Sur le calcul du groupe de Galois de polynômes de degrés ≥ 5

Mémoire

Nicolas Bureau

Maîtrise en mathématiques
Maître ès sciences (M.Sc.)

Québec, Canada

Résumé

Déterminer le groupe de Galois d'un polynôme rationnel ou encore d'une extension de corps n'est pas, en général, un travail de tout repos s'il est effectué manuellement. La difficulté de ce problème nous amène donc à vouloir automatiser le processus à l'aide d'algorithmes qui prennent le polynôme en entrée et ressortent son groupe de Galois en un temps raisonnable. Le présent mémoire a pour but de mettre la lumière sur deux algorithmes connus tout en présentant les résultats nécessaires pour les comprendre et les reproduire. Le tout est ensemencé d'exemples pour aider à comprendre certaines notions utilisées. Dans un niveau d'ordre un peu différent, nous analysons une particularité du deuxième algorithme, c'est-à-dire la provenance des polynômes à plusieurs variables utilisés lors de la construction de la résolvante du polynôme dont nous voulons trouver le groupe de Galois.

Table des matières

Liste des tableaux

Liste des figures

À Roma

If one proves the equality of two numbers a and b by showing first that $a \leq b$ and then $a \geq b$, it is unfair ; one should instead show that they are really equal by disclosing the inner ground for their equality.

Emmy Noether

Remerciements

Je tiens à remercier tout d'abord mon directeur de maîtrise, M. Claude Levesque, professeur à la retraite au Département de mathématiques et de statistique de l'Université Laval. Ce mémoire n'aurait jamais vu le jour si ce n'était de ses judicieux conseils, de ses encouragements et de sa confiance en mon travail. Source inépuisable d'instructions indispensables et d'anecdotes des plus comiques, Claude a toujours su remplir nos rencontres d'une atmosphère conviviale. Je le remercie également pour son soutien financier.

Mes remerciements vont également à mon codirecteur de recherche, M. Hugo Chapdelaine. Avec la flamme pour les mathématiques qu'on lui connaît, il avait toujours une idée à me faire part. Nos discussions ont été des plus enrichissantes et passionnantes. Je tiens de plus à lui faire part de ma gratitude pour sa contribution financière.

Je voudrais aussi remercier mes parents, Andrée et Roma, pour m'avoir encouragé et soutenu durant tant d'années. Je suis très reconnaissant à leur égard et je ne pourrais oublier tout ce qu'ils ont fait pour moi durant tout mon cheminement académique. J'adresse un remerciement tout spécial à Guillaume, qui m'a épaulé avec ses innombrables conseils de grand frère. Finalement, j'envoie des remerciements distingués pour ma copine Maryse, qui a été mon pilier. Son amour et toute la confiance qu'elle a eue en moi m'ont permis de surmonter tous les obstacles que j'ai rencontrés.

Pour terminer, je désire remercier le Département de mathématiques et de statistique de l'Université Laval pour m'avoir aidé à financer cette maîtrise et, ultimement, ce mémoire.

Avant-propos

Les deux premiers chapitres de ce mémoire ont été publiés sans coauteur dans le troisième volume des Cahiers de Mathématique de l'Université de Sherbrooke. Seuls le formatage et les introductions de ces deux chapitres ont été modifiés.

Introduction

Avant d'entrer dans le coeur du sujet, nous rappellerons le théorème fondamental de la théorie de Galois. Ce résultat sera illustré avec une extension de corps de degré 24 sur les rationnels, soit le corps $\mathbb{Q}(\omega, \theta, \xi)$ où

$$\omega = \sqrt[6]{M}, \quad \zeta = \frac{1}{2}(1+\theta), \quad \theta = \sqrt{-3}, \quad \xi = \sqrt{m},$$

avec M et m deux entiers copremiers > 1 sans facteur carré et ζ une sixième racine primitive de l'unité. Cet exemple présentera de façon exhaustive tous les calculs menant au groupe de Galois en question, $D_6 \times C_2$, où D_6 est le groupe diédral d'ordre 12 et $C_2 = \mathbb{Z}/2\mathbb{Z}$. Nous décrirons les automorphismes qui le composent tout en donnant sa table de Cayley. Nous déterminerons la liste de tous les 54 sous-groupes de $D_6 \times C_2$ pour ensuite identifier la liste des 54 sous-corps de l'extension $\mathbb{Q}(\omega, \theta, \xi)/\mathbb{Q}$. Finalement, pour bien visualiser la bijection issue du théorème fondamental de la théorie de Galois, nous dresserons l'imposant diagramme de Hasse des relations groupes–sous-groupes, identiquement corps–sous-corps, de cette liste.

Une fois la table mise, nous allons passer au repas principal : la détermination du groupe de Galois d'un polynôme de degré n, en particulier lorsque $n = 5, 6, 7$.

En premier lieu, nous commencerons par exposer une condition suffisante pour construire un polynôme ayant S_n comme groupe de Galois. Ensuite viendra le temps d'exhiber une méthode dite probabiliste qui donne très rapidement, et avec une bonne précision, le groupe de Galois d'un polynôme donné. Cette méthode consiste à factoriser le polynôme réduit modulo p pour un bon nombre de premiers p qui ne sont pas facteurs du discriminant du polynôme en question. Nous pourrons ensuite conclure de quel groupe de Galois il s'agit à l'aide d'un corollaire du théorème de densité de Tchebotariov. Ce résultat lie la fréquence de chaque type de cycles de décomposition du groupe recherché à la distribution des degrés de facteurs irréductibles du polynôme modulo p. En guise de complément et dans le but d'aider à mieux visualiser les concepts présentés, la théorie sera parsemée d'exemples détaillés.

Le prochain chapitre aura pour but de présenter une méthode exacte, pensée par L. Soicher et améliorée par H. Cohen, pour le calcul du groupe de Galois d'un polynôme. Comme chaque degré fait intervenir son propre algorithme, nous n'investiguerons que les degrés 5, 6 et 7.

L'astuce réside dans la construction d'un polynôme dit résolvant à partir d'un polynôme à plusieurs inconnues. Cette méthode requiert également la connaissance du treillis des sous-groupes transitifs de S_n. Il s'agira d'appliquer un puissant résultat qui lie les deux notions. Dans le cas du cinquième degré, qui ne comporte que 5 groupes transitifs (à conjugaison près), la démarche sera assez simple : le treillis sera séparé judicieusement grâce à certaines hypothèses sur le discriminant du polynôme de départ et grâce à l'origine des racines de la résolvante. Ce sera plutôt pour les degrés 6 et 7, qui comportent respectivement 16 et 7 groupes transitifs (à conjugaison près), que la proposition sera utilisée à son plein potentiel. En effet, nous aurons à comparer la liste des degrés des facteurs irréductibles de la résolvante à la liste des longueurs d'orbites des actions de chacun des possibles groupes de Galois. Cette comparaison aura pour effet de subdiviser le diagramme en petits amas de groupes ; nous serons ainsi en mesure de déterminer le groupe de Galois approprié. Chaque démarche sera accompagnée d'un algorithme écrit en pseudo-code pour faciliter la compréhension.

Dans le dernier chapitre, nous nous concentrerons sur la notion d'invariant primitif qui est utile tant dans la théorie de Galois que dans d'autres domaines. Dans notre cas, les invariants nous serviront à produire les résolvantes déjà mentionnées. Un G-invariant primitif est un polynôme F à n variables qui est stabilisé par l'action d'un sous-groupe G de permutations de S_n, c'est-à-dire

$$\sigma.F = F,$$

pour tout σ dans G. Une permutation agit sur un polynôme en permutant les indices de ses n inconnues :

$$\sigma.F(X_1, \ldots, X_n) = F\left(X_{\sigma(1)}, \ldots, X_{\sigma(n)}\right),$$

où σ est une permutation quelconque du groupe symétrique sur n éléments. En d'autres mots, un polynôme F est un G-invariant primitif si $G = Stab(F, S_n)$. Le terme *primitif* signifie que les permutations du stabilisateur proviennent de S_n. La première partie de cette section couvrira brièvement une intuition utilisée dans un chapitre précédent pour déterminer un tel invariant de façon simple. Nous verrons que cette méthode ne fonctionne pas toujours, mais qu'elle se rapproche d'une démarche dite naïve développée par R.L. Wilson. Cette dernière porte ce nom, car elle est très peu optimale en termes de temps d'exécution, bien qu'elle donne un invariant primitif à tout coup. Finalement, nous aborderons un algorithme conçu par I. Abdeljaouad, basé sur les travaux de K. Girstmair. Sa procédure nous donne, de façon beaucoup plus performante, la liste de tous les invariants de degré minimal qui sont stabilisés par un sous-groupe de S_n donné en passant par la notion de système des représentants des orbites d'un groupe et par la notion d'ensemble essentiel d'un ensemble de monômes.

Chapitre 1

Théorème fondamental de la théorie de Galois

La théorie de Galois est très utile dans plusieurs sphères des mathématiques telles que l'arithmétique ainsi que l'algèbre. Le théorème fondamental de cette théorie est inévitable lorsque vient le moment de faire l'éventail des sous-corps d'une extension donnée de $\mathbb{Q}$. En effet, elle permet de passer d'un problème *a priori* continu à un problème discret : celui des sous-groupes d'un groupe. Ce changement transforme la chasse aux sous-corps en une chasse aux sous-groupes.

Le but de ce chapitre est de faire un simple rappel du théorème fondamental avant d'entrer dans le coeur du sujet [DF04].

1.1 Théorème fondamental

Avant d'énoncer le théorème fondamental de la théorie de Galois, quelques rappels seront utiles. Nous disons qu'un automorphisme σ d'un corps K *fixe* un élément $\alpha \in K$ si $\sigma(\alpha) = \alpha$. Si un tel automorphisme fixe tous les éléments d'un sous-corps F de K, nous disons simplement que σ *fixe* F. Inversement, étant donné un sous-groupe H du groupe $Aut(K)$ des automorphismes de K, le sous-corps de K fixé par tous les automorphismes de ce sous-groupe est dit le corps *laissé fixe* par H. Dans le cas où nous avons une extension de corps K/F de degré fini, nous notons alors par $Aut(K/F)$ le groupe des automorphismes de K qui fixent F. Cette extension est dite *galoisienne* si son degré $[K : F]$ est fini et égal au cardinal de $Aut(K/F)$. De plus, en supposant l'extension K/F galoisienne, nous identifions $Aut(K/F)$ comme étant le *groupe de Galois* de K/F et nous le notons $Gal(K/F)$.

Cette petite mise en contexte nous amène à énoncer le résultat fondamental suivant.

Théorème 1.1.1 (Théorème fondamental de la théorie de Galois). *Soit K/F une extension galoisienne et soit $G = Gal(K/F)$. Alors il y a une bijection entre les ensembles suivants :*

$$\{\textit{sous-corps } E \textit{ de } K \textit{ contenant } F\} \longleftrightarrow \{\textit{sous-groupes } H \textit{ de } G\}$$

$$\begin{array}{ccc} K & \longleftrightarrow & \mathbb{I} \\ | & & | \\ E & \longleftrightarrow & H \\ | & & | \\ F & \longleftrightarrow & G \end{array}$$

avec $\mathbb{I} = \{id\}$ où id est l'élément neutre de G. Cette bijection est donnée par les correspondances

$$E \longmapsto \{\textit{les éléments de } G \textit{ qui laissent } E \textit{ fixe}\},$$

$$\{\textit{les éléments du corps laissé fixe par } H\} \longmapsfrom H,$$

qui sont inverses l'une de l'autre. De plus, nous avons les résultats suivants :

(1) Si les corps E_1 et E_2 correspondent respectivement aux groupes H_1 et H_2, alors $E_1 \subseteq E_2$ si et seulement si $H_2 \leq H_1$.

(2) Le degré $[K : E]$ de l'extension K/E est égal à la cardinalité du groupe H associé à E. En d'autres termes, $[K : E] = |H|$. De plus, le degré de l'extension E/F est égal à l'indice du sous-groupe H dans G. En d'autres termes, $[E : F] = [G : H]$:

$$\begin{array}{ll} K & \\ | & \} \, |H| \\ E & \\ | & \} \, |G : H| \\ F. & \end{array}$$

(3) L'extension K/E est toujours galoisienne avec $H = Gal(K/E)$ comme groupe de Galois.

(4) L'extension E/F est galoisienne si et seulement si H est un sous-groupe distingué de G. Si c'est le cas, alors le groupe de Galois $Gal(E/F)$ est isomorphe au quotient de groupes G/H.

(5) Si les corps E_1 et E_2 correspondent respectivement aux groupes H_1 et H_2, alors l'intersection $E_1 \cap E_2$ correspond au groupe $\langle H_1, H_2 \rangle$ engendré par H_1 et H_2. De plus, le corps composé E_1E_2 est associé à l'intersection $H_1 \cap H_2$.

Chapitre 2

Illustration du théorème fondamental

Le chapitre 1 rappelle brièvement le théorème fondamental de la théorie de Galois. Maintenant que le résultat est énoncé, nous pouvons détailler une application directe et non triviale pour bien illustrer toute la puissance de cette théorie.

Il s'agit d'étudier la classe d'extensions de la forme $\mathbb{Q}(\omega, \theta, \xi)/\mathbb{Q}$ où

$$\omega = \sqrt[6]{M}, \quad \zeta = \frac{1}{2}(1+\theta), \quad \theta = \sqrt{-3}, \quad \xi = \sqrt{m},$$

avec M et m deux entiers copremiers > 1 sans facteur carré et ζ une sixième racine primitive de l'unité.

Dès maintenant, nous pouvons remarquer que $\mathbb{Q}(\omega, \theta, \xi)$ est une extension de degré 24 sur $\mathbb{Q}$. En effet,

$$[\mathbb{Q}(\omega, \theta, \xi) : \mathbb{Q}] = [\mathbb{Q}(\omega, \theta, \xi) : \mathbb{Q}(\theta, \xi)] \times [\mathbb{Q}(\theta, \xi) : \mathbb{Q}(\xi)] \times [\mathbb{Q}(\xi) : \mathbb{Q}] = 6 \times 2 \times 2 = 24.$$

Nous verrons dans les sections qui suivent que le diagramme de Hasse des sous-corps de $\mathbb{Q}(\omega, \theta, \xi)$ a l'allure de la figure 2.1.

2.1 En quête des sous-corps de $\mathbb{Q}(\omega, \theta, \xi)/\mathbb{Q}$

Par l'intermédiaire du théorème fondamental de la théorie de Galois, nous trouverons la liste des sous-corps de l'extension galoisienne $K/\mathbb{Q}$ où $K = \mathbb{Q}(\omega, \theta, \xi)$. En premier lieu, sachant que le degré de l'extension est 24, nous définirons les automorphismes de K qui forment le groupe de Galois de $K/\mathbb{Q}$. Finalement, nous expliciterons tous les sous-groupes de $G = Gal(K/\mathbb{Q})$ ainsi que tous les sous-corps laissés fixes par ces derniers.

2.1.1 Automorphismes du groupe de Galois

Comme mentionné, l'extension galoisienne est de degré 24. Nous sommes donc à la recherche d'un groupe d'automorphismes ayant ce même nombre d'éléments. La table 2.1 explicite les

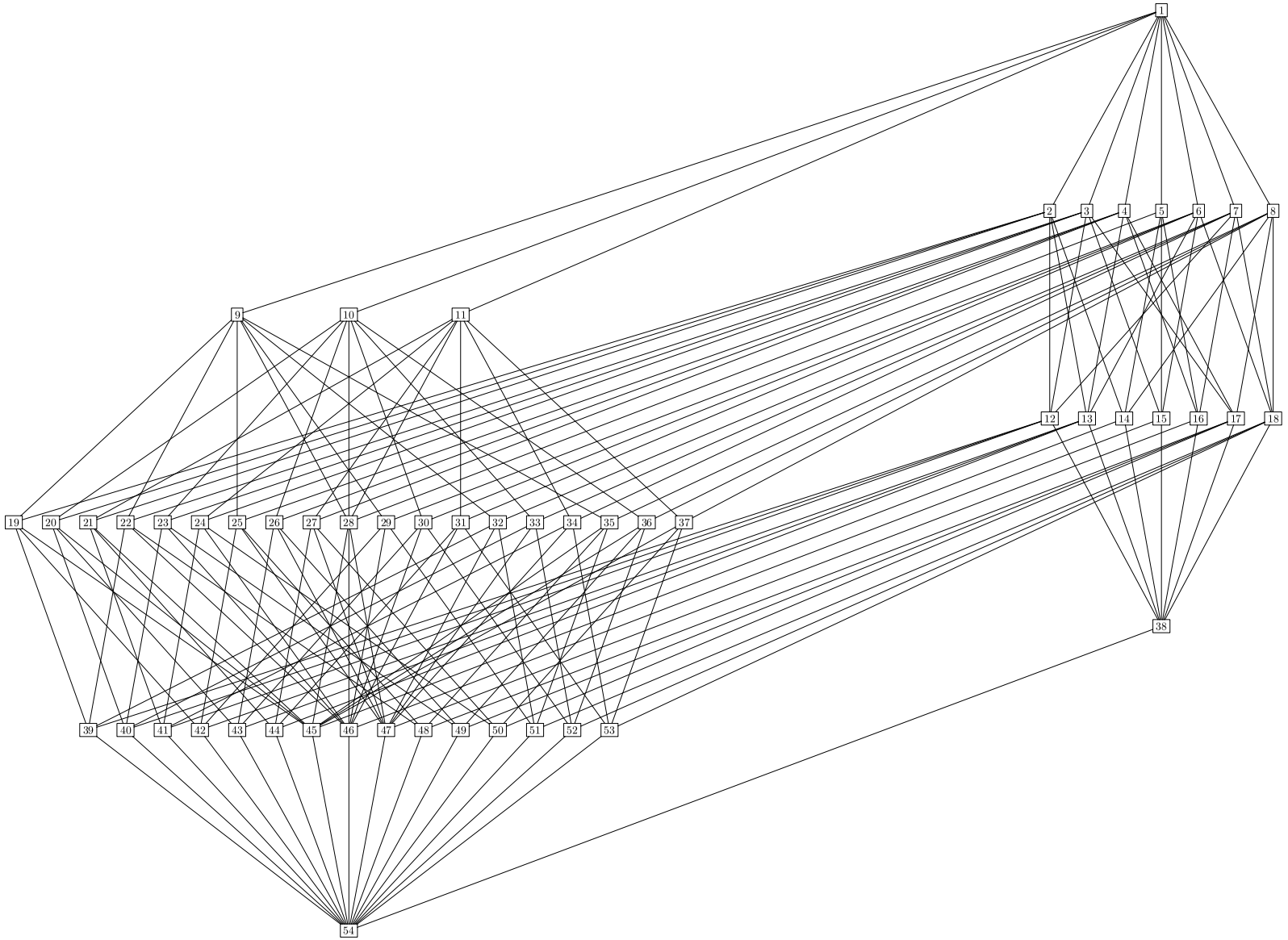


FIGURE 2.1: Diagramme de Hasse des sous-groupes de G et des sous-corps de K (en inversant l'ordre)

trois générateurs de $Gal(K/\mathbb{Q})$ ainsi que leurs effets sur certains éléments clefs du corps K. Remarquons que $\omega\zeta^2 = \sigma(\omega\zeta) = \sigma(\omega)\sigma(\zeta) = \omega\zeta \cdot \sigma(\zeta)$ de sorte que $\sigma(\zeta) = \zeta$. De plus, $\tau(\zeta) = \tau(\frac{1}{2}(1+\theta)) = \frac{1}{2}(1-\theta) = -\left[\frac{1}{2}(1+\theta)\right]^2 = -\zeta^2$.

