N°d'ordre : 2450

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Bill ALLOMBERT

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

Théorie de Galois effective pour les corps de nombres et les corps finis. Développement du système PARI.

Soutenue le 13 décembre 2001.

Après avis de :

MM.	D. J. BERNSTEIN, Professeur, Université d'Illinois.	**Rapporteurs**
	J-M. COUVEIGNES, Professeur, Université Toulouse II.	
	B. H. MATZAT, Professeur, Université d'Heidelberg.	

Devant la commission d'examen formée de :

MM.	P. ZIMMERMANN, Directeur de Recherche, INRIA Lorraine	**Président**
	M. OLIVIER, Professeur, Université Bordeaux 1	**Rapporteur**
	H. COHEN, Professeur, Université Bordeaux 1	**Examinateurs**
	J-M. COUVEIGNES, Professeur, Université Toulouse II	
	F. DIAZ Y DIAZ, Professeur, Université Bordeaux 1	
	B. H. MATZAT, Professeur, Université d'Heidelberg	

- 2001 -

Chapitre 1

Représentation des nombres algébriques

> C'est vrai, 13 bis, est-ce un nombre pair ou un nombre impair ? Bah ! Voilà qui m'importe peu. En tout cas, c'est un nombre mauve.
> Raymond Queneau, *Le vol d'Icare*

1.1 Représentation polynomiale

1.1.1 Représentation des éléments d'un corps de nombres

Nous nous intéressons à la représentation des nombres algébriques appartenant à une extension finie $K/\mathbb{Q}$ du corps des rationnels. Nous supposons que K est le corps de rupture d'un polynôme irréductible T unitaire, à coefficients entiers. Soit $\alpha \in K$ une racine de T. Nous avons l'isomorphisme

$$\iota \left| \begin{array}{ccc} \mathbb{Q}[X]/(T) & \longrightarrow & K \\ \overline{P} & \longmapsto & P(\alpha) \end{array} \right.$$

Nous pouvons donc représenter un élément $\beta \in K$ par une classe de polynômes $\iota^{-1}(\beta)$ modulo T. Comme il s'agit d'un isomorphisme, les opérations algébriques sur les éléments de K se traduisent directement en opérations algébriques sur les classes de polynômes.

1.1.2 Représentation de l'anneau des entiers d'un corps de nombres

Soit $\mathbb{Z}_K$ l'anneau des entiers de K, et $\mathbb{Z}[\alpha]$ l'image de $\mathbb{Z}[X]$ par ι. Le polynôme T étant supposé unitaire, α est un entier algébrique donc $\mathbb{Z}[\alpha] \subset \mathbb{Z}_K$.

Le quotient de groupes abéliens $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ est fini, notons d son exposant, c'est-à-dire, le plus petit entier non-nul tel que $d\mathbb{Z}_K/\mathbb{Z}[\alpha] = 0$. L'entier d a la propriété suivante : c'est le plus petit entier tel que si $\beta \in K$ est entier algébrique, alors $d\beta \in \mathbb{Z}[\alpha]$.

1.1.3 Calcul d'un dénominateur commun pour les entiers algébriques

Les algorithmes Round 2 et Round 4 de H. Zassenhaus permettent le calcul exact du dénominateur d précédent, cependant ils nécessitent la factorisation du discriminant du polynôme, qui n'est pas réalisable en pratique. Inversement, le discriminant D du polynôme T est toujours un multiple de d, mais il est beaucoup plus grand que d, ce qui rend son utilisation peu commode.

Pour contourner ces difficultés, nous proposons une méthode heuristique pour trouver un petit multiple de d.

Nous utilisons trois remarques:

- Le dénominateur d divise par définition l'index $[\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ qui est le cardinal du groupe $\mathbb{Z}_K/\mathbb{Z}[\alpha]$. Or le carré de l'index divise le discriminant D de T et donc $v_p(d) \leq \frac{v_p(D)}{2}$,
- Le dénominateur d divise l'exposant du groupe abélien $\mathbb{Z}[\alpha]/T'(\alpha)\mathbb{Z}[\alpha]$ qui est appelé discriminant réduit (voir [FoLe]). Comme le calcul du discriminant réduit peut être long, il est préférable de le faire modulo les facteurs primaires du discriminant D.
- Seuls les petits nombres premiers peuvent diviser D avec un grand exposant.

Nous résumons la méthode dans l'algorithme suivant.

Algorithme 1.1.1 *Nous supposons avoir calculé tout les nombres premiers inférieurs à une borne P, que nous pouvons prendre en pratique égale à* 500000. *Nous calculons un multiple du dénominateur d ainsi.*

1. [Factorisation partielle] *Factoriser partiellement D en éliminant tous les facteurs premiers inférieurs à P. Nous écrivons*

$$D = U^u \prod_{i=1}^{n} p_i^{e_i}$$

où les p_i sont premiers et ne divisent pas U, et U n'est pas un carré parfait.

2. [Discriminant réduit] *Pour chaque $1 \leq i \leq n$ nous calculons le discriminant réduit δ_i de T modulo $p_i^{[\frac{e_i}{2}]}$.*

3. [Traitement du reste U] *Nous posons* $\delta_u = U^{[\frac{u+1}{2}]}$.

4. [Produit] *Nous retournons le produit*

$$\delta_u \prod_{i=1}^{n} \delta_i \quad .$$

1.1.4 Représentation des morphismes

Nous nous donnons deux corps de nombres K_1 et K_2, donnés comme corps de rupture d'un polynôme irréductible à coefficients entiers T_1 (resp. T_2). Notons α_i une racine de T_i dans K_i et ι_i l'isomorphisme

$$\iota_i \left| \begin{array}{ccc} \mathbb{Q}[X]/(T_i) & \longrightarrow & K_i \\ \overline{P} & \longmapsto & P(\alpha_i) \end{array} \right. ,$$

pour $i \in \{1, 2\}$. Nous souhaitons représenter un morphisme de corps $\mu : K_1 \longrightarrow K_2$. Soit M un polynôme, alors l'application

$$m_M \left| \begin{array}{ccc} \mathbb{Q}[X]/(T_1) & \longrightarrow & \mathbb{Q}[X]/(T_2) \\ \overline{P} & \longmapsto & \overline{P \circ M} \end{array} \right.$$

est bien définie si et seulement si $T_2 \mid T_1 \circ M$, et dans ce cas m_M est un morphisme de corps.

Choisissons maintenant

$$M = (\iota_2^{-1} \circ \mu \circ \iota_1)(\overline{X}) \in \mathbb{Q}[X] \quad ,$$

alors m_M et μ sont deux morphismes qui coïncident sur le générateur α_1 de K_1, ils sont donc égaux.

Les morphismes entre K_1 et K_2 sont en bijection avec les classes modulo T_2 de polynômes M vérifiant $T_2 \mid T_1 \circ$. Tous les morphismes entre K_1 et K_2 sont injectifs, de plus ce sont des isomorphismes si et seulement si K_1 et K_2 ont même degré.

1.2 Représentation des nombres algébriques par conjugués ℓ–adiques

1.2.1 Conjugué ℓ-adique

Nous souhaitons proposer une représentation modulaires des nombres algébriques. Soit K un corps de nombres comme précédemment et v une place

de $\mathbb{Q}$. Soit $(w_i)_{i=1}^g$ les places de K au-dessus de v. Notons K_{w_i} le complété de K pour la valuation w_i, et σ_i le plongement naturel de K dans le complété K_{w_i}.

Nous avons le morphisme injectif

$$\Gamma \left| \begin{array}{ccc} K & \longrightarrow & \prod_{i=1}^g K_{w_i} \\ \alpha & \longmapsto & (\sigma_i(\alpha))_{i=1}^g \end{array} \right. .$$

Si $\beta \in K$, l'image $\Gamma(\beta)$ est appelée *vecteur conjugué* de β. Nous nous contenterons ici de traiter le cas où v est une place finie correspondant à un nombre premier ℓ, le cas des places infinies étant classique (voir [Cohen, section 4.2.4]).

Nous notons $(\ell) = \prod_{i=1}^g \mathfrak{L}_i^{e_i}$ la factorisation de ℓ en produit d'idéaux premiers, indexée de sorte que $w_i = v_{\mathfrak{L}_i}$.

Soit e un entier strictement positif. Nous introduisons le morphisme

$$\Gamma_e \left| \begin{array}{ccc} \mathbb{Z}_K & \longrightarrow & \prod_{i=1}^g \mathbb{Z}_K/\mathfrak{L}_i^{e_i e} \\ \alpha & \longmapsto & (\alpha \pmod{\mathfrak{L}_i^{e_i e}})_{i=1}^g \end{array} \right. .$$

Le noyau de Γ_e est (ℓ^e). Γ_e est une approximation modulo ℓ^e de Γ.

1.2.2 Représentation simplifiée

Nous ajoutons l'hypothèse que ℓ ne divise pas le discriminant D de T. Cela implique que ℓ n'est pas ramifié dans $K/\mathbb{Q}$, et donc les exposants e_i valent tous 1.

Soit $T = \prod_{i=1}^g T_i \pmod{\ell}$ la factorisation de T modulo ℓ, que nous indexons pour que $T_i(\alpha) \in \mathfrak{L}_i$. Nous aurons besoin ultérieurement d'une base d'idempotents modulo ℓ, c'est-à-dire une famille $(U_i)_{i=1}^g$ de polynômes telle que pour tout couple $(i,j) \in \{1,\ldots,g\}^2$ nous ayons

$$U_i \equiv \delta_{i,j} \pmod{T_j, \ell} .$$

Par le procédé de relèvement de Hensel, il est possible de relever cette factorisation en une factorisation

$$T = \prod_{i=1}^g T_i \pmod{\ell^e}$$

et simultanément la famille $(U_i)_{i=1}^g$ en une base d'idempotents modulo ℓ^e, vérifiant pour tout couple $(i,j) \in \{1,\ldots,g\}^2$,

$$U_i \equiv \delta_{i,j} \pmod{T_j, \ell^e} .$$

Ainsi nous avons pour $1 \leq i \leq g$ un isomorphisme θ_i entre $\mathbb{Z}_K/\mathfrak{L}_i^e$ et $\mathbb{Z}[X]/(T_i, \ell^e)$ défini par

$$\theta_i \left| \begin{array}{ccc} \mathbb{Z}[X]/(T_i, \ell^e) & \longrightarrow & \mathbb{Z}_K/\mathfrak{L}_i^e \\ \overline{P} & \longmapsto & P(\alpha) \pmod{\mathfrak{L}_i^e} \end{array} \right. .$$

Nous introduisons le morphisme Θ_e défini par

$$\Theta_e \left| \begin{array}{ccc} \mathbb{Z}_K & \longrightarrow & \prod_{i=1}^g \mathbb{Z}[X]/(T_i, \ell^e) \\ \alpha & \longmapsto & (\theta^{-1}(\alpha \pmod{\mathfrak{L}_i^e}))_{i=1}^g \end{array} \right.$$

Ce morphisme nous permet donc de représenter un élément $\beta \in \mathbb{Z}_K$ par un élément de l'algèbre produit $\prod_{i=1}^g \mathbb{Z}[X]/(T_i, \ell^e)$, pour laquelle les opérations algébriques sont très simples et très rapides, car modulaires.

1.2.3 Représentation des morphismes

Soit $\mu : K \longrightarrow L$ un morphisme de corps entre deux corps de nombres K et L.

Soit v une place de $\mathbb{Q}$, notons $(v_i)_{i=1}^g$ les places de K au-dessus de v, et $(w_i)_{i=1}^h$ les places de L au-dessus de v. Notons K_{v_i} les complétés de K pour les valuations v_i, et σ_i les plongements naturels de K dans K_{v_i} correspondants.

De même, nous notons L_{w_i} les complétés de L pour les valuations w_i, et τ_i les plongements naturels de L dans L_{w_i} correspondants.

Nous souhaitons expliquer comment à partir d'un vecteur conjugué $\Gamma_K(\alpha)$ obtenir le vecteur conjugué $\Gamma_L(\mu(\alpha))$.

Remarquons d'abord que $w_i \circ \mu$ est une place de K. Nous construisons une application

$$\psi \left| \begin{array}{ccc} \{1, \ldots, h\} & \longrightarrow & \{1, \ldots, g\} \\ i & \longmapsto & j \text{ tel que } w_i \circ \mu = v_j \end{array} \right.$$

Nous remarquons que pour tout $1 \leq i \leq h$, les plongements $\sigma_{\psi(i)}$ et $\tau_i \circ \mu$ ont même image. Il existe donc un automorphisme φ_i de $K_{v_{\psi(i)}}$ tel que

$$\varphi_i \circ \sigma_{\psi(i)} = \tau_i \circ \mu$$

Cette identité nous permet effectivement de calculer $\Gamma_L(\mu(\alpha))$ en fonction de $\Gamma_K(\alpha)$. Ainsi un morphisme peut être entièrement spécifié par une fonction ψ et une suite d'automorphismes locaux φ.

1.2.4 Comment choisir le nombre premier ℓ

Nous avons choisi précédemment de nous restreindre aux places non-archimédiennes. Une justification est que l'arithmétique flottante (ou à virgule fixe) entraînant une perte de précision lors de chaque opération arithmétique, il est souvent difficile de contrôler l'exactitude des résultats.

Du point de vue de l'efficacité, le coût d'une addition de deux vecteurs conjugués est indépendant de ℓ. Par contre, les multiplications sont plus rapides lorsque les degrés résiduels sont faibles, en effet la complexité de la multiplication modulaire est super-linéaire. Il est donc préférable de choisir un nombre premier ℓ tel que le nombre d'idéaux g au-dessus de ℓ soit grand.

Le théorème de Čebotarev donne la densité de nombre premiers ayant des degrés résiduels fixés en fonction du groupe de Galois de la clôture normale de K. Si le corps de nombres est galoisien, il est toujours possible en pratique de trouver un nombre ℓ totalement décomposé, par essais successifs. C'est souvent le meilleur choix.

Dans le cas général, la faible densité des places finies totalement décomposées peut rendre leur détermination et/ou leur utilisation impraticable. Cependant, en fonction du groupe de Galois de la clôture normale de K, le théorème de Čebotarev permet en pratique de choisir une solution presque optimale.

Il est aussi possible de choisir ℓ de sorte que les automorphismes de Frobenius liés aux idéaux premiers au-dessus de ℓ aient certaines propriétés. C'est cette technique qui nous permettra des calculer les automorphismes de corps de nombres.

1.3 Retour à la représentation polynomiale

En pratique, nous avons un ensemble d'opérations algébriques à effectuer, et nous avons une borne *a priori* B sur le résultat final. Nous souhaitons en obtenir la représentation polynomiale.

1.3.1 Lorsque le résultat est entier

Nous savons a priori que le résultat final n est un entier. Dans ce cas, toutes les composantes de $\Gamma(n)$ sont égales, et comme les calculs sont effectués composante par composante, il est suffisant de calculer seulement la première composante $\sigma_1(n)$. Supposons connue une borne a priori B sur le résultat et choisissons e tel que $\ell^e > 2B$, alors il suffit de prendre le représentant de $\sigma_1(n)$ dans l'intervalle $]-\ell^e/2, \ell^e/2]$ pour obtenir n.

1.3.2 Lorsque le résultat est rationnel

Nous savons a priori que le résultat final p/q est un rationnel. Il suffit ici aussi de calculer la première composante $\sigma_1(p/q)$. Nous avons besoin ici de connaître a priori une borne B sur p et un multiple $D > 0$ de q. Nous appliquons la méthode précédente à l'entier $n = Dp/q$ qui est inférieur à BD, et nous obtenons p/q en calculant n/D.

Il existe un procédé appelé *reconstruction des rationnels* ([CoEn]), qui nécessite seulement une borne B_1 sur p et B_2 sur q. Il permet de reconstruire p/q à l'aide d'une approximation modulo $\ell^e > 2B_1B_2$.

La difficulté pratique est qu'il est rarement possible d'obtenir une borne sur q qui soit meilleure qu'un multiple connu, et dans ce cas la première méthode est plus rapide. Par contre elle est très utile lorsque l'on calcule des approximations successives et que l'on a un critère pour décider si le résultat obtenu est correct. Dans ce cas nous pouvons procéder de la manière heuristique suivante:

1. Supposons connus B et D comme précédemment.
2. Nous calculons une suite d'approximation jusqu'à la précision $\ell^e > 2BD$.
3. À partir de chaque approximation, nous déterminons par reconstruction des rationnels, un nombre p'/q'.
4. Nous vérifions si $q' \mid D$, dans ce cas nous vérifions si le résultat est correct, si oui nous arrêtons le calcul et retournons le résultat p'/q'.
5. Nous continuons avec la prochaine approximation.

Comme en général le multiple connu D est beaucoup plus grand que le dénominateur, cette stratégie est très supérieure. De plus le test $q' \mid D$ évite la plupart des vérifications.

1.3.3 Lorsque le résultat est un nombre algébrique

Le résultat est un nombre algébrique que nous souhaitons exprimer comme polynôme par rapport à un élément primitif α de K, que nous supposerons entier algébrique. Nous devons connaître une borne *a priori* sur les coefficients du polynôme cherché, et un multiple $D > 0$ des dénominateurs. Nous nous donnons un nombre premier ℓ ne divisant ni D, ni le discriminant $\mathrm{Disc}(T)$.

Soit donc $\beta = \frac{P(\alpha)}{D}$ un élément de K et nous supposons que P est de degré strictement inférieur au degré de T et est à coefficients entiers, inférieurs à B en valeur absolue.

Nous nous donnons l'image $\Theta_e(\beta) = (B_i)_{i=1}^{g}$ d'un nombre algébrique β et nous supposons que $\ell^e > 2BD$. Nous souhaitons retrouver P.

Nous allons utiliser ici la base $(U_i)_{i=1}^g$ d'idempotents modulo ℓ^e . Nous rappelons qu'elle vérifie pour tout couple $(i,j) \in \{1,\ldots,g\}^2$

$$U_i \equiv \delta_{i,j} \pmod{T_j, \ell^e} \ .$$

L'élément

$$Q = \sum_{i=1}^{g} B_i U_i$$

vérifie pour tout $i \in \{1,\ldots,g\}$

$$Q \equiv B_i \pmod{T_i, \ell^e}$$

Comme cette relation est aussi vérifiée par P/D, nous avons

$$Q \equiv P/D \pmod{T, \ell^e} \ .$$

Comme Q et P/D sont tous deux de degrés strictement inférieurs au degré de T nous en déduisons

$$Q \equiv P/D \pmod{\ell^e}$$

et nous pouvons déterminer chaque coefficient de P/D à l'aide des techniques de la section précédente.

1.3.4 Lorsque la place v est totalement décomposée

Nous avons vu précédemment qu'il était préférable de prendre une place totalement décomposée pour que l'arithmétique sur les plongements naturels soit plus rapide. De plus les calculs de la section précédente se simplifiant dans ce contexte, il nous a paru intéressant de les détailler.

Notons d'abord que les composantes de $\Theta_e(\beta) = (B_i)_{i=1}^g$ sont des polynômes de degré 0, donc représentables par des entiers.

Nous noterons $(\alpha_i)_{i=1}^n$ les racines de T dans $\mathbb{Q}_\ell$. Remarquons d'abord que T se factorise en

$$T = \prod_{i=1}^{n} (X - \alpha_i)$$

et par le théorème de Lagrange nous pouvons choisir

$$\begin{aligned} U_i &= \prod_{j \neq i} \frac{X - \alpha_j}{\alpha_i - \alpha_j} && (1.1) \\ &= T(X)/T'(\alpha_i)(X - \alpha_i) && (1.2) \end{aligned}$$

Nous remarquerons que les U_i forment les lignes de l'inverse M de la matrice de van der Monde (α_i^{j-1}). Les coefficients du polynôme

$$Q = \sum_{i=1}^{g} B_i U_i$$

sont simplement les composantes du vecteur $M(b_1, \ldots, b_n)^t$.

Chapitre 2

Application à la théorie de Galois

2.1 Calcul des extensions abéliennes du corps des rationnels par somme de Gauss

Comme première application de la représentation par conjugués ℓ–adiques, nous allons déterminer des polynômes définissant les extensions abéliennes des rationnels.

Soit $K/\mathbb{Q}$ une extension abélienne définie par la partie finie du conducteur f et un sous-groupe H de $G = (\mathbb{Z}/f\mathbb{Z})^*$. Notons ζ_f une racine primitive f-ième de l'unité et $\mathbb{Q}(\zeta_f)$ le f-ième corps cyclotomique. Ainsi, le corps K est le corps fixe de $\mathbb{Q}(\zeta_f)$ par H.

Nous utiliserons la proposition suivante (voir [AdLe]):

Proposition 2.1.1 *Kummer Sous les hypothèses précédentes, la trace de ζ_f sur K engendre K.*

La trace de ζ_f sur K est égale à la somme de Gauss

$$\gamma = \sum_{a \in H} \zeta_f^a \ .$$

Plus précisément, notons G/H l'ensemble des classes à gauche de G par H, et pour $C \in G/H$, notons

$$\gamma_C = \sum_{a \in C} \zeta_f^a \ .$$

Les nombres γ_C sont les conjugués de γ et le polynôme minimal de γ est

$$T = \prod_{C \in G/H} (X - \gamma_C) \ .$$

Le problème algorithmique consiste donc à calculer le polynôme T. Soit ℓ un nombre premier $\ell \equiv 1 \pmod{f}$. Ainsi le corps $\mathbb{Q}_\ell$ contient les racines ℓ-ièmes de l'unité.

Pour appliquer les résultats précédents nous avons besoin d'une borne sur les coefficients de T. Écrivons

$$T = \sum_{i=0}^{d} t_i X^i \ ;$$

en notant d le degré de T et $n = \operatorname{Card} G/H$, nous avons

$$t_i = \sum_{\substack{A \subset G/H \\ \operatorname{Card} A = d-i}} (-1)^{d-i} \prod_{C \in A} \gamma_C \ .$$

De façon évidente nous avons $|\gamma_C| \leq n$, et donc

$$|t_i| \leq \left(\begin{array}{c} d \\ d-i \end{array} \right) n^i \ .$$

De plus la quantité $\left(\begin{array}{c} d \\ d-i \end{array} \right) n^i$ étant maximale pour i valant $m = d - \left[\frac{1+d}{1+n}\right]$, nous pouvons prendre pour borne

$$B = \left(\begin{array}{c} d \\ d-m \end{array} \right) n^m \ .$$

Nous avons donc à calculer les racines f-ième de l'unité dans $\mathbb{Q}_\ell$ modulo $\ell^e > 2B$, puis à calculer ainsi T modulo ℓ^e. Chaque coefficient étant entier et inférieur à B, il est possible de reconstituer le polynôme T.

Algorithme 2.1.2 *Soit f_0 un entier et H_0 un sous-groupe de $(\mathbb{Z}/f_0\mathbb{Z})^*$. Nous déterminons un polynôme définissant le corps fixe $\mathbb{Q}(\zeta_{f_0})^{H_0}$ ainsi.*

1. [Calcul du conducteur] *Calculer la partie finie du conducteur f de l'extension abélienne $\mathbb{Q}(\zeta_f)^H$ et l'image H de H_0 dans $G = (\mathbb{Z}/f_0\mathbb{Z})^*$.*
2. [Choix de ℓ] *Déterminer un nombre premier $\ell \equiv 1 \pmod{f}$.*
3. [Calcul de B et e] *Calculer la borne B et e tel que $\ell^e > 2B$.*
4. [Calcul de ζ_f] *Calculer une racine primitive f-ième de l'unité modulo ℓ^e dans $\mathbb{Q}_\ell$.*
5. [Calcul de G/H] *Calculer l'ensemble G/H des classes à gauche de G par H.*
6. [Calcul des γ_C] *Pour chaque classe $C \in G/H$, calculer $\gamma_C = \sum_{a \in C} \zeta_f^a$.*

7. [Calcul de T modulo ℓ^e] *Calculer T modulo ℓ^e à l'aide de l'identité*

$$T = \prod_{C \in G/H} (X - \gamma_C) \ .$$

8. [Détermination de T] *Recouvrer T.*

Cet algorithme ne permet pas de faire le calcul si le conducteur est grand, par contre il peut calculer des extensions de degré arbitraire et retourne dans tous les cas un polynôme avec des coefficients raisonnables. Il existe un autre algorithme utilisant la théorie de Kummer qui permet de traiter des conducteurs élevés, mais uniquement pour obtenir des extensions de petits degrés. De plus, il retourne habituellement un polynôme avec de très gros coefficients.

2.2 Calcul de corps fixes

La connaissance du groupe de Galois d'une extension L/K permet le calcul explicite des sous-corps.

Nous utilisons le résultat suivant qui résulte de [KlMa].

Proposition 2.2.1 *Soit L/K une extension galoisienne de degré n, et α_0 un élément primitif pour cette extension. Soit $\mathcal{A}$ l'ensemble des conjugués de α_0 dans L. Soit $G = \mathrm{Gal}(L/K)$ son groupe de Galois et H un sous-groupe d'ordre h. Soit $\{O_i;\ i = 1 \text{ à } k\}$ l'ensemble des orbites de $\mathcal{A}$ sous l'action de H. Soit Σ un polynôme symétrique en h indéterminées et à coefficients entiers. Posons pour $1 \leqslant i \leqslant k$*

$$r_i = \Sigma(o_1, o_2, \ldots, o_h) \ \text{où}\ O_i = \{o_1, o_2, \ldots, o_h\}$$

et

$$R = \prod_{i=1}^{k} (X - r_i) \ .$$

Supposons le polynôme R sans facteurs carrés. Alors R est un polynôme unitaire, irréductible et une racine de R engendre le corps fixe K^σ. Il existe exactement un polynôme M de degré au plus $n-1$ tel que, pour tout $1 \leqslant i \leqslant k$ et pour tout $\alpha \in O_i$, nous ayons $M(\alpha) = r_j$. De plus, si $T = \prod_{\alpha \in \mathcal{A}}(X - \alpha)$, le polynôme M vérifie $T \mid R \circ M$ et il définit l'inclusion de L^H dans L.

Pour appliquer ce résultat effectivement, nous avons besoin d'approximation des conjugués de α_0 dans un corps local (ou éventuellement le corps

des complexes) et de trouver un polynôme symétrique Σ tel que le polynôme R en résultant est sans facteur carré. Nous avons de plus les compléments suivants:

Proposition 2.2.2 *Sous les hypothèses et notations de la proposition 2.2.1, si $\tau \in G$ est un automorphisme, nous avons $\tau(r_i) = r_j$ si et seulement si $\tau(O_i) = O_j$.*

Proposition 2.2.3 *Supposons que $K = \mathbb{Q}$, et soit p un nombre premier ne divisant pas le discriminant de T. Soit e un entier strictement positif. Soit H un sous-groupe de G qui laisse fixes les idéaux de L au-dessus de p. Sous les hypothèses et notations de la proposition 2.2.1, nous notons $T = \prod_{i=1}^{g} T_i \pmod{p^e}$ la factorisation de T en produit de polynômes irréductibles modulo p^e. Pour $1 \leq i \leq g$ nous notons R_i le polynôme minimal de $M \pmod{T_i, p^e}$, alors*

$$R = \prod_{i=1}^{g} R_i \pmod{p^e}$$

est la factorisation de R en produit de polynômes irréductibles modulo p^e. De plus si β est une racine de R dans L^H, l'idéal premier $(p, T_i(\alpha))$ de L est au-dessus de l'idéal premier $(p, R_i(\beta))$. De plus si $\tau \in G$, nous avons $\tau((p, T_i(\alpha))) = \tau((p, T_j(\alpha)))$ si et seulement si $\tau((p, R_i(\beta))) = \tau((p, R_j(\beta)))$

Pour des raisons d'efficacité, il est préférable de trouver un polynôme Σ de petit degré. De plus il est souvent souhaitable que R soit sans facteur carré modulo un ou plusieurs nombres premiers. En pratique nous utilisons l'algorithme heuristique suivant:

Algorithme 2.2.4 *Sous les hypothèses et notation de la proposition 2.2.1, nous notons par σ_j le polynôme de Newton*

$$\sigma_j((x_i)_{i=1}^{n}) = \sum_{i=1}^{n} x_i^j$$

Nous dirons qu'un ensemble S de polynômes sépare un ensemble de points E, si pour tout couple de points distincts de E, il existe un polynôme de S ayant une valeur différente sur les deux points.

1. [Initialisation] *Initialiser m à 1.*

2. [Séparation] *Tant que l'ensemble $\{\sigma_1, \ldots, \sigma_m\}$ ne sépare pas $\mathcal{A}$, incrémenter m*

3. [Boucle] *Poser $\Sigma = \sigma_m$. Pour $1 \leq j \leq 2m - 1$, exécuter les étapes suivantes.*

3.1. [Test] *Calculer le polynôme R correspondant à Σ. Si R est sans facteur carré et satisfait également les conditions locales imposées, retourner R.*

3.2. [Nouveau polynôme] *Ajouter* $\sigma_j \pmod m$ *à* Σ.

4. [Retour] *Incrémenter* m *et revenir à l'étape 3.*

2.3 Factorisation Galoisienne

La théorie de Galois nous permet d'obtenir directement la factorisation d'un polynôme définissant une extension galoisienne sur un sous-corps.

Lemme 2.3.1 (Factorisation Galoisienne) *Soit L/F une extension Galoisienne, et $\alpha \in L$ un élément primitif de l'extension. Soit T le polynôme minimal de α sur F. Soit K/F une extension algébrique de F. Pour chaque classe à gauche $C \in \mathrm{Gal}(L/F)/\mathrm{Gal}(L/L \cap K)$, le polynôme*

$$T_C = \prod_{\sigma \in C} (X - \sigma(\alpha))$$

est à coefficients dans K et est irréductible sur K. De plus, la factorisation de T en produits de polynômes irréductibles sur K est donnée par

$$T = \prod_{C \in \mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)} T_C$$

À l'aide d'une représentation convenable des nombres algébriques $\sigma(\alpha)$, nous pouvons calculer explicitement le polynôme T.

2.4 Détermination probabiliste du nombre d'automorphismes d'une extension algébrique

Nous présentons une modification du test de Čebotarev–van der Waerden pour obtenir un majorant du nombre d'automorphismes d'une extension de corps de nombres, reposant sur la proposition suivante:

Proposition 2.4.1 *Soit L/K une extension de corps de nombres. Soit $\mathfrak{p}$ un idéal premier de K non ramifié dans L/K se décomposant en $\mathfrak{p}\mathbb{Z}_L = \prod_{i=1}^{g} \mathfrak{P}_i$ dans L où les idéaux $\mathfrak{P}_i$ sont premiers de degrés résiduels f_i. Soit pour $1 \leq i \leq g$ le nombre g_i d'idéaux de degré résiduel f_i, alors le nombre h d'automorphismes de l'extension L/K divise $g_i f_i$ pour $1 \leq i \leq g$.*

Démonstration:

Soit H le groupe des automorphismes de l'extension L/K. Notons L^H le corps fixe de L par H, alors l'extension L/L^H est galoisienne. Soit $\mathfrak{p}\mathbb{Z}_{L^H} = \prod_{i=1}^{g} \mathfrak{Q}_i$ la décomposition de l'idéal $\mathfrak{p}$ dans L^H en produit d'idéaux premiers. L'extension L/L^H étant galoisienne, $\mathfrak{Q}_i$ se décompose en produit de g_i' idéaux de même degré résiduel $f'i$ et nous avons $h = g_i' f_i'$.

