nul en θ qui divise $\mathcal{L}_{\Theta,f}$, et soit ν l'entier ≥ 1 tel que h^ν divise $\mathcal{L}_{\Theta,f}$ mais $h^{\nu+1}$ ne le divise pas. Ecrivons $h(x) = (x - \theta_1) \cdots (x - \theta_d)$, avec $\theta_1 = \theta$ (donc $\theta_1, \ldots, \theta_d$ sont les Γ-conjugués de θ). Soit $\mathcal{R} = \{\Theta_1, \ldots, \Theta_e\}$ et $\mathcal{R}_i = \{\Phi \in \mathcal{R} \mid \tilde{\Phi} = \theta_i\}$ ($1 \leq i \leq d$). On a donc $\mathrm{card}(\mathcal{R}_i) = \nu$ pour tout i, et à cause du Théorème 6.3 $d = [\Gamma : \Gamma \cap \mathrm{Stab}_{\mathfrak{S}_n}(\mathcal{R}_i)]$.

De plus $\mathcal{R}_1 = \{\Theta_1, \ldots, \Theta_\nu\}$. On notera $L_i = \mathrm{Stab}_{\mathfrak{S}_n}(\mathcal{R}_i)$ (donc $L_1 = L$). L'ensemble $\bigcup_{i=1}^d \mathcal{R}_i$ est γ-stable ; notons $\mathcal{O}$ l'ensemble des Γ-orbites de $\bigcup_{i=1}^d \mathcal{R}_i$. Pour $O \in \mathcal{O}$, les $O \cap \mathcal{R}_i$ $(1 \leq i \leq d)$ sont les $\Gamma \cap L_j$-orbites de O pour n'importe quel choix de j, on a un entier m_O ne dépendant que de O tel que $m_O = \mathrm{card}(O \cap \mathcal{R}_i)$ pour tout i, et qui est, par application du Théorème 6.3, donné par $m_O = [\Gamma \cap L_j : \Gamma \cap \mathrm{Stab}_{\mathfrak{S}_n}(\Phi)]$ pour tout $j \in [1, d]$ et tout $\Phi \in O \cap \mathcal{R}_j$. Le système $(O \cap \mathcal{R}_i)_{1 \leq i \leq d}$ est un système de blocs de primitivité pour l'action de Γ sur O. On a donc $\nu = \sum_{O \in \mathcal{O}} m_O$; $h^\nu(x) = \prod_{O \in \mathcal{O}} (\prod_{\Phi \in O} (x - \tilde{\Phi}))$; $\mathrm{card}(O) = d.m_O$ pour tout $O \in \mathcal{O}$.

Pour $O \in \mathcal{O}$, soit J_O l'ensemble des indices $j \in [1, e]$ tels que $\Theta_j \in \mathcal{O}$. Par définition, le facteur parallèle à h^ν dans $\mathcal{L}_{\Psi,f}$ est $\prod_{O \in \mathcal{O}} (\prod_{j \in J_O} (x - \widetilde{\Psi_j}))$; mais si $O \in \mathcal{O}$, $\{\Psi\}_{j \in J_O}$ est une Γ-orbite, donc le polynôme $P_O(x) = \prod_{j \in J_O} (x - \widetilde{\Psi_j})$ appartient à $k[x]$, et c'est un facteur normalisé irréductible dans $k[x]$ de $\mathcal{L}_{\Psi,f}$, dont le degré est $d.m_O$. Nous en déduisons le résultat suivant :

Théorème 6.5. Théorème des multiplicités Dans les conditions ci-dessus, le facteur irréductible de $\mathcal{L}_{\Psi,f}$ parallèle à h^ν est $\prod_{O \in \mathcal{O}} P_O$, où pour chaque $O \in \mathcal{O}$, le polynôme $P_O(x)$ est un facteur irréductible dans $k[x]$ de $\mathcal{L}_{\Psi,f}(x)$ dont le degré $d.m_O$ est un multiple du degré $d = \deg(h)$.

(L'idée de comparer un résolvant séparable à un résolvant quelconque apparaît déjà dans Lagrange [J.L. Lagrange, tome IV] ; nous y reviendrons au §10 ci-après).

Remarque 8. Ce théorème revêt une importance pratique certaine. En effet, le calcul effectif des résolvantes dans des cas numériques amène très fréquemment à des facteurs multiples, surtout pour les polynômes à " petit " groupe de Galois. Ce théorème, ainsi que le Théorème 6.6 ci-dessous permettront néanmmoins d'en déduire des renseignements qui peuvent dispenser de chercher des résolvantes séparables. Par exemple, supposons que le calcul d'une résolvante par Θ, y révèle un facteur P^2 où $\deg(P) = 12$ et $P(x)$ irréductible dans $k[x]$; alors on en déduira que pour tout résolvant f-séparable Ψ du même groupe que Θ, la factorisation de $\mathcal{L}_{\Psi,f}$ fera apparaitre soit au moins 2 facteurs de degré 12, soit au moins un de degré 24.

Dans ce qui suit, sur $\mathbb{N}^r$ (où $r \in \mathbb{N}^\star$) nous utiliserons l'ordre naturel produit, noté $\preceq$, et ainsi défini : si $a = (a_1, \ldots, a_r) \in \mathbb{N}^r$ et $b = (b_1, \ldots, b_r) \in \mathbb{N}^r$, alors $a \preceq b$ ssi $a_i \leq b_i$ pour tout i. Remarquons que si deux partitions a et b d'une même entier $m \geq 1$ vérifient $a \preceq b$, alors $a = b$.

Nous rappelons que ϖ désigne la matrice des partitions définie au §3.

Théorème 6.6. Soit Θ un résolvant d'un sous-groupe H de $\mathfrak{S}_n$. Supposons que tous les facteurs irréductibles de $\mathcal{L}_{\Theta,f}$ soient séparables. Soit $\mathcal{C}$ la classe de conjugaison de H dans $\mathfrak{S}_n$; notons $e = [\mathfrak{S}_n : H]$; pour $1 \leq j \leq e$, soit α_j le nombre de facteurs irréductibles simples de $\mathcal{L}_{\Theta,f}$ de degré j ; alors

$$(\alpha_1, \ldots, \alpha_e) \preceq \varpi(\Gamma, \mathcal{C}) \qquad ;$$

si $\mathcal{L}_{\Theta,f}$ est séparable (i.e. si Θ est f-séparable), alors

$$(\alpha_1, \ldots, \alpha_e) = \varpi(\Gamma, \mathcal{C}) \qquad .$$

Démonstration. Soit $\{\gamma_m\}_{1\leq m\leq e}$ une transversale gauche de $\mathfrak{S}_n$ mod H. Posons $H_m = \gamma_m H \gamma_m^{-1}$, $\Theta_m = \gamma_m.\Theta$ avec, pour commodité, γ_1 =Id, l'élément neutre de $\mathfrak{S}_n$, d'où $H_1 = H$ et $\Theta_1 = \Theta$. Notons $\theta_m = \widetilde{\Theta_m}$. On a donc :

$$\mathcal{L}_\Theta = \prod_{m=1}^{e}(x-\Theta_m)\ ;\ \mathcal{L}_{\Theta,f} = \prod_{m=1}^{e}(x-\theta_m)\ ;$$
$$H_m = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta_m) \qquad .$$

Fixons j, $(1 \leq j \leq e)$. Soit P un facteur k-irréductible simple de degré j de $\mathcal{L}_{\Theta,f}$. Soit $P = \prod_{m\in J}(x-\theta_m)$, avec $J \subset [1,e]$ et $\mathrm{card}(J) = j$. Si $m \in J$, d'après le corollaire du Théorème 6.1, on a : $j = \deg(P) = [\Gamma : \Gamma \cap H_m]$.

Soit N_j le nombre des $m \in [1,e]$ tels que $[\Gamma : \Gamma \cap H_m] = j$. D'après ce qu'on vient de voir, on a : $j\alpha_j \leq N_j$. Or par définition (voir (13) et (14)) , $(N_1/1, N_2/2, \ldots, N_e/e) = \varpi(\Gamma, \mathcal{C})$, ce qui prouve bien que :

$$(\alpha_1, \ldots, \alpha_e) \preceq \varpi(\Gamma, \mathcal{C}) \qquad . \tag{27}$$

Si maintenant $\mathcal{L}_{\Theta,f}$ est séparable, il est clair que $\sum_{j=1}^{e} j\alpha_j = \deg(\mathcal{L}_{\Theta,f}) = e$, donc alors $(\alpha_1, \ldots, \alpha_e)$ et $(N_1/1, N_2/2, \ldots, N_e/e)$ sont deux partitions de e et à cause de (27), elles sont égales. □

Méthode de la chasse aux résolvantes

Pour chaque classe de conjugaison $\mathcal{C}_j$ de sous-groupes de $\mathfrak{S}_n$ $(1 \leq j \leq s)$, choisissons un groupe $H_j \in \mathcal{C}_j$ et une transversale gauche $\{\gamma_m\}_{1\leq m\leq e_j}$ de $\mathfrak{S}_n$ mod H_j, où $e_j = [\mathfrak{S}_n : H_j]$, de façon que γ_1 =Id, l'élément neutre de $\mathfrak{S}_n$.

Choisissons un résolvant de H_j, noté Θ_j. Posons $\Theta_{j,m} = \gamma_m.\Theta_j$ $(1 \leq m \leq e_j)$, de sorte que $\Theta_{j,1} = \Theta_j$, $\mathcal{L}_{\Theta_j} = \prod_{m=1}^{e_j}(x - \Theta_{j,m})$.

Si $\mathcal{L}_{\Theta_j,f}$ est séparable, nous noterons $\pi(\Theta_j, f)$ la partition $(\alpha_{j,1}, \ldots, \alpha_{j,e_j})$ de e_j, où $\alpha_{j,p}$ est le nombre de facteurs irréductibles de degré p sur k de $\mathcal{L}_{\Theta_j,f}$. En combinant les Théorèmes 3.1 et 6.6, on arrive au théorème principal que nous avions en vue :

Théorème 6.7. Avec les notations ci-dessus, supposons que tous les résolvants Θ_i $(1 \leq i \leq s)$ soient f-séparables. Alors la classe de conjugaison $\mathcal{G}$ du groupe de Galois $\Gamma = \mathrm{Gal}(E/k)$ est $\mathcal{G} = \mathcal{C}_r$, où r est l'indice tel que la ligne d'indice r de la matrice des partitions $\mathcal{P} = [\varpi(\mathcal{C}_i, \mathcal{C}_j)]_{\substack{1\leq i\leq s\\ 1\leq j\leq s}}$ du groupe $\mathfrak{S}_n$ coïncide avec la ligne $(\pi(\Theta_1, f), \pi(\Theta_2, f), \ldots, \pi(\Theta_s, f))$.

Le Théorème 6.7 donne une méthode effective pour calculer la classe de conjugaison $\mathcal{G}$: on détermine la matrice des partitions $\mathcal{P}$ (par exemple le logiciel G.A.P. permet aisément de calculer une intersection de groupes ainsi que l'indice d'un groupe dans un autre) ; on calcule ensuite, si c'est possible, des résolvants

f-séparables Θ_j $(1 \leq j \leq s)$, on factorise les $\mathcal{L}_{\Theta_j,f}$ dans $k[x]$, on en déduit les partitions $\pi(\Theta_j, f)$ et on applique enfin le Théorème 6.7. Si k est infini, l'existence de résolvantes f-séparables Θ_j est assurée d'après le Théorème 4.5.

Lorsqu'on appliquera cette méthode, les groupes H_j ci-dessus introduits seront appelés les *groupes tests*, et les classes $\mathcal{C}_i$ parmi lesquelles on recherche $\mathcal{G}$ seront appelées *classes candidates*, le mot " groupe " étant ici entendu à conjugaison près dans $\mathfrak{S}_n$.

Dans la pratique, il n'est pas nécessaire de calculer toutes les résolvantes $\mathcal{L}_{\Theta_j,f}$. En effet pour r fixé $(1 \leq r \leq s)$, notons $\mathcal{U}_{r,j}$ l'ensemble des $i \in [1,s]$ tels que $\varpi(\mathcal{C}_i, \mathcal{C}_j) = \varpi(\mathcal{C}_r, \mathcal{C}_j)$. Convenons de dire qu'une partie J_r de $[1,s]$ *départage* $\mathcal{C}_r$ ssi $\bigcap_{j\in J_r} \mathcal{U}_{r,j} = \{r\}$. Pour déterminer $\mathcal{G}$, il suffit pour chaque r de calculer les résolvantes $\mathcal{L}_{\Theta_j,f}$ pour j parcourant une partie J_r qui départage $\mathcal{C}_r$. Le Théorème 6.7 assure que $[1,s]$ départage chaque $\mathcal{C}_r$; appelons *système séparant* de parties de $[1,s]$ toute famille $(J_r)_{1\leq r\leq s}$ de parties de $[1,s]$ telles que J_r départage $\mathcal{C}_r$ pour tout r, et appelons *support* d'un tel système l'ensemble $J = \bigcup_{r=1}^{s} J_r$. Dans tous les cas numériques, on pourra calculer $\mathcal{G}$ en ne calculant que les résolvantes $\mathcal{L}_{\Theta_j,f}$ pour j décrivant le support d'un quelconque système séparant, pourvu que ces $\mathcal{L}_{\Theta_j,f}$ soient séparables. On choisira alors les systèmes conduisant aux calculs les plus rapides. Notons ici que ce ne sont pas forcément les résolvantes de plus bas degré qui conduisent aux calculs les plus rapides. Il existe des résolvantes de degré assez élevé dont le calcul est quasiment immédiat.

En résumé, l'utilisation optimale du Théorème 6.7 consiste en premier lieu à repérer les classes $\mathcal{C}_j$ conduisant aux calculs les plus rapides des résolvantes $\mathcal{L}_{\Theta_j,f}$; puis à former des systèmes séparants utilisant le maximum de classes $\mathcal{C}_j$ ainsi repérées, et enfin à en déduire $\mathcal{G}$.

Pour exposer la méthode nous allons détailler l'exemple du cas où $n = 4$, en supposant k de caractéristique $\neq 2$ et $\neq 3$.

A l'aide de G.A.P., on obtient d'abord une liste de représentations des classes de conjugaison de sous-groupes de $\mathfrak{S}_4$, classées par degrés décroissants :

Table 1
Représentants des classes de conjugaison de sous-groupes de $\mathfrak{S}_4$

Représentants	Générateurs	Cardinal	Nature
H_1	[ ]	1	
H_2	[(3,4)]	2	
H_3	[(1,2)(3,4)]	2	
H_4	[(2,3,4)]	3	
H_5	[(3,4), (1,2)]	4	$(\mathbb{Z}/2\mathbb{Z})^2$
$H_6 = G_1$	[(1,2)(3,4), (1,3)(2,4)]	4	$(\mathbb{Z}/2\mathbb{Z})^2$
$H_7 = G_2$	[(1,2)(3,4), (1,3,2,4)]	4	$(\mathbb{Z}/4\mathbb{Z})$
H_8	[(2,3,4), (3,4)]	6	$\mathfrak{S}_3$
$H_9 = G_3$	[(3,4), (1,2)(3,4), (1,3)(2,4)]	8	$\mathcal{D}_4$ (diédral)
$H_{10} = G_4$	[(1,2)(3,4), (1,3)(2,4), (2,3,4)]	12	$\mathfrak{A}_4$
$H_{11} = G_5$	[(1,4), (2,4), (3,4)]	24	$\mathfrak{S}_4$

Dans cette liste, les G_i désignent les représentants des classes de sous-groupes transitifs.

Table 2 : résolvants de ces groupes

H_1	$\Theta_1 = u_1x_1 + u_2x_2 + u_3x_3$ (avec (u_1, u_2, u_3) distincts et non nuls)
H_2	$\Theta_2 = x_1 + x_3x_4$
H_3	$\Theta_3 = x_1x_2 + x_1x_3 + x_2x_4$
H_4	$\Theta_4 = (x_2 - x_3)(x_3 - x_4)(x_4 - x_2)$
H_5	$\Theta_5 = x_1x_2$
H_6	$\Theta_6 = x_1x_3 + x_2x_4 - x_1x_2 - x_3x_4$
H_7	$\Theta_7 = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$
H_8	$\Theta_8 = x_1$
H_9	$\Theta_9 = x_1x_2 + x_3x_4$
H_{10}	$\Theta_{10} = \prod_{1\leq i<j\leq 4}(x_j - x_i)$
H_{11}	$\Theta_{11} = 1$

Puis en utilisant G.A.P., comme nous l'avons indiqué précédemment, nous calculons la matrice des partitions ci-dessous, où l'on convient, pour d'abréger, de noter $d_1^{\nu_1} \cdots d_r^{\nu_r}$ la partition $[(\nu_1, d_1), \ldots, (\nu_r, d_r)]$:

Table 3 : transposée de la matrice des partitions de $\mathfrak{S}_4$

	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9	H_{10}	H_{11}
H_1	1^{24}	2^{12}	2^{12}	3^8	4^6	4^6	4^6	6^4	8^3	12^2	24
H_2	1^{12}	$1^2, 2^5$	2^6	3^4	$2^2, 4^2$	4^3	4^3	$3^2, 6$	$4, 8$	12	12
H_3	1^{12}	2^6	$1^4, 2^4$	3^4	$2^2, 4^2$	2^6	$2^2, 4^2$	6^2	4^3	6^2	12
H_4	1^8	2^4	2^4	$1^2, 3^2$	4^2	4^2	4^2	$2, 6$	8	4^2	8
H_5	1^6	$1^2, 2^2$	$1^2, 2^2$	3^2	$1^2, 4$	2^3	$2, 4$	3^2	$2, 4$	6	6
H_6	1^6	2^3	1^6	3^2	2^3	1^6	2^3	6	2^3	3^2	6
H_7	1^6	2^3	$1^2, 2^2$	3^2	$2, 4$	2^3	$1^2, 4$	6	$2, 4$	6	6
H_8	1^4	$1^2, 2$	2^2	$1, 3$	2^2	4	4	$1, 3$	4	4	4
H_9	1^3	$1, 2$	1^3	3	$1, 2$	1^3	$1, 2$	3	$1, 2$	3	3
H_{10}	1^2	2	1^2	1^2	2	1^2	2	2	2	1^2	2
H_{11}	1	1	1	1	1	1	1	1	1	1	1

(Dans cette table 3, les groupes de la première ligne sont les candidats et ceux de la première colonne sont les groupes test.)

L'examen de la table 3 montre que le résolvant Θ_9, classiquement utilisé en degré 4, et qui présente le sérieux avantage que $\mathcal{L}_{\Theta_9,f}$ est toujours séparable si f l'est, n'est pourtant pas bon du point de vue du Théorème 6.7, car il départage très peu. En revanche, le couple (Θ_2, Θ_{10}) suffit à départager tous les groupes possibles sous la seule réserve que $\mathcal{L}_{\Theta_2,f}$ soit séparable. En effet $\mathcal{L}_{\Theta_{10}} = x^2 - \Delta$, où $\Delta = \prod_{1\leq i<j\leq 4}(x_j - x_i)^2 \in \mathcal{S}$ est le discriminant générique de degré 4, et puisque la caractéristique est $\neq 2$, pour tout f séparable $\mathcal{L}_{\Theta_{10},f} = x^2 - \tilde{\Delta}$ l'est aussi puisque $\tilde{\Delta} \neq 0$.