	ω	$\omega\zeta$	$\omega\zeta^2$	$-\omega$	$-\omega\zeta$	$-\omega\zeta^2$	θ	ξ	ζ
σ	$\omega\zeta$	$\omega\zeta^2$	$-\omega$	$-\omega\zeta$	$-\omega\zeta^2$	ω	θ	ξ	ζ
τ	ω	$-\omega\zeta^2$	$-\omega\zeta$	$-\omega$	$\omega\zeta^2$	$\omega\zeta$	$-\theta$	ξ	$-\zeta^2$
ρ	ω	$\omega\zeta$	$\omega\zeta^2$	$-\omega$	$-\omega\zeta$	$-\omega\zeta^2$	θ	$-\xi$	ζ

TABLE 2.1: Table des générateurs σ, τ et ρ de G et leurs effets

Montrons que l'ordre du premier automorphisme σ est 6 et que $\tau\sigma^5 = \sigma\tau$. En effet,

$$\sigma^6(\omega) = \sigma^5(\omega\zeta) = \sigma^4(\omega\zeta^2) = \sigma^3(-\omega) = -\sigma^2(\omega\zeta) = -\sigma(\omega\zeta^2) = w, \sigma^6(\theta) = \theta \text{ et } \sigma^6(\xi) = \xi,$$

$$\tau\sigma^5(\omega) = \tau\sigma^4(\omega\zeta) = \tau\sigma^3(\omega\zeta^2) = \tau\sigma^2(-\omega) = -\tau\sigma(\omega\zeta) = \omega\zeta = \sigma\tau(\omega),$$

$$\tau\sigma^5(\theta) = \tau(\theta) = -\theta = \sigma(-\theta) = \sigma\tau(\theta) \quad \text{et} \quad \tau\sigma^5(\xi) = \xi = \sigma\tau(\xi).$$

Les deux derniers automorphismes τ et ρ sont en fait d'ordre 2. Nous obtenons donc que le groupe de Galois $G = Gal(K/F) = \langle\sigma, \tau, \rho\rangle$ est isomorphe à $D_6 \times C_2$, où D_6 est le groupe diédral d'ordre 12 et C_2 est le groupe cyclique du deuxième ordre. La table de Cayley pour G est représentée à l'annexe A.

2.1.2 Sous-groupes du groupe de Galois

En vertu du théorème de Lagrange, nous savons que les cardinalités des sous-groupes de G sont des diviseurs de 24. La liste de tous les sous-groupes se trouve dans la colonne appropriée du tableau de la page 10. Selon Neubüser [Neu67], il existe sept groupes de cardinalité 12, trois de cardinalité 8, sept de cardinalité 6, dix-neuf de cardinalité 4, un seul de cardinalité 3 et finalement quinze de cardinalité 2, pour un total de 54 sous-groupes, si nous comptons le groupe lui-même $G = D_6 \times C_2$ et le sous-groupe trivial $\mathbb{I}$.

2.1.3 Liste des sous-corps

Le cinquième résultat du théorème fondamental donne une méthode efficace pour trouver tous les sous-corps à partir des sous-groupes. L'idée est de commencer avec tous les groupes engendrés par un seul élément (il y en a 18, si nous ignorons le groupe trivial) et de déterminer le sous-corps associé à chacun. Pour ce faire, il faut tout d'abord appliquer l'automorphisme générateur à un élément typique de K et nous vérifions quels termes sont fixés.

Par exemple, trouvons le sous-corps associé au groupe $\langle\tau\sigma^4\rangle$. Un élément typique z de K s'écrit

$$z = \qquad a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4 + a_5\omega^5$$

$$
\begin{aligned}
&+ b_0\theta + b_1\omega\theta + b_2\omega^2\theta + b_3\omega^3\theta + b_4\omega^4\theta + b_5\omega^5\theta \\
&+ c_0\xi + c_1\omega\xi + c_2\omega^2\xi + c_3\omega^3\xi + c_4\omega^4\xi + c_5\omega^5\xi \\
&+ d_0\theta\xi + d_1\omega\theta\xi + d_2\omega^2\theta\xi + d_3\omega^3\theta\xi + d_4\omega^4\theta\xi + d_5\omega^5\theta\xi.
\end{aligned}
$$

Par la suite, nous appliquons l'automorphisme $\tau\sigma^4$ sur z :

$$
\begin{aligned}
\tau\sigma^4(z) = \quad & a_0 - \frac{a_1}{2}\omega(1-\theta) + \frac{a_2}{4}\omega^2(1-\theta)^2 - \frac{a_3}{8}\omega^3(1-\theta)^3 + \frac{a_4}{16}\omega^4(1-\theta)^4 \\
& - \frac{a_5}{32}\omega^5(1-\theta)^5 - b_0\theta + \frac{b_1}{2}\omega(1-\theta)\theta - \frac{b_2}{4}\omega^2(1-\theta)^2\theta \\
& + \frac{b_3}{8}\omega^3(1-\theta)^3\theta - \frac{b_4}{16}\omega^4(1-\theta)^4\theta + \frac{b_5}{32}\omega^5(1-\theta)^5\theta + c_0\theta \\
& - \frac{c_1}{2}\omega(1-\theta)\xi + \frac{c_2}{4}\omega^2(1-\theta)^2\xi - \frac{c_3}{8}\omega^3(1-\theta)^3\xi + \frac{c_4}{16}\omega^4(1-\theta)^4\xi \\
& - \frac{c_5}{32}\omega^5(1-\theta)^5\xi - d_0\theta\xi + \frac{d_1}{2}\omega(1-\theta)\theta\xi - \frac{d_2}{4}\omega^2(1-\theta)^2\theta\xi \\
& + \frac{d_3}{8}\omega^3(1-\theta)^3\theta\xi - \frac{d_4}{16}\omega^4(1-\theta)^4\theta\xi + \frac{d_5}{32}\omega^5(1-\theta)^5\theta\xi \\
= \quad & a_0 - \frac{a_1}{2}\omega(1-\theta) - \frac{a_2}{2}\omega^2(1+\theta) + a_3\omega^3 - \frac{a_4}{2}\omega^4(1-\theta) - \frac{a_5}{2}\omega^5(1+\theta) \\
& - b_0\theta + \frac{b_1}{2}\omega(1-\theta)\theta + \frac{b_2}{2}\omega^2(1+\theta)\theta - b_3\omega^3\theta + \frac{b_4}{2}\omega^4(1-\theta)\theta \\
& + \frac{b_5}{2}\omega^5(1+\theta)\theta + c_0 - \frac{c_1}{2}\omega(1-\theta)\xi - \frac{c_2}{2}\omega^2(1+\theta)\xi + c_3\omega^3\xi \\
& - \frac{c_4}{2}\omega^4(1-\theta)\xi - \frac{c_5}{2}\omega^5(1+\theta)\xi - d_0\theta\xi + \frac{d_1}{2}\omega(1-\theta)\theta\xi \\
& + \frac{d_2}{2}\omega^2(1+\theta)\theta\xi - d_3\omega^3\theta\xi + \frac{d_4}{2}\omega^4(1-\theta)\theta\xi + \frac{d_5}{2}\omega^5(1+\theta)\theta\xi \\
= \quad & a_0 + \left(-\frac{a_1}{2} + \frac{3b_1}{2}\right)\omega + \left(-\frac{a_2}{2} - \frac{3b_2}{2}\right)\omega^2 + a_3\omega^3 \\
& + \left(-\frac{a_4}{2} + \frac{3b_4}{2}\right)\omega^4 + \left(-\frac{a_5}{2} - \frac{3b_5}{2}\right)\omega^5 - b_0\theta + \left(\frac{a_1}{2} + \frac{b_1}{2}\right)\omega\theta \\
& + \left(-\frac{a_2}{2} + \frac{b_2}{2}\right)\omega^2\theta - b_3\omega^3\theta + \left(\frac{a_4}{2} + \frac{b_4}{2}\right)\omega^4\theta + \left(-\frac{a_5}{2} + \frac{b_5}{2}\right)\omega^5\theta \\
& + c_0\xi + \left(-\frac{c_1}{2} + \frac{3d_1}{2}\right)\omega\xi + \left(-\frac{c_2}{2} - \frac{3d_2}{2}\right)\omega^2\xi + c_3\omega^3\xi \\
& + \left(-\frac{c_4}{2} + \frac{3d_4}{2}\right)\omega^4\xi + \left(-\frac{c_5}{2} - \frac{3d_5}{2}\right)\omega^5\xi - d_0\theta\xi + \left(\frac{c_1}{2} + \frac{d_1}{2}\right)\omega\theta\xi \\
& + \left(-\frac{c_2}{2} + \frac{d_2}{2}\right)\omega^2\theta\xi - d_3\omega^3\theta\xi + \left(\frac{c_4}{2} + \frac{d_4}{2}\right)\omega^4\theta\xi + \left(-\frac{c_5}{2} + \frac{d_5}{2}\right)\omega^5\theta\xi.
\end{aligned}
$$

Or, comme nous cherchons le corps laissé fixe par $\langle\tau\sigma^4\rangle$, nous avons $\tau\sigma^4(z) = z$, ce qui entraîne que $b_0 = 0$, $b_1 = a_1$, $b_2 = -a_2$, $b_3 = 0$, $b_4 = a_4$, $b_5 = -a_5$, $d_0 = 0$, $d_1 = c_1$, $d_2 = -c_2$, $d_3 = 0$, $d_4 = c_4$ et $d_5 = -c_5$. Ainsi, z se réduit à

$$
z = \quad a_0 + a_1\omega(1+\theta) + a_2\omega^2(1-\theta) + a_3\omega^3 + a_4\omega^4(1+\theta) + a_5\omega^5(1-\theta)
$$

$$
\begin{aligned}
& + c_0\xi + c_1\omega(1+\theta)\xi + c_2\omega^2(1-\theta)\xi + c_3\omega^3\xi + c_4\omega^4(1+\theta)\xi \\
& + c_5\omega^5(1-\theta)\xi \\
= \quad & a_0 + a_1\left(\omega(1+\theta)\right) + a_2'\left(\omega(1+\theta)\right)^2 + a_3'\left(\omega(1+\theta)\right)^3 + a_4'\left(\omega(1+\theta)\right)^4 \\
& + a_5'\left(\omega(1+\theta)\right)^5 + c_0\xi + c_1\left(\omega(1+\theta)\right)\xi + c_2'\left(\omega(1+\theta)\right)^2\xi \\
& + c_3'\left(\omega(1+\theta)\right)^3\xi + c_4'\left(\omega(1+\theta)\right)^4\xi + c_5'\left(\omega(1+\theta)\right)^5\xi.
\end{aligned}
$$

Nous pouvons ainsi conclure que comme z est un élément typique de $\mathbb{Q}(\omega(1+\theta),\xi)$, alors ce dernier corps est le corps laissé fixe par $\langle\tau\sigma^4\rangle$.

Après avoir trouvé tous les corps laissés fixes par les groupes cycliques, il ne reste qu'à tenir compte des sous-groupes engendrés par deux automorphismes ou plus. En vertu du cinquième résultat du théorème fondamental de la théorie de Galois, il suffit ensuite de prendre l'intersection des sous-corps qui correspondent aux groupes monogènes qui le composent.

Par exemple, le sous-groupe $\langle\tau\rangle$ correspond au sous-corps $\mathbb{Q}(\omega,\xi)$. En effet, $\tau(\omega)=\omega$, $\tau(\xi)=\xi$ et $|\langle\tau\rangle| = [K:\mathbb{Q}(\omega,\xi)] = 2$, alors le deuxième résultat du théorème nous assure que $\langle\tau\rangle$ ne fixe pas un corps plus grand que $\mathbb{Q}(\omega,\xi)$. De même, le sous-groupe $\langle\sigma\rangle$ est associé à $\mathbb{Q}(\theta,\xi)$, car $\sigma(\theta)=\theta$, $\sigma(\xi)=\xi$ et $\langle\sigma\rangle$ est d'ordre 6, ce qui correspond au degré de $K/\mathbb{Q}(\theta,\xi)$. Nous pouvons donc aisément déduire que le sous-groupe $\langle\tau,\sigma\rangle$ correspond à l'intersection $\mathbb{Q}(\omega,\xi)\cap\mathbb{Q}(\theta,\xi) = \mathbb{Q}(\xi)$.

Il existe des raccourcis pour déterminer les corps laissés fixes par les sous-groupes de G, mais cette technique requiert une bonne intuition et une certaine expérience. À partir d'un sous-groupe donné H, il s'agit de déduire tout d'abord un bon candidat pour le corps E, puis de vérifier que les générateurs de H le fixent bel et bien, mais qu'ils ne fixent aucun corps plus grand en comparant l'ordre de H avec le degré de l'extension K/E.

Pour illustrer cette méthode, considérons le groupe $H_{11} = \langle\sigma^3,\tau\sigma,\rho\rangle$. Notre flair nous amène à choisir $E_{11} = \mathbb{Q}(\omega^2(1-\theta))$ comme corps laissé fixe. En premier, nous vérifions les effets des générateurs sur E_{11} :

$$
\begin{aligned}
\sigma^3(\omega^2(1-\theta)) &= \left(\sigma^3(\omega)\right)^2\cdot\sigma^3(1-\theta) = (-\omega)^2(1-\theta) = \omega^2(1-\theta), \\
\tau\sigma(\omega^2(1-\theta)) &= \left(\tau\sigma(\omega)\right)^2\cdot\tau\sigma(1-\theta) = \left(\tau(\omega\zeta)\right)^2(1+\theta) = \frac{1}{4}\omega^2(1-\theta)^2(1+\theta) = \omega^2(1-\theta), \\
\rho(\omega^2(1-\theta)) &= \omega^2(1-\theta).
\end{aligned}
$$

Les trois générateurs de H_{11} fixent donc E_{11}. Finalement, comme l'ordre de H_{11} vaut 8 et que le degré de K/E_{11} donne également 8, le candidat est le bon.