■

Chapitre 3

Isomorphismes explicites entre les corps finis

> L'univers (que d'autres nomment la Bibliothèque) se compose d'un nombre indéfini, et peut-être infini, de galeries hexagonales, avec au centre de vastes puits d'aération bordés par des balustrades très basses.
> J.L. Borges, *Fictions*

3.1 Définitions

Soit $\mathbb{F}_q$ un corps fini fixé et n un entier. Soit T_1 et T_2 deux polynômes irréductibles de degré n à coefficients dans $\mathbb{F}_q$. Nous considérons les deux extensions de $\mathbb{F}_q$ définies par $K_1 = \mathbb{F}_q[X]/(T_1)$ et $K_2 = \mathbb{F}_q[X]/(T_2)$. Ces deux extensions, ayant le même degré, sont isomorphes, cependant la preuve habituelle de ce fait utilise l'existence d'une extension commune et ne fournit pas un isomorphisme explicite entre K_1 et K_2. Si σ est un tel isomorphisme, nous voulons être capable d'évaluer la fonction

$$\sigma \left| \begin{array}{ccc} \mathbb{F}_q[X]/(T_1) & \longrightarrow & \mathbb{F}_q[X]/(T_2) \\ \overline{P} & \longmapsto & \overline{Q} \end{array} \right.$$

ce qui est équivalent à connaître $\overline{S} = \sigma(\overline{X})$. Le polynôme S doit vérifier

$$T_1 \circ S \equiv 0 \pmod{T_2} \tag{3.1}$$

Réciproquement, si S vérifie (3.1), alors

$$\sigma \left| \begin{array}{ccc} \mathbb{F}_q[X]/(T_1) & \longrightarrow & \mathbb{F}_q[X]/(T_2) \\ \overline{P} & \longmapsto & \overline{P \circ S} \end{array} \right.$$

est un isomorphisme explicite.

Plus généralement, nous voulons résoudre le problème suivant:

Problème 3.1.1 *Soit F_q un corps fini fixé et n un entier. Soit T_1 et T_2 deux polynômes irréductibles de degré* multiple *de n à coefficients dans $\mathbb{F}_q$. Nous notons K_1 l'unique sous-corps de degré n de $\mathbb{F}_q[X]/(T_1)$ et K_2 l'unique sous-corps de degré n de $\mathbb{F}_q[X]/(T_2)$.*

Il s'agit de déterminer explicitement deux polynômes S_1 et S_2 tel que

– L'élément $\overline{S_1} \pmod{T_1}$ de $\mathbb{F}_q[X]/(T_1)$ engendre K_1,

– L'élément $\overline{S_2} \pmod{T_2}$ de $\mathbb{F}_q[X]/(T_2)$ engendre K_2,

– les polynômes minimaux de $\overline{S_1}$ et $\overline{S_2}$ sont égaux.

Sous ces conditions, l'application $\overline{S_1} \longmapsto \overline{S_2}$ se prolonge de façon unique en un isomorphisme

$$\left| \begin{array}{ccc} K_1 & \longrightarrow & K_2 \\ P(\overline{S_1}) \pmod{T_1} & \longmapsto & P(\overline{S_2}) \pmod{T_2} \end{array} \right. .$$

3.2 Calcul des isomorphismes explicites quand n divise $q-1$

Dans cette section, nous supposons que n divise $q-1$ ce qui implique que $\mathbb{F}_q$ contient une racine primitive n–ième de l'unité ζ, ce qui nous permet d'utiliser la théorie de Kummer.

Nous présentons ce cas séparément, car il est beaucoup simple que le cas général, bien qu'utilisant les mêmes idées. De plus il peut être préférable de le traiter à part lors de la mise en œuvre de l'algorithme.

Soit $i \in \{1,2\}$. L'extension $K_i/\mathbb{F}_q$ est cyclique de degré n et $\mathbb{F}_q$ contient une racine primitive n–ième de l'unité ζ, $K_i/\mathbb{F}_q$ est donc une extension cyclique de Kummer. L'automorphisme de Frobenius

$$\varphi_i \left| \begin{array}{ccc} K_i & \longrightarrow & K_i \\ x & \longmapsto & x^q \end{array} \right.$$

engendre le groupe de Galois $\mathrm{Gal}(K_i/\mathbb{F}_q)$. Par le théorème 90 de Hilbert, il existe α_i de K_i tel que

$$\varphi_i(\alpha_i)/\alpha_i = \zeta \ ,$$

de plus $a_i = \alpha_i^n$ appartient à $\mathbb{F}_q$ et α_i engendre $K_i/\mathbb{F}_q$, de sorte que le polynôme minimal de α_i est

$$X^n - a_i \ .$$

Remarquons que

$$a_i^{\frac{q-1}{n}} = \alpha_i^{q-1} = \varphi_i(\alpha_i)/\alpha_i = \zeta \ .$$

Nous en déduisons que

$$(a_1/a_2)^{\frac{q-1}{n}} = 1 \ ,$$

ainsi a_1/a_2 est une puissance n-ième dans $\mathbb{F}_q$. Il existe donc $c \in \mathbb{F}_q$ tel que

$$c^n = a_1/a_2 \ .$$

Nous avons

$$(c\alpha_2)^n = a_1$$

ainsi les polynômes minimaux de α_1 et de $c\alpha_2$ sont égaux, et donc nous avons une solution du problème.

Pour être complet, nous devons donner une solution explicite au théorème 90 de Hilbert. Nous la présentons dans un cadre plus général.

3.2.1 Théorème 90 de Hilbert explicite

Soit k un corps et K/k une extension cyclique de k de degré n, non multiple de la caractéristique de k. Nous notons φ un générateur du groupe de Galois $\mathrm{Gal}(K/k)$.

Proposition 3.2.1 *Le polynôme caractéristique de φ comme endomorphisme du k–espace vectoriel K est égal à $X^n - 1$.*

Démonstration:
D'une part, nous avons $\varphi^n - \mathrm{id} = 0$, d'autre part, le lemme d'indépendance des caractères de Dirichlet implique que $\mathrm{id}, \varphi, \varphi^2, \ldots, \varphi^{n-1}$ sont linéairement indépendants sur k. Nous concluons que le polynôme minimal de φ est $X^n - 1$. Par le théorème de Cayley-Hamilton, nous concluons que le polynôme caractéristique de φ est égal à $X^n - 1$. ■

Proposition 3.2.2 *Soit $\zeta \in k$ une racine n–ième de l'unité, alors* $\mathrm{Ker}(\varphi - \zeta\, id)$ *est un k–espace vectoriel de dimension* 1.

Démonstration:

L'entier n n'étant pas multiple de la caractéristique de k, ζ est racine simple du polynôme caractéristique de φ. Cela implique que le sous-espace propre de φ associé à ζ est de dimension 1.

■

Grâce à cette proposition, il suffit de résoudre un système d'équations linéaires pour obtenir une solution explicite au théorème 90 de Hilbert.

3.2.2 Description de l'algorithme

Nous résumons cette méthode dans l'algorithme suivant

Algorithme 3.2.3 *Sous les hypothèses et notations précédentes, nous notons par B_i la base de puissances $(1, \overline{X}, \ldots, \overline{X}^{n-1})$ de $\mathbb{F}_q[X]/(T_i)$, pour $i \in \{1,2\}$. Nous résolvons le problème 3.1.1 ainsi.*

1. [Calcul de ζ] *Déterminer une racine primitive n–ième de l'unité ζ dans $\mathbb{F}_q$.*
2. [Calcul des φ_i] *Calculer la matrice A_i de l'automorphisme de Frobenius φ_i sur la base B_i, pour $i \in \{1,2\}$.*
3. [Hilbert 90] *Déterminer un vecteur propre V_i de A_i pour la valeur propre ζ, pour $i \in \{1,2\}$.*
4. [Calcul des α_i] *Calculer l'élément $\alpha_i = S_i(\overline{X})$ de K_i dont la représentation sur la base B_i est V_i, pour $i \in \{1,2\}$.*
5. [Calcul des puissances] *Calculer $a_i = \alpha_i^n$ dans $\mathbb{F}_q[X]/(T_i)$ et les convertir en éléments de $\mathbb{F}_q$, pour $i \in \{1,2\}$.*
6. [Calcul de la racine n–ième] *Calculer la racine n–ième $c \in \mathbb{F}_q$ de a_1/a_2.*
7. [Fini] *Retourner S_1 et cS_2.*

3.3 Calcul des isomorphismes explicites quand n et q sont premiers entre eux

3.3.1 Extension de la Théorie de Kummer

Soit k un corps et K/k une extension cyclique de k de degré n, non multiple de la caractéristique de k, et soit C l'extension de k engendrée par une racine primitive n–ième de l'unité ζ. Nous notons $r = [C : k]$ et $\mathcal{B}$ la base de C sur k donnée par $\mathcal{B} = (\zeta^i)_{i=0}^{r-1}$.

Nous notons φ un générateur du groupe de Galois $\mathrm{Gal}(K/k)$.

Nous allons travailler dans le (K, C)–bimodule $K \otimes_k C$.

Proposition 3.3.1 *La C–algèbre $K \otimes_k C$ est une algèbre étale; en d'autre mots, elle n'a pas d'éléments nilpotents.*

Démonstration:
L'extension K/k étant de degré premier à la caractéristique est séparable. Il existe donc un polynôme irréductible $T \in k[X]$ avec corps de rupture K. Le degré de T n'étant pas multiple de la caractéristique de k, T est séparable. Le corps K est isomorphe à $k[X]/(T)$, ainsi $K \otimes_k C$ est isomorphe à $C[X]/(T)$ qui n'a pas d'éléments nilpotents. ■

Nous étendons φ en un automorphisme $\tilde{\varphi}$ de la k–algèbre $K \otimes_k C$ par

$$\tilde{\varphi} \left| \begin{array}{ccc} K \otimes_k C & \longrightarrow & K \otimes_k C \\ x \otimes y & \longmapsto & \varphi(x) \otimes y \end{array} \right.$$

Le lemme suivant étend la théorie de Galois dans ce contexte.

Lemme 3.3.2 *L'ensemble des éléments de $K \otimes_k C$ fixé par $\tilde{\varphi}$ est $k \otimes_k C$ qui est un corps isomorphe à C.*

Démonstration:
La famille $1 \otimes \mathcal{B} = \{1 \otimes b_1, \ldots, 1 \otimes b_c\}$ est une base de $K \otimes_k C$ comme K–espace vectoriel à gauche. Un élément β de $K \otimes_k C$ s'écrit donc de façon unique sous la forme $\beta = \sum_{i=1}^{c} k_i \otimes b_i$ où les k_i sont des éléments de K et $\tilde{\varphi}(\beta) = \sum_{i=1}^{c} \varphi(k_i) \otimes b_i$. Si $\tilde{\varphi}(\beta) = \beta$ alors pour tout $1 \leqslant i \leqslant c$ nous avons $\varphi(k_i) = k_i$ de sorte que $k_i \in k$, et donc $\beta \in k \otimes_k C$ qui est un corps isomorphe à C.

■

Nous généralisons la proposition 3.2.2 ainsi.

Proposition 3.3.3 *Le C–espace vectoriel* $\mathrm{Ker}(\tilde{\varphi} - \zeta id)$ *est de dimension* 1.

Démonstration:

Soit $\mathcal{B}'$ une base de K comme k–espace vectoriel, alors $1 \otimes \mathcal{B}' = \{1 \otimes b_1, \ldots, 1 \otimes b_c\}$ est une base de $K \otimes_k C$ comme C–espace vectoriel à droite. La matrice de $\tilde{\varphi}$ sur la base $1 \otimes \mathcal{B}'$ est égal à la matrice de φ sur la base $\mathcal{B}'$. En particulier $\tilde{\varphi}$ et φ ont même polynôme minimal. Ainsi ζ est aussi une valeur propre simple de $\tilde{\varphi}$ et l'espace propre est de dimension 1.

■

La proposition suivante généralise

Proposition 3.3.4 *Soit α un vecteur propre de $\tilde{\sigma}$ pour la valeur propre ζ, alors α^n est non nul et appartient à $k \otimes_k C$.*

Démonstration:
Comme dans la théorie classique, nous avons

$$\tilde{\sigma}(\alpha^n) = ((1 \otimes \zeta)\alpha)^n = \alpha^n \ ,$$

donc α^n appartient au corps fixe $k \otimes_k C$ de $\tilde{\sigma}$. ■

Proposition 3.3.5 *Soit α un vecteur propre de $\tilde{\varphi}$ pour la valeur propre ζ. Si a_0 est la première composante de α sur la base $1 \otimes \mathcal{B}$ de $K \otimes_k C$ sur C, alors a_0 engendre l'extension K/k.*

Démonstration:
Remarquons d'abord que $k(a_0)/k$ est une sous-extension d'une extension cyclique, et donc galoisienne, ainsi tous les conjugués $\{\varphi(a_0)^e; e = 0 \text{ à } n-1\}$ de a_0 sont dans $k(a_0)$.

Écrivons $\alpha = \sum_{i=0}^{r-1}(a_i \otimes \zeta^i)$. Alors $\tilde{\varphi}(\alpha) = \sum_{i=0}^{r-1}(\varphi(a_i) \otimes \zeta^i)$. Si $T = \sum_{i=0}^{r} b_i X^i$ est le polynôme minimal de ζ sur k, alors l'équation $\varphi(\alpha) = \zeta\alpha$ devient dans la base $1 \otimes \mathcal{B}$

$$\begin{pmatrix} \varphi(a_0) \\ \varphi(a_1) \\ \varphi(a_2) \\ \vdots \\ \varphi(a_{r-1}) \end{pmatrix} = \begin{pmatrix} 0 & & 0 & -b_0 \\ 1 & & & -b_1 \\ & 1 & & -b_2 \\ 0 & & \ddots & \vdots \\ & & 1 & -b_{r-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{r-1} \end{pmatrix}$$

Nous en déduisons les relations suivantes.

$$\varphi(a_0) = -b_0 a_{r-1} \tag{3.2}$$
$$\varphi(a_i) = a_{i-1} - b_i a_{r-1} \quad , \ 1 \leqslant i \leqslant r-1 \tag{3.3}$$

Comme b_0 est non nul, nous pouvons récrire l'équation (3.2) ainsi

$$a_{r-1} = -\varphi(a_0)/b_0 \ ,$$

ce qui montre que $a_{r-1} \in k(a_0)$. À l'aide du système triangulaire

$$a_{i-1} = \varphi(a_i) - b_i a_{r-1}$$

pour $i = r-1$ à 1 en décroissant, nous voyons que tous les a_i appartiennent à $k(a_0)$. Soit un entier e tel que $\varphi^e(x) = x$ pour tous les éléments $x \in k(a_0)$, alors $\tilde{\varphi}^e(\alpha) = \alpha$ et donc $\zeta^e\alpha = \alpha$, ce qui équivaut à

$$(\zeta^e - 1)\alpha = 0 \ .$$

Comme nous sommes dans un C–espace vectoriel et que α est non nul, nous concluons donc que $\zeta^e = 1$. Il en résulte que e est un multiple de n. Par théorie de Galois, nous avons nécessairement $K = k(a_0)$. ■

La résolution du système décrit dans cette preuve nous permet de calculer un vecteur propre en ne faisant que des calculs dans K et non dans C.

Algorithme 3.3.6 *Nous déterminons un vecteur propre pour $\tilde{\varphi}$ et la valeur propre ζ sans aucun calcul dans C. Nous notons $T = \sum_{i=0}^{r} b_i X^i$ le polynôme minimal de ζ.*

1. [Matrice] *Calculer la matrice M de l'endomorphisme $T(\varphi)$ dans la base $\mathcal{B}'$.*

2. [Noyau] *Déterminer un élément non nul a_0 du noyau de M.*

3. [Système triangulaire] *Résoudre le système triangulaire*

$$a_{r-1} = -\varphi(a_0)/b_0 \tag{3.4}$$
$$a_{i-1} = \varphi(a_i) + b_i a_{r-1} \quad \textit{pour } i = r-1 \textit{ à } 1 \textit{ en décroissant} \tag{3.5}$$

4. [Terminer] *Retourner* $\alpha = \sum_{i=0}^{r-1}(a_i \otimes \zeta^i)$.

3.3.2 Description de la méthode

Il s'agit d'appliquer les résultats précédents avec $k = \mathbb{F}_q$. Nous construisons d'abord l'extension cyclotomique $C = \mathbb{F}_q(\zeta)$ et nous notons $r = [C : \mathbb{F}_q]$ son degré. Le groupe de Galois $\mathrm{Gal}(C/\mathbb{F}_q)$ est généré par

$$\psi \left| \begin{array}{ccc} C & \longrightarrow & C \\ y & \longmapsto & y^q \end{array} \right.$$

.

Soit $i \in \{1, 2\}$. L'extension $K_i/\mathbb{F}_q$ est cyclique de degré n. Nous construisons le bimodule $K_i \otimes_k C$. Nous étendons l'automorphisme de Frobenius de K_i en

$$\tilde{\varphi}_i \left| \begin{array}{ccc} K_i \otimes_k C & \longrightarrow & K_i \otimes_k C \\ x \otimes y & \longmapsto & x^q \otimes y \end{array} \right.$$

et celui de C en

$$\tilde{\psi}_i \left| \begin{array}{ccc} K_i \otimes_k C & \longrightarrow & K_i \otimes_k C \\ x \otimes y & \longmapsto & x \otimes y^q \end{array} \right.$$

Ces deux automorphismes commutent et nous avons

$$\tilde{\varphi}_i \circ \tilde{\psi}_i(\gamma) = \gamma^q$$

pour tout $\gamma \in K_i \otimes_k C$. Par la proposition 3.3.3, il existe α_i de $K_i \otimes_k C$ tel que

$$\tilde{\varphi}_i(\alpha_i) = \zeta\alpha_i \ ,$$

de plus $a_i = \alpha_i^n$ appartient à C. Remarquons que

$$a_i^{\frac{q^r-1}{n}}\alpha_i = \alpha_i^{q^r} = (\tilde{\varphi}_i \circ \tilde{\psi}_i)^r(\alpha_i) = \tilde{\varphi}_i{}^r \circ \tilde{\psi}_i{}^r(\alpha_i) = \zeta^r\alpha_i \ .$$

de sorte que

$$a_i^{\frac{q^r-1}{n}} = \zeta^r \ .$$

Nous en déduisons que

$$(a_1/a_2)^{\frac{q^r-1}{n}} = 1 \ ,$$

ainsi a_1/a_2 est une puissance parfaite dans $\mathbb{F}_q(\zeta)$. Il existe donc $c \in \mathbb{F}_q(\zeta)$ tel que

$$c^n = a_1/a_2 \ .$$

Nous avons

$$(c\alpha_2)^n = a_1$$

ainsi les polynômes minimaux de α_1 et $c\alpha_2$ sont égaux, et donc nous avons une solution du problème.

3.3.3 Description de l'algorithme

Algorithme 3.3.7 *Sous les hypothèses et notations précédentes, nous notons par B_i la base de puissances $(1, \overline{X}, \ldots, \overline{X}^{n-1})$ de $\mathbb{F}_q[X]/(T_i)$, pour $i \in \{1,2\}$. Nous résolvons le problème 3.1.1 ainsi.*

1. [Calcul de ζ] *Déterminer un facteur irréductible F du n-ième polynôme cyclotomique sur $\mathbb{F}_q$ et poser $C = \mathbb{F}_p[X]/(F)$ et $\zeta = \overline{X}$.*
2. [Calcul des Frobenius] *Calculer la matrice A_i de l'automorphisme de Frobenius de K_i sur la base B_i, pour $i \in \{1,2\}$.*
3. [Algorithme 3.3.6] *Appliquer l'algorithme 3.3.6 pour obtenir un vecteur propre V_i de A_i pour la valeur propre ζ sur le corps C, pour $i \in \{1,2\}$.*
4. [Calcul des α_1] *Calculer l'élément α_i de $K_i \otimes C$ dont la représentation sur la base $B_i \otimes 1$ est V_i, pour $i \in \{1,2\}$.*
5. [Calcul des puissances] *Calculer $a_i = \alpha_i^n$ dans $K_i \otimes C$ et les convertir en éléments de C.*
6. [Calcul de la racine n-ième] *Extraire une racine n-ième c de a_1/a_2 dans le corps C.*
7. [Calcul des S_i] *Calculer la première composante S_1 de α_1 dans la base $\{1 \otimes 1, 1 \otimes \zeta, \ldots, 1 \otimes \zeta^{\deg F - 1}\}$ et la première composante S_2 de $c\alpha_2$ dans la base $\{1 \otimes 1, 1 \otimes \zeta, \ldots, 1 \otimes \zeta^{\deg F - 1}\}$.*

Dans notre implantation dans PARI/GP, l'étape 5 prends la majorité du temps, si le degré de C est grand.

Cet algorithme comporte deux étapes qui ne sont pas élémentaires :

1. La factorisation sur $\mathbb{F}_p$ des polynômes cyclotomique. Cela est résolu en pratique par [Shoup1, Théorème 9].
2. L'extraction d'une racine n-ième dans un corps fini. Pour cela nous utilisons une généralisation de l'algorithme de Shanks pour extraire les racines n-ièmes dans un corps premier fini. Notons que par extraction

successive, nous pouvons nous ramener au cas de l'extraction d'une racine ℓ-ième, où ℓ est un nombre premier divisant $q-1$.

Algorithme 3.3.8 *Soit K un corps fini avec q éléments et soit ℓ un nombre premier divisant $q-1$. Soit r et e tel que $q-1=\ell^e r$ et tel que ℓ ne divise pas r. Nous calculons une racine ℓ-ième x de l'élément $a \in K$, si elle existe comme suit :*

1. [Trouver une racine ℓ-ième] *Choisir des éléments $y \in K$ au hasard jusqu'à ce que $y^{(q-1)/\ell} \neq 1$ et alors poser $z := y^{(q-1)/\ell}$.*
2. [Bezout] *Calculer u_1 et u_2 tel que $ru_1 + \ell u_2 = 1$.*
3. [Initialisation] *Poser $x := a^{u_2}$, $b := a^{-ru_1}$.*
4. [Boucle] *Tant que $b > 1$, exécuter les étapes suivantes :*
   - *4.1.* [Calcul de l'exposant] *Trouver le plus petit entier m tel que $b^{\ell^m} = 1$. Si $m = e$, terminer et retourner «l'élément a n'est pas une puissance ℓ-ième dans K».*
   - *4.2.* [Logarithme discret] *Calculer le plus petit entier n tel que $z^n = b^{-\ell^{m-1}}$.*
   - *4.3.* [Réduire l'exposant] *Poser $w := y^{n\ell^{e-m-1}}$, $z := z^n$, $e := k$, $x := wx$, $y := w^\ell$ et $b := yb$.*
5. [Fin] *Retourner x.*

3.4 Calcul des isomorphismes quand n est une puissance de la caractéristique

3.4.1 Calcul des isomorphismes quand n est égal à la caractéristique

Soit p la caractéristique de $\mathbb{F}_q$, et r tel que $q = p^r$. Nous supposons dans cette section que $n = p$. L'extension $K_i/\mathbb{F}_q$ est une extension d'Artin–Shreier. Considérons l'endomorphisme $\mathbb{F}_q$–linéaire

$$\Delta_i \left| \begin{array}{ccc} K_i & \longrightarrow & K_i \\ \alpha & \longmapsto & \alpha^q - \alpha \end{array} \right.$$

Un calcul évident montre que $\operatorname{Ker}\Delta_i = \mathbb{F}_q$ et $\operatorname{Im}\Delta_i \subset \operatorname{Ker}\operatorname{tr}_{K_1/\mathbb{F}_q}$. Par le théorème du rang, il vient que $\operatorname{Im}\Delta_i = \operatorname{Ker}\operatorname{tr}_{K_i/\mathbb{F}_q}$.

Soit $a \in \mathbb{F}_q$, alors $\operatorname{tr}_{K/\mathbb{F}_q}(a) = 0$, ainsi $a \in \operatorname{Im}\Delta_i$. Il existe donc $\beta_i \in K_i$ tel que $\beta_i^q - \beta_i = a$. Posons $\alpha_i = \sum_{j=0}^{r-1} \beta_i^{p^j}$. Nous avons $\alpha_i^p - \alpha_i = a$ et donc

α_i annule le polynôme $X^p - X - a$. La proposition suivante découle de la théorie d'Artin-Shreier:

Proposition 3.4.1 *Soit $\mathbb{F}_q/\mathbb{F}_p$ une extension de corps finis de caractéristique p, et $a \in \mathbb{F}_q$. Alors le polynôme $X^p - X - a$ est irréductible sur $\mathbb{F}_q$ si et seulement si $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) \neq 0$.*

Il en résulte que sous la condition $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) \neq 0$, le polynôme $X^p - X - a$ est irréductible sur $\mathbb{F}_q$ et que α_i engendre K_i. De plus, les polynômes minimaux de α_1 et de α_2 sont égaux à $X^p - X - a$, et donc nous avons une solution du problème.

3.4.2 Calcul des isomorphismes quand n est une puissance de la caractéristique

Nous supposons dans cette section que $n = p^k$ pour un entier k.

Nous allons construire une chaîne de sous-corps et appliquer k fois le résultat de la section précédente, mais pour éviter de devoir déterminer k éléments de trace non nulles, nous utilisons le lemme suivant (voir [Shoup1, Lemma 2.3]).

Lemme 3.4.2 *Soit K un corps fini de caractéristique p et $a \in K$. Supposons que le polynôme $X^p - X - a$ est irréductible dans $K[X]$. Alors, si $E = K(\alpha)$ pour une racine α de $X^p - X - a$, le polynôme $X^p - X - a\alpha^{p-1}$ est irréductible sur $E[X]$.*

Notons $K_{1,0} = K_{2,0} = \mathbb{F}_p$, $a_{1,0} = a_{2,0} = a$, $\alpha_{1,0} = \alpha_{2,0} = 1$. Nous définissons par récurrence les sous-corps $K_{i,j}$ de K_i, et les éléments $a_{i,j}$ et $\alpha_{i,j}$ de $K_{i,j}$ pour $i \in \{1, 2\}$ et $1 \leq j \leq k$ par

- $a_{i,j} = a_{i,j-1}\alpha_{i,j-1}$
- $\alpha_{i,j}$ est une racine du polynôme $X^p - X - a_{i,j}$ dans le corps K_i
- $K_{i,j}$ est le sous-corps de K_i engendré par $\alpha_{i,j}$.

Pour chaque $1 \leq j \leq k$, il existe un isomorphisme entre $K_{1,j}$ et $K_{2,j}$ envoyant $\alpha_{1,j}$ sur $\alpha_{2,j}$. En particulier, pour $j = k$, nous pouvons calculer explicitement un isomorphisme entre K_1 et K_2.

3.4.3 Description de l'algorithme

Nous résumons cette méthode dans l'algorithme suivant

Algorithme 3.4.3 *Sous les hypothèses et notations précédentes, nous notons par B_i la base de puissances $(1, \overline{X}, \ldots, \overline{X}^{n-1})$ de $\mathbb{F}_q[X]/(T_i)$, pour $i \in \{1,2\}$. Nous résolvons le problème 3.1.1 ainsi.*

1. [Calcul de a] *Déterminer un élément a de $\mathbb{F}_q$ de trace non nulle. (Si q est premier, $a = 1$ convient.)*

2. [Calcul des Δ_i] *Calculer la matrice A_i de l'opérateur Δ_i sur la base B_i, pour $i \in \{1,2\}$.*

3. [Initialisation] *Poser $a_1 := a$, $a_2 := a$, $\alpha_1 := 1$ et $\alpha_2 := 1$.*

4. [Boucle] *Répéter k fois les étapes suivantes*

4.1. [Lemme 3.4.2] *Poser $a_1 := a_1\alpha_1^{p-1}$ et $a_2 := a_2\alpha_2^{p-1}$.*

4.2. [Calcul des coordonnées] *Calculer le vecteur W_i exprimant a_i sur la base B_i, pour $i \in \{1,2\}$.*

4.3. [Théorème de Hilbert] *Résoudre le système linéaire $A_iV_i = W_i$, pour $i \in \{1,2\}$.*

4.4. [Calcul des β_i] *Calculer l'élément β_i de K_i dont la représentation sur la base B_i est V_i, pour $i \in \{1,2\}$.*

4.5. [Calcul des α_i] *Calculer l'élément $\alpha_i := \sum_{j=0}^{r-1} \beta_i^{p^j}$, pour $i \in \{1,2\}$ (Si q est premier, $\alpha_i = \beta_i$).*

5. [Fini] *Retourner α_1 et α_2.*

3.5 Calcul des isomorphismes dans le cas général

Nous voulons combiner les deux algorithmes précédents pour résoudre le cas général. Écrivons $n = mp^k$ où m n'est pas multiple de la caractéristique p de $\mathbb{F}_q$. Pour $i \in \{1,2\}$, nous notons K_i' le sous-corps de degré m de K_i, et K_i'' le sous-corps de degré p^k de K_i. Par application des méthodes précédentes, nous pouvons déterminer $\alpha_1', \alpha_1'' \in K_1$ et $\alpha_2', \alpha_2'' \in K_2$ tel que

- L'élément α_i' engendre K_i' et α_i'' engendre K_i'', pour $i \in \{1,2\}$.
- Les polynômes minimaux de α_1' et de α_2' sont égaux.
- Les polynômes minimaux de α_1'' et de α_2'' sont égaux.

Nous déterminons aisément un isomorphisme entre K_1 et K_2 à l'aide de la

Proposition 3.5.1 *Sous les hypothèses précédentes, posons $\alpha_i = \alpha_i' + \alpha_i''$, pour $i \in \{1,2\}$, alors*

- *L'élément α_i engendre K_i pour $i \in \{1,2\}$.*
- *Les polynômes minimaux de α_1 et α_2 sont égaux.*

3.5.1 Solution du problème original

Pour résoudre le problème original où $\deg T_1 = \deg T_2 = n$, nous devons ajouter les étapes suivantes

1. [Changement de base] Calculer la matrice M exprimant la base $(1, \alpha_1, \ldots, \alpha_1^{n-1})$ de K_1 en fonction de B_1.
2. [Expression de $\overline{X}$] Résoudre en V le système linéaire

$$MV = (0, 1, 0, \ldots, 0)$$

   et soit S_1' le polynôme dont la représentation dans la base $(1, X, \ldots, X^{n-1})$ est V.
3. [Substituer] Calculer $S = S_1' \circ S_2 \pmod{T_2}$ et retourner S.