Or nous verrons plus loin que pour f donné numériquement, le calcul de $\mathcal{L}_{\Theta_2,f}$ est extrêmement rapide. Le calcul de $\tilde{\Delta}$, lui, est instantané. En résumé, si $\mathcal{L}_{\Theta_2,f}$ est

séparable, pour obtenir la classe de conjugaison de $\mathfrak{S}_4$ du groupe de Galois de f, il suffit de calculer le discriminant $\tilde{\Delta}$ de f et la résolvante $\mathcal{L}_{\Theta_2,f}$. Il importe ici de noter qu'il n'est pas nécessaire de calculer la résolvante formelle $\mathcal{L}_{\Theta_2}$ pour obtenir numériquement $\mathcal{L}_{\Theta_2,f}$: cette remarque est essentielle pour l'efficacité de la méthode du Théorème 6.7 (en fait, le calcul automatique de $\mathcal{L}_{\Theta_2,f}$ est instantané).

Observons encore :

Remarque 9. que dans la table 3, les lignes et les colonnes dont l'indice appartient à $\{1, 11\}$ sont superflues, leurs valeurs sont triviales. Il en est toujours ainsi dans le cas général. C'est pourquoi dans les tables ultérieures, nous omettrons les lignes et les colonnes correspondant aux classes de conjugaison $\{\mathfrak{S}_n\}$ et $\{\{\mathrm{Id}\}\}$, (où Id désigne l'élément neutre de $\mathfrak{S}_n$).

Remarque 10. que pour appliquer le Théorème 6.7, il n'est pas nécessaire d'ordonner les classes de conjugaison de sous-groupes de $\mathfrak{S}_n$ par degrés décroissants ni dans un ordre particulier pour écrire la matrice des partitions. On peut aussi travailler sur la transposée de cette matrice.

Remarque 11. que si l'on sait à l'avance que f est irréductible, il n'est pas nécessaire d'étudier la matrice des partitions $\mathcal{P}$ complète ; en effet le groupe $\Gamma = \mathrm{Gal}(E/k)$ étant alors un sous-groupe transitif de $\mathfrak{S}_n$, il suffit dans ce cas de considérer la sous-matrice de $\mathcal{P}$ formée avec les lignes qui correspondent aux classes de conjugaison de sous-groupes transitifs de $\mathfrak{S}_n$. Toutes les méthodes exposées ci-dessus s'appliquent alors de façon analogue avec cette seule sous-matrice.

Résolvantes relatives

Fixons maintenant un sous-groupe L_0 de $\mathfrak{S}_n$, et supposons dans tout ce qui suit, que $\Gamma \subset L_0$. Un tel groupe L_0 peut être obtenu par exemple à l'aide du Théorème 5.2 b) lorsqu'on aura calculé suffisamment de résolvantes. Nous poserons $e_0 = [\mathfrak{S}_n : L_0]$.

Notons $\mathcal{G}^{[L_0]}$ la classe de conjugaison dans le groupe L_0 du groupe $\Gamma = \mathrm{Gal}(E/k)$. Remarquons que par application de la formule (24) du §5, pour tout élément $\lambda \in \mathcal{A}_{L_0}$, on a $\tilde{\lambda} \in k$. (Observons que $\mathcal{G}^{[L_0]}$ est contenue dans la classe de conjugaison $\mathcal{G}$ de Γ dans $\mathfrak{S}_n$.)

Soit alors H un sous-groupe de L_0. Le corps $\mathrm{Inv}(H)$ est alors une extension séparable de degré $e = [L_0 : H]$ de $\mathrm{Inv}(L_0)$. Il existe des éléments primitifs de cette extension qui appartiennent à $\mathcal{A}_H$, et même des éléments primitifs homogènes, lorsque k est infini : par exemple tout résolvant homogène de H est un tel élément.

Définition 6.8. Avec les hypothèses et notations ci-dessus, on appelle *résolvant relatif* (de H par rapport à L_0) tout élément $\Theta \in \mathcal{A}_H$ qui est élément primitif de l'extension $\mathrm{Inv}(H)$ de $\mathrm{Inv}(L_0)$. Le polynôme minimal, que nous noterons $\mathcal{L}_\Theta^{[L_0]}$, d'un tel résolvant Θ sur le corps $\mathrm{Inv}(L_0)$ sera appelé *résolvante de Lagrange relative* associée au triplet (Θ, H, L_0). Un tel résolvant sera dit *homogène* ssi c'est un élément de $\mathcal{A}$ homogène.

Soit Θ un résolvant relatif de H par rapport à L_0. Le cardinal e de la L_0-orbite de Θ est $[L_0 : H]$. Notons $\{\Theta_1, \ldots, \Theta_e\}$ cette L_0-orbite, avec $\Theta_1 = \Theta$. On a :

$$\mathcal{L}_{\Theta}^{[L_0]}(x) = \prod_{i=1}^{e}(x - \Theta_i) \qquad ; \tag{28}$$

d'après (28), il est clair que $\mathcal{L}_{\Theta}^{[L_0]}(x) \in \mathcal{A}_{L_0}[x]$. Appliquons aux coefficients de $\mathcal{L}_{\Theta}^{[L_0]}(x)$ le morphisme $x \mapsto \tilde{x}$. D'après ce qui a été vu plus haut, on obtiendra ainsi un élément de $k[x]$, que nous noterons $\mathcal{L}_{\Theta,f}^{[L_0]}$, qui n'est autre que :

$$\mathcal{L}_{\Theta,f}^{[L_0]}(x) = \prod_{i=1}^{e}(x - \widetilde{\Theta_i}) \qquad ; \tag{29}$$

d'après (29), on déduit que $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ est un diviseur du degré e dans $k[x]$ de la résolvante "absolue" $\mathcal{L}_{\Theta,f}(x)$. Notons $H' = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta)$. On a donc $H' \cap L_0 = H$. Le degré de $\mathcal{L}_{\Theta,f}(x)$ est $[\mathfrak{S}_n : H']$. On a :

$$e\,[\mathfrak{S}_n : L_0] = [H' : H]\,[\mathfrak{S}_n : H'] \qquad ; \tag{30}$$

(on retrouve le fait que $e \leq [\mathfrak{S}_n : H']$ grâce à l'inégalité évidente $[H' : H] \leq [\mathfrak{S}_n : L_0]$, due au fait que $(xL_0) \cap H' = x(L_0 \cap H')$ pour tout $x \in H'$). On posera :

Définition 6.9. Le polynôme $\mathcal{L}_{\Theta,f}^{[L_0]}(x) \in k[x]$ défini par (29) sera appelé *résolvante de Lagrange relative* de f associée au triplet (Θ, H, L_0). Le résolvant relatif Θ sera dit *f-séparable* (ou mieux : (L_0, f)-séparable) ssi $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ est un polynôme séparable.

Remarque 12. Il convient ici de remarquer que même dans le cas particulier agréable où $H = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta)$, le polynôme $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ peut être séparable sans que $\mathcal{L}_{\Theta,f}(x)$ le soit. Donc passer à des résolvantes relatives peut être un moyen de se débarrasser des facteurs multiples des résolvantes absolues.

Toutefois, le calcul effectif d'une résolvante relative sera en général ardu. Lorsque k est de caractéristique 0, ce calcul peut formellement être exécuté en utilisant le Théorème 4.1 et les considérations qui l'entourent : on commence par déterminer les éléments $\eta_1, \ldots, \eta_{e_o}$ tels que $\mathcal{A}_{L_0} = \mathcal{S}\eta_1 \bigoplus \cdots \bigoplus \mathcal{S}\eta_{e_o}$, puis pour chaque coefficient F de $\mathcal{L}_{\Theta}^{[L_0]}(x)$ (calculé en faisant agir L_0 sur Θ), on calcule les éléments $\varphi_1, \ldots, \varphi_{e_o} \in \mathcal{S}$ tels que $F = \sum_{i=1}^{e_o} \varphi_i \eta_i$; alors le calcul de $\tilde{F}$ est ramené à celui des $\widetilde{\eta_i}$, dont on sait à l'avance qu'ils appartiennent à k. Faute de mieux, on peut obtenir les $\widetilde{\eta_i}$ par la méthode employée pour prouver le Théorème 4.3, en utilisant un résolvant f-séparable de L_0. Cette méthode a été utilisée par D. Lazard et J.M. Arnaudiès afin de calculer des résolvantes relatives en degré 5 (voir [J.M. Arnaudiès, D. Lazard]). [R.P. Stauduhar] a mis au point une méthode différente fondée sur des calculs d'approximation des racines de f et sur le fait que les coefficients de la résolvante sont des entiers. Il les a calculée pour les groupes transitifs jusqu'en degré 7. Cette

méthode a été poursuivie par M. Olivier (Université Bordeaux I) qui a pu y parvenir jusqu'au degré 10 (voir [H. Cohen] page 327).

Reprenons maintenant les notations et hypothèses générales des définitions 6.8 et 6.9. Notons $\mathcal{C}^{[L_0]}$ la classe de conjugaison du sous-groupe H de L_0 dans L_0. (Elle est donc contenue dans la classe de conjugaison $\mathcal{C}$ de H dans $\mathfrak{S}_n$.) Fixons le résolvant relatif Θ de H par rapport à L_0. Notons α_j le nombre de facteurs de degré j de $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ qui sont k-irréductibles et simples (donc si Θ est (L_0, f)-séparable, $(\alpha_1, \ldots, \alpha_e)$ est une partition de e). Dans tous les cas, nous noterons :

$$(\alpha_1, \ldots, \alpha_e) = \pi^{[L_0]}(\Theta, f) \qquad . \tag{31}$$

Le résultat essentiel concernant les résolvantes relatives est alors :

Théorème 6.10. Avec les notations et les hypothèses de (31), on a :

$$\pi^{[L_0]}(\Theta, f) \preceq \varpi(\mathcal{G}^{[L_0]}, \mathcal{C}^{[L_0]}) \qquad ,$$

où $\mathcal{G}^{[L_0]}$ désigne la classe de conjugaison de Γ dans L_0. Si de plus Θ est (L_0, f)-séparable on a :

$$\pi^{[L_0]}(\Theta, f) = \varpi(\mathcal{G}^{[L_0]}, \mathcal{C}^{[L_0]}) \qquad .$$

En vue d'établir ce résultat essentiel, nous avons besoin de la version relative des Théorèmes 6.1 et 6.3 :

Théorème 6.11. Adoptons les notations et hypothèses de (28) et (29). Posons $\theta = \tilde{\Theta}$. Supposons que θ soit racine simple de multiplicité $\nu \geq 1$ de $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$. Soit J l'ensemble $\{j \in [1, e] \mid \widetilde{\Theta_j} = \theta\}$. Notons $M = \mathrm{Stab}_{L_0}(\{\Theta_j\}_{j \in J})$.

a) Alors

$$\mathrm{Gal}(E/k(\theta)) = \Gamma \cap M \qquad ,$$

$\Gamma \cap H \subset \Gamma \cap M$, $[\Gamma : \Gamma \cap H] \leq \nu\, [k(\theta) : k]$ et $[k(\theta) : k] = [\Gamma : \Gamma \cap M]$.

b) En particulier, si θ est racine simple de $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$, on a ;

$$\mathrm{Gal}(E/k(\theta)) = \Gamma \cap H \ , \ [k(\theta) : k] = [\Gamma : \Gamma \cap H]$$

et par suite : $\theta \in k$ ssi $\Gamma \subset H$.

Démonstration. Soit $g \in \Gamma$; pour que $g(\theta) = \theta$, il faut et il suffit que, $j \in J$ étant fixé : $g(\widetilde{\Theta_j}) = \widetilde{\Theta_j}$, i.e. $\widetilde{g.\Theta_j} = \widetilde{\Theta_j}$. Or comme $\Gamma \subset L_0$, on a $g.\Theta_j \in \{\Theta_1, \ldots, \Theta_e\}$, donc la condition $g(\theta) = \theta$ équivaut à :

$$g.\Theta_j \in \{\Theta_l\}_{l \in J} \qquad ; \tag{32}$$

C'est vrai avec tout $j \in J$, donc cette condition équivaut aussi à : $g \in M$. De plus si la condition (32) est satisfaite avec un $j \in J$, elle entraîne $g \in M$; en prenant $j = 1$ cela donne : $g.\Theta = \Theta \Rightarrow g \in M$, d'où $\Gamma \cap H \subset \Gamma \cap M$. On a donc prouvé que $\mathrm{Gal}(E/k(\theta)) = \Gamma \cap M$ et que $\Gamma \cap H \subset \Gamma \cap M$. On prouve l'inégalité

$[\Gamma : \Gamma \cap H] \leq \nu\,[k(\theta) : k]$ comme au Théorème 6.3, ce qui achève d'établir toutes des assertions de a).

b) On obtient les assertions b) en faisant $\nu = 1$ dans les assertions a) □

Démonstration du Théorème 6.10. Soit $\{\tau_i\}_{1\leq i\leq e}$ une transversale gauche de L_0 mod H, avec $\tau_1 = \mathrm{Id}$, l'élément neutre de $\mathfrak{S}_n$. On supposera cette transversale indexée de façon que les Θ_i de (28) soient donnés par $\Theta_i = \tau_i.\Theta$ $(1 \leq i \leq e)$. Posons $H_i = \tau_i H \tau_i^{-1}$, $\theta_i = \widetilde{\Theta_i}$, d'où : $H_i = \mathrm{Stab}_{L_0}(\Theta_i)$, $\mathcal{L}^{[L_0]}_{\Theta,f}(x) = \prod_{i=1}^{e}(x - \Theta_i)$. Par définition, la partition $\varpi(\mathcal{G}^{[L_0]}, \mathcal{C}^{[L_0]})$ de e est $(N_1/1, \ldots, N_e/e)$, où $N_j = \mathrm{card}(\{m \in [1,e] \mid [\Gamma : \Gamma \cap H_m] = j\})$ pour $1 \leq j \leq e$. Fixons $j \in [1,e]$; soit P un facteur k-irréductible simple de degré j de $\mathcal{L}^{[L_0]}_{\Theta,f}(x)$. Par hypothèse, P est séparable, d'où $P = \prod_{m\in J}(x - \theta_m)$, où $J \subset [1,e]$ et $\mathrm{card}(J) = j$. Si $m \in J$, d'après le Théorème 6.11, on a $j = \deg(P) = [\Gamma : \Gamma \cap H_m]$, d'où $j\alpha_j \leq N_j$. Puisque c'est vrai pour tout j, on en déduit bien :

$$(\alpha_1, \ldots, \alpha_e) \preceq \varpi(\mathcal{G}^{[L_0]}, \mathcal{C}^{[L_0]}) \qquad . \tag{33}$$

Si de plus Θ est (L_0, f)-séparable, alors $(\alpha_1, \ldots, \alpha_e)$ est une partition de e, de même que $\varpi(\mathcal{G}^{[L_0]}, \mathcal{C}^{[L_0]})$. D'après (33), ces partitions sont donc égales □

Compte tenu du Théorème 3.1, le Théorème 6.10 conduit immédiatement à la version relative du Théorème 6.7 (“ méthode de la chasse aux résolvantes relatives ”) :

Théorème 6.12. Soit L_0 un sous-groupe de $\mathfrak{S}_n$ contenant le groupe de Galois $\Gamma = \mathrm{Gal}(E/k)$. Notons $\mathcal{C}_1^{[L_0]}, \ldots, \mathcal{C}_{s_0}^{[L_0]}$ les classes de sous-groupes conjugués distinctes dans le groupe L_0. Pour chaque $j \in [1, s_0]$, choisissons un groupe $H_j \in \mathcal{C}_j^{[L_0]}$ et un résolvant relatif Θ_j de H_j par rapport à L_0. Supposons que les Θ_j $(1 \leq j \leq s_0)$ soient tous (L_0, f)-séparables. Alors la classe de conjugaison $\mathcal{G}^{[L_0]}$ de Γ dans L_0 est $\mathcal{C}_r^{[L_0]}$, où r est l'indice de la ligne de la matrice des partitions

$$\mathcal{P}^{[L_0]} = [\varpi(\mathcal{C}_i^{[L_0]}, \mathcal{C}_j^{[L_0]})]_{\substack{1\leq i\leq s_0 \\ 1\leq j\leq s_0}}$$

du groupe L_0, qui est égale à la ligne :

$$(\pi^{[L_0]}(\Theta_1, f), \pi^{[L_0]}(\Theta_2, f), \ldots, \pi^{[L_0]}(\Theta_s, f)) \qquad .$$

Il va de soi que toutes les remarques faites dans le cas absolu pour affiner le Théorème 6.7 se transposent sans difficulté au cas du théorème relatif 6.12.

Résultats et améliorations

Ici le mot “ groupe ”, sera utilisé pour classe de conjugaison. Nous nous plaçons dans le cas où les facteurs irréductibles des résolvantes sont simples, même si c'est loin d'être le cas dans la pratique et qu'alors nous faisons appel au Théorème des multiplicités (voir 6.5) qui nous permet couramment de conclure. Nous employons l'expression “ savoir déterminer ” lorsque deux conditions sont à la fois réunies : la première est que les résolvantes, soient non seulement calculables, mais que les

calculs soient réalisables sur notre machine (voir [Marie]) et la deuxième est que chaque résolvante obtenue soit également factorisable sur notre machine.

Jusqu'en degré 7, nous pouvons désormais identifier le groupe de Galois de tout polynôme non nécessairement irréductible. Nous avons résolu les degrés 8,9 et 11 pour tout polynôme irréductible. Le degré 10, doit être complété par des calculs de *résolvantes relatives* pour être achevé.

Les algorithmes s'améliorent considérablement en calculant la matrice des groupes de Galois des facteurs irréductibles simples des résolvantes. La description de cette matrice est faite dans [A. Valibouze3]. Dans cet article la méthode est illustrée par l'étude en degré 8 et 10. Par exemple, en degré 8, un calcul de plusieurs heures est évité par une détermination établie en quelques secondes. Cet article explique également comment cette matrice intervient dans le problème de Galois inverse. Cette méthode est appliquée dans [I. Gil-Delessalle, A. Valibouze] pour trouver des polynômes de degré 12.

7. Application à la spécialisation des groupes de Galois

Nous conservons ci-après toutes les notations en vigueur au début du §6.

Nous allons donner une version affinée du théorème de spécialisation du groupe de Galois tel qu'il est exposé par exemple dans [R. Brauer].

Donnons-nous un sous-anneau A de k, dont k soit le corps des fractions, et un idéal premier $\mathfrak{p}$ de A ; notons $A^\bullet = A/\mathfrak{p}$, et $\alpha : A \to A^\bullet$ le morphisme canonique, $k^\bullet$ le corps des fractions de $A^\bullet$, et enfin $\hat{k^\bullet}$ une clôture algébrique de $k^\bullet$. Pour tout $h \in A[x]$, nous désignerons par $h^\bullet$ l'élément de $A^\bullet[x]$ obtenu en appliquant α aux coefficients de h. De même pour $h \in A[x, x_1, \ldots, x_n]$.

