Autour d'une conjecture de B. Gross relative à l'existence de corps de nombres de groupe de Galois non résoluble et ramifiés en un unique premier p petit

Sylla Lesseni

A la mémoire de mes parents,

De mon oncle,

Et de mon frère Jakis.

Remerciements

Arrivé au terme de ces trois années d'aventure, je me dois de remercier tous ceux et celles qui m'ont aidé et soutenu.

En tout premier lieu, je tiens à remercier mon directeur de thèse, Michel Olivier, qui avec beaucoup d'enthousiasme, de patience et de disponibilité a guidé mes premiers pas dans la recherche. Je le remercie particulièrement d'avoir su diriger mes recherches tout en me laissant une grande liberté de manoeuvre.

Je suis très sensible à l'honneur que m'ont fait Michael Pohst et Jean Cougnard, qui se sont intéressés à mon travail en acceptant d'être les rapporteurs et en y apportant d'utiles remarques et suggestions.

Je suis également très reconnaissant à Christine Bachoc, Stéphane Louboutin, Arnaud Jehanne et Abbas Movahhedi d'avoir accepté d'être membres de mon jury. Qu'ils en soient remerciés.

Je remercie l'ensemble du personnel administratif et technique de l'Institut de Mathématiques de Bordeaux pour les facilités qu'il offre aux doctorants, notamment Véronique Saint-Martin, Christine Parison et les ingénieurs responsables du réseau informatique.

Finalement, j'exprime toute mon amitié et ma sympathie à tous mes camarades de travail de la salle 374 et aussi à mes amis, ma famille et à l'association AEESIG.

Table des matières

Introduction

La conjecture de J.P Serre (cf. **[27]** p. 226 à 234) en 1973 permet de donner un lien entre les valeurs propres des opérateurs de Hecke modulo l et les représentations de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ à valeurs dans $Gl_2(F)$ où F est une extension finie du corps $\mathbb{F}_l$. Les travaux de J. Tate **[29]** dans la même année donnent une démonstration de cette conjecture dans le cas $l = 2$. Ses résultats prédisent l'inexistence d'un certain type de groupes de Galois pour l'ensemble des corps de nombres de degré n ramifiés seulement en 2. En abondant dans ce sens, J.P. Serre démontre la conjecture dans le cas $l = 3$ (cf. **[27]** p. 710), et montre ainsi qu'on peut étendre les résultats de J. Tate aux corps de nombres ramifiés seulement en 3. Ces travaux ont suscité depuis lors de nombreuses recherches de la part des théoriciens des nombres pour montrer de façon explicite ou pour généraliser ces résultats. Les recherches menées par B. Gross **[15]** en 1998 à ce sujet prédisent l'existence de corps de nombres de degré n de groupe de Galois non résoluble et ramifiés seulement en 5. Mais malheureusement les groupes de Galois (de type de Lie) possibles dans l'exemple qu'il propose sont tellement énormes qu'il est impossible de les vérifier.

Le but de notre travail a été de vérifier la conjecture de B. Gross relative à l'existence de corps de nombres de degré $n \geq 5$ ramifiés en un unique premier $p < 11$ et ayant un groupe de Galois non résoluble. Cette vérification va porter sur les cas particuliers où le degré n est égal à 8 et 9. Pour le cas $n = 5$ et $n = 6$, J. Jones (cf. **[17]**), et pour le cas $n = 7$, S. Brueggeman (cf. **[1]**) ont déterminé tous les corps de nombres vérifiant ces types de ramification. Leurs travaux ont montré que les groupes de Galois des corps obtenus sont toujours résolubles. Par abus de langage lorsque nous parlerons de groupe de Galois de corps de nombres de degré n, il va s'agir du groupe de Galois d'une clôture galoisienne.

Des travaux décrits dans **[27]** montrent que des corps de nombres de groupe de Galois résoluble peuvent être construits à partir de la théorie du corps de classes. Ceux dont le groupe de Galois est non résoluble peuvent souvent être obtenus par la théorie des courbes elliptiques ou à partir de la théorie des représentations modulaires, mais ces théories sont non appropriées à l'étude de la ramification en des premiers petits.

Comme l'ont fait la plupart des auteurs ayant étudié le problème de la détermination des discriminants minimaux de corps de nombres, nous utilisons largement des inégalités obtenues par des méthodes géométriques dans le but d'éliminer un grand nombre des polynômes qu'il faudra prendre en considération (cf. **[6]**, **[9]**, **[10]**, **[11]**, **[21]**). Des tables explicites de corps de nombres ont été élaborées jusqu'en degré $n \leq 7$ (cf. **[12]** qui contient, en plus une bibliographie complète sur ce sujet). De plus on connait les discriminants minimaux des corps de nombres de degré 8 pour les signatures $(0, 4)$ et $(8, 0)$ (cf. **[9]**, **[11]**), et pour le degré 9 seulement dans le cas totalement réel (cf. **[28]**). Les travaux

de H. Cohen, F. Diaz Y Diaz et M. Olivier (cf. **[6]**) donnent les discriminants minimaux des corps imprimitifs en degré 8 contenant un sous-corps quartique. Ceux dans le cas imprimitif en degré 9 ont été établis par F. Diaz Y Diaz et M. Olivier (cf. **[12]**).

Notre travail est divisé en quatre parties. La plupart des résultats présentés n'utilisent que des méthodes élémentaires. Il va s'agir à travers notre étude d'obtenir des résultats concrets.

La première partie est consacrée aux rappels et autres résultats, la plupart classiques, sur les discriminants et les groupes. Il ne s'agit pas ici de donner un exposé complet sur ces sujets, mais simplement d'énoncer les résultats qui seront utilisés dans la suite. Ainsi les deux premiers paragraphes concernent la formule de la majoration du discriminant sous l'hypothèse de Riemann généralisée (GRH), et des minorations de la valeur absolue du discriminant des corps de nombres en degré 8 et des corps de nombres en degré 9 en fonction de la signature. Ces résultats représentent l'un des outils principaux de l'étude de la ramification. Dans les paragraphes 3 et 4, nous rappelons quelques résultats sur les groupes de décomposition et de ramification, puis sur les groupes résolubles. Ces rappels s'avèrent essentiels par la suite car, en plus de la ramification que nous imposons, les corps recherchés doivent avoir un groupe de Galois non résoluble. Le paragraphe 5 concerne les sous-groupes transitifs du groupe symétrique S_8 et du groupe symétrique S_9 ; nous étudions ici les sous-groupes résolubles et les sous-groupes primitifs en degré 8 et en degré 9. Nous verrons par la suite que les résultats obtenus dans cette étude vont ramener notre recherche aux corps de nombres de degré 8 (resp. de degré 9) qui sont primitifs. Enfin, on termine cette partie par l'outil principal de l'étude de la ramification : la méthode de la majoration de la valuation en un premier p du discriminant du corps. Il n'est pas bien neuf, puiqu'il était déjà utilisé par Dedekind vers la fin du XIXe siècle, et par Ore en 1931 (cf. **[30]**, **[31]**) pour déterminer les valeurs possibles de la valuation en un premier p du discriminant d'un corps de nombres de degré n.

Dans la deuxième partie, on étudie les différents cas de ramification possibles. En utilisant la méthode de Ore décrite précédemment on montre que la ramification en 3, et celle en 5 en supposant GRH ne peuvent être réalisées pour les corps de nombres de degré 8. On obtient un résultat analogue dans le cas de la ramification en 5 des corps de nombres de degré 9. Pour les ramifications possibles c'est-à-dire celle en 2 et celle en 7, on donne les valeurs possibles du discriminant des corps de nombres de degré 8. L'étude menée dans le cas des corps de degré 9 permet aussi de déterminer les valeurs possibles du discriminant dans le cas de la ramification en 2, 3 et 7. De façon inconditionnelle (sans GRH), on donne les valeurs possibles du discriminant dans le cas de la ramification en 5 aussi bien pour les corps de degré 8 que ceux de degré 9.

Nous exploitons l'étape précédente dans la troisième partie pour donner des bornes pour les coefficients de polynômes générateurs des corps ayant ces discriminants. Nous utilisons d'abord le théorème de Hunter (cf. **[4]**) permettant la construction de tables de corps de nombres, ensuite les travaux de Jones et Roberts (cf. **[17]**, **[18]**, **[19]**) sur les corps primitifs. Et enfin, nous procédons à l'amélioration des bornes des coefficients en utilisant les exposants de Newton-Ore (cf. **[19]**) qui est une technique récente qui s'avère très

efficace dans cette étude. Nous employons aussi de façon inconditionnelle les méthodes de minorations de discriminants avec corrections locales d'Odlyzko, Poitou et Serre (cf. **[24]**, **[25]**). Ces minorations proviennent de propriétés analytiques de la fonction zêta attachée à un corps de nombres ; développées, en particulier, par A. Weil, A. Odlyzko, G. Poitou, F. Diaz Y Diaz et J. P. Serre. Ces différentes méthodes conduisent à des simplifications importantes dans les calculs, réduisant ainsi de façon considérable le nombre de polynômes à étudier.

C'est enfin dans la quatrième partie que nous donnons les résultats de nos recherches numériques. À partir des résultats classiques précédents, nous avons développé certaines améliorations dans le but d'accélérer la recherche des corps de nombres. On donne quelques commentaires sur les étapes de l'algorithme de construction des tables. A l'issue des recherches numériques, les seules tables obtenues sont celles de la ramification en 2 en degré 8 et celles de la ramification en 3 en degré 9 ; on n'obtient aucun corps de nombres qui soit ramifié seulement en 7. Les résultats montrent aussi de façon inconditionnelle qu'il n'existe pas de corps de nombres de degré 8 ou de degré 9 ramifié seulement en 5.

Nous donnons en annexe A les différents groupes de Galois et les graphes des inclusions à conjuguaison dans S_n près des sous-groupes transitifs primitifs, pour $8 \leq n \leq 11$. L'annexe B contient les tables des minorations des discriminants des corps de nombres de degré 7 à 10 avec corrections locales avec ou sans l'hypothèse de Riemann généralisée. Nous terminons par l'annexe C où nous donnons quelques exemples de polynômes générateurs des corps obtenus numériquement.

Notre travail n'a pas la prétention d'être autre chose qu'une modeste contribution à la théorie de ramification des corps de nombres ayant un certain groupe de Galois fixé. Il prouve toutefois que des méthodes élémentaires peuvent parfois suffire à résoudre des problèmes a priori complexes. En ce sens, les tables construites peuvent bien avoir leur utilité.

Chapitre 1

Rappels et Notations

1.1 Hypothèse de Riemann généralisée (GRH)

Considérons la fonction zêta de Dedekind attachée à un corps de nombres K de degré n définie pour $s \in \mathbb{C}$ et $Re(s) > 1$ par :

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})^s} \quad ,$$

où la sommation est étendue à tous les idéaux entiers non nuls $\mathfrak{a}$ de K. La famille du deuxième membre est sommable et on a le produit eulérien :

$$\zeta_K(s) = \prod_{\wp} \frac{1}{1 - \frac{1}{\mathcal{N}_{K/\mathbb{Q}}(\wp)^s}}$$

où le produit s'étend à tous les idéaux premiers non nuls $\wp$ du corps de nombres K.
L'hypothèse de Riemann généralisée notée en abrégé GRH affirme que :
tous les zéros non triviaux $s = \sigma + i\beta$ (s'ils existent) de la fonction $\zeta_K(s)$ tels que $0 < \sigma < 1$, sont situés sur la droite critique $\sigma = 1/2$.

Cette conjecture de Riemann, bien qu'elle réponde en grande partie aux préoccupations des mathématiciens pour de nombreux problèmes, n'a pas été démontrée. Dans la suite, chaque fois qu'il en sera fait mention, nous la supposerons vérifiée.

Rappelons le résultat suivant extrait de **[24]** qui permet sous GRH de minorer le discriminant d'un corps de nombres de degré n.

Théorème 1.1.1
Soit K un corps de nombres de degré n et de discriminant d_K. Sous GRH, on a :

$$\frac{1}{n}\log|d_K| \geq \left(\gamma + log 8\pi + \frac{r_1}{n}\frac{\pi}{2} - \frac{2\pi^2(\lambda(3) + \frac{r_1}{n}\beta(3))}{(\log n)^2} - \frac{16\pi^2(1+1/n)}{(\log n)^3\left(1 + \frac{\pi^2}{(\log n)^2}\right)^2} \right) \quad (1.1)$$

où $\gamma = 0.5772156649...$ est la constante d'euler, $\lambda(3) = 1.0517997902...$, $\beta(3) = 0.9689461462...$ et r_1 est le nombre de places réelles du corps de nombres K.

Sachant qu'une meilleure minoration (en valeur absolue) du discriminant d'un corps de nombres de degré n pair est obtenue pour un corps totalement imaginaire, l'inégalité précédente donne alors :

$$\frac{1}{n}\log|d_K| \geq \left(\gamma + log8\pi - \frac{2\pi^2\lambda(3)}{(\log n)^2} - \frac{16\pi^2(1+1/n)}{(\log n)^3\left(1+\frac{\pi^2}{(\log n)^2}\right)^2}\right). \quad (1.2)$$

Dans le cas d'un corps de nombres de degré n impair, on a la minoration suivante pour $r_1 = 1$:

$$\frac{1}{n}\log|d_K| \geq \left(\gamma + log8\pi + \frac{\pi}{2n} - \frac{2\pi^2(\lambda(3)+\frac{1}{n}\beta(3))}{(\log n)^2} - \frac{16\pi^2(1+1/n)}{(\log n)^3\left(1+\frac{\pi^2}{(\log n)^2}\right)^2}\right). \quad (1.3)$$

Sachant que la valeur absolue du discriminant d'un corps de nombres augmente avec r_1, l'inégalité précédente donne alors une meilleure minoration du discriminant dans le cas où le degré n est impair.

1.2 Minorations des valeurs absolues des discriminants des corps

Les tableaux 1 et 2 suivants établis par Diaz y Diaz dans **[8]** donnent respectivement des minorations des valeurs absolues des discriminants des corps de nombres de degré 8 et de degré 9 en fonction de leur signature (r_1, r_2) où $r_1 + 2r_2 = 8$ en degré 8 et $r_1 + 2r_2 = 9$ en degré 9. Ces résultats obtenus de façon inconditionnelle (sans GRH), ne tiennent pas compte non plus de la contribution des idéaux premiers non nuls de petite norme des corps.

Signatures	$(8,0)$	$(6,1)$	$(4,2)$	$(2,3)$	$(0,4)$
Minorations	158 960 873	42 071 532	11 660 853	3 403 708	1 052 302

Tableau 1

Signatures	$(9,0)$	$(7,1)$	$(5,2)$	$(3,3)$	$(1,4)$
Minorations	4 516 673 524	1 133 345 241	295 584 269	80 499 454	23 007 468

Tableau 2

Des travaux plus avancés du même auteur dans **[9]** ont montré que la valeur minimale du discriminant d'un corps de nombres totalement imaginaire en degré 8 est 1 257 728. Sachant que la plus petite valeur en valeur absolue du discriminant d'un corps de nombres de degré n pair est obtenue dans le cas totalement imaginaire, on en déduit alors que la valeur précédente est le minima du discriminant d'un corps octique. Le corps donnant ce minima est imprimitif (i.e contenant un sous-corps) ; c'est une extension quartique du corps quadratique $\mathbb{Q}(i)$ et le groupe de Galois de sa clôture galoisienne est $C_4^2 \rtimes C_2$, noté T_{17} suivant la notation de Butler et Mc Kay dans **[3]**.

Dans le cas totalement réel (i.e de signature $(8,0)$) en degré 8, des travaux effectués dans **[11]** ont montré que la valeur minimale du discriminant est 282 300 416. Pour les autres signatures, il n'existe pas de résultats effectifs donnant la valeur minimale du discriminant. Les seules tables existantes en degré 8 concernent les corps imprimitifs contenant un sous-corps quartique (cf. **[6]**).

Dans le cas des corps de nombres de degré 9, K. Takeuchi **[28]** a montré que la valeur minimale en valeur absolue du discriminant dans le cas totalement réel est 9 685 993 193. Le corps de nombres en question donnant cette valeur minimale du discriminant est un corps primitif. Les seules tables explicites en degré 9 concernent les corps de nombres imprimitifs et elles ont été établies par Diaz Y Diaz et Olivier (cf. **[12]**).

1.3 Groupes de décomposition et groupes de ramification

Soient K un corps de nombres, L une extension galoisienne de K de degré n, G le groupe de Galois de L/K et $\mathbb{Z}_K$ (respectivement $\mathbb{Z}_L$) l'anneau des entiers de K (respectivement de L).

$$\begin{array}{ccc} L & \mathbb{Z}_L & \mathfrak{P} \\ | & | & | \\ | \; n & | & | \\ | & | & | \\ K & \mathbb{Z}_K & \wp \end{array}$$

On note $\mathfrak{P}$ un idéal premier de $\mathbb{Z}_L$ au-dessus d'un idéal premier $\wp$ de $\mathbb{Z}_K$ et

$$D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

le groupe de décomposition de $\mathfrak{P}|\wp$.
Le groupe

$$G_0 = \{\sigma \in D_{\mathfrak{P}} \mid \forall x \in \mathbb{Z}_L,\, \sigma(x) - x \in \mathfrak{P}\}$$

est le groupe d'inertie de $\mathfrak{P}|\wp$ et son cardinal est égal à l'indice de ramification $e(\mathfrak{P}|\wp)$ de $\mathfrak{P}$ dans L/K. Tous les indices de ramification des idéaux premiers $\mathfrak{P}$ de L au-dessus de $\wp$ sont égaux car l'extension L/K est galoisienne.
Le groupe

$$G_k = \{\sigma \in G \mid \forall x \in \mathbb{Z}_L,\;\; \sigma(x) - x \in \mathfrak{P}^{k+1}\}, \quad k \geq 1$$

est le k-ième groupe de ramification.

On a le théorème suivant (cf. **[5]**) :

Théorème 1.3.1
Avec les notations précédentes, on a :
i) G_0/G_1 *est un sous-groupe cyclique du groupe multiplicatif du corps résiduel* $\mathbb{Z}_L/\mathfrak{P}$. *De plus il est d'ordre premier à la caractéristique* p *du corps résiduel* $\mathbb{Z}_K/\wp$.
ii) G_1 *est un* p*-groupe qui mesure la ramification sauvage en* $\wp$ *:* G_1 *est trivial si et seulement si l'extension* L/K *est modérément ramifiée en* $\wp$.

1.4 Groupes résolubles

Définition 1.4.1
Un groupe fini G *est résoluble s'il possède une suite* $(G_k)_{0\leq k\leq n}$ *finie décroissante de sous-groupes telle que :*
i) $G_0 = G \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$
ii) $G_{k+1} \lhd G_k$ *pour* $0 \leq k \leq n-1$ *(i.e* G_{k+1} *est distingué dans* G_k*)*
iii) G_k/G_{k+1} *est abélien* $\quad (0 \leq k \leq n-1)$.

Notation :

Un commutateur d'un groupe G est un élément de la forme $[a,b] = a^{-1}b^{-1}ab$, où $(a,b) \in G^2$. L'ensemble des commutateurs de G engendre un sous-groupe de G appelé le groupe des commutateurs de G ou groupe dérivé de G, et noté $D(G) = [G,G]$.

Rappelons quelques résultats extraits de **[7]** sur les groupes résolubles.

Proposition 1.4.2
i) Soient G *et* G' *deux groupes et* $g : G \longrightarrow G'$ *un homomorphisme de groupes ; alors on a :* $g(D(G)) = D(g(G)) \subseteq D(G')$.
ii) $D(G)$ *est un sous-groupe caractéristique de* G*, c'est-à-dire un sous-groupe stable par tout automorphisme de* G. *En particulier* $D(G)$ *est un sous groupe distingué de* G.

Proposition 1.4.3
Soit G *un groupe.*
i) G *est commutatif* $\Leftrightarrow D(G) = \{e\}$.
ii) Pour tout sous-groupe $H \lhd G$ *on a :* $D(G) \subseteq H \Leftrightarrow G/H$ *abélien. Ainsi* $D(G)$ *est le plus petit sous-groupe distingué de* G *tel que le quotient soit abélien.*

Proposition 1.4.4
Soit G *un groupe fini. Alors,* G *est résoluble si et seulement si la suite décroissante de groupes dérivés* $D^i(G)$ *définie par récurrence par* $D^0(G) = G$ *et, pour tout* $i \geq 0$ $D^{i+1}(G) = D(D^i(G))$ *prend la valeur* $\{e\}$*, c'est-à-dire s'il existe* $m \in \mathbb{N}$ *tel que* $D^m(G) = \{e\}$.

Proposition 1.4.5
Soit G un groupe.

