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. Reprsentations par permutations

En thorie de Galois explicite, on est amen reprsenter un mme groupe de Galois abstrait $\mathrm{Gal}(E/K)$ dans des groupes de permutations des racines de divers polynmes $f \in K[x]$ dont les degrs peuvent varier. En effet on a besoin de calculer beaucoup de rsolvantes en contrlant au maximun leur corps de racines (voir Thorme 4.6 par exemple). Il nous a donc paru utile de rappeler quelques faits connus concernant les reprsentations par permutations d'un groupe fini (cf. [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 $\{\mathrm{Stab}_{G,\Psi}(x)\}_{x \in E} = \{\mathrm{Stab}_{G,\Phi}(x)\}_{x \in E}$. 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 $\Theta(x) = \{g \in G \mid \Psi(g)(x_0) = x\}$ 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 $\forall H \in \mathcal{C}\,,\, \exists H' \in \mathcal{C}' \mid H \subset H'$. 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 systmes d'imprimitivit du G-ensemble $(G/H)_g$ défini par les translations à gauches. Si H'_1 et H'_2 sont deux tels H', de mme indice N' dans G, les actions par translations gauche induites sur les blocs d'imprimitivit correspondant respectivement H'_1 et H'_2 sont quivalentes ssi H'_1 et H'_2 sont conjugus dans G.

1.2. Reprsentations par permutations quelconques. Soit $\mathcal{E}$ l'ensemble des classes de conjugaison de sous-groupes de G ; chaque $\mathcal{C} \in \mathcal{E}$, nous associerons son *degr* (not $\deg(\mathcal{C})$) qui est par dfinition l'entier gal $[G : H]$ pour tout $H \in \mathcal{C}$, et sont *poids*, not $\pi(\mathcal{C})$, gal par dfinition $\mathrm{card}(G)/\deg(\mathcal{C})$. Ci-aprs, 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 reprsentation donne ρ' de G associe $\mathcal{C}'$ est le nombre des $H' \in \mathcal{C}'$ tels que $H \subset H'$. Il ne dpend 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 $[m_{i,j}] = [J(\mathcal{C}_i,\mathcal{C}_j)]_{(i,j)\in[1,s]^2}$, note $J(G)$, sera appele la *matrice d'incidence de* G. D'aprs ce qu'on vu, elle est trigonale suprieure, coefficients dans $\mathbb{N}$ et diagonale > 0 donc en particulier inversible.

Soit Ψ une reprsentation de G par permutations. Soit ω une G-orbite correspondante, de cardinal not N. Par restriction, ρ dfinit une reprsentation transitive $G \to \mathfrak{S}_\omega$, qui est donc quivalente l'une de celles dfinies par les $\mathcal{C}_i$ de degr N. Notons $\nu_i(\rho)$ le nombre de telles orbites ω qui conduisent ainsi $\mathcal{C}_i$. Il est clair que $\nu_i(\rho)$ reste invariant si on remplace ρ par une reprsentation quivalente. On peut donc associer ρ l'lment $U(\rho) = \sum_{1\leq i\leq s} \nu_i(\rho)\,\mathcal{C}_i$ 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'quivalence de reprsentations 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 [Burnside])

Théorème 1.2. *Avec les notations ci-dessus, l'application* $U : \rho \mapsto \sum_{1\leq i\leq s} \nu_i(\rho)\,\mathcal{C}_i$ *dfinit une bijection entre l'ensemble des classes d'quivalence de reprsentations de* G *par permutations de degr* n *(*$n \in \mathbb{N}^*$*), et l'ensemble des lments* $\sum_{1\leq i\leq s} \nu_i\,\mathcal{C}_i$ *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 reprsentation de degr 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 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 donns par le systme 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 reprsentations par permutations. Soit $\rho : G \to \mathfrak{S}_E$ et $\theta : G \to \mathfrak{S}_F$ deux reprsentations de G par permutations, de degrs 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 dfinissent 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.

Considrons 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 une permutation des $a_{\alpha,\beta}$, i.e. un lment 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 reprsentation de G par permutations, dont la classe d'quivalence ne dpend 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 dpend que de $(\mathcal{C}_i, \mathcal{C}_j)$, et sera not $\mathcal{C}_i \otimes \mathcal{C}_j$ et sera appel *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 vrifient

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

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

Dans le cas gnral, 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 reprsentation ρ_i de G telle que $U(\rho_i) = \mathcal{C}_i$; alors ρ et θ sont respectivement quivalentes $\bigoplus_{i=1}^{s} \nu_i(\rho)\rho_i$ et $\bigoplus_{i=1}^{s} \nu_i(\theta)\rho_i$. D'o :

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

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

Munissons $\mathcal{L}_G$ de la structure de $\mathbb{Z}$-algbre obtenue en prolongeant par $\mathbb{Z}$-linarit 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 algbre.

On a donc :

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

La $\mathbb{Z}$-algbre de $\mathcal{L}_G$ est associative et admet un lment unit, 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 dtermine les constantes $a_{i,j,r}$ puisque pour chaque (i,j), il s'agit d'un systme de Cramer en les inconnues $(a_{i,j,r})_{1 \le r \le s}$. La $\mathbb{Z}$-algbre $\mathcal{L}_G$ est essentiellement celle appele par certains auteurs, *Algbre de Burnside*, son produit $\otimes$ tant appel le *produit tensoriel*.

1.4. Reprsentations fidles. Soit $\Psi : G \to \mathfrak{S}_n$ une reprsentation symtrique de degr 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 $\{i \in [1,s] \mid \nu_i \ge 1\}$. On a : $\mathrm{Ker}(\Psi) = \bigcap_{i \in \mathrm{Supp}(\Psi)} I_{\mathcal{C}_i}$. Donc Ψ est fidle 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 cltures algbriques fixe une fois pour toutes.

2. Reprsentations et corps des racines

2.1. Soit $f \in k[X]$, normalis (unitaire), de degr $n \ge 1$, sparable. Notons E_f sa k-algbre des racines dans $\hat{k}$. On considre une numrotation 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 reprsentation symtrique de degr n :

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

associe l'action naturelle du groupe $\mathrm{Gal}(E_f/k)$ sur $\mathcal{R}_f = \{\rho_1, \ldots, \rho_n\}$. La reprsentation (8) est fidle, et elle est transitive ssi f est irrductible.

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

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

donc un changement de numrotation de $\mathcal{R}_f$ change la reprsentation de (8) en une reprsentation quivalente.

Soient $P_1, \ldots, P_r$ les facteurs irrductibles normaliss de f et soient $n_i = \deg(P_i)$, o $n_1 \ge \cdots \ge n_r$. Le groupe $\mathrm{Gal}(E_f/k)$ opre transitivement sur $\mathcal{R}_{P_i}$; soit C_i la classe de conjugaison de sous-groupes de $\mathrm{Gal}(E_f/k)$ correspondant cette reprsentation ; alors la classe d'quivalence de la reprsentation (8) est $\sum_{i=1}^{r} C_i$; puisque cette reprsentation (8) est fidle, 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 reprsentation symtrique donne

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

fidle et degr n, peut tre dfinie sous la forme (8). Supposons k infini.

Soient $\omega_1, \ldots, \omega_r$ les orbites de $[1, n]$ pour la reprsentation (10) ; posons $n_i = \mathrm{card}(\omega_i)$, supposons les ω_i ordonns 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 lment fix 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 lment ξ_i de Ω_i qui soit k-primitif, et soit P_i son polynme 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 $\xi_{i,j} = \tau_{i,j}(\xi_i)$ $(1 \leq j \leq n_i)$, o $\{\tau_{i,j}\}_{1 \leq j \leq n_i}$ dsigne une transversale quelconque de $\mathrm{Gal}(E/k) \bmod G_i$. 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 polynme sparable. 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'identit sur ω_i. Donc $\bigcap_{i=1}^r I_{C_i} = \{\mathrm{Id}_E\}$ car la reprsentation (10) est fidle. 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-algbre des racines de f.

Numrotons 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 reprsentation (10) n'est autre que celle associe cette numrotation pour f. On a donc prouv :

Proposition 2.1. *Si le corps k est infini, toute reprsentation symtrique fidle de degr n du groupe de Galois $Gal(E/k)$ d'une extension finie galoisienne E de k peut tre dfinie d'au moins une manire sous la forme (8) avec f sparable, $f \in k[x]$.*

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

Sur l'ensemble des polynmes $f \in k[x]$, normaliss, de degr $n \geq 1$, et sparables, on obtient une relation d'quivalence dont les classes sont les ensembles de polynmes ayant mme k-algbre des racines dans $\hat{k}$ et dfinissant des reprsentations quivalentes.

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

Notant $N = [E : k]$, considrons une reprsentation symtrique fidle et transitive

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

Soit ξ un lment primitif fix de E sur k. Notons $G = \mathrm{Gal}(E/k) = \{\sigma_1, \ldots, \sigma_N\}$, o $\sigma_1 = \mathrm{Id}_E$, et posons $\xi_i = \sigma_i(\xi)$. On peut supposer la numrotation (σ_i) choisie pour que $\sigma_i.1 = i$ dans la reprsentation (11). Il est alors clair que cette reprsentation n'est autre que la reprsentation rgulire gauche de G dfinie par la numrotation (σ_i). Donc la classe d'quivalence de la reprsentation rgulire gauche de G est dfinie par le polynme k-minimal de n'importe quel lment primitif de E/k.

3. La matrice des partitions associe un groupe fini

Le problme le plus naturel de la thorie de Galois explicite est de calculer le groupe de Galois sur K d'un polynme donn $f \in K[x]$. La littrature disponible sur ce sujet dveloppe la mthode suivante : partir de “ fonctions ” aussi simples que possible, on calcule des “ rsolvantes ” de f. On dresse des tables de ces rsolvantes et de leur groupe associ (voir [Berwick,1929] page 11 pour la mthode jusqu'alors employe). Quand on peut relever assez d'incompatibilits dans ces tables, qui ne peuvent tre que partielles, on en dduit le groupe de Galois cherch. On pourra suivre la progression de cette ide de Lagrange Soicher (voir [Soicher] ou [McKay-Soicher]) en passant par Cayley, Jordan, Kronecker, Netto, Berwick, Foulkes et d'autres (voir la bibliographie jointe).

L'ide de base du prsent article est d'inverser la dmarche. L'tude des auteurs cits nous a convaincus que les tables partielles en question sont en fait des parties de tables purement groupistiques. Nous avons donc dfini ces tables de faon globale, abstraite et indpendante, et nous en avons calcul un grand nombre (voir [Arnaudis-Valibouze]) grce des logiciels de calculs sur les groupes. De ces tables nous avons dduit les rsolvantes qu'il faut calculer et non l'inverse.

Nos tables permettent de travailler sur des polynmes sparables arbitraires et non seulement sur des polynmes irrductibles. Notre mthode s'applique aussi aux “ rsolvantes relatives ” dont on se contentait jusqu'ici de tester la linarit 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 $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ telle que $\sum_{i=1}^n i\alpha_i = n$. Le *support* d'une telle partition est par dfinition l'ensemble $\{i \in [1,n] \mid \alpha_i \geq 1\}$; l'entier α_i est appel *multiplicit* de i dans la partition, et le cardinal du support est appel le *nombre de composants* dans la partition. Une partition ϖ de n est dtermine de manire unique par la suite strictement croissante $(d_1, \dots, d_r)$ des termes de son support et par la suite $\nu_1 = \alpha_{d_1}, \dots, \nu_r = \alpha_{d_r}$ des multiplicits des composants. On notera

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

tant entendu que $1 \leq d_1 \leq \cdots \leq d_r \leq n$, $r \geq 1$ 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 degr $e = e_{\mathcal{C}}$. A tout couple $(H, \mathcal{C})$, o H dsigne un sous groupe de G, on va associer une partition de e.

Pour cela, fixons $H_1 \in \mathcal{C}$, soit $C_1 = H_1, C_2, \dots, C_e$ les classes gauche de G mod H_1, et faisons oprer H gauche sur $\mathcal{H}_1 = \{C_1, \dots, C_e\}$ par translations 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 $(\alpha_1, \ldots, \alpha_e)$ de e dfinie ci-dessus ne dpend que de $\mathcal{C}$ et non du choix de $H_1 \in \mathcal{C}$.*

Démonstration. Soit $\{g_1, \ldots, g_e\}$ 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 $([H : H \cap H_i])_{1 \leq i \leq e}$, on trouve donc d_ω fois l'entier d_ω, une fois pour chaque i tel que $C_i \in \omega$. Donc la partition $(\alpha_1, \ldots, \alpha_e)$ s'obtient ainsi : pour chaque entier j, $1 \leq j \leq e$, $\alpha_j = N_j/j$, o $N_j = \mathrm{card}\{i \in [1, e] \mid [H : H \cap H_i] = j\}$.

Soit maintenant $H_1' = \sigma\, H_1\, \sigma^{-1} \in \mathcal{C}$, o $\sigma \in G$. L'ensemble $\mathcal{H}_1'$ des classes gauche de $G \bmod H_1'$ est $\{g_i' H_1'\}_{1 \leq i \leq e}$, o $g_i' = \sigma\, g_i \sigma^{-1}$. La partition $(\alpha_1', \ldots, \alpha_e')$ construite comme ci-dessus partir de H_1' est donc dfinie par $\alpha_j' = N_j'/j$, o $N_j' = \mathrm{card}\{i \in [1, e] \mid [H : H \cap H_i'] = j\}$ 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'lment 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 gaux, d'o $N_j = N_j'$ pour tout j, d'o $(\alpha_1', \ldots, \alpha_e') = (\alpha_1, \ldots, \alpha_e)$. $\square$

Remarque 2. On peut donner une variante de cette dmonstration en utilisant les classes doubles modulo H.

D'aprs le Lemme 1, la partition $(\alpha_1, \ldots, \alpha_e)$ de $e = e_{\mathcal{C}}$ construite ci-dessus ne dpend que du couple $(H, \mathcal{C})$. Nous l'appellerons *partition associe* $(H, \mathcal{C})$ 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 dpend 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 $j \in [1, e]$, $\mathrm{card}\{i \mid [H : H \cap H_i] = j\} = \mathrm{card}\{i \mid [H' : H' \cap H_i'] = j\}$. $\square$

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 $\varpi(\mathcal{C}, \mathcal{D})$ gale la valeur commune des $\varpi(H, \mathcal{D})$. Cette partition $\varpi(\mathcal{C}, \mathcal{D})$ sera dite *associe* $\mathcal{C}, \mathcal{D}$.

Ordonnons $\mathcal{E}$ en une suite $\mathcal{C}_1, \ldots, \mathcal{C}_s$ par degrs dcroissants, de sorte que $\mathcal{C}_1 = \{\{e_G\}\}$ et $\mathcal{C}_s = \{G\}$. On obtient une matrice carre :

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

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

Pour calculer chaque coefficient $\varpi(\mathcal{C}_i, \mathcal{C}_j)$ de la matrice $\mathcal{P}$, choisissons des lments H_i et H_j dans les classes $\mathcal{C}_i$ et $\mathcal{C}_j$ respectivement. Soit $e_j = [G : H_j]$, et soit $\{\gamma_m\}_{1 \leq m \leq e_j}$ une transversale gauche de $G \bmod H_j$, avec $\gamma_1 = 1_G$. Alors $\varpi(\mathcal{C}_i, \mathcal{C}_j) = (\alpha_1, \ldots, \alpha_{e_j})$, o 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

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

$(1 \leq d_{i,j,1} < \cdots < d_{i,j,r_{i,j}} \leq e_j\ ,\ \nu_{i,j,l} \geq 1)$, alors il est clair d'aprs (14) que les lments $d_{i,j,l}$ 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 thorme fondamental qui va tre la base de tous les calculs explicites ultrieurs de groupes de Galois :

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

Démonstration. Choisssons dans chaque classe $\mathcal{C}_i$ un lment H_i. Fixons i et j, avec $1 \leq j < i \leq s$. 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 multiplicit $\nu_{j,j,1} = [\mathcal{N}_G(H_j) : H_j]$, o $\mathcal{N}_G(H_j)$ dsigne 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 tre gal H_i, car $\mathcal{C}_i \neq \mathcal{C}_j$, ni contenir H_i, car $e_j \geq e_i$; donc lorsque m dcrit $[1, e_j]$, les indices $[H_i : \gamma_m\, H_j\, \gamma_m^{-1} \cap H_i]$ sont tous > 1. Donc $d_{i,j,1} > 1$, d'o $\varpi(\mathcal{C}_i, \mathcal{C}_j) \neq \varpi(\mathcal{C}_j, \mathcal{C}_j)$ et les lignes d'indices i et j sont bien distinctes. $\square$

Lorsque $G = \mathfrak{S}_n$, nous avons calcul la matrice des partitions complte 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 calcul 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 degr dpasse 672 (i.e. celles qui donneraient des polynmes de degr ≥ 672 factoriser).