À l'aide de la table 2.2, nous pouvons illustrer les relations groupe–sous-groupe ou inversement corps–sous-corps. De plus, le diagramme de Hasse que nous avons exhibé nous donne une vision globale des sous-corps reproduisant le treillis des sous-groupes.

n	Sous-groupes	Sous-corps
1	$G = \langle \sigma, \tau, \rho \rangle$	$F = \mathbb{Q}$
2	$H_2 = \langle \rho\sigma, \tau \rangle$	$E_2 = \mathbb{Q}(\omega^3\xi)$
3	$H_3 = \langle \sigma, \tau \rangle$	$E_3 = \mathbb{Q}(\xi)$
4	$H_4 = \langle \sigma^2, \tau\sigma, \rho \rangle$	$E_4 = \mathbb{Q}(\omega^3\theta)$
5	$H_5 = \langle \sigma, \rho \rangle$	$E_5 = \mathbb{Q}(\theta)$
6	$H_6 = \langle \sigma, \rho\tau \rangle$	$E_6 = \mathbb{Q}(\theta\xi)$
7	$H_7 = \langle \sigma^2, \tau, \rho \rangle$	$E_7 = \mathbb{Q}(\omega^3)$
8	$H_8 = \langle \rho\sigma, \rho\tau \rangle$	$E_8 = \mathbb{Q}(\omega^3\theta\xi)$
9	$H_9 = \langle \sigma^3, \tau\sigma^2, \rho \rangle$	$E_9 = \mathbb{Q}(\omega^2(1+\theta))$
10	$H_{10} = \langle \sigma^3, \tau, \rho \rangle$	$E_{10} = \mathbb{Q}(\omega^2)$
11	$H_{11} = \langle \sigma^3, \tau\sigma, \rho \rangle$	$E_{11} = \mathbb{Q}(\omega^2(1-\theta))$
12	$H_{12} = \langle \sigma^2, \tau \rangle$	$E_{12} = \mathbb{Q}(\omega^3, \xi)$
13	$H_{13} = \langle \sigma^2, \rho\tau\sigma \rangle$	$E_{13} = \mathbb{Q}(\omega^3\xi, \theta\xi)$
14	$H_{14} = \langle \rho\sigma \rangle$	$E_{14} = \mathbb{Q}(\omega^3\xi, \theta)$
15	$H_{15} = \langle \sigma \rangle$	$E_{15} = \mathbb{Q}(\theta, \xi)$
16	$H_{16} = \langle \sigma^2, \rho \rangle$	$E_{16} = \mathbb{Q}(\omega^3, \theta)$
17	$H_{17} = \langle \sigma^2, \tau\sigma \rangle$	$E_{17} = \mathbb{Q}(\omega^3\theta, \xi)$
18	$H_{18} = \langle \sigma^2, \rho\tau \rangle$	$E_{18} = \mathbb{Q}(\omega^3, \theta\xi)$
19	$H_{19} = \langle \rho\sigma^3, \tau\sigma^2 \rangle$	$E_{19} = \mathbb{Q}(\omega(1-\theta)\xi)$
20	$H_{20} = \langle \rho\sigma^3, \tau \rangle$	$E_{20} = \mathbb{Q}(\omega\xi)$
21	$H_{21} = \langle \rho\sigma^3, \tau\sigma^4 \rangle$	$E_{21} = \mathbb{Q}(\omega(1+\theta)\xi)$
22	$H_{22} = \langle \sigma^3, \tau\sigma^2 \rangle$	$E_{22} = \mathbb{Q}(\omega^2(1+\theta), \xi)$
23	$H_{23} = \langle \sigma^3, \tau \rangle$	$E_{23} = \mathbb{Q}(\omega^2, \xi)$
24	$H_{24} = \langle \sigma^3, \tau\sigma \rangle$	$E_{24} = \mathbb{Q}(\omega^2(1-\theta), \xi)$
25	$H_{25} = \langle \tau\sigma^5, \rho \rangle$	$E_{25} = \mathbb{Q}(\omega\theta(1-\theta))$
26	$H_{26} = \langle \tau\sigma^3, \rho \rangle$	$E_{26} = \mathbb{Q}(\omega\theta)$
27	$H_{27} = \langle \tau\sigma, \rho \rangle$	$E_{27} = \mathbb{Q}(\omega\theta(1+\theta))$
28	$H_{28} = \langle \sigma^3, \rho \rangle$	$E_{28} = \mathbb{Q}(\omega^2, \theta)$
29	$H_{29} = \langle \sigma^3, \rho\tau\sigma^2 \rangle$	$E_{29} = \mathbb{Q}(\omega^2(1+\theta), \theta\xi)$
30	$H_{30} = \langle \sigma^3, \rho\tau \rangle$	$E_{30} = \mathbb{Q}(\omega^2, \theta\xi)$
31	$H_{31} = \langle \sigma^3, \rho\tau\sigma \rangle$	$E_{31} = \mathbb{Q}(\omega^2(1-\theta), \theta\xi)$
32	$H_{32} = \langle \tau\sigma^2, \rho \rangle$	$E_{32} = \mathbb{Q}(\omega(1-\theta))$
33	$H_{33} = \langle \tau, \rho \rangle$	$E_{33} = \mathbb{Q}(\omega)$
34	$H_{34} = \langle \tau\sigma^4, \rho \rangle$	$E_{34} = \mathbb{Q}(\omega(1+\theta))$
35	$H_{35} = \langle \rho\sigma^3, \rho\tau\sigma^2 \rangle$	$E_{35} = \mathbb{Q}(\omega\theta(1-\theta)\xi)$
36	$H_{36} = \langle \rho\sigma^3, \rho\tau \rangle$	$E_{36} = \mathbb{Q}(\omega\theta\xi)$
37	$H_{37} = \langle \rho\sigma^3, \tau\sigma \rangle$	$E_{37} = \mathbb{Q}(\omega\theta(1+\theta)\xi)$
38	$H_{38} = \langle \sigma^2 \rangle$	$E_{38} = \mathbb{Q}(\omega^3, \theta, \xi)$
39	$H_{39} = \langle \tau\sigma^2 \rangle$	$E_{39} = \mathbb{Q}(\omega(1-\theta), \xi)$
40	$H_{40} = \langle \tau \rangle$	$E_{40} = \mathbb{Q}(\omega, \xi)$
41	$H_{41} = \langle \tau\sigma^4 \rangle$	$E_{41} = \mathbb{Q}(\omega(1+\theta), \xi)$
42	$H_{42} = \langle \rho\tau\sigma^5 \rangle$	$E_{42} = \mathbb{Q}(\omega\theta(1-\theta), \theta\xi)$
43	$H_{43} = \langle \rho\tau\sigma^3 \rangle$	$E_{43} = \mathbb{Q}(\omega\theta, \theta\xi)$
44	$H_{44} = \langle \rho\tau\sigma \rangle$	$E_{44} = \mathbb{Q}(\omega\theta(1+\theta), \theta\xi)$
45	$H_{45} = \langle \rho\sigma^3 \rangle$	$E_{45} = \mathbb{Q}(\omega\xi, \theta)$
46	$H_{46} = \langle \sigma^3 \rangle$	$E_{46} = \mathbb{Q}(\omega^2, \theta, \xi)$
47	$H_{47} = \langle \rho \rangle$	$E_{47} = \mathbb{Q}(\omega, \theta)$
48	$H_{48} = \langle \tau\sigma^5 \rangle$	$E_{48} = \mathbb{Q}(\omega\theta(1-\theta), \xi)$
49	$H_{49} = \langle \tau\sigma^3 \rangle$	$E_{49} = \mathbb{Q}(\omega\theta, \xi)$
50	$H_{50} = \langle \tau\sigma \rangle$	$E_{50} = \mathbb{Q}(\omega\theta(1+\theta), \xi)$
51	$H_{51} = \langle \rho\tau\sigma^2 \rangle$	$E_{51} = \mathbb{Q}(\omega(1-\theta), \theta\xi)$
52	$H_{52} = \langle \rho\tau \rangle$	$E_{52} = \mathbb{Q}(\omega, \theta\xi)$
53	$H_{53} = \langle \rho\tau\sigma^4 \rangle$	$E_{53} = \mathbb{Q}(\omega(1+\theta), \theta\xi)$
54	$\mathbb{I}$	$K = \mathbb{Q}(\omega, \theta, \xi)$

TABLE 2.2: Liste des sous-groupes et des sous-corps de $\mathbb{Q}(\omega, \theta, \xi)$

Chapitre 3

Réduction modulo p

Dans cette section, nous nous intéressons au calcul du groupe de Galois d'un polynôme $f(x)$ sur $\mathbb{Q}$. Comme notre objectif est de déterminer le groupe de Galois du polynôme, nous pouvons supposer que $f(x)$ a tous ses coefficients dans $\mathbb{Z}$. Ainsi le discriminant de $f(x)$, que nous notons D_f, est un entier non nul. Pour un nombre premier p, considérons le polynôme réduit $\bar{f}(x) \in \mathbb{F}_p[x]$, qui est nul autre que $f(x)$ avec tous ses coefficients modulo p.

Si p divise le discriminant D_f de $f(x)$, alors le discriminant $D_{\bar{f}}$ de $\bar{f}(x)$ est nul dans $\mathbb{F}_p$. Le polynôme réduit $\bar{f}(x)$ n'est donc pas séparable. Si, au contraire, p ne divise pas D_f, alors nécessairement $\bar{f}(x)$ est séparable sur $\mathbb{F}_p$ et donc ce dernier peut s'exprimer comme le produit de polynômes irréductibles de $\mathbb{F}_p[x]$:

$$\bar{f}(x) = \bar{f}_1(x) \cdot \bar{f}_2(x) \cdot \bar{f}_3(x) \cdots \bar{f}_k(x).$$

Notons $n_i = \deg \bar{f}_i(x)$, pour tout $i \in \{1, \ldots, k\}$.

Le fait de réduire le polynôme $f(x)$ sur $\mathbb{F}_p$ nous amène à énoncer le prochain théorème, qui est un résultat important de la théorie algébrique des nombres et qui a de grandes répercussions dans l'étude des extensions finies de $\mathbb{Q}$.

Théorème 3.0.1. *Pour un nombre premier p qui ne divise pas le discriminant D_f de $f(x) \in \mathbb{Z}[x]$, le groupe de Galois sur $\mathbb{F}_p$ de $\bar{f}(x) := f(x) \pmod p$ est isomorphe (en tant que groupe de permutations) à un certain sous-groupe du groupe de Galois sur $\mathbb{Q}$ de $f(x)$.*

Démonstration. Soient $\alpha_1, \ldots, \alpha_n$ les racines distinctes de $f(x)$ et soient $U_1, \ldots, U_n$ des inconnues. Avec ces racines et ces inconnues, nous formons l'équation

$$\theta = U_1\alpha_1 + U_2\alpha_2 + \cdots + U_n\alpha_n.$$

Ensuite nous construisons la fonction suivante où les permutations $\sigma \in S_n$ permutent les inconnues :

$$F = F(X, U_1, \ldots, U_n) = \prod_{\sigma \in S_n} (X - \sigma(\theta)) .$$

Comme ce produit forme une fonction symétrique sur les racines de $f(x)$, les coefficients de F peuvent s'exprimer en fonction de ceux de $f(x)$ [vdW60]. Considérons ensuite la décomposition de F en facteurs irréductibles sur $\mathbb{Q}$:

$$F(X, U_1, \ldots, U_n) = F_1(X, U_1, \ldots, U_n) \cdot F_2(X, U_1, \ldots, U_n) \cdots F_k(X, U_1, \ldots, U_n).$$

Notons que le groupe formé des permutations des inconnues qui envoient le facteur F_i sur lui-même correspond (à conjugaison près) au groupe de Galois de F [vdW60]. À partir de cette décomposition, considérons maintenant sa réduction sur $\mathbb{F}_p$

$$\bar{F} = \bar{F}_1 \cdot \bar{F}_2 \cdots \bar{F}_k.$$

Même si les facteurs initiaux $F_1, \ldots, F_k$ sont irréductibles sur $\mathbb{Q}$, rien n'assure que les facteurs réduits $\bar{F}_1, \ldots, \bar{F}_k$ soient également irréductibles sur $\mathbb{F}_p$. Soit G le groupe de Galois de $f(x)$ sur $\mathbb{Q}$ et $\bar{G}$ le groupe de Galois de $\bar{f}(x)$ sur $\mathbb{F}_p$. Si nous voyons ces groupes comme des sous-groupes de S_n et si nous supposons, sans perte de généralité, que les permutations de G envoient F_1 sur lui-même, alors ces permutations envoient également $\bar{F}_1$ sur lui-même. Les permutations des groupes conjugués de G envoient donc F_1 sur $F_2, \ldots, F_k$ et $\bar{F}_1$ sur $\bar{F}_2, \ldots, \bar{F}_k$. De façon analogique, les permutations de $\bar{G}$ envoient un facteur irréductible de $\bar{F}_1$ sur lui-même de sorte qu'elles ne peuvent pas envoyer $\bar{F}_1$ sur $\bar{F}_2, \ldots, \bar{F}_k$, et donc ne peuvent qu'envoyer $\bar{F}_1$ complètement sur lui-même. Ceci entraîne que les éléments de $\bar{G}$ se retrouvent nécessairement dans G (à conjugaison près), d'où $\bar{G} \leq G$ ce qui termine la démonstration. □

Corollaire 3.0.2. *Pour un nombre premier p qui ne divise pas D_f, le groupe de Galois de $f(x) \in \mathbb{Z}[x]$ sur $\mathbb{Q}$ possède un élément ayant $(n_1, n_2, n_3, \ldots, n_k)$ comme type de décomposition en produit de cycles, où n_i est le degré du i-ième facteur irréductible de $\bar{f}(x) \equiv f(x) \pmod{p}$.*

Démonstration. Cette démonstration découle du fait que toute extension finie de $\mathbb{F}_p$ est une extension cyclique et donc que le groupe de Galois de $\bar{f}(x)$ sur $\mathbb{F}_p$ est un groupe cyclique. Remarquons que les racines de chaque facteur irréductible $\bar{f}_i(x)$ de $\bar{f}(x)$ sont permutées entre elles lorsque qu'on leur applique les éléments du groupe de Galois de $\bar{f}(x)$. Soit σ le générateur de ce groupe.

En voyant σ comme un élément de S_n, considérons sa décomposition en produit de cycles. Comme cet élément agit transitivement sur les racines de chacun des k facteurs irréductibles de $\bar{f}(x)$, alors sa décomposition doit être le produit de k permutations distinctes. L'action de σ sur le facteur $\bar{f}_i(x)$ est un cycle de longueur n_i, car autrement les puissances de σ ne pourraient pas agir transitivement sur les racines de $\bar{f}_i(x)$. Ainsi, la décomposition en produit de cycles de σ est de type $(n_1, n_2, n_3, \ldots, n_k)$. En vertu du résultat précédent, le groupe de Galois sur $\mathbb{Q}$ de $f(x)$ contient un tel élément. Ceci achève la démonstration. □

Pour les exemples qui suivent ainsi que pour certains autres résultats, nous aurons besoin de deux propositions faciles que nous acceptons sans preuve.

Proposition 3.0.3. *Soit D_f le discriminant d'un polynôme $f(x) \in \mathbb{Z}[x]$ de degré n. Le groupe de Galois de $f(x)$ sur $\mathbb{Q}$ est contenu dans le groupe alterné A_n si et seulement si D_f est un carré parfait dans $\mathbb{Z}$.*

Proposition 3.0.4. *Si un sous-groupe transitif de S_n contient une transposition ainsi qu'un élément d'ordre $n-1$, alors ce groupe est S_n.*

Exemple 1. Considérons le polynôme $f(x) = x^5 + x^3 + 1$ de $\mathbb{Z}[x]$ et trouvons son groupe de Galois sur $\mathbb{Q}$. À l'aide du logiciel Sage, nous trouvons que son discriminant D_f est $3233 = 53 \cdot 61$ [S$^+$12]. Ainsi, dans l'optique du corollaire précédent, nous pouvons utiliser les nombres premiers 2, 3 et 5, car ils ne divisent pas D_f.

Commençons par $f_1(x) \equiv f(x) \pmod 2$. Comme $f_1(x)$ n'a pas de racine dans $\mathbb{F}_2$, alors soit le polynôme est irréductible, soit le polynôme est factorisé par $x^2 + x + 1$. Or si ce dernier cas était vrai, alors $f_1(x)$ se factoriserait également soit par $x^3 + x^2 + 1$ ou par $x^3 + x + 1$, mais une simple vérification démontre que ce n'est le cas ni pour l'un, ni pour l'autre. Ceci prouve que $f_1(x)$ est irréductible et donc que $f(x)$ l'est également. Le groupe de Galois de $f(x)$ sur $\mathbb{Q}$ est donc transitif sur toutes les racines.

Considérons la réduction $f_2(x) \equiv f(x) \pmod 3$. Remarquons que ce polynôme de $\mathbb{F}_3[x]$ se factorise en $(x+2)(x^4+x^3+2x^2+2x+2)$. Le facteur quartique n'a pas de racine dans $\mathbb{F}_3$, il est donc soit irréductible, soit le produit de deux quadratiques. Soient $g_1(x) = x^2 + ax + b \in \mathbb{F}_3[x]$ et $g_2(x) = x^2 + cx + d \in \mathbb{F}_3[x]$ deux polynômes irréductibles tels que $g_1(x) \cdot g_2(x) = x^4 + x^3 + 2x^2 + 2x + 2$. Nous en déduisons les égalités suivantes : $a + c = 1$, $d + b + ac = 2$, $ad + bc = 2$ et $bd = 2$. Sans perte de généralité, choisissons $b = 1$ et $d = 2$, ainsi les identités précédentes deviennent $a + c = 1$, $ac = 2$ et $2a + c = 2$. De la première et dernière égalité, nous déduisons que $a = 1$, ce qui mène à une contradiction avec les autres équations. Le facteur quartique est donc irréductible. Ainsi, en vertu du corollaire précédent, le groupe de Galois de $f(x)$ sur $\mathbb{Q}$ contient un cycle de longueur 4.

Finalement, tenons compte de la réduction $f_3(x) \equiv f(x) \pmod 5$. Ce polynôme se factorise en $(x^2+2x+3)(x^3+3x^2+2x+2)$. Aucun de ces facteurs n'a de racine dans $\mathbb{F}_5$, donc ils sont tous deux irréductibles. Ceci entraîne que le groupe de Galois de $f(x)$ sur $\mathbb{Q}$ contient un cycle de décomposition de type (2, 3). En mettant cet élément à la troisième puissance, nous obtenons un cycle de longueur 2. Ce groupe transitif contient donc une transposition et un cycle de longueur 4. La proposition 3.0.4 nous assure donc que $Gal(f)$ est le groupe symétrique S_5. Ceci termine l'exemple.

Exemple 2. Soit le polynôme $f(x) = x^7-3x^3+3 \in \mathbb{Z}[x]$. Son discriminant D_f est $-464313951 = -1 \cdot 3^6 \cdot 636919$ [S+12], donc nous ne pouvons pas utiliser la réduction modulo 3 pour déterminer le groupe de Galois de $f(x)$ sur $\mathbb{Q}$. Sans avoir à faire les démarches au complet comme dans l'exemple précédent, contentons-nous simplement des résultats suivants qui ont été obtenus à l'aide des logiciels Sage et PARI [The12].