3.6 Factorisation sur une extension

Soit P un polynôme à coefficients dans $\mathbb{F}_q$ et soit T_2 un polynôme irréductible définissant une extension $\mathbb{F}_q[X]/(T_2)$ de $\mathbb{F}_q$ de degré n. Nous voulons factoriser P sur $\mathbb{F}_q[X]/(T_2)$ à l'aide du lemme 2.3.1. Pour cela, nous factorisons d'abord P sur $\mathbb{F}_q$ pour nous ramener à la factorisation d'un facteur irréductible T_1 de P. Posons $L = \mathbb{F}_q[X]/(T_1)$. L'extension $L/\mathbb{F}_q$ étant galoisienne, il nous suffit de calculer l'intersection $L \cap \mathbb{F}_q[X]/(T_2)$. Le degré de l'intersection étant le plus grand diviseur commun d des degrés, il suffit de calculer un isomorphisme entre les sous-corps de degré d de $\mathbb{F}_q[X]/(T_1)$ et de $\mathbb{F}_q[X]/(T_2)$.

Algorithme 3.6.1 *Il s'agit de factoriser P sur $\mathbb{F}_q[X]/(T_2)$. Factoriser P sur $\mathbb{F}_q$ et appliquer l'algorithme suivant à chaque facteur irréductible T_1 de P, et retourner la factorisation.*

1. [Calcul de l'intersection] *Calculer le plus grand diviseur commun d des degrés de T_1 et T_2.*

2. [Calcul de l'isomorphisme] *Calculer un isomorphisme entre les sous-corps K_i d'ordre d de $\mathbb{F}_q[X]/(T_i)$ pour $i \in \{1, 2\}$ donné par l'image $\alpha_2 \in K_2$ d'un α_1 de K_1.*

3. [Calcul de la factorisation] *Calculer*

$$Q_1(Y) = \prod_{0 \le k < n/d} (Y - \overline{X}^{p^{dk}})$$

dans K_1, où $\overline{X}$ représente la classe de X dans $\mathbb{F}_q[X]/(T_2)$.

4. [Appliquer l'isomorphisme] *Convertir les coefficients de* Q_1 *en éléments de* K_1 *et appliquer l'isomorphisme* $\alpha_1 \longmapsto \alpha_2$ *à chacun d'eux, pour obtenir un facteur* $Q_2 \in K_2[X]$.
5. [Calcul des facteurs conjugués] *Calculer les facteurs conjugués de* Q_2 *en appliquant les puissances successives de l'automorphisme de Frobenius du corps* K_2 *à tout les coefficients de* Q_2.

Chapitre 4

Calcul explicite des automorphismes galoisiens

They sought it with thimbles, they sought it with care;
They pursued it with forks and hope;
They threatened its life with a railway-share;
They charmed it with smiles and soap.

Lewis Carroll, The Hunting of the Snark

4.1 Introduction

4.1.1 Présentation du problème

Soit $T \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible de degré n, α une racine de T et $K = \mathbb{Q}(\alpha)$ son corps de rupture. Il s'agit de donner un algorithme qui

- détermine si K est une extension galoisienne de $\mathbb{Q}$
- dans ce cas, retourne l'image de α par chacun des automorphismes.

Dans la suite nous supposerons que l'extension *est* galoisienne. En effet, à la fin de l'algorithme, si nous avons réussi à déterminer n automorphismes distincts, nous avons *prouvé* que l'extension est galoisienne. Sinon, soit l'algorithme n'a pas été capable de résoudre le problème, soit l'extension n'est pas galoisienne. Si pour une raison ou une autre nous sommes sûrs d'être dans le cadre dans lequel l'algorithme retourne une réponse, alors nous avons prouvé que l'extension n'est pas galoisienne.

4.1.2 Représentation des automorphismes

Nous avons vu dans le premier chapitre deux façons de représenter un automorphisme.

- Soit par un polynôme S vérifiant $T \mid T \circ S$.
- Soit comme une paire ψ, φ où ψ est une permutation des places au-dessus de ℓ et φ une famille d'isomorphismes locaux.

Nous allons préciser la deuxième représentation:

Nous supposons que p est un nombre premier non ramifié et, pour des raisons algorithmiques, qu'il ne divise pas le discriminant de T.

Nous décomposons p en produits d'idéaux premiers

$$(p) = \prod_{i=1}^{g} \mathfrak{P}_i$$

et nous notons $\mathbb{F}_{\mathfrak{P}_i} = \mathbb{Z}_K/(\mathfrak{P}_i)$ les corps résiduels et $f = f_p$ le degré résiduel de p. Nous rappelons que nous avons le morphisme

$$\Gamma_1 \left| \begin{array}{ccc} \mathbb{Z}_K & \longrightarrow & \mathbb{Z}_K/(p) \cong \prod_{i=1}^{g} \mathbb{F}_{\mathfrak{P}_i} \\ \alpha & \longmapsto & (\alpha \pmod{\mathfrak{P}_i})_{i=1}^{g} \end{array} \right.$$

Proposition 4.1.1 *L'application*

$$\Delta \left| \begin{array}{ccc} \mathrm{Gal}(K/\mathbb{Q}) & \longrightarrow & \mathrm{Aut}(\mathbb{Z}_K/p\mathbb{Z}_K) \cong \mathrm{Aut}(\prod_{i=1}^{g} \mathbb{F}_{\mathfrak{P}_i}) \\ \sigma & \longmapsto & (x + p\mathbb{Z}_K \mapsto \sigma(x) + p\mathbb{Z}_K) \end{array} \right.$$

est un morphisme de groupe injectif.

Démonstration:
Soit $\sigma \in \mathrm{Ker}\,\Delta$. Alors en particulier $\sigma(x) \equiv x \pmod{\mathfrak{P}_1}$, donc σ appartient au groupe d'inertie de $\mathfrak{P}_1$ qui est réduit à l'identité car $\mathfrak{P}_1$ n'est pas ramifié dans $K/\mathbb{Q}$. ■

La proposition suivante nous donne la structure de $\mathrm{Aut}(\prod_{i=1}^{g} \mathbb{F}_{\mathfrak{P}_i})$

Proposition 4.1.2 *On note $\iota_{i,j}$ un isomorphisme de $\mathbb{F}_{\mathfrak{P}_i}$ sur $\mathbb{F}_{\mathfrak{P}_j}$. Le groupe $\mathrm{Aut}(\prod_{i=1}^{g} \mathbb{F}_{\mathfrak{P}_i})$ est isomorphe au produit en couronne $\mathcal{W} = \mathbb{Z}/f\mathbb{Z} \wr \mathfrak{S}_g = (\mathbb{Z}/f\mathbb{Z})^g \rtimes \mathfrak{S}_g$, de cardinal $f^g g!$ où la multiplication est donné par*

$$((a_i)_{i=1}^{g}; \sigma)((b_i)_{i=1}^{g}; \tau) = ((a_i + b_{\sigma(i)})_{i=1}^{g}; \sigma\tau)$$

Explicitement, l'application

$$\left|\begin{array}{ccc} \mathbb{Z}/f\mathbb{Z} \wr \mathfrak{S}_g & \longrightarrow & \mathrm{Aut}(\prod_{i=1}^{g} \mathbb{F}_{\mathfrak{P}_i}) \\ ((a_i)_{i=1}^g ; \sigma) & \longmapsto & ((x_i)_{i=1}^g \mapsto (\iota_{\sigma(i),i}(x_{\sigma(i)})^{p^{a_i}})) \end{array}\right.$$

est un isomorphisme de groupe.

Démonstration:
Soit $\rho \in \mathrm{Aut}(\mathbb{Z}_K/p\mathbb{Z}_K)$. Les idéaux maximaux de $\mathbb{Z}_K/p\mathbb{Z}_K$ sont les $(\mathfrak{P}_i/p\mathbb{Z}_K)_{i=1}^g$. L'image par un automorphisme d'un idéal maximal est un idéal maximal, donc ρ permute les $\mathfrak{P}_i$. Il existe $\sigma \in \mathfrak{S}_g$ tel que $\rho(\mathfrak{P}_i/p\mathbb{Z}_K) = \mathfrak{P}_{\sigma(i)}/p\mathbb{Z}_K$. Soit $\mathfrak{Q}_i = \bigcap_{j\neq i} \mathfrak{P}_j$, alors $\mathfrak{Q}_i/p\mathbb{Z}_K \cong \mathbb{F}_{\mathfrak{P}_i}$ et $\rho(\mathfrak{Q}_i) = \mathfrak{Q}_{\sigma(i)}$, ainsi $\iota_{i,\sigma(i)}^{-1} \circ \rho$ est un automorphisme de $\mathbb{F}_{\mathfrak{P}_i}$, or $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}_i}/\mathbb{F}_p)$ est engendré par l'automorphisme de Frobenius $x \mapsto x^p$, il existe donc $a_i \in \mathbb{Z}/f\mathbb{Z}$ tel que $\iota_{i,\sigma(i)}^{-1} \circ \rho = x \mapsto x^{p^{a_i}}$, on en déduit que [1]

$$\rho((x_i)_{i=1}^g) = (\iota_{\sigma^{-1}(i),i}(x_{\sigma^{-1}(i)})^{p^{a_i}}) \ .$$

■

Définition 4.1.3 *L'application*

$$\left|\begin{array}{ccc} G & \longrightarrow & \mathcal{W} \\ \sigma & \longmapsto & \tilde{\sigma} \ tel \ que \ f(\sigma) = g(\tilde{\sigma}) \end{array}\right.$$

est un morphisme de groupe injectif et nous noterons $\tilde{G}$ son image.

Nous pouvons donc représenter un automorphisme σ par son image $\tilde{\sigma}$ dans le groupe $\mathcal{W}$.

4.1.3 Relèvement des automorphismes modulo p

Proposition 4.1.4 *L'application h se décompose en un composé de trois applications h_1, h_2 et g comme suit:*

$$h \left|\begin{array}{ccccccc} G & \xrightarrow{h_1} & \mathrm{Aut}(\mathbb{Z}_K/(p^e)) & \xrightarrow{h_2} & \mathrm{Aut}(\mathbb{Z}_K/(p)) & \xrightarrow{g} & \mathcal{W} \\ \sigma & \longmapsto & \sigma \pmod{p^e} & \longmapsto & \sigma \pmod{p} & \longmapsto & \tilde{\sigma} \end{array}\right.$$

de plus h_1 est un morphisme injectif et h_2 un isomorphisme de groupes.

1. La première personne pouvant me convaincre que les indices sont justes a droit a un exemplaire gratuit et dédicacé de gp2c 

Nous pouvons dons relever via h_2 les automorphismes modulo p en automorphismes modulo p^e pour lequel il est facile de savoir s'ils proviennent de l'image de h_1 et d'en obtenir le cas échéant une représentation polynomiale, à l'aide des techniques déjà mentionnées que nous détaillerons plus loin.

4.1.4 Stratégie de détermination de $\tilde{G}$

Nous sommes donc capables de déterminer G à condition de connaître son image $\tilde{G}$. Pour ce faire nous allons utiliser des stratégies combinatoires.

Nous introduisons la définition suivante:

Définition 4.1.5 *Un automorphisme $\sigma \in G$ est dit **diagonal** (par rapport à p) s'il ne permute pas les idéaux premiers au-dessus de p, c'est-à-dire si $\tilde{\sigma} \in (\mathbb{Z}/f\mathbb{Z})^g \times \{1\}$*

Pour des raisons combinatoires, nous ne considérerons dans la suite que deux cas:

- Nous cherchons à relever des éléments diagonaux.
- Nous avons choisi un nombre premier totalement décomposé, de sorte que $\mathcal{W}$ est le groupe de permutation $\mathfrak{S}_n$.

En effet, en dehors de ce cadre, la combinatoire explose et rend extrêmement difficile l'utilisation de cette méthode. Cependant, nous donnerons un exemple d'application lorsque le groupe de Galois est isomorphe au groupe de permutations $\mathfrak{S}_4$.

De plus cette restriction entraîne de nombreuses simplifications algorithmique qui contribuent à l'accélération de l'algorithme. Il pourrait sembler intéressant d'utiliser les éléments *anti-diagonaux*, c'est-à-dire qui appartiennent à $0^g \times \mathfrak{S}_n$, mais cette classe n'est pas fermée sous l'action des automorphismes de G dès que le nombre premier n'est pas totalement décomposé, et donc en aucun cas nous ne pouvons être assuré de l'existence d'un tel élément dans le groupe. Cela vient de la non unicité de l'immersion de G dans $\mathcal{W}$ qui dépend du choix de l'*ordre* sur les idéaux premiers.

La stratégie de l'algorithme consiste à

1. Se ramener à l'un des deux cas précédents.
2. Générer un sous-ensemble de $\mathcal{W}$ dans lequel il est raisonnable d'espérer trouver un élément de l'image.
3. Tester tout les éléments de ce sous-ensemble.
4. Recommencer pour trouver d'autres éléments jusqu'à avoir une famille génératrice.

4.2 Procédé algorithmique pour le relèvement des automorphismes

Then a scream, shrill and high, rent the shuddering sky,
And they knew that some danger was near:
The Beaver turned pale to the tip of its tail,
And even the Butcher felt queer.

Lewis Carroll, The Hunting of the Snark

4.2.1 Calcul d'un dénominateur commun aux coefficients des automorphismes

Le polynôme T étant supposé unitaire, les images de α par les automorphismes sont des entiers algébriques. Nous pouvons donc utiliser et déterminer un dénominateur commun pour les entiers algébriques comme dans la section 1.1.3.

4.2.2 Calcul d'une borne sur les coefficients des automorphismes

Nous avons besoin d'une borne sur les coefficients des polynômes représentant les automorphismes. Nous pouvons utiliser des bornes explicites dues à Mignotte [Landau]. Cependant ces bornes sont génériques et sont en pratique beaucoup trop larges. Nous présentons un procédé permettant d'obtenir des bornes bien meilleures.

Si V est un vecteur à composantes complexes, nous notons $\|V\|$ la norme L^∞ de V. Si M est une matrice carrée à composantes complexes, nous notons $\|M\|$ sa norme matricielle relativement à la norme L^∞, de sorte que nous avons l'inégalité $\|MV\| \leq \|M\|\|V\|$. De plus nous savons que $\|M\|$ est le supremum des normes L^1 des colonnes de M.

Lemme 4.2.1 *Notons $(\sigma_i)_{i=1}^n$ les plongements complexes de K. Soit M la matrice de van der Monde $(\sigma_i(\alpha)^{j-1})$. Alors*

$$B = \|M^{-1}\| \sup(|\sigma_i(\alpha)|)_{i=1}^n$$

majore les composantes des polynômes représentant les automorphismes.

Démonstration:
Soit p la représentation par permutation des plongements complexes d'un automorphisme représenté par le polynôme $S = \sum_{i=1}^n s_i X^{i-1}$ Soit V le vecteur

$(\sigma_{p(i)}(\alpha))_{i=1}^n$. Notons que la norme L^1 ne dépend pas de l'ordre des composantes, donc $\|V\| = \sup(|\sigma_i(\alpha)|)_{i=1}^n$. Nous avons l'identité $M(s_i) = V$. Nous en déduisons

$$\|(s_i)\| = \|M^{-1}V\| \leqslant \|M^{-1}\|\|V\| \leqslant B \ .$$

■

L'utilisation de ce lemme requiert le calcul explicite d'approximations complexes des racines du polynôme. De plus il est nécessaire d'utiliser un algorithme qui retourne des approximations certifiées pour éviter d'obtenir une borne incorrecte, et ce calcul nécessite un certain temps. Néanmoins l'expérience montre que le gain de temps sur l'ensemble de l'algorithme est très important. Le gain vient de la majoration des $1/T'(\sigma_i(\alpha))$ dans l'identité 1.2.

Pour éviter les erreurs d'arrondis, nous procédons ainsi.

Algorithme 4.2.2 *Nous calculons une borne B convenable pour un polynôme T ainsi.*

1. [Mesure de la précision] *Déterminer le supremum η des valeurs absolues des coefficients de T.*
2. [Calcul des racines] *Obtenir une approximation des racines complexes α_i de T avec une erreur relative inférieure à $1/\eta$.*
3. [Plongements] *Numéroter les plongements $(\sigma_i)_{i=1}^n$ de sorte que*

$$\sigma_i(\alpha) = \alpha_i$$

4. [$T'(\alpha)$] *Pour chaque $1 \leq i \leq n$, calculer $T'(\alpha_i)$ à l'aide de la formule*

$$T'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$$

5. [van der Monde inverse] *Pour chaque $1 \leq i \leq n$ calculer la i–ième ligne $(l_j)_{j=1}^n$ de la matrice grâce à la formule*

$$T(X)/(T'(\alpha_i)(X - \alpha_i))) = \sum_{j=0}^{n-1} l_{j+1} X^j$$

4.2.3 Algorithme pour le test des permutations

Dans cette section, nous avons un nombre premier ℓ totalement décomposé ne divisant pas le discriminant de T, et une précision e. Nous allons utiliser les idées de la section 1.3.4. Nous calculons les racines $(\alpha_i)_{i=1}^n$de T modulo

ℓ et nous les relevons à l'aide du lemme de Hensel, pour obtenir les racines $(\alpha_i)_{i=1}^n$ de T modulo ℓ^e.

Nous souhaitons être capable de tester très rapidement si un élément $w = ((0), \pi) \in \mathcal{W}$ appartient à l'image $\tilde{G}$ de Γ.

Nous calculons l'inverse M de la matrice de van der Monde (α_i^{j-1}). Nous posons $V = (\alpha_{\pi(i)})_{i=1}^n$. Le relèvement modulo p^e de w est donné par le produit MV.

Pour accélérer les calculs, nous précalculons tout les produits $\omega_{i,j,k} = M_{i,j}\alpha_k$ pour $1 \leq i, j, k \leq n$.

Nous pouvons ainsi calculer MV par la formule

$$(\sum_{j=1}^{n} \omega_{i,j,\pi(i)})_{i=1}^n$$

qui ne nécessite que des additions.

Pour accélérer plus encore les tests nous utilisons quatre techniques:

- Nous choisissons une précision ℓ^e sensiblement plus grande que la borne $2BD$, de sorte que pour presque toute permutation, le produit MV n'aura pas de représentant inférieur à la borne.
- Nous ne calculons d'abord qu'une seule composante de MV et nous testons d'abord si elle admet un représentant plus petit que la borne.
- Nous réutilisons une technique décrite dans [ASZ] et utilisée pour accélérer le $d-1$–test, qui consiste à n'additionner que les premiers mots des ω pour tester l'inégalité.
- Nous essayons de générer les permutations dans un ordre tel que certains termes des additions ne changent pas entre deux permutations, ce qui permet de conserver le résultat partiel. Cette technique est très pénible à mettre en œuvre, mais permet d'améliorer beaucoup la complexité.

4.2.4 Algorithme pour le test des éléments diagonaux

L'algorithme que nous allons proposer repose sur la possibilité de tester très vite si une permutation est la représentation d'un automorphisme. Dès lors nous devons préconditionner le plus possible ce problème.

Nous avons donc choisi un nombre premier p, une précision e, nous avons calculé les plongements naturels p–adiques $(\sigma_i)_{i=1}^g$, la factorisation $T = \prod T_i \pmod{p^e}$, et la base d'idempotents $(U_i)_{i=1}^n$. Nous souhaitons être capable de tester très rapidement si un élément diagonal $w = ((b_i)_{i=1}^g, id) \in \mathcal{W}$ appartient à l'image $\tilde{G}$ de Γ.

Nous allons d'abord relever $w_1 = ((1)_{i=1}^{g}, id)$. Cet élément correspond à l'élément de Frobenius modulo chaque idéal premier au dessus de p. Nous relevons d'abord l'automorphisme de Frobenius de $\mathbb{F}_p$ en un automorphisme p-adique de l'algèbre $\mathbb{Z}_K/(p^e)$. Pour cela nous procédons comme indiqué dans [AcKl] :

Nous considérons que $X^p \pmod{T, p}$ est une racine simple du polynôme $T \pmod{T, p}$ et nous pouvons donc la relever par relèvement de Hensel en une racine de $T \pmod{T, p^e}$.

Proposition 4.2.3 *Sous les hypothèses précédentes sur T et p, soit $S_0 \in \mathbb{Z}[X]$ tel que $T \circ S_0 \equiv 0 \pmod{p, T}$, et soit $W_0 \in \mathbb{Z}[X]$ vérifiant $W_0 T'(S_0) \equiv 1 \pmod{p, T}$. Il existe une unique suite $(S_k)_{k \geqslant 1} \subset \mathbb{Z}[X]$ vérifiant*

$$T(S_k) \equiv 0 \pmod{p^{2^k}, T} \text{ et } S_k \equiv S_0 \pmod{p, T}$$

et une unique suite $(W_k)_{k \geqslant 1} \subset \mathbb{Z}[X]$ vérifiant

$$W_k T'(S_k) \equiv 1 \pmod{p^{2^k}, T} \text{ et } W_k \equiv W_0 \pmod{p, T}$$

Et nous pouvons les construire par les relations de récurrence

$$S_{k+1} \equiv S_k - W_k T(S_k) \pmod{p^{2^{k+1}}, T} \tag{4.1}$$
$$W_{k+1} \equiv (2 - W_k T'(S_{k+1}))W_k \pmod{p^{2^{k+1}}, T} \tag{4.2}$$

En pratique, nous utilisons l'algorithme suivant, qui utilise le procédé de reconstruction des rationnels et l'algorithme décrit dans [BrKu] pour le calcul de la composition modulaire de polynôme.

Algorithme 4.2.4 *Soit connue une borne B et un dénominateur D pour les automorphismes, et soit p un nombre premier ne divisant ni D ni le dénominateur de T, et un entier e tel que $p^e > 2BD$. Nous déterminons un polynôme S vérifiant*

$$S \equiv X^p \pmod{p, T} \tag{4.3}$$
$$T(S) \equiv 0 \pmod{p^e, T} \tag{4.4}$$

1. [Frobenius] *Nous calculons*

$$S_0 = X^p \pmod{p, T}$$

par exponentiation binaire

2. [Inversion] *Nous calculons*

$$W_0 = T'(S_0)^{-1} \pmod{p, T}$$

par l'algorithme d'Euclides.

3. [Exposants] *Soit* $l = [\log_2(e)]$. *Nous construisons la suite d'entiers* $(e_i)_{i=0}^{l}$ *définie par récurrence décroissante, telle que* $e_l = n$ *et* $e_{k-1} = [\frac{e_k+1}{2}]$ *pour* $l \geq k \geq 1$.

4. [Récurrence] *Pour* $i = 0$ *à* $l-1$, *exécuter les étapes suivantes:*

4.1. [Puissances] *Soit* $m = \lceil \sqrt{n} \rceil$. *Nous précalculons les puissances* $S_i^j \pmod{T, p^{e_{i+1}}}$ *pour* $0 \leq j \leq m$.

4.2. [Calcul de W_i] *Si* $i > 0$, *à l'aide de l'algorithme pour la composition modulaire de polynômes, nous calculons*

$$T'(S_i) \pmod{p^{e_i}, T}$$

et nous posons

$$W_i \equiv (2 - W_{i-1}T'(S_i))W_{i-1} \pmod{p^{e_i}, T}$$

4.3. [Calcul de S_{i+1}] *À l'aide de l'algorithme pour la composition modulaire de polynôme, nous calculons*

$$T(S_i) \pmod{p^{e_{i+1}}, T}$$

et nous posons

$$S_{i+1} \equiv S_i - W_i T(S_i) \pmod{p^{e_{i+1}}, T}$$

4.4. [Reconstruction] *Si* $i < l-1$ *Nous appliquons le procédé de reconstruction des rationnels au composantes de* S_i. *Si nous obtenons à chaque fois un dénominateur divisant* D, *nous testons si le polynôme reconstruit* S *vérifie l'identité 4.4 et dans ce cas nous retournons immédiatement* S.

5. [Fin] *Nous retournons* $S = S_l$.

Remarque:

La composition modulaire de l'étape 2 est effectuée avec une précision moindre et prend un temps négligeable par rapport à l'étape 3, ainsi nous avons préconditionné l'étape 1 pour une seule évaluation.

Nous avons donc à déterminer S tel que $g \circ h_2(S) = w_1$. Nous devons relever $w_j = ((j)_{i=1}^{g}, id)$ pour $0 \leq j < f_p$. Pour cela il suffit de remarquer que $w_j = w_1^j$ et de composer le polynôme $S \pmod{p^e, T}$ avec lui-même $j-1$ fois, avec l'aide de l'algorithme de composition modulaire précité.

Avec ces données, le relèvement modulo p^e de w est

$$Q = \sum_{i=1}^{g} w_{b_i} U_i \ .$$

Les technique décrites dans la section 4.2.3 s'appliquent ici aussi, par exemple nous ne calculons d'abord qu'un seul coefficient de Q et nous testons d'abord s'il admet un représentant plus petit que la borne.

4.3 Exemple de stratégie combinatoire

He thought of his childhood, left far far behind–
That blissful and innocent state–
The sound so exactly recalled to his mind
A pencil that squeaks on a slate!

Lewis Carroll, The Hunting of the Snark

4.3.1 Le groupe $\mathfrak{A}_4$

Une méthode simple pour calculer le groupe de Galois serait de tester toutes les permutations possibles des racines, mais il faudrait tester $n!$ et l'on serait limité au petites valeurs de n. Une méthode bien plus complexe consiste à tester tous les sous-groupes transitifs de $\mathfrak{S}_n$.

Nous allons montrer comment la mettre en œuvre en pratique dans le cas particulier où l'on veut tester si un polynôme T de degré 12 est galoisien de groupe $G \cong \mathfrak{A}_4$.
G agit simplement transitivement sur les racines. Un élément $g \in G$ agit comme une permutation dont tous les cycles sont de même longueur, sinon si l est la longueur du plus petit cycle alors $g^l \neq 1$ et a des points fixes. Le nombre de permutations décomposables en produit de cycles de longueur l est donné par

$$\frac{n!}{(n/l)!l^{(n/l)}}$$

Dans $\mathfrak{A}_4$ il y a des éléments d'ordre 2 et 3.

- Pour 2 on trouve 10395 permutations.
- Pour 3 on trouve 246400 permutations.
- En fait à n fixé, c'est une fonction croissante de l.

Nous pouvons donc déterminer un élément σ d'ordre 2 en testant au plus 10395 permutations.

Il s'agit maintenant de déterminer les deux autres automorphismes d'ordre 2, que l'on notera τ et υ. Dans $\mathfrak{A}_4$, cela nous donne les relations $\sigma\tau = \tau\sigma = \upsilon$.

En abrégeant les racines par leurs numéros et quitte à changer la numérotation, on suppose que la décomposition de σ en cycle est

$$(1,2)(3,4)(5,6)(7,8)(9,10)(11,12) \ .$$

Pour $\tau(1)$ il y a encore 10 valeurs possibles: les racines numéro 3 à 12.

Commençons par supposer que $\tau(1) = 3$ alors $\sigma\tau(1) = 4$ et donc $\tau\sigma(1) = 4$ et donc $\tau(2) = 4$, et bien sur $\tau(3) = 1$ et $\tau(4) = 2$.

Nous connaissons automatiquement 3 nouvelles valeurs de τ. Pour $\tau(5)$ il ne reste plus que 6 choix : les racines numéro 7 à 12. Cela nous donnera encore 4 nouvelle valeurs, par exemple si $\tau(5) = 7$ alors $\tau(6) = 8$.

Il ne reste plus que deux choix pour $\tau(9)$: les racines numéro 11 et 12. En résumé, nous avons τ et υ en testant en tout $10 \times 6 \times 2 = 120$ permutations.

En fait, quitte à échanger τ et υ on peut toujours supposer que $\tau(1)$ est impair, ce qui nous laisse 60 permutations à tester.

Il nous manque encore les 8 éléments d'ordres 3, il en existe un, noté ρ tel que $\rho\sigma = \tau\rho$ et $\rho\tau = \upsilon\rho$, et un raisonnement analogue nous permet de trouver ρ avec seulement 15 tests.

Comme ρ, σ et τ engendre $\mathfrak{A}_4$, nous avons terminé. Nous avons testé dans le pire cas 10470 permutations au lieu de 12!=479001600.

4.3.2 Conclusion

L'essentiel des tests est fait pour déterminer le premier élément. Il faut commencer par déterminer les éléments d'ordres minimaux. Après le nombre de tests chute beaucoup, car le nombre de sous-groupes transitifs possibles de $\mathfrak{S}_n$ décroît très vite. Il faut au moins $\frac{n!}{(n/2)!2^{(n/2)}}$ tests. Cette méthode est donc valable jusqu'à environ $n = 16$ où il faut tester 2027025 permutations. Le problème est de générer rapidement les bonnes permutations à tester dans un cadre général.

4.4 Calcul des automorphismes d'une extension de groupe de Galois $\mathfrak{S}_4$

"'Tis the voice of the Jubjub!" he suddenly cried.
(This man, that they used to call "Dunce.")
"As the Bellman would tell you," he added with pride,
"I have uttered that sentiment once."

Lewis Carroll, The Hunting of the Snark

Dans cette section nous calculons les automorphismes galoisiens d'un corps de nombres galoisien de groupe de Galois $\mathfrak{S}_4$

Nous allons adopter une stratégie en accord avec les remarques faites précédemment.

- Nous devons choisir un nombre premier p ayant le plus grand degré résiduel possible.
- Nous devons calculer des générateurs d'ordre minimal.
- Nous devons avoir des relations simples entre les générateurs.

Pour mettre en œuvre cette stratégie, nous allons utiliser un nombre premier p de degré résiduel égal à 4 et la présentation du groupe $\mathfrak{S}_4$ donnée par son isomorphisme avec le groupe de Coxeter de type $\mathbf{A}_3$,

$$\langle \alpha, \beta, \gamma | \alpha^2, \beta^2, \gamma^2, (\alpha\beta)^3, (\beta\gamma)^3, (\alpha\gamma)^2 \rangle \ ,$$

où par exemple $\alpha = (1\ 2),\ \beta = (2\ 3)$ et $\gamma = (3\ 4)$.

4.4.1 Détermination de α

Soit p un nombre premier non ramifié de degré résiduel 4. Il se décompose en 6 idéaux $(\mathfrak{P}_i)_{i=1}^6$ au-dessus de p. Nous devons donc représenter $\mathfrak{S}_4$ dans le groupe $\mathcal{W} = (\mathbb{Z}/4\mathbb{Z})^6 \rtimes \mathfrak{S}_6$.

En premier lieu, nous devons calculer l'action de G sur les idéaux$(\mathfrak{P}_i)_{i=1}^6$.

Proposition 4.4.1 *Le groupe de Galois G agit transitivement sur les idéaux $(\mathfrak{P}_i)_{i=1}^6$ et le stabilisateur* $\mathrm{Stab}(\mathfrak{P}_1)$ *est engendré par $\varphi_1 = \left(\frac{\mathfrak{P}_1}{L/K}\right)$. Notons par $(C_i)_{i=1}^6$ les classes à gauche de G modulo $\langle\varphi_1\rangle$, nous avons l'équivalence*

$$\forall i \forall j \quad \sigma(\mathfrak{P}_i) = \mathfrak{P}_j \text{ si et seulement si } \sigma C_i = C_j \ .$$

De plus l'application

$$\Omega \left| \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_6 \\ \sigma & \longmapsto & \tau \text{ tel que } \forall i \quad \sigma C_i = C_{\tau(i)} \end{array} \right.$$

est un morphisme de groupe injectif qui envoie les classes de conjugaison de $\mathfrak{S}_4$ sur celles de $\mathfrak{S}_6$ comme suit.