Rappelons que $(\mathcal{C}_1, \ldots, \mathcal{C}_s)$ désigne une ordination, par degrés décroissants, de l'ensemble $\mathcal{E}$ des classes de conjugaison des sous-groupes de $\mathfrak{S}_n$. Nous considèrerons un système séparant $(J_j)_{1 \le j \le s}$ de parties de $[1, s]$, fixé une fois pour toutes, de support J. Rappelons que pour chaque $i \in [1, s]$, on a fixé un élément H_i de $\mathcal{C}_i$.

Pour chaque $i \in [1, s]$, le groupe H_i possède au moins un résolvant élément de $A[x_1, \ldots, x_n]$: il suffit en effet, pour en construire un, de multiplier un résolvant de H_i par un élément convenable de $A \backslash \{0\}$.

On notera $E^\bullet$ la $k^\bullet$-algèbre des racines de $f^\bullet$ dans $\hat{k^\bullet}$; si $f^\bullet$ est séparable, $E^\bullet$ est une extension galoisienne de $k^\bullet$ et alors on notera $\Gamma^\bullet = \mathrm{Gal}(E^\bullet / k^\bullet)$. Observons que si A est intégralement clos, tout facteur normalisé, dans $k[x]$, d'un polynôme normalisé $F \in A[x]$ appartient nécessairement à $A[x]$. En particulier, les facteurs k-irréductibles normalisés de F appartiennent alors à $A[x]$.

Notre but est, dans l'hypothèse où $f^\bullet$ est, comme f, séparable, d'appliquer le Théorème 6.7 simultanément à f et $f^\bullet$.

Pour y parvenir, nous devons préciser une numérotation des racines de $f^\bullet$ dans $\hat{k^\bullet}$ qui soit liée à la numérotation des ρ_i. Soit un idéal premier $\mathfrak{P}$ de $B = A[\rho_1, \ldots, \rho_n]$ tel que $\mathfrak{P} \cap A = \mathfrak{p}$: un tel idéal existe puisque les ρ_i sont A-entiers. Notons $B^\bullet = B/\mathfrak{P}$ et $\beta : B \to B^\bullet = B/\mathfrak{P}$ la projection canonique ; alors β prolonge α ; posant $\rho_i^\bullet = \beta(\rho_i)$ pour $1 \le i \le n$, le corps des fractions de $B^\bullet = A^\bullet[\rho_1^\bullet, \ldots, \rho_n^\bullet]$

est une $k^\bullet$-algèbre des racines de $f^\bullet$. Les $\rho_i^\bullet$ sont distincts puisque $f^\bullet$ est séparable. Sans perte de généralité, nous pouvons supposer que $B^\bullet \subset \hat{k^\bullet}$ et donc que $E^\bullet$ est le corps des fractions $k^\bullet[\rho_1^\bullet, \dots, \rho_n^\bullet]$ de $B^\bullet$. D'où en particulier :

$$f^\bullet = \prod_{i=1}^{n}(x - \rho_i^\bullet) \qquad ; \tag{34}$$

nous conviendrons d'utiliser la numérotation $(\rho_i^\bullet)_{1\leq i\leq n}$ des racines de $f^\bullet$ dans $\hat{k^\bullet}$ pour identifier $\Gamma^\bullet$ à un sous-groupe de $\mathfrak{S}_n$ et donc pour spécialiser dans $\hat{k^\bullet}$ les éléments de $\mathcal{A}^\bullet = k^\bullet[x_1, \dots, x_n]$. Nous poserons $\mathcal{K}^\bullet = k^\bullet(\sigma_1, \dots, \sigma_n)$ et $\mathcal{F}^\bullet = k^\bullet(x_1, \dots, x_n)$, les lettres $x, x_1, \dots, x_n$ étant utilisées comme indéterminées aussi bien sur $\hat{k}$ que sur $\hat{k^\bullet}$. (Toute cette construction suppose bien entendu que l'idéal $\mathfrak{P}$ a été fixé une fois pour toutes.)

Le lemme suivant sera utile :

Lemme 3. La séparabilité de $f^\bullet$ implique la séparabilité de f.

Démonstration. D'après (34), on a : $f^\bullet = \prod_{i=1}^{n}(x - \beta(\rho_i))$; donc si les $\rho_i^\bullet = \beta(\rho_i)$ sont distincts, a fortiori les ρ_i le sont, et par suite $f = \prod_{i=1}^{n}(x-\rho_i)$ est séparable □

Théorème 7.1. Soit un résolvant $\Theta \in A[x_1, \dots, x_n]$ d'un sous-groupe H de $\mathfrak{S}_n$. Si $\mathcal{L}^\bullet_{\Theta,f}$ est séparable, alors $\Theta^\bullet$ est un résolvant de H, on a : $\mathcal{L}_{\Theta^\bullet,f^\bullet} = \mathcal{L}^\bullet_{\Theta,f}$ et $\mathcal{L}_{\Theta,f}$ est séparable.

Démonstration. Le fait que $\mathcal{L}_{\Theta,f}$ est séparable se déduit du Lemme 3 ci-dessus. Notons $\Theta_1, \dots, \Theta_e$ les conjugués de Θ sous $\mathfrak{S}_n = \mathrm{Gal}(\mathcal{F}/\mathcal{K})$, Avec $\Theta_1 = \Theta$ et $e = [\mathfrak{S}_n : H]$. On a :

$$\mathcal{L}_{\Theta,f} = \prod_{i=1}^{e}(x - \Theta_i(\rho_1, \dots, \rho_n)) \qquad ,$$

d'où puisque β prolonge α :

$$\mathcal{L}^\bullet_{\Theta,f} = \prod_{i=1}^{e}(x - \Theta_i^\bullet(\rho_1^\bullet, \dots, \rho_n^\bullet)) = \prod_{i=1}^{e}(x - \beta(\Theta_i(\rho_1, \dots, \rho_n))) \qquad ; \tag{35}$$

puisque $\mathcal{L}^\bullet_{\Theta,f}$ est séparable, les $\Theta_i^\bullet(\rho_1^\bullet, \dots, \rho_n^\bullet) = \beta(\Theta_i(\rho_1, \dots, \rho_n))$ sont distincts, et a fortiori $\Theta_1^\bullet, \dots, \Theta_e^\bullet$ sont distincts (et les $\Theta_i(\rho_1, \dots, \rho_n)$ le sont aussi, ce qui redonne la séparabilité de $\mathcal{L}_{\Theta,f}$). Mais il est clair que $H \subset \mathrm{Stab}_{\mathfrak{S}_n}(\Theta^\bullet)$; le nombre des $\mathfrak{S}_n$-conjugués de $\Theta^\bullet$ est $\geq e$, mais ce nombre est $[\mathfrak{S}_n : \mathrm{Stab}_{\mathfrak{S}_n}(\Theta^\bullet)] \leq [\mathfrak{S}_n : H] = e$, donc il vaut e. D'où $H = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta^\bullet)$, ce qui prouve bien que $\Theta^\bullet$ est un résolvant de H. On a alors $\mathcal{L}^\bullet_\Theta = \prod_{i=1}^{e}(x - \Theta_i^\bullet)$ et d'après (35), cela rend bien clair que $\mathcal{L}_{\Theta^\bullet,f^\bullet} = \mathcal{L}^\bullet_{\Theta,f}$ □

Théorème 7.2. Supposons que A soit intégralement clos. Si $f^\bullet$ est séparable, le groupe $\Gamma^\bullet = \mathrm{Gal}(E^\bullet/k^\bullet)$ s'identifie à un sous-groupe de $\Gamma = \mathrm{Gal}(E/k)$. Si de plus f est irréductible et normal sur k et $f^\bullet$ est irréductible sur $k^\bullet$, alors $\Gamma = \Gamma^\bullet$.

Démonstration. Les lettres $z, U_1, \ldots, U_n, x, x_1, \ldots, x_n$ seront utilisées comme indéterminées aussi bien sur $\hat{k}$ que sur $\widehat{k^\bullet}$. On notera $\underline{U} = (U_1, \ldots, U_n)$. Posons :

$$\begin{aligned}
\xi &= \sum_{i=1}^{n} \rho_i U_i \quad ; \quad \xi^\bullet = \sum_{i=1}^{n} \rho_i^\bullet U_i \quad ; \\
\Phi &= \prod_{\sigma\in\mathfrak{S}_n} (z - \sum_{i=1}^{n} U_i x_{\sigma(i)}) \; ; \; \varphi = \prod_{\sigma\in\mathfrak{S}_n} (z - \sum_{i=1}^{n} U_i \rho_{\sigma(i)}) \quad ; \\
\psi &= \prod_{\sigma\in\mathfrak{S}_n} (z - \sum_{i=1}^{n} U_i \rho^\bullet_{\sigma(i)}) \quad ;
\end{aligned}$$

pour toute classe à droite C de $\mathfrak{S}_n$ mod Γ, posons :

$$\begin{aligned}
\Phi_C &= \prod_{\sigma\in C} (z - \sum_{i=1}^{n} U_i x_{\sigma(i)}) \; ; \; \varphi_C = \prod_{\sigma\in C} (z - \sum_{i=1}^{n} U_i \rho_{\sigma(i)}) \quad ; \\
\psi_C &= \prod_{\sigma\in C} (z - \sum_{i=1}^{n} U_i \rho^\bullet_{\sigma(i)}) \quad .
\end{aligned}$$

Comme A est intégralement clos, on a $\varphi \in A[z, \underline{U}]$, et pour toute classe à droite C de $\mathfrak{S}_n$ mod Γ : $\varphi_C \in A[z, \underline{U}]$. De plus ψ (resp. ψ_C) s'obtiennent à partir de φ (resp. φ_C) en appliquant α aux coefficients, donc $\psi \in A^\bullet[z, \underline{U}]$ et $\psi_C \in A^\bullet[z, \underline{U}]$. L'extension $E^\bullet(\underline{U})$ de $k^\bullet(\underline{U})$ est galoisienne, c'est une $k^\bullet(\underline{U})$-algèbre des racines de $f^\bullet$. Il est clair que : $E(\underline{U}) = k(\underline{U})[\xi]$ et $E^\bullet(\underline{U}) = k^\bullet(\underline{U})[\xi^\bullet]$. Les groupes $\mathrm{Gal}(E^\bullet(\underline{U})/k^\bullet(\underline{U}))$ et $\mathrm{Gal}(E(\underline{U})/k(\underline{U}))$ s'identifient respectivement à $\Gamma^\bullet$ et Γ, et $\mathfrak{S}_n$ s'identifie de même à $\mathrm{Gal}(\mathcal{F}^\bullet(\underline{U})/\mathcal{K}^\bullet(\underline{U}))$ et à $\mathrm{Gal}(\mathcal{F}(\underline{U})/\mathcal{K}(\underline{U}))$. Le polynôme Φ (resp. Φ_C) s'entend comme élément de $A[z, x_1, \ldots, x_n, \underline{U}]$; le polynôme de même écriture dans $A^\bullet[z, x_1, \ldots, x_n, \underline{U}]$ sera noté $\Phi^\bullet$ (resp. $\Phi^\bullet_C$). Pour tous anneaux R_1, R_2 et pour tout morphisme d'anneaux $\mu : R_1 \to R_2$, on conviendra de désigner par la même lettre μ toute extension de μ en un morphisme $R_1[y_1, \ldots, y_m] \to R_2[y_1, \ldots, y_m]$, (où $(y_i)_{1\le i\le m}$ désigne une suite d'indéterminées) consistant à appliquer μ aux coefficients des éléments de $R_1[y_1, \ldots, y_m]$.

Soit alors $\tau \in \Gamma^\bullet$. De part la théorie de Galois, on a $\psi_\Gamma = \tau.\psi_\Gamma$ et d'après la formule (24) du §5, on a $\tau.\psi_\Gamma = M^\bullet(\tau.\Phi^\bullet_\Gamma)$ d'où :

$$\psi_\Gamma = M^\bullet(\tau.\Phi^\bullet_\Gamma) \quad ,$$

où $M^\bullet : \mathcal{A}^\bullet \to \hat{k^\bullet}$ désigne le morphisme de spécialisation $h \mapsto h(\rho_1^\bullet, \ldots, \rho_n^\bullet)$.

D'autre part : $M^\bullet(\tau.\Phi^\bullet_\Gamma) = \alpha.M(\tau.\Phi_\Gamma)$, où $M : \mathcal{A} \to \hat{k}$ désigne le morphisme de spécialisation $h \mapsto h(\rho_1, \ldots, \rho_n)$. Donc $\alpha.M(\tau.\Phi_\Gamma) = \psi_\Gamma$, c'est-à-dire :

$$\prod_{\sigma\in\Gamma}(z-\sum_{i=1}^{n}U_i\rho^{\bullet}_{\sigma(i)})=\prod_{\sigma\in\Gamma}(z-\sum_{i=1}^{n}U_i\rho^{\bullet}_{\tau\sigma(i)}) \qquad . \tag{36}$$

Mais le polynôme $\psi\in k^{\bullet}(\underline{U})[z]$ est à facteurs simples ; donc d'après (36), on a : $\Gamma=\{\tau\sigma\}_{\sigma\in\Gamma}=\tau\Gamma$, c'est-à-dire : $\tau\in\Gamma$. Ce qui établit que $\Gamma^{\bullet}\subset\Gamma$.

Supposons pour finir que f est irréductible dans $k[x]$ et normal sur k, et que $f^{\bullet}$ est irréductible dans $k^{\bullet}[x]$, les hypothèses ci-dessus continuant à être satisfaites. Alors $\mathrm{card}(\Gamma)=n$, et $\mathrm{card}(\Gamma^{\bullet})\geq n$ à cause de l'irréductibilité de $f^{\bullet}$. Puisque $\Gamma^{\bullet}\subset\Gamma$, nécessairement ici $\Gamma^{\bullet}=\Gamma$ □

Théorème 7.3. Supposons toujours l'anneau A intégralement clos. Pour chaque indice $i\in J$, soit un résolvant $\Theta_i\in A[x_1,\dots,x_n]$ de H_i. Supposons que $f^{\bullet}$ soit séparable, que tous les polynômes $\mathcal{L}^{\bullet}_{\Theta_i,f}$ $(i\in J)$ soient séparables, et que pour tout $i\in J$ et pour tout facteur P de $\mathcal{L}_{\Theta_i,f}$ normalisé et irréductible dans $k[x]$, le polynôme $P^{\bullet}$ soit irréductible dans $k^{\bullet}[x]$. Alors $\Gamma^{\bullet}=\Gamma$.

Démonstration. D'après le Théorème 7.2, on a déjà $\Gamma^{\bullet}\subset\Gamma$. D'après le Théorème 7.1, pour tout $i\in J$, $\Theta^{\bullet}_i$ est un résolvant de H_i, le polynôme $\mathcal{L}_{\Theta_i,f}$ est séparable et $\mathcal{L}^{\bullet}_{\Theta_i,f}=\mathcal{L}_{\Theta^{\bullet}_i,f^{\bullet}}$. Alors l'hypothèse faite entraîne que pour tout $i\in J$, les partitions $\pi(\Theta_i,f)$ et $\pi(\Theta^{\bullet}_i,f^{\bullet})$ sont égales. D'après le Théorème 6.7 et les précisions qui le suivent, on voit que les classes de conjugaison de $\mathfrak{S}_n$ des groupe Γ et $\Gamma^{\bullet}$ coïncident. A fortiori, Γ et $\Gamma^{\bullet}$ sont isomorphes. Et puisque $\Gamma^{\bullet}\subset\Gamma$, en définitive $\Gamma^{\bullet}=\Gamma$ □

En appliquant le Théorème d'irréductibilité de Hilbert, le Théorème 7.1 fournit le résultat suivant, qui précise le bien connu théorème de Noether sur la conservation des groupes de Galois par certaines spécialisations :

Corollaire 7.4. Soit K un corps de nombres et $t_1,\dots,t_m$ des indéterminées sur K. Prenons $k=K(t_1,\dots,t_m)$ et $A=K[t_1,\dots,t_m]$, et supposons $f\in A[x]$; pour tout $i\in J$, soit un résolvant $\Theta_i\in A[x_1,\dots,x_n]$ de H_i ; pour tout $a=(a_1,\dots,a_m)\in K^m$ et tout $h\in A[x]$, notons h_a l'élément de $k[x]$ obtenu en spécialisant $t_i\rightsquigarrow a_i$ $(1\leq i\leq m)$ dans les coefficients de h. Alors le groupe de Galois $\mathrm{Gal}(k,f)$ de f sur k est isomorphe au groupe de Galois $\mathrm{Gal}(K,f_a)$ de f_a sur K pour tout $a\in K^m$ vérifiant les conditions suivantes : f_a est séparable, les résolvantes $\mathcal{L}_{\Theta_i,f_a}$ $(i\in J)$ sont toutes séparables, et pour tout $i\in J$ et tout facteur k-irréductible normalisé P de $\mathcal{L}_{\Theta_i,f}$, le polynôme P_a est irréductible dans $K[x]$.

En conséquence, il y a une infinité d'éléments $a\in K^m$ tels que $\mathrm{Gal}(k,f)\cong\mathrm{Gal}(K,f_a)$.

L'intérêt des Théorèmes 7.1 à 7.3 ne se réduit pas au corollaire ci-dessus, car le cas où k et $k^{\bullet}$ n'ont pas même caractéristique n'est pas exclu, comme nous allons le voir ci-dessous.

Soit p un nombre entier rationnel premier et soit m un entier ≥ 1. Prenons :

$$(37)\qquad \begin{cases} k = \mathbb{Q}(t_1, \dots, t_m) \text{ (les } t_i \text{ indéterminées sur } \mathbb{Q}) \\ A = \mathbb{Z}[t_1, \dots, t_m] \quad ; \\ \text{pour tout } i \in J,\ \Theta_i \in A[x_1, \dots, x_n] \text{ et } \Theta_i \text{ résolvant de } H_i \end{cases} .$$

Alors $A^\bullet = \mathbb{F}_p[t_1, \dots, t_m]$ et $k^\bullet = \mathbb{F}_p(t_1, \dots, t_m)$. En particulier, ici A et $A^\bullet$ sont intégralement clos.

Pour tout élément $F \in A[x]$, notons $\mathcal{M}(F)$ le maximum des valeurs absolues des coefficients de F lorsque F est considéré comme polynôme à coefficients dans $\mathbb{Z}$ en les variables $x, t_1, \dots, t_m$. On a alors :

Théorème 7.5. Plaçons-nous sous les hypothèses (37). Supposons que $f^\bullet$ et tous les polynômes $\mathcal{L}^\bullet_{\Theta_i,f}$ $(i \in J)$ soient séparables. Pour chaque indice $i \in J$, soit $\prod_{1\le m\le \nu_i} Q_{i,m}$ une décomposition de $\mathcal{L}^\bullet_{\Theta_i,f}$ dans $k^\bullet[x]$ en facteurs normalisés irréductibles (donc nécessairement les $Q_{i.m}$ appartiennent à $A^\bullet[x]$), et soit $P_{i,m}$ $(i \in J\,,\, 1 \le m \le \nu_i)$ un polynôme normalisé, élément de $A[x]$, tel que $P^\bullet_{i,m} = Q_{i,m}$. Supposons de plus que $p > \mathcal{M}(\mathcal{L}_{\Theta_i,f}) + \mathcal{M}(\prod_{1\le m\le \nu_i} P_{i,m})$ pour tout $i \in J$. Alors $\Gamma = \mathrm{Gal}(E/k)$ est égal à $\Gamma^\bullet = \mathrm{Gal}(E^\bullet/k^\bullet)$.