La réduction $f_1(x) \equiv f(x) \pmod 2 \equiv x^7+x^3+1$ est irréductible, ce qui implique non seulement que $f(x)$ est irréductible, mais aussi que son groupe de Galois est transitif sur les 7 racines. Ensuite, considérons directement la réduction $f_2(x) \equiv f(x) \pmod{17} \equiv (x+7)(x^6+10x^5+15x^4+14x^3+x^2+10x+15)$. Le facteur de degré 6 étant irréductible, nous déduisons que le groupe de Galois recherché contient un cycle de longueur 6, selon le corollaire 3.0.2.

Finalement, le polynôme $f_3(x)$ est une version de $f(x)$ réduite dans $\mathbb{F}_{23}[x]$. Il se décompose en produits de facteurs irréductibles $(x^2+18x+5)(x^5+5x^4+20x^3+6x^2+19x+19)$, ce qui entraîne que le groupe de Galois de $f(x)$ contient un cycle de décomposition de type (2, 5). En prenant la cinquième puissance de ce cycle, nous obtenons une transposition. Le groupe de Galois de $f(x)$ sur $\mathbb{Q}$ est donc un groupe transitif qui contient un cycle de longueur 6 et une transposition ; seul le groupe symétrique S_7 répond à ces critères. Ceci achève l'exemple.

Les deux exemples précédents mettent en valeur deux polynômes ayant S_n comme groupe de Galois sur $\mathbb{Q}$. De ceux-ci nous pouvons déduire une méthode permettant de construire un polynôme $f(x)$ de degré n sur $\mathbb{Z}[x]$ ayant le groupe symétrique S_n comme groupe de Galois. La construction va comme suit.

Nous cherchons $f(x) \in \mathbb{Z}[x]$ de degré n à l'aide de trois premiers distincts arbitraires p_1, p_2, p_3. Nous construisons trois polynômes f_1, f_2, f_3 tels que :

(1) $f_1 := f \pmod{p_1}$ soit irréductible sur $\mathbb{F}_{p_1}$,

(2) $f_2 := f \pmod{p_2}$ ait une factorisation sur $\mathbb{F}_{p_2}$ de la forme :

   (a) si n est impair, $f_2 = g_1 g_2$ avec g_1, g_2 irréductibles, $\deg(g_1) = 2$ et $\deg(g_2) = n-2$,

   (b) si n est pair, $f_2 = g_1 g_2 g_3$ avec g_1, g_2, g_3 irréductibles, $\deg(g_1) = 2$, $\deg(g_2) = n-3$ et $\deg(g_3) = 1$;

(3) $f_3 := f \pmod{p_3}$ ait une factorisation sur $\mathbb{F}_{p_3}$ de la forme $f_3 = h_1 h_2$ avec h_1, h_2 irréductibles, $\deg(h_1) = 1$ et $\deg(h_2) = n - 1$.

Une fois ces f_i déterminés, il suffit de prendre $f = p_2 p_3 f_1 + p_1 p_3 f_2 + p_1 p_2 f_3$. Soit G le groupe de Galois de f. Nous pouvons ainsi déduire de (1) que f est irréductible sur $\mathbb{Q}$ et donc $G \subseteq S_n$ est transitif. Soit σ un générateur de $Gal(f_2) \subseteq G$. En vertu de (2), si n est impair, σ^{n-2} est une transposition et si n est pair, σ^{n-3} est une transposition. Dans tous les cas, G contient au moins une transposition. Finalement, de (3) nous tirons que G contient un cycle de longueur $n - 1$. La proposition 3.0.4 nous assure donc que $G = S_n$.

Il est facile de se convaincre que pour un n donné, cette construction permet de générer une infinité de polynômes ayant tous S_n comme groupe de Galois sur $\mathbb{Q}$. Ceci démontre la prochaine proposition.

Proposition 3.0.5. *Pour chaque entier positif n, il existe une infinité de polynômes $f(x)$ à coefficients entiers ayant S_n comme groupe de Galois sur $\mathbb{Q}$.*

Ainsi, nous remarquons qu'il n'est pas difficile de démontrer que le groupe de Galois d'un polynôme est S_n, ni de le construire, d'ailleurs. La difficulté survient lorsque le groupe de Galois d'un polynôme est contenu strictement dans S_n. Par exemple, si le groupe recherché est C_n, le groupe cyclique d'ordre n, la méthode utilisée dans les exemples précédents ne va que nous donner des éléments de C_n, peu importe le nombre premier avec lequel nous réduisons le polynôme original. Cependant, à moins de faire le calcul pour une infinité de nombres premiers qui ne divisent pas le discriminant du polynôme en question, rien ne démontre que le groupe de Galois est bel et bien C_n. Il existe par contre un résultat qui aide à déterminer de façon probabiliste le groupe de Galois d'un polynôme sur $\mathbb{Q}$. Il s'agit d'une conséquence directe du théorème de densité de Tchebotariov [DF04].

Définition 3.0.6. Soit T la liste non ordonnée des degrés des facteurs irréductibles d'un polynôme f. Nous disons que f se factorise en *produit de facteurs de type T*.

Définition 3.0.7. Soit σ une permutation décomposée en produit de cycles et soit T la liste non ordonnée de la longueur de chacun des cycles de σ. Nous disons que σ a un *cycle de décomposition de type T*.

Théorème 3.0.8 (Théorème de densité de Tchebotariov)**.** *Soit $G \subseteq S_n$ le groupe de Galois d'ordre N sur $\mathbb{Q}$ de $f(x) \in \mathbb{Z}[x]$. La densité de nombres premiers p pour lesquels $f(x)$ modulo p se factorise en produit de facteurs de type T est exactement $d_T = n_T/N$ où n_T est le nombre d'éléments de G dont le cycle de décomposition est de type T.*

Ainsi, si nous avions la factorisation de $f(x) \in \mathbb{Z}[x]$ pour tous les nombres premiers ne divisant pas D_f, nous aurions un bon indice pour déterminer, à isomorphisme près, le groupe de Galois

G de $f(x)$ sur $\mathbb{Q}$, car nous aurions la proportion exacte de chaque type d'éléments de G. En pratique, cela est impossible, car il faudrait effectuer une infinité de calculs. Néanmoins nous pouvons faire la factorisation pour, par exemple, les 100 premiers nombres premiers qui ne divisent pas D_f pour avoir un bon aperçu de la distribution des éléments de G et ainsi déterminer ce qui serait probablement le bon groupe de Galois de $f(x)$ à isomorphisme près. Voici deux exemples illustrant l'utilité de ce théorème.

Exemple 3. Considérons le polynôme $f(x) = x^5 - 5x + 12$ de discriminant $2^6 5^6$. Nous verrons au chapitre 5 que les groupes transitifs de degré 5 sont C_5, D_5, F_{20} (le groupe de Frobenius d'ordre 20), A_5 et S_5. Le discriminant étant un carré, nous pouvons tout de suite déduire que le groupe de Galois de $f(x)$ est un sous-groupe transitif du groupe alterné A_5, ce qui élimine donc les groupes transitifs S_5 et F_{20}. Nous pouvons factoriser $f(x)$ mod p pour les 100 premiers nombres premiers, excluant 2 et 5 [S+12]. Ensuite, nous pouvons calculer le rapport $\#T/100$ où $\#T$ est le nombre de fois que le polynôme réduit pour les 100 premiers nombres premiers (sauf pour 2 et 5) se factorise en cycle de type T. Nous trouvons les résultats suivants :

Types de factorisation	(1)	(2, 2)	(3)	(5)
$\#T/100$	0.09	0.54	0	0.37

TABLE 3.1: Distribution des types de facteurs de $f(x)$ mod p pour les cent premiers p

Nous comparons ensuite tous ces rapports aux $d_T = n_T/N$ de chaque sous-groupe transitif de A_5 [DF04] (voir Annexe B pour la liste des permutations).

Types de cycle	(1)	(2, 2)	(3)	(5)
C_5	0.2	0	0	0.8
D_5	0.1	0.5	0	0.4
A_5	0.0167	0.25	0.3333	0.4

TABLE 3.2: Distribution d_T des cycles pour chacun des sous-groupes transitifs de A_5

Nous pouvons donc conclure que le groupe de Galois associé au polynôme $f(x) = x^5 - 5x + 12$ est probablement D_5, le groupe diédral d'ordre 10. Nous pouvons par contre affirmer que le groupe de Galois de $f(x)$ n'est pas le groupe cyclique C_5, car il existe au moins une réduction de $f(x)$ de type $(2, 2)$, alors que C_5 ne contient aucun cycle de ce type. PARI nous confirme qu'il s'agit du bon groupe [The12].

Exemple 4. Considérons maintenant le polynôme $f(x) = x^7 - 7x + 3$ de discriminant $3^8 7^8$. Nous verrons au chapitre 7 que les groupes transitifs de degré 7 sont C_7, D_7, F_{21}, F_{42}, G_{168}, A_7 et S_7. Une fois de plus, comme le discriminant est un carré dans $\mathbb{Z}$, alors le groupe de

Galois du polynôme est un sous-groupe transitif de A_7. En utilisant la même méthode que dans l'exemple précédent et en utilisant les 100 premiers nombres premiers, sauf 3 et 7, nous obtenons les distributions suivantes :

Types de factorisation	(1)	(2, 2)	(3)	(2, 2, 3)	(3, 3)	(2, 4)	(5)	(7)
$\#T/100$	0	0.15	0	0	0.32	0.32	0	0.21

TABLE 3.3: Distribution des types de facteurs de $f(x) \mod p$ pour les cent premiers p

Voici ensuite la distribution des cycles pour chaque sous-groupe transitif du groupe alterné A_7 (voir [DF04] pour cette distribution) :

Types de cycle	(1)	(2, 2)	(3)	(2, 2, 3)	(3, 3)	(2, 4)	(5)	(7)
F_{21}	0.0476	0	0	0	0.6667	0	0	0.2857
G_{168}	0.006	0.125	0	0	0.3333	0.25	0	0.2857
A_7	0.0004	0.0417	0.0278	0.0833	0.1111	0.25	0.2	0.2857

TABLE 3.4: Distribution des types de facteurs de $f(x) \mod p$ pour les cent premiers p

Nous pouvons donc affirmer que le groupe de Galois de $f(x)$ n'est certainement pas F_{21} et qu'il est probable que ce soit le groupe simple d'ordre 168. PARI confirme qu'il s'agit bien de la bonne réponse.

Chapitre 4

Introduction de la méthode de la résolvante

Bien que la méthode probabiliste précédente donne une bonne idée du groupe de Galois d'un polynôme $f(x)$, il serait pertinent de démontrer rigoureusement qu'il s'agit du bon groupe. Cette tâche n'est pas, en général, de tout repos. Pour les polynômes de degrés relativement petits, certains algorithmes existent et fonctionnent en un temps raisonnable. Ces techniques utilisent ce que certains auteurs appellent les *polynômes résolvants*. L'idée derrière ces derniers est très similaire à l'approche de la résolvante cubique utilisée pour trouver le groupe de Galois d'une quartique. H. Cohen explicite des algorithmes pour des polynômes allant jusqu'au degré 7 [Coh93]. Dans le cadre de ce mémoire, nous n'allons qu'expliciter les algorithmes pour les degrés 5, 6 et 7.

Dans ce chapitre (et dans les trois chapitres suivants), $\mathbb{Q}(\alpha)$ est un corps de degré n pour un certain nombre algébrique α qui a $f(x)$ comme polynôme minimal unitaire. Notre but est de déterminer $Gal(f)$, le groupe de Galois de f, ce qui revient à trouver le groupe de Galois du corps de décomposition de f, c'est-à-dire de la fermeture galoisienne de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$ (la plus petite extension galoisienne dans $\mathbb{C}$ contenant $\mathbb{Q}(\alpha)$). Comme déjà mentionné, étant donné une liste fixe des racines de f, les éléments de $Gal(f)$ permutent ces racines et ainsi ce groupe peut être vu comme un sous-groupe de S_n. Changer l'ordre de la liste fait en sorte que $Gal(f)$ sera transformé en l'un de ses groupes conjugués. Pour ce chapitre (et pour les trois suivants), nous fixons l'ordre de la liste des racines ; bien qu'il soit arbitraire, nous aurons besoin de le changer.

Définition 4.0.9. Soit G un groupe d'automorphismes et X un ensemble sur lequel G agit. L'*orbite* d'un élément $x \in X$ par G est

$$G.x = \{\sigma(x) \mid \sigma \in G\}.$$

Comme f est irréductible, alors $Gal(f)$ est transitif dans S_n ; en d'autres termes, il n'y a qu'une orbite pour l'action de $Gal(f)$ sur les racines α_i de f (car chaque orbite correspond à un facteur irréductible de f, or f est irréductible).

Afin de trouver $Gal(f)$, nous devons connaître tous les sous-groupes transitifs de S_n à conjugaison près ainsi que leurs relations d'inclusion.

Remarquons que comme la cardinalité d'une orbite divise l'ordre du groupe $Gal(f)$, alors n divise la cardinalité d'un sous-groupe transitif de S_n.

Définition 4.0.10. Soit G un sous-groupe de S_n qui contient $Gal(f)$, le groupe de Galois du polynôme $f(x) \in \mathbb{Z}[x]$ de degré n. De plus, soit $F(X_1, X_2, \ldots, X_n)$ un polynôme dans $\mathbb{Z}[X_1, X_2, \ldots, X_n]$. Nous définissons le *stabilisateur* de F dans G comme étant

$$H = Stab(F, G) = \{\sigma \in G \mid F\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = F\left(X_1, X_2, \ldots, X_n\right)\}.$$

Nous disons que H *stabilise exactement* le polynôme F. Avec ce stabilisateur, nous définissons ensuite le *polynôme résolvant de f par rapport à F dans G* par

$$R_G(F, f)(x) = \prod_{\sigma \in G/H} \left(x - F\left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}\right)\right)$$

où les α_i sont les n racines de f et où les $\sigma \in G/H$ sont des représentants de classes à gauche de G modulo H. Il est important de ne pas confondre G/H avec le groupe quotient, il ne s'agit que d'une notation ; rien n'assure que cet ensemble soit un groupe. Le terme *résolvante* va parfois remplacer l'expression *polynôme résolvant*. Remarquons que le polynôme résolvant $R_G(F, f)$ a tous ses coefficients dans $\mathbb{Z}$.

Exemple 5. Soit le groupe $G = D_5$ et le polynôme à plusieurs variables

$$F = X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_5^2 + X^5X_1^2.$$

Trouvons $H = Stab(F, G)$ ainsi que G/H. Nous remarquons facilement que les permutations

$$id, (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3) \text{ et } (1\ 5\ 4\ 3\ 2)$$

stabilisent F. Il se trouve que ces cinq éléments forment le groupe cyclique C_5. Comme $[G : H] = 10/5 = 2$, alors l'ensemble G ne contient que deux classes d'équivalence modulo H. La première est évidemment le classe de l'identité $\widehat{id}$ et la deuxième est la classe de n'importe lequel des éléments restants de D_5 qui n'est pas dans C_5, par exemple prenons $\widehat{(1\ 2)(3\ 5)}$. Ainsi $G/H = \{\widehat{id}, \widehat{(1\ 2)(3\ 5)}\}$, mais par abus de notation, nous écrivons $G/H = \{id, (1\ 2)(3\ 5)\}$.

Il est important de noter que la définition de $R_G(F, f)$ permet de trouver facilement ses racines. Nous verrons que la manipulation des racines est préférée à la construction de la résolvante, surtout dans un algorithme.

Remarque. Lorsqu'un polynôme ne possède aucun facteur irréductible de multiplicité au moins 2, nous disons qu'il est *sans facteur carré*. Certains auteurs utilisent le terme *séparable*, qui est équivalent sous la condition de travailler dans un corps de caractéristique nulle ou de caractéristique p si tous les éléments du corps sont des p-ièmes puissances. Pour éviter la confusion, nous nous en tiendrons à la première appelation.

Théorème 4.0.11 (Cohen [Coh93], Soicher [Soi81])**.** *Soit m le degré de $R_G(F, f)$, qui est égal à l'indice $[G : H]$ de $H = Stab(F, G)$ dans G. Si $R_G(F, f)$ est un polynôme sans facteur carré, alors son groupe de Galois est $\varphi(Gal(f))$, où φ est l'homomorphisme naturel de G vers S_m défini par l'action naturelle à gauche de G sur G/H. En particulier, la liste des degrés des facteurs irréductibles de $R_G(F, f)$ dans $\mathbb{Z}[x]$ correspond à la liste des longueurs d'orbites de l'action de $\varphi(Gal(f))$ sur $\{1, 2, \ldots, m\}$.*

Corollaire 4.0.12. *Le polynôme résolvant sans facteur carré $R_G(F, f)$ a une racine entière si et seulement si $Gal(f)$ est conjugué à un sous-groupe de $H = Stab(F, G)$ par un élément de G.*

Typiquement les éléments de G/H seront l'identité et des transpositions. La proposition qui suit est un peu plus forte que le théorème et le corollaire précédents, dans le sens où l'hypothèse ne requiert pas que le polynôme résolvant soit sans facteur carré.

Proposition 4.0.13 (Cohen [Coh93])**.** *Si $R_G(F, f)$ a une racine simple dans $\mathbb{Z}$, alors $Gal(f)$ est conjugué à un sous-groupe de $H = Stab(F, G)$ par un élément de G.*

Ainsi, lorsque nous voulons déterminer si le polynôme résolvant est irréductible, il suffit d'approximer ses racines avec une assez bonne précision et de constater qu'aucune d'entre elles n'est entière. En plus, si nous voulons savoir si $R_G(F, f)$ est sans facteur carré ou non, il suffit d'utiliser la même approximation des racines et de constater ou non qu'aucune de ses racines n'est multiple. D'un point de vue efficacité informatique, il est beaucoup plus simple d'approximer les racines d'un polynôme que de le factoriser. Ainsi, pour la construction d'un algorithme, par exemple, nous favorisons habituellement l'approximation plutôt que la factorisation. H. Cohen laisse en exercice la précision des racines requise pour laquelle ses algorithmes restent exacts.