Ordre	*Classe dans* $\mathfrak{S}_4$	*Card.*	*Classe dans* $\mathfrak{S}_6$	*Card.*	*ratio*
1	*id*	1	*id*	1	1
2	(1 2)	6	(1 2)(3 4)(5 6)	15	2/5
2	(1 2)(3 4)	3	(1 2)(3 4)	45	1/15
3	(1 2 3)	8	(1 2 3)(4 5 6)	40	1/5
4	(1 2 3 4)	6	(1 2 3 4)	90	1/15

Le meilleur ratio est obtenu pour la classe de conjugaison de (1 2), ce qui justifie notre choix de α. Dans la suite, nous notons par $\mathcal{C}$ la classe de conjugaison de (1 2)(3 4)(5 6) dans $\mathfrak{S}_6$.

Proposition 4.4.2 *Les classes à gauche de* $\mathfrak{S}_4$ *modulo* (1 2 3 4) *sont*

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

Soit Σ l'application

$$\Sigma \left| \begin{array}{ccc} \mathcal{W} & \longrightarrow & \mathfrak{S}_6 \\ ((a_i)_{i=1}^g; \sigma) & \longmapsto & \sigma \end{array} \right.$$

Proposition 4.4.3 *L'ensemble* $\mathcal{S}$ *des éléments* h *de* $\mathcal{W}$ *d'ordre* 2 *tel que*

$$\Sigma(h) \in \{(1\ 2)(3\ 4)(5\ 6), (1\ 2)(3\ 5)(4\ 6), (1\ 2)(3\ 6)(4\ 5)\}$$

contient au moins un élément de $\tilde{G}$.

Démonstration:

En regardant les classes à gauche de $\mathfrak{S}_4$ modulo (1 2 3 4) listées dans la proposition 4.4.2, nous voyons que chaque classe à gauche contient l'identité où une transposition. Par conjugaison, cette remarque reste vraie pour les classes à gauche de G par $\langle\varphi_1\rangle$. Nous concluons qu'il existe au moins une transposition $\sigma \in G$ tel que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. Par la proposition 4.4.1, $\Omega(\sigma) \in \mathcal{C}$ et $\Omega(\sigma)(1) = 2$, ainsi $\Omega(\sigma) \in \mathcal{S}$. ■

Proposition 4.4.4 *Le cardinal de* $\mathcal{S}$ *est* 192.

Démonstration:

Soit $g = ((a, b, c, d, e, f), (1\ 2)(3\ 4)(5\ 6)) \in \mathcal{W}$. Un calcul trivial nous donne

$$g^2 = ((a+b, b+a, c+d, d+c, e+f, f+e), id)$$

ainsi g est d'ordre 2 si et seulement si $a + b = c + d = e + f = 0$. Ce système admet exactement 64 solutions $(a, b, c, d, e, f) \in (\mathbb{Z}/4\mathbb{Z})^6$. Les deux autres permutations conduisant au même résultat, le cardinal de $\mathcal{S}$ est 192. ■

La conclusion de cette section est que nous pouvons trouver un automorphisme α correspondant à une transposition avec seulement 192 tests.

4.4.2 Détermination de γ

Dans cette section nous déterminons un automorphisme $\gamma \neq \alpha$ correspondant à une transposition commutant avec α.

Proposition 4.4.5 *L'ensemble* $\mathcal{S}'$ *des éléments* t *de* $\mathcal{W}$ *d'ordre* 2 *commutant avec* $\tilde{\alpha}$ *tel que* $\Sigma(t)$ *est dans* $\mathcal{C}$ *contient exactement un élément de* $\tilde{G}$.

Démonstration:
Il existe exactement un élément $\gamma \neq \alpha$ dans G tel que γ est conjugué à α et commute avec α. Les deux éléments $\tilde{\gamma}$ et $\tilde{\alpha}$ commutent et $\Sigma(\tilde{\gamma})$ est dans $\mathcal{C}$, ainsi $t = \tilde{\gamma}$ est la seule solution. ■

Proposition 4.4.6 *Le cardinal de $\mathcal{S}'$ est* 48.
Démonstration:
L'ensemble des éléments de $\mathcal{C}$ commutant avec $(1\ 2)(3\ 4)(5\ 6)$ est

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

Par conjugaison, il y a exactement six éléments de $\mathcal{C}$ commutant avec $\Sigma(\alpha)$. Soient

$$s = ((a, -a, c, -c, e, -e), (1\ 2)(3\ 4)(5\ 6)) \text{ et}$$
$$t = ((a', b', c', d', e', f'), (1\ 3)(2\ 4)(5\ 6))$$

des éléments de $\mathcal{W}$, nous avons les identités

$$\begin{aligned} st &= ((a+b', a'-a, c+d', c'-c, e+f', e'-e), (1\ 4)(2\ 3)(5\ 6)) \\ ts &= ((a'-a, b'+a, c'-c, d'+c, e'-e, f'+e), (1\ 4)(2\ 3)(5\ 6)) \\ t^2 &= ((a'+c', b'+d', c'+a', b'+d', e'+f', f'+e'), id) \end{aligned}$$

ainsi les conditions $st = ts$ et $t^2 = 1$ sont équivalentes à

$$\begin{cases} a'+c' = b'+d' = e'+f' = 0 \\ a+b' = a'-a, \quad c+d' = c'-c, \quad e+f' = e'-e \end{cases}$$

qui conduit à

$$\begin{cases} c' = -a', \quad d' = -b', \quad f' = -e' \\ b' = a'-2a, \quad c' = 2c-b', \quad 2e' = 2e \end{cases} .$$

Les solutions de ce système sont déterminées par les valeurs de a' et e' donc il y a 8 solutions. Par conjugaison, nous concluons que le cardinal de $\mathcal{S}'$ est $8 \times 6 = 48$. ■
Nous concluons que nous pouvons trouver γ avec seulement 48 tests.

4.4.3 Détermination de β

Dans cette section, nous déterminons β correspondant à une transposition telle que $(\alpha\beta)^3 = (\beta\gamma)^3 = id$

Proposition 4.4.7 *Si s et t sont dans $\mathcal{C}$ et commutent, il existe exactement* 4 *éléments u de $\mathcal{C}$ vérifiant la relation $(us)^3 = (ut)^3 = 1$.*

Démonstration:
Par conjugaison, nous pouvons réduire le problème au cas où

$$s = (1\ 2)(3\ 4)(5\ 6) \text{ et } t = (1\ 3)(2\ 4)(5\ 6)\ .$$

Notons d'abord que deux éléments de $\mathcal{C}$ ayant une transposition commune dans leur décomposition en produit de cycles à support disjoint doivent commuter. L'élément u ne peut pas commuter avec s sinon nous aurions $(us)^3 = u^3s^3 = us = 1$ et donc $u = s$ et finalement $(st)^3 = st = 1$ qui est faux, et de la même façon u ne peut pas commuter avec t. Nous concluons que les seules valeurs possibles de u sont

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

toutes vérifiant $(us)^3 = (ut)^3 = 1$. ■

Proposition 4.4.8 *Soient $s = \Sigma(\tilde{\alpha})$, $t = \Sigma(\tilde{\gamma})$ et $u \in \mathfrak{S}_6$ vérifiant la relation $(us)^3 = (ut)^3 = 1$. L'ensemble $\mathcal{S}''$ de tout les éléments h de $\mathcal{W}$ d'ordre 2 tel que $(\tilde{\alpha}h)^3 = (\tilde{\gamma}h)^3 = 1$ et $\Sigma(h) = u$, contient exactement un élément de $\tilde{G}$.*
Démonstration:

Il existe exactement 4 transpositions $\beta \in G$ tel que $(\alpha\beta)^3 = (\beta\gamma)^3 = id$, et elles sont en bijection par $\Sigma \circ I$ avec les quatre éléments donnés par la proposition 4.4.7. Nous concluons qu'il existe $\beta \in G$ tel que $\Sigma(\tilde{\beta}) = u$. En posant $h = \tilde{\beta}$, nous voyons que h est d'ordre 2 et $(\tilde{\alpha}h)^3 = (\tilde{\gamma}h)^3 = 1$. ■

Proposition 4.4.9 *Le cardinal de $\mathcal{S}''$ est 8.*
Démonstration:
Par conjugaison et pour simplifier, nous supposons que

$$\tilde{\alpha} = ((a, -a, b, -b, c, -c), (1\ 2)(3\ 4)(5\ 6))\ ,$$

$$\tilde{\gamma} = ((e, f, -e, -f, g, -g), (1\ 3)(2\ 4)(5\ 6))\ ,$$

$u = (1\ 4)(2\ 5)(3\ 6)$ et $\tilde{\beta} = ((h, i, j, -h, -i, -j), u)$. Nous avons les relations

$$\begin{aligned}
\tilde{\beta}\tilde{\alpha} &= ((h-b, i+c, j-c, a-h, -a-i, b-j), (1\ 5\ 3)(2\ 4\ 6)) \\
(\tilde{\beta}\tilde{\alpha})^2 &= ((h-b-a-i, i+c+a-h, j-c+h-b, a-h+b-j, \\
&\quad -a-i+j-c, b-j+i+c), (1\ 3\ 5)(2\ 6\ 4)) \\
(\tilde{\beta}\tilde{\alpha})^3 &= ((h-b-a-i+j-c, i+c+a-h+b-j, j-c+h-b-a-i, \\
&\quad a-h+b-j+i+c, -a-i+j-c+h-b, b-j+i+c+a-h), id))
\end{aligned}$$

$$
\begin{aligned}
\tilde{\beta}\tilde{\gamma} &= ((h-f, i+g, j-g, -h+e, -i+f, -j-e), (1\ 6\ 2)(3\ 4\ 5)) \\
(\tilde{\beta}\tilde{\gamma})^2 &= ((h-f-j-e, i+g+h-f, j-g-h+e, -h+e-i+f, \\
&\quad -i+f+j-g, -j-e+i+g), (1\ 2\ 6)(3\ 5\ 4)) \\
(\tilde{\beta}\tilde{\gamma})^3 &= ((h-f-j-e+i+g, i+g+h-f-j-e, j-g-h+e-i+f, \\
&\quad e-h-i+f+j-g, f-i+j-g-h+e, i+g-j-e+h-f), id))
\end{aligned}
$$

dons la condition $(\tilde{\beta}\tilde{\alpha})^3 = (\tilde{\beta}\tilde{\gamma})^3 = 1$ équivaut à

$$
\begin{cases}
h-b-a-i+j-c=0 \\
h-f-j-e+i+g=0
\end{cases}
$$

qui conduit à

$$
\begin{cases}
2h = a+b+c+f+e-g, \\
i-j = f+e-g-h
\end{cases}
.
$$

Les solutions de ce système sont déterminées par les valeurs de h et de i donc il y a exactement 8 solutions. Par conjugaison, cela est vrai pour toutes valeurs de u,$\tilde{\alpha}$ et de $\tilde{\gamma}$.

Nous concluons donc que le cardinal de $\mathcal{S}'$ est $8 \times 6 = 48$. ■

Nous pouvons donc trouver β avec seulement 8 tests. Puisque α, β et γ engendrent le groupe entier, nous avons résolu le problème avec au plus 248 tests et en 117.6 tests en moyenne.

4.5 Calcul des automorphismes pour une extension de groupe de Galois faiblement hyper-résoluble

"'Tis the note of the Jubjub! Keep count, I entreat;
You will find I have told it you twice.
'Tis the song of the Jubjub! The proof is complete,
If only I've stated it thrice."

Lewis Carroll, The Hunting of the Snark

4.5.1 Résultats sur les groupes hyper-résolubles

Nous rappelons la définition suivante.

Définition 4.5.1 (hyper-résoluble) *Un groupe G est hyper-résoluble si il*

admet une suite croissante de sous-groupes $(H_i)_{i=0}^n$ *telle que*

1. *nous avons* $H_0 = \{1\}$ *et* $H_n = G$,
2. *pour tout* $0 \leqslant i \leqslant n$ *le sous-groupe* H_i *est distingué dans* G,
3. *pour tout* $0 \leqslant i < n$ *le quotient* H_{i+1}/H_i *est cyclique.*

Jusqu'à $n \leqslant 100$, il n'existe des groupes non hyper-résolubles que de cardinal multiple de 12, de 56, de 75 ou de 80. Il y a un seul groupe non hyper-résoluble d'ordre 12, le groupe $\mathfrak{A}_4$.
Nous admettrons le théorème de structure suivant(voir [Hall, page 169]):

Théorème 4.5.2 *Soit* G *un groupe hyper-résoluble d'ordre* $\prod_{i=1}^{n} p_i$ *avec* $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_n$ *premiers, alors il existe une suite* $(h_i)_{i=1}^n$ *d'éléments de* G *telle que pour tout* $1 \leqslant i < n$ *le sous-groupe* H_i *engendré par* $(h_j)_{j=1}^i$ *est distingué dans* G *et de cardinal*

$$C_i = \prod_{j=1}^{i} p_j$$

De plus toute suite croissante de sous-groupes distingués peut-être raffinée en une suite de cette nature.

Corollaire 4.5.3 *Si* m *est un entier tel que* $1 \leqslant m < n$ *et* $p_m \neq p_{m+1}$ *alors il existe un et un seul seul sous-groupe d'ordre* C_m *et il est distingué . De plus tout sous-groupe dont l'ordre divise* C_m *est inclus dans* H_m

Corollaire 4.5.4 *Les* p_1*-Sylow de* G *sont distingués.(i.e. il n'y en a qu'un seul).*

Nous utiliserons aussi le résultat suivant:
Théorème 4.5.5 *Soit* G *un groupe et* p *le plus petit diviseur premier de son ordre. Alors tous les sous-groupes d'indice* p *sont distingués.*
Imaginons que l'on trouve un élément g d'ordre C_m dans le groupe, alors il engendre H_m et donc un sous-groupe distingué et même tous les éléments d'ordre C_m sont des puissances de g. De plus s'il apparaît que le groupe engendré par g n'est pas distingué, cela prouve que le groupe n'est pas hyper-résoluble.

4.5.2 Groupes faiblement hyper-résolubles

Nous introduisons par commodité pour l'étude du champ d'application de l'algorithme la définition suivante:

Définition 4.5.6 (faiblement hyper-résoluble) *Un groupe* G *est faiblement hyper-résoluble s'il admet une suite croissante de sous-groupes* $(H_i)_{i=0}^n$

telle que

1. *nous avons* $H_0 = \{1\}$,
2. *pour tout* $0 \leqslant i \leqslant n$ *le sous-groupe* H_i *est distingué dans* G,
3. *pour tout* $0 \leqslant i < n$ *le quotient* H_{i+1}/H_i *est cyclique,*
4. *et soit* $H_n = G$ *soit* G/H_n *est isomorphe à* $\mathfrak{A}_4$ *ou* $\mathfrak{S}_4$.

La table 4.1 nous montre le nombre de groupes non hyper-résolubles et non faiblement hyper-résolubles d'ordre inférieur à 100.

ordre	nb groupe	nb non H.R.	nb non F.H.R
12	5	1	0
24	15	3	0
36	14	3	1
48	52	10	2
56	13	1	1
60	13	2	1
72	50	13	5
80	52	1	1
84	15	2	0
96	231	36	10

TAB. 4.1 – *Groupes non hyper-résolubles*

4.5.3 Relèvement d'un élément diagonal

Lemme 4.5.7 *L'ensemble des automorphismes diagonaux est l'intersection des groupes de décomposition des idéaux au-dessus de* p

Démonstration:
σ est diagonal si et seulement si pour tout $1 \leqslant i \leqslant g$ il existe a_i tel que $\sigma(x) \equiv x^{p^{a_i}} \pmod{\mathfrak{P}_i}$, ce qui équivaut à σ appartient à $\langle \varphi_i \rangle$ qui est précisément le groupe de décompositions de $\mathfrak{P}_i$. ■
La proposition suivante nous permettra de déterminer les automorphismes diagonaux:

Proposition 4.5.8 *Il existe un automorphisme diagonal* $\sigma \neq id$ *si et seulement il existe un diviseur strict* d *de* f *tel que* $\langle \varphi_1^d \rangle \trianglelefteq G$. *De plus, dans ce cas*

– *il existe une application* $\psi | \{1, \ldots, g\} \longrightarrow (\mathbb{Z}/\frac{f}{d}\mathbb{Z})^*$ *telle que*

$$\forall i \in \{1, \ldots, g\} \quad \sigma = \varphi_i^{d\psi(i)}$$

– $\operatorname{Im}\psi$ *est un sous-groupe et tous les éléments de* ψ *admettent le même nombre d'antécédents.*

Démonstration:
Soit σ un automorphisme diagonal alors $\sigma \in \langle\varphi_i\rangle$ et donc $\sigma = \varphi_i^{a_i}$. Comme les φ_i ont tous le même ordre, il existe $d = f/|\sigma|$ et $\psi(i) \in (\mathbb{Z}/\frac{f}{d}\mathbb{Z})^*$ tel que $d\psi(i) = a_i$. Si $\tau \in G$ alors il existe i tel que

$$\tau\varphi_1^d\tau^{-1} = \varphi_i^d = \varphi_1^{d\psi(1)/\psi(i)} \in \langle\varphi_1^d\rangle \tag{4.5}$$

et donc $\langle\varphi_1^d\rangle \trianglelefteq G$.
Réciproquement si il existe $d|f, d \neq f$ tel que $\langle\varphi_1^d\rangle \trianglelefteq G$, soit $\sigma = \varphi_1^d$ et τ tel que $\tau\varphi_1\tau^{-1} = \varphi_i$ alors il existe $\psi(i) \in (\mathbb{Z}/\frac{f}{d}\mathbb{Z})^*$ indépendant de τ tel que $\tau\varphi_1^d\tau^{-1} = \varphi_i^d = \varphi_1^{d\psi(i)^{-1}}$ et donc $\varphi_1^d = \varphi_i^{d\psi(i)}$ appartient au groupe de décomposition de $\mathfrak{P}_i$
Il nous reste à prouver les propriétés de ψ, qui se factorise de la façon suivante:

$$\begin{array}{ccccccccc} \{1,,g\} & \overset{\psi_1}{\longleftrightarrow} & G/\langle\varphi_1\rangle & \overset{\psi_2}{\twoheadrightarrow} & G/C_G(\langle\varphi_1^d\rangle) & \overset{\psi_3}{\hookrightarrow} & Aut(\langle\varphi_1^d\rangle) & \overset{\psi_4}{\longleftrightarrow} & (\mathbb{Z}/\frac{f}{d}\mathbb{Z})^* \\ i & \mapsto & \{\tau;\tau(\mathfrak{P}_1) = \mathfrak{P}_i\} & \mapsto & \{\tau;\tau\varphi_1^d\tau^{-1} = \varphi_i^d\} & \mapsto & i_\tau & \mapsto & \psi(i) \end{array}$$

où $C_G(\langle\varphi_1^d\rangle)$ est le centralisateur de $\langle\varphi_1^d\rangle$ et i_τ est l'automorphisme intérieur associé à τ, de plus $\operatorname{Ker} i = C_G(\langle\varphi_1^d\rangle)$ ce qui prouve que ψ_3 est un morphisme de groupe injectif bien défini. ψ_1 correspond à la bijection de $G/Stab_{\mathfrak{P}_1}$ sur $Orb_{\mathfrak{P}_1}$ et ψ_4 est un isomorphisme de groupe. ψ_2 est la projection canonique de $G/\langle\varphi_1\rangle$ sur $G/C_G(\langle\varphi_1^d\rangle)$, elle est donc surjective et tout éléments de $\operatorname{Im}\psi_2$ admet le même nombre d'antécédents par ψ_2, il en est donc de même pour ψ et $\operatorname{Im}\psi = \operatorname{Im}\psi_3$ est un sous-groupe ■
Pour un groupe H fixé, il y a $\frac{g!}{h(g/h)!^h}$ applications ψ possibles. Nous pouvons donc tester si σ^d est un automorphisme diagonal de la façon suivante

Algorithme 4.5.9 *Soient* T *et* p *comme précédemment, et* d *un entier divisant strictement* f*, nous déterminons* φ_1^d *si* $\langle\varphi_1^d\rangle \trianglelefteq G$

1. [Boucle sur les sous-groupes] *Pour chaque sous-groupe* $H \subset (\mathbb{Z}/\frac{f}{d}\mathbb{Z})^*$ *d'ordre* h *divisant* g*,*

1.1. [Boucle sur les ψ] *Pour chaque surjection* ψ *de* $\{1,\ldots,g\}$ *dans* H *vérifiant* $\psi(1) = 1$ *et telle que chaque élément de* H *admette* g/h *antécédents, tester si* $(d\psi(i))_{i=1}^g, id) \in \tilde{G}$*.*

1.2. [Succès?] *Dans ce cas retourner* ψ*.*

2. [Fin] *Retourner «*$\langle\varphi_1^d\rangle \not\trianglelefteq G$ *ou* T *non galoisien».*

4.5.4 Stratégie de détermination du groupe de Galois

Nous devons donc choisir un nombre premier p dont une puissance non-trivialle de l'automorphisme de Frobenius φ_1 engendre un sous-groupe cyclique distingué. Le groupe étant supposé faiblement hyper-résoluble, il possède des sous-groupes cycliques distingués, à moins qu'il ne s'agisse de $\mathfrak{A}_4$ ou de $\mathfrak{S}_4$ déjà traités précédemment.

Nous utilisons l'algorithme suivant pour obtenir un bon candidat pour le nombre premier p.

Algorithme 4.5.10 *Soit $T \in \mathbb{Z}[X]$ irréductible unitaire de degré n*

1. [Factorisation] *Factoriser n en $\prod_{i=1}^{r} p_i$ avec $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_r$ premiers.*

2. [Calcul des C_m] *Poser $m_{max} := 0$, $p_{max} := 0$ et*

$$M := \{1 \leqslant m < r-1; p_m \neq p_{m+1}\} \cup \{r-1\} \ .$$

3. [Boucle] *Pour les $n/2+8$ premiers nombres premiers $p > n$, effectuer les étapes suivantes :*

3.1. [Décomposition] *Factoriser T modulo p.*

3.2. [Ramifié ?] *Si T a un facteur carré, ne pas le compter et passer au suivant.*

3.3. [Galois ?] *Si les facteurs de T n'ont pas tous le même degré, échouer avec « T n'est pas galoisien. »*

3.4. [Qualité] *Sinon soit f le degré commun des facteurs de T, si $f = n/p_r$, poser $m = n/p_r$, sinon calculer le plus grand $m \in M$ tel que $C_m | f$.*

3.5. [Meilleur ?] *si $m > m_{max}$ ou si $m = m_{max}$ et $f > f_{max}$, poser $m_{max} = m$, $p_{max} = p$ et $f_{max} = f$.*

4. [Fin] *Retourner p_{max} et m_{max}.*

Si à la fin de l'algorithme $m_{max} > 1$, nous sommes sûrs que si le groupe de Galois est hyper-résoluble, la puissance $f_p/m_{max}^{ème}$ de l'automorphisme de Frobenius engendre un sous-groupe cyclique distingué dans G. Sinon, nous nous sommes donné une « meilleure » chance, puisqu'il y au moins un sous groupe cyclique distingué non trivial de G dont l'ordre divise f_p.

Nous procédons donc ainsi :

Algorithme 4.5.11 *Soit $T \in \mathbb{Z}[X]$ irréductible unitaire de degré n*

1. [Algorithme 4.5.10] *Appliquer l'algorithme 4.5.10 pour déterminer un bon candidat p.*

2. [Factorisation] *Factoriser f_p en $f_p = \prod_{i=1}^{r} p_i^{e_i}$.*

3. [Boucle sur les premiers] *Pour $1 \leq i \leq r$, exécuter les étapes suivantes*

3.1. [Boucle sur les exposants] *Poser $S_p = X$, $H_0 = 1$, $d_p = e_i$ et $\psi_0(k) = 1$ pour $1 \leq k \leq f_p$. Pour $1 \leq j \leq e_i$, exécuter les étapes suivantes,*

3.2. [Choix du degré] *Calculer $d = f_p/p_i^j$.*

3.3. [Relèvement du groupe] *Déterminer la liste L des sous-groupes de $(\mathbb{Z}/p_i^j\mathbb{Z})^*$ qui admettent H_{j-1} pour quotient.*

3.4. [Algorithme 4.5.9] *Appliquer l'algorithme 4.5.9 à p avec le paramètre $d = f_p$, seulement pour les sous-groupes de la liste L et pour les fonctions ψ compatibles avec ψ_{i-1}.*

3.5. [Échec ?] *Si l'algorithme échoue, poser $d_p = j - 1$ et passer au nombre premier suivant.*

3.6. [Succès ?] *Appeler H_i le groupe, ψ_i la fonction et S_p le polynôme retournés par l'algorithme.*

4. [Théorème chinois] *Par application du théorème des restes chinois, combiner les polynômes S_p pour obtenir un automorphisme S d'ordre $\prod_{i=1}^{r} p_i^{d_{p_i}}$. De même calculer la fonction ψ correspondante par application du théorème des restes chinois.*

5. [Fin] *Retourner S et ψ.*

4.5.5 Calcul des autres automorphismes par tests des permutations

Nous supposons que l'algorithme précédent a réussi et qu'il nous a retourné $\sigma = \varphi_1^d$ et la fonction ψ correspondante.

Remarquons que le groupe $\langle\sigma\rangle$ étant distingué dans G, le corps fixe est aussi Galoisien et faiblement hyper-résoluble. Nous utilisons les techniques de la section 2.2.1 pour déterminer un polynôme R définissant le corps fixe K^σ et nous lui appliquons récursivement notre algorithme, et nous obtenons explicitement les automorphismes de $\mathrm{Gal}(K^\sigma/\mathbb{Q}) = G/\langle\sigma\rangle$. Il s'agit de relever $\overline{\tau} \in G/\langle\sigma\rangle$ en $\tau \in G$

Proposition 4.5.12 *Notons $t = |\overline{\tau}|$, $s = |\sigma| = f/d$. Il existe $(\overline{u}, \overline{v}) \in (\mathbb{Z}/s\mathbb{Z})^2$ tel que*

$$\tau\sigma\tau^{-1} = \sigma^u \tag{4.6}$$

$$\tau^t = \sigma^v \tag{4.7}$$

- *$\overline{u}$ ne dépend que de $\overline{\tau}$*
- *Si $\tau(\mathfrak{P}_1) = \tau(P_c)$ alors $\overline{u} = \psi(1)/\psi(c)$ convient.*

- $(u-1)v \equiv 0 \pmod{s}$
- *Si* $w = PGCD((\sum_{i=1}^{t} u^i), s)$, *alors la classe de* v *modulo* w *ne dépend que de* $\overline{\tau}$.

Démonstration:
Soit c tel que $\tau(\mathfrak{P}_1) = \tau(P_c)$, alors l'identité 4.5 nous donne $\tau\sigma\tau^{-1} = \sigma^{\psi(1)/\psi(c)}$ et $u = \psi(1)/\psi(c)$ L'identité $\overline{\tau}^t = 1$ implique que $\tau^t \in \langle\sigma\rangle$. Il existe donc v défini modulo s tel que $\tau^t = \sigma^v$. Comme

$$\sigma^{uv} = (\tau\sigma\tau^{-1})^v = \tau\sigma^v\tau^{-1} = \tau\tau^t\tau^{-1} = \sigma^v$$

il vient $\sigma^{(u-1)v} = 1$ et donc $(u-1)v \equiv 0 \pmod{s}$. Soit $\rho = \tau\sigma^k$ un autre représentant de $\overline{\tau}$, alors

$$\rho\sigma\rho^{-1} = \tau\sigma^k\sigma\sigma^{-k}\tau^{-1} = \tau\sigma\tau^{-1} = \sigma^u$$

donc u est indépendant de k. Par contre

$$\rho^t = \prod_{i=1}^{t} \tau\sigma^k = (\prod_{i=1}^{t} \tau^i\sigma^k\tau^{-i})\tau^t = (\prod_{i=1}^{t} \sigma^{ku^i})\tau^t = \sigma^{\sum_{i=1}^{t} u^i}\sigma^u = \sigma^{v+w'k}$$

avec $w' = \sum_{i=1}^{t} u^i$, ainsi la classe de v modulo $w = PGCD(w', s)$ ne dépend que de $\overline{\tau}$. ■

La proposition 2.2.3 nous permet de calculer directement u.

Algorithme 4.5.13 *Supposons* R *sans facteur carré modulo* p, *soit* $\overline{\tau} \in G/\langle\sigma\rangle$ *et* $Q = \tau(X) \pmod{R, p}$, *nous déterminons un entier* c *tel que* $\tau(\mathfrak{P}_1) = \tau(\mathfrak{P}_c)$ *ainsi:*

1. [Factorisation] *Nous obtenons une factorisation* $\overline{R} = \prod_{i=1}^{g} R_i \pmod{p}$ *comme indiqué dans la proposition 2.2.3*
2. [Action de τ] *Nous calculons* $P = PGCD(R \pmod{p}, R_1 \circ Q \pmod{p})$.
3. [Recherche] *Nous déterminons* c *tel que* $P = R_c \pmod{p}$ *par tests successifs.*
4. [Fin] *Nous retournons* $u = \psi(c)$.

Proposition 4.5.14 *Soit* $\sigma, \overline{\tau}, u$ *et* v *comme précédemment. Calculons les décompositions en cycles de* σ *comme permutation des racines de* T *et de* $\overline{\tau}$ *comme agissant sur les racines de* R *et ordonnons les cycles et numérotons les racines par des triplets* $[a, b, c] \in \mathbb{Z}/\frac{n}{st}\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ *désignant le* $c^{ème}$ *élément du* $b^{ème}$ *cycle de la* $a^{ème}$ *orbite de* τ. *Nous avons les règles suivantes, découlant de (4.6)*

$$\sigma([a, b, c]) = [a, b, c+1] \tag{4.8}$$

$$\tau([a, b, c]) = [a, b+1, d] \Rightarrow \tau([a, b, e]) = [a, b+1, u(e-c)+d] \tag{4.9}$$

Supposons choisies les valeurs $\tau([a,b,0])$ pour tout couple (a,b) avec $b \neq t-1$ alors l'équation (4.7) détermine automatiquement $\tau([a,t-1,0])$ et l'implication (4.9) détermine automatiquement les autres valeurs de τ.

