Introduction à la Théorie de Galois Effective

Guénaël Renault

Introduction à la Théorie de Galois Effective

Draft version of 2008-10-13 00:33

http://www-salsa.lip6.fr/~renault/jncf08/

Guénaël Renault

Équipe-projet SALSA INRIA/LIP6 - Université Pierre et Marie Curie

Première partie

Prémices et définitions de la théorie de Galois

Préambule

Dans cette partie nous nous intéressons à la résolution d'équation de la forme

$$P(x) = 0$$

où P est un polynôme à coefficients dans $\mathbb{Q}$. Le problème principal qui a fait naître la théorie de Galois est de savoir si une telle équation peut toujours être résolue en exprimant ses solutions à partir de rationnels et de radicaux successifs. Le problème est résolu pour le degré 2 depuis l'antiquité. Celui des degrés 3 et 4 ont été résolu par les géomètres italiens du 16ème siècle (Fontana (dit Tartaglia), Cardan, Ferrari). La résolution des degrés supérieurs reste inconnue jusqu'àu 18ème siècle où, par les travaux de Vandermonde et Lagrange, on commence à entrevoir une explication que donnera Abel dans le cas du degré 5 et Galois en toute généralité.

Plutôt que de refaire la théorie de résolution par radicaux nous allons nous restreindre au problème suivant

Problème 1. Étant donnée une équation $P(x) = 0$ de degré n, est-il possible d'exprimer ses solutions en fonction de celles d'une équation de degré inférieur à n ?

Dans tout le restant de cette partie nous parlerons de manière équivalente des zéros du polynôme P et des solutions de l'équation $P(x) = 0$. Ainsi, tout au long de cette partie nous chercherons à exprimer le *corps des racines* du polynôme P, c'est-à-dire la plus petite extension de $\mathbb{Q}$ qui contient l'ensemble des zéros de P. Pour construire cette extension, nous allons ajouter successivement des valeurs irrationnelles au corps de base $\mathbb{Q}$ en considérant des extensions successives de ce corps. Ceci nous amènera à définir les objets fondamentaux de la théorie de Galois qui est effective par essence puisqu'elle fournit les méthodes de résolution du problème 1.

Nous commencerons, au chapitre 1, par voir comment les idées de Lagrange, développées pour la résolution des équations du degré 3 et 4, peuvent être vues comme les semences de cette théorie. Nous verrons ensuite, au chapitre 2, comment Galois donne une réponse infirmative au problème de la résolution d'équation par radicaux en faisant le lien entre deux catégories d'objets mathématiques : les groupes de permutations et les équations.

CHAPITRE 1

Lagrange : les prémices de théorie de Galois

1.1. Introduction

Ce chapitre retrace les travaux de Lagrange sur la résolution des équations de degré 3 et 4. Ces travaux sont exposés dans ses *Réflexions Sur La Résolution Algébrique Des Équations* (voir [29, Page 205]).

Dans ce mémoire, Lagrange donne un nouveau point de vue sur le problème en étudiant de manière systématique les méthodes pour la résolution d'équations par radicaux ; Vandermonde a aussi mené le même genre d'étude parallèlement à Lagrange mais le mémoire de ce dernier développe plus d'idées générales que celui de Vandermonde. Lagrange emploie les permutations comme outil de base pour cette étude sans introduire la notion de groupe que Galois donnera 60 ans plus tard. Il développe ainsi un cadre général pour expliquer la résolution des équations de degré inférieur à 5 et il propose de l'utiliser en toute généralité, sans aller plus loin.

Ainsi, dans son étude sur les méthodes de résolution par radicaux de l'équation $P(x) = 0$ de degré 3 ou 4, Lagrange se détache de l'empirisme classique. Au contraire, il donne dans son mémoire une vision novatrice pour la résolution des équations algébriques générales et, en particulier, comme il énonce le principe général de résolution de l'équation $P(x) = 0$ de degré n en essayant d'exhiber des formules qui permettent de construire ses solutions en fonctions de celles d'une équation de degré plus petit (voir Figure 1.1). Comme on peut le lire dans le résumé de ce principe, Lagrange ne considère

> **86.** On a dû voir par l'analyse que nous venons de donner des principales méthodes connues pour la résolution des équations, que ces méthodes se réduisent toutes à un même principe général, savoir à trouver des fonctions des racines de l'équation proposée, lesquelles soient telles : 1° que l'équation ou les équations par lesquelles elles seront données, c'est-à-dire dont elles seront les racines (équations qu'on nomme communément les *réduites*), se trouvent d'un degré moindre que celui de la proposée, ou soient au moins décomposables en d'autres équations d'un degré moindre que celui-là ; 2° que l'on puisse en déduire aisément les valeurs des racines cherchées.

FIG. 1.1. [29, Page 355]

pas des équations particulières mais il propose de calculer formellement avec les racines $x_1, \ldots, x_n$ du polynôme P.

Ainsi, toute son étude se fait à partir de l'équation générale de degré n. Pour cela, on considère $x_1, \ldots, x_n$ des variables algébriquement disjointes sur le corps $\mathbb{Q}$ et le *polynôme*

générique P ayant pour racines les x_i sera

$$P(x) = x^n + \sigma_1 x^{n-1} - \sigma_2 x^{n-2} + \ldots + (-1)^n \sigma_n$$

Les coefficients de P sont alors les n fonctions symétriques σ_i élémentaires en les $x_1, \ldots, x_n$ (au signe près). Le corps de base sur lequel nous commencerons tout notre raisonnement sera donc le corps $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$.

L'étude que fait Lagrange, sans avoir les objets mathématiques à disposition, est celle de l'extension $\mathbb{Q}(x_1, \ldots, x_n)$ sur $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ au regard du groupe symétrique S_n. Ceci peut se voir comme les prémices de la théorie que Galois développera plus tard.

1.2. Action du groupe des permutations et résolvantes absolues

À partir des racines $x_1, \ldots, x_n$ Lagrange montre comment construire de nouvelles équations dont il essaie de faire baisser le degré en utilisant des propriétés connues *a priori* (ceci correspond à la première étape de son principe). Cette étude *a priori* se fait en étudiant l'action du groupe symétrique S_n de degré n sur les éléments du corps de fonctions $\mathbb{Q}(x_1, \ldots, x_n)$. Sans les définir explicitement, il utilise les notions suivantes (rappelons encore une fois que la notion de groupe n'existait pas encore).

Définitions 1.1. *Soit $f(x_1, \ldots, x_n)$ une fonction de $\mathbb{Q}(x_1, \ldots, x_n)$ et ρ une permutation de S_n. L'action de ρ sur f est définie par*

$$\rho \cdot f = f(x_{\rho(1)}, \ldots, x_{\rho(n)}).$$

Pour un sous-groupe G de S_n le stabilisateur (ou groupe d'isotropie) de f dans G est définie et noté par

$$\mathrm{Stab}_G(f) = \{\rho \in G \,:\, \rho \cdot f = f\},$$

l'orbite de f sous l'action de G est le sous-ensemble de $\mathbb{Q}(x_1 \ldots, x_n)$ définie par

$$\mathrm{Orb}_G(f) = \{\rho \cdot f \,:\, \rho \in G\}$$

Soient $H \subset G$ deux sous-groupes de S_n un ensemble de représentants des classes de G/H est appelé transversale *à gauche.*

À partir d'une fonction f dans $\mathbb{Q}(x_1, \ldots, x_2)$, Lagrange considère le polynôme

$$\Theta_f(t) = \prod_{s \in S_n} (t - s \cdot f(x_1, \ldots, x_n))$$

Par construction, ce polynôme est stable sous l'action du groupe S_n sur les x_i, ainsi ses coefficients sont des fonctions symétriques des x_i et, d'après les travaux de Newton, bien connus par Lagrange, ses coefficients sont des éléments de $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$. En utilisant toujours ce principe, Lagrange va ramener la résolution de l'équation $P(x) = 0$ à celle de la résolution de plusieurs équations à coefficients dans ce corps. En des termes plus modernes, il va étudier le lien entre l'action de S_n sur les x_i et l'extension $\mathbb{Q}(x_1, \ldots, x_n)$ sur $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$.

À partir du polynôme Θ_f il essaye de trouver des facteurs *a priori* (ici le degré de Θ est $n!$). Plus exactement il étudie les différentes *formes* que peut prendre la fonction rationnelle f sous l'action des différentes permutations des racines de P. En des termes plus modernes, il exhibe l'orbite et le stabilisateur de f sous l'action de S_n. Il montre alors, que le cardinal du stabilisateur est un diviseur de l'ordre de S_n (ce résultat est énoncé aujourd'hui plus généralement pour tout groupe et porte de le nom de *Théorème de Lagrange*). Il en déduit que si le stabilisateur de f à un cardinal $k > 1$ alors le

polynôme Θ_f pourra se factoriser puisque des formes identiques vont se répéter lors de la construction. Lagrange propose alors de ne considérer qu'un facteur de Θ_f.

DÉFINITION 1.2. *Soit $f \in \mathbb{Q}(x_1, \ldots, x_n)$ la* résolvante absolue *de f est définie par*

$$\theta_f(t) = \prod_{g \in \mathrm{Orb}_{S_n}(f)} (t - g).$$

D'après ce que nous venons de voir, nous connaissons *a priori* le degré du polynôme θ_f et plus généralement nous avons le résultat suivant.

PROPOSITION 1.3. *La résolvante θ est un polynôme à coefficients dans $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ qui est séparable et de degré $\frac{n!}{k}$.*

On peut montrer aussi que ce polynôme est irréductible sur $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$, nous verrons cela au chapitre suivant.

Il sera donc toujours possible de construire une résolvante à coefficients dans le corps $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ mais qu'en sera-t-il de ses solutions ? Pourrons nous les exprimer à partir de quantités connues ? Le résultat qui suit donne une réponse à ces questions, Lagrange le donne dans [29, Article 104] et ceci peut être vu comme le point de départ à la théorie de Galois.

THÉORÈME 1.4. *Soit f et g deux fonctions de $\mathbb{Q}(x_1, \ldots, x_n)$ telles que $\mathrm{Stab}_{S_n}(f)$ soit inclus dans $\mathrm{Stab}_{S_n}(g)$. Alors g est une fonction rationnelle de f à coefficients dans $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$*

Une traduction en terme de théorie des corps et des groupes de ce théorème peut se voir comme suit. Posons $K = \mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ et $L = \mathbb{Q}(x_1, \ldots, x_n)$, nous avons le diagramme d'inclusion qui suit

$$\begin{array}{ccccccc} K & \hookrightarrow & K(g) & \hookrightarrow & K(f) & \hookrightarrow & L \\ | & & | & & | & & | \\ S_n & \hookleftarrow & \mathrm{Stab}_{S_n}(g) & \hookleftarrow & \mathrm{Stab}_{S_n}(f) & \hookleftarrow & \langle \mathrm{Id} \rangle \end{array}$$

Rappelons que les racines des résolvantes que nous considérons sont des fonctions rationnelles des $x_1, \ldots, x_n$. Ainsi, ce théorème nous montre qu'il est possible d'exprimer les racines de θ_g à partir des coefficients du polynôme de départ P et des racines de θ_f. On en déduit une méthode pour dévisser le problème de départ : on cherche une suite décroissante de groupes de S_n et des fonctions de $\mathbb{Q}(x_1, \ldots, x_n)$ stables par chacun des éléments de cette suite. On forme les résolvantes correspondant et on les résout en utilisant les racines des précédentes plutôt que de se restreindre au corps de base $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$. On recommence le procédé jusqu'à pouvoir exprimer les racines $x_1, \ldots, x_n$ de l'équation de départ en fonction de celles que nous avons calculées tout au long du procédé. En résumé, on construit des extensions intermédiaires entre $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ et $\mathbb{Q}(x_1, \ldots, x_n)$ en adjoignant des fonctions rationnelles des racines de l'équation de départ jusqu'à atteindre son corps des racines.

La démonstration que nous donnons pour ce théorème est une reformulation de celle Lagrange, tout comme la version originelle elle est constructive et se base sur des principes d'interpolation.

DÉMONSTRATION DU THÉORÈME 1.4. Soient $f = f_1, \ldots, f_r$ les différentes images de la fonction f sous l'action de S_n, chacun de ces éléments correspond à une classe à gauche

de $\mathrm{Stab}_{S_n}(f)$ dans S_n, en d'autres termes, pour $i = 1, \ldots, r$ il existe un unique $\sigma_i \in S_n$ tel que $f_i = \sigma_i \,\mathrm{Stab}_{S_n}(f) \cdot f$ (la suite finie $\mathrm{Id} = \sigma_1, \ldots . \sigma_r$ est appelée transversale pour ce quotient à gauche). D'après les hypothèses faites sur f et g, nous avons r images distincts de g en considérants les éléments $\sigma_1 \cdot g, \ldots, \sigma_r \cdot g$.

Soit la fonction interpolatrice

$$I(x) = \theta_f(x) \left(\frac{g_1}{x - f_1} + \cdots + \frac{g_r}{x - f_r} \right)$$

Rappelons que la résolvante est stable sous l'action de S_n, ainsi, cette action sur I ne fait que permuter les éléments de la somme et donc I reste globalement stable. Ce qui implique que I est à coefficients dans $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$.

En évaluant I en f_1 on obtient

$$I(f_1) = g_1 \prod_{i=2}^{r} (f_1 - f_i)$$

et comme $\theta_f(x) = \prod_{i=1}^{r}(x - f_i)$ on a $\theta'_f(f_1) = \prod_{i=2}^{r}(f_1 - f_i)$ et finalement on obtient une expression de g comme fonction rationnelle d'éléments de $\mathbb{Q}(\sigma_1, \ldots, \sigma_n, f)$

$$g = \frac{I(f)}{\theta'_f(f)}.$$

ce qui termine la démonstration. □

Nous avons vu jusque là comment l'adjonction de fonction des racines permet de remonter de proche en proche vers le corps $\mathbb{Q}(x_1, \ldots, x_n)$ et donc vers les racines de l'équation de départ. Nous allons voir maintenant comment l'adjonction de racines de polynômes indépendants de l'équation de départ permet aussi de la réduire et surtout comment exprimér les racines $x_1, \ldots, x_n$ en fonction de ces dernières.

1.3. Racine n-ème de l'unité et résolvantes de Lagrange

Dans cette section, on lâche un peu de contrainte sur la résolution du problème 1 en autorisant l'adjonction de racines primitives de l'unité au corps de base et, de manière équivalente, l'extraction de racine est permise. Ceci est une hypothèse standard pour la résolution par radicaux.

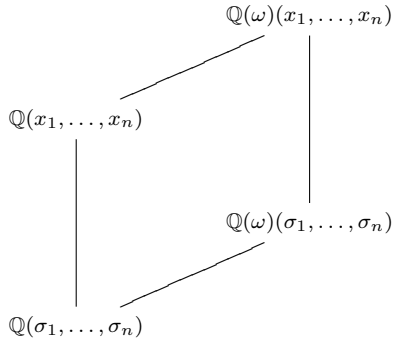
Bézout, dans son article sur la résolution des équations par radicaux, met en avant l'utilisation des racines n-ème pour mener à bien les résolution des équations de degré 3 et 4 et propose d'en faire usage dans un cadre plus général mais sans être concluant. C'est Lagrange qui proposa cette méthode générale. Pour ce faire il construit ce que nous appelons aujourd'hui les *résolvantes de Lagrange* et qui interviennent généralement dans la construction des extensions cycliques.

Définition 1.5. *Soit ω une racine primitive n-ème de l'unité la* résolvante de Lagrange *est la résolvante absolue qui a pour racine la fonction rationnelle t_1 définie par :*

$$t_1 = x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{n-1} x_n$$

D'un point de vue des extensions de corps, pour pouvoir considérer de telles résolvantes, Lagrange a donc effectué une translation par adjonction de ω la racine n-ème de

l'unité. Ceci peut se résumer comme suit :



Même si Lagrange a mené une étude générale sur les résolvantes absolues, celles qui portent son nom sont celles qu'il a le plus étudiées. En effet, il a découvert qu'elles sont la clé pour la résolution des équations 3 et 4. Ces résolvantes particulières ont de multiples propriétés qu'il exhibe et utilise tout au long de son mémoire. Par exemple, puisque ce sont des résolvantes absolues, d'après la proposition 1.3, ces résolvantes sont à coefficients dans $\mathbb{Q}(\omega)(\sigma_1,\ldots,\sigma_n)$ et de degré $n!$, on peut aussi montrer qu'elles sont à coefficients dans $\mathbb{Q}(\sigma_1,\ldots,\sigma_n)$. Ces résolvantes particulières ont deux propriétés importantes pour ce qui est de la résolution de l'équation $P(x)=0$:

(1) les solutions de cette équations peuvent être exprimées en fonctions des racines de la résolvante de Lagrange qui correspond ;

(2) la résolvante de Lagrange peut être décomposée.

Ce sont ces deux propriétés que nous allons présenter maintenant.

Commençons par voir comment on peut décomposer une telle résolvante. On peut facilement voir que l'action des puissances du cycle $\sigma=(1,2,\ldots,n)$ sur t_1 nous donne

$$\sigma^k\cdot t_1=\omega^k t_1$$

ainsi tous les $\omega^k t_1$ seront aussi des racines pour la résolvante de Lagrange et on en conclut que chacun de ses monômes ne pourra être que d'un degré un facteur de n. En faisant un changement de variable, on peut alors résoudre un polynôme de degré $(n-1)!$ qui aura pour racine $T_1=t_1^n$. Les autres racines de ce polynômes seront obtenues en permutant les $x_2,\ldots,x_n$ dans T_1.

Ainsi, plutôt que de résoudre une équation de degré $n!$ pour retrouver t_1, on pourra résoudre une équation de degré $(n-1)!$ et extraire une racine n-ème.

Voyons maintenant comment déduire les racines x_i à partir des t_i. Par construction, la racine T_1 s'écrira

$$T_1=\zeta_1+\omega\zeta_2+\cdots+\omega^{n-1}\zeta_n$$

où chacun des ζ_i est une fonction rationnelle des x_i qui est stable sous l'action du groupe cyclique engendré par le cycle $(1,2,\ldots,n)$. Dès que les ζ_i sont connues, nous allons voir comment en déduire les racines x_i par les formules que l'on construit ci-après.

Notons plus généralement

$$t_i=x_1+\omega^i x_2+\omega^{i2}x_3+\cdots+\omega^{i(n-1)}x_n\quad(i=0,\ldots,n-1)$$

et $T_i=t_i^n$, (on retrouve les t_1 et T_1 définis précédemment). Alors nous avons

$$x_i=\frac{1}{n}(t_0+\sum_{j=1}^{n-1}\omega^i t_j)=\frac{1}{n}(t_0+\sum_{j=1}^{n-1}\omega^i\sqrt[n]{T_j})$$

Pour calculer les T_j (ou de manière équivalente les ζ_i), Lagrange propose une première méthode basée sur l'élimination mais il préfère considérer le polynôme de degré $n-1$ dont les racines sont $T_1, T_2, \ldots, T_{n-1}$. Il montre que dans le cas où n est premier les coefficients de ce polynôme peuvent être calculés en résolvant une équation de degré $(n-2)!$ ce qui lui fait penser (voir Figure 1.2) qu'il n'y a que très peu de chance de voir ce type de résolvantes utilisées pour résoudre l'équation générale de degré 5 et que si elle pouvait être résolue alors il faudrait employer un nouveau type de résolvantes.

109. Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire; tout se réduit, comme on voit, à une espèce de calcul des combinaisons, par lequel on trouve *à priori* les résultats auxquels on doit s'attendre. Il serait à propos d'en faire l'application aux équations du cinquième degré et des degrés supérieurs, dont la résolution est jusqu'à présent inconnue; mais cette application demande un trop grand nombre de recherches et de combinaisons, dont le succès est encore d'ailleurs fort douteux, pour que nous puissions quant à présent nous livrer à ce travail; nous espérons cependant pouvoir y revenir dans un autre temps, et nous nous contenterons ici d'avoir posé les fondements d'une théorie qui nous paraît nouvelle et générale.

FIG. 1.2. [29, Page 403]

1.4. Résolution des équations de degré trois et quatre vue par Lagrange

Voyons comment Lagrange résout l'équation de degré 3 et 4 avec les résultats que nous venons de présenter.