Démonstration. Pour tout $i \in J$, on a : $\mathcal{L}^\bullet_{\Theta_i,f} = \prod_{1\le m\le \nu_i} P^\bullet_{i,m} = (\prod_{1\le m\le \nu_i} P_{i,m})^\bullet$. Posons $F_i = \mathcal{L}_{\Theta_i,f} - \prod_{1\le m\le \nu_i} P_{i,m}$. D'après ce qui précède, $F_i \in pA[x]$. Mais $\mathcal{M}(F_i) \le \mathcal{M}(\mathcal{L}_{\Theta_i,f}) + \mathcal{M}(\prod_{1\le m\le \nu_i} P_{i,m}) < p$, d'où forcément $F_i = 0$, i.e. $\mathcal{L}_{\Theta_i,f} = \prod_{1\le m\le \nu_i} P_{i,m}$. Puisque $P^\bullet_{i,m} = Q_{i,m}$ est $k^\bullet$-irréductible et normalisé, il est $A^\bullet$-irréductible donc $P_{i,m}$ est irréductible dans $A[x]$; mais $P_{i,m}$ étant normalisé et $A^\bullet$ étant intégralement clos, on voit que $P_{i,m}$ est irréductible dans $k[x]$. Autrement dit, $\prod_{1\le m\le \nu_i} P_{i,m}$ est une décomposition de $\mathcal{L}_{\Theta_i,f}$ en facteurs irréductibles dans $k[x]$ et normalisés. De plus $\mathcal{L}_{\Theta_i,f}$ est séparable, et on voit alors que le Théorème 7.3 s'applique et donne bien $\Gamma^\bullet = \Gamma$ □

Le Théorème 7.5 est un cas de remontée de la caractéristique p à la caractéristique 0 dans le problème de Galois inverse. Soit G un groupe fini, sous-groupe d'un groupe $\mathfrak{S}_n$, réalisable comme groupe de Galois d'un polynôme sur $\mathbb{F}_p(t_1, \dots, t_m)$ à coefficients dans un anneau du type $\mathbb{F}_p[t_1, \dots, t_m]$ et normalisé. Si l'on peut trouver f et des Θ_i satisfaisant les hypothèses du Théorème 7.5, alors G sera réalisable comme groupe de Galois sur $\mathbb{Q}(t_1, \dots, t_m)$; puis grâce au corollaire 7.5, G sera réalisable comme groupe de Galois sur $\mathbb{Q}$.

8. Groupe de Galois métacycliques de degré premier

Nous allons ici rappeler quelques faits connus sur les groupes métacycliques de degré premier.

Définition 8.1. Un groupe fini G est dit *métacyclique* ssi il admet une suite de composition de la forme $\{e_G\} \to C \to G$ $(C \lhd G)$ telle que G et G/C soient cycliques.

(En particulier, tout produit semi-direct de deux groupes cycliques est métacyclique.)

Soit p un nombre premier impair. Dans le groupe de permutation $\mathfrak{S}_{\mathbb{F}_p}$, le groupe $\mathfrak{M}_p$ des similitudes $s_{a,b} : x \mapsto ax + b$ (où $(a, b) \in \mathbb{F}_p^\star \times \mathbb{F}_p$ est fixé) est transitif (et même doublement transitif) et il est métacyclique. Il possède un unique p-Sylow $\mathfrak{C}_p$, engendré par le cycle $\tau = s_{1.1}$; ce groupe $\mathfrak{C}_p$ est p-cyclique, et $\mathfrak{M}_p/\mathfrak{C}_p \cong \mathbb{F}_p^\star$ est $(p-1)$-cyclique. Le groupe $\mathfrak{M}_p$ est le produit semi-direct de ses sous-groupes $\mathfrak{C}_p$ et $S_p = \{s_{a,0}\}_{a\in\mathbb{F}_p^\star}$. On a $\mathrm{card}(\mathfrak{M}_p) = p(p-1)$, et pour tout groupe H tel que $\mathfrak{C}_p \subset H \subset \mathfrak{M}_p$, le normalisateur de H dans $\mathfrak{S}_{\mathbb{F}_p}$ est $\mathfrak{M}_p$.

Le groupe $\mathfrak{M}_p$ sera appelé le *groupe métacyclique canonique de degré* p, et son sous-groupe d'indice 2 : $\mathfrak{M}_p \cap \mathfrak{A}_{\mathbb{F}_p}$, que nous noterons $\mathfrak{M}_p^+$, sera appelé le *groupe métacyclique pair* canonique de degré p. On a : $\mathfrak{C}_p \subset \mathfrak{M}_p^+$, et $\mathfrak{M}_p^+/\mathfrak{C}_p \cong \mathbb{F}_p^{\star\square}$, où $\mathbb{F}_p^{\star\square}$ désigne le sous-groupe des carrés dans $\mathbb{F}_p^\star$ (donc $\mathbb{F}_p^{\star\square}$ est cyclique de cardinal $(p-1)/2$, et $\mathfrak{M}_p^+$ est un sous-groupe métacyclique de cardinal $p(p-1)/2$). Le groupe $\mathfrak{M}_p^+$ est le produit semi-direct de ses sous-groupes $\mathfrak{C}_p$ et $S_p^+ = \{s_{a,0}\}_{a\in\mathbb{F}_p^{\star\square}}$.

Chaque bijection $\mathbb{F}_p \to [1, p]$ tansporte $\mathfrak{M}_p$ (resp. $\mathfrak{M}_p^+$) sur un sous-groupe de $\mathfrak{S}_p$. Les sous-groupes ainsi obtenus serons appelés les *sous-groupes métacycliques principaux* (resp. *sous-groupes métacycliques principaux pairs*) de $\mathfrak{S}_p$. Ils forment une classe de conjugaison de sous-groupes de $\mathfrak{S}_p$; cette classe est formée de $(p-2)!$ sous-groupes. Tout sous-groupe de $\mathfrak{S}_p$ de cardinal p est contenu dans un et un seul sous-groupe métacyclique principal (resp. métacyclique principal pair) de $\mathfrak{S}_p$, et le sou-groupe métacyclique principal pair qui le contient et évidemment le sous-groupe métacyclique pair du sous-groupe métacyclique principal qui le contient. Le résultat ci-après est bien connu :

Théorème 8.2. Soit $\mathfrak{R}$ un sous-groupe transitif résoluble de $\mathfrak{S}_p$. Alors $\mathfrak{R}$ est contenu dans un et un seul sous-groupe métacyclique principal de $\mathfrak{S}_p$. En conséquence, les sous-groupes résolubles transitifs maximaux de $\mathfrak{S}_p$ sont les sous-groupes métacycliques principaux, et les sous-groupes résolubles transitifs maximaux $\mathfrak{A}_p$ sont les sous-groupes métacycliques principaux pairs de $\mathfrak{S}_p$.

Démonstration. Si M_1 et M_2 sont deux sous-groupes métacycliques principaux de $\mathfrak{S}_p$, $(M_1 \neq M_2)$, alors $M_1 \cap M_2$ n'est pas transitif. Il suffit donc pour établir toutes les assertions du théorème, de prouver que $\mathfrak{R}$ est contenu dans un sous-groupe métacyclique principal de $\mathfrak{S}_p$. Considérons une suite de composition

$$\{\mathrm{Id}\} = G_0 \hookrightarrow G_1 \hookrightarrow \cdots \hookrightarrow G_m \hookrightarrow \mathfrak{R} = G_{m+1}$$

de $\mathfrak{R}$ (où $m \geq 0$) telle que les quotients G_{i+1}/G_i $(0 \leq i \leq m)$ soient tous cycliques de cardinal premier.

- Si $m = 0$, alors $\mathfrak{R} = G_1$ est cyclique ; comme p est premier, et comme $\mathfrak{R}$ est transitif, G_1 ne peut dans ce cas qu'être l'un des sous-groupes cycliques de cardinal p de $\mathfrak{S}_p$, i.e. l'un des sous-groupes engendrés par un p-cycle. On a déjà signalé plus haut qu'un tel sous-groupe est contenu dans un et un seul des sous-groupes métacycliques principaux de $\mathfrak{S}_p$.

- Si $m \geq 1$, nous allons montrer que G_1 est transitif : par récurrence évidente, il suffit pour cela de prouver que G_m est transitif. Soit $\mathcal{G}$ l'ensemble des G_m-orbites dans $[1, p]$. Puisque $G_m \lhd \mathfrak{R}$ et puisque $\mathfrak{R}$ est transitif, on déduit que $\mathcal{G}$ est $\mathfrak{R}$-stable et que $\mathfrak{R}$ opère transitivement sur $\mathcal{G}$. Les éléments $\omega \in \mathcal{G}$ forment donc une partition de $[1, p]$ en parties de même cardinal ; p étant premier, et G_m étant $\neq \{\mathrm{Id}\}$, il en découle que $\mathcal{G}$ n'a qu'un élément, donc G_m est bien transitif.

Ainsi G_1 est transitif ; il contient donc un p-cycle τ ; comme G_1 est cyclique, nécessairement G_1 est le sous-groupe $\mathfrak{C}$ engendré par τ. Soit M l'unique sous-groupe métacyclique principal de $\mathfrak{S}_p$ contenant $\mathfrak{C}$. On a vu plus haut que pour tout sous-groupe H de $\mathfrak{S}_p$ tel que $\mathfrak{C} \subset H \subset M$, le normalisateur de H dans $\mathfrak{S}_p$ est M. Comme $G_1 = \mathfrak{C} \lhd G_2$, on en déduit que $G_2 \subset M$, puis par une récurrence immédiate, que $G_3 \subset M, \ldots, G_{m+1} = \mathfrak{R} \subset M$ □

Exemple 1. : $p = 5$

Les sous-groupes métacycliques principaux de $\mathfrak{S}_5$, au nombre de 6, sont de cardinal 20. Ce sont des sous-groupes maximaux de $\mathfrak{S}_5$; leurs 6 sous-groupes d'indice 2 sont les sous-groupes métacycliques principaux pairs de $\mathfrak{S}_5$, isomorphes au groupe diédral $\mathcal{D}_5$. Ils sont maximaux dans $\mathfrak{A}_5$. Les seuls sous-groupes résolubles transitifs de $\mathfrak{S}_5$ sont les 12 sous-groupes ci-dessus et les 6 sous-groupes cycliques de cardinal 5.

Exemple 2. : $p = 7$

Les sous-groupes métacycliques principaux de $\mathfrak{S}_7$, au nombre de 120, sont de cardinal 42. Ils sont maximaux dans $\mathfrak{S}_7$. En revanche, les 120 sous-groupes métacycliques principaux pairs, de cardinal 21, ne sont pas maximaux dans $\mathfrak{A}_7$. Si M est un sous-groupe métacyclique principal, ses sous-groupes transitifs sont, outre M : l'unique sous-groupe métacyclique pair qu'il contient, que nous notons M^+ ; l'unique sous-groupe 7-cyclique qu'il contient, que nous noterons $\mathfrak{C}_M$; et l'unique sous-groupe isomorphe au groupe diédral $\mathcal{D}_7$ qu'il contient, et que nous noterons $\mathfrak{D}_M$. On a $\mathfrak{C}_M \subset \mathfrak{D}_M \subset M$, $\mathfrak{C}_M \subset M^+ \subset M$, $\mathfrak{D}_M \cap \mathfrak{A}_7 = \mathfrak{C}_M$ (donc $\mathfrak{D}_M \not\subset M^+$). Par suite les sous-groupes résolubles transitifs de $\mathfrak{S}_7$ sont : les 120 groupes M, les 120 groupes M^+, les 120 groupes $\mathfrak{D}_M$ et les 120 groupes $\mathfrak{C}_M$, soit en tout 480 groupes.

9. Groupes de Galois et résultants

Nous allons voir que pour obtenir des polynômes ayant pour groupe de Galois une extension d'un groupe par un autre, il y a intérêt à former certains résultants. Dans tout ce paragraphe le corps k sera supposé infini.

9.1. Cas d'un seul paramètre. Donnons-nous d'abord deux indéterminées x et y sur k, et deux polynômes :

$$F = x^m - s_1 x^{m-1} + \cdots + (-1)^m s_m \in k[y][x] \qquad (m \geq 2) \tag{38}$$

$$\psi = y^\nu - t_1 y^{\nu-1} + \cdots + (-1)^\nu t_\nu \in k[y] \qquad (\nu \geq 2) \qquad , \tag{39}$$

où nous notons $F = F(x, y)$, vérifiant les quatres conditions suivantes :

$$\psi \text{ est séparable, et irréductible dans } k[y] \qquad ; \tag{40}$$

$$k(s_1, \ldots, s_m) = k(y) \tag{41}$$

(on plonge $k[y][x]$ dans $k(y)[x]$), et il existe $U, V \in k[T_1, \ldots, T_m]$ tels que $y = U(s_1, \ldots, s_m)/V(s_1, \ldots, s_m)$ et $\text{pgcd}(\psi, V(s_1, \ldots, s_m)) = 1$. Notons $\mu = \deg_y(F)$; d'après (41), on a $\mu \geq 1$. Nous écrivons :

$$F = A_0(x) y^\mu + \cdots + A_\mu(x) \tag{42}$$

avec $A_i(x) \in k[x]$ pour tout i, et nous supposerons que :

$$\text{pgcd}(A_0(x), \ldots, A_\mu(x)) = 1 \qquad ; \tag{43}$$

il est clair que $A_\mu(x) = F(x, 0) = x^m - s_1(0)x^{m-1} + \cdots + (-1)^m s_m(0)$, et que $\deg_x(A_i) < m$ pour $i < \mu$. Donc le résultant R de F et ψ (considérés comme polynômes en y) est un polynôme en x de degré $m\nu$, de terme dominant $(-1)^{\mu\nu} x^{m\nu}$, à coefficients dans k. On supposera :

$$R \text{ est séparable} \qquad . \tag{44}$$

On désigne par L le corps des racines de R sur k dans $\hat{k}$, et K celui de ψ. Dans $K[x]$, on a $\psi = \prod_{i=1}^{\nu}(y - y_i)$ ($y_i \in K$, $K = k(y_1, \ldots, y_\nu)$). D'après les conditions ci-dessus, L et K sont des extensions galoisiennes de k. Nous allons comparer $\text{Gal}(L/k)$ et $\text{Gal}(K/k)$ sous certaines hypothèses.

On notera $\mathcal{R}_i$ l'ensemble des racines de $F(x, y_i)$ dans $\hat{k}$ et $\mathcal{R}$ l'ensemble des racines de R, de sorte que $\mathcal{R} = \bigcup_{i=1}^{\nu} \mathcal{R}_i$, puisque

$$R = (-1)^{\mu\nu} \prod_{i=1}^{\nu} F(x, y_i) \qquad ; \tag{45}$$

Considérons les conditions suivantes :

(I) Pour tout $\rho \in \mathcal{R}$, on a $\deg(\text{pgcd}(F(\rho, y), \psi(y))) = 1$;
(II) R est irréductible dans $k[x]$;
(III) F est un polynôme en x normal sur $k[y]$;
(IV) ψ est normal sur k.

Notons $K_i = k(y_i)$ et L_i le corps des racines de $F(x, y_i)$ sur K_i dans $\hat{k}$; puisque R est séparable, L_i est une extension galoisienne de K_i.

Théorème 9.1. Soient F et ψ vérifiant les conditions (38) à (44) ci-dessus.

a) Si la condition (I) est satisfaite, alors $K \subset L$.

b) Si les conditions (I) et (II) sont satisfaites : F est irréductible et séparable sur $k(y)$; $F(x, y_i)$ est irréductible sur K_i, et $(\mathcal{R}_1, \ldots, \mathcal{R}_\nu)$ est un système d'imprimitivité pour l'action de $\mathrm{Gal}(L/k)$ sur $\mathcal{R}$. Notons dans ce cas G le groupe de Galois de F sur $k(y)$. Alors pour tout $i \in [1, \nu]$, il y a un quotient de $\mathrm{Gal}(L/K_i)$ isomorphe à un sous-groupe transitif de G (l'action de G considérée étant l'action naturelle sur les racines de F dans $\widehat{k(y)}$).

c) Si les conditions (I),(II) et (IV) sont satisfaites, les K_i sont égaux à K, et (45) est une décomposition de R en facteurs irréductibles dans $K[x]$.

d) Si les conditions (I) à (IV) sont satisfaites, il y a un quotient de $\mathrm{Gal}(L/K)$ isomorphe à G, et si de plus R est k-normal, alors $\mathrm{Gal}(L/K) \cong G$.

Démonstration. Notons d'abord que d'après (44) et (45), chaque $F(x, y_i)$ est séparable.

a) Fixons $\rho \in \mathcal{R}$. D'après (43), on a $F(\rho, y) \neq 0$ et d'après (I), $F(\rho, y)$ ne peut pas être constant. Il y a un pgcd de $F(\rho, y)$ et $\psi(y)$ dont tous les coefficients appartiennent à $k(\rho)$, donc à L et ce pgcd est de degré 1 d'après (I). Donc on a $i \in [1, \nu]$ et $a \in L^\star$, $b \in L$ tels que $ay + b = a(y - y_i)$, d'où $y_i = -b/a \in L$: comme $\mathcal{R} \neq \emptyset$, on a un indice i tel que $y_i \in L$. Le groupe $\mathrm{Gal}(\hat{k}/k)$ agit transitivement sur $\{y_1, \ldots, y_\nu\}$ d'après (40), et il laisse L invariant ; d'où $\{y_1, \ldots, y_\nu\} \subset L$, i.e. $K \subset L$.

b) L'action $\mathrm{Gal}(L/k)$ sur $\mathcal{R}$ est transitive d'après (II). Mais si $\sigma \in \mathrm{Gal}(L/k)$ envoie y_i sur y_j, il est clair que $\sigma(\mathcal{R}_i) = \mathcal{R}_j$, donc $\mathrm{Gal}(L/k)$ permute les $\mathcal{R}_i$ entre eux et les $\mathcal{R}_i$ étant disjoints, nécessairement $\mathrm{Gal}(L/k)$ agit transitivement sur chaque $\mathcal{R}_i$. Donc $(\mathcal{R}_1, \ldots, \mathcal{R}_\nu)$ est bien un système d'imprimitivité du groupe $\mathrm{Gal}(L/k)$. Supposons que $\sigma \in \mathrm{Gal}(L/k)$ vérifie $\sigma(\mathcal{R}_i) = \mathcal{R}_i$, alors d'après (41), on a aussi $\sigma(y_i) = y_i$, i.e. $\sigma \in \mathrm{Gal}(L/K_i)$. Donc $\mathrm{Gal}(L/K_i)$ opère transitivement sur $\mathcal{R}_i$, ce qui prouve que $F(x, y_i)$ est irréductible dans $K_i[x]$. On en déduit aussitôt que $F(x, y)$ est irréductible dans $k[y][x]$, donc aussi dans $k(y)[x]$ d'après le Lemme de Gauss. Puisque $F(x, y_1)$ est séparable, F l'est aussi en tant qu'élément de $k(y)[x]$ d'après le Lemme 3 du §7. Puisque $k[y]$ est intégralement clos, le Théorème 7.2 montre que $\mathrm{Gal}(L_i/K_i)$ s'identifie à un sous-groupe de G, qui est transitif puisque $F(x, y_i)$ est irréductible dans $K_i[x]$. Mais $\mathrm{Gal}(L_i/K_i) \cong \mathrm{Gal}(L/K_i)/\mathrm{Gal}(L/L_i)$.

c) Cette assertion est immédiate.

d) Dans ce cas, pour tout i, $\mathrm{Gal}(L_i/K_i) = \mathrm{Gal}(L_i/K)$ est isomorphe à G à cause du Théorème 7.2, d'où $G \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_i)$. Dans ce cas on a les suites exactes suivantes qui donnent une description partielle de $\mathrm{Gal}(L/k)$ en fonction de G et de $\mathrm{Gal}(K/k)$:

$$(46) \quad 1 \ \to \ \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/k) \to \mathrm{Gal}(K/k) \to 1$$
$$(47) \quad 1 \ \to \ \mathrm{Gal}(L/L_i) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_i/K) \cong G \to 1 \ \ (1 \leq i \leq \nu).$$

lorsque de plus R est normal, les L_i sont tous égaux à L, et alors (47) se réduit à

$$(48) \qquad \mathrm{Gal}(L/K) \cong G \qquad ,$$

autrement dit dans ce dernier cas, $\mathrm{Gal}(L/k)$ est une extension de $\mathrm{Gal}(K/k)$ par G □

Signalons que le Théorème 9.1 admet une réciproque partielle, bien connue (voir par exemple [E. Netto], pages 268-269) :

Théorème 9.2. Soient m et ν des entiers ≥ 2, et soit R un élément de $k[x]$ normalisé et séparable de degré $m\nu$, notons L la k-algèbre des racines de R dans $\hat{k}$ et $\mathcal{R}$ l'ensemble des racines de R dans $\hat{k}$. Supposons R irréductible et qu'il existe un système d'imprimitivité $(\mathcal{R}_1, \ldots, \mathcal{R}_\nu)$ pour l'action de $\mathrm{Gal}(L/k)$ sur $\mathcal{R}$, tel que $\mathrm{card}(\mathcal{R}_i) = m$ pour tout i. Alors il existe $\psi = \prod_{i=1}^{\nu}(y - y_i) \in k[y]$ avec $\{y_1, \ldots, y_\nu\} \subset L$ et $F = x^m - s_1 x^{m-1} + \cdots + (-1)^m s_m \in k[y][x]$ tel que : ψ est irréductible dans $k[y][x]$ et séparable, et $R = \prod_{i=1}^{\nu} F(x, y_i)$, i.e. R est le résultant de F et ψ considérés comme polynômes en y.