1. *Si G est un groupe résoluble et si $H \lhd G$ alors G/H est résoluble.*
2. *Si $H \lhd G$, et si H et G/H sont résolubles alors G est résoluble.*

Exemples de groupes résolubles
1) Tout groupe abélien est résoluble et tout sous-groupe d'un groupe résoluble est résoluble.
2) Tout groupe fini G d'ordre $p^n q^m$ avec p, q des nombres premiers et $n, m \in \mathbb{N}$ est résoluble (théorème de Burnside, cf. **[14]**).
3) Les groupes symétriques S_3 et S_4 sont résolubles.
4) Tout groupe d'ordre pqr avec p, q et r des nombres premiers distincts deux à deux est résoluble.
5) Tout groupe d'ordre strictement inférieur à 60 est résoluble (cf. **[16]**).
Remarque :
Pour $n \geq 5$ le groupe symétrique S_n et le sous-groupe alterné A_n sont non résolubles.

1.5 Groupes transitifs en degré n

Désignons par G le groupe de Galois d'un polynôme irréductible et séparable $f(x) \in K[X]$ où K est un corps, Ω l'ensemble des racines θ_i de f dans le corps de décomposition L et n le nombre de racines de f. Dans les conditions précédentes, G est isomorphe à un sous-groupe du groupe de permutations des éléments de Ω noté $S(\Omega) = S_n$. Le polynôme f de degré n étant irréductible et séparable alors le groupe de Galois G considéré comme un groupe de permutations des racines de f est un sous-groupe transitif de S_n (ou encore un groupe transitif de degré $n = |\Omega|$).

Ainsi pour $K = \mathbb{Q}$, si f est irréductible de degré 8 (resp. de degré 9), son groupe de Galois G est un sous-groupe transitif de S_8 (resp. de S_9).

1.5.1 Groupes transitifs en degré 8

Les travaux réalisés sur les corps de nombres de degré 8 ont montré qu'il existe à conjuguaison près 50 sous-groupes transitifs du groupe symétrique S_8, notés respectivement $T_1, ..., T_{50}$ suivant les notations de Butler et Mc Kay (cf.**[3]**). Les groupes de Galois en degré 8 étant considérés comme les sous-groupes transitifs du groupe symétrique S_8 (noté T_{50}), Butler et Mc Kay ont donné pour chacun d'eux un système de générateurs. Nous donnons dans les tableaux en annexe A quelques résultats extraits de **[3]** sur ces groupes.

On montre que seuls cinq parmi ces groupes de Galois en degré 8 sont non résolubles. Ces résultats sont resumés dans le tableau suivant où le symbôle '+' indique que le groupe est pair (i.e un sous-groupe du groupe alterné A_8).

Groupes	T_{37}	T_{43}	T_{48}	A_8	S_8
Ordres	168	336	1 344	20 160	40 320
Parité	+		+	+	

Tableau 3

Remarque :
Dans toute la suite, nous utiliserons les numérotations de Butler et Mc Kay des groupes transitifs en degré 8 ; on désigne donc par T_{50} le groupe symétrique S_8 et par T_{49}^+ le groupe alterné A_8.

Nous donnons ici (cf. **[3]**) un système de générateurs de chacun de ces sous-groupes non résolubles. En posant :

$A = (1,2,3,4,5,6,7)$, $B = (2,4,3,7,5,6)$, $C = (2,3)(4,7)$, $D = (1,8)(2,4)(3,7)(5,6)$
$E = (1,8)(2,7)(3,4)(5,6)$, $t = (1,2)$ et $z = (6,8,7)$; on a

$$T_{37}^+ =< A, B^2, E >$$
$$T_{43} =< A, B, E >$$
$$T_{48}^+ =< A, C, D >$$
$$T_{49}^+ =< A, z >$$
$$T_{50} =< A, z, t >.$$

Les travaux de Eichenlaub (cf. **[13]**) sur les groupes de Galois des corps octiques en fonction de la signature sont donnés dans le tableau 4 ci-dessous.

Signature	Groupes de Galois possibles	Nombre de groupes possibles
$(8,0)$	tous les groupes sont possibles	50
$(6,1)$	$T_{27}, T_{31}, T_{35}, T_{38}, T_{44}, T_{47}, T_{50}$	7
$(4,2)$	T_7, T_9^+, T_{10}^+ ,T_{11}^+, T_{15}, T_{16}, T_{17}, T_{18}^+, T_{19}^+, T_{20}^+, T_{21}, T_{22}^+, T_{24}^+, T_{26}, T_{27}, T_{28}, T_{29}^+, T_{30}, T_{31}, T_{32}^+, T_{33}^+, T_{34}^+, T_{35}, T_{38}, T_{39}^+, T_{40}, T_{41}^+, T_{42}^+, T_{44}, T_{45}^+, T_{46}, T_{47}, T_{48}^+, T_{49}^+, T_{50}	35
$(2,3)$	T_6, T_8, T_{15}, T_{23}, T_{26}, T_{27}, T_{30}, T_{31}, T_{35}, T_{38}, T_{40}, T_{43}, T_{44}, T_{47}, T_{50}	15
$(0,4)$	tous les groupes sont possibles	50

Tableau 4

1.5.2 Groupes transitifs en degré 9

Il existe à conjuguaison près 34 sous-groupes transitifs du groupe symétrique S_9, notés respectivement $T_1, ..., T_{34}$ suivant toujours les notations de Butler et Mackay (voir Annexe A). Les groupes non résolubles sont donnés dans le tableau suivant

Groupes	T_{27}^+	T_{32}^+	T_{33}^+	T_{34}
Ordres	504	1 512	181 440	362 880

Tableau 5

Comme dans le cas des groupes transitifs de degré 8, nous donnons ici un système de générateurs de chacun de ses groupes non résolubles en degré 9. En posant :

$$J = (1,2,3,4,5,6,7),\ R = (1,8)(2,4)(3,7)(5,6),\ S = (2,7)(3,6)(4,5)(8,9)$$
$$M = (2,4,3,7,5,6),\ p = (7,8,9) \text{ et } q = (2,3)\,;\ \text{on a}$$
$$T_{27}^+ =< J, R, S >$$
$$T_{32}^+ =< J, M^2, R, S >$$
$$T_{33}^+ =< J, p >$$
$$T_{34} =< J, p, q >.$$

Avant de poursuivre notre étude, voyons une notion très utile dans nos recherches : il s'agit de la notion de groupe primitif.

1.5.3 Groupes de Galois primitifs de degré n

Définition 1.5.1

Sous les hypothèses précédentes, le groupe transitif G de degré n sur Ω est dit imprimitif s'il existe une partition $\{\Omega_1, \Omega_2, \ldots, \Omega_s\}$ de Ω qui soit stable par tout élément de G, et telle que $|\Omega_i| \geq 2$ pour au moins un $i \leq s$. Le système $\Omega = \bigcup_{i=1}^{s} \Omega_i$ est appelé système d'imprimitivité.

Quand un tel système n'existe pas, on dit que G est primitif. Autrement dit le groupe transitif G sur Ω est primitif si les seules partitions de Ω que G conserve sont les partitions triviales, à savoir Ω lui-même et l'ensemble des singletons de Ω.

Remarque :
Tous les blocs Ω_i du système d'imprimitivité ont le même cardinal.
Exemples de groupes primitifs (cf. **[2]**) :
1) Pour tout n, S_n et A_n sont primitifs sur $\Omega = \{1, 2, \ldots, n\}$.
2) Pour n premier, tout groupe transitif de S_n est primitif.

Voyons la proposition suivante qui permet de caractériser les groupes de Galois primitifs à partir de corps de nombres de degré n qui sont primitifs.

Proposition 1.5.2

Sous les hypothèses précédentes, si $f(x)$ est un polynôme unitaire, irréductible de degré n dans $\mathbb{Z}[x]$ et $K = \mathbb{Q}(\theta)$ un corps de rupture de f, alors G est primitif si et seulement si K ne contient pas de corps intermédiaire.

Preuve :
Donnons d'abord ce résultat (cf. **[2]**) : G est imprimitif si et seulement si pour tout $\theta \in \Omega$, il existe un sous-groupe H tel que $\Gamma_\theta \subsetneq H \subsetneq G$ où Γ_θ est le stabilisateur de θ dans G. Donc dire que G est primitif revient à dire que le stabilisateur de tout élément de Ω est maximal dans G.

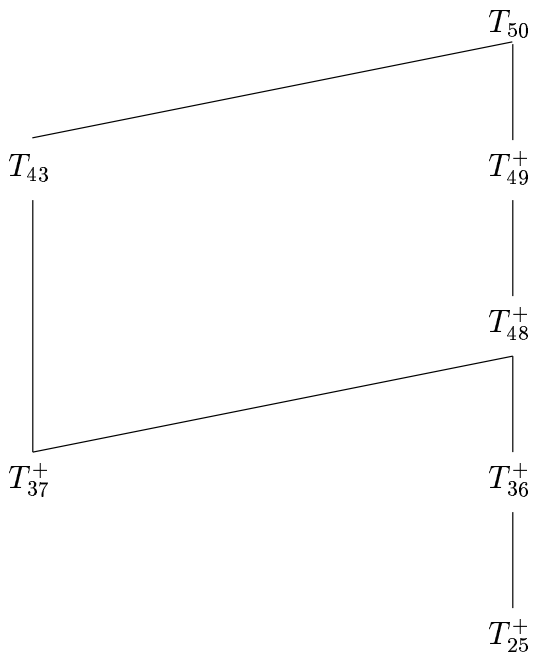
Notons L une clôture galoisienne fixe du corps de rupture K. Nous allons montrer par le théorème de Galois que $\Gamma = Gal(L/K)$ est maximal si et seulement si G est primitif. En

effet l'extension L/K étant galoisienne, Γ est un sous-groupe de G. Donc dire qu'il existe un sous-groupe H de G tel que $\Gamma \subsetneq H \subsetneq G$, en prenant $R = L^H$, on aurait R un sous-corps de K. Les sous-extensions R de K sont en bijection avec les partitions stables de Ω par G. En effet se donner une partition $G-$stable de Ω, c'est se donner un sous-groupe H tel que $\Gamma_\theta \subsetneq H \subsetneq G$. Il suffit de prendre $H = \Gamma_{\Omega_\theta}$ i.e le stabilisateur dans G du bloc Ω_θ contenant θ. Par la théorie de Galois on a le sous-corps $R = L^H$ de K. Reciproquement se donner une sous-extension R de K, c'est se donner un sous-groupe $H = Gal(L/R)$ de G tel que $\Gamma \subsetneq H \subsetneq G$. On définit alors une partition $G-$stable $\{\Omega_1, \Omega_2, \ldots, \Omega_r\}$ de Ω telle que Ω_1 est l'orbite de θ sous H et les autres blocs $\Omega_2, \ldots, \Omega_r$ sont les images de Ω_1 par des représentants de G/H.

Or, on a vu que G est primitif est équivalent à dire que Γ_{θ_i} est maximal pour tout $\theta_i \in \Omega$. Comme $L^{\Gamma_{\theta_i}} = K_i = \mathbb{Q}(\theta_i)$, on a alors $\Gamma_\theta = \Gamma$; d'après ce qui précède, cela équivaut à dire aussi que K ne contient pas de corps intermédiaire. □

Groupes de Galois primitifs en degré 8 :

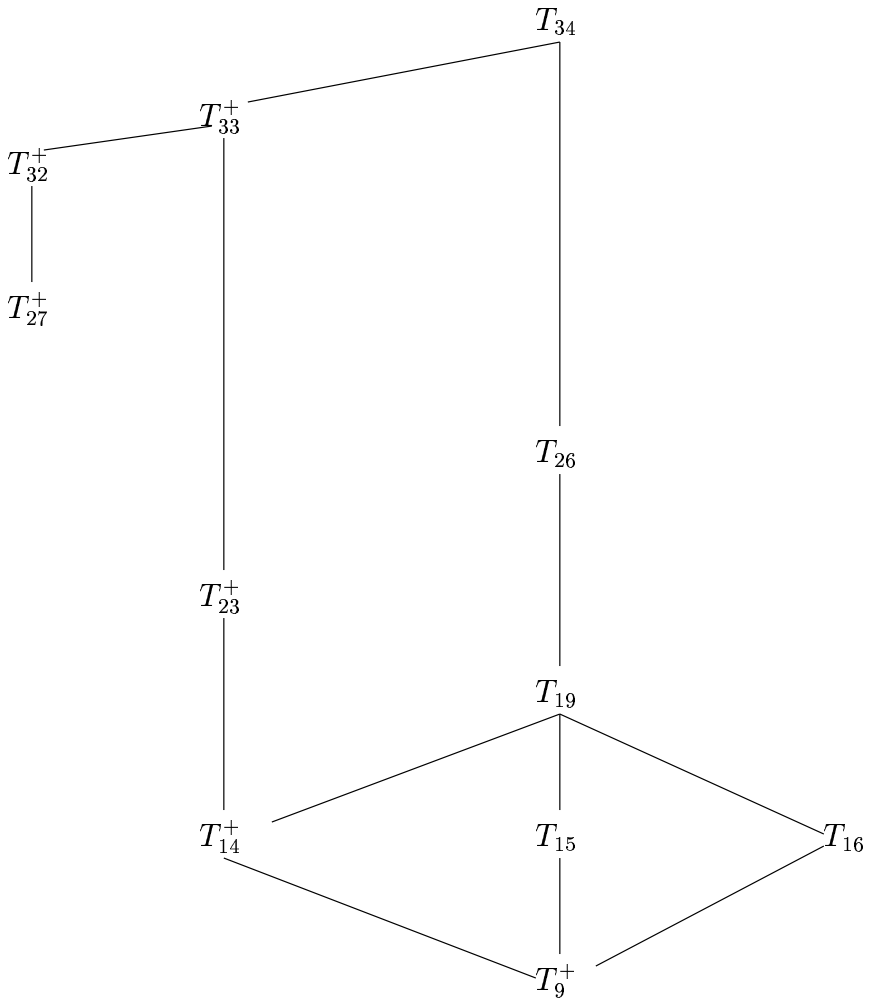
Dans le cas du degré $n = 8$, les travaux de Eichenlaub (cf. **[13]**) donnent en plus le graphe suivant des inclusions à conjuguaison dans T_{50} près des sous-groupes transitifs primitifs de T_{50}.



A travers le graphe ci-dessus, on remarque que tous les groupes non résolubles du tableau 3 sont primitifs. D'après la proposition 1.5.2, les corps K dont les clôtures galoisiennes L ont ces groupes de Galois non résolubles sont tous primitifs. Nous pouvons donc restreindre notre recherche aux corps de nombres de degré 8 qui sont primitifs.

Groupes de Galois primitifs en degré 9 :

Dans le cas du degré $n = 9$, on a aussi le graphe (cf. **[13]**) donnant les inclusions à conjuguaison dans T_{34} près des sous-groupes transitifs primitifs de T_{34}.



De façon analogue au graphe précédent, on remarque que tous les groupes non résolubles du tableau 5 sont primitifs. Nous pouvons donc comme précédemment restreindre notre recherche aux corps de nombres de degré 9 qui sont primitifs.

1.6 Les travaux de Dedekind et de Ore

Tous les résultats donnés dans ce paragraphe sont extraits de **[30]** et **[31]**.

Soit K un corps de nombres de degré n, de discriminant d_K, $\mathbb{Z}_K$ l'anneau des entiers de K et p un nombre premier. L'idéal $p\mathbb{Z}_K$ engendré par le nombre premier p dans $\mathbb{Z}_K$ se décompose de la façon suivante :

$$p\mathbb{Z}_K = \prod_{\wp|p} \wp^{e_\wp}, \tag{1.4}$$

où le produit s'étend aux idéaux premiers $\wp$ de $\mathbb{Z}_E$ au-dessus de p, $e_\wp$ est l'indice de ramification de $\wp$ dans $K/\mathbb{Q}$, $f_\wp$ le degré résiduel, et on a $\sum_{\wp|p} e_\wp f_\wp = n$, et $\mathcal{N}(\wp) = p^{f_\wp}$.

Le corps K est ramifié en p si et seulement si p divise d_K. Dedekind montre que la valuation en p du discriminant d_K du corps de nombres K, notée $v_p(d_K)$ dépend de la relation (1.4), et, de plus si le corps de nombres est modérement ramifié en p (i.e pour tout $\wp|p$ on a $p \nmid e_\wp$) alors on a :

$$v_p(d_K) = \sum_{\wp|p} f_\wp(e_\wp - 1).$$

Ore traite le cas général, c'est-à-dire le cas modérement ramifié et le cas sauvagement ramifié à travers le théorème suivant :

Théorème 1.6.1 (Ore)
Avec les notations précédentes, si K est ramifié en p on a :

$$v_p(d_K) \leq \sum_{\wp|p} f_\wp(e_\wp + e_\wp v_p(e_\wp) - 1), \tag{1.5}$$

où la somme s'étend aux idéaux premiers $\wp$ de $\mathbb{Z}_K$ au-dessus de p.
Plus précisement en posant $n = \sum_{i=0}^{q} b_i p^i$ avec $0 \leq b_i < p$ et $b_q \neq 0$, le développement p-adique de n, on a

i) la valeur maximale possible de $v_p(d_K)$, notée $N_{n,p}$ est donnée par :

$$N_{n,p} = \sum_{i=0}^{q} b_i(i+1)p^i - h, \tag{1.6}$$

où h désigne le nombre de coefficients b_i non nuls.

ii) Si p est impair, alors $v_p(d_K)$ peut prendre toutes les valeurs comprises entre 0 et $N_{n,p}$ à l'exception de $\alpha p^\alpha - 1$ pour $n = p^\alpha$, $\alpha \geq 1$ ou pour $n = p^\alpha + 1$ avec $\alpha \geq 2$.

iii) Si $p = 2$ le résultat est le même qu'en ii) avec en plus $v_p(d_K) \neq 1$.

Les résultats ci-dessus sont essentiels dans le cas où le nombre premier p considéré est inférieur au degré n du corps de nombres. Dans le cas $p > n$, on a le corollaire plus simple suivant :

Corollaire 1.6.2
Si $p > n$ alors les valeurs possibles de $v_p(d_K)$ sont comprises entre 0 et $n-1$. De plus si $f_\wp = 1$ pour tout $\wp|p$, alors $v_p(d_K) = n - j$, où j est le nombre de $\wp$ divisant p.

Preuve :
En effet si $p > n$ alors le développement p-adique de n donne $n = b_0 p^0$ avec $b_0 = n$, et donc $N_{n,p} = n - 1$. Dans ce cas $v_p(d_K)$ prend ses valeurs dans l'intervalle $[0, n-1]$.
La condition $p > n$ implique que le corps de nombres est modérément ramifié en p, et si $f_\wp = 1$ pour tout $\wp|p$, dans ce cas, d'après les travaux de Dedekind, on a $v_p(d_K) = n - j$ où j est le nombre d'idéaux premiers $\wp|p$ tel que $1 \leq j \leq n$. □

Nous terminons cette partie par le théorème de Stickelberger sur les valeurs prises par le discriminant d'un corps de nombres.

Théorème 1.6.3 (Stickelberger)
Soient K un corps de nombres de degré n, d_K son discriminant et $(\alpha_1, \ldots, \alpha_n)$ une base d'entiers de K. Alors on a :

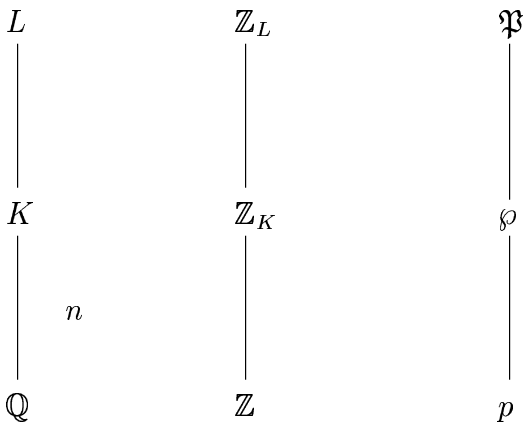
$$d_K \equiv 0 \text{ ou } 1 \pmod 4.$$

Dans le chapitre qui suit où nous aurons à déterminer les valeurs possibles prises par le discriminant du corps de nombres, le théorème ci-dessus s'avère très utile dans la détermination du signe du discriminant. Mais avant, voyons les notations qui seront utilisées pour la suite de notre étude.

1.7 Notations

Dans toute la suite, on désigne sauf mention du contraire, par :

1. K un corps de nombres de degré 8 (resp. de degré 9)
2. L la clôture galoisienne de K
3. $\mathbb{Z}_K$ (resp. $\mathbb{Z}_L$) l'anneau des entiers de K (resp. de L)
4. d_K (resp. d_L) le discriminant de K (resp. de L)
5. (r_1, r_2) la signature du corps de nombres K où $r_1 + 2r_2 = n$ avec $n = 8$ (resp. $n = 9$)
6. le nombre premier $p = 2, 3, 5$ ou 7
7. $\wp$ un idéal premier de K au dessus du nombre premier p
8. $\mathfrak{P}$ un idéal premier de L au dessus de $\wp$.