1.4.1. Équations de degré 3. Soit à résoudre l'équation générale du troisième degré, on peut toujours se ramener, après un changement de variable (transformation de Tschirnhaus), à la résolution de l'équation $P(x) = 0$ avec

$$P(x) = x^3 + 3px + 2q = (x - x_1)(x - x_2)(x - x_3)$$

Ici $n = 3$ ainsi $(n-1)! = 2$ et l'utilisation des résolvantes de Lagrange est tout indiquée puisque l'on sait résoudre une équation de degré 2. Soit j la racine primitive du troisième degré, plutôt que de considérer la fonction $(x_1 + jx_2 + j^2x_3)$ nous allons, pour faciliter l'écriture des solutions, prendre $T_1 = (\frac{1}{3}(x_1 + jx_2 + j^2x_3))^3$. T_1 étant stable sous l'action du groupe cyclique engendré par le cycle $(1, 2, 3)$, la deuxième forme possible de T_1 sous l'action de S_3 est

$$T_2 = (1, 2)T_1 = (\frac{1}{3}(x_2 + jx_1 + j^2x_3))^3$$

et l'on obtient le polynôme de degré 2

$$(x - T_1)(x - T_2)$$

stable sous l'action de S_3, donc ses coefficients pourront s'écrire comme fonction rationnelles de $\mathbb{Q}(j)(p, q)$ en vertu du théorème 1.4. Plus exactement, ce polynôme est à coefficients dans $\mathbb{Q}(p, q)$ et est donné par :

$$(x - T_1)(x - T_2) = x^2 + 2qx - p^3 = (x + q + s)(x + q - s)$$

où s est une des deux racines carrées de p^3+q^2. On obtient donc une résolution de cette équation et nous obtenons les valeurs de T_1 et T_2. On peut donc en déduire les valeurs de x_1, x_2, x_3 :

$$x_i = j^i \sqrt[3]{T_1} + j^i \sqrt[3]{T_2}$$

Ceci termine la résolution de l'équation générale du degré 3. La résolvante exhibée ici par Lagrange permet de retrouver la méthode de Cardan.

1.4.2. Équations de degré 4. Passons maintenant à la résolution de l'équation générale de degré 4. Soit à résoudre l'équation générale $P(x) = 0$ avec

$$P(x) = x^4 - \sigma_1 x^3 + \sigma_2 x^2 - \sigma_3 x + \sigma_4$$

Dans ce cas $(n-1)! = 6$, ainsi l'application directe des résolvantes de Lagrange ne suffit pas à résoudre le problème. Soit f la fonction rationnelle $x_1x_2 + x_3x_4$ qui est laissée stable par le groupe H d'ordre 8 engendré par $\{(1,2), (3,4), (1,3,2,4)\}$. D'après la proposition 1.3, la résolvante correspondante sera de degré 3. Soient y_1, y_2, y_3 ses trois racines :

$$y_1 = x_1x_2 + x_3x_4,\ y_2 = x_1x_3 + x_2x_4,\ y_3 = x_3x_2 + x_1x_4$$

cette résolvante $(y-y_1)(y-y_2)(y-y_3)$ sera alors à coefficients dans $\mathbb{Q}(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ et peut être calculée explicitement :

$$y^3 - \sigma_2 y^2 + (\sigma_1\sigma_3 - 4\sigma_4)y - (\sigma_3^2 + \sigma_1^2\sigma^4 - 4\sigma_2\sigma_4)$$

Ses racines sont calculables par la méthode du degré 3 vue ci-avant, reste alors à pouvoir exprimer les solutions de départ x_1, x_2, x_3, x_4 en fonction de ces dernières. Pour ce faire, on peut considérer une résolvante de Lagrange qui a l'avantage d'avoir ses solutions facilement exprimables à partir des x_i et *vice versa*. Pour utiliser le calcul déjà fait ici et ne pas avoir à résoudre une équation de degré 6, il faut pourvoir exprimer les racines de cette résolvante de Lagrange en fonction des y_i en espérant réduire la taille des calculs. Pour cela, on utilise le théorème 1.4, on procède à une analyse préalable sur les sous-groupes de S_4.

Plutôt que de considérer une racine 4-ème de l'unité, Lagrange propose de découper le problème selon les facteurs du degré de l'équation de départ. Ici, $4 = 2 \times 2$, il suffit donc de considérer ω une racine carrée primitive de l'unité (donc $\omega = -1$) et de former des sommes de racines. Nous ne ferrons pas ici l'analyse de toute cette théorie, mais le lecteur pourra retrouver ceci dans le mémoire de Lagrange. Soit donc la fonction rationnelle $t = (x_1 + x_2) - (x_3 + x_4)$, cette dernière est elle aussi laissée stable par le groupe H, ainsi par le théorème 1.4, la fonction rationnelle t peut s'écrire comme fonction rationnelle de $\mathbb{Q}(\sigma_1, \ldots, \sigma_4, y_1)$ et nous obtenons un polynôme de degré 2 à résoudre :

$$t^2 - 4y_1 - \sigma_1^2 + 4\sigma_2$$

Ainsi, en changeant y_1 en y_2 et y_3 nous avons trois couples de conjugués t_i

$$t_i = \pm\sqrt{-4y_i - \sigma_1^2 + 4\sigma_2}$$

Reste un problème : comment choisir le conjugué de t_i (un par équation de degré 2) afin de reconstruire les racines x_i comme vue ci-avant ? Lagrange montre qu'il suffit de choisir deux racines t_1 et t_2 et la troisième sera donnée par la relation

$$t_1t_2t_3 = \sigma^3 - 4\sigma_1\sigma_2 + 8\sigma_3$$

qui s'obtient en utilisant le fait que la fonction rationnelle $t_1t_2t_3$ est stable sous l'action de S_4 et peut donc s'écrire dans $\mathbb{Q}(\sigma_1, \ldots, \sigma_4)$.

D'un point de vue moderne, Lagrange dévisse l'extension $\mathbb{Q}(x_1, \ldots, x_4)/\mathbb{Q}(\sigma_1, \ldots, \sigma_4)$ en construisant deux étapes intermédiaires et ceci à partir de fonctions rationnelles choisies après une étude faite sur le groupe S_4 :

$$K = \mathbb{Q}(\sigma_1, \ldots, \sigma_4) \subset K(y_1) \subset K(t_1) \subset \mathbb{Q}(x_1, x_2, x_3, x_4)$$

1.5. Conclusion

Les travaux de Lagrange ont permis de sortir le problème de la résolution d'équations de l'empirisme dans lequel il était plongé depuis l'antiquité. Il a développé les premières interactions entre résolution d'équations et étude des permutations des solutions qui vont permettre à Abel et Galois de donner un cadre théorique satisfaisant à ce problème, c'est ce qui va être présenté dans le chapitre suivant.

CHAPITRE 2

Définition du groupe de l'équation et résolution

2.1. Introduction

C'est Abel qui donne une réponse négative au doute de Lagrange sur la possibilité de résoudre une équation de degré 5 et Galois fournit la théorie permettant de répondre à cette question en toute généralité. Ces deux démonstrations se basent sur les travaux de Lagrange et mettent en relation la théorie des groupes de permutations et celles des corps.

Dans le chapitre 1 nous avons cherché à résoudre l'équation générale de degré n. À partir de maintenant, le polynôme P étudié sera à coefficients spécifiés dans $\mathbb{Q}$ et ses racines $(\alpha_1, \ldots, \alpha_n)$ seront algébriquement liées, toutefois, nous les supposerons simples. Ainsi, le corps $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ est isomorphe à l'anneau $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ et donc, plutôt que de considérer des fonctions des racines de l'équation comme précédemment, nous considérerons des évaluations de polynômes multivariés en les racines de P.

Une autre différence importante avec ce qui a été vu précédemment est le caractère séparable et irréductible des résolvantes considérées. En effet, les racines de l'équation étant liées algébriquement, il se peut qu'une résolvante ait deux racines égales. On verra que l'on peut toujours construire une résolvante séparable et donc se ramener a ce que l'on a vu précédemment, notamment utiliser le théorème 1.4.

Dans tout ce chapitre, le corps de base $\mathbb{Q}$ peut être remplacé par un corps de caractéristique 0, les démonstrations resteront les mêmes.

2.1.1. Résolvante et groupe de Galois. Soit P un polynôme à coefficients dans $\mathbb{Q}$ de degré n et supposé séparable. Nous allons construire une résolvante séparable qui nous permettra de d'exprimer le n-uplet $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ des solutions de l'équation $P(x) = 0$ en fonction de celles de cette dernière. D'après le théorème 1.4 il suffit de trouver un polynôme qui, après évaluation des permutations des racines de P, donne $n!$ valeurs différentes. C'est exactement ce que propose Galois dans son mémoire [18] et ceci ce traduit par le résultat suivant.

Proposition-Définition 2.1. *Il existe un n-uplet d'entiers $(k_1, \ldots, k_n)$ tel que, en notant $V \in \mathbb{Q}[x_1, \ldots, x_n]$ le polynôme $k_1x_1 + \cdots, k_nx_n$ et $\mathcal{O}$ son orbite sous l'action de S_n, l'ensemble*

$$\{g(\underline{\alpha}) \,:\, g \in \mathcal{O}\}$$

soit de cardinal $n!$. La résolvante de degré $n!$ correspondant à cet ensemble est appelée résolvante de Galois.

Démonstration. Puisque le corps $\mathbb{Q}$ est infini l'anneau des entiers s'injecte dans ce dernier. Comme les α_i sont distinctes on pourra toujours trouver un n-uplet d'entiers qui soit à l'extérieur de l'ensemble fini des solutions du système formé des équations $k_1(\alpha_1 - \alpha_{\sigma(1)}) + \cdots + k_n(\alpha_n - \alpha_{\sigma(n)})$ avec $\sigma \in S_n$. □

Galois ne donne pas de preuve pour cette proposition qui lui semble immédiate. C'est ce qui lui vaudra, en partie, les mauvais commentaires de Poisson lors de la lecture de son mémoire.

D'après le théorème 1.4, comme le polynôme V est laissé stable par un unique élément, l'identité dans S_n, nous pouvons identifier les racines $\alpha_1, \ldots, \alpha_n$ à des éléments de $\mathbb{Q}(V)$, en des termes plus modernes, nous venons de montrer comment construire un *élément primitif* pour le corps $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Même si Lagrange avait tous les éléments pour établir un tel résultat, c'est bien Galois qui le donne en premier (voir Figure 2.1).

Lemme III. « La fonction V étant choisie comme il est indiqué » dans l'article précédent, elle jouira de cette propriété, que toutes » les racines de l'équation proposée s'exprimeront rationnellement en fonction de V. »

FIG. 2.1. [18, Page 420]

Comme nous venons de le voir, pour qu'une résolvante de Galois soit séparable il faut pouvoir donner un polynôme V qui soit spécifique au polynôme P ou, de manière équivalente, à ses racines $\underline{\alpha}$. Nous définissons ainsi la notion importante qui suit.

DÉFINITIONS 2.2. *Soient $H \subset G$ deux sous-groupes de S_n. Un polynôme de $\mathbb{Q}[x_1, \ldots, x_n]$ dont le stabilisateur dans G est H est appelé* H-invariant G-relatif *et sera noté I_H^G. Lorsque $G = S_n$ on dira juste H-invariant et on le notera I_H.*

Un H-invariant G-relatif est dit $\underline{\alpha}$-séparant *si l'ensemble $\{(\sigma \cdot I_H^G)(\underline{\alpha}) : \sigma \in G\}$ est de cardinal $\frac{|G|}{|H|}$*

Étant donné I_H un H-invariant, pour que la résolvante correspondante soit séparable il faut et il suffit que I_H soit $\underline{\alpha}$-séparant. Comment pouvons nous être sur qu'un tel H-invariant existe ? En fait il est toujours possible de construire un tel polynôme à partir du $\langle \mathrm{Id} \rangle$-invariant utilisé dans la définition de la résolvante de Galois mais nous verrons à la section 3.4 comment en obtenir un plus efficacement.

À un H-invariant relatif, nous allons associer la notion plus générale de résolvante relative. Jusqu'à présent, les résolvantes que nous avons rencontrées étaient construites en étudiants des orbites de l'action du groupe S_n, nous allons maintenant généraliser ce principe pour des sous-groupes de S_n.

PROPOSITION-DÉFINITION 2.3. *Soient $H \subset G$ deux sous-groupes de S_n et I un H-invariant G-relatif. Le polynôme*

$$\theta_I(t) = \prod_{\gamma \in \mathrm{Orb}_G(I)} (t - \gamma(\underline{\alpha}))$$

est appelé résolvante G-relative de $\underline{\alpha}$ *(les résolvantes S_n-relative sont les résolvantes absolues).*

Le degré de θ_I est donné par $\frac{|G|}{|H|}$, de plus, si l'invariant I est $\underline{\alpha}$-séparant alors θ_I sera séparable.

Nous venons de définir la résolvante de Galois comme une résolvante absolue construite à partir d'un $\langle \mathrm{Id} \rangle$-invariant $\underline{\alpha}$-séparant. Cette résolvante a pour racine un élément $V(\underline{\alpha})$ permettant de définir toutes les solutions de l'équation $P(x) = 0$. Son degré est donné par $n!$ mais *a priori* n'est pas irréductible (contrairement à ce que nous avons pu voir

au chapitre précédent où les racines de P étaient algébriquement libres). Nous allons maintenant chercher à retrouver un facteur irréductible de cette résolvante qui s'annule en $V(\underline{\alpha})$, en fait, nous construisons un *polynôme minimal* de $V(\underline{\alpha})$ à partir d'un sous-groupe G de S_n.

THÉORÈME 2.4. *Soit V un $\langle \mathrm{Id} \rangle$-invariant $\underline{\alpha}$-séparant et θ_V la résolvante de Galois correspondant. Il existe un sous groupe G de S_n tel que*

$$\mu_V(x) = \prod_{g \in G} (x - (g \cdot V)(\underline{\alpha}))$$

soit un facteur irréductible à coefficients dans $\mathbb{Q}$ de θ_V s'annulant en $V(\underline{\alpha})$.

Le groupe G est caractérisé par le fait qu'un polynôme $W \in \mathbb{Q}[x_1, \ldots, x_n]$ évalué en les racines $\underline{\alpha}$ est à valeur dans $\mathbb{Q}$ si et seulement si $W(\underline{\alpha})$ est stable sous l'action de G (i.e. $\forall g \in G$, $(g \cdot W)(\underline{\alpha}) = W(\underline{\alpha})$).

DÉMONSTRATION. Soit G le sous-ensemble de S_n contenant Id tel que

$$\mu_V = \prod_{g \in G} (x - (g \cdot V)(\underline{\alpha}))$$

soit un facteur irréductible sur $\mathbb{Q}$ de θ_V s'annulant en $V(\underline{\alpha})$, notons k son degré.

Soit $W(\underline{\alpha})$ un élément de $\mathbb{Q}(\underline{\alpha})$ qui reste invariable sous l'action des éléments de G. D'après le théorème 1.4 cet élément s'exprime rationnellement en $V(\underline{\alpha})$, i.e. il existe un polynôme ψ en une variable à coefficients dans $\mathbb{Q}$ tel que

$$W(\underline{\alpha}) = \psi(V(\underline{\alpha})).$$

Par hypothèse, $\psi(V(\underline{\alpha}))$ reste invariable sous l'action des éléments de G. Ainsi,

$$\psi(V(\underline{\alpha})) = \frac{1}{k} \left(\sum_{g \in G} \psi((g \cdot V)(\underline{\alpha})) \right)$$

et la partie de droite de l'expression précédente est une fonction symétrique des racines du polynôme $\mu_V \circ \psi$ qui sera rationnel, donc $W(\underline{\alpha}) \in \mathbb{Q}$.

Réciproquement, supposons que $W(\underline{\alpha})$ soit rationnelle. Il existe un polynôme ψ tel que $\psi(V(\underline{\alpha})) = W(\underline{\alpha})$ soit rationnel. Ainsi le polynôme $\psi(x) - W(\underline{\alpha})$ est à coefficients dans $\mathbb{Q}$ et s'annule en $V(\underline{\alpha})$, comme μ_V est irréductible, ce polynôme s'annule en toutes les racines de μ_V et donc $\psi((e \cdot V)(\underline{\alpha})) = W(\underline{\alpha})$ pour tout e dans G. On en conclut que $W(\underline{\alpha})$ est stable sous l'action des éléments de G.

Reste à montrer que G est un groupe. D'après ce que nous venons de voir, comme les coefficients de μ_V sont des éléments de $\mathbb{Q}(\underline{\alpha})$ qui sont rationnels ils doivent être stable sous l'action des éléments de G. En conséquence, le polynôme μ_V est stable sous l'action de ces mêmes éléments. Pour qu'il en soit ainsi, il faut et il suffit que cette action se traduise par la permutation des facteur binômes entrant dans la définition de ce polynôme. Comme $\mathrm{Id} \in G$ on se rend compte rapidement que pour tout élément $g \in G$ son inverse sera présent dans G et donc G est un sous-groupe de S_n. □

Ce théorème nous donne une condition nécessaire et suffisante pour qu'un élément de $\mathbb{Q}(\underline{\alpha})$ soit rationnel, cette condition se faisant à l'aide d'un groupe, ce théorème est le point central de la théorie de Galois.

PROPOSITION-DÉFINITION 2.5. *Le groupe G du théorème précédent ne dépend pas du choix de l'élément primitif $V(\underline{\alpha})$ et est appelé* groupe de Galois sur $\mathbb{Q}$ *de P. Par contre, le groupe G dépend de l'ordre donné aux racines de P, pour être plus précis, on parlera donc du groupe de Galois de l'extension $\mathbb{Q}(\underline{\alpha})$ sur $\mathbb{Q}$ et que l'on notera* $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$.

DÉMONSTRATION. Soit $V'(\underline{\alpha})$ un deuxième élément primitif pour $\mathbb{Q}(\underline{\alpha})$. Le polynôme minimal $\mu_{V'}$ de cet élément est rationnel ainsi, d'après le théorème 2.4, tous les éléments du groupe de Galois G (obtenu à partir de $V(\underline{\alpha})$) doivent le stabiliser. Soit G' le groupe de Galois défini à partir de $V'(\underline{\alpha})$. Par définition, nous avons

$$\mu_{V'}(x) = \prod_{g \in G'} (x - (g \cdot V')(\underline{\alpha}))$$

et donc pour que les éléments de G stabilisent ce polynôme il faut qu'ils s'identifient à ceux de G'. En échangeant le rôle de G et G' on obtient l'égalité entre ces deux groupes. □

Le théorème 2.4 permet de caractériser les éléments rationnels de $\mathbb{Q}(\underline{\alpha})$ à partir d'un groupe de permutations. Nous allons maintenant voir comment caractériser ses sous-corps à partir des sous-groupes de $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$ mais avant de donner ces résultats, nous donnons ici une traduction du théorème de Lagrange (Théorème 1.4) avec ce nouveau regard galoisien.

THÉORÈME 2.6. *Soit β_1 et β_2 deux éléments de $\mathbb{Q}(\underline{\alpha})$ tels que $\mathrm{Stab}_G(\beta_1)$ soit inclus dans $\mathrm{Stab}_G(\beta_2)$ où G est le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$. Alors β_2 est un élément de $\mathbb{Q}(\beta_1)$*

DÉMONSTRATION. La démonstration du théorème 1.4 peut être reprise *mutatis mutandis* en utilisant la caractérisation du groupe de Galois. □

Les deux lemmes qui suivent nous donnent les premiers résultats de correspondance entre les sous-groupes du groupe de Galois et des sous-corps du corps de décomposition.

LEMME 2.7. *Soit H un sous-groupe de $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$. L'ensemble des éléments de $\mathbb{Q}(\underline{\alpha})$ laissés stables sous l'action de H forme un sous-corps de $\mathbb{Q}(\underline{\alpha})$ noté $\mathbb{Q}(\underline{\alpha})^H$*

DÉMONSTRATION. Il est immédiat de vérifier que la partie $\mathbb{Q}(\underline{\alpha})^H$ de $\mathbb{Q}(\underline{\alpha})$ est un corps. □

LEMME 2.8. *Soit L une extension intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(\underline{\alpha})$. Le groupe de Galois de $\mathbb{Q}(\underline{\alpha})$ sur L est un sous-groupe de $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$, il est noté $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/L)$.*

Pour rester dans l'esprit de la résolution de l'équation $P(x) = 0$ le lemme qui précède peut se reécrire de la manière suivante : soit f un polynôme irréductible ayant une racine β dans $\mathbb{Q}(\underline{\alpha})$. Le groupe de Galois de P vu à coefficients dans $\mathbb{Q}(\beta)$ est un sous-groupe de $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$. En d'autres termes, en rajoutant des solutions de l'équation $f(x) = 0$ au problème de départ (la résolution de $P(x) = 0$), ce dernier devient moins difficile puisque que le groupe à considérer s'affine, et le nombre de permutations à considérer est donc plus petit.