Exemple 4.5.15 *Supposons que σ et τ correspondent aux permutations suivantes*

$$\begin{aligned} \sigma &= (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)(11\ 12\ 13\ 14\ 15) \\ &\quad (16\ 17\ 18\ 19\ 20)(21\ 22\ 23\ 24\ 25)(26\ 27\ 28\ 29\ 30) \\ \overline{\tau} &= (123)(456) \end{aligned}$$

avec $o=2, t=3$ et $s=5$. Les nombres représentés par les triplets, sont par ordre lexicographique

$$\begin{array}{ccc} (1\ \ 2\ \ 3\ \ 4\ \ 5\ \ ) & (6\ \ 7\ \ 8\ \ 9\ \ 10\ \ ) & (11\ 12\ 13\ 14\ 15\ ) \\ (16\ 17\ 18\ 19\ 20) & (21\ 22\ 23\ 24\ 25) & (26\ 27\ 28\ 29\ 30) \end{array}$$

où par exemple,

$$[0,0,0]=1;\ [0,0,1]=2;\ [0,1,0]=6;\ [1,0,0]=16;\ [1,1,4]=25\ .$$

Algorithme 4.5.16 *Soit σ, $\overline{\tau}$ et u comme précédemment. Il s'agit de relever $\overline{\tau}$ en un élément τ de G.*

1. [Décomposition en cycles] *Calculer les décompositions en cycles de σ comme permutation des racines de T et de $\overline{\tau}$ comme agissant sur les racines de R.*

2. [Numérotation] *Ordonner les cycles et numéroter les racines avec 3 composantes comme dans la proposition 4.5.14*

3. [Calcul de u et w] *Calculer u et w à l'aide de la proposition 4.5.12 et de l'algorithme 4.5.13*

4. [Boucle] *Pour chaque valeur de $0 \leqslant v \leqslant w$ et pour chaque application C de $\{0,\ldots,\frac{n}{st}-1\} \times \{0,\ldots,t-2\}$*

4.1. [Calcul de τ] *Déterminer τ tel que*

$$\forall (a,b) \in \{0,\ldots\frac{n}{st}-1\} \times \{0,\ldots,t-2\} \quad \tau([a,b,0]) = C(a,b)$$

d'après la proposition 4.5.14

4.2. [Test] *Tester si τ correspond effectivement à un élément du groupe de Galois de T.*

4.3. [Succès ?] *Si oui, retourner τ.*

5. [Échec] *Retourner «G non galoisien».*

Pour chaque u, le nombre d'applications à tester est de $s^{(t-1)(n/st)} = s^{n/s(1-1/t)}$.

Il apparaît donc que le nombre de tests croît avec t. Il est donc préférable de procéder ainsi:

Algorithme 4.5.17 *1.* [Factorisation] *Factoriser t en $t = \prod_{i=1}^{r} p_i^{e_i}$.*
2. [Boucle sur les premiers] *Pour $1 \leq i \leq r$, exécuter les étapes suivantes*
2.1. [Relèvement] *Poser $d_i = t/p_i^{e_i}$ et relever $\overline{\tau}^{d_i}$ pour obtenir τ_i.*
3. [Théorème chinois] *Par application du théorème des restes chinois, reconstruire τ à partie des $(\tau_i)_{i=1}^{r}$ et retourner τ.*

4.6 Résumé de l'algorithme

> The Beaver had counted with scrupulous care,
> Attending to every word:
> But it fairly lost heart, and outgrabe in despair,
> When the third repetition occurred.
>
> Lewis Carroll, The Hunting of the Snark

Algorithme 4.6.1 *Soit $T \in \mathbb{Z}[X]$ irréductible unitaire de degré n. Si T est galoisien hyper-résoluble, l'algorithme retourne $(\sigma_i)_{i=1}^{n}$ du groupe de Galois G tel que pour tout $1 \leqslant m \leqslant n$ nous ayons $\langle \sigma_i \rangle_{i=1}^{m} \trianglelefteq G$ et $\langle \sigma_i \rangle_{i=1}^{n} = G$*
1. [Étude du groupe] *Appliquer l'algorithme 4.5.10 pour obtenir p_{max} et m_{max}.*
2. [$\mathfrak{A}_4$ ou $\mathfrak{S}_4$?] *Si $n = 12$ (resp. $n = 24$) et que $f_{p_{max}} = 3$, le groupe de Galois est très probablement $\mathfrak{A}_4$ (resp. 24). Tester d'abord l'algorithme spécifique pour ce groupe. En cas d'échec, retourner à l'étape 1, en regardant les nombre premiers suivants.*
3. [Premier élément] *Appliquer l'algorithme 4.5.11. S'il échoue, si $m_{max} > 0$ retourner «T non galoisien ou non faiblement hyper-résoluble», sinon retourner à l'étape 1, en regardant les nombre premiers suivants.*
4. [Fin?] *L'étape précédente a retourné un automorphisme $\sigma = \varphi_1^d$. Si $|\sigma| = n$, retourner σ.*
5. [Corps fixe] *Appliquer la proposition 2.2.1 pour obtenir un polynôme R.*
6. [Appel récursif] *Appliquer récursivement l'algorithme pour déterminer une famille $(\overline{\tau_1}, \ldots, \overline{\tau_t})$ génératrice de $G/\langle\sigma\rangle$.*
7. [Relèvement] *Appliquer l'algorithme 4.5.17 pour obtenir $(\tau_1, \ldots, \tau_t)$ et nous retournons $(\sigma, \tau_1, \ldots, \tau_t)$.*

Si T est galoisien et non hyper-résoluble, l'algorithme peut boucler indéfiniment. En pratique cela se produit pour $n \leqslant 100$ seulement si $36|n$.

4.7 Exemple

It felt that, in spite of all possible pains,
It had somehow contrived to lose count,
And the only thing now was to rack its poor brains
By reckoning up the amount.

Lewis Carroll, The Hunting of the Snark

Comme exemple, nous allons calculer les automorphismes du polynôme

$$\begin{aligned} T = x^{21} - 7x^{20} - 21x^{19} + 238x^{18} - 245x^{17} - 1848x^{16} + 4732x^{15} + 1861x^{14} \\ -18536x^{13} + 16856x^{12} + 14819x^{11} - 32431x^{10} + 8897x^9 + 16660x^8 \\ -13533x^7 + 392x^6 + 3514x^5 - 1547x^4 + 161x^3 + 49x^2 - 14x + 1 \end{aligned}$$

dont le groupe de Galois est le seul groupe non-abélien d'ordre 21, mais nous n'utiliserons pas la connaissance de ce fait dans le calcul.

Nous commençons par écrire $21 = p_1 p_2$ avec $p_1 = 7$ et $p_2 = 3$. Nous posons $M = \{0, 1, 2\}$.

Nous factorisons maintenant T modulo les premiers nombres premiers plus grands que 42. Nous obtenons

p	43	47	53	59	61	67	71	73	79	83	89
f_p	7	3	3	3	3	3	7	3	3	7	3
$\sup\{m \in M; C_m \mid f_p\}$	1	0	0	0	0	0	1	0	0	1	0

Nous sommes dans un cas favorable car $m_{max} = 1$. Nous n'avons pas encore trouvé de nombre premier totalement décomposé, donc nous continuons les factorisations jusqu'à trouver que $\ell = 449$ convient. Nous calculons le discriminant de T ainsi que la borne BD.

$$\mathrm{Disc}(T) = (2)^{18}(7)^{32}(181)^6(2339)^6 = D^2$$

$$BD \leqslant 10^{44}$$

Nous calculons les racines de T modulo ℓ, $\{2, 35, 45, 51, 66, 79, 96, 109, 174, 180, 223, 225, 236, 301, 305, 342, 370, 373, 397, 440, 448\}$ et nous les relevons jusqu'à la précision ℓ^{17} pour que $\ell^{17} > 2BD$. Nous posons $p = p_{max} = 43$, $f = f_p = 7$, $g = g_p = 3$ et $d = 1$, et nous appliquons l'algorithme 4.5.9. Nous devons tester 3 applications ψ de $\{1, 2, 3\}$ dans $(\mathbb{Z}/7\mathbb{Z})^*$,

$$\begin{array}{lll} 1 \mapsto 1 & 1 \mapsto 1 & \\ 2 \mapsto 1 \ , & 2 \mapsto 2 & \text{et} \\ 3 \mapsto 1 & 3 \mapsto 4 & \end{array} \qquad \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 4 \\ 3 \mapsto 2 \end{array}$$

La dernière nous donne l'automorphisme
$\alpha \mapsto (-14791767248\alpha^{20} + 95714137173\alpha^{19} + 361204094449\alpha^{18}$
$- 3328779599255\alpha^{17} + 1864224944156\alpha^{16} + 28304237511321\alpha^{15}$
$- 55006453622284\alpha^{14} - 56486002410703\alpha^{13} + 244003596280558\alpha^{12}$
$- 120533924745455\alpha^{11} - 281694320179321\alpha^{10} + 330143856833197\alpha^{9}$
$+ 41475180195786\alpha^{8} - 222891172143821\alpha^{7} + 82722087561988\alpha^{6}$
$+ 36804911589073\alpha^{5} - 32245355397328\alpha^{4} + 6074801569203\alpha^{3}$
$+ 699019170541\alpha^{2} - 345689725163\alpha + 29710312476)/76627979$
correspondant à la permutation suivante des racines ℓ-adiques

$(2, 301, 96, 66, 370, 342, 440)(35, 225, 109, 180, 236, 305, 51)$
$(45, 223, 373, 79, 448, 397, 174)$.

Nous calculons alors le corps fixe en utilisant la proposition 2.2.1 et nous obtenons $R = x^3 - x^2 - 9x + 1$. Nous appliquons récursivement l'algorithme au polynôme R : nous trouvons que R est irréductible modulo 11 et alors en relevant l'automorphisme de Frobenius, nous trouvons l'automorphisme $-1/2x^2 + 7/2$ qui engendre le groupe de Galois du corps fixe. Nous devons donc le relever en un automorphisme de G. En utilisant l'algorithme 4.5.13, nous obtenons $u = 2$ et nous appliquons l'algorithme 4.5.16 : nous devons tester les sept permutations suivantes

$(2, 35, 45)(301, 109, 448)$	$(96, 236, 223)(66, 51, 397)$
	$(370, 225, 373)(342, 180, 174)(440, 305, 79)$,
$(2, 35, 223)(301, 109, 397)$	$(96, 236, 373)(66, 51, 174)$
	$(370, 225, 79)(342, 180, 45)(440, 305, 448)$,
$(2, 35, 373)(301, 109, 174)$	$(96, 236, 79)(66, 51, 45)$
	$(370, 225, 448)(342, 180, 223)(440, 305, 397)$,
$(2, 35, 79)(301, 109, 45)$	$(96, 236, 448)(66, 51, 223)$
	$(370, 225, 397)(342, 180, 373)(440, 305, 174)$,
$(2, 35, 448)(301, 109, 223)$	$(96, 236, 397)(66, 51, 373)$
	$(370, 225, 174)(342, 180, 79)(440, 305, 45)$,
$(2, 35, 397)(301, 109, 373)$	$(96, 236, 174)(66, 51, 79)$
	$(370, 225, 45)(342, 180, 448)(440, 305, 223)$,
$(2, 35, 174)(301, 109, 79)$	$(96, 236, 45)(66, 51, 448)$
	$(370, 225, 223)(342, 180, 397)(440, 305, 373)$

La seconde permutation correspond à un automorphisme, que nous calculons:
$\alpha \mapsto (-194129435\alpha^{20} + 1263256585\alpha^{19} + 4695474072\alpha^{18} - 43866808007\alpha^{17}$
$+26044995959\alpha^{16}+370791458219\alpha^{15}-735728499700\alpha^{14}-716698532307\alpha^{13}+$
$3233978982336\alpha^{12}-1696567684697\alpha^{11}-3658157589221\alpha^{10}+4481659267398\alpha^{9}+$
$407309044781\alpha^{8} - 2976215526118\alpha^{7} + 1190032598839\alpha^{6} + 464793759571\alpha^{5}$

$-447754215324\alpha^4 + 90593004738\alpha^3 + 9006434498\alpha^2 - 5016784391\alpha$
$+ 438769426)/423359$.

Nous avons donc une partie génératrice du groupe de Galois, et nous pouvons en calculer tous les éléments.

4.8 Mise en œuvre

"Two added to one–if that could but be done,"
It said, "with one's fingers and thumbs!"
Recollecting with tears how, in earlier years,
It had taken no pains with its sums.

Lewis Carroll, The Hunting of the Snark

Cet algorithme a été mis en œuvre et intégré à [PARI, fonction `nfgaloisconj`]. Il est capable en pratique de traiter tous les groupes de Galois faiblement hyper-résolubles d'ordre inférieur ou égal à 95. Les mesures de temps ont été effectuées sur un Pentium III à 800MHz ayant 1 Go de mémoire vive. Dans la première partie, nous utilisons des polynômes de notre base de données dont le degré est multiple de 4. Les classes d'isomorphismes des groupes de

Galois des polynômes sont toutes distinctes.

degré	nb	temps moyen
20	5	0,33 s
24	14	0,62 s
28	4	1,66 s
32	20	1,57 s
36	8	1,67 s
40	5	4,78 s
44	4	15,82 s
48	12	17,44 s
52	2	5,48 s
56	3	2,88 s
60	3	3,93 s
64	14	29,51 s
68	1	4,78 s
72	5	4,35 s
76	1	87,0 s
80	4	77,79 s
84	3	110,21 s
88	3	9,44 s
92	1	10,25 s
96	5	10,8 s

Dans la seconde partie, nous utilisons les polynômes minimaux des racines indiquées.

degré	nb	temps moyen	Racine
160	1	49 min	$\sqrt[20]{2} + \zeta_{20}$
192	1	108 min	$\sqrt[24]{5} + \zeta_{24}$
220	1	85 min	$\sqrt[22]{2}(\zeta_{22} - 2)$
240	1	19 min	$\sqrt[30]{2}(\zeta_{30} + 2)$
252	1	1h, 7min	$\sqrt[21]{2}(\zeta_{21} - 1)$
336	1	13h, 43min	$\sqrt[28]{2}(\zeta_{28} + 2)$

Chapitre 5

Le compilateur GP2C

5.1 GP2C le compilateur de GP en C

5.1.1 Introduction

Il s'agit d'écrire un programme [GP2C] permettant l'implantation rapide de fonction C dans la bibliothèque PARI à partir de leur équivalent en langage GP.

La pratique courante de développement de PARI consiste à d'abord écrire un script GP, le tester à l'aide de GP, puis à le convertir en langage C. Cette façon de procéder est courante dans les systèmes de calcul formel.

En l'état la traduction manuelle est malcommode et est souvent source d'erreur[1]. En effet

- La syntaxe est très différente, par exemple l'expression simple `a*b+c` devient `gadd(gmul(a,b),c)`.
- Les fonctions GP et PARI n'ont pas toujours le même nom.
- Il faut gérer la mémoire manuellement à l'aide de `gerepile`.
- GP ne connaît qu'un type de donnée, les `GEN`, pour des raisons d'efficacité il est nécessaire d'utiliser d'autres types, en particulier les entiers C `long`, ou des sous-classes du type `GEN`, les entiers PARI `t_INT`, les réels PARI `t_REAL`, etc...

5.1.2 Cahier des charges

En partant du principe qu'il est beaucoup plus simple d'optimiser un programme que de l'écrire, j'ai donc cherché à résoudre ces problèmes à l'aide

1. appelé bugs par les programmeurs, bogues (n.f.) par les académiciens qui n'en ont jamais vu et beugues par les Lyonnais traditionalistes.

d'un programme GP2C, ayant le cahier des charges suivant :

- Le code généré devait être très proche du code GP pour être compréhensible facilement par le programmeur. En particulier, il devait conserver autant que possible les noms de fonctions et de variables.
- Le code généré devait suivre les « standards » de la bibliothèque PARI, pour pouvoir y être intégré et modifié.
- Le code devait pouvoir utiliser la fonction PARI la plus efficace dans le contexte correspondant à une fonction GP donnée.
- Il n'était pas nécessaire que 100% du code GP soit traductible par le compilateur, en effet certaines instructions ne sont utiles que pour l'usage interactif.

5.1.3 Problèmes à résoudre

J'ai été confronté aux problèmes suivants :

- La grammaire de GP n'est pas LALR(1). Dans les arguments des fonctions ayant un code de prototype `s*` correspondant à la concaténation automatique et dans les déclarations de fonctions, la règle qui prévaut est celle de la plus grande sous-expression. Par exemple l'expression `print(1-[2])` est ambiguë, il s'agit soit de la soustraction de `1` et `[2]` (qui est invalide) ou bien de la concaténation de `1` et de l'opposé de `[2]` (qui est valide). L'interpréteur GP choisit la première option et retourne une erreur. De même, dans l'expression `f(x)=g(x)=x++; print(x)`, l'instruction `print(x)` fait partie de la fonction g et non de la fonction f.
- Usuellement, un compilateur transforme une expression complexe comme `x=a*d-b*c` en une suite d'expressions élémentaires à l'aide de variables intermédiaires `p1=a*d;p2=b*c;x=p1-p2` pour garantir l'ordre d'exécution des opérations et protéger contre les effets de bords, malheureusement cette approche aurait rendu le code illisible.
- Pour GP les fonctions C de type `void` retournent le pointeur spécial `gnil` qui est égal à zéro mais n'est pas affiché. Ce n'est pas le cas en C, ainsi il faut couper certaines expressions, par exemple `a=5+print(2);` doit être transformé par le compilateur en `print(2);a=5`
- Pour GP, les structures de contrôle sont des fonctions. Il a été nécessaire de créer des blocs pour les contenir. Cela fonctionne ainsi, le code

```
a=if(b,print(3);5,7)
```

est transformé en pseudocode GP

```
local(p1); a={/*la valeur du bloc est dans p1*/
           if(b,print(3);p1=5, p1=7)}
```

Puis une phase de déplacement des blocs a lieu pour obtenir

```
local(p1); if(b,print(3);p1=5, p1=7); a=p1
```

Nous voyons que le code précédent est maladroit, il aurait été préférable d'écrire `if(b,print(3);a=5, a=7)`. Ainsi nous avons ajouté une phase du compilateur qui nettoie les variables inutiles créées par le compilateur.

5.2 Typage des objets PARI

Pour améliorer les performances du code produit par le compilateur nous avons introduit un typage sur les objets PARI.

5.2.1 Définition de types principaux

Un type représente une classe d'objets PARI sur lesquels certaines opérations sont valides. Les types les plus importants sont les suivants:

nom	description
`void`	comme en C, mais doit être converti en 0 si évalué.
`bool`	booléen, vrai (1) ou faux (0) stocké dans un entier C.
`small`	entier C de type long.
`int`	entier PARI multiprécision, i.e. GEN de type t_INT.
`real`	réel PARI, i.e. GEN de type t_REAL.
`mp`	multiprécision, i.e. GEN de type t_INT ou t_REAL.
`gen`	générique, objet PARI de type GEN.

De nombreux autres types existent, en particulier pour spécifier les « member functions » (fonctions composantes) de GP. La liste complète est accessible via gp2c -t.

Par défaut, les variables GP seront donc de type `gen`. Toutefois les indices de boucles seront normalement de type `small` si le domaine de la boucle le permet.

5.2.2 Ajout des types à la syntaxe GP

Nous étendons la syntaxe GP pour accepter les constructions suivantes :

- `expr:type` signifie que l'expression `expr` a le type `type`.
- `var:type` dans une déclaration signifie que la variable `var` a le type `type` pour tout le bloc.

Nous n'autoriserons donc pas les variables à changer de type en cours de bloc. De toute façon il n'est pas considéré comme une bonne pratique de programmation d'utiliser une variable pour plusieurs usages différents.

Cela permet à l'utilisateur d'améliorer le code produit par GP2C en spécifiant le type de ses variables. Par exemple la fonction gp suivante essaie de factoriser n à l'aide de la méthode ρ de Pollard.

```
rho(n)=
{
  local(x,y);

  x=2; y=5;
  while(gcd(y-x,n)==1,
    x=(x^2+1)%n;
    y=(y^2+1)%n;
    y=(y^2+1)%n
   );
  gcd(n,y-x)
}
```

```
GEN rho(GEN n)
{
  GEN x;
  GEN y;
  x = gdeux;
  y = stoi(5);
  while (gegalgs(ggcd(gsub(y, x), n), 1))
  {
    x = gmod(gaddgs(gsqr(x), 1), n);
    y = gmod(gaddgs(gsqr(y), 1), n);
    y = gmod(gaddgs(gsqr(y), 1), n);
  }
  return ggcd(n, gsub(y, x));
}
```

Comme les variables n, x et y contiennent des entiers PARI, il n'est pas satisfaisant d'utiliser les fonctions génériques gsqr, gaddgs et gmod. Grâce à l'extension de la syntaxe, il est possible de préciser le type de ces variables au compilateur :

```
rho(n:int)=
{
  local(x:int,y:int);

  x=2; y=5;
  while(gcd(y-x,n)==1,
    x=(x^2+1)%n;
    y=(y^2+1)%n;
    y=(y^2+1)%n
   );
  gcd(n,y-x)
}
```

```
GEN rho(GEN n)   /* int */
{
  GEN x;          /* int */
  GEN y;          /* int */
  x = gdeux;
  y = stoi(5);
  while (cmpis(mppgcd(subii(y, x), n), 1) == 0)
  {
    x = modii(addis(sqri(x), 1), n);
    y = modii(addis(sqri(y), 1), n);
    y = modii(addis(sqri(y), 1), n);
  }
  return mppgcd(n, subii(y, x));
}
```

Le code généré tient compte des types de n, x et y et utilise les fonctions spécialisées sqri, addis et modii.

5.2.3 Préordre sur les types

Nous préordonnons comme indiqué dans la figure 5.1 l'ensemble des types. L'ordre correspond à l'inclusion des classes. Un type t sera inférieur à un type s s'il est possible de convertir tout objet du type t en objet du type s.

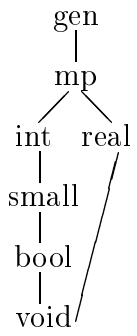

FIG. 5.1 – *Préordre sur les types*

5.3 Descriptions des fonctions et opérateurs GP

5.3.1 Présentation du langage de description

Nous avons créé un langage de description des fonctions et opérateurs GP. La syntaxe est proche de celle du langage yacc. Voila un exemple : la description de l'opérateur `+`

```
_+_:
 (small,small):small:parens     $(1) + $(2)
|(int,small):int         addis($1, $2)
|(small,int):int         addsi($1, $2)
|(int,int):int           addii($1, $2)
|(mp,real):real          mpadd($1, $2)
|(real,mp):real          mpadd($1, $2)
|(mp,mp):mp              mpadd($1, $2)
|(gen,small):gen         gaddgs($1, $2)
|(small,gen):gen         gaddsg($1, $2)
|(gen,gen):gen           gadd($1, $2)
;
```

Pour chaque type d'arguments, le type du résultat est indiqué ainsi que le code C correspondant. Dans l'exemple de la fonction `rho`, avant typage l'opérateur `+` prend un argument de type `gen` et une constante de type `small` le code généré est donc `gaddgs($1, $2)` et le type du résultat `gen`. Par contre après typage, l'opérateur `+` prend un argument de type `int` et une constante de type `small` le code généré est donc `addis($1, $2)` et le type du résultat `int`.

5.3.2 Présentation formelle du langage

Nous décrivons formellement le langage par sa forme de Backus-Naur étendue.

```
type := void | bool | small | int | real | mp | gen
attribut := prec | parens | copy
élément := type | [0-9]+
règle :=  '(' ')'  |  '(' { objet ',' }* objet ')'
champs := règle ':' type { ':' attribut }*
entrée := fonction ':' { champs code '|' }* champs code ';'
```

Pour les opérateurs, nous dérivons un nom de fonction en substituant les arguments par un caractère `_`. Ainsi `+` devient `_+_`, la factorielle devient `_!` et la négation logique devient `!_`.

- L'attribut `prec` précise que la variable `prec` est nécessaire.
- L'attribut `parens` signifie que le résultat doit être mis entre parenthèse dans un conteste qui requiert un atome (c.f. 5.4.2).
- L'attribut `copy` signifie que l'objet créé référence ses arguments et n'est donc pas autonôme. Il devra donc être copier avec `gcopy` avant d'être affecté à une variable.

5.4 Propagation des types

5.4.1 Règle de typage

Les types sont propagés des feuilles à la racine de l'arbre syntaxique.
Pour les feuilles, les règles suivantes sont utilisées :

- Les types spécifiés par l'utilisateur sont laissés tels quels.
- Les variables ont leur type de déclaration, `gen` par défaut.
- Les constantes ont leur type naturel. De plus les constantes entières représentables par un entier C `long` sont de type `small`.

Nous propageons les types vers la racine à l'aide de la table de description de la manière suivante :

Soit f une fonction ou un opérateur, et $x_1, \ldots, x_n$ ses arguments. Nous examinons les règles correspondant à l'entrée f. Nous rejetons d'abord les règles ne satisfaisant pas aux conditions suivantes

- La règle doit comporter autant d'élément que la fonction a d'arguments.
- Si l'un des éléments de la règle est un nombre, l'argument correspondant doit être une constante égale à ce nombre. Cela est utile pour tester les drapeaux (flags).
- Si l'un des éléments de la règle est un type, l'argument correspondant doit être comparable pour le préordre.

Parmi les règles restantes, nous sélectionnons une règle ainsi:

- Pour chaque élément qui est de type strictement inférieur au type de l'argument correspondant, la règle perd un point.
- La règle ayant le plus de points (i.e le moins de points négatifs) gagne.
- En cas d'égalité la première règle gagne.

Une fois que la règle est déterminée, le type du nœud [2] est défini par le type de la règle, de plus le nœud récupère aussi les attributs de la règle.

5.4.2 Génération des types

Pour chaque nœud, la règle à appliquer est déterminée comme précédemment. Le code à générer est obtenu à parti de l'atome `code` du champ contenant la règle, en substituant les `$i` par le i-ième argument. Si le numéro est entre parenthèses, comme dans `$(i)`, et que le i-ième argument possède l'attribut `parens`, alors il sera substitué entre parenthèse. Ce mécanisme évite la pulsion paranoïaque des compilateurs consistant à mettre des parenthèses partout. Ainsi l'expression `a+b+c` où `a,b,c` sont de type `small` devient `(a+b)+c` au lieu de `(((a)+(b))+(c))`.

5.5 Gestion de la mémoire

La gestion de la mémoire dans la bibliothèque PARI s'effectue ainsi :

- Les objets sont créés consécutivement dans la pile PARI.
- Chaque fonction a la responsabilité de supprimer les objets créés par les calculs intermédiaires, à l'aide de la fonction `gerepile`

2. j'en profite pour rappeler que les alphabets ISO 8859-1 et ISO 8859-15 ne comportent pas le symbole œ, ce qui les rend impropres à la représentation de texte en français.

– Lors de boucles importantes, il est nécessaire de prévoir d'effectuer une instruction gerepile si la place dans la pile risque d'être insuffisante pour finir la boucle, le test s'effectuant avec la macro lowstack.
– Les composantes d'un objet doivent être individualisées à l'aide de gcopy.

Pour générer automatiquement les instructions gerepile convenables, le compilateur maintient une liste des accès aux variables avec le type d'accès: lecture, écriture, ou écriture d'une composante (correspondant à `a[n]=b`). Il calcule les accès en écriture aux variables globales à travers les appels au sous-fonctions (voir ex. 5.5.1) par clôture. Cela lui permet de savoir quelles sont les variables qui ont été modifiées et celles qui doivent être préservées. Le compilateur génère automatiquement les tests de taille de pile dans toutes les boucles.

Exemple 5.5.1

```
global(G=vector(10));
f(x)=G[x]++;
g(x)=if(x>=1 && x<=length(G),f(x),error("x too large"));
```

La variable globale `G` *est modifiée par la fonction* `g` *à travers l'appel à la fonction* `f`.

5.6 Architecture du compilateur

J'ai suivi une architecture classique, une forme de code GP simplifié servant de code intermédiaire.

1. Un analyseur syntaxique en langage « yacc » convertit le code GP en un arbre syntaxique.
2. Pour simplifier la syntaxe, les structures de contrôles sont traduites par des instructions C simples.
3. Propagation des types à l'aide de règles de typage.
4. Déplacement des blocs.
   Après cette phase, nous avons vraiment le code intermédiaire.
5. Détermination des affectations des variables par blocs.
6. Génération des instructions gerepile.
7. Optimisation des variables créées par le compilateur.
8. Suppression des blocs vides.
9. Génération du code C à partir de l'arbre syntaxique typé et de la description des fonctions et opérateurs.

Annexe A

Table de polynômes galoisiens

> Simultanément, des milliers.
> Raymond Queneau, *Le Chiendent*

La complexité de notre algorithme dépendant de la complexité des groupes de Galois, nous avons été amené à construire une base de données de polynômes galoisiens ayant des groupes de Galois distincts. Les polynômes ont été construits à l'aide de plusieurs méthodes:

- Par clôture galoisienne de polynômes donnés par [Eichenlaub] et [KlMa], représentant tous les sous-groupes transitifs de $\mathfrak{S}_n$ pour $n \leq 15$.
- Par application de la théorie algorithmique du corps de classes, pour construire des extensions abéliennes des corps de nombres.
- *au petit bonheur* suivant [Perec], par extension des précédents et par calculs de corps fixes.

Nous avons utilisé intensivement la fonction `galoisinit` que nous avons implanté dans PARI, et le programme d'identification des groupes de permutations et la table des groupes finis du système [GAP].

Lorsque nous avions plusieurs polynômes de même groupe de Galois, nous avons sélectionné celui ayant les plus petits automorphismes, au sens suivant, tel que, α étant une racine du polynôme, le groupe abélien

$$\mathbb{Z}[\sigma(\alpha), \sigma \in G]/\mathbb{Z}[\alpha]$$

ait un exposant minimal.

Je tiens à remercier Igor Schein pour sa contribution à l'établissement et à la vérification de cette table.

Pour des raisons de place, nous avons limité la table aux polynômes de groupes de Galois non abéliens et de degré inférieur à 100.