L
K
n
$\mathbb{Q}$
$\mathbb{Z}_L$
$\mathbb{Z}_K$
$\mathbb{Z}$
$\mathfrak{P}$
$\wp$
p

Chapitre 2

Ramification

Les différents résultats du paragraphe 1.5 du chapitre précédent simplifient considérablement nos recherches dans la mesure où ils permettent de ne prendre en compte que les corps de nombres de degré 8 (resp. de degré 9) qui sont primitifs. Dans ce chapitre, notre étude va consister d'abord en la détermination des différentes ramifications possibles des corps octiques (resp. noniques) en un unique $p < 11$. Ensuite nous verrons pour les cas possibles, les différentes décompositions de l'idéal $p\mathbb{Z}_K$. Enfin nous terminerons ce chapitre par les valeurs possibles du discriminant d_K. Par abus de langage lorsque nous parlerons de la ramification de la clôture galoisienne L en un premier p, il va s'agir de la ramification en un idéal $\mathfrak{P}|p$. On dira aussi que L est ramifié en un unique premier p si les idéaux premiers $\mathfrak{P}$ ramifiés dans L sont ceux au-dessus de p.

Nous allons maintenant entamer l'étude de la ramification dans $K/\mathbb{Q}$ dans le cas où il n'y a qu'un seul nombre premier p ramifié. Voyons d'abord les propositions suivantes concernant les ramifications aussi bien du corps K que de sa clôture galoisienne L.

Proposition 2.0.1
Les corps K et L sont ramifiés en les mêmes premiers p.

Preuve :
Si K est ramifié en un premier p alors il en est de même dans sa clôture galoisienne L.

Réciproquement si L est ramifié en un premier p, nous allons montrer par l'absurde que K ne peut être non ramifié en ce premier. Supposons donc L ramifié en p et K non ramifié.

$$\begin{array}{ccc} L & & \mathfrak{P} \\ | & & | \\ K & & \wp \\ | & & | \\ \mathbb{Q} & & p \end{array}$$

Le corps L étant galoisien et ramifié en p, on a alors la décomposition $p\mathbb{Z}_L = \prod_{\mathfrak{P}|p} \mathfrak{P}^e$ où le produit s'étend aux idéaux premiers $\mathfrak{P}$ de $\mathbb{Z}_L$ au-dessus du nombre premier p. Le corps K étant non ramifié en p alors il est non ramifié en tout idéal premier $\wp$ de $\mathbb{Z}_K$ au-dessus de p ; on a donc la décomposition suivante $p\mathbb{Z}_K = \prod_{\wp|p} \wp$. Pour chaque $\mathfrak{P}$ au-dessus de p, il existe $\wp$ au-dessus de p tel que $\mathfrak{P}$ soit au-dessus de $\wp$; de plus pour tout $\wp|p$, on a $\wp\mathbb{Z}_L = \prod_{\mathfrak{P}|\wp} \mathfrak{P}^e$. Pour chaque $\mathfrak{P}|p$ fixé, notons $K_{\mathfrak{P}}$ la sous-extension maximale

de L non ramifiée en $\mathfrak{P}$. On a $K \subset K_{\mathfrak{P}}$ et par suite $K \subseteq \cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$. Le corps $\cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$ est une extension galoisienne de $\mathbb{Q}$ contenant K.
En effet pour tout $\sigma \in Gal(L/\mathbb{Q})$, on a $\sigma(\cap_{\mathfrak{P}|p} K_{\mathfrak{P}}) = \cap_{\sigma(\mathfrak{P}|p)} K_{\sigma(\mathfrak{P})} = \cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$.
Comme L est la plus petite extension galoisienne de $\mathbb{Q}$ contenant K alors $L \subseteq \cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$. Mais le corps $\cap_{\mathfrak{P}|p} K_{\mathfrak{P}}$ n'étant ramifié en aucun $\mathfrak{P}|p$, et donc non ramifié en p, ce qui implique que son sous-corps L est non ramifié en p. Ceci est impossible. □

Proposition 2.0.2
Les corps K et L sont sauvagement ramifiés en les mêmes nombres premiers p.

Preuve :
Si K est sauvagement ramifié en p alors il en est de même pour sa clôture galoisienne L.

Supposons maintenant L sauvagement ramifié en un premier p et K modérement ramifié.

$$\begin{array}{cc} L & \mathfrak{P} \\ | & | \\ K & \wp \\ | & | \\ \mathbb{Q} & p \end{array}$$

On a les décompositions suivantes :
$p\mathbb{Z}_L = \prod_{\mathfrak{P}|p} \mathfrak{P}^e$ où p divise l'indice de ramification e et $p\mathbb{Z}_K = \prod_{\wp|p} \wp^{e_\wp}$ où p ne divise aucun indice de ramification $e_\wp$ des idéaux $\wp$ au-dessus de p.
Pour chaque $\mathfrak{P}|p$ fixé, on note $L_{\mathfrak{P}}$ la sous-extension maximale de L modérement ramifiée en $\mathfrak{P}$. On montre que le corps $\cap_{\mathfrak{P}|p} L_{\mathfrak{P}}$ est une extension galoisienne de $\mathbb{Q}$ contenant K. Comme cette extension est modérement ramifiée en p et qu'elle contient L alors cela entraine que L est modérement ramifié en p. Cette situation contredit donc notre hypothèse de départ. □

2.1 Etude de la ramification des corps de degré 8

2.1.1 Les minima des discriminants

Nous commençons ce paragraphe par ces résultats extraits de **[20]** qui donnent les sous-groupes transitifs G de T_{50} qui sont primitifs et, pour chaque possibilité de signature du corps de nombres K, le discriminant minimum quand il est connu ou une majoration du minimun de $|d_K|$ quand le minimum est inconnu. Tous ces résultats sont consignés dans le tableau 6. A la lecture des données, nous pouvons remarquer que tous les groupes primitifs peuvent être réalisés à partir de corps K totalement réels ou totalement imaginaires. Le groupe T_{50} peut être réalisé à partir de toutes les signatures du corps K.

G	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{25}^+	594 823 321	impossible	impossible	impossible	9 745 585 291 264
T_{36}^+	1 817 487 424	impossible	impossible	impossible	$\leq$ 6 423 507 767 296
T_{37}^+	$\leq$ 37 822 859 361	impossible	impossible	impossible	$\leq$ 8 165 659 002 209 296
T_{43}	$\leq$ 418 195 492	$\leq$ 1 997 331 875	impossible	impossible	$\leq$ 312 349 488 740 352
T_{48}^+	$\leq$ 32 684 089	impossible	$\leq$ 351 075 169	impossible	$\leq$ 81 366 421 504
T_{49}^+	$\leq$ 20 912 329	impossible	$\leq$ 144 889 369	impossible	$\leq$ 46 664 208 361
T_{50}	$\leq$ 1 282 789	$\leq$ 4 296 211	$\leq$ 15 908 237	$\leq$ 65 106 259	483 345 053

Tableau 6

2.1.2 Ramification en p=2

Proposition 2.1.1
Si le corps K est ramifié seulement en 2, alors il est sauvagement ramifié.

Preuve :
Supposons K modérement ramifié en 2 : la relation (1.5) du théorème 1.6.1 de Ore donne :

$$v_2(d_K) \leq 8 - \sum_{\wp|2} f_\wp \, .$$

Le corps K étant modérement ramifié en 2, il y a au moins deux idéaux $\wp|2$. On a alors $v_2(d_K) \leq 6$. Le calcul donne $|d_K| < 1\ 257\ 728$, ce qui est en contradition avec la valeur minimale (en valeur absolue) du discriminant d'un corps de nombres de degré 8. □

Corollaire 2.1.2
Si la clôture galoisienne L est ramifiée seulement en 2 alors le corps K l'est sauvagement.

Preuve :
Le corps K étant un sous-corps de la clôture galoisienne L, si L est ramifiée seulement en 2 alors il en est de même du corps K. On conclut d'après la proposition précédente. □

Notons que le calcul par la méthode de Ore (cf. théorème 1.6.1) donne comme valeur maximale de la valuation $v_2(d_K)$ la valeur $N_{8,2} = 31$. On en déduit donc que $|d_K| \leq 2^{31}$. Cette valeur est atteinte pour la décomposition suivante :

$$2\mathbb{Z}_K = \wp^8$$

c'est à dire pour K totalement ramifié en 2.

Voyons ce qu'il en est du type de ramification du corps L grâce au corollaire suivant qui découle des propositions 2.0.2 et 2.1.1.

Corollaire 2.1.3
Si le corps L est ramifié seulement en 2 alors il est sauvagement ramifié.

Le type de ramification étant connu aussi bien pour le corps K que pour le corps L, nous allons maintenant déterminer les différentes décompositions de l'idéal $2\mathbb{Z}_K$ engendré par 2 dans l'anneau $\mathbb{Z}_K$.

Théorème 2.1.4
Si le corps K est ramifié seulement en 2, alors les seules décompositions possibles de l'idéal engendré par 2 dans l'anneau $\mathbb{Z}_K$ sont : $2\mathbb{Z}_K = \wp^8$, $2\mathbb{Z}_K = \wp_1^4\wp_2^4$ et $2\mathbb{Z}_K = \wp^4$, où le degré résiduel est égal à 1 dans les deux premières décompositions et à 2 dans la dernière.

Preuve :
Le corps K étant ramifié seulement en 2 on sait d'après ce qui précède qu'il est sauvagement ramifié. Voyons parmi les différentes décompositions de

$$2\mathbb{Z}_K = \prod_{\wp|2} \wp^{e_\wp} \text{ avec } \sum_{\wp|2} e_\wp f_\wp = 8$$

celles qui donnent la plus grande valeur de $v_2(d_K)$.

1) Si $v_2(e_\wp) = 0$ ou 1 pour tout $\wp|2$:
   1.1) si $f_\wp = 1$ pour tout $\wp|2$:
   La décomposition donnant la plus grande valeur de $v_2(d_K)$ dans ce cas est :

$$2\mathbb{Z}_K = \wp_1^6\wp_2^2.$$

   Le calcul à partir de la relation (1.5) du théorème 1.6.1 de Ore donne $v_2(d_K) \leq 14$. Ce cas est impossible car $2^{14} < 1\ 257\ 728$.
   1.2) S'il existe un $\wp|2$ tel que $f_\wp \geq 2$:
   La décomposition donnant la plus grande valeur de $v_2(d_K)$ est :

$$2\mathbb{Z}_K = \wp_1\wp_2^6$$

   avec $f_1 = 2$ et $f_2 = 1$.
   Le calcul donne $v_2(d_K) \leq 13$. Ce cas est impossible pour la même raison que précédemment.

2) S'il existe $\wp|2$ tel que $v_2(e_\wp) = 2$:
   2.1) si $f_\wp = 1$ pour tout $\wp|2$:
   La plus grande valeur de $v_2(d_K)$ est atteinte par la décomposition :

$$2\mathbb{Z}_K = \wp_1^4\wp_2^4, \text{ et on a } v_2(d_K) \leq 22.$$

   Ce cas est possible car $2^{22} > 1\ 257\ 728$.
   2.2) S'il existe $\wp|2$ tel que $f_\wp = 2$:
   La décomposition donnant la plus grande valeur de $v_2(d_K)$ est :

$$2\mathbb{Z}_K = \wp^4 \text{ avec } f_\wp = 2.$$

Le calcul donne $v_2(d_K) \leq 22$. Ce cas est possible car $2^{22} > 1\ 257\ 728$.

3) S'il existe $\wp|2$ tel que $v_2(e_\wp) = 3$:
La seule décomposition possible est alors :

$$2\mathbb{Z}_K = \wp^8$$

et on a $v_2(d_K) \leq 31$; ce cas est possible car $2^{31} > 1\ 257\ 728$. □

Remarque :
Nous voyons bien à travers ce théorème que si le corps de nombres K est ramifié seulement en 2 alors il contient des idéaux premiers de norme 2 ou des idéaux premiers de norme 4.

En appliquant le théorème 1.6.1 de Ore, nous allons montrer que le groupe T_{37}^+ ne peut être le groupe de Galois de la clôture galoisienne L d'un corps de nombres K ramifié seulement en 2.

Théorème 2.1.5
Si le corps K est ramifié seulement en 2 alors le groupe de Galois $Gal(L/\mathbb{Q})$ ne peut être isomorphe à T_{37}^+.

Preuve :
Supposons $Gal(L/\mathbb{Q}) = T_{37}^+$. Le corps de nombres K étant ramifié seulement en 2, alors, d'après la proposition 2.0.1 sa clôture galoisienne L l'est aussi. Du corollaire 2.1.2 on en déduit que L est sauvagement ramifié en 2. La plus grande puissance de 2 divisant $|T_{37}^+| = 168$ est 8, et donc $v_2(e) \leq 3$, car l'indice de ramification e divise $|Gal(L/\mathbb{Q})|$. La relation (1.5) du théorème 1.6.1 de Ore dans le cas d'une extension galoisienne donne :

$$|d_L|^{1/|T_{37}^+|} \leq 2^{1+v_2(e)-1/e}, \text{ c'est-à-dire}$$

$|d_L|^{1/168} \leq 2^{4-1/168}$ car $e \leq 168$;
d'où

$$|d_L|^{1/168} \leq 15.934.$$

Or, la table donnant de façon inconditionnelle la minoration de la racine n-ième du discriminant d'un corps de nombres (cf. **[8]**) donne :

$$|d_L|^{1/168} \geq 17.982$$

ce qui contredit l'inégalité précédente. □

Déterminons maintenant les valeurs possibles du discriminant d_K dans le cas où K est ramifié seulement en 2.

Théorème 2.1.6
Si le corps K est ramifié seulement en 2 alors les valeurs possibles prises par le discriminant d_K appartiennent à l'ensemble :

$$\{\pm 2^{21}, \pm 2^{22}, \pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{27}, \pm 2^{28}, \pm 2^{29}, \pm 2^{30}, \pm 2^{31}\}.$$

Preuve :
En calculant la plus grande puissance de 2 divisant d_K par la méthode de Ore, on obtient $N_{8,2} = 31$. Le résultat s'ensuit en utilisant le *iii*) du théorème 1.6.1 de Ore donnant les valeurs possibles de $v_2(d_K)$, et en remarquant que $2^{20} < 1\,257\,728 < 2^{21}$. Le théorème de Stickelberger ($d_K \equiv 0, 1 \pmod 4$) ne permet pas ici d'avoir des renseignements supplémentaires sur le signe de d_K. □

Grâce au tableau 1 du paragraphe 1.2 et au tableau 6 du paragraphe 2.1, nous donnons ici pour chaque discriminant d_K possible, les signatures (r_1, r_2) susceptibles de réaliser les groupes de Galois non résolubles dans le cas de la ramification en 2. Nous éliminons certains groupes en utilisant le fait que le discriminant $d_{f_\theta} = \prod_{i<j}(\theta_i - \theta_j)^2$ du polynôme générateur f_θ du corps K est un carré (dans $\mathbb{Z} - \{0\}$) si et seulement si le groupe de Galois de f_θ est un sous-groupe de T_{49}^+. D'après la relation $d_{f_\theta} = d_K a^2$ où $a = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$, la condition précédente reste valable en remplaçant d_{f_θ} par d_K.

$d_K = \pm 2^{21}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	**oui**	non	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	**oui**	non	non	non	non

$d_K = \pm 2^{22}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	**oui**	non	non	non	non
T_{49}^+	**oui**	non	non	non	non
T_{50}	non	non	non	non	non

$d_K = \pm 2^{24}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	**oui**	non	**oui**	non	non
T_{49}^+	**oui**	non	**oui**	non	non
T_{50}	non	**oui**	non	non	non

$d_K = \pm 2^{25}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	**oui**	**oui**	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	**oui**	**oui**	**oui**	non	non

$d_K = \pm 2^{26}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	**oui**	non	**oui**	non	non
T_{49}^+	**oui**	non	**oui**	non	non
T_{50}	non	**oui**	non	**oui**	non

$d_K = \pm 2^{27}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	**oui**	**oui**	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	**oui**	**oui**	**oui**	**oui**	non

$d_K = \pm 2^{28}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	**oui**	non	**oui**	non	**oui**
T_{49}^+	**oui**	non	**oui**	non	**oui**
T_{50}	non	non	non	**oui**	non

$d_K = \pm 2^{29}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	**oui**	**oui**	non	non	**oui**
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	**oui**	**oui**	**oui**	**oui**	**oui**

$d_K = \pm 2^{30}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	**oui**	non	**oui**	non	**oui**
T_{49}^+	**oui**	non	**oui**	non	**oui**
T_{50}	**oui**	**oui**	non	**oui**	non

	$Gal(L/\mathbb{Q})$	$r_1=0$	$r_1=2$	$r_1=4$	$r_1=6$	$r_1=8$
$d_K=\pm 2^{31}$	T_{37}^+	non	non	non	non	non
	T_{43}	**oui**	**oui**	non	non	**oui**
	T_{48}^+	non	non	non	non	non
	T_{49}^+	non	non	non	non	non
	T_{50}	**oui**	**oui**	**oui**	**oui**	**oui**

2.1.3 Ramification en p=3

Nous allons montrer dans ce paragraphe que le corps K et sa clôture galoisienne L ne peuvent être ramifiés seulement en 3.

Proposition 2.1.7
Le corps de nombre K ne peut être ramifié seulement en 3.

Preuve :
Si K est ramifié seulement en 3, on a $N_{8,3}=12$ d'après le théorème 1.6.1 de Ore. On en déduit que

$$|d_K| \leq 3^{12} < 1\ 257\ 728.$$

Ceci est impossible. □

Nous avons le corollaire suivant qui découle de cette proposition précédente et de celle vue en 2.0.1.

Corollaire 2.1.8
Le corps L ne peut être ramifié seulement en 3.

2.1.4 Ramification en p=5

En utilisant la méthode de Ore décrite dans le paragraphe 1.6 et le fait que $8 = 3\times 5^0 + 1\times 5$, on a $N_{8,5} = 3\times 1 + 1\times 2\times 5 - 2 = 11$. On en déduit donc que $|d_K| \leq 5^{11}$. Ce résultat ne permet pas a priori de savoir si la ramification seulement en 5 du corps K est possible. Nous montrerons, en supposant vérifiée l'hypothèse de Riemann généralisée (GRH), que ni le corps L, ni le corps K ne peuvent être ramifiés seulement en 5.

Tout d'abord commençons par démontrer que la ramification modérée seulement en 5 n'est possible ni pour le corps K ni pour le corps L.

Proposition 2.1.9
Si le corps K est ramifié seulement en 5 *alors il ne peut l'être modérement.*

Preuve :
Supposons K modérement ramifié en 5 alors la relation (1.5) du théorème 1.6.1 de Ore

donne :

$$v_5(d_K) \leq 8 - \sum_{\wp|5} f_\wp \leq 7.$$

D'où

$$|d_K| \leq 5^7 < 1\ 257\ 728$$

ce qui est impossible car la valeur absolue du discriminant d'un corps de nombres K de degré 8 ne peut vérifier de cette inégalité. □

Corollaire 2.1.10
Si L est ramifié seulement en 5 alors il ne peut l'être modérement.

Preuve :
Ce résultat découle des propositions 2.0.2 et 2.1.9. □

Ramification sous GRH :

Proposition 2.1.11
Sous GRH, le corps L ne peut être ramifié seulement en 5.

Avant de démontrer cette proposition, voyons d'abord le lemme suivant

Lemme 2.1.12
Soient G_1 un sous-groupe de S_8 engendré par un 5-cycle et $N_{S_8}(G_1)$ (resp. $N_{A_8}(G_1)$) le normalisateur de G_1 dans S_8 (resp. le groupe alterné A_8). Alors

i) $N_{S_8}(G_1)/G_1 \simeq S_3 \times C_4$

ii) $N_{A_8}(G_1)/G_1 \simeq S_3 \times C_2$.

Preuve :
Notons σ le 5-cycle qui engendre G_1, par exemple $\sigma = (1\,2\,3\,4\,5)$ (on peut toujours se ramener à ce cas), B (resp. B^C) le support de σ (resp. le complémentaire de B) et I l'ensemble $\{0, 1, 2, 3, 4\}$. Le normalisateur $N_{S_8}(G_1)$ de G_1 dans S_8 est l'ensemble

$$\{g \in S_8 \,|\, \forall i \in I, \exists k \in I \,|\, g\sigma^i g^{-1} = \sigma^k\}.$$

On montre que $S_{(B^C)} \simeq S_3$ est contenu dans $N_{S_8}(G_1)$ car pour tout $g \in S_{(B^C)}$, on a $g\sigma g^{-1} = \sigma$.

i) *a)* Montrons d'abord que $N_{S_8}(G_1) \simeq S_3 \times N_{S_5}(G_1)$.
Pour tout $h \in N_{S_8}(G_1)$ on a

$$h(\{1, 2, 3, 4, 5\}) = \{1, 2, 3, 4, 5\} \text{ et } h(\{6, 7, 8\}) = \{6, 7, 8\}.$$

En effet soit $h \in N_{S_8}(G_1)$ tel qu'il existe $(i, j) \in \{1, 2, 3, 4, 5\} \times \{6, 7, 8\}$ avec $h(i) = j$. En utilisant le fait que $h\sigma h^{-1} = (h(1)\, h(2)\, h(3)\, h(4)\, h(5))$, cela montre que j appartient au Supp$(h\sigma h^{-1})$= B. Ceci est impossible car pour tout entier k, $j \notin$ Supp(σ^k).