Pour $n = \{9, 10, 11\}$, nous avons calcul 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'intrt compte tenu des matrices dj obtenues en degr < 9 : pour ces 3 tables, nous avons utilis la nomenclature des sous-groupes transitifs de $\mathfrak{S}_n$ pour $n \leq 11$ donne par [Butler-McKay].

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

Par exemple, il apparait qu'en degr 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 extrmement rapide d'identifier un polynme de degr 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 rsolvantes relatives (cf. Thorme 6.11 ci-aprs), les calculs de tables sont bien videmment 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 t excuts l'aide du logiciel [G.A.P] (=Groups, Algorithms and Programming).

4. La notion de rsolvante de Lagrange

Nous donnons ici la dfinition de la rsolvante de Lagrange *gnrique* (terme qui traduit l'ancienne expression " fonction en forme " par opposition "fonction en valeur ", qui en sont les diverses spcialisations), et nous verrons dans les paragraphes ultrieurs des proprits que l'on peut tirer de ses spcialisations. Elle est, entre autres, l'outil technique permettant d'identifier la classe de conjugaison du groupe de Galois d'un polynme donn.

On considre n indtermines $x_1, \ldots, x_n$ 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 symtriques lmentaires 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 $\mathcal{K}$-algbre 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 reprsentation par permutations $\mathrm{Gal}(\mathcal{F}/\mathcal{K}) \to \mathfrak{S}_n$ associe la numrotation $(x_i)_{1 \leq i \leq n}$ est un isomorphisme de groupes ; et que $\mathcal{A}$ est la clture intgrale de $\mathcal{S}$ dans $\mathcal{F}$.

Ci-aprs nous identifierons les groupes $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$ et $\mathfrak{S}_n$ l'aide de la reprsentation 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 clture intgrale $\mathcal{A}_H$ de $\mathcal{S}$ dans $\mathrm{Inv}(H)$ est $\mathcal{A} \cap \mathrm{Inv}(H)$. L'anneau $\mathcal{A}_H$ est intgralement clos, noethrien et c'est une k-algbre de type fini. Puisque $\mathcal{S}$ est noethrien et intgralement clos, on en dduit que $\mathcal{A}_H$ est un $\mathcal{S}$-module de type fini. En d'autres termes, $\sigma_1, \ldots, \sigma_n$ est un *systme homogne de paramtres* au sens de Stanley (voir [Stanley]) pour la k-algbre $\mathcal{A}_H$. 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 caractristique 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 dcoule de ce que $(\sigma_1, \ldots, \sigma_n)$ est un systme homogne de paramtres de $\mathcal{A}_H$. (voir [Stanley]).

Le rang r de ce module est videmment $r = \dim_{|\mathcal{K}}(\mathcal{K} \bigotimes_{\mathcal{S}} \mathcal{A}_H)$. 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'aprs la thorie de Galois, on a bien $r = \dim_{\mathcal{K}}(\mathrm{Inv}(H)) = [\mathfrak{S}_n : H]$ $\square$

On peut construire concrtement une base du $\mathcal{S}$-module $\mathcal{A}_H$ de la manire suivante : notons $\mathfrak{I}_H$ l'idal de $\mathcal{A}_H$ engendr par $\sigma_1, \ldots, \sigma_n$. On sait (voir [Stanley]) que des lments homognes $\eta_1, \ldots, \eta_e$ 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 homognes de degr m de $\mathfrak{I}_H$ et $\mathcal{A}_H$; soit $\mathfrak{I}$ l'idal de $\mathcal{A}$ engendr par $(\sigma_1,\dots,\sigma_n)$ et $\mathfrak{I}_m$ la composante homogne de degr 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 $(P_\alpha)_{\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n,\alpha_1<1,\dots,\alpha_n<n} = (x_1^{\alpha_1}\cdots x_n^{\alpha_n})_{\alpha_1<1,\dots,\alpha_n<n}$ tant une base de $\mathcal{A}$ comme $\mathcal{S}$-module et de $\mathcal{A}/\mathfrak{I}$ comme k-espace vectoriel. Supposons toujours la caractristique 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 engendr par les lments homognes de degr m du type $\sum_\alpha \eta_\alpha\hat{P}_\alpha$, o $\eta_\alpha \in k[\sigma_1,\dots,\sigma_n]$ est un polynme sans terme constant en les σ_i, tandis que $(\mathcal{A}_H)_m$ est engendr par les $\sum_\alpha \eta_\alpha\hat{P}_\alpha$, o $\eta_\alpha \in k[\sigma_1,\dots,\sigma_n]$ est un polynme homogne en les x_i tel que $\deg(\eta_\alpha P_\alpha) = m$ (voir [Stanley]).

Existence d'lments primitifs homognes

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 prcisment, comme nous l'avons vu juste avant le Thorme 4.1, on a : $\mathrm{Inv}(H) \cong \mathcal{K}\bigotimes_{\mathcal{S}}\mathcal{A}_H$. Comme $\mathrm{Inv}(H)$ est sparable sur $\mathcal{K}$, il admet des lments $\mathcal{K}$-primitifs. Donc il existe des lments $\Psi \in \mathcal{A}_H$ qui sont $\mathcal{K}$-primitifs pour le corps $\mathrm{Inv}(H)$. En fait il existe toujours de tels lments qui soient homognes, pourvu que k soit infini. En effet, soit $\Psi \in \mathcal{A}_H$ lment $\mathcal{K}$-primitif de degr d ; soit λ une indtermine sur $\mathcal{K}$, notons Ψ_λ l'homognis de Ψ par $\lambda\sigma_1$:

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

Soit $(t_i)_{1\leq i\leq e}$ une transversale 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 polynme minimal de Ψ sur $\mathcal{K}$. Donc $\mathcal{D}(\lambda)\neq 0$. Le corps k tant infini, on a $\tilde{\lambda}\in k$ tel que $\mathcal{D}(\tilde{\lambda})\neq 0$, d'o alors $\Theta = \Psi_{\tilde{\lambda}}$ est encore $\mathcal{K}$-primitif, est homogne de degr d et $\mathcal{L}_\Theta = P_{\tilde{\lambda}}(x)$ est le polynme 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 lment $\Psi\in\mathrm{Inv}(H)$ qui est $\mathcal{K}$-primitif et qui appartient $\mathcal{A}_H$ est appel un *rsolvant* de H. Un tel rsolvant est dit *homogne* ssi c'est un polynme homogne des x_i. Le polynme $\mathcal{K}$-minimal d'un tel rsolvant Ψ sera appel *rsolvante de Lagrange* de H associes Ψ et not $\mathcal{L}_\Psi$: on a donc $\mathcal{L}_\Psi\in\mathcal{S}[x]$.

D'aprs la thorie de Galois, tant donn $\Psi\in\mathcal{A}$, si on pose $H = \mathrm{Stab}_{\mathfrak{S}_n}(\Psi)$, alors Ψ est un rsolvant de H.

Remarque 3. Il existe un algorithme paralllisable (voir [avb1] page 99) permettant de calculer le polynme minimal d'un nombre algbrique obtenus par une relation algbrique entre les racines de polynmes d'une variable donns. Cet algorithme s'optimise grce au Thorme de l'arit (voir [avb2] ou [avb1]). Cet algorithme tait utilis par Lagrange (voir par exemple [Lagrange, tome VIII] page 236, le calcul d'une rsolvante produit) pour calculer des rsolvantes particulires ; c'est pourquoi nous proposons de l'appeler *Algorithme de Lagrange*. Dans [Arnaudis-Valibouze] nous donnons diverses formules et amliorations de cet algorithme qui ainsi le rendent praticable. Par exemple nous savons calculer en degr 8, avec les rsolvants $\prod_{1\leq i<j\leq k}(x_i - x_j)$ pour $k = 3, 7$ ($k = 8$ fournit le discriminant), ou bien $x_1x_2\ldots x_i + x_{i+1}$, $1 \leq i \leq 7$ (pour $i = 3$, le degr de la rsolvante est 280). Toutes ces rsolvantes sont accessibles dans la dernire version du systme de calcul formel [MAXIMA]. Ainsi, il existe bon nombre de rsolvantes, plus facilement calculables que factorisables.

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

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

Démonstration. (d'aprs Lagrange) Soit $e = [\mathfrak{S}_n : H]$ et $\{t_i\}_{1\leq i\leq e}$ une transversale de $\mathfrak{S}_n$ mod H, avec $t_1 = \mathrm{Id}_{\mathfrak{S}_n}$. Posons $\Psi_i = t_i \star \Psi$ (donc $\Psi = \Psi_1$), d'o $\mathcal{L}_\Psi = \sum_{i=1}^{e}(x - \Psi_i) = x^e - C_1x^{e-1} + \cdots + (-1)^eC_e$ ($\mathcal{L}_\Psi \in \mathcal{S}[x]$). (Notons que $\mathcal{L}_\Psi$ est thoriquement calculable l'aide du thorme fondamental sur les fonctions symtriques.)

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 thoriquement calculable). On considre (15) comme un systme de Cramer en les g_j. La rsolution donne :

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

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

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

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

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 symtrique en $T_2, \dots, T_e$ (c'est vident sur δ_Ψ et sur $\mathcal{D}$).

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

Remarque 4. *Analyse de la dmonstration du Thorme* 4.3 : Cette dmonstration est en substance celle donne par Lagrange dans ses Rflexions sur la rsolution des quations algbriques. Il est intressant de la situer par rapport la thorie moderne des corps ; pour cela, conservons-en toutes les notations. Le corps $\mathrm{Inv}(H)$ est une extension finie sparable 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 $\frac{p(x)}{x-\Psi} = \alpha_0 + \alpha_1 x + \dots + \alpha_{e-1}x^{e-1}$. Soit Tr la trace de $\mathrm{Inv}(H)$ relativement $\mathcal{K}$. 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'aprs le Thorme d'Euler bien connu, la base complmentaire de $\mathcal{B}$ dans $\mathrm{Inv}(H)$ est $(\alpha_i/p'(\Psi))_{1\le i\le e-1}$, c'est--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'o l'on dduit classiquement (puisque $\mathcal{A}_H$ est la clture intgrale 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'lment de $\mathrm{Hom}_\mathcal{K}(\mathrm{Inv}(H))$ dfini 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 coefficients dans $\mathcal{S}$. Les formules de Cramer permettent donc partir de : $u(\mathcal{A}_H) \subset \mathcal{S}[\Psi]$, de dduire que $\det(u)\mathcal{A}_H \subset \mathcal{S}[\Psi]$. Mais en notant $\mathcal{N}$ la norme de $\mathrm{Inv}(H)$ relative $\mathcal{K}$, on a : $\det(u) = \mathcal{N}(\eta) = (1-)^{e(e-1)/2}\Delta_\Psi$, ce qui redmontre que $\Delta_\Psi\mathcal{A}_H \subset \mathcal{S}[\Psi]$.

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

Spcialisation d'une rsolvante

Dans ce sous-paragraphe, nous fixons un polynme $f \in k[x]$, de degr $n \ge 1$, sparable, normalis, et nous notons E la k-algbre de ses racines dans $\hat{k}$. On numrote 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 hypothses de la Dfinition 4.2. Posons :

$$f = x^n - c_1x^{n-1} + \dots + (-1)^n c_n \qquad ; \tag{18}$$

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

Les rsolvantes les plus commodes utiliser sont les rsolvantes sparables. 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 rsolvant $\Psi \in A[x_1, \dots, x_n]$ de H tel que $\mathcal{L}_{\Psi,f}$ soit sparable, et on peut choisir Ψ homogne.*

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

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

les φ_C $(C \in \mathcal{H})$ sont aussi deux 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 lments $(\varphi_C(u_1, \dots, u_n))_{C\in\mathcal{H}}$ soient distincts. Pour un tel choix de $(u_1, \dots, u_n)$ posons :

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

on a : $\Psi \in \mathrm{Inv}(H) \cap A[x_1, \dots, x_n]$. Les conjugus 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'aprs le choix des u_i, ces conjugus sont distincts, donc Ψ est un rsolvant de H. Il est clair que

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

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

Pour obtenir un rsolvant homogne, raisonnons comme nous l'avons fait prcdemment. Soit λ une indtermine sur $\mathcal{F}$. Posons $(\Psi_C)_\lambda$ l'homognis 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 spcialisant 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'aprs ce qu'on vient de voir. Posons, aprs avoir fix un tel $\tilde\lambda$:

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

Alors $\Theta \in \mathrm{Inv}(H) \cap A[x_1, \dots, x_n]$; Θ est homogne de degr $\deg(\Psi)$ (=card(H)) en les x_i. Les conjugus 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 $\rho_1, \dots, \rho_n$ $x_1, \dots, x_n$ 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 ncessairement tous distincts, ce qui prouve que Θ est un rsolvant de H, et d'autre part le polynme $\mathcal{L}_{\Theta,f}$ est sparable, i.e. ce rsolvant est sparable $\square$

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

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

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

on a une reprsentation naturelle de $\mathfrak{S}_n$ par permutations de $\{\Psi_1, \dots, \Psi_e\}$, qui est fidle et transitive, et qui associe 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 reprsentation, alors Γ_n est l'image naturelle dans $\mathfrak{S}_e$ de $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$, i.e. de la $\mathcal{K}$-algbre des racines dans $\mathcal{F}$ du polynme $\mathcal{L}_\Psi$. Puisque les lments $(\sum_{i=1}^{e} a_i \Psi_{s(i)})_{s \in \Gamma_n}$ de $\mathcal{F}$ sont distincts, on voit que $\Phi = \sum_{i=1}^{e} a_i \Psi_i$ est lment primitif de $\mathcal{F}$ sur $\mathcal{K}$. D'aprs le Thorme 4.3, appliqu avec $H = \{1\}$, et avec le rsolvant Φ de ce H, on a (puisque $\mathcal{A}_{\{1\}} = \mathcal{A}$) : $\mathcal{A} \subset \frac{1}{\Delta_\Phi}\mathcal{S}[\Phi]$, o Δ_Φ est le x-discriminant du polynme

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

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

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

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

(o $\epsilon = (-1)^{n!(n!-1)/2}$). Par le choix mme de Φ, on a $\tilde{\Delta}_\Phi \neq 0$. En spcialisant 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'o $E = (= k[\rho_1, \dots, \rho_n]) = k[\tilde{\Psi}_1, \dots, \tilde{\Psi}_e]$ $\square$

Remarque 5. Ce Thorme 4.6 amliore le rsultat donn par [Dickson] pages 190 et suivantes ; les groupes nots G et Γ dans cette rfrence sont respectivement $\mathrm{Gal}(f/k)$ et $\mathrm{Gal}(\mathcal{L}_{\Psi,f}/k)$, et Dickson dit que " G est simplement ou multiplement isomorphe Γ, et donc que $\mathrm{card}(G) \geq \mathrm{card}(\Gamma)$. ".