Si nous voulons utiliser le théorème précédent, mais que nous sommes en présence d'une résolvante qui a au moins un facteur carré, nous pouvons effectuer une *transformation de*

Tschirnhaus. Cette transformation remplace f par un autre polynôme minimal unitaire ayant le même corps de décomposition $\mathbb{Q}(\alpha)$.

L'algorithme est plutôt simple ; à partir d'un polynôme arbitraire $A(x)$ dans $\mathbb{Z}[x]$ et de degré strictement inférieur au degré de f, nous construisons un polynôme $C(x)$:

$$C(x) = \prod_{1 \leq i \leq n} (x - A(\alpha_i)).$$

Tant et aussi longtemps que C possède un facteur carré, nous recommençons à l'étape de création de A. Si, par contre, C respecte cette condition, alors ce polynôme remplace le f original.

Algorithme 4.1 Transformer un polynôme pour que sa résolvante soit sans facteur carré

Requis: $f(x) \in \mathbb{Z}[x]$ irréductible unitaire et α_i ses racines.

1: **Procédure:** $(C, A) =$ TSCHIRNHAUS(f)
2: $n \leftarrow \deg(f)$
3: $V(x) \leftarrow x$
4: **while** $\deg V \neq 0$ **do**
5: $A(x) \leftarrow$ POLYNÔMEALÉATOIRE$(n-1) \in \mathbb{Z}[x]$ ▷ le degré de A doit être $\leq n-1$
6: $C(x) \leftarrow \prod_{1 \leq i \leq n} (x - A(\alpha_i))$
7: $V(x) \leftarrow$ PGCD(C, C') ▷ C' est la dérivé de C
8: **end while**
9: **return** (C, A) ▷ C est le polynôme transformé et A aide à trouver ses racines
10: **end Procédure:**

Cette transformation ne va pas nécessairement nous donner un polynôme dont la résolvante est sans facteur carré, mais H. Cohen nous assure qu'en pratique, l'algorithme n'a besoin d'être répété que quelques fois avant de donner le résultat espéré. Nous acceptons également que la transformation en soi converge en un temps acceptable et est très efficace [Coh93]. À la ligne 6, nous créons ce qui s'appelle le *polynôme caractéristique de* $A(\alpha)$. La définition utilisée n'est pas la plus optimale. En effet, H. Cohen consacre plusieurs sous-sections de son volume *A Course in Computational Algebraic Number Theory* sur celle-ci. Une série de résultats aboutissent à une alternative qui permet d'éviter de passer par les racines de f, ce qui augmente la précision de l'algorithme de Tschirnhaus.

Chapitre 5

Le cinquième degré

5.1 Démarche

À conjugaison près, S_5 possède 5 sous-groupes transitifs. Nous rappelons qu'ils sont :

C_5, le groupe cyclique d'ordre 5 ;
D_5, le groupe diédral d'ordre 10 ;
F_{20}, le groupe de Frobenius d'ordre 20 ;
A_5, le groupe alterné ;
S_5, le groupe symétrique.

La définition générale d'un groupe de Frobenius ainsi que quelques informations suppplémentaires sont données dans l'annexe C. Nous pouvons également définir

$$F_{20} \simeq \langle \sigma, \tau \,|\, \sigma^4 = \tau^5 = 1, \tau\sigma = \sigma\tau^2 \rangle$$

(voir Annexe D pour la table de Cayley et Annexe E pour le bigraphe de Cayley).

Le treillis des sous-groupes transitifs de degré 5 (c'est-à-dire les sous-groupes transitifs de S_5) de la figure 5.1 est particulièrement utile pour visualiser les étapes à suivre.

La démarche pour déterminer le groupe de Galois d'un polynôme consiste essentiellement à séparer le graphe grâce à un choix judicieux de résolvante. Il s'agit en fait de bien appliquer les résultats 3.0.3 et 4.0.12. L'explication ci-après tient pour acquis que les résolvantes construites sont sans facteur carré, même si en pratique, ce n'est pas toujours le cas. Néanmoins, l'algorithme présenté subséquemment en tient compte.

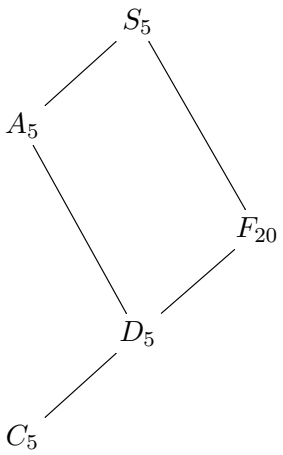


FIGURE 5.1: Sous-groupes transitifs de degré 5

En premier lieu, nous déterminons le stabilisateur dans S_5 du polynôme à plusieurs variables

$$\begin{aligned} F_1 = &X_1^2(X_2X_5 + X_3X_4) + X_2^2(X_1X_3 + X_4X_5) + X_3^2(X_1X_5 + X_2X_4) \\ &+ X_4^2(X_1X_2 + X_3X_5) + X_5^2(X_1X_4 + X_2X_3) \end{aligned}$$

et nous trouvons $Stab(F_1, S_5) = F_{20}$. Puis nous construisons la résolvante R associée. Ainsi, le corollaire 4.0.12 nous assure que le groupe recherché est (respectivement n'est pas) contenu dans F_{20} si la résolvante possède (respectivement ne possède pas) une racine entière. Ensuite, en vertu de la proposition 3.0.3, si le discriminant du polynôme initial est un carré entier, alors nous nous retrouvons dans A_5. Combinées, les deux vérifications précédentes coupent le graphe en quatre :

Racine entière de R ?	Discriminant carré ?	Endroit dans le graphe
Non	Non	S_5
Non	Oui	A_5
Oui	Non	F_{20}
Oui	Oui	D_5 / C_5

Finalement, il ne reste qu'à séparer le cas D_5 du cas C_5. Il suffit de considérer le stabilisateur de

$$F_2 = X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_5^2 + X_5X_1^2$$

pour D_5 pour obtenir nul autre que $Stab(F_2, D_5) = C_5$. Encore une fois, si la résolvante associée comporte une racine entière, alors le groupe de Galois est C_5, sinon c'est D_5.

Cette démarche est simple et directe, même si elle fait intervenir deux polynômes résolvants. Son avantage, comparativement aux degrés supérieurs, c'est qu'il n'est pas nécessaire de factoriser ceux-ci, ce qui diminue considérablement le temps d'exécution.

5.2 Algorithme

Nous présentons ici le pseudo-code de l'algorithme proposé par H. Cohen [Coh93].

Algorithme 5.1 Calculer le groupe de Galois d'un polynôme de degré 5

Requis: $f(x) \in \mathbb{Z}[x]$ irréductible unitaire de degré 5 et α_i ses racines.

1: **Procédure:** GALOISDEG5(f)
2: $F_1 \leftarrow X_1^2(X_2X_5 + X_3X_4) + X_2^2(X_1X_3 + X_4X_5)$
3: $\quad + X_3^2(X_1X_5 + X_2X_4) + X_4^2(X_1X_2 + X_3X_5) + X_5^2(X_1X_4 + X_2X_3)$
4: $r_j \leftarrow$ RACINES($R_G(F_1, f)$) pour $G = S_5$
▷ Ici, $H = F_{20}$ et $G/H = \{id, (12), (13), (14), (15), (25)\}$
5: **while** $\exists j_1, j_2$ **s.t.** $r_{j_1} = r_{j_2}$ **do** ▷ Racines multiples
6: $(f, A) \leftarrow$ TSCHIRNHAUS(f)
7: $\alpha_i \leftarrow A(\alpha_i)$ ▷ Les nouvelles racines de f
8: $r_j \leftarrow$ RACINES($R_G(F_1, f)$) pour $G = S_5$
9: **end while**
10: **if** $\nexists j$ **s.t.** $r_j \in \mathbb{Z}$ **then** ▷ Résolvante irréductible
11: **if** $\sqrt{D_f} \notin \mathbb{Z}$ **then return** S_5 ▷ D_f est le discriminant de f
12: **else return** A_5
13: **end if**
14: **else if** $\exists j$ **s.t.** $r_j \in \mathbb{Z}$ **then** ▷ Résolvante réductible
15: **if** $\sqrt{D_f} \notin \mathbb{Z}$ **then return** F_{20}
16: **else** ▷ R a une seule racine entière et D_f est un carré
17: $\sigma \leftarrow$ l'élément de G/H qui correspond à la racine entière r_j
18: $\alpha_i \leftarrow \alpha_{\sigma(i)}$ ▷ Renumérotation des racines de T selon σ
19: $F_2 \leftarrow X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_5^2 + X_5X_1^2$
20: $s_j \leftarrow$ RACINES($R_G(F_2, f)$) pour $G = D_5$
▷ Ici, $H = C_5$ et $G/H = \{id, (12)(35)\}$
21: **while** $\exists j_1, j_2$ **s.t.** $s_{j_1} = s_{j_2}$ **do**
22: $(f, A) \leftarrow$ TSCHIRNHAUS(f)
23: $\alpha_i \leftarrow A(\alpha_i)$
24: $s_j \leftarrow$ RACINES($R_G(F_2, f)$) pour $G = D_5$
25: **end while**
26: **if** $\nexists j$ **s.t.** $s_j \in \mathbb{Z}$ **then return** D_5
27: **else if** $\exists j$ **s.t.** $s_j \in \mathbb{Z}$ **then return** C_5
28: **end if**
29: **end if**
30: **end if**
31: **end Procédure:**

Aux lignes 4 et 8, il n'est pas nécessaire de construire la résolvante : nous pouvons simplement utiliser la définition de cette dernière pour construire explicitement les racines.

À la ligne 19, il est possible d'éviter d'utiliser la résolvante [Coh93]. De façon un peu plus efficace, nous pourrions construire le discriminant de $R_G(F_2, f)$ avec $G = D_5$, c'est-à-dire

$$d = (\alpha_1\alpha_2(\alpha_2 - \alpha_1) + \alpha_2\alpha_3(\alpha_3 - \alpha_2) + \alpha_3\alpha_4(\alpha_4 - \alpha_3) + \alpha_4\alpha_5(\alpha_5 - \alpha_4) + \alpha_5\alpha_1(\alpha_1 - \alpha_5))^2.$$

Ensuite il suffirait de vérifier si d est nul ou non. Dans le cas où d est non nul, le groupe de Galois serait C_5 si cette quantité est un carré parfait et D_5 sinon. Dans le cas où d serait nul, il faudrait remplacer f avec une transformation de Tschirnhaus et renuméroter ses racines jusqu'à ce que le discriminant de $R_G(F_2, f)$ soit non nul pour ensuite se retrouver dans le cas précédent.

Chapitre 6

Le sixième degré

6.1 Démarche

Il existe 16 groupes transitifs de degré 6 à conjugaison près, ce qui est beaucoup plus que dans le chapitre précédent. Il est important de remarquer que le groupe symétrique d'ordre 4 apparaît à deux reprises, car ces copies sont dans des classes de conjugaison différentes. Nous ajouterons un astérisque à tous les sous-groupes du groupe transitif A_6, ainsi nous pourrons non seulement différencier ces deux classes, mais également différencier les deux groupes d'ordre 36 en plus de nous aider à mieux nous situer lors de l'élaboration de l'algorithme.

La liste des 16 sous-groupes transitifs de S_6 est donnée dans la table 6.1.

Sous-groupes	Informations
S_6	
A_6^*	
$PGL_2(\mathbb{F}_5)$	$\simeq S_5$
G_{72}	$= (C_3)^2 \rtimes D_4$
$PSL_2^*(\mathbb{F}_5)$	$\simeq A_5$ et $\subset A_6^*$
$S_4 \times C_2$	
G_{36}	$= (C_3)^2 \rtimes (C_2)^2 \simeq S_3 \times S_3$
G_{36}^*	$= (C_3)^2 \rtimes C_4 \subset A_6^*$
S_4	
$A_4 \times C_2$	
S_4^*	$\subset A_6^*$
G_{18}	$= (C_3)^2 \rtimes C_2 \simeq S_3 \times A_3$
D_6	$\simeq S_3 \times C_2$
A_4^*	$\subset A_6^*$
C_6	$\simeq A_3 \times C_2$
S_3	

TABLE 6.1: Liste et informations sur les groupes transitifs de degré 6

Les groupes $PGL_2(\mathbb{F}_5)$ et $PSL_2^*(\mathbb{F}_5)$ de la table 6.1 sont respectivement le groupe projectif général linéaire de degré 2 sur le corps $\mathbb{F}_5$ et le groupe projectif spécial linéaire de même degré sur le même corps. Ils sont respectivement définis comme le quotient de $GL_2(\mathbb{F}_5)$ par son centre et le quotient de $SL_2(\mathbb{F}_5)$ par son centre.

Avec un petit programme construit à l'aide de SAGE [S+12] (voir Annexe F), nous pouvous facilement obtenir le treillis de la figure 6.1 qui illustre les relations groupes–sous-groupes des entrées de la table 6.1.

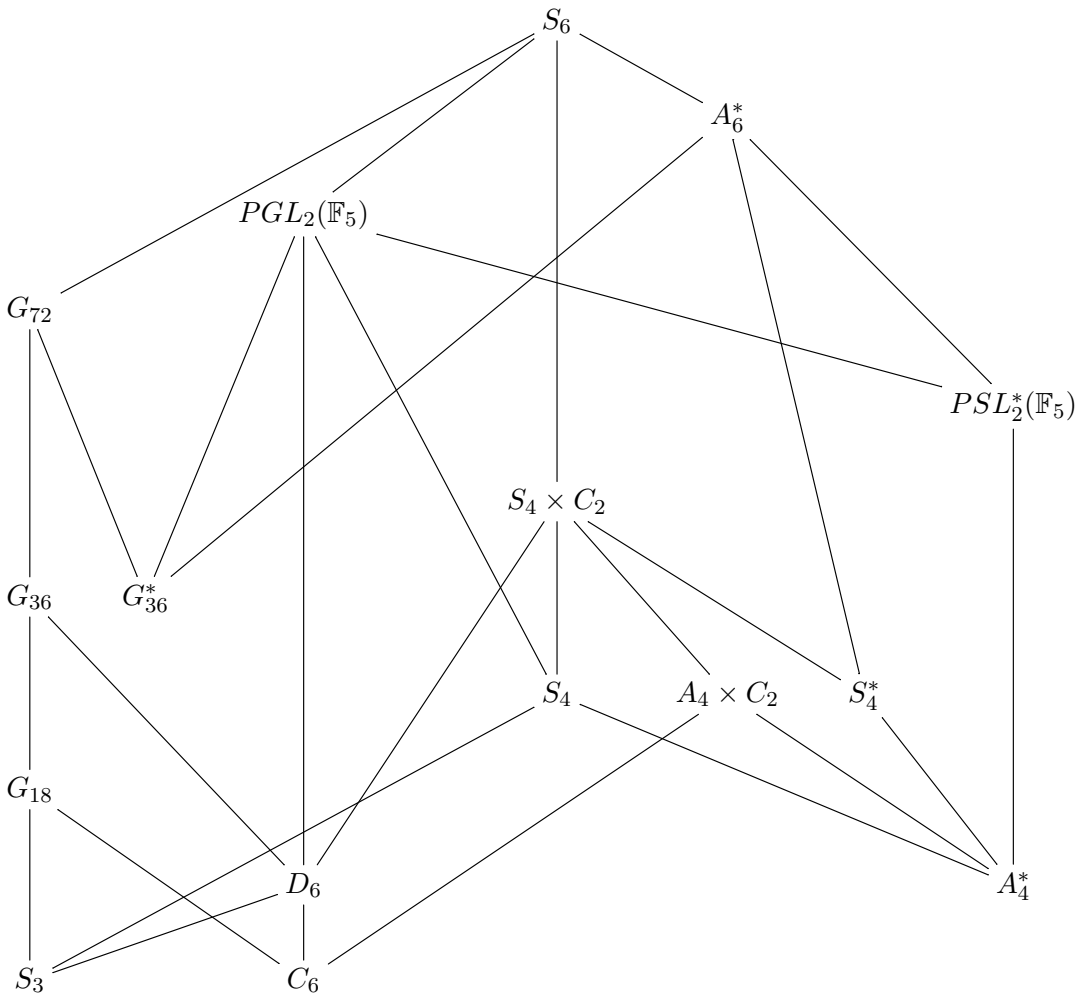


FIGURE 6.1: Treillis des groupes transitifs de degré 6

Tout d'abord, comme pour l'algorithme pour un polynôme f de degré 5, nous devons construire la résolvante R pour le groupe $G = S_6$ du polynôme

$$F = X_1^2X_5^2(X_2X_4 + X_3X_6) + X_2^2X_4^2(X_1X_5 + X_3X_6) + X_3^2X_6^2(X_1X_5 + X_2X_4)$$

$$+ X_1^2X_6^2(X_2X_5 + X_3X_4) + X_2^2X_5^2(X_1X_6 + X_3X_4) + X_3^2X_4^2(X_1X_6 + X_2X_5)$$
$$+ X_1^2X_3^2(X_2X_6 + X_4X_5) + X_2^2X_6^2(X_1X_3 + X_4X_5) + X_4^2X_5^2(X_1X_3 + X_2X_6)$$
$$+ X_1^2X_4^2(X_2X_3 + X_5X_6) + X_2^2X_3^2(X_1X_4 + X_5X_6) + X_5^2X_6^2(X_1X_4 + X_2X_3)$$
$$+ X_1^2X_2^2(X_3X_5 + X_4X_6) + X_3^2X_5^2(X_1X_2 + X_4X_6) + X_4^2X_6^2(X_1X_2 + X_3X_5).$$

Le stabilisateur de ce polynôme est $H = PGL_2(\mathbb{F}_2)$. Dans le but d'utiliser la deuxième partie du théorème 4.0.11, nous déterminons la liste des longueurs d'orbites de l'action de $\varphi(Gal(f))$ sur $\{1, 2, 3, 4, 5, 6\}$ où φ est l'endomorphisme naturel de $G = S_6$ défini par l'action naturelle à gauche de G sur l'ensemble de classes à gauche G/H. Une fois de plus, un programme développé avec SAGE permet de déterminer la liste de chacun des $\varphi(Gal(f))$ possibles (voir Annexe G).