DÉMONSTRATION. Soit β un élément primitif de L sur $\mathbb{Q}$. L'ensemble des éléments de $G = \mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$ qui stabilisent β est le sous-groupe de G défini par $H = \mathrm{Stab}_G(\beta)$. Par la caractérisation du groupe de Galois (voir le théorème 2.4) on a alors $H = \mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q}(\beta))$. □

Des deux lemmes précédents et du théorème 2.4 on déduit le résultat suivant.

THÉORÈME 2.9. *(Correspondance galoisienne) Soient $\mathcal{G}$ l'ensemble des sous-groupes de $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$ et $\mathcal{K}$ l'ensemble des sous-corps de $\mathbb{Q}(\underline{\alpha})$. L'application qui fait correspondre un élément H de $\mathcal{G}$ le sous-corps $\mathbb{Q}(\underline{\alpha})^H$ des éléments de $\mathbb{Q}(\underline{\alpha})$ laissés stables sous l'action de H est bijective.*

Les lemmes précédents sont très théoriques, ils nous donnent l'existence d'un corps correspondant à un sous-groupe du groupe de Galois mais, ils ne donnent aucun moyen de le définir explicitement. La proposition qui suit résout ce problème. Ce résultat est fondamental pour l'utilisation des résolvantes relatives en théorie de Galois.

PROPOSITION 2.10. *Soit L une extension intermédiaire entre $\mathbb{Q}(\underline{\alpha})$ et $\mathbb{Q}$ correspondant à un sous-groupe H de $G = \mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$ et soit I un H-invariant G-relatif supposé $\underline{\alpha}$-séparable. La résolvante relative*

$$\theta_I(t) = \prod_{\gamma \in \mathrm{Orb}_G(I)} (t - \gamma(\underline{\alpha}))$$

est un polynôme définissant L sur $\mathbb{Q}$. En particulier, le degré $[L : \mathbb{Q}]$ est donné par le degré $\frac{|G|}{|H|}$ de cette résolvante.

En d'autres termes, cette proposition nous donne la définition d'un élément minimal de L sur $\mathbb{Q}$ défini par $I(\underline{\alpha})$ qui est de polynôme minimal $\theta_I(t)$.

DÉMONSTRATION. Montrons que le polynôme θ_I ainsi défini est un polynôme irréductible à coefficients dans $\mathbb{Q}$. Le fait qu'il soit à coefficients dans $\mathbb{Q}$ découle du théorème 2.4 puisque les coefficients de θ_I sont stable par G par construction.

Supposons que θ_I soit réductible, alors il existe E un sous-ensemble strict de $G//H$ contenant Id tel que

$$f(t) = \prod_{\tau \in E} (t - (\tau \cdot I)(\underline{\alpha}))$$

soit un polynôme annulateur de $I(\underline{\alpha})$ à coefficients dans $\mathbb{Q}$. D'après la caractérisation du groupe de Galois (voir le théorème 2.4) le polynôme f doit donc être stable sous l'action G. Ainsi, si on prend un élément τ de $G//H$ en dehors de E, le polynôme $\tau \cdot f$ doit rester inchangé sans pouvoir être annulateur de $I(\underline{\alpha})$ puisque I est supposé $\underline{\alpha}$-séparant, ce qui est absurde. Ainsi, le polynôme θ_I est irréductible sur $\mathbb{Q}$.

Le corps $\mathbb{Q}(I(\underline{\alpha}))$ est laissé stable par les éléments de H par hypothèse sur I, ainsi $\mathbb{Q}(I(\underline{\alpha})) \subset \mathbb{Q}(\underline{\alpha})^H$. Pour obtenir l'inclusion inverse, il suffit d'appliquer le théorème 2.6. □

Maintenant que nous avons défini l'objet essentiel de ce cours voyons son application pour la résolution de l'équation $P(x) = 0$.

2.1.2. Quelques propriétés sur les groupes de permutations finis. Puisque nous allons utiliser des résultats sur les groupes de permutations finis, nous rappelons ici certaines de leurs propriétés et définitions. Dans toute la suite nous étudions l'action canonique du groupe symétrique sur l'ensemble $X = \{1 \ldots, n\}$. Les définitions que nous donnons ici seront données sur les sous-groupes de S_n plutôt que sur les actions correspondantes.

DÉFINITION 2.11. *Un sous-groupe G de S_n est dit* transitif *si pour tout entier i de $\{1, \ldots, n\}$ il existe un élément $g \in G$ tel que $g(1) = i$.*

Soit G un sous-groupe de S_n et Π une partition de l'ensemble X. Nous dirons que G stabilise Π dès que, pour tout ensemble e de Π on a $\{g \cdot e \, : \, g \in G\} \in \Pi$. Nous appellerons partition triviale d'un ensemble E la partition réduit au seul élément E et celle composée des singletons. Il est clair que tout sous-groupe G de S_n stabilise les partitions triviales de X, les groupes qui ne stabilisent que ceux ci sont :.

DÉFINITIONS 2.12. *Un sous-groupe G de S_n est dit* primitif *s'il ne stabilise que les partitions triviales de X. Dans le cas contraire le groupe G sera dit* imprimitif. *Une partition de X qui est stable sous l'action de d'un groupe imprimitif est appelé* système complet de bloc (d'imprimitivité).

L'exemple le plus simple de groupe imprimitif est S_n pour $n > 0$. Les groupes primitifs sont rares, par exemple, on ne connaît pas de formule simple qui prédise le nombre de tels groupes de permutations pour un degré donné.

PROPOSITION 2.13. *Soit $G \subset S_n$ un groupe transitif qui soit aussi imprimitif. Toute partition non triviale de X stable sous l'action de G est formée de sous-ensembles de même cardinal.*

DÉMONSTRATION. Soit Π une partition de X stable sous l'action de G transitif. Supposons que Π possède deux sous-ensembles A_1, A_2 de tailles différentes. Donc $g \cdot A_1 \cap A_2 = \emptyset$ pour tout élément g de G, ce qui est impossible puisque G est transitif. □

Nous rappelons deux dernières définitions qui permettent de caractériser des corps de décomposition de polynômes différents de P et inclus dans $\mathbb{Q}(\underline{\alpha})$.

DÉFINITION 2.14. *Soit $G \supset H$ deux groupes de S_n. Nous dirons que H est un sous-groupe* distingué *(ou* normal*) de G s'il est stable par conjugaison de G, c'est-à-dire*

$$\forall g \in G, \quad g^{-1}Hg = H$$

Le groupe G sera dit simple *s'il ne possède aucun sous-groupe distingué autre que ses groupes triviaux (celui réduit à l'identité et G tout entier).*

La notion de groupe simple est centrale dans la résolution des équations s'appuyant sur la théorie de Galois, le groupe A_5 représentant un des exemples les plus connus. C'est ce que nous allons voir maintenant. Chacune des notions introduites ci-avant sur les groupes va être reliée à une propriété sur les polynômes.

2.1.3. Propriétés sur les corps obtenues à partir de celles du groupe de Galois. Une première caractérisation du polynôme P à partir du groupe de Galois est celle de son irréductibilité.

PROPOSITION 2.15. *Un polynôme irréductible de degré n a pour groupe de Galois un sous-groupe transitif de S_n et réciproquement.*

DÉMONSTRATION. Soit $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ le polynôme irréductible de degré n, supposons que son groupe de Galois G ne soit pas transitif. Soit $\mathcal{O}$ l'orbite de α_1 sous l'action de G. Par hypothèse, $\mathcal{O}$ est un sous-ensemble strict de $\{1, \ldots, n\}$. Le polynôme $\prod_{\alpha\in\mathcal{O}}(x-\alpha)$ est alors stable sous l'action de G et donc à coefficients rationnels d'après le théorème 2.4. Ce dernier polynôme est annulateur de α_1 de degré strictement inférieur à n ce qui est absurde.

Réciproquement, soit G, sous-groupe transitif de S_n, le groupe de Galois de $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$. Supposons que ce polynôme n'est pas irréductible. Soit $\prod_{\alpha\in\mathcal{O}}(x-\alpha)$ le facteur de ce polynôme qui s'annule en α_1, alors par hypothèse $\mathcal{O}$ est un sous-ensemble strict de $\{1, \ldots, n\}$. Le groupe G étant transitif, on pourra toujours trouver $g \in G$ tel que $g \cdot \mathcal{O} \neq \mathcal{O}$ ce facteur irréductible n'est pas stable sous l'action de G et donc ne peut être à coefficients rationnels, ce qui termine la démonstration. □

Nous avons la définition qui suit.

DÉFINITION 2.16. *Soit α une racine d'un polynôme irréductible $\mu(x)$ sur $\mathbb{Q}$. Les racines de μ sont appelées* conjugués *de α.*

De la proposition précédente, on tire que l'ensemble des conjugués d'un élément algébrique sur $\mathbb{Q}$ est donné par l'orbite de cet élément sous l'action du groupe de Galois d'un de ses polynômes annulateur.

Nous allons maintenant voir comment détecter les sous-corps de $\mathbb{Q}(\underline{\alpha})$ qui sont eux mêmes des corps de décomposition de polynômes.

PROPOSITION-DÉFINITION 2.17. *Soit f un polynôme irréductible qui a une de ses racines dans $\mathbb{Q}(\underline{\alpha})$ alors toutes ses racines sont dans $\mathbb{Q}(\underline{\alpha})$, plus généralement une extension de corps qui a cette propriété est dite* normale.

DÉMONSTRATION. Soit β la racine de f qui est dans $\mathbb{Q}(\underline{\alpha})$. Il existe donc un polynôme W de $\mathbb{Q}[x_1, \ldots, x_n]$ tel que $\beta = W(\underline{\alpha})$. Formons le polynôme

$$\Theta(x) = \prod_{g \in G} (x - (g \cdot W)(\underline{\alpha}))$$

qui, par le théorème 2.4, sera à coefficients rationnels et donc un multiple de f, on en déduit alors le résultat. □

COROLLAIRE 2.18. *En reprenant les mêmes notations que celles utilisées dans la démonstration de la proposition 2.17. Soit W un polynôme de $\mathbb{Q}[x_1, \ldots, x_n]$ tel que $\beta = \beta_1 = W(\underline{\alpha})$ et $\{\tau_1 = \mathrm{Id}, \ldots, \tau_k\}$ une transversale à gauche de $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$ sur $H = \mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q}(\beta_1))$. Les racines de f dans $\mathbb{Q}(\underline{\alpha})$ sont les éléments*

$$\beta_1 = (\tau_1 \cdot W)(\underline{\alpha}), \ldots, \beta_k = (\tau_k \cdot W)(\underline{\alpha})$$

et les groupes de Galois correspondants sont

$$\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q}(\beta_1)) = \tau_1 H \tau_1^{-1}, \ldots, \mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q}(\beta_k)) = \tau_1 H \tau_k^{-1}$$

DÉMONSTRATION. Pour montrer ce corollaire il suffit de montrer l'assertion sur l'ensemble des racines de f, la deuxième assertion étant obtenue par application directe du théorème 2.9.

Pour montrer cette première assertion il suffit de remarquer que le polynôme Θ de la preuve précédente peut être factorisé en facteurs irréductibles sur $\mathbb{Q}$ de la manière suivante (comme nous l'avons déjà fait à plusieurs reprises)

$$\Theta(x) = ((x - (\tau_1 \cdot W)(\underline{\alpha})) \cdots (x - (\tau_k \cdot W))^{|H|}.$$

Le polynôme mis à la puissance est donc f et le résultat suit. □

Nous venons de voir qu'un corps de décomposition est une extension normale sur un quelconque de ses sous-corps. Nous allons voir comment caractériser si un tel sous-corps est lui même un corps de décomposition.

PROPOSITION 2.19. *Une extension intermédiaire L entre $\mathbb{Q}$ et $\mathbb{Q}(\underline{\alpha})$ est le corps de décomposition d'un polynôme f irréductible à coefficients dans $\mathbb{Q}$ (extension normale de $\mathbb{Q}$) si et seulement si le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/L)$ est un sous groupe distingué de $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$.*

DÉMONSTRATION. Soit $L = \mathbb{Q}(\beta_1, \ldots, \beta_k)$, contenu dans $\mathbb{Q}(\underline{\alpha})$, le corps de décomposition du polynôme f. D'après le corollaire 2.18 et le théorème 2.9, le groupe de Galois de $\mathbb{Q}(\underline{\alpha})$ sur L est l'intersection des $\tau_i H \tau_i^{-1}$ (en reprenant les mêmes notations que dans

la démonstration du corollaire 2.18). Cet intersection est un groupe qui par construction est distingué dans $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha}), \mathbb{Q})$.

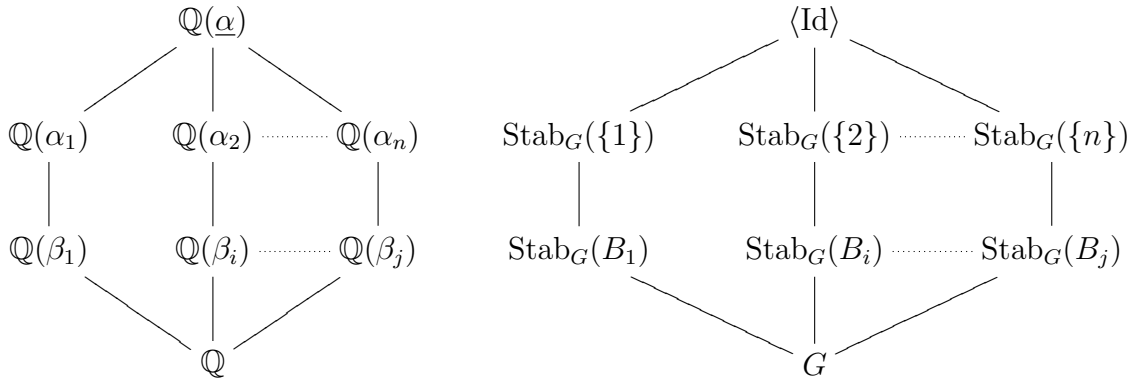
Réciproquement, considérons une extension L de $\mathbb{Q}$ telle que le groupe de Galois de $\mathbb{Q}(\underline{\alpha})$ sur L soit distingué dans $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$ et soit f un polynôme définissant cette extension. Notant β_1 une racine de f dans $\mathbb{Q}(\underline{\alpha})$, nous avons $L = \mathbb{Q}(\beta)$. Comme $H = \mathrm{Gal}(\mathbb{Q}(\underline{\alpha}/L)$ est distingué dans $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$, d'après le corollaire 2.18 et le théorème 2.9 nous avons égalité entre les corps $\mathbb{Q}(\beta_i)$ définis à partir de chacune des racines de f et donc $\mathbb{Q}(\beta_1, \ldots, \beta_k) = \mathbb{Q}(\beta_1) = L$ est un corps de décomposition d'un polynôme irréductible à coefficients dans $\mathbb{Q}$. □

Le restant de cette section peut être passé en première lecture. Les résultats suivants ne rentrent pas dans le cadre strict de la résolution de l'équation $P(x) = 0$ par adjonction d'éléments irrationnels. Les résultats qui suivent permettent d'identifier si l'équation $P(x) = 0$ peut être décomposée, c'est-à-dire, telle que le polynôme P puisse s'écrire $P = f \circ g$ pour f et g deux polynômes irréductibles, ainsi, le problème de la résolution de l'équation $P(x) = 0$ peut être découpée. Ceci revient à caractériser la présence d'un sous corps non trivial entre $\mathbb{Q}$ et le *corps de rupture* $\mathbb{Q}(\alpha_1)$ de P. Supposons pour le restant de cette section que le polynôme P est irréductible.

Lemme 2.20. *Soit $\mathcal{B}_i$ l'ensemble des blocs d'imprimitivité de $\{1, \ldots, n\}$ contenant i et $\mathcal{K}_i$ l'ensemble des sous-corps de $\mathbb{Q}(\alpha_i)$. L'application qui a $B \in \mathcal{B}_i$ fait correspondre le corps $K \in \mathcal{K}_i$ défini par $K = \mathbb{Q}(\underline{\alpha})^B$ est une bijection.*

Démonstration. Ceci est une conséquence directe du théorème 2.9. □

D'après le lemme 2.20, nous pouvons donc associer de manière unique un *système complet* de $\{1, \ldots, n\}$ à un sous-corps de $\mathbb{Q}(\alpha_1)$. Ceci peut se représenter par la figure suivante



Étant donné une décomposition du polynôme P, ou de manière équivalente, d'un corps K contenu dans $\mathbb{Q}(\alpha_1)$ nous allons voir comment construire le système complet correspondant.

Lemme 2.21. *Soit $\mathbb{Q}(\beta_1)$ un sous-corps de $\mathbb{Q}(\alpha_1)$, g le polynôme minimal de β de degré k et h un polynôme tel que $h(\alpha_1) = \beta$. L'ensemble $B_1 = \{i : h(\alpha_i) = \beta_1\}$ est le bloc d'imprimitivité qui définit le corps $\mathbb{Q}(\beta_1)$. Le système complet correspondant est donné par les blocs $B_j = \{i : h(\alpha_i) = \beta_j\}$ de taille $\frac{n}{k}$.*

Démonstration. Comme P est supposé irréductible, d'après la proposition 2.15, le groupe de Galois de P sur $\mathbb{Q}$ est transitif et les blocs d'imprimitivité d'un système complet seront donc de la même taille comme le montre la proposition 2.15. Pour obtenir

le résultat il suffit donc de montrer que B_1 est bloc d'imprimitivité, ce qui est immédiat par construction. □

Réciproquement, nous allons voir comment construire le sous-corps de $\mathbb{Q}(\alpha_1)$ correspondant à un système complet. Jusqu'à présent, lorsque nous utilisions les résolvantes nous nous sommes restreints à utiliser des résolvantes absolues, pour la construction de ces sous-corps, nous allons voir l'utilité des résolvantes relatives.

LEMME 2.22. *Soit V le monôme $\prod_{i\in B_1} x_i$. Le polynôme V est un* $\mathrm{Stab}_{\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})}(B_1)$*-invariant* $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$ *relatif. Si de plus V est $\underline{\alpha}$-séparant, alors la résolvante relative*

$$\prod_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})//\mathrm{Stab}_{\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})}(B_1)} (x-(\sigma\cdot V)(\underline{\alpha}))$$

est un polynôme minimal pour le sous-corps de $\mathbb{Q}(\alpha_1)$ correspondant à B_1.

DÉMONSTRATION. Tous les résultats énoncés dans ce lemme sont des conséquences directes de la construction et des raisonnements déjà utilisés pour les résolvantes. □

2.2. Résolution de l'équation et groupe de Galois

Dans cette section nous finissons d'étudier le problème 1 en lui donnant une réponse négative basée sur les résultats obtenus dans les sections précédentes.

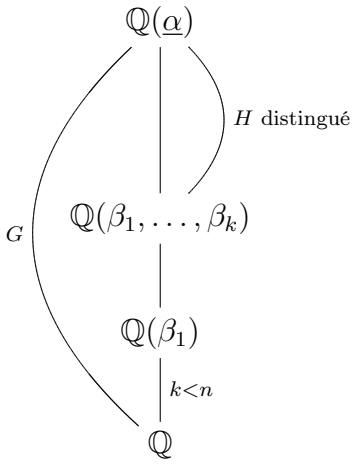
2.2.1. L'impossibilité de résoudre une équation de degré $n > 5$ en résolvant des équations de plus petit degré. Rappelons que le problème 1 est de savoir si l'on peut toujours résoudre l'équation $P(x) = 0$ avec P un polynôme à coeficients rationnels de degré n en résolvant des équations de degrés inférieurs.

De manière équivalente, ce problème revient à savoir s'il est toujours possible de construire L, une extension intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(\underline{\alpha})$, qui soit le corps de décomposition d'un polynôme f de degré inférieur à n et telle que l'extension $\mathbb{Q}(\underline{\alpha})/L$ soit de degré inférieur à n.