Ordre: 6, Indice: 2, Nom: $\mathfrak{S}_3$
$x^6 + 108$
Ordre: 8, Indice: 4, Nom: D_8
$x^8 + 28x^4 + 2500$
Ordre: 8, Indice: 5, Nom: Q_8
$x^8 - 12x^6 + 36x^4 - 36x^2 + 9$
Ordre: 10, Indice: 2, Nom: D_{10}
$x^{10} - 10x^8 - 75x^6 + 1500x^4 - 5500x^2 + 16000$
Ordre: 12, Indice: 3, Nom: D_{12}
$x^{12} - 572x^6 + 470596$
Ordre: 12, Indice: 4, Nom: 6.2
$x^{12} + 3x^{11} + 74x^{10} - 1106x^9 + 2292x^8 - 66585x^7 + 662303x^6 - 2691684x^5 + 21082717x^4 - 153539367x^3 + 510340995x^2 - 741257485x^1 + 404146861$
Ordre: 12, Indice: 5, Nom: $\mathfrak{A}_4$
$x^{12} + 36x^{10} + 456x^8 + 2672x^6 + 7632x^4 + 10368x^2 + 5184$
Ordre: 14, Indice: 2, Nom: D_{14}
$x^{14} + 98x^{10} + 343x^8 + 343x^6 + 3773x^4 - 2058x^2 + 343$
Ordre: 16, Indice: 6, Nom: $D_8 \times 2$
$x^{16} - 30x^{14} + 125x^{12} + 1650x^{10} + 3612x^8 + 17670x^6 + 64325x^4 + 25350x^2 + 28561$
Ordre: 16, Indice: 7, Nom: $Q_8 \times 2$
$x^{16} - 16x^{14} + 124x^{12} - 376x^{10} + 1408x^8 - 1264x^6 + 4888x^4 + 1136x^2 + 8836$
Ordre: 16, Indice: 8, Nom: $D_8 \curlyvee 4$
$x^{16} - 20x^{14} + 302x^{12} - 2140x^{10} + 11851x^8 - 33900x^6 + 151002x^4 + 10260-0x^2 + 50625$
Ordre: 16, Indice: 9, Nom: 10
$x^{16} - 16x^{14} + 136x^{12} - 416x^{10} - 464x^8 + 5760x^6 + 18560x^4 + 12800x^2 + 6400$
Ordre: 16, Indice: 10, Nom: $(2 \times 4).2$
$x^{16} - 8x^{15} - 201x^{14} + 892x^{13} + 18358x^{12} - 9048x^{11} - 797829x^{10} - 22050-79x^9 + 10359868x^8 + 71311097x^7 + 144533539x^6 + 42113061x^5 - 26788-0287x^4 - 400831191x^3 - 192428094x^2 - 11135339x^1 + 4621601$
Ordre: 16, Indice: 11, Nom: 10
$x^{16} - 130x^{14} - 260x^{13} + 4875x^{12} + 14300x^{11} - 64870x^{10} - 238940x^9 + 231985x^8 + 1250600x^7 - 2366000x^5 - 1318200x^4 + 1216800x^3 + 1487200x^2 + 540800x^1 + 67600$
Ordre: 16, Indice: 12, Nom: D_{16}
$x^{16} + 2x^{14} - 21x^{12} - 14x^{10} + 217x^8 - 308x^6 + 168x^4 - 40x^2 + 4$
Ordre: 16, Indice: 13, Nom: QD_{16}
$x^{16} - 48x^{12} + 2496x^8 + 9216x^4 + 36864$

Ordre: 18, Indice: 3, Nom: D_{18}
$x^{18} + 18x^{16} + 27x^{14} + 459x^{10} + 3402x^8 - 3915x^6 + 13284x^4 - 12636x^2 + 3456$
Ordre: 18, Indice: 4, Nom: $\mathfrak{S}_3 \times 3$
$x^{18} + 171x^{12} + 5130x^6 + 27$
Ordre: 18, Indice: 5, Nom: $3^2 \rtimes 2$
$x^{18} - 63x^{12} + 1971x^6 + 27$
Ordre: 20, Indice: 3, Nom: D_{20}
$x^{20} + 8x^{18} - 84x^{16} - 1734x^{14} - 4124x^{12} + 72374x^{10} + 515369x^8 + 884616x^6 + 54854x^4 + 8816108x^2 + 29300569$
Ordre: 20, Indice: 4, Nom: 10.2
$x^{20} - 3x^{19} - 119x^{18} + 177x^{17} + 5889x^{16} - 1381x^{15} - 152812x^{14} - 117981x^{13} + 2164979x^{12} + 3491841x^{11} - 15663089x^{10} - 38883595x^9 + 42546574x^8 + 187263905x^7 + 52059719x^6 - 314665312x^5 - 318011368x^4 + 4965810x^3 + 106222904x^2 + 21505161x^1 - 6072119$
Ordre: 20, Indice: 5, Nom: $5 \rtimes 4$
$x^{20} + 2500x^{10} + 50000$
Ordre: 21, Indice: 2, Nom: $7 \rtimes 3$
$x^{21} - 98x^{19} + 3920x^{17} - 83496x^{15} - 686x^{14} + 1037232x^{13} + 32928x^{12} - 7760032x^{11} - 576240x^{10} + 34881728x^9 + 4609920x^8 - 90287204x^7 - 17748-192x^6 + 119800296x^5 + 30118144x^4 - 58622816x^3 - 15059072x^2 + 134456$
Ordre: 22, Indice: 2, Nom: D_{22}
$x^{22} + 24x^{20} + 250x^{18} + 1464x^{16} + 5189x^{14} + 11253x^{12} + 15224x^{10} + 14538x^8 + 9602x^6 + 4600x^4 + 1337x^2 + 167$
Ordre: 24, Indice: 4, Nom: $D_8 \times 3$
$x^{24} - 80x^{22} + 2238x^{20} - 29894x^{18} + 223781x^{16} - 1017496x^{14} + 2914259x^{12} - 5287975x^{10} + 5946850x^8 - 3933875x^6 + 1405625x^4 - 243750x^2 + 15625$
Ordre: 24, Indice: 5, Nom: $Q_8 \times 3$
$x^{24} + 8x^{23} - 24x^{22} - 328x^{21} - 90x^{20} + 5056x^{19} + 7000x^{18} - 38144x^{17} - 78904x^{16} + 147968x^{15} + 414204x^{14} - 266424x^{13} - 1153342x^{12} + 92848x^{11} + 1740480x^{10} + 321856x^9 - 1420137x^8 - 426160x^7 + 591816x^6 + 195232x^5 - 104924x^4 - 33128x^3 + 4040x^2 + 928x^1 - 71$
Ordre: 24, Indice: 6, Nom: $\mathfrak{S}_3 \times 2^2$
$x^{24} - 80x^{22} + 2328x^{20} - 32148x^{18} + 230904x^{16} - 929240x^{14} + 2169688x^{12} - 2925232x^{10} + 2172144x^8 - 799192x^6 + 117088x^4 - 6192x^2 + 100$
Ordre: 24, Indice: 7, Nom: $\mathfrak{S}_3 \times 4$
$x^{24} - 64x^{22} + 1736x^{20} - 26136x^{18} + 240152x^{16} - 1393584x^{14} + 5101236x^{12} - 11397664x^{10} + 14412192x^8 - 8822384x^6 + 1829968x^4 - 125600x^2 + 2500$
Ordre: 24, Indice: 8, Nom: 2×6.2
$x^{24} - 36x^{22} + 20x^{21} + 642x^{20} - 720x^{19} - 6792x^{18} + 12060x^{17} + 43803x^{16} - 118240x^{15} - 140712x^{14} + 705960x^{13} - 120532x^{12} - 2367360x^{11} + 30278-$

$88x^{10} + 2400280x^9 - 9582057x^8 + 9070560x^7 + 2157868x^6 - 20076540x^5 + 40120722x^4 - 53553840x^3 + 53140344x^2 - 36475380x^1 + 15562381$
Ordre: 24, Indice: 9, Nom: 12.2
$x^{24} + 11x^{23} - 314x^{22} - 4942x^{21} + 18284x^{20} + 683470x^{19} + 2461319 \times x^{18} - 28936790x^{17} - 262331975x^{16} - 276203240x^{15} + 5021512205x^{14} + 21510167645x^{13} - 3917351678x^{12} - 221767368751x^{11} - 446623951567x^{10} + 394461454530x^9 + 2431575723468x^8 + 2146941393467x^7 - 2555036459478x^6 - 5605355205205x^5 - 2425530991885x^4 + 1237257113143x^3 + 1183192406717x^2 + 192698935305x^1 - 18574137871$
Ordre: 24, Indice: 10, Nom: $\mathfrak{A}_4 \times 2$
$x^{24} + 342x^{22} + 49301x^{20} + 3912326x^{18} + 187678554x^{16} + 5650086198x^{14} + 108154225181x^{12} + 1319599431258x^{10} + 10174131603706x^8 + 4829932175-6202x^6 + 133582201676853x^4 + 191341955314810x^2 + 104669084485681$
Ordre: 24, Indice: 12, Nom: D_{24}
$x^{24} - 348x^{22} + 49254x^{20} - 3716012x^{18} + 164442273x^{16} - 4424980560x^{14} + 72739682272x^{12} - 717145908480x^{10} + 4063089676032x^8 - 1208693156-6592x^6 + 15608839200768x^4 - 6732557844480x^2 + 896702939136$
Ordre: 24, Indice: 14, Nom: $\mathfrak{S}l(2,3)$
$x^{24} - 90x^{22} + 3375x^{20} - 69012x^{18} + 846125x^{16} - 6454530x^{14} + 30881393x^{12} - 91668116x^{10} + 164273115x^8 - 170113210x^6 + 95359797x^4 - 25847876x^2 + 2521744$
Ordre: 24, Indice: 15, Nom: $\mathfrak{S}_4$
$x^{24} + 12x^{23} + 114x^{22} + 748x^{21} + 4057x^{20} + 17932x^{19} + 68274x^{18} + 22378-8x^{17} + 660446x^{16} + 1757564x^{15} + 4534274x^{14} + 11185948x^{13} + 27788031x^{12} + 64634552x^{11} + 140677848x^{10} + 268118788x^9 + 527507906x^8 + 95064-9552x^7 + 2089102884x^6 + 3628184976x^5 + 8367636821x^4 + 11478945892x^3 + 21189734384x^2 + 15943995288x^1 + 5607107728$
Ordre: 26, Indice: 2, Nom: D_{26}
$x^{26} - 10x^{24} - 117x^{22} + 493x^{20} + 7429x^{18} + 35144x^{16} + 84444x^{14} + 12274-3x^{12} + 113404x^{10} + 70253x^8 + 29953x^6 + 9113x^4 + 1882x^2 + 191$
Ordre: 27, Indice: 4, Nom: $3^2 \rtimes 3$
$x^{27} - 853x^{25} + 1677x^{24} + 300981x^{23} - 1096758x^{22} - 56977801x^{21} + 29262-8115x^{20} + 6262298949x^{19} - 41388105096x^{18} - 401368678145x^{17} + 33781-12766301x^{16} + 138961906032229x^{15} - 162481805891262x^{14} - 17857889549-5435x^{13} + 4529497506622959x^{12} - 2989340523410765x^{11} - 6969374926-8510822x^{10} + 124612551331390513x^9 + 527907780509368077x^8 - 14031-75114327466233x^7 - 1522558748101069692x^6 + 5706545152536212569x^5 + 1997685375401190423x^4 - 100522400375817554813x^3 - 2565262903158932886 \times x^2 + 676947847659058930 5x^1 + 30660168638240922 69$
Ordre: 27, Indice: 5, Nom: $9 \rtimes 3$
$x^{27} - 219x^{25} - 219x^{24} + 17739x^{23} + 27594x^{22} - 694303x^{21} - 1276770x^{20}$

$+ 14344062x^{19} + 27787815x^{18} - 162347985x^{17} - 314144550x^{16} + 10185-$
$26441x^{15} + 1943875317x^{14} - 3523055190x^{13} - 6703796736x^{12} + 6512416359 \times$
$x^{11} + 12788576832x^{10} - 5984482987x^{9} - 13395411378x^{8} + 1936137609x^{7}$
$+ 7523977797x^{6} + 619704081x^{5} - 2069181423x^{4} - 546179868x^{3} + 18906-$
$2262x^{2} + 94531131x^{1} + 10503459$
Ordre: 28, Indice: 3, Nom: D_{28}
$x^{28} + 8x^{27} - 62x^{26} - 640x^{25} + 1323x^{24} + 21520x^{23} - 5952x^{22} - 40636-$
$8x^{21} - 290853x^{20} + 4656932x^{19} + 8077060x^{18} - 28496176x^{17} - 10386-$
$2019x^{16} + 14938224x^{15} + 626545050x^{14} + 1036218808x^{13} + 137659210x^{12}$
$- 5411270852x^{11} - 15589187184x^{10} - 18615903316x^{9} + 15034352743x^{8} +$
$113013075944x^{7} + 236543210810x^{6} + 258688165952x^{5} + 108427933059x^{4} +$
$17876061076x^{3} + 30120151370x^{2} - 15584410248x^{1} + 5920993129$
Ordre: 28, Indice: 4, Nom: 14.2
$x^{28} - 15x^{27} - 1441x^{26} + 20567x^{25} + 898244x^{24} - 12054892x^{23} - 31605-$
$8032x^{22} + 3932876584x^{21} + 68591802295x^{20} - 778724284249x^{19} - 94001-$
$42118906x^{18} + 95683111322717x^{17} + 797935007348745x^{16} - 7169725776-$
$035490x^{15} - 39407258690315632x^{14} + 311631021150225524x^{13} + 1019492544-$
$140511247x^{12} - 7357043398815725090x^{11} - 13515683448617609523x^{10} + 92749-$
$062054830408061x^{9} + 866585153315176934328 - 607599126832470928925x^{7} -$
$216546923064728618878x^{6} + 192029815084251824233 4x^{5} - 10148-$
$0772659000099110x^{4} - 23727814364251114283 76x^{3} + 986540399380600550277x^{2} + 386338046253060504659x^{1} - 172268099115883904311$
Ordre: 30, Indice: 2, Nom: $D_{10} \times 3$
$x^{30} + 10x^{29} + 25x^{28} - 70x^{27} - 525x^{26} - 1078x^{25} - 170x^{24} + 2930x^{23} +$
$15345x^{22} + 92510x^{21} + 275272x^{20} + 233570x^{19} - 1271465x^{18} - 5535310x^{17}$
$- 3400440x^{16} + 27262114x^{15} + 53295255x^{14} - 24373750x^{13} - 131372930x^{12}$
$- 39767070x^{11} + 130328267x^{10} + 67845450x^{9} + 43908280x^{8} + 263620990x^{7}$
$+ 344149465x^{6} + 191239554x^{5} + 223335890x^{4} + 216511170x^{3} + 96832320x^{2}$
$+ 20316880x^{1} + 40207721$
Ordre: 30, Indice: 3, Nom: $\mathfrak{S}_3 \times 5$
$x^{30} - 1174x^{29} + 373465x^{28} - 44675488x^{27} + 2796090542x^{26} - 1056744370-$
$22x^{25} + 2593807705842x^{24} - 42958742516328x^{23} + 487374402855723x^{22} -$
$3754410282689253x^{21} + 18652836409635384x^{20} - 49108153278373279x^{19} -$
$15630015362956957x^{18} + 57432996634865885 3x^{17} - 1565253882101447967 \times$
$x^{16} - 183852684373715990x^{15} + 890263670138989645 4x^{14} - 1307962982-$
$5149956059x^{13} - 146291320296600043 60x^{12} + 521272650547559291 41x^{11} -$
$13148449852417381975x^{10} - 807815372347707374 20x^{9} + 671285309165250-$
$22632x^{8} + 457835658466583147 15x^{7} - 678702682166484858 17x^{6} + 15945-$
$25347792164315x^{5} + 196563872843837741 18x^{4} - 290889659169097101 3x^{3} -$
$17581688684404821 84x^{2} + 201643982094491887x^{1} + 9948096306162167$
Ordre: 30, Indice: 4, Nom: D_{30}

$x^{30} - 40x^{28} + 360x^{26} + 786x^{24} + 2680x^{22} + 3670x^{20} + 17287x^{18} + 77210x^{16}$ $+ 212810x^{14} + 472993x^{12} + 825585x^{10} + 1121375x^8 + 1259075x^6 + 92137-$ $5x^4 + 569375x^2 + 29375$
Ordre: 32, Indice: 8, Nom: $D_8 \times 2^2$
$x^{32} + 12x^{30} + 72x^{28} + 528x^{26} + 2945x^{24} + 6912x^{22} + 10296x^{20} + 14148x^{18}$ $+ 16608x^{16} + 14148x^{14} + 10296x^{12} + 6912x^{10} + 2945x^8 + 528x^6 + 72x^4 +$ $12x^2 +$
Ordre: 32, Indice: 9, Nom: $Q_8 \times 2^2$
$x^{32} - 56x^{30} + 1380x^{28} - 19312x^{26} + 172226x^{24} - 1014504x^{22} + 3942088x^{20}$ $- 9290600x^{18} + 9686421x^{16} + 9825760x^{14} - 19617860x^{12} - 21258024x^{10} +$ $105665096x^8 + 286780592x^6 + 319339992x^4 + 186365680x^2 + 46430596$
Ordre: 32, Indice: 10, Nom: $D_8 \curlyvee 4 \times 2$
$x^{32} + 16x^{31} + 64x^{30} - 280x^{29} - 2436x^{28} + 1624x^{27} + 51616x^{26} + 73840x^{25}$ $- 487194x^{24} - 1214168x^{23} + 3158304x^{22} + 11808688x^{21} - 9017556x^{20} -$ $56648888x^{19} + 55417264x^{18} + 383500768x^{17} + 342750185x^{16} - 70648120 \times$ $x^{15} + 1671423424x^{14} + 8305475848x^{13} + 17464276000x^{12} + 22340954112x^{11}$ $+ 23737598480x^{10} + 33943306928x^9 + 66912179880x^8 + 115365216800x^7$ $+ 98829250432x^6 - 9147025888x^5 + 62327512896x^4 + 228133593216x^3 +$ $102638344000x^2 - 25235939136x^1 + 123640037776$
Ordre: 32, Indice: 12, Nom: $2 \times (2 \times 4).2$
$x^{32} + 10x^{31} - 31x^{30} - 500x^{29} + 525x^{28} + 12370x^{27} - 7628x^{26} - 19317-$ $0x^{25} + 121576x^{24} + 2089590x^{23} - 1712111x^{22} - 16298560x^{21} + 18174-$ $362x^{20} + 92990680x^{19} - 139842902x^{18} - 383271540x^{17} + 790088533x^{16} +$ $1062844880x^{15} - 3267183438x^{14} - 1450571900x^{13} + 9881218302x^{12} - 24445-$ $21190x^{11} - 20237261319x^{10} + 18426891040x^9 + 24158414946x^8 - 49813-$ $637570x^7 + 7345386208x^6 + 59920589310x^5 - 57823701425x^4 - 2539339755-$ $0x^3 + 112285667941x^2 - 113647483280x^1 + 54148638581$
Ordre: 32, Indice: 14, Nom: $D_8 \times 4$
$x^{32} + 8x^{31} + 36x^{30} + 120x^{29} + 442x^{28} + 1568x^{27} + 4508x^{26} + 9752x^{25} +$ $28159x^{24} + 92544x^{23} + 156404x^{22} - 519216x^{21} - 4665528x^{20} - 14419496 \times$ $x^{19} - 29345896x^{18} - 54554216x^{17} - 18637695x^{16} + 197034456x^{15} + 11943-$ $6944x^{14} - 1609516776x^{13} + 9660333564x^{12} + 37847628736x^{11} + 2396449602-$ $0x^{10} - 51668363536x^9 + 176305354979x^8 + 490907559208x^7 - 2845439894-$ $36x^6 + 739553546928x^5 + 952265897934x^4 - 1363864630168x^3 - 29568-$ $43416404x^2 + 1832349655720x^1 + 38614571220961$
Ordre: 32, Indice: 15, Nom: $Q_8 \times 4$
$x^{32} + 8x^{31} - 12x^{30} - 240x^{29} - 162x^{28} + 3280x^{27} + 5336x^{26} - 24576x^{25} -$ $55605x^{24} + 117400x^{23} + 345228x^{22} - 348976x^{21} - 1415178x^{20} + 574200x^{19}$ $+ 4108780x^{18} + 121008x^{17} - 8313952x^{16} - 2690352x^{15} + 12612100x^{14} +$ $8508480x^{13} - 11080866x^{12} - 10767520x^{11} + 11638956x^{10} + 23537560x^9 +$ $13299510x^8 + 530280x^7 + 5923532x^6 + 16536328x^5 + 13391232x^4 + 12637-$

$44x^3 + 7544100x^2 + 1000496x^1 + 3268201$
Ordre: 32, Indice: 17, Nom: $D_8 \curlyvee 8$
$x^{32} - 204x^{30} + 15300x^{28} - 597312x^{26} + 13860729x^{24} - 204001632x^{22} + 1975438692x^{20} - 12877852716x^{18} + 57219835968x^{16} - 173668281012x^{14} + 357140532132x^{12} - 488355187104x^{10} + 430652400057x^8 - 233805346560x^6 + 72333529092x^4 - 10959625620x^2 + 547981281$
Ordre: 32, Indice: 21, Nom: $8 + Q_8$
$x^{32} - 384x^{31} + 70496x^{30} - 8229248x^{29} + 685587920x^{28} - 43395770496x^{27} + 2170659946688x^{26} - 88166507113088x^{25} + 2966962444402280x^{24} - 84017846151918336x^{23} + 2026966787010729280x^{22} - 42076514544324902656x^{21} + 757525433777614337760x^{20} - 11903020972795842877184x^{19} + 164046406451522272480128x^{18} - 1990579200699928150412032x^{17} + 213275552506580691414468808x^{16} - 20219295986784876922662348 8x^{15} + 1698665667942765453544142976x^{14} - 126596677002275284071633863 68x^{13} + 837559733535956611992304096 64x^{12} - 492112685481916273201438836224x^{11} + 256786792226981963508242958 2592x^{10} - 11891244137895781956313259113984x^9 + 4876510255408588730670012707 6768x^8 - 17629664935001729599326503567872 0x^7 + 55721083118107870816930628813388 8x^6 - 15186848498134574492783955431106 56x^5 + 34933837710689497471453734992881 92x^4 - 65576427714872121558032593983211 52x^3 + 95090603821167877124073748838691 84x^2 - 9631601385091006671623137215226880x^1 + 532684721787522071385330391516571 2$
Ordre: 32, Indice: 23, Nom: $D_{16} \times 2$
$x^{32} + 16x^{31} + 140x^{30} + 860x^{29} + 4056x^{28} + 15372x^{27} + 48188x^{26} + 127556x^{25} + 291008x^{24} + 587636x^{23} + 1084760x^{22} + 1881452x^{21} + 3096898x^{20} + 4800796x^{19} + 6929020x^{18} + 9292052x^{17} + 11743788x^{16} + 14399476x^{15} + 17700452x^{14} + 22115436x^{13} + 27692448x^{12} + 33693484x^{11} + 38735912x^{10} + 41146084x^9 + 39884993x^8 + 34911748x^7 + 27454784x^6 + 19107424x^5 + 11724016x^4 + 6147168x^3 + 2716224x^2 + 880128x^1 + 242496$
Ordre: 32, Indice: 24, Nom: $QD_{16} \times 2$
$x^{32} + 80x^{30} + 2904x^{28} + 67120x^{26} + 1156796x^{24} + 15257040x^{22} + 158520616x^{20} + 1414095920x^{18} + 11713769958x^{16} + 82046146160x^{14} + 416920989928x^{12} + 1299139126800x^{10} + 3509297019644x^8 + 2659952210800x^6 + 3748631514648x^4 - 2226040547440x^2 + 2154698116321$
Ordre: 32, Indice: 26, Nom: $D_{16} \curlyvee 4$
$x^{32} + 48x^{31} + 1000x^{30} + 12416x^{29} + 114080x^{28} + 930384x^{27} + 6848296x^{26} + 42836128x^{25} + 244619012x^{24} + 1382129456x^{23} + 7162106632x^{22} + 35879192768x^{21} + 194489433488x^{20} + 991300363984x^{19} + 4829886546120x^{18} + 23220735386976x^{17} + 91230949065166x^{16} + 339320100632592x^{15} + 1257488339027640x^{14} + 3213379502138624x^{13} + 9645688523839424x^{12} + 25625059867967600x^{11} + 69873571195659128x^{10} + 330152912653104480x^9 + 1085524879540625108x^8 + 4456438147781685392x^7 + 154905248799602-

$71960x^6 + 269973807522136099 20x^5 + 796509218443878252 96x^4 + 18559-2174973428342384x^3 + 4695648193574840386 4x^2 + 5302009654057396041 28-8x^1 + 2195815816486535786201$
Ordre: 32, Indice: 35, Nom: $Q_8 + Q_8$
$x^{32} - 192x^{30} + 16848x^{28} - 849600x^{26} + 25640820x^{24} - 447087168x^{22} + 3882270384x^{20} - 3812391360x^{18} - 91359208746x^{16} - 1775497734720x^{14} + 30280491884016x^{12} - 90440865389376x^{10} + 936251640197460x^8 - 14042-81065187520x^6 + 7242495778908432x^4 - 4877143440312384x^2 + 6835182246-375921$
Ordre: 32, Indice: 42, Nom: $D_8 \curlyvee D_8$
$x^{32} - 16x^{30} + 300x^{28} + 256x^{27} - 4520x^{26} - 7376x^{25} + 38048x^{24} + 87872 \times x^{23} - 201088x^{22} - 474672x^{21} + 653628x^{20} + 693024x^{19} - 337208x^{18} + 3995328x^{17} - 5778074x^{16} - 24079104x^{15} + 26418896x^{14} + 53426816x^{13} - 56657932x^{12} - 55577856x^{11} + 70785032x^{10} + 22900048x^9 - 47297040x^8 - 32271040x^7 + 105656768x^6 - 71328016x^5 + 14966436x^4 - 9891360x^3 + 11059480x^2 + 1107200x^1 + 360025$
Ordre: 32, Indice: 43, Nom: $D_8 \curlyvee Q_8$
$x^{32} - 180x^{30} + 12204x^{28} - 430920x^{26} + 9041319x^{24} - 120894120x^{22} + 1073392236x^{20} - 6484139100x^{18} + 26998923969x^{16} - 77809669200x^{14} + 154568481984x^{12} - 208905039360x^{10} + 187480790784x^8 - 107226685440x^6 + 36440948736x^4 - 6449725440x^2 + 429981696$
Ordre: 32, Indice: 49, Nom: D_{32}
$x^{32} - 8x^{31} + 34x^{30} - 91x^{29} + 161x^{28} - 157x^{27} + 126x^{25} + 481x^{24} - 2526x^{23} + 5420x^{22} - 6563x^{21} + 3729x^{20} + 872x^{19} - 214x^{18} - 11285x^{17} + 31222x^{16} - 51808x^{15} + 66851x^{14} - 73179x^{13} + 69871x^{12} - 59956x^{11} + 47265x^{10} - 34428x^9 + 25033x^8 - 19040x^7 + 13622x^6 - 9009x^5 + 5021x^4 - 1946x^3 + 641x^2 - 140x^1 + 25$
Ordre: 34, Indice: 2, Nom: D_{34}
$x^{34} - 45x^{33} + 2570x^{32} - 81246x^{31} + 2720455x^{30} - 67022203x^{29} + 16628-82505x^{28} - 33654992099x^{27} + 673358658706x^{26} - 11542981096918x^{25} + 194136244917212x^{24} - 2872416510118911x^{23} + 41570232426849823x^{22} - 53714-3556136833083x^{21} + 678281956263509943 9x^{20} - 770665632064734669 78x^{19} + 856035172768352848242x^{18} - 857884920061250374451 0x^{17} + 8416067271-1612743325484x^{16} - 743682336556983262608175x^{15} + 644814917595226928 60-31745x^{14} - 500463472295688824124397 73x^{13} + 382608752742575836362928 0-39x^{12} - 258694146277589933481407 8664x^{11} + 173387353257647847955348 6-6207x^{10} - 100672008960274375778266247153x^9 + 585747181189428213 10-4327321898x^8 - 285005510057440425640962925016 1x^7 + 141732681306189-57884379483963567x^6 - 553192985739716491714433295773 45x^5 + 2294738758-14380208361622318903968x^4 - 657079714188709698768877360712134x^3 + 21853-8685149600150219436667441 3605x^2 - 359301495093023233087350212133 0952 \times$

$x^1 + 893260957937212492775625371593625 9$
Ordre: 36, Indice: 5, Nom: $6 \times \mathfrak{S}_3$
$x^{36} - 84x^{34} + 3152x^{32} - 69842x^{30} + 1018040x^{28} - 10297384x^{26} + 74348-101x^{24} - 388584808x^{22} + 1477217628x^{20} - 4076051390x^{18} + 8098386352x^{16} - 11423185988x^{14} + 11196020694x^{12} - 7389755784x^{10} + 3139412060x^8 - 803447252x^6 + 111564448x^4 - 6598664x^2 + 38809$
Ordre: 36, Indice: 6, Nom: 3×6.2
$x^{36} - 166x^{34} - 80x^{33} + 11117x^{32} + 7680x^{31} - 406784x^{30} - 320040x^{29} + 9164152x^{28} + 7606640x^{27} - 134877072x^{26} - 113897960x^{25} + 1338603388 \times x^{24} + 1121374880x^{23} - 9106952832x^{22} - 7385200600x^{21} + 42777911722x^{20} + 32657017520x^{19} - 138870299852x^{18} - 96457489080x^{17} + 310393409110x^{16} + 187920406400x^{15} - 473616279104x^{14} - 237004066520x^{13} + 486098439936x^{12} + 189500833680x^{11} - 327710333600x^{10} - 94758927320x^9 + 140230246700 \times x^8 + 29670687200x^7 - 36446214400x^6 - 5775871400x^5 + 5355362525x^4 + 649778000x^3 - 381822750x^2 - 31939000x^1 + 8615125$
Ordre: 36, Indice: 7, Nom: $\mathfrak{A}_4 \times 3$
$x^{36} - 261x^{34} + 84x^{33} + 29874x^{32} - 16380x^{31} - 1981104x^{30} + 1351308 \times x^{29} + 84888818x^{28} - 61909120x^{27} - 2485698600x^{26} + 1738803906x^{25} + 51342844156x^{24} - 31120621728x^{23} - 761139535454x^{22} + 354483883250x^{21} + 8152705393366x^{20} - 2421703706660x^{19} - 62936429800642x^{18} + 7509851571-684x^{17} + 346224533099824x^{16} + 17119361405020x^{15} - 1329884444980562 \times x^{14} - 257685527123136x^{13} + 3459590120621496x^{12} + 1040447283988238 \times x^{11} - 5841740274601156x^{10} - 2098668284216224x^9 + 6045997736957797 \times x^8 + 2176393095972830x^7 - 3540663683962081x^6 - 1063365055447184x^5 + 1010009558684544x^4 + 184072043547728x^3 - 98042591982960x^2 - 16420-52087424x^1 + 1686327332544$
Ordre: 36, Indice: 13, Nom: $\mathfrak{S}_3^2$
$x^{36} - 12x^{34} + 69x^{32} - 12x^{31} - 240x^{30} + 24x^{29} + 216x^{28} + 52x^{27} + 1116x^{26} + 576x^{25} - 6132x^{24} - 5148x^{23} + 36432x^{22} + 59304x^{21} - 56214x^{20} - 13489-2x^{19} + 254292x^{18} + 413712x^{17} - 147114x^{16} - 567492x^{15} + 870624x^{14} + 311400x^{13} - 513120x^{12} - 779364x^{11} + 2359044x^{10} - 1116320x^9 - 18756x^8 - 446484x^7 + 2421312x^6 - 2488872x^5 + 1405149x^4 - 509412x^3 + 116952x^2 - 14256x^1 + 733$
Ordre: 36, Indice: 14, Nom: $3^2 \rtimes 4$
$x^{36} + 12x^{34} - 144x^{32} - 5040x^{30} - 61290x^{28} - 220968x^{26} + 9627444 \times x^{24} + 148891392x^{22} + 622214865x^{20} - 323381700x^{18} - 4405276044x^{16} + 20225527632x^{14} + 108505417536x^{12} - 737226774720x^{10} + 1790972907840x^8 - 2437435411200x^6 + 1387815379200x^4 + 141647616000x^2 + 1492992000$
Ordre: 38, Indice: 2, Nom: D_{38}
$x^{38} - 23x^{37} + 1775x^{36} - 35103x^{35} + 1447927x^{34} - 24964853x^{33} + 72363-2749x^{32} - 10990404216x^{31} + 248953082928x^{30} - 3355690412130x^{29} + 62744-$