La restriction de h au cinq premiers symbôles appartient donc au normalisateur de G_1 dans S_5, noté $N_{S_5}(G_1)$. On peut aussi choisir h librement sur l'ensemble $B^C = \{6, 7, 8\}$.
Considérons le morphisme

$$\begin{array}{rcl} \varphi : N_{S_8}(G_1) & \longrightarrow & S_3 \times N_{S_5}(G_1) \\ h & \longmapsto & (h_1, h_2) \end{array}$$

où h_1 est la restriction de h à B et h_2 sa restriction à B^C.
Le noyau de φ est l'ensemble

$$ker\varphi = \{h \in N_{S_8}(G_1) \mid \varphi(h) = (h_1, h_2) = (Id, Id)\} = \{Id\}.$$

Le morphisme φ est surjectif car tout $(h_1, h_2) \in S_3 \times N_{S_5}(G_1)$ est l'image par φ de $h_1 h_2$.

b) Précisons à présent la structure du groupe $N_{S_5}(G_1)$. Nous allons montrer que $N_{S_5}(G_1)$ est le groupe H produit semi-direct du sous-groupe distingué G_1 par un sous-groupe d'ordre 4.
Considérons $s \in S_5$ tel que $s\sigma s^{-1} = \sigma^2$. On en déduit que le 4-cycle $s = (2\,3\,5\,4)$ convient, et que $s \in N_{S_5}(G_1)$ car pour tour $i \in I$, il existe $j \in I$ tel que $s\sigma^i s^{-1} = \sigma^j$. Le sous-groupe engendré par s est le groupe cyclique C_4 d'ordre 4, et on vérifie aussi que $C_4 \cap G_1 = \{Id\}$. Le sous-groupe du $N_{S_5}(G_1)$ engendré par σ et s est d'ordre 20 et est égal à H. On vérifie que H n'est pas contenu dans A_5 (car il contient la permutation s qui est impaire). Le groupe $H \cap A_5$ est un sous-groupe pair engendré par σ et s^2 (la seule puissance de s qui est paire est s^2). C'est un sous-groupe diédral d'ordre 10 produit semi-direct de G_1 par le sous-groupe engendré par s^2 qui est lui-même isomorphe à C_2. Comme H est contenu dans $N_{S_5}(G_1)$, on en déduit que $N_{S_5}(G_1) \cap A_5$ contient un sous-groupe d'ordre 10 et que l'ordre de $N_{S_5}(G_1) \cap A_5$ est $10, 20, 30$ ou 60 (car contenu dans A_5). Or il n'y a pas de sous-groupe de A_5 d'ordre 20 ou 30, et si on avait $N_{S_5}(G_1) \cap A_5 = A_5$ alors G_1 serait distingué dans A_5 ; cela est impossible car A_5 est simple. D'où $N_{S_5}(G_1) \cap A_5 = H \cap A_5$. Comme $N_{S_5}(G_1)$ contient le groupe H d'ordre 20 et que l'ordre d'un sous-groupe de S_5 est 5, 10, 20, 60 ou 120 ; on vérifie alors que la seule possibilité est que l'ordre de $N_{S_5}(G_1)$ est 20. On a donc $N_{S_5}(G_1) = H = G_1 \rtimes C_4$. Le résultat s'ensuit en utilisant le fait que

$$N_{S_8}(G_1) \simeq S_3 \times (G_1 \rtimes C_4)$$

et en quotientant par le sous-groupe G_1.

ii) Le groupe $N_{A_8}(G_1)$ est égal à $N_{S_8}(G_1) \cap A_8$. On montre comme précédemment que $N_{A_8}(G_1) \simeq S_3 \times N_{A_5}(G_1)$. Le groupe $N_{A_5}(G_1)$ est un sous-groupe de A_5 engendré par σ et s^2. On vérifie que c'est un sous-groupe diédral d'ordre 10 produit semi-direct du sous-groupe distingué G_1 par le sous-groupe engendré par s^2 qui est lui-même isomorphe à C_2. Le résultat s'ensuit en utilisant le fait que

$$N_{A_8}(G_1) \simeq S_3 \times (G_1 \rtimes C_2)$$

et en quotientant par le sous-groupe G_1. $\square$

Preuve de la Proposition 2.1.11 :
Si le corps L est ramifié seulement en 5 alors d'après la proposition précédente il ne peut l'être que sauvagement.

Supposons L sauvagement ramifié en 5 ; le groupe $G = Gal(L/\mathbb{Q})$ est un sous-groupe transitif de T_{50} suivant la numérotation de Butler et Mckay. L'extension $L/\mathbb{Q}$ étant galoisienne on a :

$$5\mathbb{Z}_L = \prod_{i=1}^{g} \mathfrak{P}_i^e,$$

où les $\mathfrak{P}_i$ sont les idéaux premiers de $\mathbb{Z}_L$ au-dessus de 5 avec $|G| = efg$ et 5 divise $|G|$ (car 5 divise e et e divise $|G|$). Comme 5 est sauvagement ramifié dans L et que 25 ne divise pas $|T_{50}|$ alors $v_5(e) = 1$. La relation

$$|G| = [L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 8[L : K]$$

montre que 8 divise $|G|$. On en déduit que 40 divise $|G|$ (car $(8, 5) = 1$), et donc $G = T_{50}$ ou T_{49}^+.

Désignons par G_0 le groupe d'inertie et par G_1 le premier groupe de ramification d'un idéal premier $\mathfrak{P}$ de l'anneau $\mathbb{Z}_L$ au-dessus du nombre premier 5. D'après le théorème 1.3.1 du paragraphe 1.3, G_1 est un 5-sous-groupe distingué non trivial de G_0 tel que G_0/G_1 est cyclique d'ordre premier à 5 . Comme $|G_1| = 5^r$ (où l'entier $r \geq 1$) divise $|G_0| = e$ et que e divise $|G|$ alors $|G_1|$ divise $|G|$, et par suite $r = 1$ car la plus grande puissance de 5 qui divise $|T_{50}|$ ou $|T_{49}^+|$ est 5. D'où $|G_1| = 5$.

Nous allons étudier séparément le cas où $G = T_{50}$ et celui où $G = T_{49}^+$.

1. Si $G = T_{50}$: on note $N_{T_{50}}(G_1)$ le normalisateur de G_1 dans T_{50}. Comme $G_1 \lhd G_0$ et que $N_{T_{50}}(G_1)$ est le plus grand sous-groupe de T_{50} dans lequel G_1 est distingué, alors G_0 est un sous-groupe de $N_{T_{50}}(G_1)$ car $G_0 = N_{G_0}(G_1) \subseteq N_{T_{50}}(G_1)$. On en déduit donc que $|G_0| = e$ divise $|N_{T_{50}}(G_1)|$. Or d'après le lemme précédent le cardinal du normalisateur d'un 5-cycle dans T_{50} est 120. Mais si $e = 120$ alors $G_0 = N_{T_{50}}(G_1)$, et dans ce cas $G_0/G_1 = N_{T_{50}}(G_1)/G_1$ n'est pas cyclique. Ce cas est impossible. On a donc $G_0 \subset N_{T_{50}}$ et $e|60$.

2. Si $G = T_{49}^+$: on note $N_{T_{49}^+}(G_1)$ le normalisateur de G_1 dans T_{49}^+. D'après le lemme précédent, le cardinal du normalisateur d'un 5-cycle dans T_{49}^+ est 60. On montre comme précédemment que G_0 est un sous-groupe de $N_{T_{49}^+}(G_1)$; on en déduit donc que $|G_0|$ divise $|N_{T_{49}^+}(G_1)| = 60$.

Dans les deux cas l'indice de ramification e divise 60 et $v_5(e) = 1$. En utilisant la relation (1.5) du théorème 1.6.1 pour une extension galoisienne, on a :

$$v_5(d_L) \leq f(e + e - 1)g = f(2e - 1)g = |G|(2 - 1/e) \text{ et } \frac{1}{60} \leq \frac{1}{e} \leq \frac{1}{5} \ .$$

Comme

$$\frac{9}{5} \leq 2 - \frac{1}{e} \leq \frac{119}{60} \ ,$$

on en déduit :

$$|d_L|^{1/|G|} \leq 5^{\frac{119}{60}} \approx 24.338.$$

Supposons que l'hypothèse de Riemann généralisée soit vraie pour la fonction zêta de Dedekind du corps L. On peut , dans ces conditions , améliorer sensiblement les minorations de discriminants avec corrections locales (cf. **[24]** pour les détails concernant le calcul de ces corrections locales). La relation (1.2) du paragraphe 1.1 donne alors :

$$\frac{1}{|G|}\log|d_L| \geq \left(3.801 - \frac{20.766}{(\log|G|)^2} - \frac{157.914(1+1/|G|)}{(\log|G|)^3\left(1+\frac{\pi^2}{(\log|G|)^2}\right)^2}\right).$$

On obtient :
si $G = T_{50}$ alors $|d_L|^{(1/|T_{50}|)} \geq 33.248$
si $G = T_{49}^+$ alors $|d_L|^{(1/|T_{49}^+|)} \geq 31.678$.
Ces deux résultats sont en contradition avec la majoration précédente. □

Corollaire 2.1.13

Sous GRH le corps K ne peut être ramifié seulement en 5.

Ramification sans GRH :

De façon inconditionnelle (sans GRH), on obtient les résultats suivants

Proposition 2.1.14

Si K est ramifié seulement en 5 alors il l'est sauvagement. De plus les différentes décompositions possibles de l'idéal engendré par 5 dans $\mathbb{Z}_K$ sont de la forme :

i) $5\mathbb{Z}_K = \wp_1^5\wp_2^3$ *avec* $f_1 = f_2 = 1$,
ii) $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3$ *avec* $f_1 = f_2 = f_3 = 1$,
iii) $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3$ *avec* $f_1 = f_2 = 1$ *et* $f_3 = 2$,
iv) $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3\wp_4$ *avec* $f_1 = f_2 = f_3 = f_4 = 1$.
v) $5\mathbb{Z}_K = \wp_1^5\wp_2$ *avec* $f_1 = 1$ *et* $f_2 = 3$.

Déterminons maintenant grâce à la proposition qui suit les différentes valeurs possibles du discriminant.

Proposition 2.1.15

Si K est ramifié seulement en 5 alors le discriminant d_K appartient à l'ensemble

$$\{5^9, 5^{10}, 5^{11}\}.$$

Preuve : Le calcul de la plus grande puissance de 5 divisant d_K par la méthode de Ore donne $N_{8,5} = 11$. Le résultat s'ensuit en utilisant le théorème de Stickelberger ($d_K \equiv 0, 1 \pmod 4$) et le fait que $|d_K| \geq 1\ 257\ 728$. $\square$

Par application du tableau 1 et des résultats du paragraphe 2.1, nous donnons ici pour chaque discriminant d_K possible, les signatures (r_1, r_2) susceptibles de réaliser les groupes de Galois non résolubles dans le cas de la ramification sans GRH en $p = 5$.

$d_K = 5^9$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	**oui**	non	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	**oui**	non	non	non	non

$d_K = 5^{10}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	**oui**	non	non	non	non
T_{43}	non	non	non	non	non
T_{48}^+	**oui**	non	non	non	non
T_{49}^+	**oui**	non	non	non	non
T_{50}	non	non	non	non	non

$d_K = 5^{11}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	**oui**	non	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	**oui**	non	**oui**	non	non

Remarque :
À la lecture de ces tableaux, on remarque bien que les signatures $(2, 3), (6, 1)$ et $(8, 0)$ ne sont pas possibles pour réaliser les groupes de Galois non résolubles dans le cas de la ramification en 5.

2.1.5 Ramification en p=7

Nous allons étudier maintenant le dernier cas de ramification, soit en $p = 7$. Nous terminerons ce paragraphe en donnant les différentes valeurs possibles du discriminant d_K.

Proposition 2.1.16
Si le corps K est ramifié seulement en 7 alors il est sauvagement ramifié.

Preuve :
Supposons K modérement ramifié en 7 alors la relation (1.5) du théorème 1.6.1 de Ore

permet d'écrire :

$$v_7(d_K) \leq 8 - \sum_{\wp|7} f_\wp \leq 7$$

et donc

$$|d_K| \leq 7^7 < 1\ 257\ 728$$

ce qui est impossible car la valeur absolue du discriminant d'un corps de nombres de degré 8 ne peut vérifier de telle inégalité. □

Corollaire 2.1.17

Si L est ramifié seulement en 7 alors il est sauvagement ramifié.

Corollaire 2.1.18

Si L est ramifié seulement en 7 alors le sous-corps K est sauvagement ramifié en 7.

Preuve :
Si L est ramifié seulement en 7 alors le sous-corps K est aussi ramifié seulement en 7. Le résultat découle de ce qui précède. □

Voyons comment se décompose l'idéal $7\mathbb{Z}_K$ engendré par le nombre premier 7 dans le cas où la ramification en 7 est possible.

Théorème 2.1.19

Si le corps K est ramifié seulement en 7 alors la seule décomposition possible de l'idéal engendré par 7 dans l'anneau $\mathbb{Z}_K$ est de la forme :

$$7\mathbb{Z}_K = \wp_1^7 \wp_2,$$

où $f_1 = f_2 = 1$.

Preuve :
D'après les résultats qui précédent, on sait que si le corps K est ramifié seulement en 7 alors il l'est sauvagement. La décomposition :

$$7\mathbb{Z}_K = \wp_1^7 \wp_2$$

est alors évidente. □

Théorème 2.1.20

Si le corps K est ramifié seulement en 7 alors le discriminant d_K prend ses valeurs dans l'ensemble suivant :

$$\{7^8, -7^9, 7^{10}, -7^{11}, 7^{12}, -7^{13}\}.$$

Preuve :
Le corps K étant ramifié seulement en 7, on sait qu'il l'est sauvagement. En appliquant la méthode de calcul de Ore, on a $N_{8,7} = 13$. On en déduit $|d_K| \leq 7^{13}$.
Le corps K étant ramifié seulement en 7, on a $d_K = \pm 7^s$ avec $s \in \mathbb{N} - \{0\}$. Comme $7^7 < 1\ 257\ 728 < 7^8$ alors les valeurs possibles de $|d_K| = 7^s$ sont les suivantes :

$$7^8, 7^9, 7^{10}, 7^{11}, 7^{12}, 7^{13}.$$

En utilisant le théorème de Stickelberger ($d_K \equiv 0, 1 \pmod 4$) et le fait que $7 \equiv -1 \pmod 4$ alors on a $d_K \equiv 1 \pmod 4$. Deux cas se présentent en fonction de la parité de s :

1. pour s pair : $d_K = 7^s$.
   En effet, si $d_K = -7^s$ alors $d_K \equiv -1 \pmod 4$, ce qui est impossible .
2. Pour s impair : $d_K = -7^s$.
   En effet, si $d_K = 7^s$ alors $d_K \equiv -1 \pmod 4$, ce qui est impossible. □

Après avoir déterminé les valeurs possibles du discriminants d_K des corps de nombres de degré 8 ramifiés seulement en 7, nous donnons dans les tableaux suivants, les signatures (r_1, r_2) possibles des corps K ramifiés seulement en 7 qui permettent de réaliser les groupes de Galois non résolubles. Nous éliminons certains groupes en utilisant le fait que le discriminant du polynôme générateur f_θ du corps K est un carré (dans $\mathbb{Z} - \{0\}$) si et seulement si le groupe de Galois de f_θ est pair.

$d_K = 7^8$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	**oui**	non	non	non	non
T_{43}	non	non	non	non	non
T_{48}^+	**oui**	non	non	non	non
T_{49}^+	**oui**	non	non	non	non
T_{50}	non	non	non	non	non

$d_K = -7^9$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	non	**oui**	non	non	non

$d_K = 7^{10}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	**oui**	non	non	non	**oui**
T_{43}	non	non	non	non	non
T_{48}^+	**oui**	non	**oui**	non	**oui**
T_{49}^+	**oui**	non	**oui**	non	**oui**
T_{50}	non	non	non	non	non

$d_K = -7^{11}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	non	**oui**	non	**oui**	non

$d_K = 7^{12}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	**oui**	non	non	non	**oui**
T_{43}	non	non	non	non	non
T_{48}^+	**oui**	non	**oui**	non	**oui**
T_{49}^+	**oui**	non	**oui**	non	**oui**
T_{50}	non	non	non	non	non

$d_K = -7^{13}$

$Gal(L/\mathbb{Q})$	$r_1 = 0$	$r_1 = 2$	$r_1 = 4$	$r_1 = 6$	$r_1 = 8$
T_{37}^+	non	non	non	non	non
T_{43}	non	**oui**	non	non	non
T_{48}^+	non	non	non	non	non
T_{49}^+	non	non	non	non	non
T_{50}	non	**oui**	non	**oui**	non

De la même manière qu'en $p = 2$, la recherche des corps de nombres L ramifiés seulement en 7 et de groupe de Galois non résoluble peut se faire en fixant la signature et le discriminant du corps K.

Notre étude dans ce chapitre a permis de montrer que seules les ramifications en $p = 2$, en $p = 5$ de façon inconditionnelle et en $p = 7$ sont possibles.

2.2 Etude de la ramification des corps de degré 9

2.2.1 Les minima des discriminants

Comme dans le cas des corps de degré 8, nous commençons ce paragraphe par le tableau (cf. **[20]**) qui donne les sous-groupes transitifs G de T_{34} qui sont primitifs et, pour chaque possibilité de signature du corps de nombres K, le discriminant minimum en valeur absolue quand il est connu.

G	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_9	493455671296	impossible	impossible	impossible	1870004703089601
T_{14}^+	990677827584	impossible	impossible	impossible	34967472899872522224
T_{15}	218070794717793	impossible	impossible	impossible	17832200896512000000
T_{16}	467288576	2191933899	impossible	impossible	1128762254528
T_{19}	419853238272	204128387072	imossible	impossible	51032096768000000
T_{23}^+	89526025681	impossible	impossible	impossible	51032096768000000
T_{26}	2751651100197	9155562688	impossible	impossible	262 284245009280000
T_{27}^+	4169931445681	impossible	imossible	impossible	inconnu
T_{32}^+	72313663744	impossible	impossible	impossible	inconnu
T_{33}^+	92371321	impossible	3200504329	impossible	11729467378561
T_{34}	29510281	109880167	453771377	2307632671	9685993193

Tableau 7

A la lecture de ce tableau, nous pouvons remarquer que tous les groupes primitifs peuvent être réalisés à partir de corps K totalement réels ou totalement imaginaires. Le groupe T_{34} peut être réalisé à partir de toutes les signatures du corps K.

2.2.2 Ramification en p=2

Proposition 2.2.1
Si le corps K est ramifié seulement en 2, alors il est sauvagement ramifié.

Preuve :
Supposons K modérement ramifié en 2 : la relation (1.5) du théorème 1.6.1 de Ore donne :

$$v_2(d_K) \leq 9 - \sum_{\wp|2} f_\wp \, .$$

D'où $v_2(d_K) \leq 8$.
Le calcul donne alors $|d_K| < 23\ 007\ 468$, ce qui est en contradition avec la minoration du discriminant d'un corps de nombres de degré 9 donnée par Diaz Y Diaz. □

Dans le cas de la ramification en 2, le corps K et sa clôture galoisienne L seraient alors sauvagement ramifiés. Déterminons les différentes décompositions de l'idéal engendré par 2 dans l'anneau $\mathbb{Z}_K$.

Théorème 2.2.2
Si le corps K est ramifié seulement en 2, alors la seule décomposition possible de l'idéal engendré par 2 dans l'anneau $\mathbb{Z}_K$ est : $2\mathbb{Z}_K = \wp_1^8 \wp_2$.

Preuve :
Le corps K étant ramifié seulement en 2 on sait d'après ce qui précède qu'il est sauvagement ramifié. En étudiant parmi les différentes décompositions de

$$2\mathbb{Z}_K = \prod_{\wp|2} \wp^{e_\wp} \quad \text{avec} \quad \sum_{\wp|2} e_\wp f_\wp = 9$$

celles qui donnent la plus grande valeur de $v_2(d_K)$ et en utilisant la minoration du discriminant donnée par Diaz Y Diaz on obtient le résultat. □

Théorème 2.2.3
Si le corps K est ramifié seulement en 2 alors le groupe de Galois $Gal(L/\mathbb{Q})$ ne peut être isomorphe à T_{27}^+ et à T_{32}^+.