D'après la proposition 2.19 et le théorème de correspondance galoisienne 2.9, ceci revient à se demander s'il existe toujours un sous-groupe distingué H d'un groupe $G \subset S_n$ vérifiant les hypothèses suivantes

- $\frac{|G|}{|H|} < n$
- il existe un polynôme f de degré $k < n$ tel que son corps de décomposition L vérifie $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q}) = H$.

En notant $\beta_1, \ldots, \beta_k$ les racines de f, on peut représenter ceci à l'aide la figure suivante.



Le problème 1 se réduit donc à l'analyse des sous-groupes de S_n et on en déduit le résultat suivant.

THÉORÈME 2.23. *Soit K une extension de $\mathbb{Q}$ et G le groupe de Galois sur K de P supposé de degré n. Si G est simple alors l'équation $P(x) = 0$ ne pourra pas être résolue en utilisant une équation de degré plus petit que n. Plus précisément, cette équation auxiliaire sera de degré un facteur de $|G|$.*

Ce théorème est la réponse tant attendue à la résolution des équations. C'est Galois qui la donna en premier et lui permit de caractériser les équations de degré n qui sont résolubles à l'aide d'équations auxiliaires de degrés inférieurs. Ceci permet de montrer que l'équation générale de degré $n > 4$ répond négativement au problème 1 en reprenant les mêmes arguments que ceux que l'on a développés dans le cas des équations définies sur $\mathbb{Q}$.

THÉORÈME 2.24. *L'équation générale de degré n a pour groupe de Galois sur le corps $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ le groupe S_n. Pour $n > 4$ ce groupe ne possède qu'un seul sous-groupe propre distingué, le groupe alterné A_n qui est simple.*

La première assertion de ce théorème est immédiate, la seconde assertion est classique et se trouve déjà dans l'ouvrage de Jordan [26]. De ce résultat et de tout ce que nous venons de développer, on déduit :

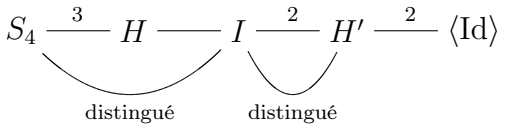
COROLLAIRE 2.25. *L'équation générale de degré $n > 4$ ne peut être résolue à l'aide d'équations auxiliaires de degrés inférieurs.*

DÉMONSTRATION. Le seul moyen de résoudre l'équation générale de degré $n > 4$ est, d'après le théorème précédent, de considérer le corps de décomposition d'une équation de degré 2 (la résolvante correspondant au groupe A_n). Le groupe de Galois de l'équation de départ se réduira à A_n en la considérant sur cette extension et donc, pour la résoudre, il faudra considérer le corps de décomposition d'un polynôme de degré un multiple de $|A_n| = \frac{n!}{2}$ puisque le groupe alterné de degré $n > 4$ est simple. □

Si l'on reprend ce que nous avions fait au chapitre 1 pour le degré 4 nous pouvons redonner une explication qui ne se fait qu'en utilisant les sous-groupes de S_4.

Soit H le sous-groupe d'ordre 8 de S_4 engendré par les permutations $(1, 2)$, $(3, 4)$, $(1, 3)(2, 4)$ (c'est le groupe diédral, celui qui laisse fixe un carré). Nous avons vu au chapitre 1 que la résolvante absolue correspondant à ce groupe est de degré 3. Une fois cette équation résolue, nous pouvons considérer le corps de décomposition K_1 de cette dernière et alors le groupe de Galois de $\mathbb{Q}(x_1, \ldots, x_4)$ sur K_1 sera le groupe $I = \cap_{g \in S_n} gHg^{-1}$ (voir la preuve de la proposition 2.19) qui se réduit au groupe d'ordre 4 engendré par les permutations $(1, 2)(3, 4)$ et $(1, 3)(2, 4)$. Le groupe H' engendré par l'élément $(1, 2)(3, 4)$ est un sous-groupe d'ordre 2 distingué dans I. Ainsi, en considérant une résolvante séparable H-relative pour un H'-invariant H-relatif, ce polynôme sera d'ordre 2 sur K_1 et son corps de décomposition K_2 a pour propriété que le groupe de Galois de l'équation de départ sur K_2 se réduira H'. Comme H' n'est plus d'ordre 4, il ne peut plus être transitif, ainsi l'équation ne peut plus être irréductible et, plus exactement, se factorise en deux équations de degré 2 que nous pourrons résoudre (la résolution d'une seule des deux équations permettra de réduire le groupe de Galois à l'identité et on obtiendra l'ensemble des solutions de l'équation de départ). Tout ceci peut se résumer par la descente de

groupes qui suit



2.2.2. Résolution par radicaux. Pour caractériser les équations qui sont résolubles par radicaux il faut, en plus de considérer les sous groupes distingués de S_n, étudier le lien entre les groupes abéliens et les extensions de corps obtenues par adjonction de racine primitive de l'unité. Ce lien se fait à l'aide des résolvantes de Lagrange que nous avons vues au chapitre 1. Pour plus de détails sur ces résultats, on pourra lire les ouvrages [12] [42] et pour une vision plus algorithmique de la résolution par radicaux on pourra consulter les articles [3] [47] [24].

Deuxième partie

Calcul du groupe de Galois et du corps de décomposition

Préambule

Comme nous avons pu le voir dans la partie précédente, le calcul du groupe de Galois et du corps de décomposition d'un polynôme P permet de construire les différentes relations entre ses racines et permet ainsi de résoudre l'équation $P(x) = 0$ formellement. Rappelons que d'après la correspondance de Galois, l'étude des sous-groupes de groupe de Galois permet de construire l'ensemble des sous-corps du corps de décomposition qui peuvent posséder des caractéristiques arithmétiques intéressantes pour le mathématicien.

Il y a différents problèmes liés au calcul du groupe de Galois d'un polynôme. Étant donné un polynôme f de degré n nous avons, par ordre croissant de difficulté, les problèmes suivants

(1) Calculer une représentation dans S_n du groupe de Galois de f ;
(2) calculer une représentation dans S_n de l'action du groupe de Galois de f sur des approximations des racines de f ;
(3) calculer une représentation dans S_n de l'action du groupe de Galois de f sur des représentations formelles des racines de f.

Si le but du calcul du groupe de Galois est de pouvoir utiliser cet objet pour effectuer des constructions mathématiques, la résolution du premier point ne sera pas d'une très grande utilité. Le troisième problème peut se voir comme le calcul du corps de décomposition du polynôme f et du groupe de Galois correspondant et le deuxième comme une approxiamtion de cette action. Dans cette partie nous traiterons principalement les deux derniers points

D'un point de vue historique, la première méthode pour le calcul du groupe de Galois d'une équation est donnée par Galois lui même dans sa définition de ce groupe (c'est celle

> **388. Pour appliquer les résultats qui précèdent, il est nécessaire, une équation étant donnée, de savoir déterminer son groupe.**
>
> **La marche à suivre pour traiter cette question sera celle-ci : 1° on formera les divers groupes de substitutions possibles G, G′,... entre les racines $x_1, \ldots, x_n$ de l'équation; 2° soit G l'un de ces groupes, choisi à volonté : on s'assurera s'il contient ou non le groupe de l'équation en formant une fonction φ des racines, invariable par les substitutions de G et variable par toute autre substitution, calculant par la méthode des fonctions symétriques l'équation qui a pour racines les diverses valeurs de φ, et cherchant si cette équation a, oui ou non, une racine rationnelle. Parmi les groupes de la suite G, G′,... qui contiennent ainsi le groupe de l'équation, le plus petit sera ce groupe lui-même.**

FIG. 2.2. [26, Page 355]

que nous avons présentée au chapitre précédent). Bien que constructive, cette méthode

est loin d'être effective, en effet, il s'agit ici de factoriser un polynôme de degré $n!$ où n est le degré de l'équation. D'ailleurs c'est pour résoudre formellement ce genre de problème de factorisation que Kronecker construit un tel algorithme dans [28]. Cette méthode, bien que de complexité exponentielle, est celle que reprend Van der Waerden dans son livre [43, 44] alors que Jordan donnait déjà dans son ouvrage [26] (voir Figure 2.2), une méthode qui parait beaucoup plus prometteuse. Ceci c'est révélé être vrai puisque les algorithmes utilisés aujourd'hui découlent tous du même principe basé sur le calcul de résolvantes qui ne se résume pas à l'utilisation de celle définie par Galois (de degré $n!$).

CHAPITRE 3

Calcul du groupe de Galois

3.1. Introduction

Dans ce chapitre, nous présentons des méthodes de calcul permettant de retrouver le groupe de Galois d'un polynôme donné en entrée. Nous présenterons, en particulier, des algorithmes permettant de retrouver l'action de ce groupe sur des approximations des racines de ce polynôme. Dans tout ce chapitre, le polynôme étudié P sera supposé **irréductible** de degré n et à coefficients dans le corps des **rationnels**. Tout comme nous l'avons déjà fait précédemment, nous fixons $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ un ensemble ordonné fixé des racines de P.

3.2. Groupe de Galois, automorphismes et conjugaisons

Nous avons vu au chapitre 2, une définition du groupe de Galois d'un corps de décomposition sous la forme d'un sous-groupe du groupe symétrique qui repose sur un ordre fixé des racines du polynôme. Nous allons ici montrer comment passer d'une représentation de ce groupe en passant d'une numérotation à une autre et le lien avec le groupe des $\mathbb{Q}$-automorphismes d'un corps de décomposition. Ces résultats très généraux pourront être retrouvés et développés dans un ouvrage général comme celui de Lang (voir [30]).

Représentation par permutations. Soit G un groupe agissant sur un ensemble E. À une telle action on peut associer un homomorphisme ρ du groupe G dans le groupe $\mathrm{Perm}(E)$ des permutations de l'ensemble E, où l'image par ρ d'un élément g de G est définie par

$$\begin{array}{rccc} \rho(g) & : & E & \longrightarrow & E \\ & & e & \longmapsto & g \cdot e \end{array}$$

Inversement, si on se donne un homomorphisme ρ du groupe G dans le groupe $\mathrm{Perm}(E)$, alors on peut en déduire une action de G sur E (notée $\cdot$). En effet, si on considère l'application définie par

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, e) & \longmapsto & g \cdot e := \rho(g)(e) \end{array}$$

on vérifie aisément que ceci est action de G sur E.

Un homomorphisme du groupe G dans le groupe des permutations $\mathrm{Perm}(E)$ est appelé *représentation par permutations* du groupe G. D'après ce que nous venons de voir, il est donc équivalent de se donner une action d'un groupe G sur un ensemble E ou une représentation par permutations du groupe G. Ainsi nous ne distinguerons plus une action de sa représentation par permutations qui lui est associée. Nous allons maintenant nous concentrer sur le cas où l'ensemble E est fini.

Représentation symétrique. Soit G un groupe agissant sur un ensemble **fini** E de cardinal l'entier n. Notons ρ la représentation par permutations qui est associée à cette action.

Une *numérotation de E* peut être vue comme une application bijective de l'ensemble $\{1, \ldots, n\}$ dans E. Fixons $\mathcal{N}$ une telle numérotation de E. Nous avons alors l'isomorphisme de groupe :

$$\begin{array}{rcl} \mathrm{Perm}(E) & \longrightarrow & S_n \\ s & \longmapsto & \mathcal{N}^{-1} \circ s \circ \mathcal{N} \end{array}$$

et nous en déduisons l'homomorphisme de groupe suivant :

$$\begin{array}{rcl} \phi_{\mathcal{N}} : G & \longrightarrow & S_n \\ g & \longmapsto & \mathcal{N}^{-1} \circ \rho(g) \circ \mathcal{N} \end{array}$$

Un tel homomorphisme sera appelé *représentation symétrique par rapport à la numérotation $\mathcal{N}$* et lorsque la situation est sans ambiguïté sur $\mathcal{N}$, c'est-à-dire lorsque la numérotation est fixée, nous parlerons de *représentation symétrique*.

Soit $\mathcal{N}_1$ et $\mathcal{N}_2$ deux numérotations de E. Alors, il existe une permutation σ dans S_n telle que :

$$\mathcal{N}_2 = \sigma \circ \mathcal{N}_1 \,,$$

et donc :

$$\phi_{\mathcal{N}_2} = \sigma^{-1} \circ \phi_{\mathcal{N}_1} \circ \sigma \,.$$

Soit $\hat{G}$ le sous-groupe de S_n image d'une représentation symétrique de G. D'après ce qui précède, G peut être représenté par un groupe quelconque de la classe de conjugaison de $\hat{G}$ dans S_n mais aucun autre.

L'action du groupe G sur l'ensemble E est dite *fidèle* si la représentation symétrique correspondante est injective, ou si, de manière équivalente, le sous-groupe $\cap_{e \in E} \mathrm{Stab}_G(e)$ de G est réduit à l'élément unité.

Groupe des automorphismes. Soit P un polynôme séparable et $\underline{\alpha}$ l'ensemble fini de ses racines (distinctes) dans une clôture de $\mathbb{Q}$. Notons L un corps intermédiaire entre le corps de décomposition $\mathbb{Q}_P$ de P et $\mathbb{Q}$. Le corps de décomposition de P est alors engendré sur L par $\underline{\alpha}$. Comme la restriction à L d'un élément ϕ du groupe des L-automorphismes de $\mathbb{Q}_P$ se réduit à l'identité, la définition de ϕ ne dépend que des images qu'il prend sur les éléments de $\underline{\alpha}$. Ainsi nous pouvons construire un homomorphisme injectif ρ de la forme

$$\mathrm{Aut}_L(\mathbb{Q}_P) \longrightarrow \mathrm{Perm}(\underline{\alpha})$$

et défini par

$$\begin{array}{rcl} \rho(\phi) : \underline{\alpha} & \longrightarrow & \underline{\alpha} \\ e & \longmapsto & \phi(e) \end{array}$$

De cette manière, nous obtenons une action fidèle du groupe des L-automorphismes sur l'ensemble $\underline{\alpha}$. Soit $\mathcal{N}$ une numérotation des racines de P, c'est-à-dire des éléments de $\underline{\alpha}$, alors nous avons une représentation symétrique injective du groupe G dans S_n. Soit $\hat{G}$ l'image dans S_n de cette représentation, alors G est isomorphe à $\hat{G}$ et, d'après ce que nous avons vu plus haut, nous pouvons construire un isomorphisme entre G et chacun des conjugués de $\hat{G}$ dans S_n en changeant de numérotation. On a la définition qui suit.

DÉFINITION 3.1. *Soit P un polynôme séparable de $\mathbb{Q}[x]$ de degré n un entier strictement positif et L un corps intermédiaire entre $\mathbb{Q}_P$ et $\mathbb{Q}$. Nous appellerons groupe de Galois de P sur L, un représentant quelconque de la classe de conjugaison dans S_n du groupe de Galois du corps $\mathbb{Q}_P$ sur L. Ce groupe sera noté* $\mathrm{Gal}_L(f)$.

EXEMPLE 3.2. *Soit $\mathbb{Q} = \mathbb{Q}$ et $f = x^6 - 10x^4 + 31x^2 - 30$. Comme f se factorise sur $\mathbb{Q}$ en $f = (x^2-2)(x^2-3)(x^2-5)$ les racines de f sont toutes réelles et sont données par $\underline{\alpha} = \{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}, \sqrt{5}, -\sqrt{5}\}$.*

Exhibons le groupe des $\mathbb{Q}$-automorphismes du corps $\mathbb{Q}_P = \mathbb{Q}[\underline{\alpha}]$. Le groupe $Aut_{\mathbb{Q}}(\mathbb{Q}_P)$ contient $[\mathbb{Q}_P : \mathbb{Q}]$ éléments et ici nous avons clairement $[\mathbb{Q}_P : \mathbb{Q}] = 8$. Soit $\phi \in Aut_{\mathbb{Q}}(K_P)$ et $\alpha \in \underline{\alpha}$. Comme l'image de α par ϕ ne peut être qu'un conjugué de α dans $\underline{\alpha}$ nous avons :

$$\phi(\alpha) = -\alpha\,.$$

Nous obtenons ainsi la définition de chacun des éléments du groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}_P = \mathbb{Q}[\underline{\alpha}]$ à partir de leur action sur l'ensemble $\underline{\alpha}$. Si l'on choisit de numéroter $\underline{\alpha}$ à l'aide de la fonction $\mathcal{N}$ définie par :

$$\begin{array}{rcl} \mathcal{N} : \underline{\alpha} & \longrightarrow & \{1, \ldots, 6\} \\ \sqrt{i} & \longmapsto & i + (i \bmod 2) \\ -\sqrt{i} & \longmapsto & \mathcal{N}(\sqrt{i}) - 1 \end{array}$$

alors le groupe $Aut_{\mathbb{Q}}(\mathbb{Q}_P)$ est représenté symétriquement par le sous-groupe $\hat{G}$ de S_6 engendré par l'ensemble de permutations $\{(12), (34), (56)\}$ noté $C(2) \times C(2) \times C(2)$. Si nous avions choisi une autre numérotation $\mathcal{N}_2$ pour l'ensemble $\underline{\alpha}$ alors, en notant σ l'unique élément de $\mathrm{Perm}(\{1, \ldots, 6\})$ *tel que $\mathcal{N}_2 = \sigma \circ \mathcal{N}$, le groupe des $\mathbb{Q}$-automorphismes de $\mathbb{Q}_P$ serait représenté par le sous-groupe de S_6 engendré par l'ensemble de permutations*

$$\{(\sigma(1), \sigma(2)), (\sigma(3), \sigma(4)), (\sigma(5), \sigma(6))\}$$

qui n'est autre que le conjugué de $\hat{G}$ par σ^{-1}. Quel que soit la numérotation choisie, nous dirons que le polynôme f a pour groupe de Galois $C(2) \times C(2) \times C(2)$.

Soit L le corps $\mathbb{Q}[\sqrt{2}]$ intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}_P$. Le groupe des L-automorphismes de $\mathbb{Q}_P$ est isomorphe à $C(2) \times C(2)$. Si nous choisissons de numéroter l'ensemble $\underline{\alpha}$ à l'aide de $\mathcal{N}$ alors une représentation symétrique de $Aut_L(\mathbb{Q}_P)$ sera donnée par le sous-groupe de S_6 engendré par l'ensemble des permutations $\{(3, 4), (5, 6)\}$.

3.3. Théorème fondamental sur les résolvantes et détermination du groupe de Galois

Dans cette section nous présentons les critères permettant de distinguer les sous-groupes transitifs dans leur ensemble. Ces critères reposent sur le calcul de résolvantes et permet de distinguer le groupe de Galois d'un polynôme.

Soit P un polynôme irréductible de degré n, d'après la proposition 2.15 le groupe de Galois de ce polynôme est transitif. Peut on obtenir d'autres types de caractéristiques sur ce groupe lorsque l'hypothèse d'irréductibilité n'est plus vraie ? Supposons que h soit réductible sur $\mathbb{Q}$, séparable et factorisable sous la forme $h = fg$, où f et g sont des polynômes irréductibles à coefficients rationnels. Le groupe de Galois de h, noté G, n'est donc pas transitif et on peut lui associer un système complet composé de deux blocks de transitivité. En effet, l'action de G sur les racines de h a deux orbites correspondant chacune à l'ensemble des racines de f et g car, si ça n'était pas le cas, ces deux polynômes ne pourraient être irréductibles à coefficients dans $\mathbb{Q}$ (voir la preuve de la proposition 2.15).

En fait, l'action de G sur l'orbite des racines de f peut être représentée fidèlement comme un sous-groupe T_f de S_k où k est le cardinal de cette orbite. On voit immédiatement que le groupe T_f est transitif et qu'il correspond au groupe de Galois de f.

Ainsi, à un polynôme réductible et séparable, on peut associer l'ensemble des groupes de Galois de chacun de ses facteurs en analysant l'action canonique de son groupe de Galois. Mais le groupe de Galois d'un polynôme réductible n'est pas, en générale, égal au produit direct des groupes de Galois de ses facteurs.

Plus généralement, nous pouvons appliquer le même genre de raisonnement au résolvantes séparable. On rappelle que P est un polynôme irréductible sur $\mathbb{Q}$ et que l'on note $\mathbb{Q}(\underline{\alpha})$ un corps de décomposition de P. Nous rappelons la notion de classe de double.