Remarque 6. Sous les hypothses du Thorme 4.6, Soit $P_1 P_2 \ldots P_r$ une dcomposition dans $k[x]$ en facteurs irrductibles normaliss 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 $\mathrm{Gal}(E/k)$:

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

o K_i dsigne le corps des racines de $P_1 P_2 \ldots P_i$ dans E $(1 \leq i \leq r)$. Cette tour donne videmment, 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 Thorme 4.6 est trs utile pour construire des polynmes particuliers de groupe de Galois donn. On en verra plus loin quelques exemples.

5. Rsolvantes et idaux de $k[x_1, \ldots, x_n]$

Reprenons les notations du §4. Nous utiliserons ci-dessous la terminologie et les rsultats de [Arnaudis] relatifs aux varits de dimension zro. (Rappelons que selon cette terminologie, le mot varit dsigne des ensembles de points.) Donc nous supposerons ici que k est de caractristique nulle. Nous noterons : $\hat{\mathcal{A}} = \hat{k} \bigotimes_k \mathcal{A}$; $\mathfrak{I}$ l'idal de $\mathcal{A}$ engendr par $\{\sigma_1 - c_1, \ldots, \sigma_n - c_n\}$ dit *idal des relations symtriques* ; $\hat{\mathfrak{I}} = \hat{k} \bigotimes \mathfrak{I}$ l'idal de $\hat{\mathcal{A}}$ engendr par $\{\sigma_1 - c_1, \ldots, \sigma_n - c_n\}$; $\mathcal{W}$ la varit de dimension zro dfinie par $\hat{\mathfrak{I}}$ dans $\hat{k}^n$; $\Gamma = \mathrm{Gal}(E/k)$; $N = \mathrm{card}(\Gamma)$. Dans [Mach-Valibouze] on trouvera une formule close donnant une base standard de l'idal $\mathfrak{I}$ relativement l'ordre lexicographique.

On a une reprsentation par permutations fidle $R : \Gamma \to \mathfrak{S}_n$ qui associe, tout lment $u \in \Gamma$, 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 un sous-groupe de $\mathfrak{S}_n$ l'aide de R. Cette identification sera systmatiquement utilise par la suite. Notons ici que pour tout $g \in \mathcal{A}$ et tout $s \in \Gamma$, on a :

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

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

La varit $\mathcal{W}$

Il est clair que $\mathcal{W} = \{(\rho_{s(1)}, \ldots, \rho_{s(n)})\}_{s \in \mathfrak{S}_n}$; 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 dcomposition en facteurs irrductibles de $k[T, U]$ est $\Psi_{\mathcal{W}}(T, U) = \prod_{C \in \mathcal{H}} P_C$, o $\mathcal{H} = (\mathfrak{S}_n/\Gamma)_d$ et o, pour tout $C \in \mathcal{H}$, on a pos $P_C = \prod_{s \in C}(T - \sum_{i=1}^{n} U_i \rho_{s(i)})$.

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

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

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 engendr par les reprsentants des $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ pour $\alpha_1 < 1, \ldots, \alpha_n < n$ (c'est une consquence facile des formules de Girard-Newton, ou d'une base standard de $\mathfrak{I}$ donne dans [Mach-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 dduit 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-rsultant 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 varit $\mathcal{T}_C$, $C \in \mathcal{H}$. Pour chaque $C \in \mathcal{H}$, l'idal $\mathfrak{M}_C = \{g \in \mathcal{A} \mid g = 0 \text{ sur } \mathcal{T}_C\}$ de $\mathcal{A}$ est maximal, et dfinit la varit $\mathcal{T}_C$, et on a $E \cong \mathcal{A}/\mathfrak{M}_C$. Les $\mathfrak{M}_C$ sont les idaux premiers associs $\mathfrak{I}$ 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 $\mathfrak{N} = \{g \in \mathcal{A} \mid g(\rho_1, \ldots, \rho_n) = 0\}$ dit *idal des relations entre les racines de f*.) On voit comme ci-dessus que pour chaque $C \in \mathcal{H}$, le U-rsultant de $\mathfrak{M}_C$ est P_C, la forme fondamentale de $\mathcal{T}_C$.

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

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

Démonstration. Notons $\mathfrak{a}$ l'idal de $\mathcal{A}$ engendr par $\{\sigma_1 - c_1, \ldots, \sigma_n - c_n, g\}$. Les hypothses entranent $\mathcal{V}(\mathfrak{a}) = \mathcal{V} = \mathcal{V}(\mathfrak{N})$, d'o :

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

pour tout $l \in \mathbb{N}$, les idaux $\mathfrak{N}^l$ et $J = \bigcap_{C\in\mathcal{H}\,,\,C\neq\Gamma}\mathfrak{M}_C$ de $\mathcal{A}$ sont comaximaux. Choisissons $l \in \mathbb{N}$ de faon que $\mathfrak{N}^l \subset \mathfrak{a}$, ce qui est possible car $\mathfrak{N} = \sqrt{\mathfrak{a}}$ et car $\mathcal{A}$ est noethrien. 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'o $x \in \mathfrak{a}$. Donc $\mathfrak{N} = \mathfrak{a}$ □

Commentaires sur le Thorme 5.1

Ce thorme est implicitement latent dans toute la littrature ancienne sur la thorie de Galois.

Application du Thorme 5.1 aux rsolvantes

Théorème 5.2. *Soit Θ un rsolvant 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 rsolvante $\mathcal{L}_{\Theta,f}$, 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'idal $\mathfrak{N}$ est engendr par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n, \Theta - \theta\}$.*

Démonstration. Notons $g \mapsto \tilde{g}$ le morphisme de k-algbre $\mathcal{A} \to E$, $g \mapsto g(\rho_1, \dots, \rho_n)$. 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'o $\theta \in k$.

b) Soient $\Theta_1 = \Theta, \Theta_2, \dots, \Theta_\nu$ les conjugus 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 hypothse $\theta_i \neq \theta_1 = \theta$ 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--dire $s \in H$; d'o $\Gamma \subset H$.

c) D'aprs les hypothses, on a $\theta \in k$. d'aprs le Thorme 5.1, pour que l'idal $\mathfrak{N}$ soit engendr 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 engendr par $\{\sigma_1 - c_1, \dots, \sigma_n - c_n, \Theta - \theta\}$ " quivaut " $s \in \mathfrak{S}_n \backslash \Gamma$ implique $s \notin H$ ", c'est--dire $H \subset \Gamma$. Comme on a dj $\Gamma \subset H$, en fin de compte cette condition quivaut : $\Gamma = H$ □

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

Théorème 5.3. *Soit Θ un rsolvant d'un sous-groupe H de $\mathfrak{S}_n$. Posons $\theta = \Theta(\rho_1, \dots, \rho_n)$, notons $\Theta_1, \dots, \Theta_\nu$ les conjugus 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 rsolvante $\mathcal{L}_{\Theta,f}$; soit h le facteur normalis irrductible dans $k[x]$ de $\mathcal{L}_{\Theta,f}$ qui s'annule en θ. Supposons la numrotation (Θ_i) choisie pour que $h(x) = (x - \widetilde{\Theta_1}) \cdots (x - \widetilde{\Theta_r})$ $(1 \leq r \leq \nu)$, notons $S = Stab_{\mathfrak{S}_n}(\{\Theta_1, \dots, \Theta_r\})$. 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'idal $\mathfrak{N}$ est engendr 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 irrductible dans $k[x]$. Alors $\widetilde{\gamma\Theta} = \gamma(\tilde{\Theta}) = \widetilde{\Theta_i}$, ce qui force $\gamma.\Theta = \Theta_i$ pour les mmes 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 (d ce que $s \in \Gamma$) que $s(\widetilde{\Theta_i}) = \widetilde{s.\Theta_i}$, on dduit que $\widetilde{s.\Theta_i} \in \{\widetilde{\Theta_1}, \dots, \widetilde{\Theta_r}\}$ par le mme argument qu'en a), d'o $s(\Theta_i) \in \{\Theta_1, \dots, \Theta_r\}$, d'o $s \in S$. 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'o $r = [\Gamma : \Gamma \cap H] = [S : S \cap H]$, d'o $[S : \Gamma] = [S \cap H : \Gamma \cap H]$.

c) Il est clair que $h(\Theta)$ est nul sur $\mathcal{T}_\Gamma$. D'aprs le Thorme 5.1, pour que l'idal $\mathfrak{N}$ soit engendr 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--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'crit : $h(\widetilde{s.\Theta}) \neq 0$ 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 vrifient $s.\Theta \in \{\Theta_1, \dots, \Theta_r\}$, i.e. les lments de $\bigcup_{i=1}^{r} C_i$. Donc $\mathfrak{N}$ est engendr par $\mathcal{G}$ ssi $s \in \mathfrak{S}_n \backslash \Gamma$ puisque $s \notin \bigcup_{i=1}^{r} C_i$, c'est--dire ssi $\bigcup_{i=1}^{r} C_i \subset \Gamma$, et d'aprs b) cette condition quivaut bien : $\Gamma = S = \bigcup_{i=1}^{r} C_i$ $\square$

Sous les hypothses du Thorme 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'o $s \in S$ puisque h est facteur simple de la rsolvante $\mathcal{L}_{\Theta,f}$.

6. Rsolvantes de Lagrange et groupes de Galois

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

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

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 dduit : $\widetilde{g.\Theta} = \tilde{\Theta} = \theta = g(\tilde{\Theta}) = g(\theta)$. Donc, $\Gamma \cap H \subset \mathrm{Stab}_\Gamma(\theta)$. Si $g \in \Gamma \backslash H$, alors $\Theta' = g.\Theta$ est un conjugu de Θ dans $\mathcal{F}$ sur $\mathcal{K}$ distinct de Θ. Donc puisque θ est racine simple de $\mathcal{L}_{\Theta,f}(x) = \prod(x - \tilde{\Psi})$, o le produit est tendu aux Ψ conjugus de Θ dans $\mathcal{F}$ sur $\mathcal{K}$, on a $\theta' = \tilde{\Theta}' \neq \theta$, d'o $\theta' = \widetilde{\Theta'} = \widetilde{g.\Theta} = g(\tilde{\Theta}) = g(\theta) \neq \theta$, i.e. $g \notin \mathrm{Stab}_\Gamma(\theta)$. En dfinitive, $\mathrm{Stab}_\Gamma(\theta) = \Gamma \cap H$ □

Corollaire 6.2. *Dans les conditions du thorme* 6.1*, le degr du polynme minimal de θ sur k est* $[\Gamma : \Gamma \cap H]$.

Théorème 6.3. *Soit Θ un rsolvant d'un groupe H de $\mathfrak{S}_n$; posons $\theta = \tilde{\Theta}$. Supposons que θ soit une racine de multiplicit 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 $L = Stab_{\mathfrak{S}_n}(\{\Theta_1, \ldots, \Theta_\nu\})$. On a : $Gal(E/k(\theta)) = Stab_\Gamma(\theta) = \Gamma \cap L$; 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--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'o $\mathrm{Gal}(E/k(\theta)) = \mathrm{Stab}_\Gamma(\theta) = \Gamma \cap L$. En particulier si $g.\Theta_1 = \Theta_1$, i.e. si $g \in H$, alors $g \in L$, d'o $\Gamma \cap H \subset \Gamma \cap L$. En faisant oprer $\Gamma \cap L$ sur $\{\Theta_1, \ldots, \Theta_\nu\}$, on voit que le stabilisateur de Θ_1 dans $\Gamma \cap L$ est $\Gamma \cap H$ cause de ce qui prcde. D'o $[\Gamma \cap L : \Gamma \cap H] = \mathrm{card}(\mathrm{Orb}_{\Gamma \cap L}(\Theta)) \leq \mathrm{card}(\mathrm{Orb}_L(\Theta)) = \nu$; d'autre part, $[\Gamma : \Gamma \cap L] = [k(\theta) : k]$, d'o enfin $[\Gamma : \Gamma \cap H] = [\Gamma : \Gamma \cap L]\,[\Gamma \cap L : \Gamma \cap H] \leq [k(\theta) : k]\,\nu$ □

De la dmonstration ci-dessus, il se dgage immdiatement :

Corollaire 6.4. *Avec les notations et hypothses du Thorme* 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 rsout la question des conditions imposes au groupe de Galois Γ par l'existence de relations algbriques entre les racines de f. De faon prcise, supposons connu un lment $\Psi \in k[x_1, \ldots, x_n]$ tel que $\Psi(\rho_1, \ldots, \rho_n) = 0$. Formons la rsolvante $\mathcal{L}_{\Psi,f}(x) = \prod_{i=1}^{m}(x - \tilde{\Psi}_i)$, o $\mathcal{L}_\Psi = \prod_{i=1}^{m}(x - \Psi_i)$, $\Psi_1 = \Psi$, $m = [\mathfrak{S}_n : \mathrm{Stab}_{\mathfrak{S}_n}(\Psi)]$. Soit J l'ensemble des $i \in [1, m]$ tels que $\widetilde{\Psi_i} = 0$. Alors d'aprs le corollaire du Thorme 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 Thorme 6.3. Dsignons par $C_1, \dots, C_e$ les classes gauche de $\mathfrak{S}_n$ mod H, ordonnes de faon 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 Thorme 6.3 en introduisant un deuxime rsolvant Ψ de H. Notons Ψ_i la valeur commune des $\sigma.\Psi$ pour $\sigma \in C_i$ $(1 \leq i \leq e)$. Deux facteurs normaliss F et G de $\mathcal{L}_{\Theta,f}$ et $\mathcal{L}_{\Psi,f}$ respectivement seront dits *parallles* ssi on a une mme 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 rsolvante est f-sparable, J est alors unique.

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

Notons h l'lment irrductible dans $k[x]$ et normalis 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 $\theta_1, \dots, \theta_d$ sont les Γ-conjugus de θ). Soit $\mathcal{R} = \{\Theta_1, \dots, \Theta_e\}$ 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 cause du Thorme 6.3 $d = [\Gamma : \Gamma \cap \mathrm{Stab}_{\mathfrak{S}_n}(\mathcal{R}_i)]$.

De plus $\mathcal{R}_1 = \{\Theta_1, \dots, \Theta_\nu\}$. 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 dpendant que de O tel que $m_O = \mathrm{card}(O \cap \mathcal{R}_i)$ pour tout i, et qui est, par application du Thorme 6.3, donn 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 systme $(O \cap \mathcal{R}_i)_{1 \leq i \leq d}$ est un systme de blocs de primitivit 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 dfinition, le facteur parallle 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 polynme $P_O(x) = \prod_{j \in J_O}(x - \widetilde{\Psi_j})$ appartient $k[x]$, et c'est un facteur normalis irrductible dans $k[x]$ de $\mathcal{L}_{\Psi,f}$, dont le degr est $d.m_O$. Nous en dduisons le rsultat suivant :

Théorème 6.5. ***Thorme des multiplicits*** *Dans les conditions ci-dessus, le facteur irrductible de $\mathcal{L}_{\Psi,f}$ parallle h^ν est $\prod_{O \in \mathcal{O}} P_O$, o pour chaque $O \in \mathcal{O}$, le polynme $P_O(x)$ est un facteur irrductible dans $k[x]$ de $\mathcal{L}_{\Psi,f}(x)$ dont le degr $d.m_O$ est un multiple du degr $d = deg(h)$.*

(L'ide de comparer un rsolvant sparable un rsolvant quelconque apparat dj dans Lagrange [Lagrange, tome IV] ; nous y reviendrons au §10 ci-aprs).

Remarque 8. Ce thorme revt une importance pratique certaine. En effet, le calcul effectif des rsolvantes dans des cas numriques amne trs frquemment des facteurs multiples, surtout pour les polynmes " petit " groupe de Galois. Ce thorme, ainsi que le Thorme 6.6 ci-dessous permettront nanmmoins d'en dduire des renseignements qui peuvent dispenser de chercher des rsolvantes sparables. Par exemple, supposons que le calcul d'une rsolvante par Θ, y rvle un facteur P^2 o $\deg(P) = 12$ et $P(x)$ irrductible dans $k[x]$; alors on en dduira que pour tout rsolvant f-sparable Ψ du mme groupe que Θ, la factorisation de $\mathcal{L}_{\Psi,f}$ fera apparaitre soit au moins 2 facteurs de degr 12, soit au moins un de degr 24.