Preuve :
Le corps de nombres K étant sauvagement ramifié en 2, alors, d'après la proposition 2.0.2 sa clôture galoisienne L l'est aussi. La plus grande puissance de 2 divisant $|T_{27}^+| = 504$ (resp. $|T_{32}^+| = 1512$) est 8, et donc $v_2(e) \leq 3$, car l'indice de ramification e divise $|Gal(L/\mathbb{Q})|$. La relation (1.5) du théorème 1.6.1 de Ore dans le cas d'une extension galoisienne donne :

$$|d_L|^{1/|Gal(L/\mathbb{Q})|} \leq 2^{1+v_2(e)-1/e}, \text{ c'est-à-dire}$$

$|d_L|^{1/|Gal(L/\mathbb{Q})|} \leq 2^{4-1/|Gal(L/\mathbb{Q})|}$. D'où

$$|d_L|^{1/504} \leq 15.978 \text{ pour } T_{27}^+ \text{ (resp. } |d_L|^{1/1512} \leq 15.993 \text{ pour } T_{32}^+).$$

Or, la table donnant de façon inconditionnelle la minoration de la racine n-ième du discriminant d'un corps de nombres (cf. **[8]**) donne :

$$|d_L|^{1/504} \geq 20.114 \text{ (resp. } |d_L|^{1/1512} \geq 21.253)$$

ce qui contredit les inégalités précédentes. □

Terminons cette partie par les valeurs possibles du discriminant d_K dans le cas où K est ramifié seulement en 2.

Théorème 2.2.4
Si le corps K est ramifié seulement en 2 alors les valeurs possibles prises par le discriminant d_K appartiennent à l'ensemble :

$$\{\pm 2^{25}, \pm 2^{26}, \pm 2^{27}, \pm 2^{28}, \pm 2^{29}, \pm 2^{30}, \pm 2^{31}\}.$$

Preuve :
En calculant la plus grande puissance de 2 divisant d_K par la méthode de Ore, on obtient $N_{8,2} = 31$. Le résultat s'ensuit en utilisant *iii*) du théorème 1.6.1 de Ore donnant les valeurs possibles de $v_2(d_K)$, et en remarquant que $2^{24} < 23\,007\,468 < 2^{25}$. Le théorème de Stickelberger ($d_K \equiv 0, 1 \pmod 4$) ne permet pas ici d'avoir des renseignements supplémentaires sur le signe de d_K. □

Grâce au tableau 2 du paragraphe 1.1 et au tableau 7 du paragraphe 2.2, nous donnons ici pour chaque discriminant d_K possible, les signatures (r_1, r_2) susceptibles de réaliser les groupes de Galois non résolubles dans le cas de la ramification en 2. Comme dans le cas des corps de degré 8, nous éliminons certains groupes en utilisant le fait que le discriminant d_{f_θ} du polynôme générateur f_θ du corps K est un carré (dans $\mathbb{Z} - \{0\}$) si et seulement si le groupe de Galois de f_θ est un sous-groupe de T_{33}^+.

$d_K = \pm 2^{25}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	**oui**	non	non	non	non

$d_K = \pm 2^{26}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	**oui**	non	non	non	non

$d_K = \pm 2^{27}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	**oui**	**oui**	non	non	non

$d_K = \pm 2^{28}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	**oui**	**oui**	non	non	non

$d_K = \pm 2^{29}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	**oui**	**oui**	**oui**	non	non

$d_K = \pm 2^{30}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	**oui**	**oui**	**oui**	non	non

$d_K = \pm 2^{31}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	**oui**	**oui**	**oui**	non	non

2.2.3 Ramification en p=3

Nous commençons cette étude par les différentes décompositions de l'idéal engendré par 3. Des arguments du type de ceux utilisés précédemment dans la proposition 2.2.1 montrent que la ramification en 3 est sauvage. Ceci nous amène au résultat suivant

Théorème 2.2.5
Si le corps K est ramifié seulement en 3, alors les seules décompositions possibles de l'idéal engendré par 3 dans l'anneau $\mathbb{Z}_K$ sont : $3\mathbb{Z}_K = \wp_1^9$ et $3\mathbb{Z}_K = \wp_1^6\wp_2^3$.

Preuve :
Le corps K étant ramifié seulement en 3 on sait d'après ce qui précède qu'il est sauvagement ramifié. En étudiant parmi les différentes décompositions de

$$3\mathbb{Z}_K = \prod_{\wp|3} \wp^{e_\wp} \text{ avec } \sum_{\wp|3} e_\wp f_\wp = 9$$

celles qui donnent la plus grande valeur de $v_3(d_K)$ et en utilisant la minoration du discriminant donnée par Diaz Y Diaz on obtient le résultat. □

Donnons maintenant les différentes valeurs possibles du discrimant d_K dans le cas de la ramification en 3.

Théorème 2.2.6
Si le corps K est ramifié seulement en 3 alors les valeurs possibles prises par le discriminant d_K appartiennent à l'ensemble :

$$\{3^{16}, 3^{18}, -3^{19}, 3^{20}, -3^{21}, 3^{22}, -3^{23}, 3^{24}, -3^{25}, 3^{26}\}.$$

Preuve :
En calculant la plus grande puissance de 3 divisant d_K, on obtient $N_{9,3} = 26$. Le résultat s'ensuit en utilisant ii) du théorème 1.6.1 de Ore donnant les valeurs possibles de $v_3(d_K)$, et en remarquant que $3^{15} < 23\ 007\ 468 < 3^{16}$. Le théorème de Stickelberger ($d_K \equiv 0, 1 \pmod 4$) permet de donner le signe de d_K. □

Remarque :

En tenant compte des corrections locales (la contribution des idéaux premiers de petite norme **[24]**, **[25]**) de façon inconditionnelle, on montre que la décomposition $3\mathbb{Z}_K = \wp_1^6\wp_2^3$ n'est pas possible. De plus on montre aussi que les valeurs $\pm 2^{25}, \pm 2^{26}$ et 3^{16} ne peuvent pas être atteintes par le discriminant d_K.

Nous terminons ce paragraphe par les groupes de Galois non résolubles susceptibles d'être réalisés en fonction de la signature et de la valeur du discriminant.

$d_K = 3^{18}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	non	non	non	non	non

$d_K = -3^{19}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	non	**oui**	non	non	non

$d_K = 3^{20}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	**oui**	non	non
T_{34}	non	non	non	non	non

$d_K = -3^{21}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	non	**oui**	non	**oui**	non

$d_K = 3^{22}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	**oui**
T_{32}^+	non	non	non	non	**oui**
T_{33}^+	**oui**	non	**oui**	non	non
T_{34}	non	non	non	non	non

$d_K = -3^{23}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	non	**oui**	non	**oui**	non

$d_K = 3^{24}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	**oui**
T_{32}^+	**oui**	non	non	non	**oui**
T_{33}^+	**oui**	non	**oui**	non	non
T_{34}	non	non	non	non	non

$d_K = -3^{25}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	non	**oui**	non	non	non

$d_K = 3^{26}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	**oui**
T_{32}^+	**oui**	non	non	non	**oui**
T_{33}^+	**oui**	non	**oui**	non	non
T_{34}	non	non	non	non	non

2.2.4 Ramification en p=5

En utilisant la méthode de Ore décrite dans le paragraphe 1.6 et le fait que $9 = 4 \times 5^0 + 1 \times 5$, on a $N_{9,5} = 4 \times 1 + 1 \times 2 \times 5 - 2 = 12$. On en déduit donc que $|d_K| \leq 5^{12}$. Ce résultat ne permet pas a priori de savoir si la ramification seulement en 5 du corps K est possible. Nous montrerons, en supposant vérifiée l'hypothèse de Riemann généralisée (GRH), que ni le corps L, ni le corps K ne peuvent être ramifiés seulement en 5.

D'abord montrons que la ramification modérée seulement en 5 ne peut être possible pour le corps K et sa clôture galoisienne L.

Proposition 2.2.7
Si le corps K est ramifié seulement en 5 alors il ne peut l'être modérement.

Preuve :
Supposons K modérement ramifié en 5 alors la relation (1.5) du théorème 1.6.1 de Ore donne :

$$v_5(d_K) \leq 9 - \sum_{\wp|5} f_\wp \leq 8.$$

D'où

$$|d_K| \leq 5^8 < 23\ 007\ 468$$

ce qui est impossible car la valeur absolue du discriminant d'un corps de nombres K de degré 9 ne peut vérifier cette inégalité. □

Ce résultat montre bien que si la ramification en 5 du corps K (resp. L) est possible alors elle est sauvage.

Ramification sous GRH :

Commençons par ce lemme qui permet de calculer le cardinal du normalisateur d'un 5-cycle dans le groupe symétrique S_9 (resp. le groupe alterné A_9).

Lemme 2.2.8
Soient G_1 un sous-groupe de S_9 engendré par un 5-cycle et $N_{S_9}(G_1)$ (resp. $N_{A_9}(G_1)$) le normalisateur de G_1 dans S_9 (resp. le groupe alterné A_9). Alors

i) $N_{S_9}(G_1)/G_1 \simeq S_4 \times C_4$

ii) $N_{A_9}(G_1)/G_1 \simeq S_4 \times C_2$.

Proposition 2.2.9
Sous GRH, le corps L ne peut être ramifié seulement en 5.

Preuve :
Si le corps L est ramifié seulement en 5 alors d'après ce qui précède il ne peut être que sauvagement ramifié en 5.

Supposons L sauvagement ramifié en 5 ; le groupe $G = Gal(L/\mathbb{Q})$ est un sous-groupe transitif de T_{34} suivant la notation de Butler et McKay. L'extension $L/\mathbb{Q}$ étant galoisienne on a :

$$5\mathbb{Z}_L = \prod_{i=1}^{g} \mathfrak{P}_i^e,$$

où les $\mathfrak{P}_i$ sont les idéaux premiers de $\mathbb{Z}_L$ au-dessus de 5 avec $|G| = efg$ et 5 divise $|G|$. De plus $v_5(e) = 1$ car 25 ne divise pas $|T_{33}|$. La relation

$$|G| = [L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 9[L : K]$$

montre que 9 divise $|G|$. On en déduit que 45 divise $|G|$ (car $(9, 5) = 1$), et donc $G = T_{34}$ ou T_{33}^+.

Désignons par G_0 le groupe d'inertie et par G_1 le premier groupe de ramification d'un idéal premier $\mathfrak{P}$ de l'anneau $\mathbb{Z}_L$ au-dessus du nombre premier 5. On montre comme dans le cas du degré 8 que G_1 est un 5-cycle. Nous allons étudier séparément le cas où $G = T_{34}$ et celui où $G = T_{33}^+$.

1. Si $G = T_{33}$, on montre d'après le lemme précédent que G_0 est un sous-groupe strict de $N_{T_{33}}(G_1)$ et que $|N_{T_{33}}(G_1)| = 480$. On a donc $e|240$.

2. Si $G = T_{33}^+$, on montre que e divise $|N_{T_{33}^+}(G_1)|$ qui est lui même égal à 240 d'après le lemme 2.2.8.

Dans les deux cas l'indice de ramification e divise 240 et $v_5(e) = 1$. En utilisant la relation (1.5) du théorème 1.6.1 pour une extension galoisienne, on a :

$$v_5(d_L) \leq f(e + e - 1)g = f(2e - 1)g = |G|(2 - 1/e) \; et \frac{1}{240} \leq \frac{1}{e} \leq \frac{1}{5} \; .$$

Comme

$$\frac{9}{5} \leq 2 - \frac{1}{e} \leq \frac{479}{240} \quad ,$$

on en déduit :

$$|d_L|^{1/|G|} \leq 5^{\frac{479}{240}} \approx 24.833.$$

Supposons que l'hypothèse de Riemann généralisée soit vraie pour la fonction zêta de Dedekind du corps L. La relation (1.2) du théorème 1.1.1 donne alors :

$$\frac{1}{|G|}\log|d_L| \geq \left(3.801 - \frac{20.766}{(\log|G|)^2} - \frac{157.914(1+1/|G|)}{(\log|G|)^3\left(1+\frac{\pi^2}{(\log|G|)^2}\right)^2}\right).$$

On obtient donc :
si $G = T_{34}$ alors $|d_L|^{(1/|T_{34}|)} \geq 36.22$
si $G = T_{33}^+$ alors $|d_L|^{(1/|T_{33}^+|)} \geq 35.09$.
Ces deux résultats sont en contradition avec la majoration précédente. □

Corollaire 2.2.10

Sous GRH le corps K ne peut être ramifié seulement en 5.

Ramification sans GRH :

De façon inconditionnelle (sans GRH), on obtient les résultats suivants

Proposition 2.2.11

Si K est ramifié seulement en 5 alors il l'est sauvagement. De plus les différentes décompositions possibles de l'idéal engendré par 5 dans $\mathbb{Z}_K$ sont de la forme :

i) $5\mathbb{Z}_K = \wp_1^5\wp_2^4$ *avec* $f_1 = f_2 = 1$,

ii) $5\mathbb{Z}_K = \wp_1^5\wp_2^3\wp_3$ *avec* $f_1 = f_2 = f_3 = 1$,

iii) $5\mathbb{Z}_K = \wp_1^5\wp_2^2$ *avec* $f_1 = 1$ *et* $f_2 = 2$,

iv) $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3^2$ *avec* $f_1 = f_2 = f_3 = 1$.

Une fois les différentes décompositions primaires obtenues, nous donnons dans ce qui suit les valeurs possibles du discriminant.

Proposition 2.2.12

Si K est ramifié seulement en 5 alors le discriminant d_K appartient à l'ensemble

$$\{5^{11}, 5^{12}\}.$$

Preuve : Le calcul de la plus grande puissance de 5 divisant d_K par la méthode de Ore donne $N_{9,5} = 12$. Le résultat s'ensuit en utilisant le fait que $|d_K| \geq 23\ 007\ 468$. □

Par application du tableau 2 et des résultats du tableau 7, nous donnons ici pour chaque discriminant d_K possible, les signatures (r_1, r_2) susceptibles de réaliser les groupes de Galois non résolubles dans le cas de la ramification sans GRH en $p = 5$.

$d_K = 5^{11}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	**oui**	non	non	non	non

$d_K = 5^{12}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	non	non	non	non	non

2.2.5 Ramification en p=7

Terminons cette étude par le dernier cas de ramification, soit en $p = 7$. Nous donnons aussi comme dans le cas des corps de degré 8, les différentes valeurs possibles du discriminant d_K.

Proposition 2.2.13
Si le corps K est ramifié seulement en 7 alors il est sauvagement ramifié.

Preuve :
Supposons K modérement ramifié en 7 alors la relation (1.5) du théorème 1.6.1 de Ore permet d'écrire :

$$v_7(d_K) \leq 9 - \sum_{\wp|7} f_\wp \leq 8$$

et donc

$$|d_K| \leq 7^8 < 23\ 007\ 468$$

ce qui est impossible car la valeur absolue du discriminant d'un corps de nombres de degré 9 ne peut vérifier cette inégalité. □

Corollaire 2.2.14
Si L est ramifié seulement en 7 alors il est sauvagement ramifié.

Le résultat précédent montre que la ramification en 7 du corps K (resp. du corps L) est sauvage. Voyons comment se décompose l'idéal $7\mathbb{Z}_K$ engendré par le nombre premier 7 dans le cas où la ramification en 7 est possible.

Théorème 2.2.15
Si le corps K est ramifié seulement en 7 alors les seules décompositions possibles de l'idéal engendré par 7 dans l'anneau $\mathbb{Z}_K$ sont de la forme :

i) $7\mathbb{Z}_K = \wp_1^7\wp_2^2$ *où* $f_1 = f_2 = 1$

ii) $7\mathbb{Z}_K = \wp_1^7\wp_2\wp_3$ *où* $f_1 = f_2 = f_3 = 1$

iii) $7\mathbb{Z}_K = \wp_1^7\wp_2$ *où* $f_1 = 1$ *et* $f_2 = 2$.

Preuve :
Elle résulte de $\sum_{\wp|7} e_\wp f_\wp = 9$ avec un $e_\wp = 7$. □

Théorème 2.2.16
Si le corps K est ramifié seulement en 7 alors le discriminant d_K prend ses valeurs dans l'ensemble suivant :

$$\{-7^9, 7^{10}, -7^{11}, 7^{12}, -7^{13}, 7^{14}\}.$$

Preuve :
En appliquant la méthode de calcul de Ore, on a $N_{9,7} = 14$. On en déduit $|d_L| \leq 7^{14}$. Le corps K étant ramifié seulement en 7, on a $d_K = \pm 7^s$ avec $s \in \mathbb{N} - \{0\}$. Comme $7^8 < 23\ 007\ 468 < 7^9$ alors les valeurs possibles de $|d_K| = 7^s$ sont les suivantes :

$$7^9, 7^{10}, 7^{11}, 7^{12}, 7^{14}.$$

Le théorème de Stickelberger permet alors de donner le signe du discriminant . □

Après avoir déterminé les valeurs possibles du discriminants d_K des corps de nombres de degré 9 ramifiés seulement en 7, nous donnons dans les tableaux suivants, les signatures (r_1, r_2) possibles des corps K qui permettent de réaliser les groupes de Galois non résolubles. Nous éliminons certains groupes en utilisant le fait que le discriminant du polynôme générateur f_θ du corps K est un carré (dans $\mathbb{Z} - \{0\}$) si et seulement si le groupe de Galois de f_θ est pair.

$d_K = -7^9$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	non	non	non	non	non

$d_K = 7^{10}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	**oui**	non	non	non	non
T_{34}	non	non	non	non	non

$d_K = -7^{11}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	non	**oui**	non	non	non

$d_K = 7^{12}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	**oui**
T_{32}^+	non	non	non	non	**oui**
T_{33}^+	**oui**	non	**oui**	non	non
T_{34}	non	non	non	non	non

$d_K = -7^{13}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	non
T_{32}^+	non	non	non	non	non
T_{33}^+	non	non	non	non	non
T_{34}	non	**oui**	non	**oui**	non

$d_K = 7^{14}$

$Gal(L/\mathbb{Q})$	$r_1 = 1$	$r_1 = 3$	$r_1 = 5$	$r_1 = 7$	$r_1 = 9$
T_{27}^+	non	non	non	non	**oui**
T_{32}^+	**oui**	non	non	non	**oui**
T_{33}^+	**oui**	non	**oui**	non	non
T_{34}	non	non	non	non	non

L'étude (théorique) faite dans ce chapitre nous a permis de déterminer les différentes ramifications possibles et le cas échéant de donner les valeurs possibles du discriminant. En fixant la valeur du discriminant et la signature du corps K, nous avons pu déterminer les différents groupes de Galois non résolubles qui sont réalisables.

Nous allons dans le chapitre qui suit donner des conditions sur les coefficients des polynômes susceptibles d'engendrer les différents corps obtenus à la suite de l'étude théorique aussi bien en degré 8 que 9.

Chapitre 3

Polynômes définissant les corps

Dans ce chapitre nous allons déterminer les polynômes susceptibles d'engendrer les corps de nombres de degré 8 (resp. de degré 9) vérifiant les différentes ramifications obtenues de façon théorique au chapitre précédent. Il faut rappeler que les groupes de Galois non résolubles dont il est question dans notre étude sont des groupes de Galois de corps K primitifs. Ce résultat simplifie considérablement notre recherche. Dans toute la suite, tous les corps K dont il sera question seront supposés primitifs. Comme l'ont fait la plupart des auteurs ayant étudié le problème de la détermination des discriminants minimaux, nous allons utiliser largement les inégalités obtenues par des méthodes géométriques dans le but de limiter le nombre de polynômes qu'il faut prendre en considération. Nous rappelons d'abord le théorème de Hunter **[8]** qui assure dans le cas de notre étude l'existence d'un élément primitif du corps de nombres K. Ensuite nous utiliserons une version de ce théorème adaptée à ce contexte par Jones et Roberts (cf. **[18]** et **[19]**) dans le cas des corps de nombres primitifs de degré n vérifiant un certain type de ramification. Nous emploierons pour terminer, de façon inconditionnelle, la méthode analytique de minoration de discriminants avec corrections locales d'Odlyzko, Poitou et Serre (cf. **[24]** et **[25]**). Cette utilisation des méthodes analytiques nous conduit à des simplifications importantes dans les calculs.

Suivant les notations de **[1]**, soient :

$\mathcal{P}_1$ l'ensemble fini des nombres premiers ramifiés dans K,

$\mathcal{P}_2$ l'ensemble fini des idéaux premiers de $\mathbb{Z}_K$ au-dessus des éléments de$\mathcal{P}_1$,

et

$$I = \prod_{\wp \in \mathcal{P}_2} \wp.$$

Dans le cas général d'un corps primitif K de degré n, tout élément $\theta \in I \backslash \mathbb{Z}$ a un polynôme minimal f_θ défini par :

$$f_\theta(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + a_3 x^{n-3} + \ldots + a_{n-1} x + a_n, \quad a_k \in \mathbb{Z}.$$

Tout élément $\theta \in I \backslash \mathbb{Z}$ (et donc $\theta \notin \mathbb{Q}$) est un élément primitif du corps K. On peut donc choisir les polynômes générateurs parmi les polynômes irréductibles des éléments $\theta \in I \backslash \mathbb{Z}$.