DÉFINITION 3.3. *Soit G et H deux sous-groupes du groupe $U \subset S_n$. Une* (G,U)-classe double *est une classe de la relation d'équivalence qui met en relation deux éléments x et y de U dès qu'il existe un couple $(g,h) \in G \times H$ tel que $gxh = y$. L'ensemble des (G,H) classes doubles de U est noté $G\backslash U/U$.*

En gardant les mêmes notations que dans la définition précédente, les (G,H)-classes doubles de U sont de la forme GuH où $u \in U$ et U peut être partitionné selon ces classes doubles. Chacune de ces classes doubles est l'union de classes à droite de U selon G (de la forme Gu) et de classes à gauche de U selon H (de la forme uH). Nous pouvons maintenant énoncer le résultat fondamental qui suit.

THÉORÈME 3.4. *Soit $U \subset S_n$ contenant les deux sous-groupes $G = \mathrm{Gal}(\mathbb{Q}(\underline{\alpha}), \mathbb{Q})$ et H. Si F est H-invariant G-relatif alors la résolvante relative à U de F s'écrit*

$$R(x) = \prod_{\tau \in U//H} (x - \tau \cdot F(\underline{\alpha})) = \prod_{i=1}^{k} g_i^{a_i}(x)$$

avec g_i irréductible sur $\mathbb{Q}$ et si l'on note $\mathcal{I}_R$ l'ensemble des facteurs $\{g_1^{a_1}, \ldots, g_k^{a_k}\}$ alors l'application de $G\backslash U/H$ dans $\mathcal{I}_R$ qui fait correspondre une (G,H)-classe double GuH de U au polynôme

$$g_u(x) = \prod_{\tau \in U//H \ tq\ \tau H \subset GuH} (x - (\tau \cdot F)(\underline{\alpha}))$$

est bijective. Les éléments τ de $U//H$ rentrant dans la définition du polynôme g_u sont exactement ceux définis par $\tau = u'u$ avec $u' \in G//(G \cap uHu^{-1})$.

DÉMONSTRATION. La dernière assertion sur l'ensemble des éléments entrant dans la définiton du polynôme est claire, il s'agit uniquement de réécrire l'inclusion qui définit le produit.

Soit GuH une (G,H)-classe double de U. Commençons par montrer que le polynôme g_u est à coefficients dans $\mathbb{Q}$. Pour cela il suffit de montrer qu'il est stable sous l'action de G. Le groupe G agit naturellement sur la transversale à gauche $G//(G \cap uHu^{-1})$, ainsi, d'après l'assertion finale du théorème, G agit naturellement sur l'ensemble des éléments de $U//H$ entrant dans la définition de g_u en les échangeant. On en conclut que l'action de G sur g_u le laisse stable puisque les classes rentrant dans sa définition ne changent pas.

Clairement, g_u est un diviseur de R, et il est clair aussi que tous les facteurs irréductibles de R sont des diviseurs des polynômes dans $\mathcal{I}_R$. Montrons que les zéros de g_u sont conjugués sous l'action de G. Soient τ_1, τ_2 deux éléments de $U//H$ tels que $\tau_1 H, \tau_2 H \subset GuH$ alors il existe deux éléments u_1', u_2' dans G tels que $\tau_1 = u_1'u$ et $\tau_2 = u_2'u$ et donc $\tau_1 = u_1'u'^{-1}u_2$ ce qui nous donne la conjugaison des racines de g_u sous l'action de G.

Montrons que les zéros de R qui sont conjugués sous l'action de G correspondent à la même (G,H)-classe double de U. Soient $(\sigma\cdot(\tau_1\cdot F))(\underline{\alpha})=(\tau_2\cdot F)(\underline{\alpha})$ avec $\tau_1,\tau_2\in U$ et $\sigma\in G$ deux racines de R qui sont conjuguées sous l'action de G. Nous avons alors $\tau_2^{-1}\sigma\tau_1\in H$ et donc $\sigma\tau_1 H=\tau_2 H$, on en conclut $G\tau_1 U=G\tau_2 U$.

D'après ce que nous venons de voir, les polynômes de $\mathcal{I}_R$ sont des produits de puissances des facteurs irréductibles de R, sachant que tous ces facteurs irréductibles y apparaîtront. Reste à montrer que les puissances maximales des facteurs irréductibles de R sont exactement les polynômes de $\mathcal{I}_R$. Puisque les zéros de g_u sont conjugués sous l'action du groupe de Galois G, g_u ne peut être qu'une puissance d'un facteur irréductible et d'après la correspondance avec les classes doubles, ce facteur irréductible ne peut pas apparaître dans un autre polynôme de $\mathcal{I}_R$. Ainsi $g_u=g_i^{b_i}$ et pour finir la démonstration de ce théorème, il reste montrer que $b_i=a_i$.

Le degré du polynôme g_u est donné par

$$\mathrm{Deg}(g_u)=\frac{|GuH|}{|H|}=\frac{|G|}{|G\cap(uHu^{-1})|}$$

et comme les (G,H)-classes doubles de U forment une partition de U. On obtient alors le degré du produit Q des g_{v_i} où v_i prend ses valeurs dans l'ensemble des représentants des (G,H)-classes doubles de U et donc

$$\mathrm{Deg}(Q)=\sum_i \mathrm{Deg}(g_{v_i})=\sum_i\frac{|GuH|}{|H|}=\frac{|U|}{|H|}$$

et donc $\mathrm{Deg}(Q)=\mathrm{Deg}(R)$ et le résultat suit. □

De ce théorème on peut en déduire deux méthodes générales pour distinguer le groupe de Galois d'un polynôme. Ces deux méthodes sont basées sur les corollaires qui suivent. Le premier corollaire permet de distinguer le groupe de Galois de P à partir de valeurs qualitatives des facteurs irréductibles de résolvantes calculées à partir de P.

Corollaire 3.5. *En reprenant les mêmes notations que dans le théorème 3.4 et en notant m le degré de R. Si la résolvante R est séparable alors la représentation symétrique dans S_m de l'action de G sur la transversale $U//H$ est égale au groupe de Galois sur $\mathbb{Q}$ du corps de décomposition de R. En particulier, cette action sur chacune (resp. la tailles) de ses orbites peut être mis en relation avec les groupes de Galois sur $\mathbb{Q}$ (resp. le degré) de chacun des facteurs irréductibles de R.*

Le deuxième corollaire permet d'identifier les sous-groupes de S_n contentant le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha}),\mathbb{Q})$.

Corollaire 3.6. *En reprenant les mêmes notations que dans le théorème 3.4. La résolvante R possède un* **facteur linéaire simple** *correspondant à la classe double GuH si et seulement si le groupe uHu^{-1} contient G.*

Démonstration. En reprenant les mêmes notations que dans la preuve du théorème 3.4. Supposons que g_u soit linéaire, alors nous avons

$$1=\mathrm{Deg}(g_u)=\frac{|G|}{|G\cap uHu^{-1}|}$$

et ceci nous donne le résultat. □

Remarque 3.7. *Notez que si la résolvante R du corollaire précédent ne possède aucun facteur linéaire alors G ne pourra pas être un sous-groupe d'un conjugué de H dans U. Si R ne possède que des facteurs linéaires multiples on ne peut rien conclure.*

La méthode proposée par Jordan (voir le préambule) repose sur ces résultats et plus particulièrement sur le corollaire 3.6. En effet il propose de calculer des résolvantes absolues et après factorisation de rejeter les groupes correspondants aux résolvantes ne possédant pas de facteur linéaire. De proche en proche on pourra en déduire le groupe de Galois de P. Les algorithmes actuels pour le calcul du groupe de Galois reposent sur le même genre d'idée mais l'utilisent de meilleure manière

EXEMPLE 3.8. *Soit $F = \prod_{i<j}(x_i - x_j)$. Le polynôme F est un A_n-invariant, il est immédiat que la résolvante*

$$R_F(x) = (x - F(\underline{\alpha}))(x - (1,2) \cdot F(\underline{\alpha})) = (x - F(\underline{\alpha}))(x + F(\underline{\alpha}))$$

est séparable de degré 2 dès que le polynôme f est séparable. Comme $\Delta(f)$, le discriminant de f, vérifie $\Delta(f) = F(\underline{\alpha})^2$, le groupe de Galois d'un polynôme f est contenu dans A_n (dans ce cas on dit qu'il est pair) si et seulement si son discriminant est un carré dans $\mathbb{Q}$.

Distinction par résolvantes absolues. L'application du corollaire 3.5 peut se faire de la manière suivante. Comme groupe de base on prend $U = S_n$ ainsi les hypothèses d'inclusions seront toujours vérifiées et les résolvantes seront absolues. De cette manière, on peut distinguer les groupes transitifs de degré n en fonction des différentes lignes d'un tableau mettant en correspondance les degrés (ou groupes de Galois) des différents facteurs irréductibles des résolvantes absolues calculées à partir des sous-groupes de S_n. Un tel tableau est appelé *table des partitions* et fût utilisées par Girstmair [22], Mc Kay, Soicher, Casperson (voir [40, 7]) pour déterminer les groupes de Galois de polynômes de degrés modérés. Arnaudiès et Valibouze ont montré que ce moyen de déterminer le groupe de Galois d'un polynôme est déterministe (voir [4]) et ont fourni des tables de partitions jusqu'au degré 11. Cette détermination ne se fait qu'à conjugaison près, ceci permet de résoudre le problème 1 du calcul du groupe de Galois mais, comme nous l'avons dit dans l'introduction, ceci n'a que très peu d'intérêt si l'on veut pouvoir calculer formellement des actions du groupe de Galois sur le corps de décomposition de P.

Nous allons maintenant présenter des résultats qui permettront de construire une approximation de l'action du groupe de Galois sur le corps de décomposition.

Distinction par descente dans l'arbre des sous-groupes. Ici on utilise le corollaire 3.6 pour descendre dans l'arbre des sous-groupes de S_n jusqu'à obtenir le groupe de Galois du polynôme. On commence par prendre $U = S_n$ en testant tous les sous-groupes maximaux par une recherche de racine simple de chacune des résolvantes correspondantes et on itère le principe en prenant pour groupe U le premier qui contient le groupe de Galois. On arrête le calcul lorsqu'aucun sous-groupe maximal ne peut contenir le groupe de Galois. On en déduit l'algorithme 1.

Pour mettre en pratique cette méthode il faut donner un ordre particulier au racines de P et le conserver tout au long du calcul, c'est le rôle que remplit la fonction Ψ. Cette fonction permet de vérifier si l'évaluation d'un polynôme en les racines de f est rationnelle, l'ordre des racines se raffinant au cours du calcul. De cette manière, le calcul du groupe de Galois ne se fait pas à conjugaison près, la sortie obtenue en fin de calcul est la représentation symétrique de l'action du groupe de Galois sur les racines ordonnées données par Ψ. *A priori*, pour utiliser Ψ, nous devons connaître les racines de f pour réaliser une telle descente, ce qui est contradictoire. Pour ce faire on peut utiliser des approximations numériques ou p-adiques. Stauduhar est le premier à donner un algorithme et une implantation basée sur cette méthode (voir [41]), il utilise des approximations numériques des racines de P pour calculer les racines des résolvantes relatives. L'utilisation des

Algorithme 1 `Stauduhar`(f,Ψ)

Entrée : $f \in \mathbb{Q}[X]$ irréductible de degré n, Ψ une fonction qui vérifie si l'évaluation en les racines de f d'un polynôme en n variables est rationnelle et la renvoie le cas échéant.

Sortie : Le groupe de Galois de f correspond à l'ordre des racines de f donné par Ψ.

1: $U = S_n$
2: Calculer $\mathcal{T}$ l'ensemble des sous-groupes transitifs maximaux de U (à conjugaison près dans U)
3: Si $\mathcal{T}$ est vide renvoyer U
4: Soit T un élément de $\mathcal{T}$. Calculer F un T-invariant U-relatif.
5: Calculer $\mathcal{S} = \{\sigma \in U//T \text{ tq } \Psi N(\sigma \cdot F) \text{ est rationnel}\}$
6: Si $\mathcal{S}$ est vide, exclure T de $\mathcal{T}$ continuer à l'étape 3
7: S'il existe $\sigma_1 \in \mathcal{S}$ tel que pour tout $\sigma_2 \in \mathcal{S}$ on a $\Psi N(\sigma_1 \cdot F) \neq \Psi N(\sigma_2 \cdot F)$, remplacer U par $\sigma_1 T \sigma_1^{-1}$ et continuer à l'étape 2. Sinon appliquer une transformation de Tschirnhaus sur F et retourner à l'étape 5

approximations numériques est très efficace pour calculer les racines des résolvantes mais devient coûteuse lorsqu'il faut certifier les inclusions (voir [17]). C'est pour cette raison que Yokoyama [46] introduit des approximations p-adiques pour effectuer ce calcul, c'est ce type d'approximation que nous retenons, nous présenterons ceci au chapitre suivant. Darmon et Ford (voir [14]) ont aussi utilisé des approximations p-adiques pour calculer le groupe de Galois de deux polynômes mais l'article de Yokoyama établit de nouveaux résultats et développe complètement la version p-adique de l'algorithme de Stauduhar.

Il reste un problème que nous devons traiter avant de pouvoir mettre en place une implantation pour le calcul du groupe de Galois basée sur la stratégie de Stauduhar : comment obtenir une résolvante qui soit séparable ou, au moins, qui possède un facteur linéaire simple ?

Remarque 3.9. *Colin, dans [10, 11], propose une méthode symbolique basée sur l'algorithme de Stauduhar. Pour un degré donné n, il calcule les formes génériques des résolvantes relatives correspondant aux différentes étapes de la descente dans l'arbre des sous-groupes transitifs de S_n. Les coefficients de ces résolvantes sont des éléments d'anneaux d'invariants. Pour calculer le groupe de Galois d'un polynôme f irréductible de degré n, on évalue, au fur et à mesure de la descente, les coefficients des résolvantes à l'aide de ceux de f et de ceux des résolvantes déjà calculées.*

3.4. Calcul d'invariant et transformation de Tschirnhaus pour le calcul de résolvante séparable

Dans cette section on introduit un moyen permettant d'obtenir une résolvante qui soit séparable pour un groupe donné. Soit $U \supset H$ deux sous-groupes de S_n tel que U contienne $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$.

3.4.1. Transformation de Tschirnhaus. Dans un premier temps, nous supposons connu F un H-invariant U relatif. Nous utilisons ces données afin d'obtenir une résolvante U-relative qui soit $\underline{\alpha}$-séparant.

Proposition-Définition 3.10. *Soit R une résolvante U-relative de F et t un polynôme de degré $[U : H] - 1$. On appelle* transformation de Tschirnhaus *de R selon t le polynôme*

$$R^t(x) = \prod_{\tau \in U//H} x - (\tau \cdot F)(t(\alpha_1), \ldots, t(\alpha_n)).$$

Le polynôme R^t est à coefficients dans $\mathbb{Q}$ et est une résolvante U-relative pour le H-invariant U-relatif $F(t(x_1), \ldots, t(x_n))$.

DÉMONSTRATION. Cette proposition repose sur le fait que le polynôme $F(t(x_1), \ldots, t(x_n))$ est un H-invariant U-relatif, ce qui est clair. □

Étant donné un H-invariant U-relatif, il est donc possible d'obtenir une infinité de résolvantes U-relatives en appliquant des transformations de Tschirnhaus successives. Dans [22], Girstmair montre que ce genre de transformation permet de construire une résolvante U-relative qui soit $\underline{\alpha}$-séparante. Colin détermine dans [10] le nombre maximal de transformations qu'il faudra appliquer avant d'obtenir une telle résolvante séparable en étudiant le degré d'une hypersurface paramétrant l'ensemble des transformations qui vérifient cette hypothèse. En pratique, le nombre de transformations de Tschirnhaus à appliquer est très faible en comparaison avec la borne théorique obtenue par Colin.

PROPOSITION 3.11. *Il existe toujours une transformation de Tschirnhaus qui permet d'obtenir une résolvante U-relative qui soit $\underline{\alpha}$-séparant.*

Nous avons donc vu comment obtenir une résolvante séparable à partir d'une résolvante qui ne l'est pas. Reste à savoir comment construire une résolvante, et en particulier, comment construire un H-invariant U-relatif.

3.4.2. Calcul d'un H-invariant U-relatif. Soit R l'anneau des polynômes en n variables $\mathbb{Q}[x_1, \ldots, x_n]$ et $U \supset H$ deux sous-groupes de S_n. L'orbite d'un monôme de R sous l'action de H est un ensemble de monômes de même degré. Ainsi, sans aucune perte de généralité, nous pouvons considérer des H-invariants qui soient homogènes et construits comme une somme des éléments d'une H-orbite d'un monôme m. Pour qu'un tel H-invariant soit U-relatif il faut et il suffit que $|H \cdot m| < |U \cdot m|$. On peut facilement construire un H-invariant U-relatif en prenant le monôme $m = x_1^1 x_2^2 \cdots x_n^n$:

$$F = \sum_{\sigma \in H} \sigma \cdot (x_1^1 x_2^2 \cdots x_n^n).$$

En fait, F est un H-invariant G-relatif pour tout sous-groupe G de S_n contenant H. Le problème de cet invariant est sont degré : $\frac{n(n-1)}{2}$ et aussi son nombre de monômes $|G|$ ce qui n'est vraiment pas bon dès que l'on veut un tant soit peu calculer !

Pour construire des invariants de plus petit degré, nous allons exposer une méthode reposant sur l'étude de la série de Hilbert des anneaux de polynômes invariants. Cette méthode repose sur des résultats classiques de la théorie des invariants (voir le livre de Derksen et Kemper [15]) et est, par exemple, exposée dans les articles de Hulpke [25] et aussi de Geissler et Klüners [21].

On note R^H le sous-anneau des polynômes de R qui sont stables sous l'action de H. De la décomposition des éléments de R en sommes de composantes homogènes on déduit le même genre de décomposition pour R^H :

$$R^H = \sum_{d=0}^{\infty} R_d^H$$

où R_d^H représente l'ensemble des composantes homogènes de R^H de degré fixé d. On associe à cette décomposition une série génératrice dont les coefficients sont les dimensions des R_d^H en tant que $\mathbb{Q}$-espace vectoriel, elle est appelée *série de Hilbert* :

$$\mathrm{Hilb}(H, t) = \sum_{d=0}^{\infty} \mathrm{Dim}_{\mathbb{Q}}(R_d^H) t^d \in \mathbb{Z}[[t]]$$

Le principe de base pour trouver un H-invariant U-relatif dans le cas où H *est un sous-groupe maximal de* U repose sur la remarque suivante. Plutôt que de chercher un invariant quelconque choisissons en un qui soit homogène, dans ce cas nous pouvons utiliser les résultats qui précèdent. Comme $U \supset H$ nous avons $R_d^H \supset R_d^U$ pour tout degré d et donc, si $U \neq H$, il existe un certain indice minimal d_0 tel que les coefficients d'indice d_0 des séries de Hilbert de H et U diffèrent. On pourra donc trouver un invariant H-invariant U-relatif homogène de degré d_0 qui sera donc minimal. On déduit l'algorithme 2 `Invariant`(H,U) qui calcule un H-invariant U-relatif.

Algorithme 2 `Invariant`(H,U)

Entrée : $H \subset U \subset S_n$ tel que H soit maximal dans U
Sortie : Un H-invariant U-relatif
1: Calculer le plus petit indice d_0 qui diffère entre $\mathrm{Hilb}(H,t)$ et $\mathrm{Hilb}(U,t)$
2: Calculer une base de $\mathcal{I} = R_{d_0}^H$
3: Extraire de $\mathcal{I}$ les U-invariants
4: Renvoyer un H-invariant de $\mathcal{I}$ qui ait un nombre minimal de monômes

Chacune des étapes de cet algorithme peut être calculée efficacement (voir [27] et [15]) avec les logiciels de calcul formel comme Magma [6] et GAP [19].

Dans le cas où H n'est pas maximal dans U, le d_0 que nous venons de calculer correspond à une chute de dimension dûe à un sous-groupe maximal de U contenant H. Dans ce cas, il faudra utiliser le même principe en recommençant l'étude récursivement sur une chaîne de sous-groupes maximaux allant de H à U.

Pour des familles de groupes particuliers, il est possible de calculer plus efficacement des invariants, le lecteur intéressé pourra se référer aux articles [23, 25, 21] et ouvrage [15].