Démonstration. (abrégée) Posons $\Phi_i(x) = \prod_{\rho \in \mathcal{R}_i}(x - \rho)$, et soit K_i le corps engendré par k et les coefficients de Φ_i. On a $K_i \subset k(\rho)$ pour tout $\rho \in \mathcal{R}_i$ parce que $(\mathcal{R}_1, \ldots, \mathcal{R}_\nu)$ est un système d'imprimitivité : tout élément $\sigma \in \mathrm{Gal}(L/k)$ tel que $\sigma(\mathcal{R}_i) = \mathcal{R}_i$ appartient à $\mathrm{Gal}(L/K_i)$; on en déduit que Φ_i est le polynôme minimal sur K_i de tout $\rho \in \mathcal{R}_i$. Alors $m\nu = [k(\rho) : k] = [k(\rho) : K_i]\,[K_i : k] = [K_i(\rho) : K_i]\,[K_i : k]$ pour $\rho \in \mathcal{R}_i$, et $[K_i(\rho) : K_i] = m$, d'où $[K_i : k] = \nu$.

Soit y_1 un élément primitif de K_1 sur k, et soit ψ son polynôme minimal sur k ; puisque L est séparable sur k, ψ est séparable. Les k-conjugués de y_1 sont des éléments k-primitifs de $K_1, \ldots, K_\nu$. Soit $\mathcal{C}_i$ l'ensemble $\{\sigma \in \mathrm{Gal}(L/k) \mid \sigma(\mathcal{R}_1) = \mathcal{R}_i\}$: pour tout $\sigma \in \mathcal{C}_i$, $\sigma(y_1)$ a la même valeur, notée y_i. Il est clair que y_i est élément primitif de K_i sur k, et que $\psi(y) = \prod_{i=1}^{\nu}(y - y_i)$ (on notera que ψ est séparable alors même que les K_i ne sont pas nécessairement distincts). Par construction, ψ est irréductible sur k. On a des polynômes $s_1, \ldots, s_m$, éléments de $k[y]$ et de degré $< \nu$, tels que $\Phi_1(x) = x^m - s_1(y_1)x^{m-1} + \cdots + (-1)^m s_m(y_1)$. Posons alors $F(x, y) = x^m - s_1 x^{m-1} + \cdots + (-1)^m s_m$ ($F \in k[y][x]$). On voit aisément que $F(x, y_i) = \Phi_i(x)$ pour $1 \leq i \leq \nu$. Comme Φ_i est séparable et K_i-irréductible, on en déduit comme au Théorème 9.1 que F est séparable et irréductible dans $k(y)[x]$. Comme $R = \prod_{i=1}^{\nu} F(x, y_i)$, on voit bien que R est le résultant de F et ψ □

9.2. Cas de plusieurs paramètres. Le lemme suivant nous sera utile :

Lemme 4. Soient $\alpha, \nu_1, \dots, \nu_d$ des entiers ≥ 1. Soient $\psi_1, \dots, \psi_d$ des éléments de $k[y_1, \dots, y_d]$, de degrés respectifs $\nu_1, \dots, \nu_d$. Notons r_∞ le résultant des polynômes $\mathrm{In}(\psi_1), \dots, \mathrm{In}(\psi_d)$, où $\mathrm{In}(\psi)$ désigne la partie homogène de (ψ)de degré $\deg(\psi)$. Supposons $r_\infty \neq 0$. Désignons par $\mathcal{V}$ la variété de dimension 0 définie par $\psi_1, \dots, \psi_d$ dans $\hat{k}^d$. Supposons que $\mathrm{card}(\mathcal{V}) = \nu_1 \dots \nu_d$ (i.e. que tous les points de $\mathcal{V}$ sont simples). Soit φ un élément de $k[y_1, \dots, y_d]$ qui s'annule sur $\mathcal{V}$ en un et un seul point θ. Alors $\theta \in k^d$.

Démonstration. Soient $z, U_1, \dots, U_d, T$ de nouvelles indéterminées. Posons $\psi_i^\star = z^{\nu_i}\psi_i(\frac{y_1}{z}, \dots, \frac{y_d}{z})$, $\Lambda = \sum_{i=1}^d U_i y_i$ et, pour $\xi = (\xi_1, \dots, \xi_d) \in \hat{k}^d$: $\Lambda(\xi) = \sum_{i=1}^d U_i \xi_i$. Soit $R_\mathcal{V}(T) = \text{Résultant}_{z, y_1, \dots, y_d}(Tz - \sum_{i=1}^d U_i y_i, \psi_1^\star, \dots, \psi_d^\star)$. D'après la formule de Poisson-Perron (cf [J.M. Arnaudiès]), on a :

$$R_\mathcal{V}(T) = r_\infty \prod_{\xi \in \mathcal{V}} (T - \Lambda(\xi)) \qquad ; \tag{49}$$

d'après (49), $R_\mathcal{V}(T)$ est dissocié à facteurs simples dans $\hat{k}(\underline{U})[T]$, où $\underline{U} = (U_1, \dots, U_d)$. De plus, $R_\mathcal{V}(T) \in k(\underline{U})[T]$.

Soit δ le degré de φ ; choisissons un entier $r \geq 1$ tel que $r\nu_1 > \delta$, posons $\Theta = (\psi_1^\star)^r + z^{r\nu_1}\varphi(\frac{y_1}{z}, \dots, \frac{y_d}{z})$; le résultant à l'infini de $\psi_1^r + \varphi, \psi_2, \dots, \psi_d$ est $(r_\infty)^r \neq 0$, donc ces polynômes définissent dans $\hat{k}^d$ une variété de dimension zéro $\mathcal{W}$ et on a des entiers $(l_\xi)_{\xi \in \mathcal{W}}$ non nuls tels que le résultant $R_\mathcal{W}(T)$ des formes $Tz - \sum_{i=1}^d U_i y_i, \Theta, \psi_2^\star, \dots, \psi_d^\star$ de $z, y_1, \dots, y_d$ soit donné par :

$$R_\mathcal{W}(T) = r_\infty \prod_{\xi \in \mathcal{W}} (T - \Lambda(\xi))^{l_\xi} \qquad , \tag{50}$$

de sorte que :

$$\sum_{\xi \in \mathcal{W}} l_\xi = r\nu_1 \dots \nu_d \tag{51}$$

(voir [J.M. Arnaudiès]).

D'après l'hypothèse, le pgcd dans $\hat{k}(\underline{U})[T]$ de $R_\mathcal{V}(T)$ et $R_\mathcal{W}(T)$ est de degré 1 : les pgcd de $R_\mathcal{V}(T)$ et $R_\mathcal{W}(T)$ sont les $\lambda(T - \Lambda(\theta))$, $\lambda \in \hat{k}(\underline{U})$. Mais l'un de ces pgcd appartient à $k(\underline{U})[T]$, puisque $R_\mathcal{V}(T) \in k(\underline{U})[T]$ et $R_\mathcal{W}(T) \in k(\underline{U})[T]$. Donc $\Lambda(\theta) \in k(\underline{U})[T]$, ce qui entraîne immédiatement que $\theta \in k^d$ □

Donnons-nous dans ce qui suit un entier $m \geq 2$, un polynôme $F = F(x, \underline{Y})$:

$$F = x^m - s_1 x^{m-1} + \dots + (-1)^m s_m \in k[\underline{Y}][x] \tag{52}$$

où $\underline{Y} = (Y_1, \dots, Y_d)$, et supposons satisfaistes les conditions ci-après, dans lesquelles $\mathcal{V}$ est définie comme au Lemme 1, sous les mêmes hypothèses mais en supposant de plus $\nu_1\nu_2 \dots \nu_d \geq 2$.

$$k(s_1, \dots, s_m) = k(\underline{Y}) \qquad , \tag{53}$$

et $\forall i \in [1, d], \exists C_i, D_i \in k[z_1, \dots, z_m]$, $\mathcal{V} \cap \mathrm{Z}(D_i) = \emptyset$ (où $\mathrm{Z}(D_i)$ est l'ensemble des zéros de D_i) et que $Y_i = \frac{C_i(s_1,\dots,s_m)}{D_i(s_1,\dots,s_m)}$;

$$\mathcal{V} \text{ est } k\text{-irréductible ;} \tag{54}$$

(55) le pgcd dans $k[x]$ des coefficients de F ordonné en les y_i est égal à 1.

Il est clair que le terme constant de F ordonné en les Y_i est $x^m - s_1(0)x^{m-1} + \dots + (-1)^m s_m(0)$, les autres termes ayant des coefficients de degré $< m$ en x.

Donc le résultant R de $F^\star = z^\mu F(x, \frac{Y_1}{z}, \dots, \frac{Y_d}{z})$ (où $\mu = \deg_{\underline{Y}}(F)$) et de $\psi_1^\star, \dots, \psi_d^\star$, considérés comme polynôme homogènes de $Y_1, \dots, Y_d, z$, est un polynôme en x de degré $m\nu_1\nu_2 \dots \nu_d$, de monôme dominant $(-1)^{\mu\nu_1\nu_2\dots\nu_d} x^{m\nu_1\nu_2\dots\nu_d}$. Nous supposerons que

$$R \quad (= R(x) \in k[x]) \text{ est séparable.} \tag{56}$$

On désignera par L le corps des racines de R sur k dans $\hat{k}$, et par K le corps engendré par k et les coordonnées des points de $\mathcal{V}$. D'après les hypothèses, K et L sont des extensions galoisiennes de k (pour K, cela provient de ce que $\mathrm{card}(\mathcal{V}) = \nu_1 \dots \nu_d$). On notera $\mathcal{R}$ l'ensemble des racines de R dans $\hat{k}$, et, pour $\xi \in \mathcal{V}$, on notera $\mathcal{R}_\xi$ l'ensemble des racines de $F(x, \xi)$ dans $\hat{k}$, de sorte que $\mathcal{R}$ est union disjointe des $\mathcal{R}_\xi$. En effet d'après la formule Poisson-Perron

$$R = (r_\infty)^\mu \prod_{\xi \in \mathcal{V}} F(x, \xi) \qquad ; \tag{57}$$

enfin on désigne par K_ξ le corps engendré par k et les coordonnées de ξ ($\xi \in \mathcal{V}$), et par L_ξ le corps des racines de $F(x, \xi)$ sur K_ξ dans $\hat{k}$; il est clair, à cause des hypothèses, que L_ξ est une extension galoisienne de K_ξ. On considère maintenant les conditions suivantes :

(V) Pour tout $\rho \in \mathcal{R}$, $F(\rho, \underline{Y})$ s'annule en un et un seul point de $\mathcal{V}$;
(VI) R est irréductible dans $k[x]$;
(VII) F est un polynôme de x normal sur $k(\underline{Y})$;
(VIII) $[K : k] = \nu_1 \dots \nu_d$.

Théorème 9.3. Soient $F, \psi_1, \dots, \psi_d$ vérifiant les conditions (52) à (56).

a) Si la condition (V) est satisfaite, on a $K \subset L$.
b) Si les conditions (V) à (VI) sont satisfaites, alors : F est irréductible et séparable sur $k(\underline{Y})$; $F(x,\xi)$ est irréductible dans $K_\xi[x]$, et $(\mathcal{R}_\xi)_{\xi\in\mathcal{V}}$ est un système d'imprimitivité pour l'action de $\mathrm{Gal}(L/k)$ sur $\mathcal{R}$. Notons dans ce cas G le groupe de Galois de F sur $k(\underline{Y})$. Alors pour tout $\xi \in \mathcal{V}$, il y a un quotient de K_ξ isomorphe à un sous-groupe de G transitif sur les racines de F en x dans $\widehat{k(\underline{Y})}$.
c) Si les conditions (V),(VI) et (VIII) sont satisfaites, les K_ξ sont égaux à K, et 57 est une décomposition de R en facteurs irréductibles dans $K[x]$.
d) Si les conditions (V) à (VIII) sont satisfaites, il y a un quotient de $\mathrm{Gal}(L/K)$ isomorphe à G, et si de plus R est normal, alors $\mathrm{Gal}(L/K) \cong G$.

Démonstration. D'après (56) et (57), chaque polynôme $F(x,\xi)$ ($\xi \in \mathcal{V}$) est séparable, $\mathrm{card}(\mathcal{R}) = m\nu_1 \dots \nu_d$, $\mathrm{card}(R_\xi) = m$ pour tout $\xi \in \mathcal{V}$.

a) Fixons $\rho \in \mathcal{R}$. On a $F(\rho,\underline{Y}) \neq 0$ d'après (55), et d'après (V), $F(\rho,\underline{Y})$ est non constant. Toujours à cause de (V), en appliquant le Lemme 4, on voit qu'il existe $\xi \in \mathcal{V}$ tel que les coordonnées de ξ appartiennent à $k(\rho)$, donc aussi à L. Mais $\mathrm{Gal}(\hat{k}/k)$ laisse L invariant, et agit transitivement sur $\mathcal{V}$ par suite de (54), donc tout point $\xi \in \mathcal{V}$ a toutes ses coordonnées dans L. D'où $K \subset L$.

b) D'après (VI), l'action de $\mathrm{Gal}(L/k)$ sur $\mathcal{R}$ est transitive. Si $\sigma \in \mathrm{Gal}(L/k)$ envoie ξ sur η, il est clair que $\sigma(\mathcal{R}_\xi) = \mathcal{R}_\eta$. Donc $\mathrm{Gal}(L/k)$ permute entre eux les $\mathcal{R}_\xi$, donc son action sur chaque $\mathcal{R}_\xi$ est nécessairement transitive. Ainsi $(\mathcal{R}_\xi)_{\xi\in\mathcal{V}}$ est bien un système d'imprimitivité de $\mathrm{Gal}(L/k)$. Si $\sigma \in \mathrm{Gal}(L/k)$ vérifie $\sigma(\mathcal{R}_\xi) = \mathcal{R}_\xi$, alors d'après (53) $\sigma(\xi) = \xi$, donc $\sigma \in \mathrm{Gal}(L/K_\xi)$. Donc $\mathrm{Gal}(L/K_\xi)$ opére transitivement sur $\mathcal{R}_\xi$, donc $F(x,\xi)$ est irréductible dans $K_\xi[x]$.

Il s'ensuit que $F(x,\underline{Y})$ est irréductible dans $k[\underline{Y}][x]$, donc aussi dans $k(\underline{Y})[x]$ d'après le Lemme de Gauss. La séparabilité de F dans $k(\underline{Y})[x]$ se déduit du Lemme 3 du §7. Comme $k(\underline{Y})$ est intégralement clos, d'après le Théorème 7.2, le groupe $\mathrm{Gal}(L_\xi/K_\xi)$ s'identifie à un sous-groupe de G, nécessairement transitif puisque les $F(x,\xi)$ sont irréductibles dans $K_\xi[x]$. De plus, on a bien toutes les assertions de b) puisque $\mathrm{Gal}(L_\xi/K_\xi) \cong \mathrm{Gal}(L/K_\xi)/\mathrm{Gal}(L/L_\xi)$.

c) Cette assertion est immédiate, compte tenu de ce que $[K_\xi : k] = \nu_1 \dots \nu_d$ pour tout $\xi \in \mathcal{V}$.

d) Ici, d'après le Théorème 7.2, $\mathrm{Gal}(L_\xi/K_\xi)$ ($= \mathrm{Gal}(L_\xi/K)$) est isomorphe à G, d'où $G \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_\xi)$. On a alors une description partielle de $\mathrm{Gal}(L/K)$ en fonction de G et $\mathrm{Gal}(K/k)$ à l'aide des suites exactes ci-après :

$$1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/k) \to \mathrm{Gal}(K/k) \to 1 \tag{58}$$

$$1 \to \mathrm{Gal}(L/L_\xi) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_\xi/K) \cong G \to 1 \tag{59}$$

où $\xi \in \mathcal{V}$. Lorsque de plus R est normal, les L_ξ sont tous égaux à L, et alors (59) se réduit à

$$\mathrm{Gal}(L/K) \cong G \quad \square \tag{60}$$

10. Résolvantes et Résultant

Nous reprenons ici les notations et hypothèses des §§4 et 5. En particulier, le corps k sera supposé de caractéristique 0. L'idéal de $\mathcal{A}$ engendré par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n\}$ est noté $\mathfrak{I}$, et $\mathcal{W}$ est la variété de dimension 0 définie par $\mathfrak{I}$ dans $\hat{k}^n$. On a vu au §5 que $\mathfrak{I} = \sqrt{\mathfrak{I}}$, et $\mathcal{W} = \{(\rho_{s(1)}, \dots, \rho_{s(n)})\}_{s \in \mathfrak{S}_n}$.

Les composantes k-irréductibles de $\mathcal{W}$ sont les $\mathcal{T}_C = \{(\rho_{s(1)}, \dots, \rho_{s(n)})\}_{s \in C}$, où C parcourt l'ensemble $\mathcal{H}$ des classes à droite de $\mathfrak{S}_n$ mod Γ ($\Gamma = \mathrm{Gal}(E/k)$).