3.1 Les travaux de Hunter

Les travaux de Hunter permettant la construction de tables de corps de nombres de degré n utilisent l'énoncé suivant (cf. **[8]**) :

Théorème 3.1.1 (Hunter)
Soit K un corps de nombres de degré n et de discriminant d_K. Alors, il existe $\theta \in \mathbb{Z}_K \backslash \mathbb{Z}$ tel que :

$$\sum_{i=1}^{n} |\theta_i|^2 \leq \frac{1}{n}(Tr(\theta))^2 + \gamma_{n-1}\left(\frac{|d_K|}{n}\right)^{1/n-1}$$

où les θ_i sont les conjugués de θ,

$$Tr(\theta) = \sum_{i=1}^{n} \theta_i \ ,$$

et γ_n est la constante d'Hermite en dimension n . On peut imposer à θ la condition supplémentaire :

$$0 \leq Tr(\theta) \leq [\frac{n}{2}].$$

Ce théorème a été généralisé dans le cas imprimitif par J. Martinet (cf. **[8]**).

Théorème 3.1.2 (Martinet)
Soit K un corps de nombres de degré n, extension de degré h d'un sous-corps K' de degré n'. Il existe un élément θ de K, qui n'appartient pas à K', et qui vérifie l'inégalité suivante :

$$\sum_{i=1}^{n} |\theta_i|^2 \leq \frac{1}{h} \sum_{\sigma \in J(K')} |Tr_{\sigma,K/K'}(\theta)|^2 + \gamma_{n-n'} |\frac{d_K}{h^{n'} d_{K'}}|^{1/n-n'}$$

avec $Tr_{\sigma,K/K'}(\theta) = \sum_{t \in J_\sigma(K)} t(\theta)$ où $J_\sigma(K)$ est l'ensemble des $\mathbb{Q}$-homomorphismes de K dans $\mathbb{C}$ qui ont σ pour restriction à K'.

Pour pouvoir calculer une majoration de $\sum_{i=1}^{n} |\theta_i|^2$, il nous faut connaître la valeur de la constante d'Hermite en dimension n. Le tableau suivant donne les différentes valeurs de γ_n pour $n \leq 8$; elles ne sont pas connues pour $n \geq 9$.

n	1	2	3	4	5	6	7	8
γ_n^n	1	4/3	2	4	8	64/3	64	256

Pour les valeurs supérieures de n, on donne une majoration de γ_n (cf. **[8]**) :

$$\gamma_n^n \leq \gamma_{n-1}^{(n-1)n/(n-2)}.$$

Les meilleures majorations connues à partir de cette inégalité sont données pour $n \leq 24$.
Remarque :

L'élément θ donné dans le théorème de Hunter n'est en général pas un élémént primitif lorsque le corps de nombres K est quelconque. Mais dans le cas d'un corps de nombres primitif de degré n, il est bien un élément primitif et le théorème assure son existence. Dans le cas imprimitif, on utilise la version générale du théorème de Hunter.

Notation.

$$\text{Soit } f_\theta(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

le polynôme minimal de θ.
Soit $\mathcal{T}_2$ la forme quadratique définie par :

$$\mathcal{T}_2 = \mathcal{T}_2(\theta) = \sum_{i=1}^{n} |\theta_i|^2, \quad \text{et} \quad S_k = \sum_{i=1}^{n} \theta_i^k,$$

où $k \in \mathbb{Z}$ et les θ_i sont les conjugués de l'élément primitif θ.

Pour mener à bien notre étude, nous utiliserons une version du théorème de Hunter adaptée à ce contexte par les travaux de Jones et Roberts (cf. **[17]**, **[18]** et **[19]**).

3.2 Les travaux de Jones et Roberts

Dans le cas d'un corps de nombres K primitif de degré n, la majoration de $\mathcal{T}_2(\theta)$ donne un nombre fini de valeurs possibles pour les coefficients a_k du polynôme minimal de l'élément θ. Le polynôme f_θ est bien un polynôme générateur du corps de nombres K. Les travaux de Jones et Roberts (1998, 1999) (cf. **[18]** et **[19]**) permettent d'améliorer le théorème de Hunter dans le cas d'un corps de nombres primitif ramifié en un unique premier. Les résultats de leurs travaux sont donnés dans le théorème suivant :

Théorème 3.2.1 (Jones et Roberts 1998, 1999***)***
Soit K un corps de nombres primitif de degré $n \geq 3$, de discriminant d_K, I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus des nombres premiers ramifiés, l le plus petit entier positif non nul de I et m la norme absolue de l'idéal I. Soit γ_n la constante d'Hermite en dimension n. Alors il existe un élément $\theta \in I \backslash \mathbb{Z}$ de polynôme minimal $f_\theta(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ tel que :

i) $\mathcal{T}_2(\theta) \leq \frac{a_1^2}{n} + \gamma_{n-1}\left(\frac{m^2|d_K|}{l^2 n}\right)^{1/n-1}$

ii) $0 \leq a_1 \leq n.l/2$.

Remarque :
En remplaçant I par $\mathbb{Z}_K$, on retrouve les résultats de Hunter. Ce théorème simplifie en particulier celui de Hunter dans la mesure où la recherche des polynômes f_θ se fait pour un élément θ appartenant à un idéal propre de $\mathbb{Z}_K$.

Nous donnerons dans la suite des bornes pour les différents coefficients du polynôme générateur f_θ.

3.3 Bornes des coefficients en degré n

On a les relations de Newton (cf. **[1]**) qui lient les coefficients a_k du polynôme minimal f_θ aux sommes S_k par :

$$S_k + \sum_{i=1}^{k-1} a_i S_{k-i} + k a_k = 0, \quad 1 \leq k \leq n.$$

Avec les notations précédentes, et en posant :

$$U_2 = \frac{1}{n}(Tr(\theta))^2 + \gamma_{n-1}\left(\frac{m^2|d_K|}{l^2 n}\right)^{1/n-1}$$

le majorant de la forme quadratique $\mathcal{T}_2$ dans le théorème 3.2.1 de Jones et Roberts ; on a alors (voir paragraphe 9.3 de **[5]**) :

i) $|a_k| \leq \mathrm{C}_n^k \mathcal{T}_2^{k/2}, \quad 1 \leq k \leq n.$
En effet, le k-ième coefficient a_k est une fonction élémentaire symétrique des θ_i. Or $|\theta_i|^2 \leq \mathcal{T}_2 = \sum_{j=1}^n |\theta_j|^2$ implique que $|\theta_i| \leq \mathcal{T}_2^{1/2}$ pour $1 \leq i \leq n$. Comme

$$a_k = (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \theta_{i_1} \cdots \theta_{i_k},$$

la sommation s'étend sur le nombre de possibilités de prendre k éléments parmi n éléments (tous distincts) et donc $|a_k| \leq \mathrm{C}_n^k \mathcal{T}_2^{k/2}$.

ii) La somme S_k des puissances k-ième des conjugués θ_i de θ est aussi définie pour $k \in \mathbb{Z}$ (car $\theta_i \neq 0$) ; en prenant $k = -1$, on a :

$$S_{-1} = -\frac{a_{n-1}}{a_n}\ .$$

En effet, on a :

$$S_{-1} = \sum_{i=1}^n \theta_i^{-1} = \frac{\sum_{1 \leq i_1 < i_2 \cdots < i_{n-1} \leq n} \theta_{i_1} \cdots \theta_{i_{n-1}}}{\prod_{i=1}^n \theta_i} = \frac{(-1)^{n-1} a_{n-1}}{(-1)^n a_n} = -\frac{a_{n-1}}{a_n}.$$

iii)

$$\left[\prod_{i=1}^n |\theta_i|^2\right]^{1/n} \leq \frac{1}{n}\sum_{i=1}^n |\theta_i|^2.$$

C'est l'inégalité entre la moyenne géométrique de n réels positifs et la moyenne arithmétique.

iv)

$$\frac{a_1^2 - U_2}{2} \leq a_2 \leq \frac{\frac{n-2}{n}a_1^2 + U_2}{2}.$$

En effet :
$|S_2| = |\sum_{i=1}^n \theta_i^2| \leq \mathcal{T}_2 \leq U_2$ et donc $-U_2 \leq -\mathcal{T}_2 \leq S_2 \leq \mathcal{T}_2 \leq U_2$. Comme θ_j est

élément de $\mathbb{C}$, on pose $\theta_j = x_j + iy_j$ avec $x_j, y_j \in \mathbb{R}$. Mais a_1, a_2 et S_2 étant réels ($S_2 = a_1^2 - 2a_2 \in \mathbb{Z}$), on a :

$a_1 = \sum_{j=1}^{n} \theta_j = \sum_{j=1}^{n} x_j + i \sum_{j=1}^{n} y_j = \sum_{j=1}^{n} x_j$;

$\mathcal{T}_2 = \sum_{j=1}^{n} |\theta_j|^2 = \sum_{j=1}^{n} (x_j^2 + y_j^2) = \sum_{j=1}^{n} x_j^2 + \sum_{j=1}^{n} y_j^2$ et

$S_2 = \sum_{j=1}^{n} \theta_j^2 = \sum_{j=1}^{n} (x_j^2 - y_j^2 + 2ix_jy_j) = \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} y_j^2$. Il s'ensuit que

$S_2 + \mathcal{T}_2 = 2\sum_{j=1}^{n} x_j^2 \geq \frac{2}{n}\left(\sum_{j=1}^{n} x_j\right)^2 = \frac{2}{n}a_1^2$ d'après l'inégalité de Cauchy-Schwarz ; car, en prenant

$$\mathbf{U} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad et \quad \mathbf{V} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix},$$

on a : $| < U, V > |^2 \leq (\sum_{i=1}^{n} x_i^2)n$. D'où $\frac{2}{n}a_1^2 - \mathcal{T}_2 \leq S_2 \leq \mathcal{T}_2 \leq U_2$ et $\frac{2}{n}a_1^2 - U_2 \leq S_2 \leq U_2$. En utilisant le fait que $S_2 = a_1^2 - 2a_2$, on a alors $\dfrac{a_1^2 - U_2}{2} \leq a_2 \leq \dfrac{\frac{n-2}{n}a_1^2 + U_2}{2}$.

v) Pour $1 \leq k \leq n$, on a $|S_k| = |\sum_{j=1}^{n} \theta_j^k| \leq \sum_{j=1}^{n} |\theta_j|^k$. En posant $\mathcal{T}_k = \sum_{j=1}^{n} |\theta_j|^k$ on a $-\mathcal{T}_k \leq S_k \leq \mathcal{T}_k$. La relation de Newton $ka_k = -\sum_{i=1}^{k-1} a_i S_{k-i} - S_k$ pour $1 \leq k \leq n$ entraine alors $-\sum_{i=1}^{k-1} a_i S_{k-i} - \mathcal{T}_k \leq ka_k \leq -\sum_{i=1}^{k-1} a_i S_{k-i} + \mathcal{T}_k$, et par suite

$$\frac{-\sum_{i=1}^{k-1} a_i S_{k-i} - \mathcal{T}_k}{k} \leq a_k \leq \frac{-\sum_{j=1}^{k-1} a_i S_{k-i} + \mathcal{T}_k}{k}.$$

Cette inégalité donne un encadrement des coefficients a_k en fonction de $\mathcal{T}_k$ pour $3 \leq k \leq n$. Le lemme suivant (cf. **[5]**) permet de majorer $\mathcal{T}_k$:

Lemme 3.3.1

Soit $n \in \mathbb{N}$ et $x_j \geq 0$ pour $1 \leq j \leq n$, alors pour tout $k \geq 2$ on a :

$$\sum_{j=1}^{n} x_j^k \leq \left(\sum_{j=1}^{n} x_j^2\right)^{k/2}.$$

Preuve : On raisonne par récurrence sur n.

Pour $n = 1$ la proposition est vraie. Pour $n = 2$: $\quad x_1^k + x_2^k \leq (x_1^2 + x_2^2)^{k/2}$ (car pour tout $a \geq 0$ la fonction $f(x) = (x^2 + a^2)^{k/2} - (x^k + a^k)$, pour $x \geq 0$, est une fonction croissante et $f(0) = 0$).

Supposons la vraie jusqu'à l'ordre $n-1$; c'est-à-dire : $\sum_{j=1}^{n-1} x_j^k \leq (\sum_{j=1}^{n-1} x_j^2)^{k/2}$;

alors

$$\sum_{j=1}^{n} x_j^k = \sum_{j=1}^{n-1} x_j^k + x_n^k \leq x_n^k + (\sum_{j=1}^{n-1} x_j^2)^{k/2} = x_n^k + \left[\left(\sum_{j=1}^{n-1} x_j^2\right)^{1/2}\right]^k \leq \left[x_n^2 + \left[\left(\sum_{j=1}^{n-1} x_j^2\right)^{1/2}\right]^2\right]^{k/2}$$

et donc

$$\sum_{j=1}^{n} x_j^k \leq \left[x_n^2 + \sum_{j=1}^{n-1} x_j^2\right]^{k/2} = \left(\sum_{j=1}^{n} x_j^2\right)^{k/2}. \ \square$$

vi) D'après le lemme précédent, on a donc $\sum_{j=1}^{n} |\theta_j|^k \leq \left[\sum_{j=1}^{n} |\theta_j|^2\right]^{k/2}$ ou encore $\mathcal{T}_k \leq \mathcal{T}_2^{k/2} \leq U_2^{k/2}$. On en déduit que $|S_k| \leq \mathcal{T}_k \leq U_2^{k/2}$. En utilisant l'inégalité précédente, on a

$$\frac{-\sum_{i=1}^{k-1} a_i S_{k-i} - U_2^{k/2}}{k} \leq a_k \leq \frac{-\sum_{i=1}^{k-1} a_i S_{k-i} + U_2^{k/2}}{k}.$$

En particulier pour $k = 3$ on a :

$$\frac{-a_1^3 + 3a_1a_2 - U_2^{3/2}}{3} \leq a_3 \leq \frac{-a_1^3 + 3a_1a_2 + U_2^{3/2}}{3}.$$

vii) A partir des inégalités entre moyennes arithmétique et géométrique on en déduit :

$$1 \leq |a_n|^2 \leq \left(\frac{\mathcal{T}_2}{n}\right)^n.$$

En effet, le polynôme f_θ est irréductible dans $\mathbb{Z}[x]$; donc le coefficient a_n est non nul et l'inégalité *iii*) permet d'écrire

$$|a_n|^{2/n} = \left[\prod_{j=1}^{n} |\theta_j|^2\right]^{1/n} \leq \frac{1}{n}\sum_{j=1}^{n} |\theta_j|^2 = \frac{\mathcal{T}_2}{n}.$$

D'où $1 \leq |a_n|^2 \leq \left(\frac{\mathcal{T}_2}{n}\right)^n$.

viii)

$$1 \leq |a_n| \leq \left(\frac{\mathcal{T}_2}{n}\right)^{n/2} \leq \left(\frac{U_2}{n}\right)^{n/2}.$$

Remarque :
La borne U_2 de la forme quadratique $\mathcal{T}_2$ donnée dans le théorème 3.2.1 permet de réduire l'ensemble des polynômes à prendre en considération. Nous pouvons donner de meilleures bornes pour les coefficients a_k du polynôme f_θ. Cette amélioration des bornes est discutée dans les paragraphes suivants grâce aux exposants de Newton-Ore et aux bornes de M. Pohst (cf. **[23]**) pour les fonctions $\mathcal{T}_k(\theta) = \sum_{i=0}^{n} |\theta_i|^k$ pour $k \in \mathbb{Z} - \{0, 2\}$.

3.4 Exposants de Newton-Ore

Une méthode pour obtenir un polynôme générateur d'un corps de nombres de discriminant $\pm p^\alpha$ avec $\alpha \in \mathbb{N} - \{0\}$ et p un nombre premier, consiste en l'utilisation de la

méthode des exposants de Newton-Ore. Elle permet d'obtenir à isomorphisme près des polynômes générateurs, si le corps existe.

Définition 3.4.1
L'exposant de Newton-Ore (cf. **[1]** *et* **[19]**) *en p du coefficient a_i $(1 \leq i \leq n)$ du polynôme $f_\theta(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$, est la plus petite valuation en p du coefficient a_i de tous les polynômes f_θ (avec $\theta \in I\backslash\mathbb{Z}$) susceptibles d'engendrer le corps de nombres K de degré n, et dont p divise tous les coefficients $a_1, a_2, \cdots, a_{n-1}$ et a_n.*

Remarque :
Cette définition a bien un sens dans la mesure où le nombre premier ramifié p divise tous les coefficients a_i du polynôme minimal f_θ de l'élément $\theta \in I\backslash\mathbb{Z}$. La méthode des exposants de Newton-Ore s'applique bien aux corps de nombres primitifs qui sont ramifiés en un unique premier p. Le polynôme générateur étant un polynôme unitaire, on impose la condition que p divise tous les coefficients a_i $(1 \leq i \leq n)$. Le discriminant du corps étant de la forme $\pm p^\alpha$, pour chaque valeur de α fixée, on détermine la plus petite valuation en p pour chaque coefficient a_i de telle sorte que p^α divise le discriminant du polynôme. La détermination des exposants de Newton-Ore de chaque coefficient a_i du polynôme générateur f_θ assure que le discriminant du corps de rupture K est une puissance de p.

Donnons maintenant une méthode très efficace permettant de calculer les exposants de Newton-Ore pour les coefficients a_i. On obtient des résultats analogues pour les sommes S_k des puissances k-ième des conjugués de θ en utilisant les relations de Newton : $S_k + \sum_{i=1}^{k-1} a_i S_{k-i} + ka_k = 0$.

Remarquons que p divise le terme constant a_n pour tout polynôme f_θ.
En effet :

$$a_n = \prod_{i=1}^{n} \theta_i = N_{K/\mathbb{Q}}(\theta)$$

on a alors

$$\frac{a_n}{\theta} = \prod_{\theta_i \neq \theta} \theta_i \in \overline{\mathbb{Z}} \cap K = \mathbb{Z}_K$$

et par suite $a_n \in I$ car I est un idéal de $\mathbb{Z}_K$ contenant θ.
D'où

$$a_n \in \mathbb{Z} \cap I = p\mathbb{Z}.$$

On montre par exemple que dans le cas de la ramification en 2

$$a_n \in \mathbb{Z} \cap I = 2\mathbb{Z}.$$

On obtient un résultat analogue dans le cas où $p = 3, 5$ et 7. Le nombre premier p divise aussi les autres coefficients $a_1, \cdots, a_{n-1}$. En effet soient I_i le produit des idéaux premiers de $K_i = \mathbb{Q}(\theta_i)$ au-dessus des nombres premiers ramifiés (avec $\theta_i \in I_i\backslash\mathbb{Z}$) et $I' = \prod \mathfrak{P}$ où le produit s'étend aux idéaux premiers de L au-dessus des nombres premiers ramifiés dans K_i ; pour tout $i = 1, \cdots, n$ on a $I' \cap K_i = I_i$, et donc $I' \cap \mathbb{Z} = I \cap \mathbb{Z} = p\mathbb{Z}$. Comme I' est un idéal de L et que $\theta_k \in I'$ pour tout k alors pour tout $j = 1, \cdots, n-1$

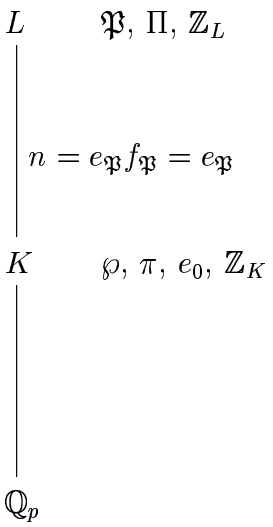
on a $a_j \in I' \cap \mathbb{Z} = p\mathbb{Z}$; d'où le résultat.
La détermination des exposants de Newton-Ore des coefficients de f_θ résulte des travaux de Ore (cf. **[30]** et **[31]**) sur la détermination des valeurs possibles de la valuation $v_p(d_K)$ d'un corps de nombres K de degré n.