3.5. Conclusion

Pour finir l'implantation de l'algorithme 1 il nous faut un moyen de tester si une résolvante relative possède un facteur linéaire simple sur $\mathbb{Q}$. Pour ce faire nous allons présenter une méthode p-adique dans le chapitre 4 qui permet d'approximer ces calculs et de les certifier. Pour rendre plus efficace les calculs du groupe de Galois il est nécessaire d'utiliser des techniques permettant de réduire le nombre de tests à effectuer lors de la descente dans l'arbre des sous-groupes (voir [25, 21, 20]).

Une implantation de l'algorithme 1 tel que nous l'avons présenté, nécessite d'avoir préalablement calculé l'arbre d'inclusion des groupes transitifs d'un degré donné auquel on peut associer un ensemble d'invariants relatifs correspondants aux différentes arrêtes. Une implantation très récente de Fieker et Klüners dans Magma (datant de 2007) permet de se détacher de ce genre de données (tous les calculs étant réalisés dynamiquement), il n'y pas encore d'article correspondant mais leur implantation est stupéfiante d'efficacité. Certaines idées de ce genre sont déjà présentent dans l'article de Hulpke [25].

CHAPITRE 4

Calcul du corps de décomposition

4.1. Introduction

Dans ce chapitre, on montre comment calculer efficacement le corps de décomposition d'un polynôme. Nous commencerons par donner un encodage de ce corps à l'aide d'un ensemble triangulaire et nous étudierons quels les propriétés de son image modulo un nombre premier p et ses approximations p-adiques. Nous finirons pas donner des techniques de calculs efficaces pour calculer cet ensemble triangulaire.

Dans tout ce chapitre, le polynôme f sera supposé unitaire et à coefficients entiers et nous le supposerons aussi irréductible.

4.2. Représentation du corps de décomposition de f

Dans toute cette section, on considère un corps $\mathbb{K}$ parfait tel que si f est vu à coefficients dans $\mathbb{K}$ il reste séparable (pour faire plus simple, $\mathbb{K}$ sera soit $\mathbb{Q}$ soit $\mathbb{Q}_p$ soit $\mathbb{Z}/p\mathbb{Z}$).

4.2.1. Idéal des relations. Le corps de décomposition de f sur $\mathbb{K}$, noté $\mathbb{K}_f$, est une extension de $\mathbb{K}$ et on peut le représenter à l'aide d'un polynôme minimal μ d'un élément primitif comme le faisait Galois (voir section 2.1.1). De cet manière nous avons l'isomorphisme

$$\mathbb{K}_f \simeq \mathbb{K}[x]/\langle\mu\rangle$$

et les racines de f peuvent être représentées par des polynômes de degré au plus $N-1$, où N est le degré de μ, par l'intermédiaire de cet isomorphisme.

Dès que l'on voudra faire des calculs avec les racines de f, il faudra donc manipuler des polynômes de degré $N-1$. L'encodage du corps $\mathbb{K}_f$ que nous présentons maintenant permet de réduire ce degré en découpant l'extension simple $\mathbb{K}_f/\mathbb{K}$ en plusieurs extensions successives.

Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ les n racines de f dans une clôture algébrique de $\mathbb{K}$ données dans un ordre fixé. Nous avons le morphisme surjectif canonique $\Psi_{\underline{\alpha}}$, appelé *morphisme d'évaluation* :

$$\begin{aligned} \Psi_{\underline{\alpha}} : \quad & \mathbb{K}[x_1, \ldots, x_n] \longrightarrow\!\!\!\!\!\rightarrow \mathbb{K}_f \\ & P \longmapsto P(\underline{\alpha}) \end{aligned}$$

Le noyau $\mathcal{M}$ de ce morphisme est appelé *idéal des relations* et rassemble, comme son nom l'indique, toutes les relations algébriques en les racines $\underline{\alpha}$ de f (attention, $\mathcal{M}$ dépend du choix de l'ordre donné à $\underline{\alpha}$). Nous allons voir que cet idéal peut être engendré par un système de polynômes de forme particulière.

Définition 4.1. *Un ensemble de polynômes $\mathcal{S} \in \mathbb{K}[x_1, \ldots, x_n]$ sera dit* triangulaire *lorsque $\mathcal{S}$ est composé de n polynômes $f_1, |dots, f_n$ vérifiant*

– $f_i \in \mathbb{K}[x_1, \ldots, x_i]$;

– *f_i est séparable en tant que polynôme en une variable x_i à coefficients dans $\mathbb{K}[x_1, \ldots, x_{i-1}$.*

La proposition qui suit nous donne la forme particulière de $\mathcal{M}$.

PROPOSITION 4.2. *L'idéal $\mathcal{M}$ est maximal et est engendré par un ensemble triangulaire $\mathcal{T}$.*

DÉMONSTRATION. Le fait que cet idéal soit maximal est immédiat. Pour voir que cet idéal est engendré par un ensemble triangulaire nous allons procéder par récurrence. Soit $K_0 = \mathbb{K}$ et $K_i = K_{i-1}[x_i]/\langle \mu_i \rangle$ avec μ_i le polynôme minimal de α_i sur K_{i-1}. Le polynôme μ_i peut être vu comme un polynôme à coefficients dans $\mathbb{K}[x_1, \ldots, x_i]$. Pour tout $0 < i < n$, il existe un idéal $\mathcal{M}_i$ tel que $K_i[x_{i+1}, \ldots, x_n]/\mathcal{M}_i \simeq \mathbb{K}_f$ et nous avons alors $\mathcal{M} = \langle \mu_1(x_1), \ldots, \mu_i(x_1, \ldots, x_i), \mathcal{M}_i \rangle K_1[x_1, \ldots, x_n]$. L'idéal $\mathcal{M}$ est donc engendré par le système de polynômes de $\mathbb{K}[x_1, \ldots, x_n]$

$$\langle \mu_1(x_1), \mu_2(x_1, x_2), \ldots, \mu_n(x_1, \ldots, x_n) \rangle$$

qui est triangulaire. □

La preuve qui précède donne un premier algorithme pour construire le système triangulaire $\mathcal{T}$ de l'idéal $\mathcal{M}$ et de cette manière un encodage du corps de décomposition de f.

Algorithme 3 `Kronecker-Tchebotarev`(f)

Entrée : $f \in \mathbb{Z}[X]$ unitaire et irréductible de degré n.
Sortie : Un ensemble triangulaire définissant le corps $\mathbb{K}_f$.

1: Soit $i = 1$, $\mu_i(x_i)$ un facteur irréductible de $f(x_i)$ sur $\mathbb{K}$ et $K_i = \mathbb{K}[x_i]/\langle \mu_i \rangle$.
2: $i = i + 1$
3: Factoriser $\frac{f}{\mu_1 \cdots \mu_{i-1}}$ sur K_{i-1}
4: Soit μ_i un des facteurs irréductibles que nous venons de calculer, il peut être vu comme un polynôme de $\mathbb{Q}[x_1, \ldots, x_i]$
5: Si $i < n$ on définit $K_i = K_{i-1}[x_i]/\langle \mu_i \rangle$ et continue à l'étape 2
6: Renvoyer $\{\mu_1, \ldots, \mu_n\}$.

Nous venons de voir que l'idéal des relations est engendré par l'ensemble triangulaire

$$\{\mu_1(x_1), \mu_2(x_1, x_2), \ldots, \mu_n(x_1, \ldots)\}$$

qui est une base de Gröbner pour l'ordre lexicographique $x_1 < x_2 < \cdots < x_n$. Ainsi, pour calculer dans le corps de décomposition de f, on pourra encoder ce corps à l'aide de cette base et calculer des formes normales modulo cet ensemble triangulaire pour manipuler ses éléments. En particulier, on pourra évaluer en $\underline{\alpha}$ un polynôme en n variables F en calculant sa forme normale modulo l'ensemble $\mathcal{T}$.

En utilisant une représentation symétrique du groupe de Galois il est immédiat que ce groupe est caractérisé par le résultat suivant :

PROPOSITION 4.3. *Le groupe de Galois* $\mathrm{Gal}(\mathbb{K}_f/\mathbb{K})$ *est donné par*

$$\mathrm{Stab}_{S_n}(\mathcal{M}) = \{\sigma \in S_n \ tq \ \forall F \in \mathcal{M}, \sigma \cdot F \in \mathcal{M}\}$$

Ainsi, étant donné l'idéal $\mathcal{M}$, ou plus exactement un ensemble triangulaire le définissant, on pourra calculer le groupe de Galois correspondant (voir [2], [1] par exemple et [32] pour des améliorations).

La variété associée à l'idéal des relations est équiprojectable (voir [5]) mais sa nature est encore plus particulière. En effet, il est immédiat de voir qu'elle est définie à partir du stabilisateur de $\mathcal{M}$ et de $\underline{\alpha}$, plus exactement nous avons

$$\mathcal{Z}(\mathcal{M}) = \mathrm{Stab}_{S_n}(\mathcal{M}).\underline{\alpha}$$

4.2.2. Variétés galoisiennes. Plus généralement, une variété possédant la propriété d'être définie comme l'orbite de $\underline{\alpha}$ sous l'action d'un sous-groupe U de S_n ne pourra être une $\mathbb{K}$-variété que si elle est stable sous l'action de $G = \mathrm{Gal}(\mathbb{K}(\underline{\alpha})/\mathbb{K})$. Ceci est vérifié si et seulement si le groupe U contient G. Un telle $\mathbb{K}$-variété est appelée *variété galoisienne* et peut être partitionnée selon les classes à gauche de U dans G, on en déduit la décomposition suivante :

$$U \cdot \underline{\alpha} = \bigcup_{\tau \in U//G} \tau G \cdot \underline{\alpha}$$

La $\mathbb{K}$-variété $U \cdot \underline{\alpha}$ est équirojectable, l'idéal radical sur $\mathbb{K}$ sera donc triangulaire (voir [5],[13]) et de la décomposition de la variété ci-avant on en déduit la proposition qui suit.

Proposition 4.4. *Soit I un idéal radical sur $\mathbb{K}$ de variété galoisienne définie par le groupe de U (le stabilisateur de I) et $\underline{\alpha}$, alors*

$$I = \bigcap_{\tau \in U//G} \tau \cdot \mathcal{M}$$

Dans la décomposition de l'idéal I, les idéaux $\tau \cdot \mathcal{M}$ sont maximaux de stabilisateur $\tau G \tau^{-1}$ et sont les idéaux de relations pour l'ordre des racines donné par $\tau \cdot \underline{\alpha}$.

Remarque 4.5. *Tels qu'ils sont définis ici, les idéaux triangulaires sont de dimension 0 et le cardinal de leur variété se lit sur les éléments de sa base triangulaire, il est égal au produit des degrés des monômes initiaux. De cette manière, l'ordre du groupe définissant une variété galoisienne peut être retrouvé facilement à partir des polynômes intervenant dans la base de l'idéal de cette variété.*

Les idéaux de variété galoisienne sont aussi appelés idéaux de Galois et sont utilisés pour l'étude de l'idéal des relations (voir [16],[5]). Une étude duale de ce genre de décomposition basée sur les idempotents de l'algèbre de décomposition universel est décrite par Pohst et Zassenhaus dans [34].

Nous allons maintenant nous intéresser à l'image de l'idéal des relations de f modulo un nombre premier et aux remontées p-adiques correspondantes.

4.3. Approximations p-adiques des racines de f

L'idéal $\mathcal{M}$ est à partir de maintenant l'idéal des relations de f sur $\mathbb{Q}$ pour l'ordre $\underline{\alpha}$ des racines.

Calculer formellement avec les racines de f revient à calculer modulo l'ensemble triangulaire $\mathcal{T}$ qui définit l'idéal des relations $\mathcal{M}$. Si l'on veut obtenir une approximation modulo une puissance d'un nombre premier p d'un tel calcul renvoyant des rationnels ceci revient à renvoyer le résultat de l'opération suivante

$$(F \mod \mathcal{T}) \mod p^k$$

Il faut donc savoir dans quelle mesure une telle opération est possible. De plus, on aimerait pouvoir faire ce calcul sans connaître $\mathcal{T}$. Pour cela nous allons étudier la construction de l'idéal des relations de f vu à coefficients dans le corps des nombres p-adiques. Donnons un bref rappel sur cette structure.

Soit $\mathbb{Z}_p$ la limite projective des anneaux $\mathbb{Z}/p^k\mathbb{Z}$ pour la projection canonique, c'est-à-dire l'ensemble des suites $(a_k)_{k>0}$ telles que $a_k \in \mathbb{Z}/p^k\mathbb{Z}$ et $a_{k+1} \mod p^k = a_k$ pour tout indice $k > 0$. L'ensemble $\mathbb{Z}_p$ est un anneau appelé *anneau des entiers p-adiques.*

Clairement $\mathbb{Z}$ s'injecte dans $\mathbb{Z}_p$ (pour $m \in \mathbb{Z}$ il suffit de considérer la suite $(m \mod p^k)_{k>0}$) et on montre facilement que $\mathbb{Z}_p$ ne contient pas de diviseur de zéro. On peut donc considérer $\mathbb{Q}_p$ le corps des fractions de $\mathbb{Z}_p$ qui contiendra le corps des rationnels $\mathbb{Q}$.

L'anneau $\mathbb{Z}_p$ a une structure d'anneau local d'idéal maximal $\langle p \rangle$, c'est une autre manière de le construire, on localise $\mathbb{Z}$ en p et on le complète selon la distance définie par la valuation v_p qui à un entier n fait correspondre la plus grande puissance k telle que p^k divise n. Ainsi tout élément $a \in \mathbb{Q}_p$ peut être représenté sous la forme d'une série

$$a = \sum_{i \geqslant k} a_i p^i$$

où les a_i sont des représentants des classes $\mathbb{Z}_p/\langle p \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ et l'on choisit de représenter les classes de $\mathbb{Z}/p^k\mathbb{Z}$ par les éléments de $\{\frac{-p^k+1}{2}, \ldots, \frac{p^k}{2}\}$ pour des raisons d'efficacité. ($\mathbb{Z}_p$ correspond donc aux éléments de $\mathbb{Q}_p$ de valuation positive ou nulle.)

Le résultat fondamental attaché aux nombres p-adiques est celui qui permet de ramener des connaissances obtenues modulo p à des connaissances dans $\mathbb{Q}_p$.

Lemme 4.6. *(Hensel) Soit f un polynôme de $\mathbb{Z}_p[X]$ et π le morphisme canonique de projection de $\mathbb{Z}_p$ dans $\mathbb{Z}/p\mathbb{Z}$. Si $\pi(f)$ s'écrit*

$$\pi(f) = \hat{g}\hat{h}$$

dans $\mathbb{Z}/p\mathbb{Z}[x]$ avec $\hat{g}$ et $\hat{h}$ premiers entre eux. Alors ils existent g et h uniques dans $\mathbb{Z}_p[x]$ tels que

$$f = gh$$

dans $\mathbb{Z}_p[x]$ avec $\pi(g) = \hat{g}$ et $\pi(h) = \hat{h}$.

Démonstration. La démonstration de ce lemme peut être retrouvée dans n'importe quel ouvrage de calcul formel. La démonstration de la proposition générale qui suit peut être adaptée à ce cas plus simple. □

D'après ce lemme, un polynôme à coefficients entiers sera irréductible sur $\mathbb{Q}_p$ si et seulement s'il le reste modulo p. Ce résultat peut être généralisé au cas des extensions de $\mathbb{Q}_p$ et en particulier on a la proposition qui suit.

Proposition 4.7. *Soit $l \in \mathbb{Z}_p[x]$ irréductible sur $\mathbb{Q}_p$ et α une racine de l. L'idéal $\mathfrak{P} = pR$ avec $R = \mathbb{Z}_p[\alpha]$ est maximal et si un polynôme $f \in R[x]$ vérifie*

$$f = \hat{g}\hat{h} \mod \mathfrak{p}$$

pour $\hat{g}$ et $\hat{h}$ des polynômes de $R/\mathfrak{p}[x]$ premiers entre eux alors ils existent g et h uniques dans $R[x]$ tel que

$$f = gh \text{ et } \hat{g} = g,\ \hat{h} = h \mod \mathfrak{p}$$

Nous donnons une démonstration basée sur la version simple de la remontée de Hensel. On peut tout aussi bien appliquer une version quadratique comme celle donnée dans [45] ou [9].

Démonstration. Nous avons l'isomorphisme $R/\mathfrak{p} \simeq \mathbb{Z}_p[x]/\langle l, p \rangle$ et en posant $\hat{l} = l \mod p$ on obtient

$$R/\mathfrak{p} \simeq (\mathbb{Z}/p^{\mathbb{Z}})[x]/\langle \hat{l} \rangle$$

qui sera un corps puisque $\hat{l}$ est irréductible comme l d'après le lemme de Hensel. Ainsi l'idéal $\mathfrak{p}$ est maximal.

Soit $\mathfrak{p}^k$ l'idéal p^kR. Nous allons montrer comment construire pour tout $k \geqslant 1$ des polynômes $g^{(k)}$ et h^k tels que

$$f = g^k h^k \mod \mathfrak{p}^k \text{ et } g^k = \hat{g},\ h^k = \hat{g} \mod \mathfrak{p}$$

ainsi en faisant tendre k vers l'infini on obtiendra le résultat.

Fixons $k \geqslant 1$ et supposons que g^k et h^k existent. Les polynômes g^{k+1} et h^{k+1} vérifient

$$f - g^k h^k \in p^k R \text{ ainsi } t = \frac{f - g^k h^k}{p^k} \in R.$$

Comme $\hat{g}$ et $\hat{h}$ sont étrangers et à coefficients dans un corps, nous pouvons calculer les facteurs de Bézout u et v par l'algorithme d'Euclide dans $\mathbb{F}_p[x]$:

$$u\hat{g} + v\hat{h} = 1$$

En posant $g' = tv \mod \hat{h}$ et $h' = tu\hat{g}$ on peut prendre $g^{k+1} = g^k + p^k g'$ et $h^{k+1} = h^k + p^k h'$.

Il suffit de voir que $f = g^{k+1}h^{k+1} \mod \mathfrak{p}^{k+1}$ équivaut à $tp^k = g^k p^k h' + h^k p^k g' \mod \mathfrak{p}^{k+1}$ et en divisant par p^k on a $t = g^k h' + h^k g' \mod \mathfrak{p}^{k+1}$ ce qui nous donne le résultat. □

Corollaire 4.8. *Soit $f \in \mathbb{Z}[x]$ et p un nombre premier. Le polynôme f vu à coefficients dans $\mathbb{Z}_p$ est séparable si et seulement si il l'est vu à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.*

Et on obtient immédiatement

Corollaire 4.9. *Soit $f \in \mathbb{Z}[X]$ et p un nombre premier. Le polynôme f vu à coefficients dans $\mathbb{Z}_p[x]$ est séparable si et seulement si le discriminant* $\mathrm{Disc}(f) \in \mathbb{Z}$ *de f n'est pas divisible par p.*

L'utilisation du lemme de Hensel se fait à l'aide de la remontée utilisée dans la démonstration précédente. On effectue des calculs modulo p et on les remonte modulo p^k pour $k > 0$. Pour cela il faut s'assurer que le résultat que l'on cherche à calculer peut être inclus dans l'anneau $\mathbb{Z}_p$. En ce qui nous concerne ici, puisque nous sommes intéressés par représenter une approximation des racines d'un polynôme f à coefficients dans $\mathbb{Z}$ nous allons chercher à approximer un de ses idéaux de relations.

Proposition 4.10. *Soit $\mathcal{T}$ la base triangulaire d'un idéal des relations de f. Nous avons*

$$\mathcal{T} \subset \frac{1}{\mathrm{Disc}(P)^D}\mathbb{Z}[x_1, \ldots, x_n]$$

où $D > 0$ est un entier obtenu à partir de f.

Démonstration. La démonstration de cette proposition découlera d'un résultat sur interpolation des éléments de $\mathcal{T}$ que nous donnerons plus loin. □

La proposition qui précède nous donne une condition nécessaire et suffisante pour que la base triangulaire $\mathcal{T}$ soit des éléments à coefficients dans $\mathbb{Z}_p$.

Corollaire 4.11. *Si f est séparable modulo p alors l'idéal $\mathcal{M}_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M}$ est engendré par $\mathcal{T}$ sur $\mathbb{Q}_p[x_1, \ldots, x_n]$ et nous avons*

$$\mathcal{T} \subset \mathbb{Z}_p[x_1, \ldots, x_n]$$

Démonstration. Conséquence directe du corollaire 4.8 et la proposition 4.10. □

À partir de maintenant, et jusqu'à la fin de ce chapitre, **le premier p sera supposé**, sauf mention du contraire, **non ramifié dans le corps de rupture de f**.