Liste des longueurs d'orbites	Groupe(s) associé(s)
$[6]$	$S_6,\ A_6,\ G_{72},\ G_{36}^*$
$[1, 5]$	$PGL_2(\mathbb{F}_5),\ PSL_2^*(\mathbb{F}_5)$
$[2, 4]$	$S_4 \times C_2,\ A_4 \times C_2,\ S_4^*$
$[1, 1, 4]$	$S_4,\ A_4^*$
$[3, 3]$	$G_{36},\ G_{18}$
$[1, 2, 3]$	$D_6,\ C_6$
$[1, 1, 1, 3]$	S_3

TABLE 6.2: Liste des longueurs d'orbites des actions des groupes transitifs de degré 6

Ensuite, il suffit de factoriser R (à l'aide d'un algorithme quelconque) et de comparer la liste L des degrés de chaque facteur irréductible à la table 6.2. Si $L = [1, 1, 1, 3]$, alors le groupe est nécessairement S_3. Si $L = [1, 2, 3]$, remarquons que $D_6 \simeq S_3 \times C_2$ et $C_6 \simeq A_3 \times C_2$. Donc si nous considérons le facteur irréductible de degré 3 de R, tout dépendant si son discriminant est un carré dans $\mathbb{Z}$ ou non, alors le groupe de Galois de ce facteur est dans A_3 ou dans S_3 exclusivement, d'où le groupe recherché est C_6 ou D_6. Si $L = [3, 3]$, comme $G_{36} \simeq S_3 \times S_3$ et $G_{18} \simeq S_3 \times A_3$, alors il suffit de vérifier si l'un des facteurs irréductibles de degré 3 a un discriminant carré dans $\mathbb{Z}$ ou non, dans lequel cas le groupe de Galois du polynôme initial est G_{18} ou G_{36}. Si $L = [1, 1, 4]$, alors le résultat découle du fait que A_4^* est sous-groupe de A_6^* alors que S_4 ne l'est pas : si le discriminant de f est le carré d'un entier, alors $Gal(f) = A_4^*$; sinon $Gal(f) = S_4$. Dans le cas où $L = [2, 4]$, nous commençons par vérifier si $\sqrt{D_f}$ est entier. Dans le cas échéant, $Gal(f) = S_4^*$, car il est le seul sous-groupe de A_6^* de cette branche. Ensuite, nous considérons le discriminant du facteur de degré 4 de R, à savoir s'il est carré d'un entier ou non, ce qui résulte en $Gal(f) = A_4 \times C_2$ ou $Gal(f) = S_4 \times C_2$. Si $L = [1, 5]$, alors comme $PSL_2^*(\mathbb{F}_5)$ est dans A_6^* et que $PGL_2(\mathbb{F}_5)$ ne l'est pas, il suffit de faire la vérification usuelle sur le discriminant de f.

Finalement, le travail est un peu plus long si R est irréductible. Nous devons considérer une

nouvelle résolvante R construite à partir de $G = S_6$ et de

$$F = X_1X_2X_3 + X_4X_5X_6,$$

ce qui nous donne le stabilisateur $H = G_{72}$. Si R a une racine entière ou non, alors en vertu de la proposition 4.0.13, $Gal(f)$ se trouve sous G_{72} ou S_6. Dans le cas où R a une racine entière, si $\sqrt{D_f}$ est entier, alors le groupe de Galois de f est G_{36}^*, sinon $Gal(f) = G_{72}$. Dans le cas où R n'a pas de racine entière, si $\sqrt{D_f}$ est entier, alors $Gal(f) = A_6^*$, sinon $Gal(f) = S_6$.

6.2 Algorithme

À la lumière de l'explication précédente, l'algorithme que H. Cohen [Coh93] présente se divise en trois grandes parties :

1. La construction de la résolvante de f.
2. L'analyse des facteurs irréductibles du polynôme résolvant.
3. L'étude du cas où la résolvante est irréductible.

Contrairement à la démarche, l'algorithme s'assure que les résolvantes construites n'ont pas de facteurs carrés afin de pouvoir utiliser les résultats cités. Voici la première partie du pseudo-code.

Algorithme 6.1 Calculer le groupe de Galois d'un polynôme de degré 6 (partie 1)

Requis: $f(x) \in \mathbb{Z}[x]$ irréductible unitaire de degré 6 et α_i ses racines.

1: **Procédure:** GaloisDeg6(f)
2: $n = 1$
3: **while** $n \neq 0$ **do**
4: $F \leftarrow X_1^2X_5^2(X_2X_4 + X_3X_6) + X_2^2X_4^2(X_1X_5 + X_3X_6) + X_3^2X_6^2(X_1X_5 + X_2X_4)$
5: $+X_1^2X_6^2(X_2X_5 + X_3X_4) + X_2^2X_5^2(X_1X_6 + X_3X_4) + X_3^2X_4^2(X_1X_6 + X_2X_5)$
6: $+X_1^2X_3^2(X_2X_6 + X_4X_5) + X_2^2X_6^2(X_1X_3 + X_4X_5) + X_4^2X_5^2(X_1X_3 + X_2X_6)$
7: $+X_1^2X_4^2(X_2X_3 + X_5X_6) + X_2^2X_3^2(X_1X_4 + X_5X_6) + X_5^2X_6^2(X_1X_4 + X_2X_3)$
8: $+X_1^2X_2^2(X_3X_5 + X_4X_6) + X_3^2X_5^2(X_1X_2 + X_4X_6) + X_4^2X_6^2(X_1X_2 + X_3X_5)$
9: $R \leftarrow R_G(F, f)$ pour $G = S_6$
▷ Ici, $H = PGL_2(\mathbb{F}_5)$ et $G/H = \{id, (12), (13), (14), (15), (16)\}$
10: $R \leftarrow$ Round(R) ▷ Les coefficients de R arrondis aux entiers près
11: $V(x) \leftarrow$ pgcd(R, R') ▷ R' est la dérivé de R
12: $n \leftarrow \deg V$
13: **if** $n \neq 0$ **then**
14: $(f, A) \leftarrow$ Tschirnhaus(f)
15: $\alpha_i \leftarrow A(\alpha_i)$ ▷ Les nouvelles racines de f
16: **end if**
17: **end while**

L'assignation de la ligne 2 sert à assurer que la condition de la boucle soit respectée au moins une fois et donc d'entrer dans celle-ci. La boucle en soi permet de construire un polynôme résolvant sans facteur carré. Si le plus grand commun diviseur entre R et sa dérivée n'est pas une constante, alors R contient au moins un facteur de puissance deux et donc l'algorithme (en ligne 14) génère un nouveau polynôme f tant et aussi longtemps que sa résolvante pour F et $G = S_6$ ne soit pas sans facteur carré.

Algorithme 6.2 Calculer le groupe de Galois d'un polynôme de degré 6 (partie 2)

18: $R \leftarrow \textsc{Factor}(R)$
19: $L \leftarrow \textsc{SortedDegreeList}(R)$
▷ Liste ascendante des degrés des facteurs irréductibles de R
20: **if** $L = [1, 2, 3]$ **then**
21: $t \leftarrow$ «facteur de R de degré 3»
22: **if** $\sqrt{D_t} \in \mathbb{Z}$ **then return** C_6
23: **else return** D_6
24: **end if**
25: **else if** $L = [3, 3]$ **then**
26: $t_1 \leftarrow$ «premier facteur de R»
27: $t_2 \leftarrow$ «deuxième facteur de R»
28: **if** $\sqrt{D_{t_1}} \notin \mathbb{Z}$ **and** $\sqrt{D_{t_2}} \notin \mathbb{Z}$ **then return** G_{36}
29: **else return** G_{18}
30: **end if**
31: **else if** $L = [2, 4]$ **then**
32: **if** $\sqrt{D_f} \in \mathbb{Z}$ **then return** S_4^*
33: **else**
34: $t \leftarrow$ «facteur de R de degré 4»
35: **if** $\sqrt{D_t} \in \mathbb{Z}$ **then return** $A_4 \times C_2$
36: **else return** $S_4 \times C_2$
37: **end if**
38: **end if**
39: **else if** $L = [1, 1, 4]$ **then**
40: **if** $\sqrt{D_f} \in \mathbb{Z}$ **then return** A_4^*
41: **else return** S_4
42: **end if**
43: **else if** $L = [1, 5]$ **then**
44: **if** $\sqrt{D_f} \in \mathbb{Z}$ **then return** $PSL_2^*(\mathbb{F}_5)$
45: **else return** $PGL_2(\mathbb{F}_5)$
46: **end if**
47: **else if** $L = [1, 1, 1, 3]$ **then return** S_3

À la ligne 18, l'algorithme demande de factoriser la résolvante à l'aide de son algorithme de factorisation de polynômes favori. À la ligne qui suit, la procédure prend la liste des degrés des facteurs irréductibles de R et la trie en ordre croissant pour mieux l'identifier dans les étapes qui suivent.

Dans la troisième partie, comme nous créons une nouvelle résolvante, nous devons nous assurer une fois de plus qu'elle est sans facteur carré avec l'algorithme de Tschirnhaus.

Algorithme 6.3 Calculer le groupe de Galois d'un polynôme de degré 6 (partie 3)

48: **else if** $L = [6]$ **then** ▷ R irréductible
49: $F \leftarrow X_1X_2X_3 + X_4X_5X_6$
50: $r_j \leftarrow \text{RACINES}(R_G(F, f))$ pour $G = S_6$ et $H = G_{72}$
▷ Ici, $G/H = \{id, (14), (15), (16), (24), (25), (26), (34), (35), (36)\}$
51: **while** $\exists j_1, j_2$ **s.t.** $r_{j_1} = r_{j_2}$ **do** ▷ Racines multiples
52: $(f, A) \leftarrow \text{TSCHIRNHAUS}(f)$
53: $\alpha_i \leftarrow A(\alpha_i)$ ▷ Les nouvelles racines de f
54: $r_j \leftarrow \text{RACINES}(R_G(F, f))$ pour $G = S_6$
55: **end while**
56: **if** $\nexists j$ **s.t.** $r_j \in \mathbb{Z}$ **then**
57: **if** $\sqrt{D_f} \in \mathbb{Z}$ **then return** A_6^*
58: **else return** S_6
59: **end if**
60: **else if** $\exists j$ **s.t.** $r_j \in \mathbb{Z}$ **then**
61: **if** $\sqrt{D_f} \in \mathbb{Z}$ **then return** G_{36}^*
62: **else return** G_{72}
63: **end if**
64: **end if**
65: **end if**
66: **end Procédure:**

En fin de compte, bien que le degré 6 ait beaucoup de groupes transitifs, une fois que le treillis des groupes–sous-groupes est dressé, il suffit de bien choisir la résolvante pour appliquer judicieusement les résultats présentés.

Chapitre 7

Le septième degré

7.1 Démarche

Le septième degré est nettement plus simple que le sixième. En effet, il n'existe que 7 groupes transitifs de ce degré à conjugaison près. Ceux-ci sont

$$C_7,\ D_7,\ F_{21},\ F_{42},\ G_{168},\ A_7,\ S_7.$$

Notons que G_{168} est le groupe simple d'ordre 168. Il est isomorphe au groupe $PSL_3(\mathbb{F}_2)$ et au groupe $PSL_2(\mathbb{F}_7)$. Remarquons également que F_{21} et F_{42} sont respectivement les groupes de Frobenius d'ordre 21 et 42. Ils peuvent également être vus comme des groupes métacycliques, c'est-à-dire que F_{21}/N et F_{42}/M sont cycliques pour certains sous-groupes cycliques normaux N et M. Nous pouvons également voir ces derniers de la façon suivante :

$$\begin{cases} F_{21} \simeq \langle \sigma, \tau \mid \sigma^3 = \tau^7 = id,\ \tau\sigma = \sigma\tau^2 \rangle ; \\ F_{42} \simeq \langle \sigma, \tau, \rho \mid \sigma^2 = \tau^3 = \rho^7 = e,\ \rho\sigma = \sigma\rho^6,\ \rho\tau = \tau\rho^2 \rangle . \end{cases}$$

La figure 7.1 illustre le treillis des groupes nommés, obtenu avec le code de l'annexe F.

Tout comme dans les sections précédentes, pour le polynôme de départ f de degré 7, nous construisons une résolvante R à partir du groupe $G = S_7$ et du polynôme à plusieurs variables

$$\begin{aligned} F = {} & X_1(X_2 + X_3)X_4 + X_2(X_3 + X_4)X_5 + X_3(X_4 + X_5)X_6 + X_4(X_5 + X_6)X_7 \\ & + X_5(X_6 + X_7)X_1 + X_6(X_7 + X_1)X_2 + X_7(X_1 + X_2)X_3 \end{aligned}$$

pour obtenir le stabilisateur $H = F_{42}$. Le processus de création de ce polynôme dit F_{42}-*invariant* est expliqué dans le chapitre 8. Une fois de plus, afin d'utiliser le théorème 4.0.11, nous déterminons la liste des longueurs d'orbites de l'action de chacun des groupes par φ sur $\{1, 2, 3, 4, 5, 6, 7\}$ à l'aide du programme fait avec SAGE (voir Annexe G). La liste en question est présentée dans la table 7.1.

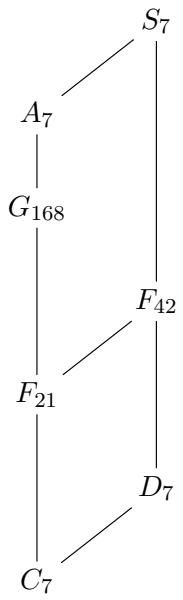


FIGURE 7.1: Treillis des groupes transitifs de degré 7

Liste des longueurs d'orbites	Groupe(s) associé(s)
$[7]$	$S_7,\ A_7$
$[3,4]$	G_{168}
$[1,2,4]$	F_{42}
$[1,1,1,4]$	F_{21}
$[1,1,2,3]$	D_7
$[1,1,1,1,3]$	C_7

TABLE 7.1: Liste des longueurs d'orbites des actions des groupes transitifs de degré 7

Le reste de la démarche est assez direct ; il suffit de factoriser R en facteurs irréductibles et de comparer la liste des degrés avec la table 7.1. Si le polynôme résolvant est irréductible, alors il suffit de vérifier si son discriminant est le carré d'un entier ou non pour savoir si le groupe de Galois de f est A_7 ou S_7.

7.2 Algorithme

Dans le volume *A Course in Computational Algebraic Number Theory*, l'algorithme proposé n'utilise pas les résultats cités plus haut. Pour cette raison, nous allons détailler un algorithme différent, quoiqu'un peu plus long, mais beaucoup plus efficace [Coh93].

La liste des représentants de G/H n'est pas explicitée, puisqu'elle est assez longue ($7!/42 = 5!$ éléments). De son côté, H. Cohen préfère construire un polynôme résolvant de degré 35 pour ensuite le factoriser.

Algorithme 7.1 Calculer le groupe de Galois d'un polynôme de degré 7

Requis: $f(x) \in \mathbb{Z}[x]$ irréductible unitaire de degré 7 et α_i ses racines.

Procédure: GaloisDeg7(f)
  $F \leftarrow X_1(X_2+X_3)X_4+X_2(X_3+X_4)X_5+X_3(X_4+X_5)X_6+X_4(X_5+X_6)X_7+X_5(X_6+X_7)X_1+X_6(X_7+X_1)X_2+X_7(X_1+X_2)X_3$
  $n = 1$
  while $n \neq 0$ **do**
    $R \leftarrow R_G(F, f)$ pour $G = S_7$
    ▷ Ici, $H = F_{42}$
    $R \leftarrow$ Round(R) ▷ Les coefficients de R arrondis aux entiers près
    $V(x) \leftarrow$ pgcd(R, R') ▷ R' est la dérivé de R
    $n \leftarrow \deg V$
    if $n \neq 0$ **then**
      $(f, A) \leftarrow$ Tschirnhaus(f)
      $\alpha_i \leftarrow A(\alpha_i)$ ▷ Les nouvelles racines de f
    end if
  end while
  $R \leftarrow$ Factor(R)
  $L \leftarrow$ SortedDegreeList(R)
    ▷ Liste ascendante des degrés des facteurs irréductibles de R
  if $L = [1, 1, 1, 1, 3]$ **then return** C_7
  else if $L = [1, 1, 2, 3]$ **then return** D_7
  else if $L = [1, 1, 1, 4]$ **then return** F_{21}
  else if $L = [1, 2, 4]$ **then return** F_{42}
  else if $L = [3, 4]$ **then return** G_{168}
  else if $L = [7]$ **then** ▷ Si R est irréductible
    if $\sqrt{D_f} \in \mathbb{Z}$ **then return** A_7
    else return S_7
    end if
  end if
end Procédure:

Chapitre 8

Polynômes invariants pour un sous-groupe de S_n

Ce dernier chapitre couvre brièvement la construction des polynômes à plusieurs variables utilisés dans le chapitre précédent dans le but de générer ce que nous nommions le *stabilisateur*. De tels polynômes se nomment des *invariants* pour un certain sous-groupe de S_n. Nous allons nous limiter à présenter la méthode utilisée pour générer le polynôme dont F_{42} est le stabilisateur sous S_7 (voir chapitre 7) et nous allons décrire un algorithme non performant, mais qui assure un résultat valide. Finalement, nous joindrons l'algorithme efficace développé par I. Abdeljaouad dans un but informatif seulement.