Méthode de Ore :
Soit K un corps de nombres (ou une extension finie d'un corps p-adique $\mathbb{Q}_p$), soit n un entier, L/K une extension de degré n de K et $\wp$ un idéal premier non nul de K. L'exposant $v_\wp(\delta(L/K))$ de $\wp$ dans le discriminant relatif $\delta(L/K)$ d'une extension L/K ne peut prendre qu'un nombre fini de valeurs dont on peut dresser la liste en fonction de la caractéristique résiduelle p de $\wp$, du degré n, et de l'indice absolu de ramification e_0 de $\wp$. Cela résulte des travaux de Ore et de Thompson (cf. **[30]** et **[31]**).
Voici le principe de Ore :
On commence par étudier le cas local totalement ramifié. Une uniformisante Π de L est racine d'un polynôme d'Eisenstein $f(x) \in K[x]$:

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + \pi, \quad \text{où } a_i \in \wp \text{ et } \pi \text{ est une uniformisante de } K.$$

La valuation dans K du discriminant de L/K est égale à la valuation dans L de la différente de L/K, qui est engendrée par

$$f'(\Pi) = n\Pi^{n-1} + (n-1)a_1\Pi^{n-2} + \ldots + a_{n-1}.$$



Il faut remarquer que l'indice de ramification de $\wp$ dans K appelé ici indice absolu de ramification de $\wp$, est noté e_0 au lieu de $e_\wp$. On a : $p\mathbb{Z}_K = \wp^{e_0}$, $p\mathbb{Z}_L = \mathfrak{P}^{e_0 e_\mathfrak{P}} = \mathfrak{P}^{ne_0}$ et $\wp\mathbb{Z}_L = \mathfrak{P}^{e_\mathfrak{P}} = \mathfrak{P}^n$. On en déduit donc que $v_\mathfrak{P}(p) = ne_0$.
Comme L est totalement ramifié (extension du corps local K), $L = K(\Pi)$. On a $v_\wp(\pi) = 1$ et $v_\mathfrak{P}(\Pi) = 1$. De plus $v_\mathfrak{P}(\pi) = e_\mathfrak{P} v_\wp(\pi) = e_\mathfrak{P} = n$ et $v_\mathfrak{P}(\Pi) = nv_\wp(\Pi) = 1$; ce qui permet d'en déduire que $v_\wp(\Pi) = \frac{1}{n}$.

La différente $\mathcal{D}(L/K)$ est un idéal entier de L et donc $\mathcal{D}(L/K) = \mathfrak{P}^{n_\mathfrak{P}}$ pour un certain entier $n_\mathfrak{P}$ car il n'y a qu'un seul idéal premier $\mathfrak{P}$ dans L. Le discriminant $\delta(L/K)$ est un idéal entier de K et s'écrit donc $\delta(L/K) = \wp^{n_\wp}$ pour un certain entier $n_\wp$. On a $\delta(L/K) =$

$N_{L/K}(\mathcal{D}(L/K))$ et donc $N_{L/K}(\mathcal{D}(L/K)) = N_{L/K}(\mathfrak{P}^{n_\mathfrak{P}}) = \wp^{f_\mathfrak{P} n_\mathfrak{P}} = \wp^{n_\mathfrak{P}}$, car L/K est totalement ramifiée. D'où $v_\wp(\delta(L/K)) = v_\wp(N_{L/K}(\mathcal{D}(L/K))) = n_\mathfrak{P} = v_\mathfrak{P}(\mathcal{D}(L/K))$.
Les différents termes de la somme $f'(\Pi) = n\Pi^{n-1} + (n-1)a_1\Pi^{n-2} + \ldots + a_{n-1}$ ont des valuations dans L deux à deux incongrues modulo n, si bien que la valuation cherchée est la valeur minimum des valuations des différents termes ci-dessus car l'on a :

$$v_\mathfrak{P}(n\Pi^{n-1}) = v_\mathfrak{P}(n) + (n-1) = ne_0 v_p(n) + (n-1) \equiv n-1 \ (mod\, n)$$

$$v_\mathfrak{P}((n-1)a_1\Pi^{n-2}) = v_\mathfrak{P}(n-1)+v_\mathfrak{P}(a_1)+(n-2) = ne_0 v_p(n-1)+nv_\wp(a_1)+(n-2) \equiv n-2 \ (mod\, n)$$

$$\vdots$$

$$v_\mathfrak{P}((n-i)a_i\Pi^{n-i-1}) = v_\mathfrak{P}(n-i)+v_\mathfrak{P}(a_i)+(n-i-1) = ne_0 v_p(n-i)+nv_\wp(a_i)+(n-i-1) \equiv n-i-1 \ (mod\, n)$$

$$\vdots$$

$$v_\mathfrak{P}(a_{n-1}) = nv_\wp(a_{n-1}) \equiv 0 \ (mod\, n).$$

D'où la valuation $n_\mathfrak{P}$ cherchée est le minimum des valuations des différents termes. On trouve ainsi (cf. **[21]**) une liste de valeurs possibles pour $v_\wp(\delta(L/K)$, qui se présentent toutes effectivement. La plus petite est n, ou $n-1$, que l'on obtient par exemple pour le polynôme :

$$x^n + \pi x + \pi$$

car $v_\mathfrak{P}(f'(\Pi)) = \text{Min}\{nv_p(n) + n - 1, n\}$ qui donne le résultat selon que p divise ou non n. La plus grande valuation est $nv_\wp(n) + n - 1$, que l'on obtient par exemple pour le polynôme :

$$x^n - \pi$$

car $v_\mathfrak{P}(f'(\Pi)) = nv_p(n) + n - 1$.

On passe au cas local général en écrivant L comme extension totalement ramifiée d'une extension K non ramifiée, puis on globalise en approchant par le théorème d'approximation un produit de polynômes de $K_\wp[x]$ par un polynôme de $K[x]$ dont on peut assurer l'irréductibilité en lui imposant d'être un polynôme d'Eisenstein en un idéal premier autre que $\wp$; le théorème d'approximation montre également que l'on peut imposer le nombre de places réelles de K ramifiées dans L.

Remarque :
Dans le cas d'un corps de nombres de degré n, l'indice de ramification absolue e_0 vaut 1. Appliquons les résultats précédents aux corps de nombres de degré 8 (resp. 9) ramifiés en un unique premier p.

3.4.1 Applications au cas $n = 8$

Le cas totalement ramifié :

Dans le cas d'un corps de nombres de degré 8 totalement ramifié en p on a :

$$f_\theta(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_5x^3 + a_6x^2 + a_7x + a_8 \text{ avec } a_i \in \mathbb{Z}.$$

$$f'_\theta(\Pi) = 8\Pi^7 + 7a_1\Pi^6 + 6a_2\Pi^5 + 5a_3\Pi^4 + 4a_4\Pi^3 + 3a_5\Pi^2 + 2a_6\Pi + a_7.$$

D'où la valuation $v_p(d_K)$ est donnée par

$$v_p(d_K) = \text{Min}\{8v_p(8) + 7, 8v_p(7) + 8v_p(a_1) + 6, 8v_p(6) + 8v_p(a_2) + 5, 8v_p(5) + 8v_p(a_3) + 4, 8v_p(4) + 8v_p(a_4) + 3, 8v_p(3) + 8v_p(a_5) + 2, 8v_p(2) + 8v_p(a_6) + 1, 8v_p(a_7)\}.$$

A partir de la relation

$$8v_p(8-i) + 8v_p(a_i) + 8 - i - 1 \geq v_p(d_K) \quad \text{avec} \quad 1 \leq i \leq 7,$$

on obtient les différents exposants de Newton-Ore des coefficients a_i $(1 \leq i \leq 8)$ et des sommes S_i $(1 \leq i \leq 7)$ qui sont consignés dans les tableaux suivants.

$2\mathbb{Z}_K = \wp^8$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$\pm 2^{31}$	4	3	4	2	4	3	4	1	4	3	4	2	4	3	4
$\pm 2^{30}$	3	3	4	2	4	3	4	1	3	3	4	2	4	3	4
$\pm 2^{29}$	3	2	4	2	4	3	4	1	3	2	4	2	4	3	4
$\pm 2^{28}$	3	2	3	2	4	3	4	1	3	2	4	2	4	3	4
$\pm 2^{27}$	3	2	3	1	4	3	4	1	3	2	3	1	4	3	4
$\pm 2^{26}$	3	2	3	1	3	3	4	1	3	2	3	1	3	3	4
$\pm 2^{25}$	3	2	3	1	3	2	4	1	3	2	3	1	3	2	4
$\pm 2^{24}$	3	2	3	1	3	2	3	1	3	2	3	1	3	2	3
$\pm 2^{22}$	2	2	3	1	3	2	3	1	2	2	3	1	3	2	3
$\pm 2^{21}$	2	1	3	1	3	2	3	1	2	1	3	1	3	2	3

Autres cas :

1. Si tous les degrés résiduels $f_\wp$ sont égaux à 1 :
   Dans le cas où le corps de nombres n'est pas totalement ramifié en p et que tous les degrés résiduels sont égaux à 1, on utilise une méthode décrite par Jones et Roberts. Tout d'abord, on a la décomposition suivante : $p\mathbb{Z}_K = \prod_{i=1}^{l} \wp_i{}^{e_i}$ où les $\wp_{i\,(1\leq i\leq l)}$ sont les idéaux premiers de $\mathbb{Z}_K$ au-dessus de p, d'indice de ramification e_i et de degré résiduel $f_{\wp_i} = 1$. On écrit alors $f_\theta = \prod_{i=1}^{l} f_{\theta_i}$ suivant la décomposition primaire donnée, où les $f_{\theta_{i\,(1\leq i\leq l)}}$ sont des polynômes d'Eisenstein de degré respectif e_i engendrant respectivement les corps $K_1, \ldots, K_l$ totalement ramifiés. On note c_i les valuations respectives $v_p(d_{K_i})$ avec $(1 \leq i \leq l)$. En utilisant la méthode décrite dans le cas totalement ramifié, on détermine les exposants de Newton-Ore des coefficients des différents polynômes f_{θ_i}. La valuation $v_p(d_K)$ est donnée par $\sum_{i=1}^{l} c_i$ et on détermine alors les exposants de Newton-Ore de f_θ à partir du produit $\prod_{i=1}^{l} f_{\theta_i}$. En fonction des différentes décompositions primaires, nous donnons les exposants de Newton-Ore dans les exemples qui suivent.

Exemple 1. Cas de la décomposition primaire $2\mathbb{Z}_K = \wp_1^4\wp_2^4$.

On écrit f_θ comme produit de deux polynômes d'Eisenstein f_{θ_1} et f_{θ_2} qui sont respectivement des polynômes générateurs des corps K_1 et K_2 totalement ramifiés de degré 4 suivant la décomposition primaire donnée. En notant c_1 la valuation $v_2(d_{K_1})$ et c_2 la valuation $v_2(d_{K_2})$, on détermine facilement les exposants de Newton-Ore des polynômes f_{θ_1} et f_{θ_2}. La valuation $v_2(d_K)$ est donnée par $c_1 + c_2$ et on détermine alors les exposants de Newton-Ore de f_θ à partir du produit de f_{θ_1} et f_{θ_2}. Les valeurs possibles du discriminant d_K sont $\pm 2^{21}$ et $\pm 2^{22}$.

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$\pm 2^{22}$	3	2	3	1	4	3	4	2	3	2	3	1	4	3	4
$\pm 2^{21}$	2	2	3	1	3	3	4	2	2	2	3	1	3	3	4

Exemple 2. Cas de la décomposition primaire $5\mathbb{Z}_K = \wp_1^5\wp_2^3$.

On écrit f_θ comme produit de deux polynômes d'Eisenstein f_{θ_1} et f_{θ_2} qui sont respectivement des polynômes générateurs des corps K_1 et K_2 totalement ramifiés de degré respectif 5 et 3 suivant la décomposition primaire donnée.

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
5^9	1	1	1	2	1	2	2	2	1	1	1	2	1	2	2
5^{10}	1	1	1	2	1	2	2	2	1	1	1	2	1	2	2
5^{11}	1	1	1	2	1	2	2	2	1	1	1	2	1	2	2

Exemple 3. Cas de la décomposition primaire $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3$.

On écrit f_θ comme produit de trois polynômes d'Eisenstein f_{θ_1}, f_{θ_2} et f_{θ_3} qui sont respectivement des polynômes générateurs des corps K_1, K_2 et K_3 totalement ramifiés de degré respectif 5, 2 et 1 suivant la décomposition primaire donnée. Les valeurs possibles du discriminant d_K sont 5^9 et 5^{10}.

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
5^9	1	1	2	2	1	2	2	3	1	1	2	2	1	2	2
5^{10}	1	1	2	2	1	2	2	3	1	1	2	2	1	2	2

Exemple 4. Cas de la décomposition primaire $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3\wp_4$.

On écrit f_θ comme produit de quatre polynômes d'Eisenstein f_{θ_1}, f_{θ_2}, f_{θ_3} et f_{θ_4} qui sont respectivement des polynômes générateurs des corps K_1, K_2, K_3 et K_4 totalement ramifiés de degré respectif 5, 1, 1 et 1 suivant la décomposition primaire donnée. La seule valeur possible du discriminanat d_K est 5^9.

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
5^9	1	2	2	2	1	2	3	4	1	2	2	2	1	2	3

Exemple 5. Cas de la décomposition primaire $7\mathbb{Z}_K = \wp_1^7\wp_2$.

On écrit f_θ comme produit de deux polynômes d'Eisenstein f_{θ_1} et f_{θ_2} qui sont respectivement des polynômes générateurs des corps K_1 et K_2 totalement ramifiés de degré respectif 7 et 1 suivant la décomposition primaire donnée.

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
-7^{13}	1	1	2	2	2	2	2	1	1	1	2	2	2	2	2
7^{12}	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
-7^{11}	1	1	1	1	2	2	2	1	1	1	1	1	2	2	2
7^{10}	1	1	1	1	1	2	2	1	1	1	1	1	1	2	2
-7^9	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2
$\pm 7^8$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

2. Si l'un des degrés résiduels est tel que $f_{\wp i} > 1$:
Dans le cas où un degré résiduel $f_{\wp_i}$ est supérieur ou égal à 2 et que l'indice de ramification est $e_{\wp i}$ dans la décomposition primaire donnée, on écrit ce corps K_i comme produit de corps K_{i_j} $(1 \leq j \leq f_{\wp i})$ totalement ramifiés de degré $e_{\wp i}$ sur le corps d'inertie $K_i^{G_0}$ (i.e formé des invariants par le groupe d'inertie G_0). On se ramène alors au cas précédent.

Exemple 6. Cas de la décomposition primaire $2\mathbb{Z}_K = \wp_1^4$ où le degré résiduel $f_\wp$ vaut 2. On prend θ_1 le générateur du corps K_1 sur le corps d'inertie K^{G_0} et f_{θ_1} son polynôme minimal sur ledit corps. On considère ensuite les conjugués de f_{θ_1} par les prolongements des isomorphismes de K^{G_0} dans une clôture algébrique. Dans le cas présent, il n'y a qu'un seul conjugué de f_{θ_1} qu'on note f_{θ_2}. On écrit $f_\theta = \prod_{i=1}^2 f_{\theta_i}$ où les f_{θ_i} sont des polynômes d'Eisenstein de degré 4. On se ramène alors au cas précédent.

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$\pm 2^{22}$	3	2	3	1	4	3	4	2	3	2	3	1	4	3	4
$\pm 2^{21}$	2	2	3	1	3	3	4	2	2	2	3	1	3	3	4

Exemple 7. Cas de la décomposition primaire $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3$ où le degré résiduel $f_{\wp_3}$ vaut 2 et $5\mathbb{Z}_K = \wp_1^5\wp_2$ où le degré résiduel $f_{\wp_2}$ vaut 3.

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	S_1	S_2	S_3	S_4	S_5	S_6	S_7
5^9	1	2	2	2	1	2	3	4	1	2	2	2	1	2	3

3.4.2 Applications au cas $n = 9$

Le cas totalement ramifié :

Dans le cas d'un corps de nombres de degré 9 totalement ramifié en p on a :

$$f_\theta(x) = x^9 + a_1x^8 + a_2x^7 + a_3x^6 + a_4x^5 + a_5x^4 + a_6x^3 + a_7x^2 + a_8x + a_9 \text{ avec } a_i \in \mathbb{Z}.$$

$$f'_\theta(\Pi) = 9\Pi^8 + 8a_1\Pi^7 + 7a_2\Pi^6 + 6a_3\Pi^5 + 5a_4\Pi^4 + 4a_5\Pi^3 + 3a_6\Pi^2 + 2a_7\Pi + a_8.$$

D'où

$$v_p(d_K) = Min\{9v_p(9) + 8, 9v_p(8) + 9v_p(a_1) + 7, 9v_p(7) + 9v_p(a_2) + 6, 9v_p(6) + 9v_p(a_3) + 5, 9v_p(5) + 9v_p(a_4) + 4, 9v_p(4) + 9v_p(a_5) + 3, 9v_p(3) + 9v_p(a_6) + 2, 9v_p(2) + 9v_p(a_7) + 1, 9v_p(a_8)\}.$$

A partir de la relation

$$9v_p(9-i)+9v_p(a_i)+9-i-1 \geq v_p(d_K) \quad \text{avec} \quad 1 \leq i \leq 8,$$

on obtient les différents exposants de Newton-Ore des coefficients a_i $(1 \leq i \leq 8)$ et des sommes S_i qui sont consignés dans les tableaux suivants.

$3\mathbb{Z}_K = \wp^9$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
3^{26}	3	3	2	3	3	2	3	3	1	3	3	2	3	3	2	3	3
-3^{25}	2	3	2	3	3	2	3	3	1	2	3	2	3	3	2	3	3
3^{24}	2	2	2	3	3	2	3	3	1	2	2	2	3	3	2	3	3
-3^{23}	2	2	1	3	3	2	3	3	1	2	2	1	3	3	2	3	3
3^{22}	2	2	1	2	3	2	3	3	1	2	2	1	2	3	2	3	3
-3^{21}	2	2	1	2	2	2	3	3	1	2	2	1	2	2	2	3	3
3^{20}	2	2	1	2	2	1	3	3	1	2	2	1	2	2	1	3	3
-3^{19}	2	2	1	2	2	1	2	3	1	2	2	1	2	2	1	3	3
3^{18}	2	2	1	2	2	1	2	2	1	2	2	1	2	2	1	2	2

Autres cas :

1. Si tous les degrés résiduels sont égaux à 1 :
   Exemple 1. Il n'y a qu'une décomposition possible dans le cas de la ramification en 2 : $2\mathbb{Z}_K = \wp_1^8\wp_2$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
$\pm 2^{31}$	1	3	4	2	3	3	4	1	2	1	3	4	2	3	3	4	1
$\pm 2^{30}$	1	3	4	2	3	3	4	1	2	1	3	4	2	3	3	4	1
$\pm 2^{29}$	1	2	3	2	3	3	4	1	2	1	2	3	2	3	3	4	1
$\pm 2^{28}$	1	2	3	2	3	3	4	1	2	1	2	3	2	3	3	4	1
$\pm 2^{27}$	1	2	3	1	2	3	4	1	2	1	2	3	1	2	3	4	1

Exemple 2. Cas de la décomposition $5\mathbb{Z}_K = \wp_1^5\wp_2^4$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
5^{11}	1	1	1	1	1	2	2	2	2	1	1	1	1	1	2	2	2
5^{12}	1	1	1	1	1	2	2	2	2	1	1	1	1	1	2	2	2

Exemple 3. Cas où $5\mathbb{Z}_K = \wp_1^5\wp_2^3\wp_3$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
5^{11}	1	1	1	2	1	2	2	2	3	1	1	1	2	1	2	2	2

Exemple 4. Cas où $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3^2$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
5^{11}	1	1	2	2	1	2	2	3	3	1	1	2	2	1	2	2	3

Exemple 5. Cas où $7\mathbb{Z}_K = \wp_1^7\wp_2^2$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
7^{14}	1	1	2	2	2	2	1	2	2	1	1	2	2	2	2	1	2
-7^{13}	1	1	2	2	2	2	1	2	2	1	1	2	2	2	2	1	2
7^{12}	1	1	2	2	2	2	1	2	2	1	1	2	2	2	2	1	2
-7^{11}	1	1	1	2	2	2	1	2	2	1	1	1	2	2	2	1	2
7^{10}	1	1	1	1	2	2	1	2	2	1	1	1	1	2	2	1	2
-7^9	1	1	1	1	1	2	1	2	2	1	1	1	1	1	2	1	2

Exemple 6. Cas où $7\mathbb{Z}_K = \wp_1^7\wp_2\wp_3$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
-7^{13}	1	2	2	2	2	2	1	2	3	1	2	2	2	2	2	1	2
7^{12}	1	2	2	2	2	2	1	2	3	1	2	2	2	2	2	1	2
-7^{11}	1	1	2	2	2	2	1	2	3	1	1	2	2	2	2	1	2
7^{10}	1	1	1	2	2	2	1	2	3	1	1	1	2	2	2	1	2
-7^9	1	1	1	1	2	2	1	2	3	1	1	1	1	2	2	1	2

2. Si l'un des degrés résiduels $f_{\wp_i} > 1$:
Exemple 7. Cas où $5\mathbb{Z}_K = \wp_1^5\wp_2^2$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
5^{11}	1	1	2	2	1	2	2	3	3	1	1	2	2	1	2	2	3

Exemple 8. Cas où $7\mathbb{Z}_K = \wp_1^7\wp_2$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
-7^{13}	1	2	2	2	2	2	1	2	3	1	2	2	2	2	2	1	2
7^{12}	1	2	2	2	2	2	1	2	3	1	2	2	2	2	2	1	2
-7^{11}	1	1	2	2	2	2	1	2	3	1	1	2	2	2	2	1	2
7^{10}	1	1	1	2	2	2	1	2	3	1	1	1	2	2	2	1	2
-7^9	1	1	1	1	2	2	1	2	3	1	1	1	1	2	2	1	2

Dans cette partie nous allons donner de meilleures bornes pour les coefficients des polynômes générateurs f_θ des corps de nombres K en utilisant les exposants de Newton-Ore et les bornes de M. Pohst pour les fonctions $\mathcal{T}_k$. Dans toute la suite nous utiliserons donc le théorème de Jones et Roberts pour donner des bornes pour les coefficients des polynômes f_θ.