Plus généralement on peut montrer, en adaptant la proposition 4.24.

PROPOSITION 4.12. *Tout idéal sur $\mathbb{Q}_p$ de variété galoisienne construit à partir des racines de f a une base triangulaire à coefficients dans $\mathbb{Z}_p$.*

D'après la proposition 4.12, les idéaux que nous considérons ont tous des bases que nous pourront relever par le principe de Hensel et d'après le corollaire 4.9 nous pouvons appliquer les résultats de la section 4.2 avec $\mathbb{K} = \mathbb{Q}_p$ où $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. À partir de ces résultats, nous allons donc maintenant étudier la décomposition de l'idéal $\mathcal{M}$ vu dans $\mathbb{Q}_p[x_1, \ldots, x_n]$ par extension des constantes :

$$\mathcal{M}_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{M}$$

. L'idéal $\mathcal{M}_p$ va nous permettre de représenter les racines $\underline{\alpha}$ de f modulo une puissance de p comme désiré.

PROPOSITION 4.13. *L'idéal $\mathcal{M}_p$ est contenu dans un idéal des relations de f sur $\mathbb{Q}_p$ et $\mathcal{M}_p$ est stable sous l'action de* $\mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q})$.

DÉMONSTRATION. Comme $f(x_i)$ s'annule modulo $\mathcal{M}$ pour tout i dans $\{1, \ldots, n\}$ il en sera de même pour $f(x_i)$ modulo $\mathcal{M}_p$ ce qui nous donne la première assertion. Nous avons $\mathrm{Stab}(\mathcal{M}) \subset \mathrm{Stab}(\mathcal{M}_p)$. De plus, comme $\mathcal{M}_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} \langle \mathcal{T} \rangle$ nous avons $|\mathcal{Z}(\mathcal{M}_p)| \leqslant |\mathcal{Z}(\mathcal{M})|$ (voir remarque 4.5 et le résultat suit. □

De cette proposition on obtient la décomposition qui suit.

COROLLAIRE 4.14. *Soit $\mathcal{N}_p$ un idéal des relations de f sur $\mathbb{Q}_p$ contenant $\mathcal{M}_p$ et $G_p := \mathrm{Stab}_{S_n}(\mathcal{N}_p)$ le groupe de Galois de f sur $\mathbb{Q}_p$ correspondant à cet idéal maximal. Nous avons*

$$G_p \subset G = \mathrm{Gal}(\mathbb{Q}(\underline{\alpha})/\mathbb{Q}) \text{ et } \mathcal{M}_p = \bigcap_{\sigma \in G//G_p} \sigma \cdot \mathcal{N}_p$$

De plus, l'idéal $\mathcal{M}$ est l'unique idéal des relations de f sur $\mathbb{Q}$ contenu dans $\mathcal{N}_p$ sur $\mathbb{Q}_p$.

DÉMONSTRATION. Ceci est une conséquence directe de la proposition 4.4 et de la proposition 4.13. □

De ce corollaire on tire qu'un idéal des relations de f sur $\mathbb{Q}_p$ ne peut correspondre qu'un unique idéal $\mathcal{M}$. Nous allons nous servir de cet idéal pour approximer les racines de f.

PROPOSITION 4.15. *Soit f un polynôme à coefficients entiers séparable modulo le premier p. La base triangulaire $\hat{\mathcal{T}}$ d'un idéal des relations de $f \mod p$ peut être remontée en une base triangulaire $\mathcal{T}_p$ d'un idéal des relations $\mathcal{N}_p$ de f sur $\mathbb{Q}_p$. En particulier $\mathcal{T}_p \subset \mathbb{Z}_p[x_1, \ldots, x_n]$*

DÉMONSTRATION. Ce résultat est une conséquence directe de la proposition 4.7 ou plutôt de sa démonstration en construisant récursivement les éléments de la base selon les puissances croissantes. Plus généralement on pourra se référer à la construction de Newton-Hensel pour les ensembles triangulaires décrite par Schost (voir [39]). □

Pour calculer avec des approximations p-adiques des racines de f on commence par calculer $\hat{\mathcal{T}}_p$ puis on remonte cette base modulo des puissances de p pour obtenir $\mathcal{N}_p \mod p^k$ et on pourra calculer des formes normales modulo cet idéal.

DÉFINITION 4.16. *L'approximation modulo p^{k+1} de la base $\mathcal{T}_p \in \mathbb{Z}_p[x_1, \ldots, x_n]$ est notée $\mathcal{T}_p^k$*

4.4. Calcul des racines d'une résolvante et test d'inclusion dans le groupe de Galois

Soit $f \in \mathbb{Z}[x]$ un polynôme unitaire de degré n et supposé irréductible. Dans cette section nous allons montrer comment tester l'inclusion du groupe de Galois de f dans un sous-groupe H de S_n en faisant des calculs avec des approximations p-adiques des racines de f où p est un nombre premier ne divisant pas le discriminant de f. On définit ainsi une fonction Ψ prenant place dans l'algorithme 1.

Ce test d'inclusion, comme décrit dans le chapitre 3, s'effectue en testant si une résolvante d'un H-invariant U-relatif I possède une racine dans $\mathbb{Q}$ (Le groupe $U \in S_n$ contenant le groupe de Galois). Si I est choisi à coefficients entiers (ce qui est toujours possible), ceci revient à tester s'il existe une permutation $\sigma \in U//H$ telle que $(\sigma \cdot I)(\underline{\alpha})$ est un entier puisque les racines de f sont des entiers algébriques. Voyons comment ce test se traduit lorsque que l'on fait les calculs dans $\mathbb{Q}_p$.

PROPOSITION 4.17. *Soit U et H des sous-groupe de S_n tel que U contienne G le groupe de Galois de f et I un H-invariant U-relatif à coefficients entiers. Soit $\mathcal{M}$ l'idéal des relations de f sur $\mathbb{Q}$ de stabilisateur G et $\mathcal{N}_p$ un idéal des relations de f sur $\mathbb{Q}_p$ contenant $\mathcal{M}_p$. S'il existe une permutation $\sigma \in U//H$ et un entier A tel que*

$$(\sigma \cdot I - A) \in \mathcal{N}_p \text{ et } \forall \sigma' \neq \sigma \in U//H,\ (\sigma \cdot I - A) \notin \mathcal{N}_p$$

alors A est une racine simple de la résolvante relative de I et G est contenu dans $\sigma H \sigma^{-1}$.

DÉMONSTRATION. Soit R la résolvante relative de f construite à partir de I. Par hypothèse R est à coefficients entiers et est donnée par

$$R(x) = NF(\prod_{\sigma U//H} (x - \sigma \cdot I), \mathcal{M})$$

Ainsi, en passant au p-adique, nous avons

$$R(A) = NF(\prod_{\sigma U//H} (x - \sigma \cdot I), \mathcal{M}_p) = NF(\prod_{\sigma U//H} (x - \sigma \cdot I), \bigcap_{\tau \in G//G_p} \tau \cdot \mathcal{N}_p)$$

Comme G est contenu dans U et que R est laissée stable par U par définition, on a égalité des $NF(\prod_{\sigma U//H}(x - \sigma \cdot I), \tau \cdot \mathcal{N}_p)$ pour tout $\tau \in U//H$. Comme la transversale $U//H$ contient l'identité et que $NF(\prod_{\sigma U//H}(x - \sigma \cdot I), \mathcal{N}_p) = 0$ par hypothèse, par le *théorème des restes chinois* on a

$$NF(\prod_{\sigma U//H} (x - \sigma \cdot I), \bigcap_{\tau \in G//G_p} \tau \cdot \mathcal{N}_p) = 0$$

et donc A est une racine de R sur $\mathbb{Q}_p$ et $\mathbb{Q}$. Si cette racine n'était pas simple elle ne le serait pas dans $\mathbb{Q}_p$ ce qui est absurde par hypothèse. Le résultat suit. □

COROLLAIRE 4.18. *Soit U et H des sous-groupe de $\S_n$ tel que U contienne G le groupe de Galois de f et I un H-invariant U-relatif à coefficients entiers. Soit $\mathcal{M}$ l'idéal des relations de f sur $\mathbb{Q}$ de stabilisateur G et $\mathcal{N}_p$ un idéal des relations de f sur $\mathbb{Q}_p$ contenant $\mathcal{M}_p$. La résolvante relative R de f construite à partir de I est à coefficients entiers et vérifie*

(1) *Si $R \mod p$ possède une racine dans $\mathbb{Z}/p\mathbb{Z}$ de multiplicité v alors elle peut être remontée en v racine de R sur $\mathbb{Q}_p[x_1, \ldots, x_n]/\mathcal{N}_p$*

(2) *Supposons qu'il existe* $\sigma \in U$ *tel que* $(\sigma \cdot I - a \mod p) \in \hat{\mathcal{N}_p}$ *pour* $a \in \mathbb{Z}/p\mathbb{Z}$ *(a est une racine de* $R \mod p$*) et tel que la remontée* A *de la racine* a *est une racine entière simple de* R *sur* $\mathbb{Q}_p[x_1, \ldots, x_n]/\mathcal{N}_p$*. Alors* $\sigma H \sigma^{-1}$ *contient* G*. Au contraire, si aucune des racines de* R *dans* $\mathbb{Z}/p\mathbb{Z}$ *ne peuvent être remontées en des racines dans* $\mathbb{Z}$ *pour* R *sur* $\mathbb{Q}_p$ *alors* G *ne peut être contenu dans aucun des* U*-conjugués de* H*.*

Cette proposition et son corollaire nous donne un test d'inclusion sur $\mathbb{Q}_p$ nécessitant la connaissance de $\mathcal{N}_p$ qui est aussi dur à calculer que $\mathcal{M}$. Nous avons le corollaire qui suit par application du principe de Hensel.

C'est le point 2 du corollaire précédent que nous allons mettre en pratique pour faire nos tests d'inclusion selon des approximations p-adiques des racines de f. Le point 1 permet de rejeter de suite des groupes H.

Proposition 4.19. *En reprenant les mêmes hypothèses que dans le corollaire 4.18. Soit* M *une borne entière sur la norme des racines de* R *dans* $\mathbb{C}$ *et un entier* k *tel que* $p^{k+1} > (2M)^{[U:H]}$*. Nous avons les tests suivants*

(1) *Si* R *ne possède aucune racine dans* $\mathbb{Z}/p\mathbb{Z}$ *alors* G *n'est contenu dans aucun des* U*-conjugués de* H*.*

(2) *Supposons qu'il existe un sous-ensemble* $\mathcal{S}$ *de* $U//H$ *tel que pour tout* $\sigma \in \mathcal{S}$ *il existe un élément* $a_\sigma \in \mathbb{Z}/p\mathbb{Z}$ *vérifiant* $\sigma \cdot I - a_\sigma \in \hat{\mathcal{N}_p}$*. S'il existe* $\sigma \in \mathcal{S}$ *tel que* $A_\sigma = NF(\sigma \cdot I, \mathcal{T}_p^{k+1})$ *vérifie*

$$A_\sigma \in \mathbb{Z}/p^{k+1}\mathbb{Z},\ |A_\sigma| < M,\ A_\sigma \neq NF(\sigma' \cdot I, \mathcal{T}^k)\ \forall \sigma' \neq \sigma \in \mathcal{S}$$

alors G *est contenu dans* $\sigma H \sigma^{-1}$

Démonstration. Le premier point est immédiat. Comme $\sigma \cdot I - A_\sigma$ est à coefficients entiers, nous pouvons considérer la réduction modulo p^{k+1} de cet élément de $\mathbb{Z}_p[x_1, \ldots, x_n]$. Nous avons $\sigma \cdot I - A_\sigma \mod (\mathcal{N}_p, p^{k+1}) = \sigma \cdot I - A_\sigma \mod (\mathcal{T}_p^{k+1}, p^{k+1}) = 0$. En appliquant le même raisonnement pour la résolvante R et en posant $A = A_\sigma$, nous avons :

$$R(A) \mod p^{k+1} = NF(\prod_{\sigma \in U//H} (A - \sigma \cdot I), \mathcal{M}_p) \mod p^{k+1}$$

Comme

$$NF(\prod_{\sigma \in U//H} (A - \sigma \cdot I), \mathcal{N}_p) \mod p^{k+1} = NF(\prod_{\sigma \in U//H} (A - \sigma \cdot I), \mathcal{T}_p^k) \mod p^{k+1} = 0$$

en appliquant le même raisonnement que dans la démonstration de la proposition 4.17) on a

$$R(A) = NF(\prod_{\sigma \in U//H} (A - \sigma \cdot I), \cap_{\tau \in G//G_p} \tau \cdot \mathcal{N}_p) \mod p^{k+1} = 0$$

Donc $R(x) = (x - A)h(x) + p^{k+1}g(x)$ avec h et g des polynômes dans $\mathbb{Z}[x]$. Par hypothèse, $|R(A)| < (2M)^{[U:H]} < p^{k+1}$ ainsi $R(A) = 0$. Pour montrer que A est une racine simple de R on fait comme dans la preuve de la proposition 4.17. □

De cette proposition on tire tous les instruments permettant de modifier l'algorithme de Stauduhar pour calculer le groupe de Galois à partir d'approximations p-adiques des racines de f. Dans la pratique, on commence par calculer $\hat{\mathcal{N}_p}$ et son stabilisateur G_p en faisant des calculs modulo p. On fixe l'ordre des racines à l'aide de cet idéal : au départ on a $G_p \subset G \subset S_n$ et au fur et à mesure des tests d'inclusion on trouvera le stabilisateur G de

$\mathcal{M}$ contenu dans $\mathcal{N}_p$. L'action de G sur les racines de f dans $(\mathbb{Z}/p^{k+1}\mathbb{Z}[x_1,\ldots,x_n])/\langle\mathcal{T}_p^k\rangle$ sera vue comme l'action du groupe de Galois sur des approximations p-adiques des racines.

4.5. Calcul de l'ensemble triangulaire $\mathcal{T}$ à partir de la sortie de l'algorithme de Stauduhar p-adique.

Dans cette section nous allons montrer comment calculer efficacement l'ensemble triangulaire $\mathcal{T} \in \mathbb{Q}[x_1,\ldots,x_n]$ d'un idéal des relations $\mathcal{M}$ de $f \in \mathbb{Z}[x]$ à partir de la sortie de l'algorithme de Stauduhar en version p-adique comme élaboré dans la section précédente.

4.5.1. Interpolation de l'ensemble $\mathcal{T}$. Dans [13] Dahan et Schost proposent une formule d'interpolation générale pour chacun des polynômes intervenant dans un ensemble triangulaire $\mathcal{T}$ (Lederer a proposé le même genre de formules d'interpolation dans [31] en se limitant aux idéaux de relations). Ces formules se basent sur l'analyse de la variété équiprojectable définie par l'ensemble $\mathcal{T}$.

Nous allons voir ici comment l'analyse du groupe G, stabilisateur de l'idéal $\mathcal{T}$ peut réduire le nombre de coefficients à calculer.

La forme générique de $\mathcal{T}$. L'étude de G nous donne facilement une forme générique pour l'ensemble triangulaire $\mathcal{T} = \{f_1(x_1), f_2(x_1,x_2),\ldots,f_n(x_1,\ldots,x_n)\}$ que l'on suppose réduit. En effet, puisque $f_i(\underline{\alpha}, x_i)$ est le polynôme définissant de l'extension $K_i = \mathbb{Q}(\alpha_1,\ldots,\alpha_i)$ sur $K_{i-1} = \mathbb{Q}(\alpha_1,\ldots,\alpha_{i-1})$ dont le degré est donné par $\frac{|\operatorname{Gal}(\mathbb{Q}(\underline{\alpha})/K_{i-1})|}{|\operatorname{Gal}(\mathbb{Q}(\underline{\alpha})/K_i)|}$ d'après la correspondance galoisienne. Ainsi, pour tout $i \in \{1,\ldots,n\}$ on a $\operatorname{Deg}_{x_i}(f_i) = |\operatorname{Stab}_G[1,\ldots,i-1]|/|\operatorname{Stab}[1,\ldots,i]|$ et pour tout $j \in \{1,\ldots,i-1\}$

$$\operatorname{Deg}_{x_j}(f_i) < |\operatorname{Stab}_G[1,\ldots,j-1]|/|\operatorname{Stab}[1,\ldots,j]|$$

A partir de ces bornes on obtient une forme générique (c'est celle que nous obtenons en appliquant [13] ou [31]) pour les éléments de $\mathcal{T}$, c'est à dire un polynôme à coefficients indéterminés

$$f_i = x_i^{d_i} + \sum c_j x_1^{j_1}\cdots x_n^{j_n}$$

dont le nombre de coefficients indéterminés est donné par $\prod_{j\in\{1,\ldots,n\}}(d_j-1)$ où $d_j = |\operatorname{Stab}_G[1,\ldots,j-1]|/|\operatorname{Stab}[1,\ldots,j]| < |G|$. Ce nombre peut être très grand (borné par $n!$) et l'on aimerait pouvoir le réduire.

Réduction du nombre d'indéterminées : i-relations. Pour réduire ce nombre d'indéterminées, nous allons chercher des relations entre les $\underline{\alpha}$ qui peuvent remplacer $f_i \in \mathcal{T}$ et qui comporteront moins de coefficients indéterminés à calculer.

Définition 4.20. *Soit E un sous-ensemble de $\{1,\ldots,i\}$, nous noterons X_E l'ensemble des indéterminée $\{x_i : i \in E\}$. L'ensemble E est appelé* i-relation *si* $\max(E) = i$ *et s'il existe un polynôme $r_i \in \mathbb{Q}[X_E]$ tel que*

$$\alpha_i^{d_i} + r_i(\underline{\alpha}) \text{ avec } \operatorname{Deg}_{x_i}(r_i) < d_i$$

L'exemple le plus simple de i-relation est donné par l'ensemble $\{1,\ldots,i\}$ et dans ce cas une relation correspondant pourra être le polynôme f_i. Pour ce polynôme nous avons vu comment identifier les bornes sur les multi-degrés de ses termes. Le résultat qui suit permet de faire de même avec des i-relations plus générales.

Proposition 4.21. *Soit $E = \{e_1 < e_2 < \cdots < e_s = i\}$ une i-relation. Il existe un polynôme $r_i \in \mathbb{Q}[X_E]$ comme dans la définition 4.20 tel que pour tout $j \in \{1,\ldots,s\}$*

$$\operatorname{Deg}_{x_j}(r_i) < \frac{|\operatorname{Stab}_G[e_1,\ldots,e_{s-1}]|}{|\operatorname{Stab}_G[e_1,\ldots,e_s]|}$$

DÉMONSTRATION. Est une conséquence directe de la correspondance galoisienne. □

Pour calculer des i-relations non triviales, on peut utiliser le résultat immédiat suivant

LEMME 4.22. *Soit $1 < i \leqslant n$ un entier et $1 < m < i$ le plus petit entier tel que*

$$d_i = \frac{|\operatorname{Stab}_G[1,\ldots,m]|}{|\operatorname{Stab}_G[e_1,\ldots,m,i]|}.$$

Il existe une i-relation dans $\{1,\ldots,m\}$.

Ce lemme permet de calculer rapidement des i-relations mais ne permettra pas de trouver les meilleurs. Ci-après nous définissons ce qu'est la meilleure i-relation possible.

DÉFINITION 4.23. *Soit $E_i = \{e_1 < e_2 < \cdots < e_s = i\}$ une i-relation. Le degré $\operatorname{Deg}_{e_j}(E_i)$ de E_i en $e_j \in E_i$ est défini comme suit*

$$\operatorname{Deg}_{e_j}(E_i) = \frac{|\operatorname{Stab}_G[e_1,\ldots,e_{j-1}]|}{|\operatorname{Stab}_G[e_1,\ldots,e_j]|}$$

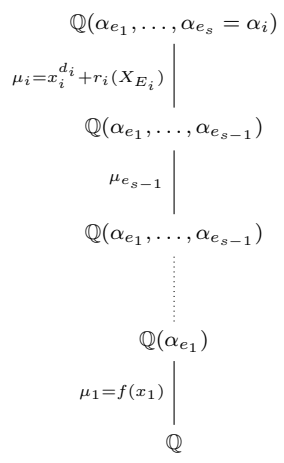
Le degré $\operatorname{Deg}(E_i)$ est donné par le produit des degrés de E_i en les $e_j \in E_i$. La i-relation E_i est dite minimale *lorsqu'elle est minimale pour son degré et son cardinal dans l'ensemble des i-relations.*

Le problème de calculer une i-relation minimale relève de la combinatoire et il n'y a pas d'algorithme efficace connu mais, étant donné un groupe G, ce calcul peut être fait une fois pour toute et stocké.