Commençons par fixer un corps K dans lequel habiteront les coefficients de nos polynômes à n indéterminés et énonçons quelques définitions importantes.

Définition 8.0.1. La degré d'un polynôme de $K[X_1, \ldots, X_n]$ est le maximum des degrés de ses termes de somme. La degré d'un terme est la somme du degré de chacune de ses inconnues.

Définition 8.0.2. Pour chaque permutation $\sigma \in G \leq S_n$ et pour $F \in K[X_1, \ldots, X_n]$, nous définissons la notation $\sigma.F = F(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.

Définition 8.0.3. Un polynôme $F \in K[X_1, \ldots, X_n]$ est dit *H-invariant G-primitif* si $H = Stab(F, G)$ pour $H \leq G \leq S_n$. Si $G = S_n$, F est dit *H-invariant primitif*.

8.1 Intuition du degré 7

Dans le chapitre 7, nous avons déterminé que F_{42} était le stabilisateur du polynôme

$$\begin{aligned} F = &X_1(X_2 + X_3)X_4 + X_2(X_3 + X_4)X_5 + X_3(X_4 + X_5)X_6 + X_4(X_5 + X_6)X_7 \\ &+ X_5(X_6 + X_7)X_1 + X_6(X_7 + X_1)X_2 + X_7(X_1 + X_2)X_3 \end{aligned}$$

pour le groupe S_7. Ce polynôme n'est pas sorti de nulle part, sa construction étant intimement liée aux générateurs du stabilisateur. En effet, après avoir découvert que F_{42} est un bon candidat pour obtenir des listes de longueurs d'orbites convenables, nous devons déterminer un polynôme à 7 inconnues dont seuls les éléments de l'un des conjugués de F_{42} le rendent invariant primitif.

A priori, trouver un tel polynôme qui respecte une propriété d'invariance pour 42 permutations peut paraître difficile, mais il n'en est point. Il suffit de vérifier cette propriété pour les trois générateurs et comme toutes les permutations du groupe peuvent s'exprimer en fonction d'eux, alors tout élément stabilise le polynôme en question. Ces générateurs sont

$$\sigma = (2,3,5)(4,7,6),\ \tau = (2,7)(3,6)(4,5) \text{ et } \rho = (1,2,3,4,5,6,7).$$

La méthode imaginée est de choisir l'une de ces trois permutations et de la transformer en polynôme de la manière suivante :

$$\begin{gathered}(n_1^1, n_2^1, \ldots, n_{r_1}^1)(n_1^2, n_2^2, \ldots, n_{r_2}^2)\cdots(n_1^k, n_2^k, \ldots, n_{r_k}^k) \\ \downarrow \\ X_{n_1^1}X_{n_2^1}\cdots X_{n_{r_1}^1} + X_{n_1^2}X_{n_2^2}\cdots X_{n_{r_2}^2} + \cdots + X_{n_1^k}X_{n_2^k}\cdots X_{n_{r_k}^k}.\end{gathered}$$

Ce ne sont pas toutes les permutations qui font le travail. Effectivement, choisir ρ et la transformer en $X_1X_2\cdots X_7$ ne fonctionne pas ; n'importe quel élément de S_7 stabilise cette expression. Il faut plutôt transformer soit σ ou soit τ. Nous verrons qu'en fait, seulement l'un de ces éléments peut être utilisé.

La permutation σ se transforme en $\mathfrak{F}_1 = X_2X_3X_5 + X_4X_6X_7$ et τ donne $\mathfrak{F}_2 = X_2X_7 + X_3X_6 + X_4X_5$. Remarquons que ces deux polynômes sont stabilisés par les deux permutations qui ont servi à leur création. Donc, il ne reste plus qu'à modifier chacun d'eux de telle sorte que ρ les stabilise.

Pour ce faire, il suffit de faire la somme de chacun des éléments de l'orbite de ρ sur $\mathfrak{F}_i$ pour chaque i :

$$F_i = \mathfrak{F}_i + \rho.\mathfrak{F}_i + \rho^2.\mathfrak{F}_i + \ldots + \rho^6.\mathfrak{F}_i.$$

Les deux polynômes obtenus sont

$$\begin{aligned}F_1 = {} & (X_2X_3X_5 + X_4X_6X_7) + (X_3X_4X_6 + X_5X_7X_1) + (X_4X_5X_7 + X_6X_1X_2) + (X_5X_6X_1 \\ & + X_7X_2X_3) + (X_6X_7X_2 + X_1X_3X_4) + (X_7X_1X_3 + X_2X_4X_5) + (X_1X_2X_4 + X_3X_5X_6),\end{aligned}$$

$$\begin{aligned}F_2 = {} & (X_2X_7 + X_3X_6 + X_4X_5) + (X_3X_1 + X_4X_7 + X_5X_6) + (X_4X_2 \\ & + X_5X_1 + X_6X_7) + (X_5X_3 + X_6X_2 + X_7X_1) + (X_6X_4 + X_7X_3\end{aligned}$$

$$+ X_1X_2) + (X_7X_5 + X_1X_4 + X_2X_3) + (X_1X_6 + X_2X_5 + X_3X_4).$$

Malheureusement, seulement l'un d'eux est bel et bien un F_{42}-invariant primitif. Il s'agit de F_1 qui, à réécriture près, est celui utilisé dans la démarche du septième degré. De son côté, F_2 est stabilisé par S_7 au complet.

Cette intuition de construction ne fonctionne malheureusement pas toujours, comme nous avons pu le remarquer. Même que certains groupes n'ont aucun élément qui se transforme en un polynôme convenable. En effet, il est impossible de trouver un C_7-invariant primitif par cette méthode, car ce groupe est généré par $(1, 2, \ldots, 7)$, à conjugaison près, et que $X_1X_2 \ldots X_7$ est un S_7-invariant primitif, comme mentionné plus haut. Est-ce un hasard que cette méthode ait fonctionné dans ce cas-ci ? Peut-on modifier cette technique pour s'assurer d'avoir des invariants primitifs de degrés raisonnables à tout coup ? Nous ne répondons pas à ces questions, mais elles semblent accessibles à quiconque s'intéresse au sujet des polynômes invariants.

8.2 Algorithme naïf

L'intuition précédente n'est pas totalement étrangère. Il existe une méthode semblable qui fonctionne à tout coup, mais qui donne des polynômes de degrés relativement élevés.

Le principe est assez simple : nous commençons avec un polynôme $F \in K[X_1, \ldots, X_n]$ qui n'est stabilisé par aucun élément de S_n (hormis l'identité) (typiquement ce polynôme est $F = X_2X_3^2 \cdots X_n^{n-1}$), puis sommons l'image de ce dernier par tous les éléments du stabilisateur voulu.

Lemme 8.2.1 (Wilson [Wil50]). *Soit $H \leq S_n$ un groupe de permutations et soit $F = X_2X_3^2 \cdots X_n^{n-1} \in K[X_1, \ldots X_n]$. Alors*

$$\mathfrak{F} = \sum_{\sigma \in H} \sigma.F$$

est un H-invariant primitif.

La validité de ce lemme est claire par la construction de l'invariant. Le problème avec cette méthode est surtout que le degré de chaque terme est $n(n-1)/2$, ce qui peut relativement alourdir la performance des algorithmes présentés dans les chapitres précédents.

8.3 Algorithme de I. Abdeljaouad

L'auteur I. Abdeljaouad, dans son article *Calculs d'invariants primitifs de groupes finis*, construit un algorithme plutôt efficace qui trouve tous les H-invariants G-primitifs de de-

gré minimal [Abd99]. Son algorithme a été implémenté dans le système GAP [GAP13] en tant que *Package PrimitiveInvariant*. Nous présentons ici un bref aperçu des définitions et résultats qui mènent à l'élaboration de cette méthode plutôt judicieuse. Il est à noter que l'étude des invariants primitifs s'applique à un cadre beaucoup plus large qu'à celui de la théorie de Galois calculatoire.

Dans cette section, $G \leq S_n$ est un groupe de permutations de degré n et H est un sous-groupe de G.

Nous commençons par une longue série de définitions toutes aussi importantes les unes que les autres.

Définition 8.3.1. Un *monôme* de $K[X_1, \ldots, X_n]$ est un polynôme unitaire de la forme $X_1^{d_1} \cdots X_n^{d_n}$ où les d_i sont des entiers naturels possiblement nuls. Le *degré* d'un ensemble de tels monômes est le maximum des degrés de ceux-ci.

Définition 8.3.2. Soit $M \in K[X_1, \ldots, X_n]$ un monôme. Nous définissons la *trace réduite de M par H* comme étant le polynôme

$$Tr_H(M) = \sum_{P \in H.M} P$$

où $H.M$ est l'orbite de M sous l'action du groupe de permutation H.

La trace réduite de M par H a la propriété intéressante que son stabilisateur contient le groupe H [Abd99].

Définition 8.3.3. Soit E un ensemble fini de monômes de $K[X_1, \ldots, X_n]$. Nous notons

$$H_G(E) = \bigcap_{M \in E} Stab(Tr_H(M), G)$$

le *(G, H)-groupe de E*. Si $H_G(E) = H$, nous disons que E est un *ensemble essentiel pour* (G, H).

Les concepts de (G, H)-groupe d'un ensemble et d'ensemble essentiel jouent un rôle crucial dans le calcul de H-invariants G-primitifs comme nous le verrons un peu plus loin.

Définition 8.3.4. Soit E un ensemble fini de monômes de $K[X_1, \ldots, X_n]$. Une *E-fonction élémentaire* est le polynôme

$$\mathcal{P}_E = \sum_{P \in E} a_P Tr_H(P)$$

où les a_P sont des éléments non nuls deux à deux distincts du corps K.

Nous verrons que les fonctions élémentaires sont intimement liées aux invariants. Ces outils puissants ont des propriétés intéressantes lorsque utilisés sous les bonnes hypothèses.

Définition 8.3.5. Un *système de représentants des orbites de* H, que l'on note $\mathcal{S}$, est un ensemble de tous les monômes de $K[X_1, \ldots, X_n]$ dont les orbites sous l'action de H sont distinctes. Si nous précisons que $\mathcal{S}$ est un système de représentants des orbites de H *de degré* $\leq k$, alors chaque monôme est de degré $\leq k$.

Cette dernière définition est exactement le nœud du prochain algorithme. Nous y construisons le sous-ensemble d'un système de représentants des orbites de H de degré inférieur ou égal à $n(n-1)/2$.

La manœuvre `SystèmeReprésentants` consiste simplement à comparer les orbites sous l'action de H de toutes les paires de monômes de même degré. Chaque fois qu'une paire d'orbites coïncide, nous éliminons l'un des deux monômes.

Algorithme 8.1 Construction d'un système de représentants des orbites de H de degré inférieur ou égal à $n(n-1)/2$

Requis: H un sous-groupe de S_n et $\mathcal{A}$ l'ensemble (fini) de tous les monômes de $K[X_1, \ldots, X_n]$ de degrés $\leq n(n-1)/2$.

1: **Procédure:** SystèmeReprésentants($H, \mathcal{A}$)
2: **for** $M_1, M_2 \in \mathcal{A}$ **s.t.** deg(M_1) = deg(M_2) **do**
3: **if** $H.M_1 = H.M_2$ **then** $\mathcal{A} \leftarrow \mathcal{A} \backslash \{M_2\}$
4: **end if**
5: **end for**
6: **return** $\mathcal{A}$
7: **end Procédure:**

Comme l'ensemble de départ $\mathcal{A}$ contient un nombre fini de monômes, alors la boucle de la ligne 2 a nécessairement une fin. Dans cette même boucle, seulement les orbites de monômes de mêmes degrés sont comparées pour diminuer le nombre de vérifications. En effet, des monômes de degrés différents ont évidemment de différentes orbites sous l'action de H.

Le prochain algorithme détermine un ensemble essentiel de (G, H), s'il existe, à partir d'un sous-ensemble $\mathcal{A}$ de $\mathcal{S}$. Pour ce faire, la procédure `EnsembleEssentiel` commence avec un ensemble E qui ne contient que le monôme de degré nul. Tant et aussi longtemps que le (G, H)-groupe de E correspond à H, nous débarassons $\mathcal{A}$ de tous ses monômes de degré minimal et les ajoutons à E et la boucle recommence. Lorsque la condition de fin est atteinte, E est exactement un ensemble essentiel pour (G, H). Ultimement, $\mathcal{A}$ sera un système de représentants des orbites de H de degré plus petit ou égal à $n(n-1)/2$ et proviendra de l'algorithme 8.1.

Algorithme 8.2 Construction d'un ensemble essentiel E pour (G, H) à partir d'un sous-ensemble $\mathcal{A}$ de $\mathcal{S}$

Requis: $\mathcal{A}$ un sous-ensemble de $\mathcal{S}$, G un sous-groupe de S_n et H un sous-groupe de G.

1: **Procédure:** EnsembleEssentiel($\mathcal{A}, G, H$)
2: $E \leftarrow \{1\}$
3: **while** $H_G(E) \neq H$ **and** $\mathcal{A} \neq \emptyset$ **do**
4: $E \leftarrow E \cup \text{MIN}(\mathcal{A})$
5: $\mathcal{A} \leftarrow \mathcal{A} \backslash \text{MIN}(\mathcal{A})$
6: **end while**
7: **if** $\mathcal{A} \neq \emptyset$ **then return** E
8: **else return** « $\mathcal{A}$ ne contient pas d'ensemble essentiel pour (G, H) »
9: **end if**
10: **end Procédure:**

À la ligne 4, la notation $\min(\mathcal{A})$ désigne l'ensemble de tous les éléments de $\mathcal{A}$ de degré minimal. Remarquons que la construction 8.2 fait beaucoup plus que simplement donner un ensemble essentiel $E \subset \mathcal{A}$ pour (G, H). En effet, $E \subset \mathcal{A}$ est de degré minimal sous la condition de contenir tous les autres ensembles essentiels (contenus dans $\mathcal{A}$) de même degré.

Théorème 8.3.6 (Abdeljaouad)**.** *Soit E un ensemble fini de monômes de $K[X_1, \ldots, X_n]$. Toute fonction élémentaire $\mathcal{P}_E$ est un $H_G(E)$-invariant G-primitif.*

Corollaire 8.3.7. *Soit E un ensemble fini de monômes de $K[X_1, \ldots, X_n]$. Si E est un ensemble essentiel pour (G, H), alors $\mathcal{P}_E$ est un H-invariant G-primitif.*

Le corollaire 8.3.7 est très important. Il indique qu'un ensemble essentiel pour (G, H) est suffisant pour trouver des H-invariants G-primitifs. À l'aide de résultats intermédiaires, Abdeljaouad fait mieux et fortifie ce constat.

Corollaire 8.3.8. *Les ensembles essentiels pour (G, H) déterminent tous les H-invariants G-primitifs.*

La manœuvre `InvariantsPrimitifs` génère un système de représentants $\mathcal{A}$ à l'aide de la procédure 8.1 et l'utilise pour créer un ensemble essentiel E avec l'algorithme 8.2. Par la suite, une boucle vérifie si chaque sous-ensemble P de E est un ensemble essentiel *réduit* (ensemble essentiel qui ne contient aucun ensemble essentiel). La collection $\mathcal{I}$ de tous ceux-ci est ensuite converti en l'ensemble $\mathcal{T}$ de toutes les U-fonctions élémentaires pour chaque U dans $\mathcal{I}$. En vertu du corollaire 8.3.7, $\mathcal{T}$ est exactement la collection de tous les H-invariants G-primitifs de degré minimal.

À la ligne 5, la notation $\wp(E)$ désigne la liste de tous les sous-ensembles de E triés en ordre non décroissant selon leur cardinalité.

Algorithme 8.3 (Abdeljaouad) Énumération de la liste de tous les H-invariants G-primitifs de degré minimal

Requis: G un sous-groupe de S_n, H un sous-groupe de G et $\mathcal{A}$ l'ensemble (fini) de tous les monômes de $K[X_1, \ldots, X_n]$ de degrés $\leq n(n-1)/2$

1: **Procédure:** InvariantsPrimitifs($\mathcal{A}, G, H$)
2: $\mathcal{A} \leftarrow$ SystèmeReprésentants($H, \mathcal{A}$)
3: $E \leftarrow$ EnsembleEssentiel($\mathcal{A}, G, H$)
4: $\mathcal{I} \leftarrow \emptyset$ ▷ Ensemble des ensembles essentiels pour (G, H)
5: $\wp \leftarrow \wp(E)$
6: **for** $P \in \wp$ **do**
7: **if** $H_G(P) = H$ **then**
8: $\mathcal{I} \leftarrow \mathcal{I} \cup \{P\}$
9: **for** $Q \in \wp$ **s.t.** $P \subset Q$ **do**
10: $\wp \leftarrow \wp \backslash \{Q\}$
11: **end for**
12: **end if**
13: **end for**
14: $\mathcal{T} \leftarrow \emptyset$ ▷ Ensembles des H-invariants G-primitifs
15: **for** $U \in \mathcal{I}$ **do**
16: $\mathcal{T} \leftarrow \mathcal{T} \cup \{\mathcal{P}_U\}$
17: **end for**
18: **return** $\mathcal{T}$
19: **end Procédure:**

I. Abdeljaouad décrit une deuxième méthode qu'il nomme l'algorithme de *Girstmair-Jordan*, une version modifiée de la démarche élaborée par K. Girstmair qui utilise une représentation particulière des polynômes imaginée par C. Jordan.