Soit maintenant Θ un résolvant d'un sous-groupe H de $\mathfrak{S}_n$ ($\Theta \in \mathcal{A}$). Posons $e = [\mathfrak{S}_n : H]$; et $h = n!/e = \mathrm{card}(H)$. Nous supposerons Θ non constant, de degré d. Le résultant de $(\sigma_1, \dots, \sigma_n)$ (considérés comme polynômes homogènes en $(x_1, \dots, x_n)$) est 1. Soit z une variable d'homogénéisation. Posons :

$$\Theta_\clubsuit = z^d \Theta\left(\frac{x_1}{z}, \dots, \frac{x_n}{z}\right) ; \; F_i = \sigma_i - c_i z^i \qquad .$$

Soit μ_i l'endomorphisme de k-espace vectoriel $\mathcal{A}/\mathfrak{I}$ induit par la multiplication par x_i. D'après ce qui précède, le Théorème I.3.1 de [J.M. Arnaudiès] s'applique ici et donne le polynôme caractéristique $\chi_{\Theta(\mu_1, \dots, \mu_n)}(x)$ de $\Theta(\mu_1, \dots, \mu_n)$:

$$\chi_{\Theta(\mu_1, \dots, \mu_n)}(x) = \text{Résultant}(F_1, \dots, F_n, xz^d - \Theta_\clubsuit) \qquad , \tag{61}$$

le résultant étant entendu comme résultant de polynômes homogènes en $(x_1, \dots, x_n, z)$. Le Théorème I.3.3 de [J.M. Arnaudiès] donne alors immédiatement :

$$\chi_{\Theta(\mu_1, \dots, \mu_n)}(x) = \prod_{\xi \in \mathcal{W}} (x - \Theta(\xi)) \qquad ; \tag{62}$$

Ci-dessous nous allons calculer $\chi_{\Theta(\mu_1, \dots, \mu_n)}$ de deux manières. La première avec $(\mathfrak{S}_n/H)_g$ et la seconde avec $(\mathfrak{S}_n/\Gamma)_g$. Ce qui nous permettra d'aboutir au Théorème 10.4.

Soit $(\mathfrak{S}_n/H)_g = \{C_1, \dots C_e\}$, avec $C_1 = H$, et soit Θ_i la valeur constante de $\Theta(x_{s(1)}, \dots, x_{s(n)})$ pour $s \in C_i$ (donc $\Theta_1 = \Theta$). Notons $g \mapsto \tilde{g}$ le morphisme de spécialisation $\mathcal{A} \to \hat{k}$, $g \mapsto g(\rho_1, \dots, \rho_n)$. Par définition de la résolvante de Lagrange on a:

$$\mathcal{L}_\Theta(x) = \prod_{i=1}^{e} (x - \Theta_i) \qquad . \tag{63}$$

On en déduit :

Théorème 10.1. On a :

$$\chi_{\Theta(\mu_1,\dots,\mu_n)}(x) = \text{Résultant}(F_1,\dots,F_n,xz^d-\Theta_{\clubsuit}) = (\mathcal{L}_{\Theta,f}(x))^h \qquad . \tag{64}$$

Démonstration. D'après (61) et (62) :

$$\begin{aligned}\chi_{\Theta(\mu_1,\dots,\mu_n)}(x) &= \text{Résultant}(F_1,\dots,F_n,xz^d-\Theta_{\clubsuit}) = \prod_{\tau\in\mathfrak{S}_n}(x-\Theta(\rho_{\tau(1)},\dots,\rho_{\tau(n)}))\\ &= \prod_{i=1}^{e}(\prod_{\tau\in C_i}(x-\Theta(\rho_{\tau(1)},\dots,\rho_{\tau(n)})) = \prod_{i=1}^{e}(x-\widetilde{\Theta_i})^h\\ &= (\prod_{i=1}^{e}(x-\widetilde{\Theta_i}))^h = (\mathcal{L}_{\Theta,f})^h \qquad ,\end{aligned}$$

car par définition $\mathcal{L}_{\Theta,f} = \prod_{i=1}^{e}(x-\widetilde{\Theta_i})$. On peut également le démontrer ainsi : comme $\mathcal{L}_{\Theta,f}(x)$ est le polynôme minimal de Θ sur $\mathcal{K}$ on a immédiatement l'égalité $\chi_{\Theta(\mu_1,\dots,\mu_n)}(x) = (-1)^{n!}(\mathcal{L}_{\Theta,f}(x))^h$. □

Les endomorphismes $\{g(\mu_1,\dots,\mu_n)\}_{g\in\mathcal{A}}$ du k-espace vectoriel $\mathcal{A}/\mathfrak{I}$ sont deux à deux permutables, et tous semi-simples puisque $\mathfrak{I} = \sqrt{\mathfrak{I}}$ (cf. Proposition II.5.3 de [J.M. Arnaudiès]). Posons $m = [\mathfrak{S}_n : \Gamma]$, $N = \text{card}(\Gamma)$, et soit $\{\tau_i\}_{1\le i\le m}$ une transversale droite de $\mathfrak{S}_n$ mod Γ. Notons $\mathfrak{M}_i$ l'idéal maximal $\{g\in\mathcal{A} \mid \widetilde{\tau_i g} = 0\}$ de $\mathcal{A}$, E_i le corps $\mathcal{A}/\mathfrak{M}_i$, avec τ_1 =Id. On écrira $\mathfrak{N} = \mathfrak{M}_1$. La projection $p_i : \mathcal{A}\to E$, $g\mapsto\widetilde{\tau_i g}$ définit par passage au quotient un k-isomorphisme de E_i sur E, avec lequel on identifiera E_i et E ; la collection des p_i définit alors par passage au quotient un isomorphisme π de k-algèbre entre $\mathcal{A}/\mathfrak{I}$ et $\prod_{i=1}^{m}E_i = E^m$. Il est clair que pour tous i et j, le j-ième facteur E_j de $\mathcal{A}/\mathfrak{I}$, (identifié à E^m au moyen de π) est μ_i-stable, et que $\mu_{i||_{E_j}}$ est la multiplication par $\widetilde{\tau_j x_i} = \rho_{\tau_j(i)}$ dans E. Donc pour tout $g\in\mathcal{A}$, E_j est $g(\mu_1,\dots,\mu_n)$-stable, et $g(\mu_1,\dots,\mu_n)_{||_{E_j}}$ est la multiplication par $\widetilde{\tau_j g} = g(\rho_{\tau_j(1)},\dots,\rho_{\tau_j(n)})$ dans E.

Théorème 10.2. Les notations et hypothèses étant celles du Théorème 10.1, posons $[\Theta] = \Theta(\mu_1,\dots,\mu_n)$, $[\Theta]_i = [\Theta]_{||_{E_i}}$, $\theta_i = \widetilde{\tau_i\Theta}$; notons P_i le polynôme k-minimal de $[\Theta]_i$ et $d_i = \deg(P_i)$ (d'où d_i divise N). Alors pour tout i, $1\le i\le m$:

$$\chi_{[\Theta]}(x) = \prod_{\sigma\in\Gamma}(x-\sigma(\theta_i)) = P_i(x)^{N/d_i} \qquad . \tag{65}$$

Démonstration. C'est une conséquence immédiate du fait que $[\Theta]_i$ est la multiplication par θ_i dans $E = E_i$ □

On obtient ainsi la relation cherchée:

$$(\mathcal{L}_{\Theta,f}(x))^h = \prod_{i=1}^{n}P_i(x)^{N/d_i} \qquad , \tag{66}$$

et une autre formulation de la résolvante de Lagrange :

Corollaire 10.3. Dans les conditions du Théorème 10.2, le polynôme minimal de $[\Theta] = \Theta(\mu_1, \dots, \mu_n)$ est $\mathrm{ppcm}(P_1(x), \dots, P_m(x)) = \mathcal{L}_{\Theta,f}(x)$.

Remarque 13. Soit $\hat{\mathcal{A}} = \hat{k} \bigotimes_k \mathcal{A}$ $(= \hat{k}[x_1, \dots, x_n])$, $\hat{\mathfrak{I}} = \hat{k} \bigotimes_k \mathfrak{I}$, $\hat{\mathfrak{M}}_i = \hat{k} \bigotimes_k \mathfrak{M}_i$. On a $\hat{k} \bigotimes_k \mathcal{A}/\mathfrak{I} = \hat{\mathcal{A}}/\hat{\mathfrak{I}}$; $\hat{\mathfrak{M}}_i$ est l'idéal maximal de $\hat{\mathcal{A}}$ défini par $(\rho_{\tau_i(1)}, \dots, \rho_{\tau_i(n)})$, et $\hat{\mathfrak{I}} = \bigcap_{i=1}^m \hat{\mathfrak{M}}_i$. Posant $\hat{E}_i = \hat{k} \bigotimes_k E_i = \hat{k} \bigotimes_k E$, (noté aussi $\hat{E}$), on a $\hat{\mathcal{A}}/\hat{\mathfrak{I}} \cong \hat{E}^m$. Notons $\widehat{[\Theta]}$ l'endomorphisme de $\hat{k}$-espace vectoriel de $\hat{\mathcal{A}}/\hat{\mathfrak{I}}$ qui prolonge $[\Theta]$, définissons de même $\widehat{[\Theta]}_i$, alors $\widehat{[\Theta]}_i = \widehat{[\Theta]}_{||_{\hat{E}_i}}$ (ce qui a un sens car $\hat{E}_i$ est $\widehat{[\Theta]}$-stable). Puisque $[\Theta]$ est semi-simple et k est de caractéristique nulle, $\widehat{[\Theta]}$, et donc les $\widehat{[\Theta]}_i$, sont diagonalisables. Il est aisé de définir une base de vecteurs propres de chaque $\widehat{[\Theta]}_i$ dans $\hat{E}_i$: en fait, soit $P_\tau \in \hat{k}[x_1, \dots, x_n]$ vérifiant, pour $\tau \in \mathfrak{S}_n$, les relations $P_\tau(\rho_{\tau(1)}, \dots, \rho_{\tau(n)}) = 1$ et $P_\tau(\rho_{\tau'(1)}, \dots, \rho_{\tau'(n)}) = 0$ si $\tau' \in \mathfrak{S}_n$, $\tau' \neq \tau$. Soit V_τ l'image naturelle de P_τ dans $\hat{\mathcal{A}}/\hat{\mathfrak{I}}$. Alors $(V_\tau)_{\tau \in \mathfrak{S}_n}$ est une base de vecteurs propres de $\widehat{[\Theta]}$ dans $\hat{\mathcal{A}}/\hat{\mathfrak{I}}$, car $\widehat{[\Theta]}(V_\tau) = \widetilde{\tau.\Theta}.V_\tau$ pour $\tau \in \mathfrak{S}_n$. Pour i fixé, $1 \leq i \leq m$, $V_{\sigma\tau_i} \in \hat{E}_i$ pour tout $\sigma \in \Gamma$, car $\tau_j P_{\sigma\tau_i} = 0$ pour $j \neq i$ et $\sigma \in \Gamma$. Donc $(V_{\sigma\tau_i})_{\sigma\in\Gamma}$ est une base de vecteurs propres de $\widehat{[\Theta]}_i$ dans E_i, la valeur propre associée à $V_{\sigma\tau_i}$ étant $\widetilde{\sigma\tau_i\Theta} = \sigma(\widetilde{\tau_i\Theta}) = \sigma(\theta_i)$, la dernière égalité étant due au fait que $\sigma \in \Gamma$. On retrouve ainsi la relation (65).

Théorème 10.4. Les notations et hypothèses étant celles des Théorèmes 10.1 et 10.2, soit λ une racine de la résolvante $\mathcal{L}_{\Theta,f}(x)$ dans E, de multiplicité ν. Soit J la partie de $\{1, \dots, e\}$ telle que $j \in J \Leftrightarrow \widetilde{\Theta_j} = \lambda$ (donc $\mathrm{card}(J) = \nu$). Soit L le stabilisateur de $\{\Theta_j\}_{j\in J}$ dans $\mathfrak{S}_n$. Alors $\nu h = 0 \bmod \mathrm{card}(\Gamma \cap L)$.

Démonstration. On a une représentation par permutations $\mathfrak{S}_n \to \mathfrak{S}_e$, $\tau \mapsto \psi_\tau$ telle que $\tau.\Theta_j = \Theta_{\psi_\tau(j)}$ pour tout $\tau \in \mathfrak{S}_n$ et tout $j \in [1, e]$. (cette représentation est transitive, et lorsque $n \geq 5$ et $e \geq 3$ elle est fidèle, d'où alors $e \geq n$). La multiplicité de λ dans $\chi_{[\Theta]_i}(x)$ (où $i \in [1, m]$ est fixé) est, en vertu de (65), le nombre ν_i des $\sigma \in \Gamma$ tels que $\sigma(\theta_i) = \lambda$, ce qui s'écrit : $\sigma(\widetilde{\tau_i\Theta}) = \lambda$, ou encore (du fait que $\sigma \in \Gamma$) $\widetilde{\sigma\tau_i\Theta} = \lambda$, i.e. $\sigma\tau_i\Theta \in \{\Theta_j\}_{j\in J}$. Soit $\mathcal{N}_i$ l'ensemble des $\sigma \in \Gamma$ vérifiant cette relation. On a : $\mathcal{N}_i = \{\sigma \in \Gamma \mid \psi_{\sigma\tau_i}(1) \in J\} = \{\sigma \in \Gamma \mid \psi_\sigma(l_i) \in J\}$, avec $l_i = \psi_{\tau_i}(1)$. Si $\mathcal{N}_i$ est non vide, soit $\sigma_0 \in \mathcal{N}_i$. Posons $l_i' = \psi_{\sigma_0}(l_i)$. Alors $l_i' \in J$ et $\sigma \in \mathcal{N}_i$ ssi $\psi_{\sigma\sigma_0^{-1}}(l_i') \in J$; si $\sigma\sigma_0^{-1} \in L$, il est clair que $\sigma \in \mathcal{N}_i$. Inversement, si $\sigma \in \mathcal{N}_i$, posant $\tau = \sigma\sigma_0^{-1}$, on a $\tau\Theta_{l_i'} = \Theta_{l_i''}$ avec $l_i'' \in J$ donc $\widetilde{\tau\Theta_{l_i'}} = \widetilde{\tau\Theta_{l_i''}} = \lambda$ et comme par ailleurs $\widetilde{\tau\Theta_{l_i'}} = \tau(\widetilde{\Theta_{l_i'}}) = \tau(\lambda)$ (car $\tau \in \Gamma$), on prouve ainsi que $\tau(\lambda) = \lambda$ et donc pour tout $l \in J$, $\widetilde{\tau.\Theta_l} = \tau(\widetilde{\Theta_l}) = \tau(\lambda) = \lambda$, d'où $\tau\Theta_l \in \{\Theta_j\}_{j\in J}$, et donc $\tau \in L$. On en déduit de là que $\mathcal{N}_i = (\Gamma \cap L)\sigma_0$, c'est-à-dire que $\mathcal{N}_i$ est une classe à droite de $\Gamma \bmod \Gamma \cap L$, d'où $\mathrm{card}(\mathcal{N}_i) = \mathrm{card}(\Gamma \cap L)$.

Soit $\mathcal{E}_\lambda$ l'ensemble des $i \in [1, m]$ tels que $\mathcal{N}_i \neq \emptyset$ et soit $\alpha_\lambda = \mathrm{card}(\mathcal{E}_\lambda)$. D'après (65), en tenant compte que $\chi_{[\Theta]}(x) = \prod_{i=1}^m \chi_{[\Theta]_i}(x)$, la multiplicité de λ dans $\chi_{[}\Theta](x)$ est $\alpha_\lambda \mathrm{card}(\Gamma \cap L)$. Mais d'après (64), cette multiplicité est aussi νh, d'où l'équation :

$$\nu h = \alpha_\lambda \mathrm{card}(\Gamma \cap L) \qquad , \tag{67}$$

ce qui achève la démonstration □

Corollaire 10.5. Si $\lambda \in k$, alors $N = \mathrm{card}(\Gamma)$ divise νh. En particulier, si $\Gamma \subset H$, alors N divise νh.

Démonstration. On a $\lambda \in k$ ssi $\mathrm{card}(\Gamma \cap L) = N$, c'est-à-dire ssi $\Gamma \subset L$; l'assertion 1 découle alors de (67). La deuxième assertion s'en déduit à l'aide du Théorème 5.2 a) □

(Ce corollaire est latent dans [J.L. Lagrange, tome IV], (Traité des équations algébriques), bien entendu sans preuve aucune, et surtout sans langage de théorie des groupes pour l'exprimer commodément.)

Une autre conséquence de Théorème 10.4 et de sa preuve est la formule :

$$[k(\lambda) : k] = [\Gamma : \Gamma \cap L] \tag{68}$$

(qui se déduisait aussi de l'étude du Théorème 6.3).

Résolvants et résolvantes de Galois

Un résolvant $\Theta \in \mathcal{A}$ du sous-groupe $\{\mathrm{Id}\}$ de $\mathfrak{S}_n$ sera appelé un résolvant de (Lagrange-)Galois, la résolvante $\mathcal{L}_\Theta(x)$ correspondante sera appelé une *résolvante de Galois* en degré n. Pour tout n-uple $\mu = (u_1, \ldots, u_n) \in k^n$ d'éléments tous distincts, la forme linéaire $\sum_{i=1}^n u_i x_i = \Lambda_u$ est un résolvant de Galois. Les formules (64) se réduisent alors à :

$$\chi_{\sum_{i=1}^n u_i \mu_i}(x) = \mathrm{Résultant}(F_1, \ldots, F_n, xz - \Lambda_u) = \mathcal{L}_{\Lambda_u}(x) \qquad . \tag{69}$$

D'après le corollaire du Théorème 10.4, si λ est une racine dans k de la résolvante de Galois $\mathcal{L}_{\Lambda_u, f}(x)$, alors la multiplicité ν de λ dans cette résolvante est un multiple de $N = \mathrm{card}(\Gamma)$.

Si l'on connait un résolvant de Galois Λ_u qui soit f-séparable, alors le calcul d'une résolvante arbitraire se ramène au calcul du résultant de deux polynômes d'une variable ; en effet, soit Θ un résolvant d'un groupe H ($\Theta \in \mathcal{A}$). Par la méthode du Théorème 4.3 appliquée à $\Theta \in \mathcal{A}_H \subset \mathcal{A}$, on peut théoriquement déterminer $\Phi \in \mathcal{S}[x]$ tel que $\Theta = \frac{1}{\Delta}\Phi(\Lambda_u)$, où Δ est le discriminant de $\mathcal{L}_{\Lambda_u}(x)$. Soit $\varphi \in k[x]$ obtenu en spécialisant $(\sigma_1, \ldots, \sigma_n)$ en $(c_1, \ldots, c_n)$ dans les coefficients de Φ. On a (puisque $\tilde{\Delta} \neq 0$) :

$$
\begin{aligned}
(\mathcal{L}_{\Theta,f})^h &= \prod_{\tau\in\mathfrak{S}_n}(x-\frac{1}{\tilde{\Delta}}\varphi(\widetilde{\tau\Lambda_u})) \qquad \text{, tandis que :}\\
\mathcal{L}_{\Lambda_u,f}(x) &= \prod_{\tau\in\mathfrak{S}_n}(x-\widetilde{\tau\Lambda_u}) \qquad \text{, ce qui prouve que :}\\
(\mathcal{L}_{\Theta,f})^h &= \text{Résultant}_T(x-\frac{1}{\tilde{\Delta}}\varphi(T),\mathcal{L}_{\Lambda_u,f}(T)) \qquad , \qquad (70)
\end{aligned}
$$

l'indice T signifiant que le résultant considéré est celui qui élimine T.