$717941887x^{28} - 754495345570954x^{27} + 1202780666197985 2x^{26} - 1294332886-70493085x^{25} + 1795871411715327803x^{24} - 1731650917997589 4452x^{23} + 21202-1875888812598866x^{22} - 1830691508136843243263x^{21} + 199679013116460-70573595x^{20} - 153974145801731595405302x^{19} + 150593465044734044120892 4 \times x^{18} - 10317703099270209172641465x^{17} + 90900595221631494091342232x^{16} - 54884393130156062108386826 6x^{15} + 43700802668196380201008844 61x^{14} - 22966408829002007403689732452x^{13} + 16571923194486454537547339265 3 \times x^{12} - 74411612343677226348327885 8813x^{11} + 48808418271465151639653 45-331674x^{10} - 18204558705372131332594077886854x^{9} + 10908149512802330793-6928657963813x^{8} - 32324129936122377639628738872005 0x^{7} + 1786295787-01507390857861488787962 3x^{6} - 39022589740248627831718521737380 97x^{5} + 20274710253553398893747359526785395x^{4} - 28377821488851003333320229175 3-42600x^{3} + 14402373312496164008974231299616051 5x^{2} - 926331627264998-178495887125865350 37x^{1} + 49359979466704900144305882938261771 9$
Ordre: 39, Indice: 2, Nom: $13 \rtimes 3$
$x^{39} - 234x^{37} - 195x^{36} + 23634x^{35} + 33579x^{34} - 1369524x^{33} - 2524860 \times x^{32} + 50993046x^{31} + 109726461x^{30} - 1293879717x^{29} - 3076777665x^{28} + 23136775155x^{27} + 58870139211x^{26} - 297121258395x^{25} - 792695081529x^{24} + 2763239423139x^{23} + 7634693279889x^{22} - 18593030584557x^{21} - 52918-961392323x^{20} + 89502097403979x^{19} + 263399315088663x^{18} - 3004248426-71733x^{17} - 931927500966267x^{16} + 668317588182621x^{15} + 229935179545496-1x^{14} - 880844567796531x^{13} - 3836344361395923x^{12} + 458895734526762 \times x^{11} + 4128225889909329x^{10} + 326890401637527x^{9} - 2676910504332870x^{8} - 568509025209957x^{7} + 963250661818224x^{6} + 270527296711113x^{5} - 17549-1163565523x^{4} - 50022000931617x^{3} + 13884361386246x^{2} + 2740650268824x^{1} - 366701990616$
Ordre: 40, Indice: 7, Nom: $4 \times D_{10}$
$x^{40} - 70x^{39} + 2295x^{38} - 43632x^{37} + 505289x^{36} - 3242128x^{35} + 2809775x^{34} + 110119028x^{33} - 298021552x^{32} - 11200166352x^{31} + 133133865319x^{30} - 318061192054x^{29} - 3273268988655x^{28} + 48278857653924x^{27} + 1161009456-97993x^{26} - 1006777227180882x^{25} + 19638865801874539x^{24} + 1328818176-23293062x^{23} + 37964999374756489 0x^{22} + 91388513681596231 08x^{21} + 10441-5497011586337310x^{20} + 68604326182063768311 0x^{19} + 66481000923677525347-30x^{18} + 63379700412026750540334x^{17} + 48243080792633302950671 4x^{16} + 35445195925796678075085 88x^{15} + 26810337076034850657235156x^{14} + 18217-8951582132124615784232x^{13} + 11345033151278268488560316 42x^{12} + 68443-5628450961401667799740 2x^{11} + 39116729252928703187220429494x^{10} + 20342-9463322809323618239721560x^{9} + 98601828702523702569862642880 9x^{8} + 45035-1748338910765929240478503 0x^{7} + 18772919185184402467145676123729x^{6} + 695685040989564186234385218441 88x^{5} + 23228385360350221335012975671 9-497x^{4} + 68501909183480118043474037131207 8x^{3} + 16172297612729923598-$

$48832877060317x^2 + 256698111147128095074159895914713 4x^1 + 2049331429-5469397586644560858135 17$
Ordre: 40, Indice: 10, Nom: $2 \times 5 \rtimes 4$
$x^{40} + 70392x^{30} + 5660441624x^{20} - 6771345011232x^{10} + 13114052591692816$
Ordre: 42, Indice: 5, Nom: $7 \rtimes 6$
$x^{42} + 48020x^{28} + 96001584x^{14} + 52706752$
Ordre: 44, Indice: 3, Nom: D_{44}
$x^{44} + 70x^{42} + 2219x^{40} + 42148x^{38} + 535433x^{36} + 4817380x^{34} + 31779137 \times x^{32} + 157273576x^{30} + 592968375x^{28} + 1719676540x^{26} + 3852957030x^{24} + 6657149774x^{22} + 8770357215x^{20} + 8566157170x^{18} + 5861391360x^{16} + 2561971276x^{14} + 716543958x^{12} + 286653210x^{10} + 126368117x^8 - 11915402x^6 - 3223809x^4 + 1005650x^2 + 196249$
Ordre: 44, Indice: 4, Nom: 22.2
$x^{44} + 31x^{43} - 4942x^{42} - 153745x^{41} + 11139909x^{40} + 347278266x^{39} - 15142223037x^{38} - 472313661979x^{37} + 13819283433859x^{36} + 4307399626-93220x^{35} - 8916659912169237x^{34} - 277571403352942245x^{33} + 4167935095-968015363x^{32} + 12972052131221389700 8x^{31} - 14205447133458269505 34x^{30} - 4440603588802253359742 9x^{29} + 3498013552759774906369 95x^{28} + 11112-6102846822152128105 20x^{27} - 6053994239355566565999993 73x^{26} - 2008146570-8170282194250259 79x^{25} + 6958440514636381271427748587x^{24} + 2564556848-6049027357703425738 4x^{23} - 4702609181291486580501104600 15x^{22} - 22510-5090874871212829458040495 71x^{21} + 1237451398186022545557421842523 9 \times x^{20} + 1326029366809974032934026513682288x^{19} + 4332785727239178855 4-8633956396370x^{18} - 5235113305883369047657332460490235 2x^{17} - 43939-6178518608878382328824601253 43x^{16} + 1400291628141836132783828974517398218x^{15} + 1488009010788476673888939830519718065x^{14} - 2565247609-3332567679557772306089822222x^{13} - 2713312313221567792900256276874890 1-186x^{12} + 3230159828462025107873101356165320458 32x^{11} + 282459625295220-1524542418108422162437 79x^{10} - 2768394892007623090819442860857221920247 \times x^9 - 1566847601834659133589173341084678573324x^8 + 156272945949780-3522905464512276126770133 3x^7 + 3061132236000679755161906275029138906216x^6 - 5396356771050329757541499532278468044902 1x^5 + 9087101306-2936593627381390778092105999 66x^4 + 9711176702674415123164202310743623 1-853966x^3 - 4472211937572828120892545373166671520474 7x^2 - 5868512671-3345521298739585197127978255927x^1 + 3233239440520788861674109681 74-34006495389$
Ordre: 46, Indice: 2, Nom: D_{46}
$x^{46} - 19x^{45} + 3887x^{44} - 68513x^{43} + 7191254x^{42} - 117787982x^{41} + 84289-74203x^{40} - 128439871829x^{39} + 7027901220906x^{38} - 99688116391498x^{37} + 4436178213872087x^{36} - 5858182104810631 3x^{35} + 2202615138754313045x^{34} - 2706766986059976747 7x^{33} + 8822249246281617142 13x^{32} - 1007956651-

$2344388366084x^{31} + 290027192757134328917553x^{30} - 30760637558996001439-33597x^{29} + 791957166054217011387168 53x^{28} - 778072051294058932766321257x^{27} + 181076648638953499743133070 21x^{26} - 164320451887149938771890243265x^{25} + 348407394577427497216332784 0725x^{24} - 29093773350790155112-091504543973x^{23} + 565478583003613169996475854488185x^{22} - 4324380355-341582733013056840975199x^{21} + 774198248641465558270008290127488 39 \times x^{20} - 538872171244362105760759123139815271x^{19} + 8919951312834181150 1-85785456225900614x^{18} - 560657676259217309776579705898775710 58x^{17} + 860572957038468305216973645472990751632x^{16} - 4834872665834974248162359-547983538089284x^{15} + 689669551612147288523832434210327921112 60x^{14} - 341696462252545415016728280394935723152420x^{13} + 453675932178660473 23-270630573760956076950 64x^{12} - 194628320875792442323238698878051690461 0-7671x^{11} + 240770389235988976671218097098304523749347293x^{10} - 87166-321195585253309468740553171115952289236 8x^9 + 100521371186552044689386 4-702352912483026249311 7x^8 - 295581637761736279595767824030535262618 9-4448329x^7 + 317767529299559569803430212023230896544328497993x^6 - 71344-822580797264747650436254257131764382596913 6x^5 + 714691423152908102 27-677972715421882525366400310 98x^4 - 109227391651499132696413029922624465-33375738974472 7x^3 + 101859424556882030390814764606463170478679267853057x^2 - 797304286625355977003858556745991402767165840639 30x^1 + 691151302964637382241728593125662537533539084607025$

Ordre: 48, Indice: 7, Nom: $6 \times Q_8$

$x^{48} - 160x^{46} - 24x^{45} + 11544x^{44} + 3264x^{43} - 498904x^{42} - 198696x^{41} + 14467118x^{40} + 7190784x^{39} - 298788000x^{38} - 173220504x^{37} + 4553297080x^{36} + 2946375552x^{35} - 52347047320x^{34} - 36631569768x^{33} + 460410909735x^{32} + 340018195968x^{31} - 3124487887936x^{30} - 2386803504240x^{29} + 1643354601-7008x^{28} + 12761974608000x^{27} - 67072283924208x^{26} - 52131179131152x^{25} + 212088398947300x^{24} + 162626383580160x^{23} - 517266296866624x^{22} - 38615-4229416624x^{21} + 965561530863984x^{20} + 693594824782848x^{19} - 1363249012-428720x^{18} - 933398419093584x^{17} + 1430798417624959x^{16} + 9280248061-67040x^{15} - 1088822077679904x^{14} - 667855174527480x^{13} + 579483422187896 \times x^{12} + 337406759212224x^{11} - 204434796927160x^{10} - 114229651690056x^9 + 43959751863054x^8 + 24132719917824x^7 - 4981100927520x^6 - 2853634038-072x^5 + 209711556952x^4 + 158419623552x^3 + 2867507400x^2 - 2714914248 \times x^1 - 182629511$

Ordre: 48, Indice: 13, Nom: $3 \times QD_{16}$

$x^{48} + 36x^{44} - 4x^{42} + 1440x^{41} + 900x^{40} + 5904x^{38} + 51840x^{37} + 12538x^{36} + 10080x^{35} + 818496x^{34} - 66816x^{33} + 123012x^{32} + 4129920x^{31} + 418160x^{30} - 1459008x^{29} + 13702968x^{28} + 25098624x^{27} - 31808952x^{26} + 56211840x^{25} + 39858499x^{24} - 196877952x^{23} - 181349136x^{22} - 21090816x^{21} + 25988-1948x^{20} - 254095488x^{19} + 1316536400x^{18} + 312016896x^{17} - 1337789448x^{16}$

$- 9242371584x^{15} + 3032412336x^{14} + 3339152640x^{13} + 13072363210x^{12} - 5611047264x^{11} + 8087752512x^{10} - 8082867456x^9 + 409125960x^8 - 10880980992x^7 + 4408843388x^6 + 137434176x^5 + 3426668280x^4 - 9336960x^3 + 423243864x^2 - 83645568x^1 + 3922993$
Ordre: 48, Indice: 22, Nom: $2^2 \times \mathfrak{A}_4$
$x^{48} - 4x^{47} - 554x^{46} + 2296x^{45} + 132549x^{44} - 590138x^{43} - 18093820x^{42} + 88428364x^{41} + 1563728184x^{40} - 8529384410x^{39} - 89528885736x^{38} + 556055844066x^{37} + 3439510144065x^{36} - 25154879169740x^{35} - 87046186090982x^{34} + 800809593735138x^{33} + 1338976439083701x^{32} - 18066858403631970x^{31} - 8437691400833644x^{30} + 290090050204824600x^{29} - 103975814901091994 \times x^{28} - 33360604639606381 56x^{27} + 309630249873507022 0x^{26} + 27823122847923076762x^{25} - 366771216699757197 75x^{24} - 171350034849179539178x^{23} + 268286668616096488852x^{22} + 795811729088383415300x^{21} - 1332649602535250965586x^{20} - 284464133823091416335 4x^{19} + 463596023304152916316 6x^{18} + 792894693468759348223 4x^{17} - 113009290866299756240 09x^{16} - 1716308778178479848799064x^{15} + 188022111131547147500 26x^{14} + 279943877112754210998 64x^{13} - 200300366074224753663 63x^{12} - 324336208096407497391 22 \times x^{11} + 118333062276499570092 76x^{10} + 244959956760528493292 94x^9 - 2312071104892963791040x^8 - 108430683636396723211 68x^7 - 855685373484155161578x^6 + 255436892723217486188 6x^5 + 453535871009482562091x^4 - 2815282103413 41416238214x^3 - 626846428284611299 94x^2 + 11182270468087790358 \times x^1 + 2537864536396891751$
Ordre: 48, Indice: 23, Nom: $4 \times \mathfrak{A}_4$
$x^{48} + 1456x^{46} + 951808x^{44} + 370521476x^{42} + 96103164144x^{40} + 1761692587865 6x^{38} + 2364108690215922x^{36} + 237522707268881736x^{34} + 1813300082341106652 8x^{32} + 106211747770771989403 2x^{30} + 480184800676559375255 04 \times x^{28} + 168062641737105207830441 6x^{26} + 455500523805627316349867 95x^{24} + 953721975931320655032937912x^{22} + 153442952410899726612412059 36x^{20} + 188032890143550630884818427536x^{18} + 173216793690924694398883948812 8x^{16} + 117735569738407728281649731929 92x^{14} + 575097025374911665901084712752 98x^{12} + 194356414524925576769546068788888x^{10} + 428876310921078138364465689944864x^8 + 559661210477078684068225704483092x^6 + 3492404335021211530932883332581 12x^4 + 470122970364311921947133069711 68x^2 + 479198774730008813801387263 21$
Ordre: 48, Indice: 36, Nom: $2 \times \mathfrak{S}_4$
$x^{48} - 784x^{44} - 4816x^{42} + 380912x^{40} - 5931744x^{38} + 109378416x^{36} + 6515119296x^{34} - 204246260960x^{32} - 8786049238848x^{30} + 106855243485760x^{28} + 1883310325171072x^{26} + 404032896473816 00x^{24} + 889904755283568640x^{22} - 198822807820170920 96x^{20} - 579003853577746152192x^{18} + 105402137861741965081 60x^{16} - 948954079840025951677 44x^{14} - 983237989405035994455248x^{12} + 594749934987122845526937 6x^{10} + 134799876985722385774959 1-$

$04x^8 - 8902072626309649355962193 92x^6 + 76230518450298538969534330 88 \times x^4 - 12277359819215650369727612928x^2 + 73443111787307782707449244 16$
Ordre: 48, Indice: 37, Nom: $4 + \mathfrak{S}_4$
$x^{48} + 1260x^{46} + 722358x^{44} + 250155840x^{42} + 58588818813x^{40} + 9846858805-560x^{38} + 1229904966070386x^{36} + 116686668851704980x^{34} + 8525172976-207077330x^{32} + 4836001052400585673 00x^{30} + 2138886832511999503596 6 \times x^{28} + 7382952832841023185039 60x^{26} + 1985281692504973698269 4093x^{24} + 4140061523341191497160644 40x^{22} + 6646400610927591676193646678x^{20} + 8126580439691945440579689 0060x^{18} + 7454979610521407855247125249 46 \times x^{16} + 5024304085699552068001033111980x^{14} + 2414510612763116807559720-6738170x^{12} + 7923575022875968006107394509 4200x^{10} + 166736790261099-4962113822023985 25x^8 + 2064994015182286085554626374760 00x^6 + 13812-5506990823219650856561916750x^4 + 4309372469156427819809050547250 0x^2 + 4203727109635343570647003400625$
Ordre: 48, Indice: 38, Nom: $D_8 \times \mathfrak{S}_3$
$x^{48} - 4x^{47} - 22x^{46} + 146x^{45} - 71x^{44} - 2152x^{43} + 9742x^{42} + 5486 \times x^{41} - 170459x^{40} + 312640x^{39} + 1565974x^{38} - 5623850x^{37} - 7958668x^{36} + 47746344x^{35} + 6125468x^{34} - 241426140x^{33} + 145281885x^{32} + 534598952 \times x^{31} - 477649574x^{30} + 1979817580x^{29} - 1661505904x^{28} - 7426612692x^{27} + 46475551290x^{26} - 128767911466x^{25} - 599661766912x^{24} + 1465040828136x^{23} + 5984328183530x^{22} - 3575013559182x^{21} - 300037107110 95x^{20} - 66552-1886425 6x^{19} + 97972077055428x^{18} + 101451602355778x^{17} - 1468716112-02253x^{16} - 333605645971826x^{15} - 19293373248838x^{14} + 619095095719664 \times x^{13} + 1038187905704283x^{12} + 833000425718818x^{11} - 430781598742514 \times x^{10} - 2454200994041868x^9 - 3460777286577617x^8 - 1822335278517566 \times x^7 + 1500206396883790x^6 + 4584405894423376x^5 + 6831735275214634 \times x^4 + 7936827424994628x^3 + 7112116454062442x^2 + 4188376431845652x^1 + 1353246508677001$
Ordre: 48, Indice: 39, Nom: $Q_8 \times \mathfrak{S}_3$
$x^{48} + 24x^{47} + 228x^{46} + 952x^{45} + 306x^{44} - 11592x^{43} - 21804x^{42} + 139464 \times x^{41} + 612243x^{40} - 145456x^{39} - 5692344x^{38} - 10693128x^{37} + 2324072 \times x^{36} - 19475496x^{35} - 255001536x^{34} - 440822472x^{33} + 1059032106x^{32} + 5484428424x^{31} + 9988011196x^{30} + 17057703192x^{29} + 54502935870x^{28} + 128981856664x^{27} + 86545383660x^{26} - 315338635224x^{25} - 906309677169 \times x^{24} - 1236659851440x^{23} - 2137624011144x^{22} - 4241003657912x^{21} + 55088-8743192x^{20} + 26372197693992x^{19} + 52072673820496x^{18} - 1591777265976 \times x^{17} - 140625327752514x^{16} - 141883501282440x^{15} + 177087199447908x^{14} + 449372992733928x^{13} + 76820288109338x^{12} - 697562783333016x^{11} - 80915-9768870412x^{10} + 107739131579768x^9 + 1017332583579063x^8 + 8669447971-46208x^7 - 11475030753312x^6 - 545825415511800x^5 - 371875829040324x^4 + 13693577081704x^3 + 1480061770122 48x^2 + 77982869817480x^1 + 14109-$

260441761
Ordre: 48, Indice: 49, Nom: $Gl(2,3)$
$x^{48} - 480x^{46} + 106032x^{44} - 14334880x^{42} + 1330572756x^{40} - 9017212320-0x^{38} + 4632436702240x^{36} - 184932117694400x^{34} + 5836378454395900x^{32} - 147421662776595200x^{30} + 3007387769863690112x^{28} - 498727935787562-96960x^{26} + 67523000912488610774 4x^{24} - 74787172143491226137 60x^{22} + 67735-477390293773377792x^{20} - 5003333099360053549952 00x^{18} + 300133070933832-2333222640x^{16} - 145580364051967187241344 00x^{14} + 569632247860678592 04-960000x^{12} - 179517250398668753661043200x^{10} + 448010738403819871 61-0275136x^{8} - 814363021355913279012500480x^{6} + 811235058764403766088653 3-12x^{4} - 377097486722546705100288 0x^{2} + 462174213222681679073593 6$
Ordre: 50, Indice: 4, Nom: $D_{10} \times 5$
$x^{50} + 144x^{48} + 8276x^{46} + 229733x^{44} + 642334x^{42} - 272678835x^{40} - 14569-354635x^{38} - 311776014000x^{36} - 169474184484x^{34} + 163122591780489x^{32} + 4937945100032527x^{30} + 7143901851086466 1x^{28} + 623847112379751851 \times x^{26} + 191202950966742725x^{24} - 5189853007052793005 8x^{22} - 1164531435-385165806222x^{20} - 1780143591696736539641 5x^{18} - 795725449233432206 83-121x^{16} + 120612158634074580539586 3x^{14} + 155765958973977208427714 99 \times x^{12} + 308714315204627184884157 61x^{10} + 182196664776574290492974 94x^{8} + 399906636539878130988166 7182x^{6} + 167615628555467273859618 70928x^{4} + 214432713778322952244098 08212x^{2} + 760284574554797322157670 6927$
Ordre: 52, Indice: 5, Nom: $13 \rtimes 4$
$x^{52} - 156x^{48} + 2886x^{46} - 34736x^{44} + 354055x^{42} - 2076503x^{40} + 12124-060x^{38} - 34831238x^{36} + 63128260x^{34} + 227125860x^{32} - 1086058389x^{30} + 2339708332x^{28} + 898300572x^{26} - 8763639664x^{24} + 17644614507x^{22} - 34949-52448x^{20} - 14038302720x^{18} + 23472400874x^{16} + 3091442640x^{14} - 56685-30231x^{12} + 1174399759x^{10} + 340104388x^{8} - 189359430x^{6} + 16336892x^{4} + 371293$
Ordre: 54, Indice: 10, Nom: $(3^2 \rtimes 3) \rtimes 2$
$x^{54} - 12x^{52} + 66x^{50} + 270x^{48} - 4005x^{46} + 17898x^{44} - 19761x^{42} - 60264 \times x^{40} + 232779x^{38} + 123604x^{36} - 403788x^{34} - 140190x^{32} + 5706556x^{30} + 10317866x^{28} - 10512759x^{26} + 42986034x^{24} + 177565959x^{22} + 59638914 \times x^{20} + 332615797x^{18} + 1134639672x^{16} + 809469948x^{14} + 1626311948x^{12} + 3727393840x^{10} + 2186103312x^{8} + 3297227872x^{6} + 4196007232x^{4} + 60319-3600x^{2} + 1851804352$
Ordre: 54, Indice: 11, Nom: $3^2 \rtimes 6$
$x^{54} + 354x^{48} + 10635x^{42} + 593188x^{36} + 3563403x^{30} - 5994042x^{24} + 33080-6953x^{18} + 305286660x^{12} - 571514832x^{6} + 203297472$
Ordre: 54, Indice: 12, Nom: $9 \rtimes 6$
$x^{54} + 796392x^{36} + 292918032x^{18} + 1259712$
Ordre: 55, Indice: 2, Nom: $11 \rtimes 5$

$x^{55} - 363x^{53} + 60984x^{51} - 6302043x^{49} + 449130825x^{47} - 23460036237x^{45} + 107811x^{44} + 931895535879x^{43} - 24365286x^{42} - 28832257220283x^{41} + 24969-02760x^{40} + 706029614105112x^{39} - 154164986316x^{38} - 138316716108037-17x^{37} + 6426707505570x^{36} + 218308713906378150x^{35} - 192097300410972 \times x^{34} - 27873932140687835 07x^{33} + 4266860946322491x^{32} + 288420638652516-41037x^{31} - 72016498419623208x^{30} - 241795224894635099028x^{29} + 93644-0719987972914x^{28} + 16388660336439065950 44x^{27} - 9454554551838307824 \times x^{26} - 894510115198493607039 6x^{25} + 7435107028445510393 1x^{24} + 39081-014188164299179818x^{23} - 455068880659378838853x^{22} - 135530365359390-044967396x^{21} + 215799262064890879914 0x^{20} + 368820458213843142659196 \times x^{19} - 786173094040923963366 3x^{18} - 775343684524538563293816x^{17} + 21712-303942303285939221x^{16} + 123204808685604908030175 0x^{15} - 4456797262-2940864449429x^{14} - 143454067460996133940292 7x^{13} + 660293078522330-27718603x^{12} + 116821679937847950446350 2x^{11} - 675243190463597682 36-435x^{10} - 617145561838782816659226x^{9} + 443413151775248326677 72x^{8} + 184147870979966572621602x^{7} - 163863678796123892326 29x^{6} - 2222182070-6252796410364x^{5} + 24920750511353723724 72x^{4} - 1015019163870712110x^{3} - 822165522735276809 1x^{2} + 304505749161213633x^{1} - 3075815648093067$

Ordre: 56, Indice: 13, Nom: $2^3 \rtimes 7$

$x^{56} + 196x^{54} + 18648x^{52} + 1133440x^{50} + 48436640x^{48} + 1544233712 \times x^{46} + 38173818592x^{44} + 750338412032x^{42} + 12017839696576x^{40} + 16127-3296879744x^{38} + 1891145474666560x^{36} + 20779466926807680x^{34} + 22242-7012090037888x^{32} + 22625996049637514 24x^{30} + 21200197494382998784x^{28} + 17002071927024411136 0x^{26} + 11992891799209337210 88x^{24} + 8995954481-401999641600x^{22} + 60404313076782803079168x^{20} + 24265528460156612592-2304x^{18} + 65259533276272516370022 4x^{16} + 14259516179171896607457 28 \times x^{14} - 32022932478117832486416384x^{12} - 33207833866461908520790425 6x^{10} - 53309478159774591852514099 2x^{8} + 53599754412880504575005163 52x^{6} + 29207701669922718984324333568x^{4} + 58014308102576444942478475264x^{2} + 41882067330411980012414058496$

Ordre: 58, Indice: 2, Nom: D_{58}

$x^{58} + 25733x^{56} + 319664325x^{54} + 2552668884634x^{52} + 14721312894625062 \times x^{50} + 65303276614038825563x^{48} + 23173517068687021288 1152x^{46} + 67545-4590406864881730448649x^{44} + 16477053758638254083970136477 62x^{42} + 34102-1881141898004760441589171561 5x^{40} + 60493993512140885279618979232563632-07x^{38} + 92671509668510625604499525220556456565 24x^{36} + 123277148772270-7016718035141258842050294550 8x^{34} + 14295661045098716039258455335469570-887065551143x^{32} + 14487128331819044058510604145313302773285923950957 \times x^{30} + 12845100255393340285069148610978309925795650928025781x^{28} + 99648-0704748938155014022936179162837911086586068907029 0x^{26} + 6755444493-5422254424408405514006058483296493891686715816 23x^{24} + 399226798224162-$

$4400511467297329936996631935093316883177141144x^{22} + 204871420431241-$
$6006968652617936223170084010713457852206128522825x^{20} + 907901657766673-$
$858060775674562796033353063137296162313944491833810x^{18} + 3448367424-$
$925037621697818317766042273876360405632679117048790384547 27x^{16} + 11112-$
$089868583837633447271230260935547691408642820314374434163066310 7816 \times$
$x^{14} + 299670234646320539315675000027901627166820517929564771721348-$
$04070949814065x^{12} + 663778893201236267876836967296084033108342669920 77-$
$611847076180798784360452 95x^{10} + 117612879453002704392205521070502 92-$
$960384364346376375215204789621505964655913 25x^8 + 160289148193211353 06-$
$788242457259712885774399157479638711581782102113072842631092 1x^6 + 15775-$
$565405569271087040680323404564015666011621095745786214165342738814869 8-$
$81736093x^4 + 998023095782119497317809335757203567654031474441246822 7-$
$090256992870611808261264345 50x^2 + 304779934766280251385875260830176 62-$
$441569546992936101524543424728702322228375071479375$

Ordre: 64, Indice: 12, Nom: $2^3 \times D_8$

$x^{64} + 32x^{63} + 584x^{62} + 7688x^{61} + 80556x^{60} + 707216x^{59} + 5371500 \times$
$x^{58} + 36065096x^{57} + 217392842x^{56} + 1190064216x^{55} + 5968785752x^{54} +$
$27615857208x^{53} + 118496019634x^{52} + 473505957368x^{51} + 1767714180988x^{50}$
$+ 6180261291680x^{49} + 20270194060278x^{48} + 62438502903752x^{47} + 18073-$
$2475033616x^{46} + 491605430388176x^{45} + 1255879698436130x^{44} + 3009467879-$
$403096x^{43} + 6750347976954592x^{42} + 14126061046883880x^{41} + 2743782398-$
$4904746x^{40} + 49065797973119376x^{39} + 79681467354187960x^{38} + 1145437083-$
$28462248x^{37} + 13765294648971578 4x^{36} + 11503344367035091 2x^{35} - 88416-$
$03053370116x^{34} - 304064811258898824x^{33} - 828243078366567702x^{32} - 15723-$
$78647356037256x^{31} - 2382946438625471792x^{30} - 2881641625339266024 \times$
$x^{29} - 2424545786501394238x^{28} - 152313421891551368x^{27} + 4832031779-$
$791918028x^{26} + 131674774403278275 52x^{25} + 248976696396151052 10x^{24} +$
$392229452456653876 24x^{23} + 544785874302060161 68x^{22} + 684114023717132-$
$79760x^{21} + 787080374039951961 94x^{20} + 836094088925920162 80x^{19} + 82390-$
$449398700006392x^{18} + 755283881757218994 96x^{17} + 645082127541677065 37 \times$
$x^{16} + 513579460845872776 48x^{15} + 380991320006413698 24x^{14} + 2630180974-$
$1150438368x^{13} + 168603883496733905 40x^{12} + 100036031328603119 20x^{11} +$
$546896616645186480 8x^{10} + 273831767765497028 8x^9 + 124557046434894755 2 \times$
$x^8 + 509131000136960352x^7 + 184278532533761808x^6 + 5788273127752 71-$
$36x^5 + 153390593331532 80x^4 + 3291403861267200x^3 + 536230694598480x^2$
$+ 59067036483840x^1 + 3321880412004$

Ordre: 64, Indice: 18, Nom: $2 \times 4 \times D_8$

$x^{64} + 16x^{63} + 160x^{62} + 1168x^{61} + 6928x^{60} + 34768x^{59} + 153192x^{58} + 60324-$
$8x^{57} + 2161372x^{56} + 7111184x^{55} + 21688392x^{54} + 61644048x^{53} + 16427-$
$2492x^{52} + 411621568x^{51} + 974861136x^{50} + 2183804080x^{49} + 4653089209x^{48}$
$+ 9416416008x^{47} + 18218934968x^{46} + 33580608840x^{45} + 59428890698x^{44} +$

$100439239072x^{43} + 163536305508x^{42} + 254868331112x^{41} + 383262437398 \times x^{40} + 553212986304x^{39} + 768366811616x^{38} + 1030545766424x^{37} + 13157-66312684x^{36} + 1647680004672x^{35} + 1924733477180x^{34} + 2274989274160 \times x^{33} + 2469364630110x^{32} + 2794777079464x^{31} + 3037711526624x^{30} + 32655-25348336x^{29} + 4003884045086x^{28} + 3908763708400x^{27} + 5458545298464 \times x^{26} + 4792472140232x^{25} + 6595090966888x^{24} + 5418741910784x^{23} + 65227-75482832x^{22} + 4782115818896x^{21} + 5521544093588x^{20} + 2686698561520 \times x^{19} + 4046491099992x^{18} + 694575484704x^{17} + 2125947121394x^{16} - 12325-7258360x^{15} + 764698496056x^{14} - 394407702584x^{13} + 409677328582x^{12} - 379464146384x^{11} + 205802358916x^{10} - 141693889096x^{9} + 55670336144 \times x^{8} - 32976962104x^{7} + 20526344696x^{6} - 11922830416x^{5} + 5857393566x^{4} - 1413185712x^{3} + 144204488x^{2} - 5991832x^{1} + 217921$