Les i-relations minimales correspondent aux sous-corps K de $K_i = \mathbb{Q}(\alpha_1,\ldots,\alpha_i)$ de degré absolu minimal et engendrés par des racines de f prises dans $\{\alpha_1,\ldots,\alpha_{i-1}\}$. Le nombre de coefficients indéterminés à calculer pour retrouver le polynôme définissant l'extension K/K_i est donné par le degré de la i-relation correspondant. Ceci peut se résumer par la figure **??**.

4.5.2. Formules de Lagrange et i-relations. Soit E_i une i-relation, nous allons présenter une formule permettant de retrouver le polynôme associé à E_i à partir de la variété équiprojectable de $\mathcal{M}$.

Nous avons vu qu'à une i-relation $E_i = \{e_1 < e_2 < \cdots < e_s = i\}$ on peut associer une extension. En fait, on peut lui associer un ensemble triangulaire.



En effet, on peut lui associer les polynômes minimaux μ_j des extensions successives construites à partir des racines de f d'indices croissants dans E_i. Ces polynômes peuvent être représentés à l'aide de polynômes g_j dans $\mathbb{Q}[X_{E_i}]$ et l'ensemble $\{g_{e_1},\ldots,g_{e_s}\}$ sera triangulaire par définition. Le polynôme g_{e_s} étant celui qui pourra remplacer f_i dans $\mathcal{T}$. Pour calculer l'ensemble des g_j, on peut appliquer les formules de Lagrange données par Dahan et Schost dans [13] mais comme la variété utilisée ici est définie par un groupe de permutations, nous allons utiliser ce cadre particulier pour définir ces formules. Soit σ une permutation de S_n. Nous notons $\mathcal{O}(j,\sigma)$ l'orbite de $\sigma(e_j)$ sous l'action du *stabilisateur point-à-point* $\operatorname{Stab}_G[\sigma(e_1),\ldots,\sigma(e_{j-1})]$ qui est défini par l'ensemble $\{\tau \in G \,|\, \tau(\sigma(e_i))\forall i \in \{1,\ldots,j-1\}\}$. Ainsi, l'ensemble $\mathcal{O}(j,\sigma)$ représente l'ensemble des indices des racines conjuguées de $\sigma(\alpha_{e_j}) = \alpha_{\sigma(e_j)}$ sur le corps $\mathbb{Q}(\alpha_{\sigma(e_1)},\ldots,\alpha_{\sigma(e_{j-1})})$. Ceci posé, on peut donner la formule de Lagrange définissant g_i.

PROPOSITION 4.24. *Soit $E_i = \{e_1 < \ldots < e_s = i\}$ une i-relation. Le polynôme g_i correspondant à E_i peut être interpolé par la formule*

$$\sum_{\sigma \in \mathrm{Trans}} \left(\left(\prod_{j=1}^{s-1} \prod_{\substack{e \in O(j,\sigma) \\ e \neq \sigma(e_j)}} \frac{x_{e_j} - \alpha_e}{\alpha_{\sigma(e_j)} - \alpha_e} \right) \prod_{e \in O(s,\sigma)} x_i - \alpha_e \right)$$

où Trans *est la transversale* $G_f // \mathrm{Stab}_{G_f}([e_1, \ldots, e_s])$

À partir de i-relations pour chacun des polynômes de $\mathcal{T}$ et de l'action du groupe G sur des approximations des racines de f (nous connaissons une approximation $\mathcal{T}_p^k$ de l'ensemble triangulaire engendrant l'idéal maximal $\mathcal{N}_p$ contenant $\mathcal{M}_p$). En effectuant des calculs de formes normales modulo l'ensemble triangulaire $\mathcal{T}_p^k$, on pourra interpoler une approximation du polynôme g_i à l'aide de la formule de la proposition 4.24. De cette manière, on peut calculer une approximation p-adique de la base triangulaire $\mathcal{T}$. Nous verrons plus loin comment certifier qu'une approximation est suffisante, pour le moment nous allons voir comment éviter le calcul de certains polynômes de $\mathcal{T}$ grâce à la connaissance du groupe G.

4.5.3. Schéma de calcul : où comment éviter des calculs superflus. Dans [33, 35, 32] des techniques pour éviter des calculs lors de la construction $\mathcal{M}$ à partir de données partielles sur le groupe G sont introduits. Dans [38],[36, 37] ces techniques sont exploitées afin de définir un *schéma de calcul* de $\mathcal{T}$ associé au groupe G. Ce schéma de calcul ne dépend que de G et peut être calculé une fois pour toute et stocké pour des calculs ultérieurs.

Étant donné le groupe $G \subset S_n$, on suppose connue une i-relation E_i pour chacun des polynômes g_i de l'ensemble triangulaire d'un idéal de relations de stabilisateur G. Nous allons voir comment éviter le calcul de certains polynômes de $\mathcal{T}$ par simple analyse du groupe G.

Modules de Cauchy généralisés. Soit à calculer l'ensemble triangulaire $\mathcal{T} = \{g_1, \ldots, g_n\}$ de $\mathcal{M}$ et rappelons que l'on note d_i le degré de g_i en x_i. Notons $\mathcal{O} = \{i_1 = i < i_2 < \cdots < i_k\}$ l'orbite de i sous l'action du groupe $\mathrm{Stab}_G[1, \ldots, i-1]$. Nous avons $k = d_i$ et cette orbite représente les indices des racines de f qui sont les racines de g_i. Pour un polynôme multivarié g on notera $\mathrm{Ev}(g, u)$ l'évaluation de g où l'on a remplacé sa variable dominante par u. Nous définissons alors.

DÉFINITION 4.25. *Les* modules de Cauchy *généralisés de g_i sont les d_i polynômes définis par $c_1(g_i) = g_i$ et*

$$c_2(g_i) = \frac{Ev(c_1, x_{i_2}) - Ev(c_1, x_{i_1})}{(x_{i_2} - x_{i_1})}, \ \cdots, \ c_{d_i}(g_i) = \frac{Ev(c_{d_i-1}, x_{i_{d_i}}) - Ev(c_{d_i-1}, x_{i_{d_i-1}})}{(x_{i_{d_i}} - x_{i_{d_i-1}})}.$$

Les modules de Cauchy (appelés aussi différences divisées) représentent les facteurs génériques d'un polynôme dans chacune des extensions de la tour qui va jusqu'à son corps de décomposition. Ils ont été introduit par Cauchy [8] pour définit une base des fonctions symmétriques évaluées en les racines d'un polynôme. Par construction, nous avons le résultat suivant.

PROPOSITION 4.26. *Le polynôme $c_j(g_i)$ est un polynôme de $\mathbb{Q}[X_{\{1,\ldots,i_j\}}]$ unitaire en la variable x_{i_j} et de degré $d_i - j + 1$ en x_{i_j}. De plus, ce polynôme est inclus dans $\mathcal{M}$.*

La connaissance de G nous permet de calculer au préalable les degrés en leur variable dominante des polynômes g_i et des modules de Cauchy correspondants à chacune des i-relations. Par exemple, si le degré en x_{i_j} du polynôme g_j est le même que celui de $c_j(g_i)$ alors on pourra remplacer g_i par ce module de Cauchy dans l'ensemble triangulaire $\mathcal{T}$. Ainsi on remplace l'interpolation d'un polynôme par celui du calcul d'une différence divisée qui est moins coûteux en général.

Transporteur. Ici nous utilisons le fait que G est le stabilisateur de l'idéal $\mathcal{M}$.

DÉFINITION 4.27. *Soit $E_i = \{e_1 < e_2 < \cdots < e_s = i\}$ une i-relation et $j \in \{i+1, \ldots, n\}$. Une permutation $\sigma \in G_f$ est appelée* (i,j)-transporteur *dès qu'elle satisfait :*

$$\sigma(i) = j \text{ et } j = max(\{\sigma(e) : e \in E_i\})$$

Les transporteurs peuvent être déterminés par l'analyse du groupe G et à partir des la connaissance des i-relations correspondant aux polynômes de la base à calculer. Par construction nous avons.

PROPOSITION 4.28. *Soit σ un (i,j)-transporteur et g_i le polynôme à la i-relation E_i. Alors, $NF(\sigma \cdot g_i, \{g_1, \ldots, g_{j-1}\})$ est un facteur de g_j en tant que polynôme sur $\mathcal{A} = (\mathbb{Q}[X_{\{1,\ldots,j-1\}}]/\langle g_1, \ldots, g_{j-1}\rangle)[x_j]$.*

DÉMONSTRATION. Puisque σ est un (i,j)-transporter, le polynôme $NF(g_i^\sigma, \{g_1, \ldots, g_{j-1}\})$ peut être vu comme un polynôme h en une variable x_j sur $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$. De plus, puisque $\sigma \cdot g_i \in \mathcal{M}$, nous avons $h(\alpha_j) = 0$. Ainsi h est un multiple du polynôme minimal de α_j sur $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})$, donc h est un multiple de g_i en tant que polynôme sur $\mathcal{A}$ □

COROLLAIRE 4.29. *En reprenant les mêmes notations que dans la proposition 4.28. Si les degrés d_j et d_i sont égaux alors $\sigma \cdot g_i$ peut remplacer g_j dans $\mathcal{T}$.*

Comme pour les modules de Cauchy, la connaissance d'un (i,j)-transporteur vérifiant les hypothèses du corollaire 4.29 permet de remplacer l'interpolation de polynôme g_j par l'application d'un transport par σ de g_i qui sera bien moins coûteux.

L'ensemble des i-relations et des techniques permettant d'éviter des interpolations par modules de Cauchy ou transporteurs peut être stocké et forme ainsi un schéma de calcul générique pour tout idéal des relations de stabilisateur G.

4.5.4. Bornes sur les coefficients de $\mathcal{T}$ et certification préalable. Nous donnons ici une borne sur les coefficients de g_i obtenue à l'aide de la formule d'interpolation donnée dans la proposition 4.24. La démonstration faite ici reprend celle de Lederer [31] en l'adaptant aux i-relations (voir [37]). Notons L_i la formule définissant g_i, il est immédiat que la multiplication par une puissance de $\mathrm{Disc}(f)$ permet de ramener L_i à coefficients entiers. Plus exactement, la multiplication de L_i par $\mathrm{Disc}(f)$ permet de réduire deux dénominateurs de la forme $\prod_{\substack{e \in O(j,\sigma) \\ e \neq \sigma(e_j)}} \frac{1}{\alpha_{\sigma(e_j)} - \alpha_e}$. Ainsi, l'ensemble des dénominateurs pourront être réduits par la multiplication de $D_i = \mathrm{Disc}(f)^{\lceil \frac{s}{2} \rceil}$.

Le polynôme $D_i L_i$ est donc à coefficients entiers, nous allons donner une borne pour c, le coefficient correspondant au multi-degré $(k_1, \ldots, k_s)$. Soit δ une borne sur les normes des différences des racines $|\alpha_i - \alpha_j|$ et ν une borne sur les normes $|\alpha_i|$.

- Le numérateur de $D_i L_i$ est composé du produit de $n(n-1)\lceil \frac{s}{2} \rceil - d_1 - \ldots - d_s + s$ éléments de la forme $(\alpha_j - \alpha_i)$. Ce produit est distribué sur tous les coefficients de g_i et est borné par $\mathbb{B} = \delta^{n(n-1)\lceil \frac{s}{2} \rceil - d_1 - \ldots - d_s + s}$.
- La variable x_{e_i} de degré k_i dans L_i provient d'un produit de $d_i - 1$ éléments de la forme $(x_{e_i} - \alpha_j)$. Ainsi, la norme de son coefficient est majoré par $\binom{d_i - 1}{k_i} \nu^{d_i - 1 - k_i}$.

En sommant tous ces produit sur la transversale définissant la formule d'interpolation, on obtient la borne

$$|c| \leqslant d(E_i)\binom{d_1-1}{k_1}\nu^{d_1-1-k_1}\cdots\binom{d_s}{k_s}\nu^{d_s-k_s}\mathbb{B}.$$

À partir de cette borne, on pourra certifier qu'un calcul fait par approximations p-adiques peut être considéré comme celui attendu sur $\mathbb{Q}$. Cette borne est la meilleure à notre connaissance pour le calcul de l'idéal des relations mais elle est souvent très pessimiste. Nous donnons ci-après un moyen de tester si un ensemble triangulaire candidat $\mathcal{T}^c = \{h_1, \ldots, h_n\}$ obtenue par interpolation selon des approximations p-adiques et des reconstructions rationnelles est bien une base pour $\mathcal{M}$.

Pour ce faire il suffit de vérifier que l'idéal engendré par $\mathcal{T}^c$ contient les modules de Cauchy de f, le résultat suivant montrer ceci.

PROPOSITION 4.30. *Nous avons l'égalité $h_j = g_j$ si et seulement si*

$$NF(c_j(f), \{g_1, \ldots, g_{j-1}, h_j\}) = 0$$

DÉMONSTRATION. La condition nécessaire est immédiate. Montrons la réciproque. Soit $\mathcal{H}$ l'ensemble triangulaire $\{g_1, \ldots, g_{j-1}, h_j\}$. Par hypothèse, l'idéal $\langle\mathcal{H}\rangle$ contient $\{c_1(f), \ldots, c_j(f)\}$ qui est une base de Gröbner réduite de l'idéal d'élimination $\mathcal{M} \cap \mathbb{Q}[X_{\{1,\ldots,j\}}]$. Ainsi, $\langle\mathcal{H}\rangle$ est contenu dans un idéal maximal $\mathcal{M}'$ de $\mathbb{Q}[X_{\{1,\ldots,j\}}]$. Cet idéal maximal coïncide avec $\sigma \cdot \mathcal{M} \cap \mathbb{Q}[X_{\{1,\ldots,j\}}]$ pour un $\sigma \in S_n$. Mais, en comparant les dimensions des anneaux quotient correspondant, il vient que$\langle\mathcal{H}\rangle = \mathcal{M}' = \mathcal{M}^\sigma \cap \mathbb{Q}[X_{\{1,\ldots,j\}}]$. Leurs stabilisateurs seront égaux et il vient σ est l'identité et $h_j = f_j$. □

Bibliographie

[1] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *AAECC*, 15(3-4) :279–294, 2004.

[2] H. Anai, M. Noro, and K. Yokoyama. Computation of the splitting fields and the Galois groups of polynomials. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, volume 143 of *Progr. Math.*, pages 29–50. Birkhäuser, Basel, 1996.

[3] H. Anai and K. Yokoyama. Radical representation of polynomial roots. *Sūrikaisekikenkyūsho Kōkyūroku*, (920) :9–24, 1995. Research on the theory and applications of computer algebra (Japanese) (Kyoto, 1994).

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

[5] Ph. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6) :635–651, 2000. Algorithmic methods in Galois theory.

[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4) :235–265, 1997. Computational algebra and number theory (London, 1993).

[7] D. Casperson and J. McKay. Symmetric functions, m-sets, and Galois groups. *Math. Comp.*, 63(208) :749–757, 1994.

[8] A. Cauchy. Usage des fonctions interpolaires dans la détermination des fonctions symétriques des racines d'une équation algébrique donnée. *Oeuvres*, **5** :473 Extrait 108, 1840.

[9] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[10] Antoine Colin. Formal computation of Galois groups with relative resolvents. In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Comput. Sci.*, pages 169–182. Springer, Berlin, 1995.

[11] Antoine Colin. Relative resolvents and partition tables in Galois group computations. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 78–84 (electronic), New York, 1997. ACM.

[12] David A. Cox. *Galois theory*. Pure and Applied Mathematics (New York). Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2004.

[13] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC '04 : Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 103–110, New York, NY, USA, 2004. ACM Press.

[14] H. Darmon and D. Ford. Computational verification of M_{11} and M_{12} as Galois groups over $\mathbf{Q}$. *Comm. Algebra*, 17(12) :2941–2943, 1989.

[15] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

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

[17] Y. Eichenlaub. *Problèmes effectifs de théorie de Galois en degrés 8 à 11.* Thèse de Doctorat, Université Bordeaux I, 1996.
[18] E. Galois. *Œuvres Mathématiques.* Gauthier-Villars, Paris, 1897.
[19] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005. (`http://www.gap-system.org`).
[20] K. Geissler. *Berechnung von Galoisgruppen über Zhal- und Funktionenkörpern.* Dissertation, Universität Berlin, 2003.
[21] K. Geissler and J. Klüners. Galois group computation for rational polynomials. *J. Symbolic Comput.*, 30(6) :653–674, 2000. Algorithmic methods in Galois theory.
[22] K. Girstmair. On the computation of resolvents and Galois groups. *Manuscripta Math.*, 43(2-3) :289–307, 1983.
[23] K. Girstmair. On invariant polynomials and their application in field theory. *Math. Comp.*, 48(178) :781–797, 1987.
[24] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 175–182 (electronic), New York, 2001. ACM.
[25] Alexander Hulpke. Galois groups through invariant relations. In *Groups St. Andrews 1997 in Bath, II*, volume 261 of *London Math. Soc. Lecture Note Ser.*, pages 379–393. Cambridge Univ. Press, Cambridge, 1999.
[26] Camille Jordan. *Traité des substitutions et des équations algébriques.* Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Éditions Jacques Gabay, Sceaux, 1989. Reprint of the 1870 original.
[27] Gregor Kemper and Allan Steel. Some algorithms in invariant theory of finite groups. In *Computational methods for representations of groups and algebras (Essen, 1997)*, volume 173 of *Progr. Math.*, pages 267–285. Birkhäuser, Basel, 1999.
[28] L. Kronecker. Grundzüge einer Arithmetischen Theorie der Algebraischen Grössen. *J. Reine Angew. Math.*, 92 :515–534, 1882.
[29] J.-L. Lagrange. *Œvres Complètes.* Gauthier-Villars, Paris, 1867-1892. 14 volumes.
[30] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.
[31] M. Lederer. Explicit constructions in splitting fields of polynomials. *Riv. Mat. Univ. Parma (7)*, 3* :233–244, 2004.
[32] S. Orange. *Calcul de corps de décomposition et de groupes de décomposition.* Thèse de Doctorat, Université Paris 6, 2006.
[33] S. Orange, G. Renault, and A. Valibouze. Calcul efficace d'un corps de décomposition. LIP6 Research Report 005, LIP6, Laboratoire d'Informatique de Paris 6, 2003.
[34] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory.* Cambridge Univ. Press, Cambridge, 1989.
[35] G. Renault. *Calcul efficace de corps de décomposition.* Thèse de Doctorat, Université Paris 6, 2005.
[36] G. Renault and Yokoyama K. A modular method for computing the splitting field of a polynomial. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *ANTS*, volume 4076 of *Lecture Notes in Computer Science*, pages 124–140. Springer, 2006.
[37] Guénaël Renault and Kazuhiro Yokoyama. Multi-modular algorithm for computing the splitting field of a polynomial. In J. Rafael Sendra and Laureano González-Vega, editors, *ISSAC*, pages 247–254. ACM, 2008.

[38] Guénaël Renault. Computation of the splitting field of a dihedral polynomial. In Barry M. Trager, editor, *ISSAC*, pages 290–297. ACM, 2006.
[39] É. Schost. Complexity results for triangular sets. *J. Symbolic Comput.*, 36(3-4) :555–594, 2003. International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).
[40] L. Soicher and J. McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3) :273–281, 1985.
[41] R. Stauduhar. The determination of galois groups. *Math. Comp.*, 27 :981–996, 1973.
[42] Jean-Pierre Tignol. *Galois' theory of algebraic equations*. World Scientific Publishing Co. Inc., River Edge, NJ, 2001.
[43] B. L. van der Waerden. *Algebra. Vol. I.* Springer-Verlag, New York, 1991. Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberger.
[44] B. L. van der Waerden. *Algebra. Vol. II.* Springer-Verlag, New York, 1991. Based in part on lectures by E. Artin and E. Noether, Translated from the fifth German edition by John R. Schulenberger.
[45] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.
[46] K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118 :617–636, 1997. Algorithms for algebra (Eindhoven, 1996).
[47] Kazuhiro Yokoyama, Masayuki Noro, and Taku Takeshima. On determining the solvability of polynomials. In *ISSAC*, pages 127–134, 1990.