Plus généralement, soient Θ_1 et Θ_2 des résolvants respectifs de deux groupes H_1 et H_2 de $\mathfrak{S}_n$ tels que $H_1\subset H_2$; posons $\nu=[H_2:H_1]$, et supposons que Θ_1 soit f-séparable. Notons Δ_1 le discriminant de $\mathcal{L}_{\Theta_1}$ (donc $\widetilde{\Delta_1}\neq 0$). On a $\Phi\in\mathcal{S}[x]$ tel que $\Theta_2=\frac{1}{\Delta_1}\Phi(\Theta_1)$, car $\Theta_2\in\mathcal{A}_{H_2}\subset\mathcal{A}_{H_1}\subset\frac{1}{\Delta_1}\mathcal{S}[\Theta_1]$. Soit $\varphi\in k[x]$ obtenu en spécialisant $(\sigma_1,\dots,\sigma_n)$ en $(c_1,\dots,c_n)$ dans les coefficients de Φ. Soit $\mathcal{T}_i$ une transversale gauche de $\mathfrak{S}_n$ sur H_i ($i\in\{1,2\}$). Puisque $\text{card}(\mathcal{T}_1)=\text{card}(\mathcal{T}_2)\times[H_2:H_1]$, on a pour $i\in\{1,2\}$:

$$
\begin{aligned}
\mathcal{L}_{\Theta_i,f}(x) &= \prod_{\tau\in\mathcal{T}_i}(x-\widetilde{\tau\Theta_i}) \qquad \text{et :}\\
(\mathcal{L}_{\Theta_2,f}(x))^\nu &= \prod_{\tau\in\mathcal{T}_1}(x-\widetilde{\tau\Theta_2})\prod_{\tau\in\mathcal{T}_1}(x-\frac{1}{\widetilde{\Delta_1}}\varphi(\widetilde{\tau\Theta_1}))\\
&= \text{Résultant}_T(x-\frac{1}{\tilde{\Delta}_1}\varphi(T),\mathcal{L}_{\Theta_1,f}(T)) \qquad ,
\end{aligned}
$$

ces relations étant dues au fait que pour tout $\tau\in\mathfrak{S}_n$, $\tau\Theta_2=\frac{1}{\Delta_1}\Phi(\tau.\Theta_1)$, d'où $\widetilde{\tau.\Theta_2}=\frac{1}{\tilde{\Delta}_1}\widetilde{\Phi(\tau.\Theta_1)}=\frac{1}{\tilde{\Delta}_1}\varphi(\widetilde{\tau\Theta_1})$. En résumé :

$$
(\mathcal{L}_{\Theta_2,f}(x))^\nu=\text{Résultant}_T(x-\frac{1}{\tilde{\Delta}_1}\varphi(T),\mathcal{L}_{\Theta_1,f}(T)) \qquad . \qquad (71)
$$

Ceci permet, connaissant $\mathcal{L}_{\Theta_1,f}$, de ramener le calcul des $\mathcal{L}_{\Theta_2,f}$ pour $H_1\subset H_2$ à un simple calcul de résultant de deux polynômes à une variable.

Lien entre résolvante f-séparable et résolvante générale d'un même groupe H

Reprenons les hypothèses et notations générales du Théorème 10.4. Pour simplifier les notations, nous supposerons que $\lambda=\tilde{\Theta}$ $(=\widetilde{\Theta}_1)$ et que $J=[1,\nu]$. [1]

Dans ses réflexions sur la résolution des équations algébriques, art. 103, tome IV, pour étudier la racine multiple λ de $\mathcal{L}_{\Theta,f}$ (dans le cas $\nu>1$), Lagrange a proposé d'introduire un résolvant f-séparable Ψ du même groupe, et de comparer

[1] Si $\lambda=\Theta_{j_0}$, il faut remplacer le résolvant Θ par Θ_{j_0} et donc le groupe H par le groupe $\text{Stab}_{\mathfrak{S}_n}(\Theta_{j_0})$, qui est un de ses conjugués dans $\mathfrak{S}_n$.

$\mathcal{L}_{\Theta,f}$ et $\mathcal{L}_{\Psi,f}$. (il ne conclut pas nettement faute de langages appropriés de théorie des corps et de théorie des groupes.) Soit donc Ψ un résolvant f-séparable de H, notons $\mathcal{L}_\Psi(x) = \prod_{i=1}^{e}(x - \Psi_i)$, la numérotation des Ψ_i étant choisie pour que $\mathrm{Stab}_{\mathfrak{S}_n}(\Psi_i) = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta_i)$ pour tout i, $1 \leq i \leq e$ (on aura donc $\Psi_1 = \Psi$).

Il résulte maintenant du Théorème 6.3 (ou de la démonstration du Théorème 10.4) que $\mathrm{Stab}_\Gamma(\lambda) = \Gamma \cap L$. L'action de $\mathfrak{S}_n$ sur $\{\Theta_1, \ldots, \Theta_e\}$, tout comme celle de $\mathfrak{S}_n$ sur $\{\Psi_1, \ldots, \Psi_e\}$, s'identifie à l'action par translations à gauche de $\mathfrak{S}_n$ sur l'ensemble $\{C_1, \ldots, C_e\}$ des classes à gauche de $\mathfrak{S}_n$ mod H, numérotées de façon que $C_i = \{\sigma \in \mathfrak{S}_n \mid \sigma.\Theta = \Theta_i\}$ (et donc aussi $C_i = \{\sigma \in \mathfrak{S}_n \mid \sigma.\Psi = \Psi_i\}$). On en déduit que L, qui est par définition le stabilisateur de $\{\Theta_1, \ldots, \Theta_\nu\}$ dans $\mathfrak{S}_n$, est aussi celui de $\{\Psi_1, \ldots, \Psi_\nu\}$.

Soit Φ un polynôme symétrique en ν variables à coefficients dans k. Pour tout élément $\sigma \in \Gamma \cap L$, on a : $\sigma(\Phi(\widetilde{\Psi_1}, \ldots, \widetilde{\Psi_\nu})) = \Phi(\sigma(\widetilde{\Psi_1}), \ldots, \sigma(\widetilde{\Psi_\nu})) = \Phi(\widetilde{\sigma.\Psi_1}, \ldots, \widetilde{\sigma.\Psi_\nu})$ du fait que $\sigma \in \Gamma$, et donc pour τ_σ un certain élément de $\mathfrak{S}_\nu$ on a : $\sigma(\Phi(\widetilde{\Psi_1}, \ldots, \widetilde{\Psi_\nu})) = \Phi(\widetilde{\Psi_{\tau_\sigma(1)}}, \ldots, \widetilde{\Psi_{\tau_\sigma(\nu)}}) = \Phi(\widetilde{\Psi_1}, \ldots, \widetilde{\Psi_\nu})$ puisque Φ est symétrique. Par suite,

$$\Phi(\widetilde{\Psi_1}, \ldots, \widetilde{\Psi_\nu}) \in \mathrm{Inv}_E(\Gamma \cap L) = k(\lambda) \qquad . \tag{72}$$

Une conséquence évidente des relations (72) est le théorème suivant, affirmé par Lagrange dans la référence citée, mais sans véritable justification :

Théorème 10.6. Dans les conditions ci-dessus, on a :

$$(x - \widetilde{\Psi_1}) \cdots (x - \widetilde{\Psi_\nu}) \in k(\lambda)[x] \qquad .$$

Remarque 14. Notons $Q(x) = (x - \widetilde{\Psi_1}) \cdots (x - \widetilde{\Psi_\nu})$. En général, Q n'est pas irréductible dans $k(\lambda)[x]$. Les facteurs irréductibles sur $k(\lambda)$ de Q correspondent aux $\Gamma \cap L$-orbites de $\{\Theta_1, \ldots, \Theta_\nu\}$. En particulier, soit J la partie de $[1, \nu]$ telle que la $\Gamma \cap L$-orbite de Θ soit $\{\Theta_j\}_{j \in J}$. On a $\mathrm{card}(J) = [\Gamma \cap L : \Gamma \cap H]$, et le polynôme minimal de $\widetilde{\Psi_1}$ sur $k(\lambda)$ est évidemment $\prod_{j \in J}(x - \widetilde{\Psi_j})$. Dans l'article de Lagrange sus-cité, c'est le polynôme que Lagrange cherchait à concevoir.

Notons Δ le discriminant de $\mathcal{L}_\Psi(x)$. On a un polynôme $\mathcal{M} \in \mathcal{S}[x]$ tel que $\Theta = \frac{1}{\Delta}\mathcal{M}(\Psi)$ (voir §6). D'où, pour tout i $(1 \leq i \leq e)$:

$$\Theta_i = \frac{1}{\Delta}\mathcal{M}(\Psi_i) \qquad . \tag{73}$$

Puisque $\tilde{\Delta} \neq 0$, on peut spécialiser la relation (73), ce qui donne :

$$\theta_i = \frac{1}{\tilde{\Delta}}M(\widetilde{\Psi_i}) \qquad .$$

(où M se déduit de $\mathcal{M}$ en y remplaçant $(\sigma_1, \dots, \sigma_n)$ par $(c_1, \dots, c_n)$ dans les coefficients). En particulier, en faisant $i \in [1, \nu]$, on voit que le polynôme $M(x) - \tilde{\Delta}\lambda$ (qui appartient à $k(\lambda)[x]$) est un multiple de $Q(x)$.

Résolvants f-triviaux

Le résolvant Θ d'un sous-groupe H de $\mathfrak{S}_n$ sera dit *f-trivial* ssi on a un $\lambda \in E$ tel que $\mathcal{L}_{\Theta,f} = (x - \lambda)^e$. Comme on est en caractéristique 0, alors nécessairement $\lambda \in k$. Puisque $\Theta(\mu_1, \dots, \mu_n)$ est semi-simple, il revient au même de dire que Θ est f-trivial, ou que $\Theta(\mu_1, \dots, \mu_n)$ est une homothétie dans le k-espace vectoriel $\mathcal{A}/\mathfrak{I}$. De façon équivalente, Θ est f-trivial ssi il existe $\lambda \in E$ tel que $\Theta(\rho_{\sigma(1)}, \dots, \rho_{\sigma(n)}) = \lambda$ pour toute permutation $\sigma \in \mathfrak{S}_n$ et si c'est le cas alors $\lambda \in k$. Et puisque $\mathfrak{I} = \sqrt{\mathfrak{I}}$, cela s'exprime par le théorème suivant :

Théorème 10.7. Le résolvant Θ est f-trivial ssi il existe $\lambda \in k$ tel que $\Theta - \lambda \in \mathfrak{I}$.

Tout sous-groupe H admet des résolvants f-triviaux : par exemple, si Θ est un résolvant quelconque de H, alors $\Theta \times (\sigma_1 - c_1)$ est un résolvant f-trivial de H.

En raison du Théorème 10.7, il convient de disposer d'un critère d'appartenance à l'idéal $\mathfrak{I}$. On peut montrer que pour tout $\Phi \in \mathcal{A}$, la division de Macaulay de Φ par $\sigma_1 - c_1, \dots, \sigma_n - c_n$ existe de façon unique, i.e. il existe $(\Phi_0, \dots, \Phi_n)$ suite unique d'éléments de $\mathcal{A}$ telle que

$$\Phi = \Phi_0(\sigma_1 - c_1) + \cdots + \Phi_{n-1}(\sigma_n - c_n) + \Phi_n \qquad , \tag{74}$$

avec $\deg_{x_i}(\Phi_j) < i$ pour tous i, j tels que $1 \leq i \leq j \leq n$, et que de sucroît on a $\Phi \in \mathfrak{I}$ ssi $\Phi_n = 0$.

Dans (74), Φ_n s'appelle le reste de cette division de Macaulay. (Le calcul des Φ_i se ramène à résoudre un système linéaire de Cramer sur k.)

On voit donc que le résolvant Θ sera f-trivial ssi son reste dans la division de Macaulay par $\sigma_1 - c_1, \dots, \sigma_n - c_n$ est une constante. On peut également utiliser la base standard de $\mathfrak{I}$ pour l'ordre lexicographique (voir [A. Mach, A. Valibouze]).

Application au degré 5

Pour illustrer les notions ci-dessus, prenons maintenant $n = 5$, et supposons f irréductible dans $k[x]$. On a vu que Γ est alors résoluble ssi il est constant dans l'un des six sous-groupes métacycliques principaux de $\mathfrak{S}_5$, lesquels sont conjugués dans $\mathfrak{S}_5$.

Soit H l'un de ces sous-groupes métacycliques de $\mathfrak{S}_5$, soit Θ un de ses résolvants et soit Ψ un résolvant f-séparable de H. Reprenons toutes les notations des Théorèmes 10.4 et 10.6. On a ici $e = 6$, $h = 20$. Rappelons qu'on a posé $\lambda = \tilde{\Theta}$ $(= \tilde{\Theta}_1)$.

La k-algèbre des racines de $\mathcal{L}_{\Psi,f}$ dans E est E (Théorème 4.6), donc ou bien $\mathcal{L}_{\Psi,f}$ est k-irréductible, ou bien $\mathcal{L}_{\Psi,f} = UV$ avec $U \in k[x]$, $V \in k[x]$, $\deg(U) = 5$, $\deg(V) = 1$ et U irréductible sur k. Dans ce dernier cas, Γ est résoluble par simple application du Théorème 5.2. Sinon, $\Gamma \in \{\mathfrak{A}_5, \mathfrak{S}_5\}$.

Supposons $\lambda \in k$, et que la multiplicité ν de λ dans $\mathcal{L}_{\Theta,f}$ soit ≥ 2. Si $\mathcal{L}_{\Psi,f}$ est k-irréductible, i.e. Γ n'est pas résoluble, le Théorème 10.6 montre immédiatement que $\nu = 6$, c'est-à-dire que $\mathcal{L}_{\Theta,f} = (x-\lambda)^6$, autrement dit, que Θ est f-trivial. On va en déduire le résultat suivant :

Théorème 10.8. Supposons que $n = 5$, que f est k-irréductible, que H est un sous-groupe métacyclique principal de $\mathfrak{S}_5$, et que Θ est un résolvant non f-trivial de H.

a) Pour que Γ soit résoluble, il faut et il suffit que $\mathcal{L}_{\Theta,f}$ possède au moins une racine dans k (multiple ou non).
b) Si $\lambda \in k$ est une racine de $\mathcal{L}_{\Theta,f}$ de multiplicité ≥ 2, on a $\mu \in k\backslash\{\lambda\}$ tel que $\mathcal{L}_{\Theta,f} = (x-\lambda)^5(x-\mu)$.
c) Si $\mathcal{L}_{\Theta,f}$ n'a aucune racine dans k, alors $\mathcal{L}_{\Theta,f}$ est séparable, et même irréductible dans $k[x]$.

Démonstration. Les assertions a) et b) découlent du Théorème 10.6, et des considérations qui précèdent l'énoncé du Théorème 10.8. Prouvons l'assertion c) : puisque $\mathcal{L}_{\Theta,f}$ n'a pas de racine dans k, si $\mathcal{L}_{\Theta,f}$ n'était pas séparable, il serait divible dans $k[x]$ par P^2 avec P polynôme irréductible dans $k[x]$ et de degré 2 ou 3. Soit alors $\lambda \in E$ une racine de P. Puisque $[k[\lambda] : k] \in \{2,3\}$, on voit que f est irréductible dans $k(\lambda)[x]$, sinon $[E : k]$ ne pourrait pas être divisible par 5. Mais la multiplicité de λ dans $\mathcal{L}_{\Theta,f}(x)$ ne peut être que 2 ou 3 ; en remplaçant k par $k(\lambda)$, les hypothèses assurant la validité des assertions a) et b) continuent à être satisfaites. On aboutit donc à une contradiction puisque la multiplicité de λ dans $\mathcal{L}_{\Theta,f}(x)$ devrait être 5. Cette contradiction prouve donc que $\mathcal{L}_{\Theta,f}$ est séparable. Mais puisque $\mathcal{L}_{\Theta,f}$ n'a pas de racine dans k, l'étude qui précède l'énoncé du Théorème 10.8 montre que $\mathcal{L}_{\Theta,f}$ est irréductible dans $k[x]$ □

Montrons à l'aide d'un exemple que le cas b) du Théorème 10.8 peut effectivement arriver. Dans tout ce qui suit, jusqu'à la fin du paragraphe, nous supposerons que $n = 5$, et que H est le sous-groupe métacyclique principal de $\mathfrak{S}_5$ contenant le cycle $< 1,2,3,4,5 >$. On a alors deux résolvants intéressants de H, que nous noterons Φ et Ψ, donnés par :

$$\begin{aligned} \Phi &= \gamma_1^2 + \gamma_2^2 \text{ , où :} \\ \gamma_1 &= (x_1-x_2)(x_2-x_3)(x_3-x_4)(x_4-x_5)(x_5-x_1) \quad , \\ \gamma_2 &= (x_1-x_3)(x_3-x_5)(x_5-x_2)(x_2-x_4)(x_4-x_1) \quad \text{, et :} \end{aligned} \tag{75}$$

$$\begin{aligned} \Psi &= (V_1-V_2)^2 \text{ , où :} \\ V_1 &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 \quad , \\ V_2 &= x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1 \quad . \end{aligned} \tag{76}$$

Le résolvant Φ a été calculé par Berwick ([E.H. Berwick,1915]). Quant à Ψ, c'est le célèbre *résolvant de Cayley* : la résolvante correspondante $\mathcal{L}_{\Psi,f}$ (dite *de Cayley*)

a été calculé par [A. Cayley] et nous avons contrôlé son résultat. Si $f = x^5 - a$ avec $a \in k^\star$, un calcul facile donne :

$$\mathcal{L}_{\Theta,x^5-a}(x) = (x + 5^4a^2)(x + 5^3a^2)^5 \qquad . \tag{77}$$

Avec $k = \mathbb{Q}$ et $a \in \mathbb{Q}^\star$, a non puissance 5-ième dans $\mathbb{Q}$, on sait que $x^5 - a$ est $\mathbb{Q}$-irréductible et que le groupe Γ est métacyclique. On sera alors dans le cas b) du Théorème 10.8, qui peut donc arriver effectivement.

La résolvante de Cayley Ψ donnée par (76) est très remarquable en raison du résultat non-évident ci-après :

Théorème 10.9. Avec $n = 5$ et f irréductible dans $k[x]$, la résolvante de Cayley $\mathcal{L}_{\Psi,f}$ correspondant à (76) est séparable.

Démonstration. Il est bien connu que $\mathcal{L}_{\Psi,f}$ est de la forme :

$$\mathcal{L}_{\Psi,f}(x) = P^2(x) - 2^{10}\tilde{\Delta}x \qquad , \tag{78}$$

avec $\tilde{\Delta} = \prod_{1\le i<j\le 5}(\rho_i - \rho_j)^2$, et $P(x) = x^3 + a_1x^2 + a_2x + a_3 \in k[x]$ (voir par exemple [N. Tchebotarev]).