Dans ce qui suit, sur $\mathbb{N}^r$ (o $r \in \mathbb{N}^\star$) nous utiliserons l'ordre naturel produit, not $\preceq$, et ainsi dfini : 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 mme entier $m \geq 1$ vrifient $a \preceq b$, alors $a = b$.

Nous rappelons que ϖ dsigne la matrice des partitions dfinie au §3.

Théorème 6.6. *Soit Θ un rsolvant d'un sous-groupe H de $\mathfrak{S}_n$. Supposons que tous les facteurs irrductibles de $\mathcal{L}_{\Psi,f}$ soient sparables. 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 irrductibles simples de $\mathcal{L}_{\Theta,f}$ de degr j ; alors*

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

si $\mathcal{L}_{\Theta,f}$ est sparable (i.e. si Θ est f-sparable), 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 commodit, $\gamma_1 =$Id, l'lment neutre de $\mathfrak{S}_n$, d'o $H_1 = H$ 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-irrductible simple de degr 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'aprs le corollaire du Thorme 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'aprs ce qu'on vient de voir, on a : $j\alpha_j \leq N_j$. Or par dfinition (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 sparable, 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 cause de (27), elles sont gales. $\square$

Mthode de la chasse aux rsolvantes

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, o $e_j = [\mathfrak{S}_n : H_j]$, de faon que γ_m =Id, l'lment neutre de $\mathfrak{S}_n$.

Choisissons un rsolvant de H_j, not Θ_j. Posons $\Theta_{j,m} = \gamma_m.\Theta_j$ $(1 \leq m \leq e_j)$, de sorte que $\Theta_{i,1} = \Theta_i$, $\mathcal{L}_{\Theta_j} = \prod_{m=1}^{e_i}(x - \Theta_{j,m})$.

Si $\mathcal{L}_{\Theta_j,f}$ est sparable, nous noterons $\pi(\Theta_j, f)$ la partition $(\alpha_{j,1}, \ldots, \alpha_{j,e_j})$ de e_j, o $\alpha_{j,p}$ est le nombre de facteurs irrductibles de degr p sur k de $\mathcal{L}_{\Theta_j,f}$. En combinant les Thormes 3.1 et 6.6, on arrive au thorme principal que nous avions en vue :

Théorème 6.7. *Avec les notations ci-dessus, supposons que tous les rsolvants Θ_i $(1 \leq i \leq s)$ soient sparables. Alors la classe de conjugaison $\mathcal{G}$ du groupe de Galois Γ = Gal(E/k) est $\mathcal{G} = \mathcal{C}_r$, o 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 $\mathfrak{S}_n$ concide avec la ligne $(\pi(\Theta_1, f), \pi(\Theta_2, f), \ldots, \pi(\Theta_s, f))$.*

Le Thorme 6.7 donne une mthode effective pour calculer la classe de conjugaison $\mathcal{G}$: on dtermine la matrice des partitions $\mathcal{P}$ (par exemple le logiciel G.A.P. permet aisment de calculer une intersection de groupes ainsi que l'indice d'un groupe dans un autre) ; on calcule ensuite, si c'est possible, des rsolvants f-sparables Θ_j $(1 \leq j \leq s)$, on factorise les $\mathcal{L}_{\Theta_j,f}$ dans $k[x]$, on en dduit les partitions $\pi(\Theta_j, f)$ et on applique enfin le Thorme 6.7. Si k est infini, l'existence de rsolvantes f-sparables Θ_j est assure d'aprs le Thorme 4.5.

Lorsqu'on appliquera cette mthode, les groupes H_j ci-dessus introduits seront appels les *groupes tests*, et les classes $\mathcal{C}_i$ parmi lesquelles on recherche $\mathcal{G}$ seront appeles *classes candidates*, le mot “ groupe ” tant ici entendu conjugaison prs dans $\mathfrak{S}_n$.

Dans la pratique, il n'est pas ncessaire de calculer toutes les rsolvantes $\mathcal{L}_{\Theta_j,f}$. En effet pour r fix $(1 \leq r \leq s)$, 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 $[1, s]$ *dpartage* $\mathcal{C}_r$ ssi $\bigcap_{j \in J_r} \mathcal{U}_{r,j} = \{r\}$. Pour dterminer $\mathcal{G}$, il suffit pour chaque r de calculer les rsolvantes $\mathcal{L}_{\Theta_j,f}$ pour j parcourant une partie J_r qui dpartage $\mathcal{C}_r$. Le Thorme 6.7 assure que $[1, s]$ dpartage chaque $\mathcal{C}_r$; appelons *systme sparant* de parties de $[1, s]$ toute famille $(J_r)_{1 \leq r \leq s}$ de parties de $[1, s]$ telles que J_r dpartage $\mathcal{C}_r$ pour tout r, et appelons *support* d'un tel systme l'ensemble $J = \bigcup_{r=1}^{s} J_r$. Dans tous les cas numriques, on pourra calculer $\mathcal{G}$ en ne calculant que les rsolvantes $\mathcal{L}_{\Theta_j,f}$ pour j dcrivant le support d'un quelconque systme sparant, pourvu que ces $\mathcal{L}_{\Theta_j,f}$ soient sparables. On choisira alors les systmes conduisant aux calculs les plus rapides. Notons ici que ce ne sont pas forcment les rsolvantes de plus bas degr qui conduisent aux calculs les plus rapides. Il existe des rsolvantes de degr assez lev dont le calcul est quasiment immdiat (voir [Arnaudis-Valibouze]).

En rsum, l'utilisation optimale du Thorme 6.7 consiste en premier lieu reprer les classes $\mathcal{C}_j$ conduisant aux calculs les plus rapides des rsolvantes $\mathcal{L}_{\Theta_j,f}$; puis former des systmes sparants utilisant le maximum de classes $\mathcal{C}_j$ ainsi repres, et enfin en dduire $\mathcal{G}$.

Pour exposer la mthode nous allons dtailler l'exemple du cas o $n = 4$, en supposant k de caractristique $\neq 2$ et $\neq 3$.

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

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

Reprsentants	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	$\mathcal{D}_4$ (didral)
$H_{10} = G_4$	[(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 dsignent les reprsentants des classes de sous-groupes transitifs.

Table 2 : rsolvants 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	$\Theta_6 = x_1x_2 + x_2x_4 - x_1x_2 - x_3x_4$
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 indiqu prcdemment, nous calculons la matrice des partitions ci-dessous, o l'on convient, pour d'abrger, de noter $d_1^{\nu_1} \cdots d_r^{\nu_r}$ la partition $[(\nu_1, d_1), \ldots, (\nu_r, d_r)]$:

Table 3 : transpose 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 premire ligne sont les candidats et ceux de la premire colonne sont les groupes test.)

L'examen de la table 3 montre que le rsolvant Θ_9, classiquement utilis en degr 4, et qui prsente le srieux avantage que $\mathcal{L}_{\Theta_9,f}$ est toujours sparable si f l'est, n'est pourtant pas bon du point de vue du Thorme 6.7, car il dpartage trs peu. En revanche, le couple (Θ_2, Θ_{10}) suffit dpartager tous les groupes possibles sous la seule rserve que $\mathcal{L}_{\Theta_2,f}$ soit sparable. En effet $\mathcal{L}_{\Theta_{10}} = x^2 - \Delta$, o $\Delta = \prod_{1 \leq i < j \leq 4}(x_j - x_i)^2 \in \mathcal{S}$ est le discriminant gnrique de degr 4, et puisque la caractristique est $\neq 2$, pour tout f sparable $\mathcal{L}_{\Theta_{10},f} = x^2 - \tilde{\Delta}$ l'est aussi puisque $\tilde{\Delta} \neq 0$.

Or nous verrons plus loin que pour f donn numriquement, le calcul de $\mathcal{L}_{\Theta_2,f}$ est extrmement rapide. Le calcul de $\tilde{\Delta}$, lui, est instantan. En rsum, si $\mathcal{L}_{\Theta_2,f}$ est sparable, 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 rsolvante $\mathcal{L}_{\Theta_2,f}$. Il importe ici de noter qu'il n'est pas ncessaire de calculer la rsolvante formelle $\mathcal{L}_{\Theta_2}$ pour obtenir numriquement $\mathcal{L}_{\Theta_2,f}$: cette remarque est essentielle pour l'efficacit de la mthode du Thorme 6.7 (en fait, le calcul automatique de $\mathcal{L}_{\Theta_2,f}$ est instantan).

Observons encore :

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

Remarque 10. que pour appliquer le Thorme 6.7, il n'est pas ncessaire d'ordonner les classes de conjugaison de sous-groupes de $\mathfrak{S}_n$ par degrs dcroissants ni dans un ordre particulier pour crire la matrice des partitions. On peut aussi travailler sur la transpose de cette matrice.

Remarque 11. que si l'on sait l'avance que f est irrductible, il n'est pas ncessaire d'tudier la matrice des partition $\mathcal{P}$ complte ; en effet le groupe $\Gamma = \mathrm{Gal}(E/k)$ tant alors un sous-groupe transitif de $\mathfrak{S}_n$, il suffit dans ce cas de considrer la sous-matrice de $\mathcal{P}$ forme avec les lignes qui correspondent aux classes de conjugaison de sous-groupes transitifs de $\mathfrak{S}_n$. Toutes les mthodes exposes ci-dessus s'appliquent alors de faon analogue avec cette seule sous-matrice.

Rsolvantes 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 tre obtenu par exemple l'aide du Thorme 5.2 b) lorsqu'on aura calcul suffisamment de rsolvantes. 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 lment $\lambda \in \mathcal{A}_{L_0}$, 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 sparable de degr $e = [L_0 : H]$ de $\mathrm{Inv}(L_0)$. Il existe des lments primitifs de cette extension qui appartiennent $\mathcal{A}_H$, et mme des lments primitifs homognes, lorsque k est infini : par exemple tout rsolvant homogne de H est un tel lment.

Définition 6.8. Avec les hypothses et notations ci-dessus, on appelle *rsolvant relatif* (de H par rapport L_0) tout lment $\Theta \in \mathcal{A}_H$ qui est lment primitif de l'extension $\mathrm{Inv}(H)$ de $\mathrm{Inv}(L_0)$. Le polynme minimal, que nous noterons $\mathcal{L}_\Theta^{[L_0]}$, d'un tel rsolvant Θ sur le corps $\mathrm{Inv}(L_0)$ sera appel *rsolvante de Lagrange relative* associe au triplet (Θ, H, L_0). Un tel rsolvant sera dit *homogne* ssi c'est un lment de $\mathcal{A}$ homogne.

Soit Θ un rsolvant relatif de H par rapport 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'aprs (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'aprs ce qui a t vu plus haut, on obtiendra ainsi un lment 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'aprs (29), on dduit que $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ est un diviseur du degr e dans $k[x]$ de la rsolvante "absolue" $\mathcal{L}_{\Theta,f}(x)$. Notons $H' = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta)$. On a donc $H' \cap L_0 = H$. Le degr 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 $e \leq [\mathfrak{S}_n : H']$ grce l'ingalit vidente $[H' : H] \leq [\mathfrak{S}_n : L_0]$, due au fait que $(xL_0) \cap H' = x(L_0 \cap H')$ pour tout $x \in H'$). On posera :

Définition 6.9. Le polynme $\mathcal{L}_{\Theta,f}^{[L_0]}(x) \in k[x]$ dfini par (29) sera appel *rsolvante de Lagrange relative* de f associe au triplet (Θ, H, L_0). Le rsolvant relatif Θ sera dit *f-sparable* (ou mieux : (L_0, f)-sparable) ssi $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ est un polynme sparable.

Remarque 12. Il convient ici de remarquer que mme dans le cas particulier agrable o $H = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta)$, le polynme $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ peut tre sparable sans que $\mathcal{L}_{\Theta,f}(x)$ le soit. Donc passer des rsolvantes relatives peut tre un moyen de se dbarrasser des facteurs multiples des rsolvantes absolues.

Toutefois, le calcul effectif d'une rsolvante relative sera en gnral ardu. Lorsque k est de caractristique 0, ce calcul peut formellement tre excut en utilisant le Thorme 4.1 et les considrations qui l'entourent : on commence par dterminer les lments $\eta_1, \ldots, \eta_{e_o}$ tels que $\mathcal{A}_{L_0} = \mathcal{S}\eta_1 \bigoplus \cdots \bigoplus \mathcal{S}\eta_{e_o}$, puis pour chaque coefficient F de $\mathcal{L}_{\Theta}^{[L_0]}(x)$ (calcul en faisant agir L_0 sur Θ), on calcule les lments $\varphi_1, \ldots, \varphi_{e_o} \in \mathcal{S}$ tels que $F = \sum_{i=1}^{e_o} \varphi_i \eta_i$; alors le calcul de $\tilde{F}$ est ramen celui des $\tilde{\eta}_i$, dont on sait l'avance qu'ils appartiennent k. Faute de mieux, on peut obtenir les $\tilde{\eta}_i$ par la mthode employe pour prouver le Thorme 4.3, en utilisant un rsolvant f-sparable de L_0. Cette mthode a t utilise par D. Lazard et J.M. Arnaudis afin de calculer des rsolvantes relatives en degr 5 (voir [Arnaudis-Lazard]). [Stauduhar] a mis au point une mthode diffrente fonde sur des calculs d'approximation des racines de f et sur le fait que les coefficients de la rsolvante sont des entiers. Il les a calcule pour les groupes transitifs jusqu'en degr 7. Cette mthode a t utilise poursuivie galement par M. Ollivier (Universit Bordeaux I) qui a pu parvenir jusqu'au degr 10.

Reprenons maintenant les notations et hypothses gnrales des dfinitions 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 rsolvant relatif Θ de H par rapport L_0. Notons α_j le nombre de facteurs de degr j de $\mathcal{L}_{\Theta,f}^{[L_0]}(x)$ qui sont k-irrductibles et simples (donc si Θ est (L_0, f)-sparable, $(\alpha_1, \ldots, \alpha_e)$ est une partition de e). Dans tous les cas, nous noterons :

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

Le rsultat essentiel concernant les rsolvantes relatives est alors :

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

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

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

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

En vue d'tablir ce rsultat essentiel, nous avons besoin de la version relative des Thormes 6.1 et 6.3 :

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

a) Alors

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

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

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

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

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, $j \in J$ tant fix : $g(\widetilde{\Theta_j}) = \widetilde{\Theta_j}$, 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 $g(\theta) = \theta$ quivaut :

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

C'est vrai avec tout $j \in J$, donc cette condition quivaut aussi : $g \in M$. De plus si la condition (32) est satisfaite avec un $j \in J$, elle entrane $g \in M$; en prenant $j = 1$ cela donne : $g.\Theta = \Theta \Rightarrow g \in M$, d'o $\Gamma \cap H \subset \Gamma \cap M$. On a donc prouv que $\mathrm{Gal}(E/k(\theta)) = \Gamma \cap M$ et que $\Gamma \cap H \subset \Gamma \cap M$. On prouve l'ingalit $[\Gamma : \Gamma \cap H] \leq \nu\,[k(\theta) : k]$ comme au Thorme 6.3, ce qui achve d'tablir toutes des assertions de a).