Maintenant que nous avons sous la main un algorithme capable de trouver tous les H-invariants G-primitifs de degré minimal, le problème de trouver un polynôme (relativement simple) à n variables qui génère un stabilisateur prédéterminé est réglé. Cette dernière méthode n'est peut-être pas la plus optimale en terme de temps de calcul, mais au moins elle nous donne assurément une liste exhaustive de tous les polynômes qui nous intéressent.

Conclusion

Il existe une multitude de voies qui n'ont pas été empruntées lors de la rédaction de ce mémoire. Par exemple, S_8 pose problème avec ses nombreux sous-groupes transitifs (50 en tout). Il aurait par contre été possible de présenter un algorithme pour le degré 11, car il n'y a que 8 groupes transitifs de ce degré. En fait, la plupart des degrés premiers semblent comporter un nombre de groupes transitifs inférieur au degré et auraient donc été relativement simples à étudier.

Un sujet intéressant à traiter serait de donner des familles de polynômes ayant des groupes de Galois donnés. Par exemple, pour les polynômes de la forme $x^5 + ax + b$, déterminer des conditions sur les entiers relatifs a et b qui font en sorte que le groupe de Galois n'est pas S_5. En guise de compromis, l'annexe H donne un exemple de polynômes pour chaque groupe présenté dans le chapitre 4.

Additionnellement, nous aurions pu discuter des polygones de Newton qui donnent de l'information sur le groupe de Galois d'un polynôme. Plus particulièrement, ces objets nous transmettent de l'information sur la factorisation du polynôme.

Une autre avenue possible serait d'étudier les travaux de Matzat [Mat87]. Ce mathématicien a consacré plusieurs ouvrages sur l'aspect constructif du groupe de Galois d'un polynôme. Son cheminement l'amène inévitablement au problème inverse de la théorie de Galois : pour un groupe donné G et fixe, on veut exhiber un polynôme dont le groupe de Galois est G.

Hélas, l'étendue de la théorie de Galois est bien trop vaste pour être couverte par un seul mémoire de maîtrise !

Annexe A

Table de Cayley pour $D_6 \times C_2$

	id	σ	σ^2	σ^3	σ^4	σ^5	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$
id	id	σ	σ^2	σ^3	σ^4	σ^5	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$
σ	σ	σ^2	σ^3	σ^4	σ^5	id	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$
σ^2	σ^2	σ^3	σ^4	σ^5	id	σ	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$
σ^3	σ^3	σ^4	σ^5	id	σ	σ^2	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$
σ^4	σ^4	σ^5	id	σ	σ^2	σ^3	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$
σ^5	σ^5	id	σ	σ^2	σ^3	σ^4	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$
τ	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	id	σ	σ^2	σ^3	σ^4	σ^5	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	σ^5	id	σ	σ^2	σ^3	σ^4	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$
$\tau\sigma^2$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	σ^4	σ^5	id	σ	σ^2	σ^3	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$
$\tau\sigma^3$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	σ^3	σ^4	σ^5	id	σ	σ^2	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$
$\tau\sigma^4$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	σ^2	σ^3	σ^4	σ^5	id	σ	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$
$\tau\sigma^5$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	σ	σ^2	σ^3	σ^4	σ^5	id	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ
ρ	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	id	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$
$\rho\sigma$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	σ	σ^2	σ^3	σ^4	σ^5	id	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$
$\rho\sigma^2$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	σ^2	σ^3	σ^4	σ^5	id	σ	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
$\rho\sigma^3$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	σ^3	σ^4	σ^5	id	σ	σ^2	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$
$\rho\sigma^4$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	σ^4	σ^5	id	σ	σ^2	σ^3	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$
$\rho\sigma^5$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	σ^5	id	σ	σ^2	σ^3	σ^4	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ
$\rho\tau$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\rho\tau$	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	id	σ	σ^2	σ^3	σ^4	σ^5
$\rho\tau\sigma$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	id	σ	σ^2	σ^3	σ^4
$\rho\tau\sigma^2$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	σ^4	σ^5	id	σ	σ^2	σ^3
$\rho\tau\sigma^3$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	σ^3	σ^4	σ^5	id	σ	σ^2
$\rho\tau\sigma^4$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	σ^2	σ^3	σ^4	σ^5	id	σ
$\rho\tau\sigma^5$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	σ	σ^2	σ^3	σ^4	σ^5	id

Annexe B

Liste des permutations de C_5, D_5 et A_5

Groupe	**Permutations**
C_5	$id, (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2)$
D_5	$id, (2,5)(3,4), (1,2)(3,5), (1,2,3,4,5), (1,3)(4,5), (1,3,5,2,4), (1,4)(2,3),$ $(1,4,2,5,3), (1,5,4,3,2), (1,5)(2,4)$
A_5	$id, (3,4,5), (3,5,4), (2,3)(4,5), (2,3,4), (2,3,5), (2,4,3), (2,4,5), (2,4)(3,5),$ $(2,5,3), (2,5,4), (2,5)(3,4), (1,2)(4,5), (1,2)(3,4), (1,2)(3,5), (1,2,3),$ $(1,2,3,4,5), (1,2,3,5,4), (1,2,4,5,3), (1,2,4), (1,2,4,3,5), (1,2,5,4,3),$ $(1,2,5), (1,2,5,3,4), (1,3,2), (1,3,4,5,2), (1,3,5,4,2), (1,3)(4,5), (1,3,4),$ $(1,3,5), (1,3)(2,4), (1,3,2,4,5), (1,3,5,2,4), (1,3)(2,5), (1,3,2,5,4),$ $(1,3,4,2,5), (1,4,5,3,2), (1,4,2), (1,4,3,5,2), (1,4,3), (1,4,5), (1,4)(3,5),$ $(1,4,5,2,3), (1,4)(2,3), (1,4,2,3,5), (1,4,2,5,3), (1,4,3,2,5), (1,4)(2,5),$ $(1,5,4,3,2), (1,5,2), (1,5,3,4,2), (1,5,3), (1,5,4), (1,5)(3,4), (1,5,4,2,3),$ $(1,5)(2,3), (1,5,2,3,4), (1,5,2,4,3), (1,5,3,2,4), (1,5)(2,4)$

Annexe C

Définition d'un groupe de Frobenius

Soit G un groupe de permutations transitif qui agit sur un ensemble X. Le groupe G est dit de *Frobenius* si $Stab(x, G) \neq \mathbb{I}$ pour chaque $x \in X$ et si $Stab(x, G) \cap Stab(y, G) = \mathbb{I}$ pour tout choix de $x, y \in X$ avec $x \neq y$. Rappelons que $\mathbb{I} = \{id\}$.

Nous pouvons également dire que G est un groupe de Frobenius si et seulement si $H \neq \mathbb{I}$ est un sous-groupe propre de G tel que $H \cap g^{-1}Hg = \mathbb{I}$ pour tout $g \in G \backslash H$.

Soit $C = Stab(x, G)$ pour un $x \in X$ quelconque et soit $K = \mathbb{I} \cup \{g \in G \mid g.x \neq x, \ \forall x \in X\}$. Le groupe de Frobenius G peut être écrit comme $G = K \rtimes C$.

Annexe D

Table de Cayley pour le groupe F_{20}

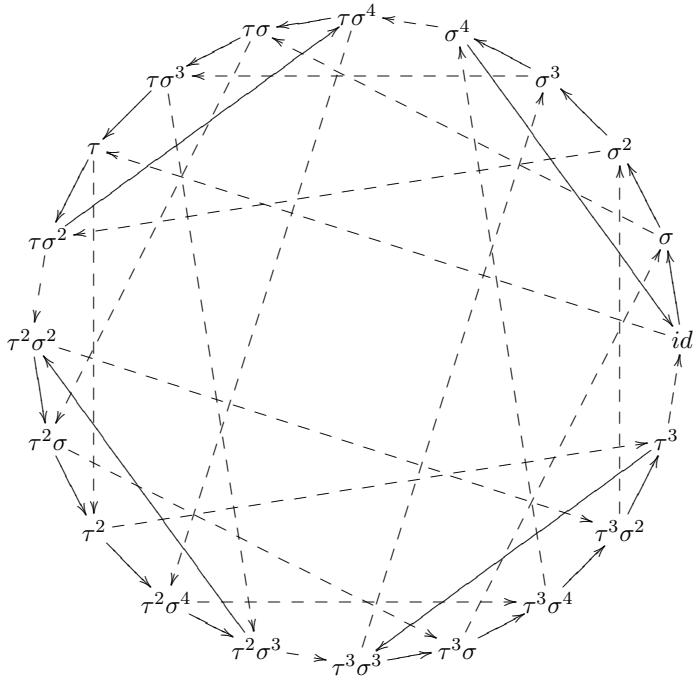
	id	σ	σ^2	σ^3	σ^4	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$
id	id	σ	σ^2	σ^3	σ^4	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$
σ	σ	σ^2	σ^3	σ^4	id	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$
σ^2	σ^2	σ^3	σ^4	id	σ	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3
σ^3	σ^3	σ^4	id	σ	σ^2	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$
σ^4	σ^4	id	σ	σ^2	σ^3	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$
τ	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	id	σ	σ^2	σ^3	σ^4
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	σ^3	σ^4	id	σ	σ^2
$\tau\sigma^2$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	σ	σ^2	σ^3	σ^4	id
$\tau\sigma^3$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	σ^4	id	σ	σ^2	σ^3
$\tau\sigma^4$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	σ^2	σ^3	σ^4	id	σ
τ^2	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	id	σ	σ^2	σ^3	σ^4	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$
$\tau^2\sigma$	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	σ^4	id	σ	σ^2	σ^3	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$
$\tau^2\sigma^2$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	σ^3	σ^4	id	σ	σ^2	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ
$\tau^2\sigma^3$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	σ^2	σ^3	σ^4	id	σ	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
$\tau^2\sigma^4$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	σ	σ^2	σ^3	σ^4	id	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$
τ^3	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	id	σ	σ^2	σ^3	σ^4	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$
$\tau^3\sigma$	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	σ^2	σ^3	σ^4	id	σ	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$
$\tau^3\sigma^2$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	σ^4	id	σ	σ^2	σ^3	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2
$\tau^3\sigma^3$	$\tau^3\sigma^3$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	σ	σ^2	σ^3	σ^4	id	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau\sigma$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$	$\tau^2\sigma^2$	$\tau^2\sigma^3$
$\tau^3\sigma^4$	$\tau^3\sigma^4$	τ^3	$\tau^3\sigma$	$\tau^3\sigma^2$	$\tau^3\sigma^3$	σ^3	σ^4	id	σ	σ^2	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	τ	$\tau^2\sigma^2$	$\tau^2\sigma^3$	$\tau^2\sigma^4$	τ^2	$\tau^2\sigma$

Note : F_{20} peut être vu comme le produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}$.

Annexe E

Bigraphe de Cayley pour le groupe F_{20}

Illustrons ici le bigraphe de Cayley pour le groupe F_{20}. Les flèches simples signifient une multiplication à gauche par σ et les flèches avec traits signifient une multiplication à gauche par τ.



Annexe F

Code SAGE du treillis des sous-groupes transitifs de degré n

```
def TransSubgrpLattice(n):
    G = SymmetricGroup(n)
    TCSG = [s for s in G.conjugacy_classes_subgroups() if s.is_transitive()]
    order_list = [order(s) for s in TCSG]
    length=len(TCSG)
    TCSGgens = [s.gens() for s in TCSG]
    CONJUGATES=[]
    print join(['TCSG complete'])
    for i in range(length):
        CONJUGATES.append([])
        for g in G:
            CONJ_GENS=[]
            for j in range(len(TCSGgens[i])):
                conj_ele = g*TCSGgens[i][j]*g^(-1)
                CONJ_GENS.append(conj_ele)
            if (not CONJ_GENS in c for c in CONJUGATES):
                CONJUGATES[i].append(CONJ_GENS)
        print join([str(i+1)+'/'+str(length)+' conjugated'])
    LATTICE=[]
    for i in range(length):
        LATTICE.append([])
        LATTICE[i].append(length-1-i)
        for j in range(length-1-i,length):
            if (not j in LATTICE[i]) and (order_list[j]/order_list[length-1-i] in ZZ) and (
    order_list[j] != order_list[length-1-i]):
                if any(all(b in TCSG[j] for b in k) for k in CONJUGATES[length-1-i]):
                    LATTICE[i].append(j)
                    for m in LATTICE[length-1-j]:
                        if not m in LATTICE[i]:
                            LATTICE[i].append(m)
        print join(['G'+str(length-1-i)+': '+join(['G'+str(s)+' ' for s in sorted(LATTICE[i]) ])
    +' ('+str(order(TCSG[length-1-i]))+')'])
```

Annexe G

Code SAGE de la liste des longueurs d'orbites des actions d'un sous-groupe de S_n sur $\{1, 2, \ldots, n\}$

```
def StabOrbitLengthList(G,STAB,SUBG):
    GH=G.cosets(STAB,side='left')
    GL=[]
    for k in range(len(SUBG)):
        GL.append([])
        for i in range(len(GH)):
            for j in range(len(GH)):
                if SUBG[k]*GH[i][0] in GH[j]:
                    GL[k].append(j+1)
    ORB=PermutationGroup(GL).orbits()
    print sorted([len(k) for k in ORB])
```

Annexe H

Exemples de polynôme pour chaque groupe de Galois de degré 5 à 7

Donnons ici des exemples de polynômes de degrés 5, 6 et 7 dont le groupe de Galois est donné par des groupes primitifs. Plusieurs exemples proviennent de [MM99].

Degré 5	
Groupe	**Polynôme**
C_5	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$
D_5	$x^5 - 5x + 12$
F_{20}	$x^5 + x^4 + 2x^3 + 4x^2 + x + 1$
A_5	$x^5 + x^4 - 2x^2 - 2x - 2$
S_5	$x^5 + x^3 + 1$

Degré 6	
Groupe	**Polynôme**
C_6	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
S_3	$x^6 + x^5 + 4x^4 + x^3 + 2x^2 - 2x + 1$
D_6	$x^6 + x^4 - 2x^3 + x^2 - x + 1$
A_4^*	$x^6 + x^4 - 2x^2 - 1$
G_{18}	$x^6 + x^4 - x^3 - 2x^2 + x + 1$
$A_4 \times C_2$	$x^6 + x^5 - 2x^3 + 2x - 1$

Degré 6 (suite)	
Groupe	**Polynôme**
S_4^*	$x^6 - x^2 - 1$
S_4	$x^6 + 2x^5 - x^4 - 4x^3 + 7x^2 - 4x + 1$
G_{36}	$x^6 - 2x^4 - 4x^3 + 6x^2 + 4x - 1$
G_{36}^*	$x^6 + x^5 + x^4 + x^3 - 4x^2 + 5$
$S_4 \times C_2$	$x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1$
$PSL_2^*(\mathbb{F}_5)$	$x^6 - 2x^5 + x^4 + 2x^3 + 2x^2 + 4x + 1$
G_{72}	$x^6 + x^5 - x^2 - x + 1$
$PGL_2(\mathbb{F}_5)$	$x^6 + 3x^4 - 2x^3 + 6x^2 + 1$
A_6^*	$x^6 - 2x^4 + x^2 - 2x - 1$
S_6	$x^6 - x^4 - x^3 + x + 1$

Degré 7	
Groupe	**Polynôme**
C_7	$x^7 - x^6 - 12x^5 + 7x^4 + 28x^3 - 14x^2 - 9x - 1$
D_7	$x^7 + x^6 + 2x^5 + 4x^3 + 2x + 1$
F_{21}	$x^7 - 8x^5 - 2x^4 + 16x^3 + 6x^2 - 6x - 2$
F_{42}	$x^7 + 2x^6 - 2x^5 - x^4 + 6x^3 - x + 4$
G_{168}	$x^7 - 7x + 3$
A_7	$x^7 + 2x^6 - 4x^4 - 5x^3 + 2x + 1$
S_7	$x^7 - 3x^3 + 3$

Bibliographie

[Abd99] I. Abdeljaouad. Calculs d'invariants primitifs de groupes finis. *Theor. Inform. Appl.*, 33(1) :59–77, 1999.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. Springer-Verlag, 1993.

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra.* Wiley, 2004.

[GAP13] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.6.4*, 2013.

[Mat87] B.H. Matzat. *Konstruktive Galoistheorie.* Lecture Notes in Mathematics. Springer, 1987.

[MM99] G. Malle and B.H. Matzat. *Inverse Galois Theory.* Monographs in Mathematics. Springer, 1999.

[Neu67] J. Neubüser. Die untergruppenverbande der gruppen der ordnungen ≤ 100 mit ausnahme der ordnungen 64 und 96. Habilitationsschrift, Universität Kiel, Kiel, Germany, 1967.

[S+12] W.A. Stein et al. *Sage Mathematics Software (Version 5.1).* The Sage Development Team, 2012. http ://www.sagemath.org.

[Soi81] L.H. Soicher. The Computation of Galois Groups. Master's thesis, Concordia University, Montréal, Canada, 1981.

[The12] The PARI Group, Bordeaux. *PARI/GP, version 2.5.1*, 2012. http ://pari.math.u-bordeaux.fr/.

[vdW60] B. L. van der Waerden. *Algebra : Volume I.* Springer-Verlag, New York, 1960.

[Wil50] R.L. Wilson. A method for the determination of the Galois group. *Duke Math. J.*, 17 :403–408, 1950.