Ordre: 64, Indice: 27, Nom: $4 \times D_8 \curlyvee 4$

$x^{64} - 32x^{63} + 688x^{62} - 10896x^{61} + 142304x^{60} - 1581232x^{59} + 15455632 \times x^{58} - 134998496x^{57} + 1069753068x^{56} - 7761976464x^{55} + 52006877360x^{54} - 323696319280x^{53} + 1881528172720x^{52} - 10255298321248x^{51} + 5260328993-8208x^{50} - 254660869852432x^{49} + 1166549958363466x^{48} - 506703547272728-0x^{47} + 20908349919642720x^{46} - 82087962814438016x^{45} + 307062191061252-496x^{44} - 1095627200904322256x^{43} + 37327082225119862224x^{42} - 1215280703-5919160816x^{41} + 37838355705977242048x^{40} - 112732241802222628032x^{39} + 321540113471172811696x^{38} - 878331629884173248400x^{37} + 2298491377-767844159648x^{36} - 576332130584558321339 2x^{35} + 13848284716825081963-312x^{34} - 31887700325347001921408x^{33} + 703607206980294837026 59x^{32} - 14875031261110527274884 8x^{31} + 30123973571291521031203 2x^{30} - 58420-4344042741256534272x^{29} + 10845560627622780966046 88x^{28} - 1926526112-176285822104080x^{27} + 32726407581142082412164 96x^{26} - 531312548656808-8047256752x^{25} + 82379632249472692301710 08x^{24} - 12188719401344121647-551296x^{23} + 17193905339875307078509424x^{22} - 23101307841430970832302 41-6x^{21} + 29530240151353594978163936x^{20} - 35870789068369642840835856 \times x^{19} + 41350567983475518062716400x^{18} - 45170272410764218010937600 \times x^{17} + 46681942743698102742972666x^{16} - 45559369651143574431852112 \times x^{15} + 41901897513750141578479088x^{14} - 36229157783862511922726448 \times x^{13} + 29361633989624889823529840x^{12} - 22224282060516721733361760 \times x^{11} + 15638931786329976235684320x^{10} - 10170033841402547917529744x^{9} + 60637959018149170472630 68x^{8} - 32796791705676645964792 16x^{7} + 15858-5047155734380160915 2x^{6} - 67148254557920404772163 2x^{5} + 241697642409068-108082864x^{4} - 70508000684552906172656x^{3} + 15442420910859377611408x^{2} - 213157484764283946667 2x^{1} + 131613281113033864561$

Ordre: 64, Indice: 34, Nom: $8 \times D_8$

$x^{64} - 32x^{63} + 528x^{62} - 5936x^{61} + 50864x^{60} - 352896x^{59} + 2058720x^{58} - 10362368x^{57} + 45852572x^{56} - 180918576x^{55} + 643657600x^{54} - 20833-$

$53776x^{53} + 6180004360x^{52} - 16904152528x^{51} + 42861793216x^{50} - 10122$-
$5392192x^{49} + 223689691950x^{48} - 464748623984x^{47} + 912698995712x^{46} -$
$1704814143680x^{45} + 3050766211584x^{44} - 5272243124272x^{43} + 8868949645$-
$040x^{42} - 14615890869472x^{41} + 23677583790484x^{40} - 37691485880288x^{39} +$
$58739391884320x^{38} - 89119663330000x^{37} + 130880383133104x^{36} - 18516$-
$9897263744x^{35} + 251559715755200x^{34} - 327530606318336x^{33} + 4082603257$-
$10219x^{32} - 486762244916464x^{31} + 554390987282240x^{30} - 601787481389536 \times$
$x^{29} + 620380804626592x^{28} - 604419521133680x^{27} + 553103397268208x^{26} -$
$471935000121312x^{25} + 372326313495188x^{24} - 269072784432576x^{23} + 17637$-
$3251441024x^{22} - 103984095176048x^{21} + 55172641273712x^{20} - 2722954978$-
$8640x^{19} + 13970699637856x^{18} - 8768065065984x^{17} + 6702948837306x^{16} -$
$5233841633968x^{15} + 3669573481520x^{14} - 2194364600432x^{13} + 1095608494$-
$912x^{12} - 448073566096x^{11} + 144987812368x^{10} - 34243109664x^{9} + 44123$-
$66728x^{8} + 578097904x^{7} - 523859040x^{6} + 125024608x^{5} + 17435624x^{4} -$
$20022736x^{3} + 6260896x^{2} - 943296x^{1} + 83521$

Ordre: 64, Indice: 35, Nom: $8 \times Q_8$

$x^{64} + 8x^{63} - 124x^{62} - 1128x^{61} + 6710x^{60} + 73056x^{59} - 202700x^{58} -$
$2891736x^{57} + 3439855x^{56} + 78507664x^{55} - 18437796x^{54} - 1554914656x^{53}$
$- 637666788x^{52} + 23324925200x^{51} + 20620425348x^{50} - 271511057120x^{49} -$
$341606563092x^{48} + 2492091428936x^{47} + 3923706991752x^{46} - 1822291027$-
$5424x^{45} - 33926286237580x^{44} + 106778943626384x^{43} + 228912125546768 \times$
$x^{42} - 502336133760512x^{41} - 1228406544663653x^{40} + 1893136218387928x^{39}$
$+ 5299394139116168x^{38} - 5672688197239960x^{37} - 18488668955819594x^{36} +$
$13299687848572576x^{35} + 52308253530528944x^{34} - 23583438777365840x^{33} -$
$120050527383299267x^{32} + 29032019253914600x^{31} + 223132481072479916x^{30}$
$- 171864720479401 76x^{29} - 334694185092478276x^{28} - 18089336574247056 \times$
$x^{27} + 403003502456820012x^{26} + 64014276036369384x^{25} - 386700817840289$-
$257x^{24} - 93907303773373440x^{23} + 292876629749281248x^{22} + 9084144968$-
$1601480x^{21} - 172929692119282470x^{20} - 62941474779645504x^{19} + 78352$-
$695295871036x^{18} + 31858722359392752x^{17} - 26697452503198414x^{16} - 11737$-
$580688568696x^{15} + 6668703634057324x^{14} + 3091870090728304x^{13} - 11833$-
$16942116630x^{12} - 564815639062072x^{11} + 143720789186184x^{10} + 6842492645$-
$1752x^{9} - 11451805057181x^{8} - 5151250319440x^{7} + 564639212408x^{6} + 21574$-
$8274032x^{5} - 15312432156x^{4} - 3888333496x^{3} + 166201688x^{2} + 5644816x^{1}$
$- 44711$

Ordre: 64, Indice: 55, Nom: $4 \times D_{16}$

$x^{64} + 16x^{63} + 144x^{62} + 940x^{61} + 4834x^{60} + 20468x^{59} + 73260x^{58} + 225676 \times$
$x^{57} + 611017x^{56} + 1502404x^{55} + 3536040x^{54} + 8473648x^{53} + 21141386x^{52} +$
$52669928x^{51} + 123279134x^{50} + 262298220x^{49} + 514012886x^{48} + 985664632 \times$
$x^{47} + 1981332292x^{46} + 4195211020x^{45} + 8909063806x^{44} + 18445618372x^{43}$
$+ 37543878588x^{42} + 75841052708x^{41} + 150461864249x^{40} + 288302537580x^{39}$

$+ 530676514970x^{38} + 942929020204x^{37} + 1624139408415x^{36} + 2706790763-812x^{35} + 4349600525538x^{34} + 6739649163612x^{33} + 10097316538738x^{32} + 14648994576580x^{31} + 20562408849478x^{30} + 27877299671148x^{29} + 36482-841118103x^{28} + 46127641778428x^{27} + 56372570666986x^{26} + 6648852914-7908x^{25} + 75511396951389x^{24} + 82456068551948x^{23} + 86607638842898x^{22} + 87556393862920x^{21} + 85085035568217x^{20} + 79218380266168x^{19} + 70611-746068562x^{18} + 60493550266912x^{17} + 50454520032473x^{16} + 4145897848-3824x^{15} + 33905363388198x^{14} + 27791713752268x^{13} + 23281227200709x^{12} + 20207936340876x^{11} + 18244042639788x^{10} + 16129044987088x^{9} + 13566-582867108x^{8} + 10079544152564x^{7} + 6705538252730x^{6} + 3735847437400x^{5} + 1823351835069x^{4} + 703848326440x^{3} + 232494383274x^{2} + 51437239088x^{1} + 9271511461$

Ordre: 64, Indice: 56, Nom: $4 \times QD_{16}$

$x^{64} + 48x^{60} + 4856x^{56} - 7536x^{52} - 610388x^{48} - 42084240x^{44} + 664367336 \times x^{40} - 15763446192x^{36} + 148240804630x^{32} + 447080751504x^{28} + 7400659531-016x^{24} + 16840951410864x^{20} + 57953635354828x^{16} + 59282186463696x^{12} + 21714585944984x^{8} - 9384154512x^{4} + 1874161$

Ordre: 64, Indice: 134, Nom: $2 \times D_{32}$

$x^{64} + 16x^{63} + 164x^{62} + 1222x^{61} + 7386x^{60} + 37570x^{59} + 166533x^{58} + 65553-4x^{57} + 2331792x^{56} + 7582514x^{55} + 22760187x^{54} + 63460928x^{53} + 16503-7765x^{52} + 400983106x^{51} + 909925516x^{50} + 1924234600x^{49} + 3775150632 \times x^{48} + 6817637386x^{47} + 11175301322x^{46} + 16178260278x^{45} + 1941725645-4x^{44} + 15602055906x^{43} - 3934333658x^{42} - 49153465242x^{41} - 1236268099-28x^{40} - 208682513496x^{39} - 241293313895x^{38} - 98278513478x^{37} + 38626-9100693x^{36} + 1336535782442x^{35} + 2669690713258x^{34} + 3899480299678 \times x^{33} + 4053289970415x^{32} + 1914697306508x^{31} - 3259415044002x^{30} - 10662-166114648x^{29} - 17031175089157x^{28} - 16750809540760x^{27} - 3603031111-404x^{26} + 26086842999158x^{25} + 70403557963869x^{24} + 121021347654338 \times x^{23} + 165870325257401x^{22} + 194274391795204x^{21} + 201522289206445x^{20} + 189947582155480x^{19} + 166119013630025x^{18} + 136665777986960x^{17} + 10592-6704939583x^{16} + 76337704875934x^{15} + 49888309891594x^{14} + 2864739395-5648x^{13} + 13960976307695x^{12} + 5565438069664x^{11} + 1780433275936x^{10} + 526724827456x^{9} + 247448314719x^{8} + 181086111342x^{7} + 116384095773x^{6} + 54149162002x^{5} + 17625402136x^{4} + 3650173450x^{3} + 554318050x^{2} + 52937-500x^{1} + 3705625$

Ordre: 64, Indice: 154, Nom: $D_8 \times D_8$

$x^{64} + 24x^{63} + 76x^{62} - 2598x^{61} - 22097x^{60} + 91410x^{59} + 1630426x^{58} + 621056x^{57} - 64236296x^{56} - 169026344x^{55} + 1563751786x^{54} + 7177388564x^{53} - 23866366387x^{52} - 178209998016x^{51} + 189428178843x^{50} + 3048460633-480x^{49} + 648334522983x^{48} - 38149276668004x^{47} - 42574081149533x^{46} + 358436254081482x^{45} + 679177159155602x^{44} - 2543501912250630x^{43} - 69271-$

$58532392329x^{42} + 13415152600260130x^{41} + 51670245166184071x^{40} - 49389809136400386x^{39} - 295496750707025191x^{38} + 96853743329413768x^{37} + 132313669901049475 2x^{36} + 158738681276637928x^{35} - 4681105719920512384x^{34} - 2189331457243900790x^{33} + 1310866351937271419 5x^{32} + 998192897016226055 8x^{31} - 2893088403506059623 5x^{30} - 2994700601086371424 2x^{29} + 497601084317518620 14x^{28} + 658657915930640648 70x^{27} - 652622462765846529 93 \times x^{26} - 109753821642925778518x^{25} + 625053765819616672 26x^{24} + 139758146077164162318x^{23} - 393096614239994092 22x^{22} - 135517739719220890000 \times x^{21} + 989469773918027769 9x^{20} + 988534150048651511 40x^{19} + 821594552076439978 5x^{18} - 531643631371161299 04x^{17} - 108027629748825428 75x^{16} + 204878688944433548 88x^{15} + 608922493364358513 6x^{14} - 545153542000943832 0x^{13} - 202619615992037569 6x^{12} + 959325391410488928x^{11} + 413237624761001312x^{10} - 107021069064226624x^{9} - 50884031757078560x^{8} + 7211739225984896x^{7} + 3591811800278272x^{6} - 272718852969728x^{5} - 128741265154048x^{4} + 5106553261568x^{3} + 1692373543168x^{2} - 41471536128x^{1} + 22640358 4$

Ordre: 64, Indice: 155, Nom: $D_8 \times Q_8$

$x^{64} + 24x^{63} + 68x^{62} - 2784x^{61} - 22618x^{60} + 111408x^{59} + 1789976x^{58} - 92272x^{57} - 75798549x^{56} - 171161704x^{55} + 2005375756x^{54} + 8255334784x^{53} - 34179299906x^{52} - 223258838664x^{51} + 338203741532x^{50} + 412044185630 4x^{49} - 417732436456x^{48} - 55475165335792x^{47} - 47773333238300x^{46} + 560570307277040x^{45} + 928154018892142x^{44} - 4285393958908208x^{43} - 1053807379352813 2x^{42} + 244792572609054 48x^{41} + 854569558393327 98x^{40} - 9920726624495596 0x^{39} - 526055623072326500x^{38} + 232507154068595544x^{37} + 2522371663564141216x^{36} + 154136619632396384x^{35} - 952890753363767980 4x^{34} - 427731560436190777 6x^{33} + 284535826195340186 97x^{32} + 221183028236536339 68x^{31} - 669335247907868727 04x^{30} - 727946471218794867 52x^{29} + 1227018349349922771 62760x^{28} + 174664315599893156336x^{27} - 1713147386657289491 04x^{26} - 318299825932431827408x^{25} + 173315677887379386480x^{24} + 4463357150504097246 1184x^{23} - 110407216633408875840x^{22} - 4815763019930605311 68x^{21} + 151714991748986516 00x^{20} + 396216095409126473120x^{19} + 5294456517307400 7936x^{18} - 244236257310300485984x^{17} - 651436697687246422 96 \times x^{16} + 109652893915820323776x^{15} + 418632061164952808 32x^{14} - 343051151003829011 20x^{13} - 169311564364441357 44x^{12} + 695440604915235884 8x^{11} + 43658275461799658 24x^{10} - 796190005711238336x^{9} - 687436953872152928 \times x^{8} + 34959013411012992x^{7} + 6109936691306348 8x^{6} + 925332409590016x^{5} - 2819401610520384x^{4} - 106296909749120x^{3} + 57816734351040x^{2} + 1709270243456x^{1} - 37862390897 6$

Ordre: 64, Indice: 156, Nom: $Q_8 \times Q_8$

$x^{64} - 2112x^{62} + 2053440x^{60} - 1224359424x^{58} + 503023587984x^{56} - 151660179093888x^{54} + 34888236394132800x^{52} - 6285103683477700608x^{50} + 9029 7$

$0003728726435232x^{48} - 104815886854899556965888x^{46} + 992361695042866-2814321920x^{44} - 771495933739250920489205760x^{42} + 49481137203983080212-897156096x^{40} - 26257963050072336802181647564 80x^{38} + 115457390614189-193628264685000704x^{36} - 42068087223263954850672908261 13024x^{34} + 12685-697621801663299650709496578944 0x^{32} - 31578406666989207197972996960 8-9325568x^{30} + 64633229828974472236946743285379321856x^{28} - 1081735254-764806033437869800562222039040x^{26} + 14697528686342807880523754676 8-18653986816x^{24} - 16062742834878668343893496793346577924 0960x^{22} + 13958-392254127516786070738784174142434508 80x^{20} - 95086089154865799225523 85-815457226276470784x^{18} + 49909193254070730188105519740733822812004352 \times x^{16} - 19776129835445904455588363883864381094271385 6x^{14} + 5777063370-753017325604819491002337257472000 00x^{12} - 12109160298213203151103 75-907422700197310889984x^{10} + 17635655730527066439431011711771701 99480-745984x^{8} - 17101562223687011066974320922211572308042055 68x^{6} + 10341-268585055371865558235000537236256443596 80x^{4} - 34574545188681380552-651918756555883544156569 6x^{2} + 476048502237021372333876764411524794-33916416$

Ordre: 78, Indice: 5, Nom: $13 \rtimes 6$

$x^{78} - 60x^{76} + 1758x^{74} - 31374x^{72} + 361545x^{70} - 2526138x^{68} + 63960-93x^{66} + 65272320x^{64} - 820344366x^{62} + 4238917560x^{60} - 11097539136x^{58} + 25998312276x^{56} - 253950442092x^{54} + 1904107366404x^{52} - 6150241590-390x^{50} - 7394115465828x^{48} + 206357506486443x^{46} - 1013203672387992x^{44} + 860274381349188x^{42} + 10628619004481202x^{40} - 32781277560497877x^{38} + 104884418145574710x^{36} - 40514064170529386 7x^{34} + 295493622562386612 \times x^{32} + 40615891703825990 31x^{30} - 12355286209448784336x^{28} + 9210801631-390598736x^{26} + 19692883183608903114x^{24} - 62999157702489094359x^{22} + 92601020895674068134x^{20} - 92503314656275396167x^{18} + 698232909262776-11352x^{16} - 41386230713232095544x^{14} + 19054958649198180912x^{12} - 64822-44193198946928x^{10} + 156562634218723488 0x^{8} - 291847113728275392x^{6} + 56287868834276352x^{4} - 10379802940157952x^{2} + 963961798754304$

Ordre: 81, Indice: 12, Nom: $3 \wr 3$

$x^{81} + 36x^{80} + 387x^{79} - 1395x^{78} - 59283x^{77} - 291276x^{76} + 2736255x^{75} + 31837212x^{74} - 4674630x^{73} - 1451329720x^{72} - 4806739671x^{71} + 3488812259-1x^{70} + 244083499593x^{69} - 313863589602x^{68} - 6648982491813x^{67} - 77187-46538009x^{66} + 115163866563177x^{65} + 355511172942642x^{64} - 1242398389-848403x^{63} - 7322238454404402x^{62} + 5466586508148315x^{61} + 9892539496-6261876x^{60} + 73884626508149289x^{59} - 941492533327045173x^{58} - 18715-27993547736388x^{57} + 620751543597480387 0x^{56} + 22246504024776587529x^{55} - 23852173983773956681x^{54} - 18010381598818691042 4x^{53} - 1550415843-8333507415x^{52} + 10705843704042585032 62x^{51} + 10060612319679809526 00 \times x^{50} - 47104834176845295755 55x^{49} - 84977835221601497461 70x^{48} + 14593-$

$078050764486298336x^{47} + 45365739603298474047051x^{46} - 249183674138811-45688752x^{45} - 17667320436646268400749x^{44} - 27645465561293206641468 \times x^{43} + 52039937434350120457294 7x^{42} + 37166856662725156398035 4x^{41} - 11548-89444202283964434103x^{40} - 14904370359343956299900 05x^{39} + 1839850738-875298038043029x^{38} + 39313204123760204906707 53x^{37} - 173493256136356-0351362280x^{36} - 76300170655744649333215 50x^{35} - 305569021795732549860192x^{34} + 11218171588883216202330279x^{33} + 45591961164056691261821 94 \times x^{32} - 12462150006648343418074572x^{31} - 93982531097345048284444 63x^{30} + 10125789560285802749575491x^{29} + 12071967934249074303335733x^{28} - 54306252633554529853205 51x^{27} - 11085629450413154889136857x^{26} + 11048-804153240612565845 91x^{25} + 75314692384358435906765 25x^{24} + 1054019273-195404621201719x^{23} - 37913040726946255812406 23x^{22} - 126564741343914-3866762462x^{21} + 13859320129404409332134 25x^{20} + 72798818381435014836-9558x^{19} - 34965729587399070645440 7x^{18} - 27196438178358812912829 9x^{17} + 53012168367031374792732x^{16} + 69684474323697479564667x^{15} - 19621-23587720577048306x^{14} - 12243084638713078235817x^{13} - 100874600221531-1183267x^{12} + 14330934704574284188 44x^{11} + 23466386695360319260 5x^{10} - 10525129116299626070 3x^{9} - 24555900023074777299x^{8} + 431352083285308-6080x^{7} + 1355841849619223837x^{6} - 752138318716899 87x^{5} - 3732315282-8193351x^{4} + 135629240062652x^{3} + 469211439690099x^{2} + 5055565068333x^{1} - 2170677442653$

Ordre: 84, Indice: 10, Nom: $2 \times 7 \rtimes 6$

$x^{84} - 476x^{82} + 108458x^{80} - 15755936x^{78} + 1639938419x^{76} - 1302978966-52x^{74} + 8221944472546x^{72} - 423270470510292x^{70} + 18123292541731321x^{68} - 654715873467280688x^{66} + 20174615399789140010x^{64} - 534765487715869-690112x^{62} + 12274114077245050080680x^{60} - 24519969610160997295570 8 \times x^{58} + 42803628909227543448111 94x^{56} - 65490659508606815411039972x^{54} + 88016362013876483369792134 0x^{52} - 10405491613396347014523135292 \times x^{50} + 10829766851308500237977539 5580x^{48} - 99244645672659490722767 33-67248x^{46} + 80046932751496678324447808 4091x^{44} - 56767550254812534403-555008449176x^{42} + 35342181242962658341041734668314 0x^{40} - 1927500693-44981985146412036179744 8x^{38} + 91837918361302031392833876449636 27x^{36} - 38101447202318865671500173622101396x^{34} + 13711053330942048980549 38-03433874506x^{32} - 42608566676747435765951451339683257 6x^{30} + 1137923144-33159780230987928595004272 3x^{28} - 25983067593890087448747385942434901-80x^{26} + 50467071256767617873993224464291591 58x^{24} - 829989735200548-99356022730342936635 88x^{22} + 11521055660498574996926017374682484650 \times x^{20} - 13492374607516429430793233645216221628x^{18} + 133902755324571-17989395242457171306596x^{16} - 11388605313347799994658937526974903992 \times x^{14} + 84402582423467763169998220357326591 37x^{12} - 55154945232452434619-50576215675598056x^{10} + 31362304934051437626191616156775961 12x^{8} - 14686-$

$549648791184386444344921647233 28x^6 + 523536669309960321470771242978-232832x^4 - 12836333939458161828280665481407283 2x^2 + 221899190815287-85292359462761140224$
Ordre: 96, Indice: 96, Nom: $96.24b$
$x^{96} + 27431992x^{72} + 3547332576024x^{48} + 797307852959968x^{24} + 16$
Ordre: 98, Indice: 4, Nom: $7 \times D_{14}$
$x^{98} + 392x^{94} + 8232x^{92} - 148862x^{90} + 5877648x^{88} - 86485392x^{86} + 12325-06114x^{84} - 8465294537x^{82} + 31774156232x^{80} + 452638133472x^{78} - 52711-85763046x^{76} + 24758438826828x^{74} - 337575600945128x^{72} + 1018348210-6441567x^{70} - 128106582223158812x^{68} + 356998484972190159x^{66} + 66998-78559450336736x^{64} - 6365396942915901506 0x^{62} + 498596007656705812 28 \times x^{60} + 128395380694772559456 2x^{58} - 178204215915539568426 0x^{56} - 26191-007981879794627238x^{54} + 181633657271413772320042x^{52} - 669435902470821-167829959x^{50} - 32975379528285644163635 6x^{48} + 728645376827365161737-72020x^{46} + 257194443229894006751121 62x^{44} - 250173144824237953810754 9-13x^{42} + 114367916571000251611961894 0x^{40} + 141274484781725677240141 1-43x^{38} - 11790817845294932717414689352x^{36} - 530364365935938293817969 6-6406x^{34} + 84151009271682546146454016236x^{32} - 438665925592094889324559847952x^{30} + 145994554130933199259563194840 2x^{28} + 114065025156759-576202606533398 63x^{26} + 197017720520793328024069572660 24x^{24} + 55960-250299746762275997352275824x^{22} + 212185051444422807096468821677202 \times x^{20} + 454971380755755492498717783634832x^{18} + 566079694350715546889645376801784x^{16} + 430169943818497417954460741073745x^{14} + 1973136061-710167941749220280517 12x^{12} + 511669604089357765165942044983 36x^{10} + 669832013667114008216762587161 6x^8 + 412487814858507698314467318016 \times x^6 + 5453813748285345256195083878 4x^4 + 112560481165462551274696867 84 \times x^2 + 52945182767281896291210035 2$

Bibliographie

[AdLe] Leonard Adleman et Hendrik W. Lenstra, *Finding irreducible polynomials over finite fields*, Proc. 18th Annual ACM Symp. on Theory of Computing, 1986 (5) 350–355.

[AcKl] Vincenzo Acciaro et Jürgen Klüners, *Computing Automorphisms of Abelian Number Fields*, Math. Comp., **68**, 1999, 1179–1186.

[ASZ] John Abbott, Victor Shoup et Paul Zimmermann *Factoring in* $\mathbb{Z}[X]$*: The Searching Phase*, ISSAC 2000, 2000, 1–7.

[Benchmark] *List of polynomials of the benchmark*, `http://www.math.u-bordeaux.fr/~allomber/nfgaloisconj_benchmark.html`

[BrKu] Richard P. Brent et H.T. Kung, *Fast algorithms for manipulating formal power series*, J. Assoc. Comput. Mach., **25**, 1978, 581–595

[CoEn] George E. Collins et Mark J. Encarnacíon, *Efficient rational number reconstruction*, J.Symbolic Comp., **20**, 1995, 287–297.

[Cohen] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics., **138**, Springer, 1993, corr. 3^{rd} printing 1996

[Eichenlaub] Yves Eichenlaub, *Problèmes effectifs de théorie de Galois en degré 8 à 11*, Thesis, Université Bordeaux I, 1996.

[FoLe] David Ford et Pascal Letard,*Implementing the Round Four maximal order algorithm*, J.T.N.B. **6**, 1994, 39–80

[GAP] The GAP Group, *GAP — Groups, Algorithms, and Programming*, Version 4.1, Aachen, St Andrews, 1999
`http://www-gap.dcs.st-and.ac.uk/~gap`

[GP2C] Bill Allombert, *GP2C, the GP to C compiler*, `ftp://megrez.math.u-bordeaux.fr/pub/pari/GP2C`

[Hall] Marshall Hall, *The theory of groups*, Macmillan, New York, 1959.

[KaSh] Erich Kaltofen et Victor Shoup, *Subquadratic-time factorization of polynomials over finite fields*, Math. Comp. **67**, 1998, 1179–1197.

[Klüners1] Jürgen KLÜNERS *Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper*, Thesis, Technischen Universität Berlin, 1997.

[Klüners2] Jürgen KLÜNERS *On computing subfields — A detailed description of the algorithm*, J. Théorie des Nombres Bordeaux, **10**, 1998, 243–271.

[KlMa] Jürgen KLÜNERS et Gunter MALLE *Explicit Galois realization of transitive groups of degree up to 15*, J. Symb. Comput. **30**, 2000, 675–716.

[KANT V4] M. DABERKOW, C. FIEKER, J. KLÜNERS, M. POHST, K. ROEGNER, M. SCHÖRNIG et K. WILDANGER, *KANT V4*, J. Symb. Comput. **24**, 1997, 267–283.

[Landau] S. Landau,*Factoring polynomials over algebraic number fields*, SIAM J. Comput. **14**, 1985, 184–195.

[Lenstra] Hendrik W. LENSTRA, *Finding isomorphism between finite fields.*, Math. Comp. **56**, 1991, 329–347.

[Magma] W. BOSMA, J. CANNON and C. PLAYOUST, *The Magma algebra system I: The user language*, J. Symb. Comput., **24**, 1997, 235–265.

[PARI] PARI, C. BATUT, K. BELABAS, D. BERNARDI, H. COHEN et M. OLIVIER, *User's Guide to PARI-GP*, version 2.2.2.

[Perec] Georges PEREC, *Cantatrix Soprano L.* J. Math. Vivisec. **27**, 1974, 134–143.

[Roblot] Xavier ROBLOT, *Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction de corps de classes de rayon*, Thesis, Université Bordeaux I, 1997.

[Shoup1] Victor SHOUP, *Fast construction of irreducible polynomials over finite fields*, J.Symbolic Comp. **17**, 1994, 371–391.

[Shoup2] Victor SHOUP, *New algorithms for finding irreducible polynomials over finite fields*, Math. Comp. **54**, 1990, 435–447.

[Shoup3] Victor SHOUP, *NTL: A Library for doing Number Theory (version 4.0a)* , http://www.shoup.net/ntl/.

Table des matières

Théorie de Galois effective pour les corps de nombres et les corps finis.
Développement du système PARI.

Je rappelle différentes façons de représenter les nombres algébriques et les morphismes entre les corps de nombres. Ensuite, je donne des algorithmes pour résoudre plusieurs problèmes liés à la théorie de Galois, dont le calcul du corps fixé par un sous-groupe du groupe de Galois. Troisièmement, je donne un algorithme efficace pour la détermination des isomorphismes explicites entre les corps finis utilisant les théories de Kummer et d'Artin-Schreier. Quatrièmement je détaille un algorithme pour le calcul des automorphismes d'une extension galoisienne de groupe de Galois « faiblement » hyper-résoluble. En dernière partie, je décris l'architecture du compilateur GP2C qui permet la mise en œuvre efficace d'algorithmes pour la théorie des nombres.

Mots clés : théorie de Galois, corps finis, automorphismes explicites, groupes hyper-résolubles.

Effective Galois Theory for number fields and finite fields.
Development of the PARI system.

I recall several ways to represent algebraic numbers and homomorphisms between number fields. Next, I give algorithms to solve several problems linked to Galois theory, including the computation of a fixed field by a subgroup of the Galois group. Third, I give an efficient algorithm for the determination of explicit isomorphisms between finite fields using Kummer theory and Artin-Schreier theory. Fourth, I detail an algorithm for the computation of the automorphisms of a Galois extension with "weakly" supersolvable Galois group. Last, I describe the architecture of the GP2C compiler, which enables the efficient implementation of algorithms related to number theory.

Keywords : Galois theory, finite fields, explicit automorphisms, supersolvable groups.

MATHEMATIQUES PURES
Laboratoire A2X, UFR Math-Info de Bordeaux, 351 Cours de la Libération, 33405 Talence Cedex, France.