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

Soit $\{\tau_i\}_{1\leq i\leq e}$ une transversale gauche de L_0 mod H, avec $\tau_1 = \mathrm{Id}$, l'lment neutre de $\mathfrak{S}_n$. On supposera cette transversale indexe de faon que les Θ_i de (28) soient donns 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'o : $H_i = \mathrm{Stab}_{L_0}(\Theta_i)$, $\mathcal{L}^{[L_0]}_{\Theta,f}(x) = \prod_{i=1}^{e}(x - \Theta_i)$. Par dfinition, la partition $\varpi(\mathcal{G}^{[L_0]},\mathcal{C}^{[L_0]})$ de e est $(N_1/1,\ldots,N_e/e)$, o $N_j = \mathrm{card}(\{m \in [1,e] \mid [\Gamma : \Gamma \cap H_m] = j\})$ pour $1 \leq j \leq e$. Fixons $j \in [1,e]$; soit P un facteur k-irrductible simple de degr j de $\mathcal{L}^{[L_0]}_{\Theta,f}(x)$. Par hypothse, P est sparable, d'o $P = \prod_{m\in J}(x - \theta_m)$, o $J \subset [1,e]$ et $\mathrm{card}(J) = j$. Si $m \in J$, d'aprs le Thorme 6.11, on a $j = \deg(P) = [\Gamma : \Gamma \cap H_m]$, d'o $j\alpha_j \leq N_j$. Puisque c'est vrai pour tout j, on en dduit bien :

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

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

Compte tenu du Thorme 3.1, le Thorme 6.10 conduit immdiatement la version relative du Thorme 6.7 (“ mthode de la chasse aux rsolvantes relatives ”) :

Dmonstration du Thorme 6.10. **Théorème 6.12.** *Soit L_0 un sous-groupe de $\mathfrak{S}_n$ contenant le groupe de Galois $\Gamma = Gal(E/k)$. Notons $\mathcal{C}^{[L_0]}_1,\ldots,\mathcal{C}^{[L_0]}_{s_0}$ les classes* *de sous-groupes conjugus 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 rsolvant relatif* Θ_j *de* H_j *par rapport* L_0. *Supposons que les* Θ_j $(1 \leq j \leq s_0)$ *soient tous* (L_0, f)*-sparables. Alors la classe de conjugaison* $\mathcal{G}^{[L_0]}$ *de* Γ *dans* L_0 *est* $\mathcal{C}_r^{[L_0]}$, *o* 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 gale 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 Thorme 6.7 se transposent sans difficult au cas du thorme relatif 6.12.

Rsultat en degr 8

Nous n'nonons pas ici les rsultats obtenus pour les autres degrs, car cela fera l'objet d'autres articles. Ici le mot “ groupe ”, sera utilis pour classe de conjugaison. Nous nous plaons dans le cas o les facteurs irrductibles des rsolvantes sont simples, mme si c'est loin d'tre le cas dans la pratique et qu'alors nous faisons appel au Thorme des multiplicits (voir 6.5) qui nous permet couramment de conclure. Nous employons l'expression “ savoir dterminer ” lorsque deux conditions sont la fois runies : la premire est que les rsolvantes, soient non seulement calculables, mais que les calculs soient ralisables sur notre machine (voir [Marie]) et la deuxime est que chaque rsolvante obtenue soit galement factorisable sur notre machine.

En degr 8, nous savons dterminer les 50 groupes transitifs avec des factorisations de polynmes de degr au plus 56. Avec la table des partitions en degr 8, nous pouvons affirmer que notre algorithme est le plus optimum pour la mthode par les rsolvantes absolues (i.e. 56 est le plus bas degr possible pour rsoudre le problme dans tous les cas).

7. Application la spcialisation des groupes de Galois

Nous conservons ci-aprs toutes les notations en vigueur au dbut du §6.

Nous allons donner une version affine du thorme de spcialisation du groupe de Galois tel qu'il est expos par exemple dans [Brauer].

Donnons-nous un sous-anneau A de k, dont k soit le corps des fractions, et un idal 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 clture algbrique de $k^\bullet$. Pour tout $h \in A[x]$, nous dsignerons par $h^\bullet$ l'lment de $A^\bullet[x]$ obtenu en appliquant α aux coefficients de h. De mme pour $h \in A[x, x_1, \ldots, x_n]$.

Rappelons que $(\mathcal{C}_1, \ldots, \mathcal{C}_s)$ dsigne une ordination, par degrs dcroissants, de l'ensemble $\mathcal{E}$ des classes de conjugaison des sous-groupes de $\mathfrak{S}_n$. Nous considrerons un systme sparant $(J_j)_{1 \leq j \leq s}$ de parties de $[1, s]$, fix une fois pour toutes, de support J. Rappelons que pour chaque $i \in [1, s]$, on a fix un lment H_i de $\mathcal{C}_i$.

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

On notera $E^\bullet$ la $k^\bullet$-algbre des racines de $f^\bullet$ dans $\hat{k^\bullet}$; si $f^\bullet$ est sparable, $E^\bullet$ est une extension galoisienne de $k^\bullet$ et alors on notera $\Gamma^\bullet = \mathrm{Gal}(E^\bullet/k^\bullet)$. Observons que si A est intgralement clos, tout facteur normalis, dans $k[x]$, d'un polynme normalis $F \in A[x]$ appartient ncessairement $A[x]$. En particulier, les facteurs k-irrductibles normaliss de F appartiennent alors $A[x]$.

Notre but est, dans l'hypothse o $f^\bullet$ est, comme f, sparable, d'appliquer le Thorme 6.7 simultanment f et $f^\bullet$.

Pour y parvenir, nous devons prciser une numrotation des racines de $f^\bullet$ dans $\hat{k^\bullet}$ qui soit lie la numrotation des ρ_i. Soit un idal premier $\mathfrak{P}$ de $B = A[\rho_1, \ldots, \rho_n]$ tel que $\mathfrak{P} \cap A = \mathfrak{p}$: un tel idal 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 $1 \leq i \leq n$, le corps des fractions de $B^\bullet = A^\bullet[\rho_1^\bullet, \ldots, \rho_n^\bullet]$ est une $k^\bullet$-algbre des racines de $f^\bullet$. Les $\rho_i^\bullet$ sont distincts puisque $f^\bullet$ est sparable. Sans perte de gnralit, nous pouvons supposer que $B^\bullet \subset \hat{k^\bullet}$ et donc que $E^\bullet$ est le corps des fractions $k^\bullet[\rho_1^\bullet, \ldots, \rho_n^\bullet]$ de $B^\bullet$. D'o en particulier :

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

nous conviendrons d'utiliser la numrotation $(\rho_i^\bullet)_{1 \leq i \leq n}$ des racines de $f^\bullet$ dans $\hat{k^\bullet}$ pour identifier $\Gamma^\bullet$ un sous-groupe de $\mathfrak{S}_n$ et donc pour spcialiser dans $\hat{k^\bullet}$ les lments de $\mathcal{A}^\bullet = k^\bullet[x_1, \ldots, x_n]$. Nous poserons $\mathcal{K}^\bullet = k^\bullet(\sigma_1, \ldots, \sigma_n)$ et $\mathcal{F}^\bullet = k^\bullet(x_1, \ldots, x_n)$, les lettres $x, x_1, \ldots, x_n$ tant utilises comme indtermines aussi bien sur $\hat{k}$ que sur $\hat{k^\bullet}$. (Toute cette construction suppose bien entendu que l'idal $\mathfrak{P}$ a t fix une fois pour toutes.)

Le lemme suivant sera utile :

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

Démonstration. D'aprs (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 sparable □

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

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

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

d'o puisque β prolonge α :

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

puisque $\mathcal{L}^\bullet_{\Theta,f}$ est sparable, 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 sparabilit de $\mathcal{L}_{\Theta,f}$). Mais il est clair que $H \subset \mathrm{Stab}_{\mathfrak{S}_n}(\Theta^\bullet)$; le nombre des $\mathfrak{S}_n$-conjugus 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'o $H = \mathrm{Stab}_{\mathfrak{S}_n}(\Theta^\bullet)$, ce qui prouve bien que $\Theta^\bullet$ est un rsolvant de H. On a alors $\mathcal{L}^\bullet_\Theta = \prod_{i=1}^{e}(x - \Theta_i^\bullet)$ et d'aprs (35), cela rend bien clair que $\mathcal{L}_{\Theta^\bullet,f^\bullet} = \mathcal{L}^\bullet_{\Theta,f}$ $\square$

Théorème 7.2. *Supposons que A soit intgralement clos. Si $f^\bullet$ est sparable, le groupe $\Gamma^\bullet = Gal(E^\bullet/k^\bullet)$ s'identifie un sous-groupe de $\Gamma = Gal(E/k)$. Si de plus f est irrductible et normal sur k et $f^\bullet$ est irrductible sur $k^\bullet$, alors $\Gamma = \Gamma^\bullet$.*

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

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

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

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

Comme A est intgralement clos, on a $\varphi \in A[z, \underline{U}]$, et pour toute classe droite C de $\mathfrak{S}_n$ mod Γ : $\varphi_C \in A[z, \underline{U}]$. De plus ψ (resp. ψ_C) s'obtiennent 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 $k^\bullet(\underline{U})$-algbre 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 $\Gamma^\bullet$ et Γ, et $\mathfrak{S}_n$ s'identifie de mme $\mathrm{Gal}(\mathcal{F}^\bullet(\underline{U})/\mathcal{K}^\bullet(\underline{U}))$ et $\mathrm{Gal}(\mathcal{F}(\underline{U})/\mathcal{K}(\underline{U}))$. Le polynme Φ (resp. Φ_C) s'entend comme lment de $A[z, x_1, \dots, x_n, \underline{U}]$; le polynme de mme criture dans $A^\bullet[z, x_1, \dots, x_n, \underline{U}]$ sera not $\Phi^\bullet$ (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 dsigner par la mme lettre μ toute extension de μ en un morphisme $R_1[y_1, \ldots, y_m] \to R_2[y_1, \ldots, y_m]$, (o $(y_i)_{1 \leq i \leq m}$ dsigne une suite d'indtermines) consistant appliquer μ aux coefficients des lments de $R_1[y_1, \ldots, y_m]$.

Soit alors $\tau \in \Gamma^\bullet$. De part la thorie de Galois, on a $\psi_\Gamma = \tau.\psi_\Gamma$ et d'aprs la formule (24) du §5, on a $\tau.\psi_\Gamma = M^\bullet(\tau.\Phi_\Gamma^\bullet)$ d'o :

$$\psi_\Gamma = M^\bullet(\tau.\Phi_\Gamma^\bullet) \qquad ,$$

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

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

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

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

Supposons pour finir que f est irrductible dans $k[x]$ et normal sur k, et que $f^\bullet$ est irrductible dans $k^\bullet[x]$, les hypothses ci-dessus continuant tre satisfaites. Alors $\mathrm{card}(\Gamma) = n$, et $\mathrm{card}(\Gamma^\bullet) \geq n$ cause de l'irrductibilit de $f^\bullet$. Puisque $\Gamma^\bullet \subset \Gamma$, ncessairement ici $\Gamma^\bullet = \Gamma$ $\square$

Théorème 7.3. *Supposons toujours l'anneau A intgralement clos. Pour chaque indice $i \in J$, soit un rsolvant $\Theta_i \in A[x_1, \ldots, x_n]$ de H_i. Supposons que $f^\bullet$ soit sparable, que tous les polynmes $\mathcal{L}_{\Theta_i,f}^\bullet$ $(i \in J)$ soient sparables, et que pour tout $i \in J$ et pour tout facteur P de $\mathcal{L}_{\Theta_i,f}$ normalis et irrductible dans $k[x]$, le polynme $P^\bullet$ soit irrductible dans $k^\bullet[x]$. Alors $\Gamma^\bullet = \Gamma$.*

Démonstration. D'aprs le Thorme 7.2, on a dj $\Gamma^\bullet \subset \Gamma$. D'aprs le Thorme 7.1, pour tout $i \in J$, $\Theta_i^\bullet$ est un rsolvant de H_i, le polynme $\mathcal{L}_{\Theta_i,f}$ est sparable et $\mathcal{L}_{\Theta_i,f}^\bullet = \mathcal{L}_{\Theta_i^\bullet,f^\bullet}$. Alors l'hypothse faite entrane que pour tout $i \in J$, les partitions $\pi(\Theta_i, f)$ et $\pi(\Theta_i^\bullet, f^\bullet)$ sont gales. D'aprs le Thorme 6.7 et les prcisions qui le suivent, on voit que les classes de conjugaison de $\mathfrak{S}_n$ des groupe Γ et $\Gamma^\bullet$ concident. A fortiori, Γ et $\Gamma^\bullet$ sont isomorphes. Et puisque $\Gamma^\bullet \subset \Gamma$, en dfinitive $\Gamma^\bullet = \Gamma$ $\square$

En appliquant le Thorme d'irrductibilit de Hilbert, le Thorme 7.1 fournit le rsultat suivant, qui prcise le bien connu thorme de Noether sur la conservation des groupes de Galois par certaines spcialisations :

Corollaire 7.4. *Soit K un corps de nombres et $t_1, \ldots, t_m$ des indtermines sur K. Prenons $k = K(t_1, \ldots, t_m)$ et $A = K[t_1, \ldots, t_m]$, et supposons $f \in A[x]$; pour tout $i \in J$, soit un rsolvant $\Theta_i \in A[x_1, \ldots, x_n]$ de H_i ; pour tout $a = (a_1, \ldots, a_m) \in K^m$ et tout $h \in A[x]$, notons h_a l'lment de $k[x]$ obtenu en spcialisant $t_i \rightsquigarrow a_i$ $(1 \leq i \leq m)$ dans les coefficients de h. Alors le groupe de Galois $Gal(k, f)$ de f sur k est isomorphe au groupe de Galois $Gal(K, f_a)$ de f_a sur K pour tout $a \in K^m$ vrifiant* *les conditions suivantes : f_a est sparable, les rsolvantes $\mathcal{L}_{\Theta_i,f_a}$ $(i \in J)$ sont toutes sparables, et pour tout $i \in J$ et tout facteur k-irrductible normalis P de $\mathcal{L}_{\Theta_i,f}$, le polynme P_a est irrductible dans $K[x]$.*

En consquence, il y a une infinit d'lments $a \in K^m$ tels que $Gal(k,f) \cong Gal(K,f_a)$.