Pour abréger, posons $R = \mathcal{L}_{\Psi,f}(x)$. D'après le Théorème 10.8, tout revient à voir que R n'admet dans $\hat{k}$ aucune racine d'ordre $\nu \ge 5$. Or supposons qu'une telle racine λ existe, d'ordre $\nu \ge 5$.

a) Montrons d'abord que $\lambda \neq 0$. On a $R' = 2PP' - 2^{10}\tilde{\Delta}$, d'où les relations :

$$P^2(\lambda) = 2^{10}\tilde{\Delta}\lambda \tag{79}$$

$$2(PP')(\lambda) = 2^{10}\tilde{\Delta} \qquad . \tag{80}$$

En élevant au carré les deux membres de (80), puis en y remplaçant $P^2(\lambda)$ par sa valeur tirée de (79), on arrive à :

$$4\lambda P'^2(\lambda) = 2^{10}\tilde{\Delta} \qquad , \tag{81}$$

d'où $\lambda \neq 0$ puisque $\tilde{\Delta} \neq 0$.

b) Puisque $\lambda \neq 0$, d'après (79) on a aussi : $P(\lambda) \neq 0$. A présent λ est racine d'ordre $\nu - 1$ de R', donc est racine d'ordre ≥ 4 à la fois de R et R', donc aussi de $R - xR' = P(P - 2xP')$. Puisque $P(\lambda) \neq 0$, c'est que λ est racine d'ordre ≥ 4 de $P - 2xP' = -5x^3 - 3a_1x^2 - a_2x + a_3$, ce qui est absurde puisque ce dernier polynôme est de degré 3 (rappelons qu'on est en caractéristique 0). Donc on arrive à une contradiction, et λ ne peut exister □

Nous remercions Daniel Lazard d'avoir apporté une notable simplification à la partie b) de cette démonstration.

Compte tenu du Théorème 10.8, le Théorème 10.9 donne

Corollaire 10.10. (" Théorème de Selivanoff ")
Si $n = 5$ et si f est irréductible dans $k[x]$, le groupe de Galois Γ de f sur k est résoluble ssi la résolvante de Cayley de f admet une racine dans k.

Le Théorème de Selivanoff est énoncé dans [N. Tchebotarev], pages 341 et 342. La preuve qui en est proposée est incomplète car l'auteur y affirme que le seul cas à écarter pour assurer que $\mathcal{L}_{\Psi,f}$ est séparable est le cas où l'on aurait $\mathcal{L}_{\Psi,f}(x) = (x-\lambda)^6$, i.e. le cas où Ψ serait f-trivial. Or l'exemple tiré de (77) montre qu'il faut impérativement écarter, outre le cas où Ψ serait f-trivial, le cas où $\mathcal{L}_{\Psi,f}(x)$ serait de la forme $(x-\lambda)^5(x-\mu)$ avec $\lambda \neq \mu$.

Détermination du groupe de Galois Γ en degré 5 dans le cas général

Il faut distinguer deux aspects dans la recherche du groupe de Galois de f sur k. Nous définissons ces deux problèmes dans le cas général où f est de degré $n \geq 2$ quelconque :

Problème I : f étant donné numériquement, calculer la classe de conjugaison de Γ dans $\mathfrak{S}_n$. (recherche de Γ " au coup par coup "). C'est ce problème dont la méthode de la "chasse aux résolvantes" exposée au §6 offre une solution, sous réserve de calculer suffisamment de résolvantes séparables et de les factoriser dans $k[x]$.

Problème II : Expliciter un système de conditions nécessaires et suffisantes portant sur les coefficients $(c_i)_{1\leq i\leq n}$ de f pour que la classe de conjugaison de Γ dans $\mathfrak{S}_n$ soit une classe donnée à l'avance.

Evidemment le Problème II est bien plus complexe que le problème I. Une solution du problème II, due aux auteurs, est exposées dans [J.M. Arnaudiès, J. Bertin] lorsque $n = 4$. Nous allons maintenant voir que ce problème II admet une solution pour $n = 5$.

Revenons donc au cas $n = 5$, et reprenons toutes les notations des Théorèmes 10.8 et 10.9, et des relations (75), (76) et (78).

Notons H_+ le sous-groupe métacyclique pair de H, et C son sous-groupe cyclique de cardinal 5 (engendré par le cycle $< 1, 2, 3, 4, 5 >$). Posons :

$$(82) \qquad \left\{ \begin{array}{ll} \gamma = & \gamma_1 = (x_1-x_2)(x_2-x_3)(x_3-x_4)(x_4-x_5)(x_5-x_1) \\ & \gamma_2 = (x_1-x_3)(x_3-x_5)(x_5-x_2)(x_2-x_4)(x_4-x_1) \\ & \gamma_3 = -\gamma_1 \\ & \gamma_4 = -\gamma_2 \qquad . \end{array} \right.$$

On vérifie que pour tout i :

$$C = \mathrm{Stab}_{\mathfrak{S}_5}(\gamma_i) \text{ , et } H_+ = \mathrm{Stab}_{\mathfrak{S}_5}(\gamma_i^2) = \mathrm{Stab}_H(\gamma_i^2) \qquad .$$

L'ensemble $\{\gamma_i\}_{1\leq i\leq 4}$ est H-stable, et l'action de H sur cet ensemble correspond à un morphisme de H dans le groupe des permutations des γ_i, dont l'image est le groupe 4-cyclique engendré par le cycle $<\gamma_1,\gamma_2,\gamma_3,\gamma_4>$. Les ensembles $\{\gamma_1,-\gamma_1\}$ et $\{\gamma_2,-\gamma_2\}$ sont H_+-stables. On voit donc que γ_1 est un résolvant relatif de C par rapport à H_+ (cf. définition 6.8 et 6.9), la résolvante relative associée étant :

$$\mathcal{L}^{[H_+]}_{\gamma_1,f}(x) = x^2 - \widetilde{\gamma_1}^2 = (x-\widetilde{\gamma_1})(x+\widetilde{\gamma_1}) \qquad ; \tag{83}$$

cette résolvante (83) est séparable ; en effet on a :

$$\widetilde{\gamma_1}^2\widetilde{\gamma_2}^2 = \tilde{\Delta}\ \text{, où}\ \tilde{\Delta} = \prod_{1\leq i<j\leq 5}(\rho_i-\rho_j)^2 \neq 0\ \text{; d'où}\ \widetilde{\gamma_i}\neq 0 \qquad . \tag{84}$$

D'après le Théorème 6.11, si $\Gamma\subset H_+$, on aura donc $\Gamma\subset C$ ssi $\tilde{\gamma_1}\in k$. Notons d'ailleurs que si $\Gamma\subset H$, nécessairement $C\subset\Gamma$ puisque Γ contient au moins un 5-cycle et puisque tout 5-cycle de H engendre C. En fin de compte, si $\Gamma\subset H_+$, alors $\Gamma = C$ ssi $\widetilde{\gamma_1}\in k$.

Rappelons que $\Phi=\gamma_1^2+\gamma_2^2$ est un résolvant absolu de H, et que la résolvante $\mathcal{L}_{\Phi,f}$ est connue génériquement. Si $\Gamma\subset H$ et si la résolvante $\mathcal{L}_{\Phi,f}$ n'est pas f-triviale, elle admet une unique racine simple dans k (que $\mathcal{L}_{\Phi,f}$ soit ou non séparable), et l'étude qui entoure le Théorème 10.8 permet de montrer que cette racine est $\widetilde{\gamma_1}^2+\widetilde{\gamma_2}^2$. Nous avons donc deux cas dans l'hypotèse où $\Gamma\subset H$:

Premier cas : $\mathcal{L}_{\Phi,f}$ est f-triviale, i.e. est de la forme $(x-\lambda)^6$ avec $\lambda\in k$. Alors

$$(x-\widetilde{\gamma_1}^2)(x+\widetilde{\gamma_2}^2) = x^2-\lambda x+\tilde{\Delta}\ \text{(cf. (84))}. \tag{85}$$

Deuxième cas : $\mathcal{L}_{\Phi,f}$ n'est pas f-triviale. Alors elle possède dans k une unique racine simple ; notons-la λ. A nouveau, on a :

$$(x-\widetilde{\gamma_1}^2)(x+\widetilde{\gamma_2}^2) = x^2-\lambda x+\tilde{\Delta} \qquad ; \tag{86}$$

lorsque $\Gamma\subset H_+$, puisque $H_+ = \mathrm{Stab}_{\mathfrak{S}_5}(\gamma_i^2)$, on a nécessairement $\gamma_i^2\in k$.

Malheureusement il n'est pas exclu que la résolvante $\mathcal{L}_{\Phi,f}(x)$ puisse être f-triviale, auquel cas elle ne permet pas à elle seule de décider si Γ est résoluble. Mais pour cela on peut utiliser la résolvante de Cayley (cf. Théorème 10.9), et exploiter le fait bien connu que $\Gamma\subset\mathfrak{A}_5$ ssi $\tilde{\Delta}$ est un carré dans $k^\star$. En résumé, on aboutit en faisant la synthèse de tout ce qui précède, à la discussion suivante qui résout complètement le problème II en degré 5 pour un polynôme k-irréductible :

Supposons f irréductible dans $k[x]$ et $n=5$. Adoptons les notations des relations (75), (76) et (82). Notons $k^{\star\square}$ l'ensemble des carrés dans $k^\star$.

A Si la résolvante de Cayley $\mathcal{L}_{\Psi,f}(x)$ est sans racine dans k :

a) pour $\tilde{\Delta} \notin k^{\star\square}$, $\Gamma = \mathfrak{S}_5$
b) pour $\tilde{\Delta} \in k^{\star\square}$, $\Gamma = \mathfrak{A}_5$.

B Si $\mathcal{L}_{\Psi,f}(x)$ possède une racine dans k :

a) pour $\tilde{\Delta} \notin k^{\star\square}$, Γ est un sous-groupe métacyclique principal de $\mathfrak{S}_5$
b) pour $\tilde{\Delta} \in k^{\star\square}$: alors la résolvante $\mathcal{L}_{\Phi,f}(x)$ soit est f-triviale soit admet dans k une unique racine simple. Notons λ son unique racine (qui est élément de k) si elle est f-triviale, et notons λ son unique racine simple dans k si elle n'est pas f-triviale. Alors $x^2 - \lambda x + \tilde{\Delta} = (x - a_1)(x - a_2)$ avec $a_1, a_2 \in k^\star$. On a :
(1) $a_1 \in k^{\star\square} \Leftrightarrow a_2 \in k^{\star\square} \Leftrightarrow \Gamma$ est un sous-groupe 5-cyclique de $\mathfrak{S}_5$,
(2) $a_1 \notin k^{\star\square} \Leftrightarrow a_2 \notin k^{\star\square} \Leftrightarrow \Gamma$ est un sous-groupe métacyclique pair de $\mathfrak{S}_5$.

On peut se demander, dans le cas B-b)-(1) ci-dessus, si on peut avoir $a_1 = a_2$. Avec $k = \mathbb{Q}$ et $f = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ (polynôme $\mathbb{Q}$-minimal de $2\cos\frac{2\pi}{11}$), le groupe Γ est bien 5-cyclique et on a $a_1 = a_2 = 11^2$, $\tilde{\Delta} = 11^4$. Dans tous les cas B-b)-(1), si $a_1 = a_2$, alors $\tilde{\Delta}$ est une puissance 4-ième dans $k^\star$. Avec f le polynôme minimal sur $\mathbb{Q}$ d'une période de Gauss appropriée qui engendre l'unique sous-extension 5-cyclique de $\mathbb{Q}$ du corps cyclotomique $\mathbb{Q}(e^{2i\pi/31})$, on constate que $\tilde{\Delta}$ n'est pas une puissance 4-ième dans $\mathbb{Q}^\star$, d'où ici $a_1 \neq a_2$.

Pour finir notons une curiosité :

Théorème 10.11. Supposons $n = 5$ et f irréductible dans $k[x]$. Supposons que la résolvante de Cayley $\mathcal{L}_{\Psi,f}(x)$ admette une racine dans k (elle est alors unique), notons-la λ, et supposons-la non nulle. Alors :

$$\lambda \in k^{\star\square} \Leftrightarrow \tilde{\Delta} \in k^{\star\square} \qquad .$$

Démonstration. (abrégée) Reprenons toutes les notations de la discussion précédente, et notamment de (76). On a $V_1 + V_2 = \sigma_2$; $(V_1 + V_2)^2 = V_1^2 + V_2^2 + 2V_1V_2 = \sigma_2^2$; $\Psi = (V_1 - V_2)^2 = V_1^2 + V_2^2 - 2V_1V_2$, d'où par différence $V_1V_2 = \frac{1}{4}(\sigma_2^2 - \Psi)$. D'autre part $\mathrm{Stab}_{\mathfrak{S}_5}(V_i) = \mathrm{Stab}_H(V_i) = H_+$, donc une résolvante relative de H_+ par rapport à H est $(x - V_1)(x - V_2) = x^2 - \sigma_2 x + \frac{1}{4}(\sigma_2^2 - \Psi)$; on peut supposer $\lambda = \tilde{\Psi}$, donc alors $\mathcal{L}^{[H]}_{V_1,f}(x) = x^2 - c_2 x + \frac{1}{4}(c_2^2 - \lambda)$; le discriminant de ce dernier polynôme est λ, qui est $\neq 0$ par hypothèse ; donc il est séparable. Le Théorème 6.11 s'applique et prouve que $\mathcal{L}^{[H]}_{V_1,f}(x)$ est dissocié dans $k[x]$ ssi $\Gamma \subset H_+$; mais cette dernière condition équivaut à : $\tilde{\Delta} \in k^{\star\square}$, tandis que $\mathcal{L}^{[H]}_{V_1,f}(x)$ est dissocié dans $k[x]$ ssi son discriminant est un carré dans k, c'est-à-dire ssi $\lambda \in k^{\star\square}$ $\square$

Remerciements

Nous tenons à remercier José Bertin qui a relu attentivement ce travail et qui y a apporté des remarques précieuses. Nous remercions également Marc Giusti qui, grâce à sa détermination en matière d'équipement du G.D.R MEDICIS, nous a permis de travailler sur une machine très performante avec les logiciels dont nous avions besoin.

References

[J.M. Arnaudiès] (1993), *Théorème de Bézout, Formule de Poisson-Perron et courbes rationnelles génériques*, (rapport interne du LITP numéro **92.94**)

[J.M. Arnaudiès, J. Bertin] **Groupes, Algèbres et Géométrie**, Tome I, Ellypses, 1993

[J.M. Arnaudiès, D. Lazard] (1993), *Equations du cinquième degré et résolutions par radicaux*, (manuscrit)

[Arnaudiès-Valibouze, (1993)] (1993), *Groupes de Galois des polynômes en degré 8*, Rapport interne du LITP 94-27

[E.H. Berwick,1915] (1915), *The Condition That A Quintic Equation Should Be Soluble By Radicals* Proc. London Math. Soc. (2) **14**. 301-307.

[E.H. Berwick,1929] (1929) *On Soluble Sextic equations* Proc. London Math. Soc. (2) **29**, 1-28.

[W. Burnside] **Theory of groups of finite order**, Dover, 1955

[G. Butler, J. McKay] (1983), *The transitive groups of degree up to 11*, Comm. Algebra **11**, 863-911.

[R. Brauer] **Galois Theory**, Harvard, Harvard University, 1964

[D. Casperson, J. McKay] *Symmetric functions, m-sets, and Galois groups.* To appear in Math. Comp. (1994)

[A. Cayley] (1961), *On a new auxiliary equation in the theory of equation of the fifth order*, Philosophical Transactions of the Royal Society of London, **CLL**

[H. Cohen] **A Course in Computational Algebraic Number Theory**, Graduate Texts in Mathematics **138**, Springer Verlag, 1993

[Dehn] **Algebraic equations** Dover, 1960

[L.E. Dickson] **Algebraic theories**, Dover publications, INC.,New-York.

[H.O. Foulkes] (1931), *The résolvents of an equation of seventh degree*, Quart. J. Math. Oxford Ser. (2), 9-19.

[E. Galois] **Oeuvres Mathématiques**, publiées sous les auspices de la SMF, Gauthier-Villars, 1897

[`G.A.P]` `Groups, Algorithms and Programming` Mathematics Research Section, ANU, Camberra, Australia

[I. Gil-Delessalle, A. Valibouze] (1996), *Galois inverse problem for some subgroups of degree 12*, proposé à MEGA'96

[Girard] , **Invention Nouvelle en Algèbre**, Amsterdam, 1629.

[K. Girstmair] (1983) *On the computation resolvents and Galois groups*, Manuscripta Math., v. 43, pp. 289-307.

[J.L. Lagrange, 1770] (1770) *Reflexions sur la résolution algébrique des équations*, Prussian Academy

[J.L. Lagrange, tome IV] *Reflexions sur la résolution algébrique des équations*, **Mémoires de l'Académie de Berlin**, 205-421, (**Oeuvres de Lagrange**, tome IV, 205-421)

[J.L. Lagrange, tome VIII] *Traité de la résolution des équations numériques : Notes sur la théorie des équations algébriques*, Oeuvres de Lagrange , Tome VIII, 133-367

[F. Lehobey] (1994), *Algorithmique Methods and Practical Issues in the Computation of Galois Group of Polynomials*, Mémoire de DEA, Univ. Rennes.

[A. Mach, A. Valibouze] (1991), *L'idéal des relations symétriques et l'idéal des relations* prépublication

[`Marie`] Sun Sparc 10/41 - 40 Mhz - 256 Mo de memoire - SunOS 4.1.3, G.D.R de Calcul Formel MEDICIS.

[J. McKay, L. Soicher] (1985), *Computing Galois Groups over the rationals*, Journal of number theory **20**, 273-281.

[MAXIMA] Maxima DOE maintenu par William SCHELTER

[E. Netto] **Theory of sustitutions**, Chelsca, reprint, 1892

[L. Soicher] *The computation of the Galois groups*, Thesis in departement of computer science, Concordia University, Montreal, Quebec, Canada, (1981).

[R.P. Stanley] (1979), *Invariants of Finite Groups and their applications to combinatorics*, Bull. amer. Society, **3**, pp. 475-511

[R.P. Stauduhar] (1973), *The determination of Galois groups*, Math. Comp. **27**, 981-996.

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

[A. Valibouze1] (1988), *Manipulations de fonctions symétriques*, Thèse de l'Université Paris VI.

[A. Valibouze2] (1992) *Sur l'arité des fonctions*, European Journal of Combinatorics, 1993, **14**, 359-372

[A. Valibouze3] *Computation of the Galois Groups of the Resolvent Factors for the Direct and Inverse Galois Problem.* , AAECC'95 (Paris, Juillet 1995), LNCS **948**.

[A. Valibouze4] (1995) *Modules de Cauchy, polynômes caractéristiques et résolvantes* Rapport interne LITP n^o 95-62

[A. Valibouze5] Valibouze A. (1996) `Extension SYM de MACSYMA, manuel de l'utilisateur`,

Laboratoire d'Algèbre et L.I.T.P., Université Paris VI, 4 place Jussieu, F-75252 Paris Cedex 05

E-mail address: jma@sysal.ibp.fr, avb@cosme.polytechnique.fr