L'intrt des Thormes 7.1 7.3 ne se rduit pas au corollaire ci-dessus, car le cas o k et $k^\bullet$ n'ont pas mme caractristique 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 :

$$(37) \qquad \left\{ \begin{array}{l} k = \mathbb{Q}(t_1,\ldots,t_m) \text{ (les } t_i \text{ indtermines sur } \mathbb{Q}) \\ A = \mathbb{Z}[t_1,\ldots,t_m] \qquad ; \\ \text{pour tout } i \in J,\ \Theta_i \in A[x_1,\ldots,x_n] \text{ et } \Theta_i \text{ rsolvant de } H_i \end{array} \right. .$$

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

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

Théorème 7.5. *Plaons-nous sous les hypothses (37). Supposons que $f^\bullet$ et tous les polynmes $\mathcal{L}^\bullet_{\Theta_i,f}$ $(i \in J)$ soient sparables. Pour chaque indice $i \in J$, soit $\prod_{1\leq m\leq \nu_i} Q_{i,m}$ une dcomposition de $\mathcal{L}^\bullet_{\Theta_i,f}$ dans $k^\bullet[x]$ en facteurs normaliss irrductibles (donc ncessairement les $Q_{i,m}$ appartiennent $A^\bullet[x]$), et soit $P_{i,m}$ $(i \in J,\ 1 \leq m \leq \nu_i)$ un polynme normalis, lment de $A[x]$, tel que $P^\bullet_{i,m} = Q_{i,m}$. Supposons de plus que $p > \mathcal{M}(\mathcal{L}_{\Theta_i,f}) + \mathcal{M}(\prod_{1\leq m\leq \nu_i} P_{i,m})$ pour tout $i \in J$. Alors $\Gamma = Gal(E/k)$ est gal $\Gamma^\bullet = Gal(E^\bullet/k^\bullet)$.*

Démonstration. Pour tout $i \in J$, on a : $\mathcal{L}^\bullet_{\Theta_i,f} = \prod_{1\leq m\leq \nu_i} P^\bullet_{i,m} = (\prod_{1\leq m\leq \nu_i} P_{i,m})^\bullet$. Posons $F_i = \mathcal{L}_{\Theta_i,f} - \prod_{1\leq m\leq \nu_i} P_{i,m}$. D'aprs ce qui prcde, $F_i \in pA[x]$. Mais $\mathcal{M}(F_i) \leq \mathcal{M}(\mathcal{L}_{\Theta_i,f}) + \mathcal{M}(\prod_{1\leq m\leq \nu_i} P_{i,m}) < p$, d'o forcment $F_i = 0$, i.e. $\mathcal{L}_{\Theta_i,f} = \prod_{1\leq m\leq \nu_i} P_{i,m}$. Puisque $P^\bullet_{i,m} = Q_{i,m}$ est $k^\bullet$-irrductible et normalis, il est $A^\bullet$-irrductible donc $P_{i,m}$ est irrductible dans $A[x]$; mais $P_{i,m}$ tant normalis et $A^\bullet$ tant intgralement clos, on voit que $P_{i,m}$ est irrductible dans $k[x]$. Autrement dit, $\prod_{1\leq m\leq \nu_i} P_{i,m}$ est une dcomposition de $\mathcal{L}_{\Theta_i,f}$ en facteurs irrductibles dans $k[x]$ et normaliss. De plus $\mathcal{L}_{\Theta_i,f}$ est sparable, et on voit alors que le Thorme 7.3 s'applique et donne bien $\Gamma^\bullet = \Gamma$ □

Le Thorme 7.5 est un cas de remonte de la caractristique p la caractristique 0 dans le problme de Galois inverse. Soit G un groupe fini, sous-groupe d'un groupe $\mathfrak{S}_n$, ralisable comme groupe de Galois d'un polynme sur $\mathbb{F}_p(t_1,\ldots,t_m)$ coefficients dans un anneau du type $\mathbb{F}_p[t_1,\ldots,t_m]$ et normalis. Si l'on peut trouver f et des Θ_i satisfaisant les hypothses du Thorme 7.5, alors G sera ralisable comme groupe de Galois sur $\mathbb{Q}(t_1,\ldots,t_m)$; puis grce au corollaire 7.5, G sera ralisable comme groupe de Galois sur $\mathbb{Q}$.

8. Groupe de Galois mtacycliques de degr premier

Nous allons ici rappeler quelques faits connus sur les groupes mtacycliques de degr premier.

Définition 8.1. Un groupe fini G est dit *mtacyclique* 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 mtacyclique.)

Soit p un nombre premier impair. Dans le groupe de permutation $\mathfrak{S}_{\mathbb{F}_p}$, le groupe $\mathfrak{M}_p$ des similitudes $s_{a,b} : x \mapsto ax + b$ (o $(a, b) \in \mathbb{F}_p^\star \times \mathbb{F}_p$ est fix) est transitif (et mme doublement transitif) et il est mtacyclique. Il possde un unique p-Sylow $\mathfrak{C}_p$, engendr 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 appel le *groupe mtacyclique canonique de degr p*, et son sous-groupe d'indice 2 : $\mathfrak{M}_p \cap \mathfrak{A}_{\mathbb{F}_p}$, que nous noterons $\mathfrak{M}_p^+$, sera appel le *groupe mtacyclique pair* canonique de degr p. On a : $\mathfrak{C}_p \subset \mathfrak{M}_p^+$, et $\mathfrak{M}_p^+/\mathfrak{C}_p \cong \mathbb{F}_p^{\star\square}$, o $\mathbb{F}_p^{\star\square}$ dsigne le sous-groupe des carrs 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 mtacyclique 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 appels les *sous-groupes mtacycliques principaux* (resp. *sous-groupes mtacycliques principaux pairs*) de $\mathfrak{S}_p$. Ils forment une classe de conjugaison de sous-groupes de $\mathfrak{S}_p$; cette classe est forme de $(p-2)!$ sous-groupes. Tout sous-groupe de $\mathfrak{S}_p$ de cardinal p est contenu dans un et un seul sous-groupe mtacyclique principal (resp. mtacyclique principal pair) de $\mathfrak{S}_p$, et le sou-groupe mtacyclique principal pair qui le contient et videmment le sous-groupe mtacyclique pair du sous-groupe mtacyclique principal qui le contient. Le rsultat ci-aprs est bien connu :

Théorème 8.2. *Soit $\mathfrak{R}$ un sous-groupe transitif rsoluble de $\mathfrak{S}_p$. Alors $\mathfrak{R}$ est contenu dans un et un seul sous-groupe mtacyclique principal de $\mathfrak{S}_p$. En consquence, les sous-groupes rsolubles transitifs maximaux de $\mathfrak{S}_p$ sont les sous-groupes mtacycliques principaux, et les sous-groupes rsolubles transitifs maximaux $\mathfrak{A}_p$ sont les sous-groupes mtacycliques principaux pairs de $\mathfrak{S}_p$.*

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

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

de $\mathfrak{R}$ (o $m \geq 0$) 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'tre l'un des sous-groupes cycliques de cardinal p de $\mathfrak{S}_p$, i.e. l'un des sous-groupes engendrs par un p-cycle. On a dj signal plus haut qu'un tel sous-groupe est contenu dans un et un seul des sous-groupes mtacycliques principaux de $\mathfrak{S}_p$.
- Si $m \geq 1$, nous allons montrer que G_1 est transitif : par rcurrence vidente, il suffit pour cela de prouver que G_m est transitif. Soit $\mathcal{G}$ l'ensemble des G_m-orbites dans $[1,p]$. Puisque $G_m \triangleleft \mathfrak{R}$ et puisque $\mathfrak{R}$ est transitif, on dduit que $\mathcal{G}$ est $\mathfrak{R}$-stable et que $\mathfrak{R}$ opre transitivement sur $\mathcal{G}$. Les lments $\omega \in \mathcal{G}$ forment donc une partition de $[1,p]$ en parties de mme cardinal ; p tant premier, et G_m tant $\neq \{\mathrm{Id}\}$, il en dcoule que $\mathcal{G}$ n'a qu'un lment, donc G_m est bien transitif.

Ainsi G_1 est transitif ; il contient donc un p-cycle τ ; comme G_1 est cyclique, ncessairement G_1 est le sous-groupe $\mathfrak{C}$ engendr par τ. Soit M l'unique sous-groupe mtacyclique 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 $G_1 = \mathfrak{C} \triangleleft G_2$, on en dduit que $G_2 \subset M$, puis par une rcurrence immdiate, que $G_3 \subset M, \ldots, G_{m+1} = \mathfrak{R} \subset M$ $\square$

Exemple 1. : $p = 5$

Les sous-groupes mtacycliques 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 mtacycliques principaux pairs de $\mathfrak{S}_5$, isomorphes au groupe didral $\mathcal{D}_5$. Ils sont maximaux dans $\mathfrak{A}_5$. Les seuls sous-groupes rsolubles 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 mtacycliques principaux de $\mathfrak{S}_7$, au nombre de 120, sont de cardinal 21. Ils sont maximaux dans $\mathfrak{S}_7$. En revanche, les 120 sous-groupes mtacycliques principaux pairs, de cardinal 21, ne sont pas maximaux dans $\mathfrak{A}_7$. Si M est un sous-groupe mtacyclique principal, ses sous-groupes transitifs sont, outre M : l'unique sous-groupe mtacyclique 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 didral $\mathcal{D}_7$ 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 rsolubles 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 rsultants

Nous allons voir que pour obtenir des polynmes ayant pour groupe de Galois une extension d'un groupe par un autre, il y a intrt former certains rsultants. Dans tout ce paragraphe le corps k sera suppos infini.

9.1. Cas d'un seul paramtre. Donnons-nous d'abord deux indtermines x et y sur k, et deux polynmes :

$$(38) \qquad F = x^m - s_1 x^{m-1} + \cdots + (-1)^m s_m \in k[y][x] \qquad (m \geq 2)$$
$$(39) \qquad \psi = y^\nu - t_1 y^{\nu-1} + \cdots + (-1)^\nu t_\nu \in k[y] \qquad (\nu \geq 2) \qquad ,$$

o nous notons $F = F(x, y)$, vrifiant les quatres conditions suivantes :

$$(40) \qquad \psi \text{ est sparable, et irrductible dans } k[y] \qquad ;$$

$$(41) \qquad k(s_1, \ldots, s_m) = k(y)$$

(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 $\mathrm{pgcd}(\psi, V(s_1, \ldots, s_m)) = 1$. Notons $\mu = \deg_y(F)$; d'aprs (41), on a $\mu \geq 1$. Nous crivons :

$$(42) \qquad F = A_0(x) y^\mu + \cdots + A_\mu(x)$$

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

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

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 rsultant R de F et ψ (considrs comme polynmes en y) est un polynme en x de degr $m\nu$, de terme dominant $(-1)^{\mu\nu} x^{m\nu}$, coefficients dans k. On supposera :

$$(44) \qquad R \text{ est sparable} \qquad .$$

On dsigne 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'aprs les conditions ci-dessus, L et K sont des extensions galoisiennes de k. Nous allons comparer $\mathrm{Gal}(L/k)$ et $\mathrm{Gal}(K/k)$ sous certaines hypothses.

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

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

Considrons les conditions suivantes :

(I) Pour tout $\rho \in \mathcal{R}$, on a $\deg(\mathrm{pgcd}(F(\rho, y), \psi(y))) = 1$;
(II) R est irrductible dans $k[x]$;
(III) F est un polynme 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 sparable, L_i est une extension galoisienne de K_i.

Théorème 9.1. *Soient F et ψ vrifiant les conditions (38) (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 irrductible et sparable sur $k(y)$; $F(x, y_i)$ est irrductible sur K_i, et $(\mathcal{R}_1, \ldots, \mathcal{R}_\nu)$ est un systme d'imprimitivit pour l'action de 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 Gal(L/K_i) isomorphe un sous-groupe transitif de G (l'action de G considre tant 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 gaux K, et (45) est une dcomposition de R en facteurs irrductibles dans $K[x]$.

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

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

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

b) L'action Gal(L/k) sur $\mathcal{R}$ est transitive d'aprs (II). Mais si $\sigma \in$ Gal(L/k) envoie y_i sur y_j, il est clair que $\sigma(\mathcal{R}_i) = \mathcal{R}_j$, donc Gal$(L/k)$ permute les $\mathcal{R}_i$ entre eux et les $\mathcal{R}_i$ tant disjoints, ncessairement Gal(L/k) agit transitivement sur chaque $\mathcal{R}_i$. Donc $(\mathcal{R}_1, \ldots, \mathcal{R}_\nu)$ est bien un systme d'imprimitivit du groupe Gal(L/k). Supposons que $\sigma \in$ Gal(L/k) vrifie $\sigma(\mathcal{R}_i) = \mathcal{R}_i$, alors d'aprs (41), on a aussi $\sigma(y_i) = y_i$, i.e. $\sigma \in$ Gal(L/K_i). Donc Gal(L/K_i) opre transitivement sur $\mathcal{R}_i$, ce qui prouve que $F(x, y_i)$ est irrductible dans $K_i[x]$. On en dduit aussitt que $F(x, y)$ est irrductible dans $k[y][x]$, donc aussi dans $k(y)[x]$ d'aprs le Lemme de Gauss. Puisque $F(x, y_1)$ est sparable, F l'est aussi en tant qu'lment de $k(y)[x]$ d'aprs le Lemme 3 du §7. Puisque $k[y]$ est intgralement clos, le Thorme 7.2 montre que Gal(L_i/K_i) s'identifie un sous-groupe de G, qui est transitif puisque $F(x, y_i)$ est irrductible dans $K_i[x]$. Mais Gal$(L_i/K_i) \cong$ Gal$(L/K_i)/$Gal(L/L_i).

c) Cette assertion est immdiate.

d) Dans ce cas, pour tout i, $\mathrm{Gal}(L_i/K_i) = \mathrm{Gal}(L_i/K)$ est isomorphe G cause du Thorme 7.2, d'o $G \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_i)$. 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 $\mathrm{Gal}(K/k)$:

$$1 \;\rightarrow\; \mathrm{Gal}(L/K) \rightarrow \mathrm{Gal}(L/k) \rightarrow \mathrm{Gal}(K/k) \rightarrow 1 \tag{46}$$

$$1 \;\rightarrow\; \mathrm{Gal}(L/L_i) \rightarrow \mathrm{Gal}(L/K) \rightarrow \mathrm{Gal}(L_i/K) \cong G \rightarrow 1 \;\; (1 \leq i \leq \nu). \tag{47}$$

lorsque de plus R est normal, les L_i sont tous gaux L, et alors (47) se rduit

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

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

Signalons que le Thorme 9.1 admet une rciproque partielle, bien connue (voir par exemple [Netto], pages 268-269) :

Théorème 9.2. *Soient m et ν des entiers ≥ 2, et soit R un lment de $k[x]$ normalis et sparable de degr $m\nu$, notons L la k-algbre des racines de R dans $\hat{k}$ et $\mathcal{R}$ l'ensemble des racines de R dans $\hat{k}$. Supposons R irrductible et qu'il existe un systme d'imprimitivit $(\mathcal{R}_1, \dots, \mathcal{R}_\nu)$ pour l'action de Gal(L/k) sur $\mathcal{R}$, tel que card$(\mathcal{R}_i) = m$ pour tout i. Alors il existe $\psi = \prod_{i=1}^{\nu}(y - y_i) \in k[y]$ avec $\{y_1, \dots, y_\nu\} \subset L$ et $F = x^m - s_1 x^{m-1} + \cdots + (-1)^m s_m \in k[y][x]$ tel que : ψ est irrductible dans $k[y][x]$ et sparable, et $R = \prod_{i=1}^{\nu} F(x, y_i)$, i.e. R est le rsultant de F et ψ considrs comme polynmes en y.*

Démonstration. (abrge) Posons $\Phi_i(x) = \prod_{\rho \in \mathcal{R}_i}(x - \rho)$, et soit K_i le corps engendr par k et les coefficients de Φ_i. On a $K_i \subset k(\rho)$ pour tout $\rho \in \mathcal{R}_i$ parce que $(\mathcal{R}_1, \dots, \mathcal{R}_\nu)$ est un systme d'imprimitivit : tout lment $\sigma \in \mathrm{Gal}(L/k)$ tel que $\sigma(\mathcal{R}_i) = \mathcal{R}_i$ appartient $\mathrm{Gal}(L/K_i)$; on en dduit que Φ_i est le polynme 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'o $[K_i : k] = \nu$.

Soit y_1 un lment primitif de K_1 sur k, et soit ψ son polynme minimal sur k ; puisque L est sparable sur k, ψ est sparable. Les k-conjugus de y_1 sont des lments k-primitifs de $K_1, \dots, K_\nu$. 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 mme valeur, note y_i. Il est clair que y_i est lment primitif de K_i sur k, et que $\psi(y) = \prod_{i=1}^{\nu}(y - y_i)$ (on notera que ψ est sparable alors mme que les K_i ne sont pas ncessairement distincts). Par construction, ψ est irrductible sur k. On a des polynmes $s_1, \dots, s_m$, lments de $k[y]$ et de degr $< \nu$, 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 aisment que $F(x, y_i) = \Phi_i(x)$ pour $1 \leq i \leq \nu$. Comme Φ_i est sparable et K_i-irrductible, on en dduit comme au Thorme 9.1 que F est sparable et irrductible dans $k(y)[x]$. Comme $R = \prod_{i=1}^{\nu} F(x, y_i)$, on voit bien que R est le rsultant de F et ψ □

9.2. Cas de plusieurs paramtres. 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 lments de $k[y_1, \dots, y_d]$, de degrs respectifs $\nu_1, \dots, \nu_d$. Notons r_∞ le rsultant des polynmes $In(\psi_1), \dots, In(\psi_d)$, o $In(\psi)$ dsigne la partie homogne de (ψ)de degr $deg(\psi)$. Supposons $r_\infty \neq 0$. Dsignons par $\mathcal{V}$ la varit de dimension 0 dfinie par $\psi_1, \dots, \psi_d$ dans $\hat{k}^d$. Supposons que $card(\mathcal{V}) = \nu_1 \dots \nu_d$ (i.e. que tous les points de $\mathcal{V}$ sont simples). Soit φ un lment 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 indtermines. 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 $R_{\mathcal{V}}(T) = \text{Rsultant}_{z,y_1,\dots,y_d}(Tz - \sum_{i=1}^d U_i y_i, \psi_1^\star, \dots, \psi_d^\star)$. D'aprs la formule de Poisson-Perron (cf [Arnaudis]), on a :

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

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

Soit δ le degr 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 rsultant l'infini de $\psi_1^r + \varphi, \psi_2, \dots, \psi_d$ est $(r_\infty)^r \neq 0$, donc ces polynmes dfinissent dans $\hat{k}^d$ une varit de dimension zro $\mathcal{W}$ et on a des entiers $(l_\xi)_{\xi \in \mathcal{W}}$ non nuls tels que le rsultant $R_{\mathcal{W}}(T)$ 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 donn 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 [Arnaudis]).

D'aprs l'hypothse, le pgcd dans $\hat{k}(\underline{U})[T]$ de $R_{\mathcal{V}}(T)$ et $R_{\mathcal{W}}(T)$ est de degr 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 $k(\underline{U})[T]$, 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 entrane immdiatement que $\theta \in k^d$ $\square$

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

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

o $\underline{Y} = (Y_1, \dots, Y_d)$, et supposons satisfaistes les conditions ci-aprs, dans lesquelles $\mathcal{V}$ est dfinie comme au Lemme 1, sous les mmes hypothses 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 $\forall i \in [1, d], \exists C_i, D_i \in k[z_1, \dots, z_m]$, $\mathcal{V} \cap \mathrm{Z}(D_i) = \emptyset$ (o $\mathrm{Z}(D_i)$ est l'ensemble des zros de D_i) et que $Y_i = \frac{C_i(s_1,\dots,s_m)}{D_i(s_1,\dots,s_m)}$;

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

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

Il est clair que le terme constant de F ordonn 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 degr $< m$ en x.

Donc le rsultant R de $F^\star = z^\mu F(x, \frac{Y_1}{z}, \dots, \frac{Y_d}{z})$ (o $\mu = \deg_{\underline{Y}}(F)$) et de $\psi_1^\star, \dots, \psi_d^\star$, considrs comme polynme homognes de $Y_1, \dots, Y_d, z$, est un polynme en x de degr $m\nu_1\nu_2 \dots \nu_d$, de monme dominant $(-1)^{\mu\nu_1\nu_2\dots\nu_d} x^{m\nu_1\nu_2\dots\nu_d}$. Nous supposerons que

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

On dsignera par L le corps des racines de R sur k dans $\hat{k}$, et par K le corps engendr par k et les coordonnes des points de $\mathcal{V}$. D'aprs les hypothses, 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'aprs la formule Poisson-Perron

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

enfin on dsigne par K_ξ le corps engendr par k et les coordonnes 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, cause des hypothses, que L_ξ est une extension galoisienne de K_ξ. On considre 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 irrductible dans $k[x]$;
(VII) F est un polynme de x normal sur $k(\underline{Y})$;
(VIII) $[K : k] = \nu_1 \dots \nu_d$.

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

a) Si la condition (V) est satisfaite, on a $K \subset L$.

b) Si les conditions (V) (VI) sont satisfaites, alors : F est irrductible et sparable sur $k(\underline{Y})$; $F(x,\xi)$ est irrductible dans $K_\xi[x]$, et $(\mathcal{R}_\xi)_{\xi\in\mathcal{V}}$ est un systme d'imprimitivit pour l'action de 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 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 gaux K, et 57 est une dcomposition de R en facteurs irrductibles dans $K[x]$.

d) Si les conditions (V) (VIII) sont satisfaites, il y a un quotient de Gal(L/K) isomorphe G, et si de plus R est normal, alors Gal$(L/K) \cong G$.

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

a) Fixons $\rho \in \mathcal{R}$. On a $F(\rho,\underline{Y}) \neq 0$ d'aprs (55), et d'aprs (V), $F(\rho,\underline{Y})$ est non constant. Toujours cause de (V), en appliquant le Lemme 4, on voit qu'il existe $\xi \in \mathcal{V}$ tel que les coordonnes de ξ appartiennent $k(\rho)$, donc aussi L. Mais 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 coordonnes dans L. D'o $K \subset L$.

b) D'aprs (VI), l'action de Gal(L/k) sur $\mathcal{R}$ est transitive. Si $\sigma \in$ Gal(L/k) envoie ξ sur η, il est clair que $\sigma(\mathcal{R}_\xi) = \mathcal{R}_\eta$. Donc Gal$(L/k)$ permute entre eux les $\mathcal{R}_\xi$, donc son action sur chaque $\mathcal{R}_\xi$ est ncessairement transitive. Ainsi $(\mathcal{R}_\xi)_{\xi\in\mathcal{V}}$ est bien un systme d'imprimitivit de Gal(L/k). Si $\sigma \in$ Gal(L/k) vrifie $\sigma(\mathcal{R}_\xi) = \mathcal{R}_\xi$, alors d'aprs (53) $\sigma(\xi) = \xi$, donc $\sigma \in$ Gal(L/K_ξ). Donc Gal(L/K_ξ) opre transitivement sur $\mathcal{R}_\xi$, donc $F(x,\xi)$ est irrductible dans $K_\xi[x]$.

Il s'ensuit que $F(x,\underline{Y})$ est irrductible dans $k[\underline{Y}][x]$, donc aussi dans $k(\underline{Y})[x]$ d'aprs le Lemme de Gauss. La sparabilit de F dans $k(\underline{Y})[x]$ se dduit du Lemme 3 du §7. Comme $k(\underline{Y})$ est intgralement clos, d'aprs le Thorme 7.2, le groupe Gal(L_ξ/K_ξ) s'identifie un sous-groupe de G, ncessairement transitif puisque les $F(x,\xi)$ sont irrductibles dans $K_\xi[x]$. De plus, on a bien toutes les assertions de b) puisque Gal$(L_\xi/K_\xi) \cong$ Gal$(L/K_\xi)/$Gal(L/L_ξ).

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

d) Ici, d'aprs le Thorme 7.2, Gal(L_ξ/K_ξ) (= Gal(L_ξ/K)) est isomorphe G, d'o $G \cong$ Gal$(L/K)/$Gal(L/L_ξ). On a alors une description partielle de Gal(L/K) en fonction de G et Gal(K/k) l'aide des suites exactes ci-aprs :

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

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

o $\xi \in \mathcal{V}$. Lorsque de plus R est normal, les L_ξ sont tous gaux L, et alors (59) se rduit

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

10. Rsolvantes et Rsultant

Nous reprenons ici les notations et hypothses des §§4 et 5. En particulier, le corps k sera suppos de caractristique 0. L'idal de $\mathcal{A}$ engendr par $\{\sigma_1 - c_1, \ldots, \sigma_n - c_n\}$ est not $\mathfrak{I}$, et $\mathcal{W}$ est la varit de dimension 0 dfinie par $\mathfrak{I}$ dans $\hat{k}^n$. On a vu au §5 que $\mathfrak{I} = \sqrt{\mathfrak{I}}$, et $\mathcal{W} = \{(\rho_{s(1)}, \ldots, \rho_{s(n)})\}_{s \in \mathfrak{S}_n}$.

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

Soit maintenant Θ un rsolvant 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 degr d. Le rsultant de $(\sigma_1, \ldots, \sigma_n)$ (considrs comme polynmes homognes en $(x_1, \ldots, x_n)$) est 1. Soit z une variable d'homognisation. Posons :

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

Soit μ_i l'endomorphisme de k-espace vectoriel $\mathcal{A}/\mathfrak{I}$ induit par la multiplication par x_i. D'aprs ce qui prcde, le Thorme I.3.1 de [Arnaudis] s'applique ici et donne le polynme caractristique $\chi_{\Theta(\mu_1, \ldots, \mu_n)}(x)$ de $\Theta(\mu_1, \ldots, \mu_n)$:

$$\chi_{\Theta(\mu_1, \ldots, \mu_n)}(x) = \mathrm{Rsultant}(F_1, \ldots, F_n, x z^d - \Theta_{\clubsuit}) \qquad , \tag{61}$$

le rsultant tant entendu comme rsultant de polynmes homognes en $(x_1, \ldots, x_n, z)$. Le Thorme I.3.3 de [Arnaudis] donne alors immdiatement :

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

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

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

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

On en dduit :

Théorème 10.1. *On a :*

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

Démonstration. D'aprs (61) et (62) :

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

car par dfinition $\mathcal{L}_{\Theta,f} = \prod_{i=1}^{e}(x-\widetilde{\Theta}_i)$. On peut galement le dmontrer ainsi : comme $\mathcal{L}_{\Theta,f}(x)$ est le polynme minimal de Θ sur $\mathcal{K}$ on a immdiatement l'galit $\chi_{\Theta(\mu_1,\dots,\mu_n)}(x) = (-1)^{n!}(\mathcal{L}_{\Theta,f}(x))^h$. □

Les endomorphismes $\{g(\mu_1,\dots,\mu_n)\}_{g\in\mathcal{A}}$ du k-espace vectoriel $\mathcal{A}/\mathfrak{I}$ sont deux deux permutables, et tous semi-simples puisque $\mathfrak{I} = \sqrt{\mathfrak{I}}$ (cf. Proposition II.5.3 de [Arnaudis]). Posons $m = [\mathfrak{S}_n : \Gamma]$, $N = \mathrm{card}(\Gamma)$, et soit $\{\tau_i\}_{1\le i\le m}$ une transversale droite de $\mathfrak{S}_n$ mod Γ. Notons $\mathfrak{M}_i$ l'idal 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 crira $\mathfrak{N} = \mathfrak{M}_1$. La projection $p_i : \mathcal{A} \to E$, $g \mapsto \widetilde{\tau_i g}$ dfinit 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 dfinit alors par passage au quotient un isomorphisme π de k-algbre 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-ime facteur E_j de $\mathcal{A}/\mathfrak{I}$, (identifi 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 hypothses tant celles du Thorme* 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 polynme* k*-minimal de* $[\Theta]_i$ *et* $d_i = deg(P_i)$ *(d'o* 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 consquence immdiate du fait que $[\Theta]_i$ est la multiplication par θ_i dans $E = E_i$ □

On obtient ainsi la relation cherche:

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

et une autre formulation de la rsolvante de Lagrange :

Corollaire 10.3. *Dans les conditions du Thorme* 10.2*, le polynme minimal de* $[\Theta] = \Theta(\mu_1, \dots, \mu_n)$ *est 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'idal maximal de $\hat{\mathcal{A}}$ dfini par $(\rho_{\tau_i(1)}, \dots, \rho_{\tau_i(n)})$, et $\hat{\mathfrak{I}} = \bigcap_{i=1}^m \hat{\mathfrak{M}}_i$. Posant $\hat{E}_i = \hat{k} \bigotimes_k E_i = \hat{k} \bigotimes_k E$, (not 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 $[\Theta]$, dfinissons de mme $\widehat{[\Theta]}_i$, 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 caractristique nulle, $\widehat{[\Theta]}$, et donc les $\widehat{[\Theta]}_i$, sont diagonalisables. Il est ais de dfinir une base de vecteurs propres de chaque $\widehat{[\Theta]}_i$ dans $\hat{E}_i$: en fait, soit $P_\tau \in \hat{k}[x_1, \dots, x_n]$ vrifiant, 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 fix, $1 \leq i \leq m$, $V_{\sigma\tau_i} \in \hat{E}_i$ 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 associe $V_{\sigma\tau_i}$ tant $\widetilde{\sigma\tau_i\Theta} = \sigma(\widetilde{\tau_i\Theta}) = \sigma(\theta_i)$, la dernire galit tant due au fait que $\sigma \in \Gamma$. On retrouve ainsi la relation (65).

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

Démonstration. On a une reprsentation 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 reprsentation est transitive, et lorsque $n \geq 5$ et $e \geq 3$ elle est fidle, d'o alors $e \geq n$). La multiplicit de λ dans $\chi_{[\Theta]_i}(x)$ (o $i \in [1, m]$ est fix) est, en vertu de (65), le nombre ν_i des $\sigma \in \Gamma$ tels que $\sigma(\theta_i) = \lambda$, ce qui s'crit : $\sigma(\widetilde{\tau_i\Theta}) = \lambda$, 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 $\sigma \in \Gamma$ vrifiant 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'o $\tau\Theta_l \in \{\Theta_j\}_{j \in J}$, et donc $\tau \in L$. On en dduit de l que $\mathcal{N}_i = (\Gamma \cap L)\sigma_0$, c'est--dire que $\mathcal{N}_i$ est une classe droite de $\Gamma \bmod \Gamma \cap L$, d'o card$(\mathcal{N}_i) = $ card$(\Gamma \cap L)$.

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

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

ce qui achve la dmonstration □

Corollaire 10.5. *Si $\lambda \in k$, alors $N = card(\Gamma)$ 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--dire ssi $\Gamma \subset L$; l'assertion 1 dcoule alors de (67). La deuxime assertion s'en dduit l'aide du Thorme 5.2 a) □

(Ce corollaire est latent dans [Lagrange, tome IV], (Trait des quations algbriques), bien entendu sans preuve aucune, et surtout sans langage de thorie des groupes pour l'exprimer commodment.)

Une autre consquence de Thorme 10.4 et de sa preuve est la formule :

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

(qui se dduisait aussi de l'tude du Thorme 6.3). En particulier, λ est lment primitif de E ssi $\Gamma \cap L = \{\mathrm{Id}\}$.

Rsolvants et rsolvantes de Galois

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

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

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

Si l'on connait un rsolvant de Galois Λ_u qui soit f-sparable, alors le calcul d'une rsolvante arbitraire se ramme au calcul du rsultant de deux polynmes d'une variable ; en effet, soit Θ un rsolvant d'un groupe H ($\Theta \in \mathcal{A}$). Par la mthode du Thorme 4.3 applique $\Theta \in \mathcal{A}_H \subset \mathcal{A}$, on peut thoriquement dterminer $\Phi \in \mathcal{S}[x]$ tel que $\Theta = \frac{1}{\Delta}\Phi(\Lambda_u)$, o Δ est le discriminant de $\mathcal{L}_{\Lambda_u}(x)$. Soit $\varphi \in k[x]$ obtenu en spcialisant $(\sigma_1, \ldots, \sigma_n)$ en $(c_1, \ldots, c_n)$ dans les coefficients de Φ. On a (puisque $\tilde{\Delta} \neq 0$) :

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

l'indice T signifiant que le rsultant considr est celui qui limine T.

Plus gnralement, soient Θ_1 et Θ_2 des rsolvants 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-sparable. 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 spcialisant $(\sigma_1, \dots, \sigma_n)$ 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 $\mathrm{card}(\mathcal{T}_1) = \mathrm{card}(\mathcal{T}_2) \times [H_2 : H_1]$, on a pour $i \in \{1,2\}$:

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

ces relations tant dues au fait que pour tout $\tau \in \mathfrak{S}_n$, $\tau\Theta_2 = \frac{1}{\Delta_1}\Phi(\tau.\Theta_1)$, d'o $\widetilde{\tau.\Theta_2} = \frac{1}{\widetilde{\Delta_1}}\widetilde{\Phi(\tau.\Theta_1)} = \frac{1}{\widetilde{\Delta_1}}\varphi(\widetilde{\tau\Theta_1})$. En rsum :

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

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

Lien entre rsolvante f-sparable et rsolvante gnrale d'un mme groupe H

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

Dans ses rflexions sur la rsolution des quations algbriques, art. 103, tome IV, pour tudier la racine multiple λ de $\mathcal{L}_{\Theta,f}$ (dans le cas $\nu > 1$), Lagrange a propos d'introduire un rsolvant f-sparable Ψ du mme groupe, et de comparer $\mathcal{L}_{\Theta,f}$ et $\mathcal{L}_{\Psi,f}$. (il ne conclut pas nettement faute de langages appropris de thorie des corps et de thorie des groupes.) Soit donc Ψ un rsolvant f-sparable de H, notons $\mathcal{L}_\Psi(x) = \prod_{i=1}^{e}(x - \Psi_i)$, la numrotation des Ψ_i tant 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 rsulte maintenant du Thorme 6.3 (ou de la dmonstration du Thorme 10.4) que $\mathrm{Stab}_\Gamma(\lambda) = \Gamma \cap L$. L'action de $\mathfrak{S}_n$ sur $\{\Theta_1, \dots, \Theta_e\}$, tout comme celle de $\mathfrak{S}_n$ sur $\{\Psi_1, \dots, \Psi_e\}$, s'identifie l'action par translations gauche de $\mathfrak{S}_n$ sur l'ensemble $\{C_1, \dots, C_e\}$ des classes gauche de $\mathfrak{S}_n$ mod H, numrotes de faon que $C_i = \{\sigma \in$

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

$\mathfrak{S}_n \mid \sigma.\Theta = \Theta_i\}$ (et donc aussi $C_i = \{\sigma \in \mathfrak{S}_n \mid \sigma.\Psi = \Psi_i\}$). On en dduit que L, qui est par dfinition le stabilisateur de $\{\Theta_1, \ldots, \Theta_\nu\}$ dans $\mathfrak{S}_n$, est aussi celui de $\{\Psi_1, \ldots, \Psi_\nu\}$.

Soit Φ un polynme symtrique en ν variables coefficients dans k. Pour tout lment $\sigma \in \Gamma \cap L$, 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 lment 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 symtrique. Par suite,

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

Une consquence vidente des relations (72) est le thorme suivant, affirm par Lagrange dans la rfrence cite, mais sans vritable 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 gnral, Q n'est pas irrductible dans $k(\lambda)[x]$. Les facteurs irrductibles 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 polynme minimal de $\widetilde{\Psi_1}$ sur $k(\lambda)$ est videmment $\prod_{j \in J}(x - \widetilde{\Psi_j})$. Dans l'article de Lagrange sus-cit, c'est le polynme que Lagrange cherchait concevoir.

Notons Δ le discriminant de $\mathcal{L}_\Psi(x)$. On a un polynme $\mathcal{M} \in \mathcal{S}[x]$ tel que $\Theta = \frac{1}{\Delta}\mathcal{M}(\Psi)$ (voir §6). D'o, 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 spcialiser la relation (73), ce qui donne :

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

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

Rsolvants f-triviaux

Le rsolvant 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 caractristique 0, alors ncessairement $\lambda \in k$. Puisque $\Theta(\mu_1, \dots, \mu_n)$ est semi-simple, il revient au mme de dire que Θ est f-trivial, ou que $\Theta(\mu_1, \dots, \mu_n)$ est une homothtie dans le k-espace vectoriel $\mathcal{A}/\mathfrak{I}$. De faon quivalente, 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 thorme suivant :

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

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

En raison du Thorme 10.7, il convient de disposer d'un critre d'appartenance l'idal $\mathfrak{I}$. 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 faon unique, i.e. il existe $(\Phi_0, \dots, \Phi_n)$ suite unique d'lments 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 sucrot 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 ramne rsoudre un systme linaire de Cramer sur k.)

On voit donc que le rsolvant 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 galement utiliser la base standard de $\mathfrak{I}$ pour l'ordre lexicographique (voir [Mach-Valibouze]).

Application au degr 5

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

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

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

Supposons $\lambda \in k$, et que la multiplicit ν de λ dans $\mathcal{L}_{\Theta,f}$ soit ≥ 2. Si $\mathcal{L}_{\Psi,f}$ est k-irrductible, i.e. Γ n'est pas rsoluble, le Thorme 10.6 montre immdiatement que $\nu = 6$, c'est--dire que $\mathcal{L}_{\Theta,f} = (x-\lambda)^6$, autrement dit, que Θ est f-trivial. On va en dduire le rsultat suivant :

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

a) Pour que Γ soit rsoluble, il faut et il suffit que $\mathcal{L}_{\Theta,f}$ possde au moins une racine dans k (multiple ou non).
b) Si $\lambda \in k$ est une racine de $\mathcal{L}_{\Theta,f}$ de multiplicit ≥ 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 sparable, et mme irrductible dans $k[x]$.

Démonstration. Les assertions a) et b) dcoulent du Thorme 10.6, et des considrations qui prcdent l'nonc du Thorme 10.8. Prouvons l'assertion c) : puisque $\mathcal{L}_{\Theta,f}$ n'a pas de racine dans k, si $\mathcal{L}_{\Theta,f}$ n'tait pas sparable, il serait divible dans $k[x]$ par P^2 avec P polynme irrductible dans $k[x]$ et de degr 2 ou 3. Soit alors $\lambda \in E$ une racine de P. Puisque $[k[\lambda] : k] \in \{2, 3\}$, on voit que f est irrductible dans $k(\lambda)[x]$, sinon $[E : k]$ ne pourrait pas tre divisible par 5. Mais la multiplicit de λ dans $\mathcal{L}_{\Theta,f}(x)$ ne peut tre que 2 ou 3 ; en remplaant k par $k(\lambda)$, les hypothses assurant la validit des assertions a) et b) continuent tre satisfaites. On aboutit donc une contradiction puisque la multiplicit de λ dans $\mathcal{L}_{\Theta,f}(x)$ devrait tre 5. Cette contradiction prouve donc que $\mathcal{L}_{\Theta,f}$ est sparable. Mais puisque $\mathcal{L}_{\Theta,f}$ n'a pas de racine dans k, l'tude qui prcde l'nonc du Thorme 10.8 montre que $\mathcal{L}_{\Theta,f}$ est irrductible dans $k[x]$ $\square$

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

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

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

Le rsolvant Φ a t calcul par Berwick ([Berwick,1915]). Quant Ψ, c'est le clbre *rsolvant de Cayley* : la rsolvante correspondante $\mathcal{L}_{\Psi,f}$ (dite *de Cayley*) a t calcul par [Cayley] et nous avons contrl son rsultat. Si $f = x^5 - a$ avec $a \in k^\star$, un calcul facile donne :

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

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

La rsolvante de Cayley Ψ donne par (76) est trs remarquable en raison du rsultat non-vident ci-aprs :

Théorème 10.9. *Avec $n = 5$ et f irrductible dans $k[x]$, la rsolvante de Cayley $\mathcal{L}_{\Psi,f}$ correspondant (76) est sparable.*

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

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

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 [Tchebotarev]).

Pour abrger, posons $R = \mathcal{L}_{\Psi,f}(x)$. D'aprs le Thorme 10.8, tout revient 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'o les relations :

$$\begin{aligned} P^2(\lambda) &= 2^{10}\tilde{\Delta}\lambda & (79)\\ 2(PP')(\lambda) &= 2^{10}\tilde{\Delta} \quad . & (80)\end{aligned}$$

En levant au carr les deux membres de (80), puis en y remplaant $P^2(\lambda)$ par sa valeur tire de (79), on arrive :

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

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

b) Puisque $\lambda \neq 0$, d'aprs (79) on a aussi : $P(\lambda) \neq 0$. A prsent λ est racine d'ordre $\nu - 1$ de R', donc est racine d'ordre ≥ 4 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 polynme est de degr 3 (rappelons qu'on est en caractristique 0). Donc on arrive une contradiction, et λ ne peut exister □

Nous remercions Daniel Lazard d'avoir apport une notable simplification la partie b) de cette dmonstration.

Compte tenu du Thorme 10.8, le Thorme 10.9 donne

Corollaire 10.10. *(“ Thorme de Selivanoff ”)*
Si $n = 5$ et si f est irrductible dans $k[x]$, le groupe de Galois Γ de f sur k est rsoluble ssi la rsolvante de Cayley de f admet une racine dans k.

Le Thorme de Selivanoff est nonc dans [Tchebotarev], pages 341 et 342. La preuve qui en est propose est incomplte car l'auteur y affirme que le seul cas carter pour assurer que $\mathcal{L}_{\Psi,f}$ est sparable est le cas o l'on aurait $\mathcal{L}_{\Psi,f}(x) = (x-\lambda)^6$, i.e. le cas o Ψ serait f-trivial. Or l'exemple tir de (77) montre qu'il faut imprativement carter, outre le cas o Ψ serait f-trivial, le cas o $\mathcal{L}_{\Psi,f}(x)$ serait de la forme $(x-\lambda)^5(x-\mu)$ avec $\lambda \neq \mu$.

Dtermination du groupe de Galois Γ en degr 5 dans le cas gnral

Il faut distinguer deux aspects dans la recherche du groupe de Galois de f sur k. Nous dfinissons ces deux problmes dans le cas gnral o f est de degr $n \geq 2$ quelconque :

Problme I : f tant donn numriquement, calculer la classe de conjugaison de Γ dans $\mathfrak{S}_n$. (recherche de Γ " au coup par coup "). C'est ce problme dont la mthode de la "chasse aux rsolvantes" expose au §6 offre une solution, sous rserve de calculer suffisamment de rsolvantes sparables et de les factoriser dans $k[x]$.

Problme II : Expliciter un systme de conditions ncessaires 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 donne l'avance.

Evidemment le Problme II est bien plus complexe que le problme I. Une solution du problme II, due aux auteurs, est exposes dans [Arnaudis-Bertin] lorsque $n = 4$. Nous allons maintenant voir que ce problme II admet une solution pour $n = 5$.

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

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

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

On vrifie 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 un morphisme de H dans le groupe des permutations des γ_i, dont l'image est le groupe 4-cyclique engendr 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 rsolvant relatif de C par rapport H_+ (cf. dfinition 6.8 et 6.9), la rsolvante relative associe tant :

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

cette rsolvante (83) est sparable ; en effet on a :

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

D'aprs le Thorme 6.11, si $\Gamma \subset H_+$, on aura donc $\Gamma \subset C$ ssi $\tilde{\gamma}_1 \in k$. Notons d'ailleurs que si $\Gamma \subset H$, ncessairement $C \subset \Gamma$ 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 rsolvant absolu de H, et que la rsolvante $\mathcal{L}_{\Phi,f}$ est connue gnriquement. Si $\Gamma \subset H$ et si la rsolvante $\mathcal{L}_{\Phi,f}$ n'est pas f-triviale, elle admet une unique racine simple dans k (que $\mathcal{L}_{\Phi,f}$ soit ou non sparable), et l'tude qui entoure le Thorme 10.8 permet de montrer que cette racine est $\widetilde{\gamma_1}^2 + \widetilde{\gamma_2}^2$. Nous avons donc deux cas dans l'hypotse o $\Gamma \subset H$:

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

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

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

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

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

Malheureusement il n'est pas exclu que la rsolvante $\mathcal{L}_{\Phi,f}(x)$ puisse tre f-triviale, auquel cas elle ne permet pas elle seule de dcider si Γ est rsoluble. Mais pour cela on peut utiliser la rsolvante de Cayley (cf. Thorme 10.9), et exploiter le fait bien connu que $\Gamma \subset \mathfrak{A}_5$ ssi $\tilde{\Delta}$ est un carr dans $k^\star$. En rsum, on aboutit en faisant la synthse de tout ce qui prcde, la discussion suivante qui rsout compltement le problme II en degr 5 pour un polynme k-irrductible :

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

$\boxed{\text{A}}$ Si la rsolvante de Cayley $\mathcal{L}_{\Psi,f}(x)$ est sans racine dans k :
- a) pour $\tilde{\Delta} \notin k^{\star\Box}$, $\Gamma = \mathfrak{S}_5$
- b) pour $\tilde{\Delta} \in k^{\star\Box}$, $\Gamma = \mathfrak{A}_5$.

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

a) pour $\tilde{\Delta} \notin k^{\star\square}$, Γ est un sous-groupe mtacyclique principal de $\mathfrak{S}_5$
b) pour $\tilde{\Delta} \in k^{\star\square}$: alors la rsolvante $\mathcal{L}_{\Phi,f}(x)$ soit est f-triviale soit admet dans k une unique racine simple. Notons λ son unique racine (qui est lment 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 mtacyclique 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 $f = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ (polynme $\mathbb{Q}$-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-ime dans $k^\star$. Avec f le polynme minimal sur $\mathbb{Q}$ d'une priode de Gauss approprie 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-ime dans $\mathbb{Q}^\star$, d'o ici $a_1 \neq a_2$.

Pour finir notons une curiosit :

Théorème 10.11. *Supposons $n = 5$ et f irrductible dans $k[x]$. Supposons que la rsolvante 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. (abrge) Reprenons toutes les notations de la discussion prcdente, 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'o par diffrence $V_1V_2 = \frac{1}{4}(\sigma_2^2 - \Psi)$. D'autre part $\mathrm{Stab}_{\mathfrak{S}_5}(V_i) = \mathrm{Stab}_H(V_i) = H_+$, donc une rsolvante relative de H_+ par rapport 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 polynme est λ, qui est $\neq 0$ par hypothse ; donc il est sparable. Le Thorme 6.11 s'applique et prouve que $\mathcal{L}^{[H]}_{V_1,f}(x)$ est dissoci dans $k[x]$ ssi $\Gamma \subset H_+$; mais cette dernire condition quivaut : $\tilde{\Delta} \in k^{\star\square}$, tandis que $\mathcal{L}^{[H]}_{V_1,f}(x)$ est dissoci dans $k[x]$ ssi son discriminant est un carr dans k, c'est--dire ssi $\lambda \in k^{\star\square}$ $\square$

Remerciements

Nous tenons remercier Jos Bertin qui a relu attentivement ce travail et qui y a apport des remarques prcieuses. Nous remercions galement Marc Giusti qui, grce sa dtermination en matire d'quipement du G.D.R MEDICIS, nous a permis

de travailler sur une machine trs performante avec les logiciels dont nous avions besoin.

References

[Arnaudis] J.M. Arnaudis, (1993), *Thorme de Bzout, Formule de Poisson-Perron et courbes rationnelles gnriques*, paratre dans Beitrag ber algebra and geometrie, (rapport interne du LITP numro **92.94**)

[Arnaudis-Bertin] J.M. Arnaudis, J. Bertin *Groupes, Algbres et Gomtrie*, Tome I, Ellypses, 1993

[Arnaudis-Lazard] J.M. Arnaudis, D. Lazard, (1993), *Equations du cinquime degr et rsolutions par radicaux*, (manuscrit)

[Arnaudis-Valibouze] J.M. Arnaudis, A. Valibouze, (1993), *Calculs de tables de partitions, de rsolvantes de Lagrange et de groupes de Galois* (manuscrit).

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

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

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

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

[Brauer] Richard Brauer **Galois Theory**, Harvard, Harvard University, 1964

[Cayley] 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**

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

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

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

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

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

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

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

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

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

[Mach-Valibouze] A. Mach, A. Valibouze, (1991), *L'idal des relations symtriques et l'idal des relations* prpublication

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

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

[MAXIMA] Maxima DOE ; MathLAP GROUP, **VAX UNIX MAXIMA, Reference manual**, Symbolics INC., Cambridge, MA, 1985

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

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

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

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

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

[avb1] A. Valibouze, (1988), *Manipulations de fonctions symétriques*, Thèse de l'Université Paris VI.

[avb2] A. Valibouze (1992) *Sur l'arité des fonctions*, European Journal of Combinatorics, 1993, **14**, 359-372

Laboratoire d'Algbre 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