3.5 Amélioration des bornes des coefficients de f_θ en degré 8

On pose :

$$f_\theta(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_5x^3 + a_6x^2 + a_7x + a_8$$

le polynôme minimal de l'élément primitif θ en degré 8.

$$\text{Soit } \mathcal{T}_2 = \mathcal{T}_2(\theta) = \sum_{i=1}^{8} |\theta_i|^2 \text{ et } U_2 = \frac{1}{8}(Tr(\theta))^2 + \gamma_7\left(\frac{m^2|d_K|}{8l^2}\right)^{1/7}$$

où les θ_i désignent les conjugués de θ, et $S_k = \sum_{i=1}^{8} \theta_i^k$ avec $k \in \mathbb{Z}$.

En appliquant les résultats du paragraphe 3.3 au cas $n = 8$, on obtient :

i) $|a_k| \leq C_8^k {U_2}^{k/2} \quad 1 \leq k \leq 8.$

ii) $\dfrac{a_1^2 - U_2}{2} \leq a_2 \leq \dfrac{\frac{3}{4}a_1^2 + U_2}{2}.$

iii) En posant $\mathcal{T}_k = \sum_{j=1}^{8} |\theta_j|^k$ on a
$\dfrac{-\sum_{i=1}^{k-1} a_i S_{k-i} - \mathcal{T}_k}{k} \leq a_k \leq \dfrac{-\sum_{j=1}^{k-1} a_i S_{k-i} + \mathcal{T}_k}{k}.$
Cette inégalité donne un encadrement par récurrence des coefficients a_k en fonction de $\mathcal{T}_k$ pour $3 \leq k \leq 8$.

iv) En prenant $k = -1$ dans la somme S_k des puissances k-ième des θ_i, on a

$$S_{-1} = -\frac{a_7}{a_8}.$$

v) A partir des inégalités entre moyennes arithmétique et géométrique on déduit :

$$1 \leq |a_8| \leq \left(\frac{\mathcal{T}_2}{8}\right)^4 \leq \left(\frac{U_2}{8}\right)^4.$$

3.5.1 Utilisation du théorème de Jones et Roberts

Le cas de la ramification en $p = 2$:

Nous avons vu dans le chapitre précédent que la ramification en $p = 2$ du corps primitif K de degré 8 est sauvage . D'après le théorème 2.1.4, les seules décompositions possibles de l'idéal engendré par 2 dans $\mathbb{Z}_K$ sont $2\mathbb{Z}_K = \wp^8$, $2\mathbb{Z}_K = \wp^4$ et $2\mathbb{Z}_K = \wp_1^4\wp_2^4$.

Nous allons donc déterminer le polynôme générateur en fonction des décompositions ci-dessus. On en déduit le corollaire suivant du théorème de Jones et Roberts :

Corollaire 3.5.1

Soit K un corps de nombres primitif de degré 8 ramifié seulement en 2 ($d_K = \pm 2^r$), I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus de 2 . Alors il existe $\theta \in I \backslash \mathbb{Z}$ tel que si :

i) $2\mathbb{Z}_K = \wp^8$ *alors on a :*
1) $\mathcal{T}_2(\theta) \leq U_2$ *où* $U_2 = \frac{a_1^2}{8} + 2^{\frac{3+r}{7}}$;
2) $0 \leq a_1 \leq 8$.

ii) $2\mathbb{Z}_K = \wp^4$ *ou* $2\mathbb{Z}_K = \wp_1^4 \wp_2^4$ *alors on a :*
1) $\mathcal{T}_2(\theta) \leq U_2$ *où* $U_2 = \frac{a_1^2}{8} + 2^{\frac{5+r}{7}}$
2) $0 \leq a_1 \leq 8$.

Preuve :
Elle découle directement du théorème de Jones et Roberts en degré $n = 8$. En effet :

i) Si $2\mathbb{Z}_K = \wp^8$ alors $I = \wp$, et donc $m = 2$ et $l = 2$ et $U_2 = \frac{a_1^2}{8} + 2^{\frac{3+r}{7}}$. Le calcul donne alors $0 \leq a_1 \leq 8$.

ii) Si $2\mathbb{Z}_K = \wp^4$ alors $I = \wp$ et donc $m = 4$, $l = 2$ et $U_2 = \frac{a_1^2}{8} + 2^{\frac{5+r}{7}}$. De même si $2\mathbb{Z}_L = \wp_1^4 \wp_2^4$, de façon analogue on a $I = \wp_1 \wp_2$, $m = 4$, $l = 2$ et $U_2 = \frac{a_1^2}{8} + 2^{\frac{5+r}{7}}$. On montre aisément que $0 \leq a_1 \leq 8$. □

Appliquons ce corollaire aux différents discriminants obtenus dans le cas de la ramification en 2.

Proposition 3.5.2

1. *Si $d_K = \pm 2^{31}$ alors $a_1 = 0$, et en fonction de la décomposition de l'idéal $2\mathbb{Z}_K$ on a $U_2 = 28.984$ ou $U_2 = 35.331$.*
2. *Si $d_K \in \{\pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{28}, \pm 2^{29}, \pm 2^{30}\}$ alors $a_1 = 0$ ou $a_1 = 8$.*
   Pour $d_K = \pm 2^{30}$, si $a_1 = 0$ (respectivement $a_1 = 8$) alors $U_2 = 26.251$ ou $U_2 = 32$ (respectivement $U_2 = 34.251$ ou $U_2 = 40$).
   Pour $d_K = \pm 2^{29}$, si $a_1 = 0$ (respectivement $a_1 = 8$) alors $U_2 = 23.776$ ou $U_2 = 28.984$ (respectivement $U_2 = 31.776$ ou $U_2 = 36.984$).
   Pour $d_K = \pm 2^{28}$, si $a_1 = 0$ (respectivement $a_1 = 8$) alors $U_2 = 21.535$ ou $U_2 = 26.251$ (respectivement $U_2 = 29.535$ ou $U_2 = 35.251$).
   Pour $d_k = \pm 2^{27}$, si $a_1 = 0$ (respectivement $a_1 = 8$) alors $U_2 = 19.505$ ou $U_2 = 23.776$ (respectivement $U_2 = 27.505$ ou $U_2 = 31.776$).
   Pour $d_K = \pm 2^{26}$, si $a_1 = 0$ (respectivement $a_1 = 8$) alors $U_2 = 17.666$ ou $U_2 = 21.535$ (respectivement $U_2 = 25.666$ ou $U_2 = 29.535$).
   Pour $d_K = \pm 2^{25}$, si $a_1 = 0$ (respectivement $a_1 = 8$) alors $U_2 = 16$ ou $U_2 = 19.505$ (respectivement $U_2 = 24$ ou $U_2 = 27.505$).
   Pour $d_K = \pm 2^{24}$, si $a_1 = 0$ (respectivement $a_1 = 8$) alors $U_2 = 14.492$ ou $U_2 = 17.666$ (respectivement $U_2 = 22.492$ ou $U_2 = 25.666$).
3. *Si $d_K \in \{\pm 2^{21}, \pm 2^{22}\}$ alors $a_1 = 0, 4$ ou 8.*
   Pour $d_K = \pm 2^{22}$, on obtient selon l'expression de U_2 les valeurs suivantes :

i) *Si* $a_1 = 0$ *alors* $U_2 = 11.888$ *ou* $U_2 = 14.492$.

ii) *Si* $a_1 = 4$ *alors* $U_2 = 13.888$ *ou* $U_2 = 16.492$.

iii) *Si* $a_1 = 8$ *alors* $U_2 = 19.888$ *ou* $U_2 = 22.492$.

Pour $d_K = \pm 2^{21}$, *on obtient selon l'expression de* U_2 *les valeurs suivantes :*

i) *Si* $a_1 = 0$ *alors* $U_2 = 10.768$ *ou* $U_2 = 13.126$.

ii) *Si* $a_1 = 4$ *alors* $U_2 = 12.768$ *ou* $U_2 = 15.126$.

iii) *Si* $a_1 = 8$ *alors* $U_2 = 18.768$ *ou* $U_2 = 21.126$.

Preuve :
Du tableau donnant les exposants de Newton-Ore des coefficients a_i de f_θ, on déduit que :
1) le coefficient a_1 est divisible par 16 lorque $d_K = \pm 2^{31}$. Mais comme $0 \leq a_1 \leq 8$ on a alors $a_1 = 0$. Les valeurs de U_2 en découle en fonction de la décomposition de l'idéal $2\mathbb{Z}_K$.
2) Pour $d_K \in \{\pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{27}, \pm 2^{28}, \pm 2^{29}, \pm 2^{30}\}$, le coefficient a_1 est divisible par 8. De l'inégalité $0 \leq a_1 \leq 8$ on en déduit les valeurs $a_1 = 0$ ou $a_1 = 8$.
3) Pour $d_K \in \{\pm 2^{21}, \pm 2^{22}\}$, le coefficient a_1 est divisible par 4 ; et comme précédemment on montre que $a_1 = 0, 4$ ou 8. □

A partir de l'inégalité suivante du paragraphe 3.5) :

$$\frac{a_1^2 - U_2}{2} \leq a_2 \leq \frac{\frac{3}{4}a_1^2 + U_2}{2}$$

et du tableau des exposants de Newton-Ore, nous avons les résultats suivants dans lesquels nous donnons l'ensemble des valeurs possibles du coefficient a_2 dans le cas où a_1 est nul et en ne tenant compte que de la plus grande valeur prise par U_2.

Corollaire 3.5.3
a) *Si* $d_K \in \{\pm 2^{30}, \pm 2^{31}\}$ *et* $a_1 = 0$ *alors* $a_2 \in \{-16, -8, 0, 8, 16\}$.
b) *Si* $d_K \in \{\pm 2^{28}, \pm 2^{29}\}$ *et* $a_1 = 0$ *alors* $a_2 \in \{-12, -8, 0, 8, 12\}$.
c) *Si* $d_K \in \{\pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{27}\}$ *et* $a_1 = 0$ *alors* $a_2 \in \{-8, -4, 0, 4, 8\}$.
d) *Si* $d_K = \pm 2^{22}$ *et* $a_1 = 0$ *alors* $a_2 \in \{-4, 0, 4\}$.
e) *Si* $d_K = \pm 2^{21}$ *et* $a_1 = 0$ *alors* $a_2 \in \{-4, -2, 0, 2, 4\}$.

Remarque :
On obtient des résultats analogues pour les autres valeurs du coefficient a_1.

On détermine alors le terme constant a_8 en utilisant l'inégalité suivante entre moyennes arithmétique et géométrique :

$$1 \leq |a_8| \leq \left(\frac{\mathcal{T}_2}{8}\right)^4 \leq \left(\frac{U_2}{8}\right)^4.$$

Dans le cas où le coefficient a_1 est nul et selon la plus grande valeur de U_2, nous obtenons les résultats suivants.

Corollaire 3.5.4
1) *Si* $d_K = \pm 2^{21}$ *alors* $a_8 \in \{-6, -4, -2, 2, 4, 6\}$.
2) *Si* $d_K = \pm 2^{22}$ *alors* $a_8 \in \{-10, -8, -6, -4, -2, 2, 4, 6, 8, 10\}$.
3) *Si* $d_K = \pm 2^{24}$ *alors* $|a_8| \leq 23$ *et est divible par* 2.
4) *Si* $d_K = \pm 2^{25}$ *alors* $1 \leq |a_8| \leq 35$ *et est divisible par* 2.
6) *Si* $d_K = \pm 2^{26}$ *alors* $1 \leq |a_8| \leq 52$ *et est divisible par* 2.
7) *Si* $d_K = \pm 2^{27}$ *alors* $1 \leq |a_8| \leq 78$ *et est divisible par* 2.
8) *Si* $d_K = \pm 2^{28}$ *alors* $1 \leq |a_8| \leq 115$ *et est divisible par* 2.
9) *Si* $d_K = \pm 2^{29}$ *alors* $1 \leq |a_8| \leq 172$ *et est divisible par* 2.
10) *Si* $d_K = \pm 2^{30}$ *alors* $1 \leq |a_8| \leq 256$ *et est divisible par* 2.
11) *Si* $d_K = \pm 2^{31}$ *alors* $1 \leq |a_8| \leq 380$ *et est divisible par* 2.

Remarque :
On obtient des résultats analogues pour les autres valeurs du coefficient a_1.

L'utilisation de l'inégalité suivante du paragraphe 3.5

$$\frac{-a_1^3 + 3a_1a_2 - {U_2}^{3/2}}{3} \leq a_3 \leq \frac{-a_1^3 + 3a_1a_2 + {U_2}^{3/2}}{3}$$

permet à partir du tableau des exposants de Newton-Ore, de calculer les différentes valeurs possibles du coefficient a_3. Comme précédemment nous obtenons le corollaire suivant pour $a_1 = 0$.

Corollaire 3.5.5
1) *Si* $d_K = \pm 2^{21}$ *alors* $a_3 \in \{-40, -32, -24, -16, -8, 0, 8, 16, 24, 32, 40\}$.
2) *Si* $d_K = \pm 2^{22}$ *alors* $a_3 \in \{-48, -40, -32, -24, -16, -8, 0, 8, 16, 24, 32, 40, 48\}$.
3) *Si* $d_K = \pm 2^{24}$ *alors* $|a_3| \leq 74$ *et est divisible par* 8.
4) *Si* $d_K = \pm 2^{25}$ *alors* $|a_3| \leq 86$ *et est divisible par* 8.
5) *Si* $d_K = \pm 2^{26}$ *alors* $|a_3| \leq 99$ *et est divisible par* 8.
6) *Si* $d_K = \pm 2^{27}$ *alors* $|a_3| \leq 115$ *et est divisible par* 8.
7) *Si* $d_K = \pm 2^{28}$ *alors* $|a_3| \leq 134$ *et est divisible par* 8.
8) *Si* $d_K = \pm 2^{29}$ *alors* $|a_3| \leq 156$ *et est divisible par* 16.
9) *Si* $d_K = \pm 2^{30}$ *alors* $|a_3| \leq 181$ *et est divisible par* 16.
10) *Si* $d_K = \pm 2^{31}$ *alors* $|a_3| \leq 210$ *et est divisible par* 16.

Remarque :
De façon analogue, on obtient les valeurs du coefficient a_3 dans le cas où a_1 est non nul. Pour les autres coefficients, c'est-à-dire pour a_4, a_5, a_6 et a_7, nous utiliserons par la suite les bornes de M. Pohst pour les fonctions $\mathcal{T}_m$ avec $m = 4, 5, 6, 7$ pour déterminer les valeurs possibles. Ces bornes permettent aussi de donner de meilleures bornes aux coefficients a_3 en utilisant les fonctions $\mathcal{T}_3$.

Le cas de la ramification en p=5 sans GRH :

Dans le cas de la ramification en 5, on a montré que les décompositions possibles sont : $5\mathbb{Z}_K = \wp_1^5\wp_2^3$, $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3$, $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3$, $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3\wp_4$ et $5\mathbb{Z}_K = \wp_1^5\wp_2$. En

fonction de ces décompositions primaires, nous avons les corollaires suivants qui découlent du théorème de Jones et Roberts.

Corollaire 3.5.6

Soit K un corps de nombres primitif de degré 8 de discriminant $d_K = 5^b$, I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus de 5 . Alors il existe $\theta \in I\backslash\mathbb{Z}$ tel que :

i) si $5\mathbb{Z}_K = \wp_1^5\wp_2^3$ alors $\mathcal{T}_2(\theta) \leq U_2$ où $U_2 = \frac{a_1^2}{8} + (8 \times 5^{b+2})^{\frac{1}{7}}$;

ii) si $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3$ alors $\mathcal{T}_2(\theta) \leq U_2$ où $U_2 = \frac{a_1^2}{8} + (8 \times 5^{b+4})^{\frac{1}{7}}$;

iii) si $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3$, $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3\wp_4$ ou $5\mathbb{Z}_K = \wp_1^5\wp_2$ alors $\mathcal{T}_2(\theta) \leq U_2$ où $U_2 = \frac{a_1^2}{8} + (8 \times 5^{b+6})^{\frac{1}{7}}$.

De plus $0 \leq a_1 \leq 20$.

En utilisant les exposants de Newton-Ore, on calcule les valeurs prises par le coefficient a_1 dans la proposition qui suit.

Proposition 3.5.7

Si le corps K est ramifié seulement en 5 alors $a_1 = 0, 5, 10, 15$ ou 20.

Suivant les différentes valeurs du coefficient a_1, on calcule les valeurs prises par U_2. Pour chaque valeur de U_2 fixée, l'utilisation de l'inégalité $\frac{a_1^2 - U_2}{2} \leq a_2 \leq \frac{\frac{3}{4}a_1^2 + U_2}{2}$ et des exposants de Newton-Ore permettent de calculer les différentes valeurs de a_2. La détermination des autres coefficients se fait en utilisant aussi la méthode vue dans le cas de la ramification en 2.

Le cas de la ramification en p=7 :

Le corps primitif K étant de degré 8 et ramifié seulement en 7, d'après la proposition 2.1.16, il est alors sauvagement ramifié. Nous avons vu à travers le théorème 2.1.19 que la seule décomposition possible de l'idéal engendré par 7 dans $\mathbb{Z}_K$ est de la forme $7\mathbb{Z}_K = \wp_1^7\wp_2$. Cela nous amène aux résultats suivants qui découlent du théorème de Jones et Roberts.

Corollaire 3.5.8

Soit K un corps de nombres primitif de degré 8 ramifié seulement en 7 ($d_K = \pm 7^s$), I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus de 7 . Alors il existe $\theta \in I\backslash\mathbb{Z}$ tel que :

1) $\mathcal{T}_2(\theta) \leq U_2$ *où* $U_2 = \frac{a_1^2}{8} + (8 \times 7^{s+2})^{\frac{1}{7}}$;
2) $0 \leq a_1 \leq 28$.

Preuve :

La seule décomposition possible de l'idéal $7\mathbb{Z}_K$ est : $7\mathbb{Z}_K = \wp_1^7\wp_2$. D'où $I = \wp_1\wp_2$, et donc $m = 49, l = 7$. Le résultat découle alors du théorème de Jones et Roberts. □

Proposition 3.5.9
Si le corps K est ramifié seulement en 7 alors le coefficient a_1 du polynôme générateur f_θ appartient à l'ensemble

$$\{0, 7, 14, 21, 28\}.$$

Preuve :
Il découle du corollaire précédent et du tableau des exposants de Newton-Ore. □

Une fois les valeurs de a_1 connues, on calcule facilement les valeurs respectives de U_2. La proposition précédente et l'inégalités *ii*) du paragraphe 3.5 conduisent aux résultats suivants dans le cas où $a_1 = 0$.

Corollaire 3.5.10
a) Pour $d_K = 7^8$ alors $U_2 = 21.692$ et $a_2 \in \{-7, 0, 7\}$.
b) Pour $d_K = -7^9$ alors $U_2 = 28.644$ et $a_2 \in \{-14, -7, 0, 7, 14\}$.
c) Pour $d_K = 7^{10}$ alors $U_2 = 37.823$ et $a_2 \in \{-14, -7, 0, 7, 14\}$.
d) Pour $d_K = -7^{11}$ alors $U_2 = 49.944$ et $a_2 \in \{-21, -14, -7, 0, 7, 14, 21\}$.
e) Pour $d_K = 7^{12}$ alors $U_2 = 65.950$ et $a_2 \in \{-28, -21, -14, -7, 0, 7, 14, 21, 28\}$.
f) Pour $d_K = -7^{13}$ alors $U_2 = 87.084$ et $a_2 \in \{-42, -35, -28, -21, -14, -7, 0, 7, 14, 21, 28, 35, 42\}$.

On détermine alors le terme a_3 à partir de l'inégalité *iii*) du paragraphe 3.5, et le terme constant a_8 en utilisant l'inégalité entre moyennes arithmétique et géométrique :

$$1 \leq |a_8| \leq \left(\frac{\mathcal{T}_2}{8}\right)^4 \leq \left(\frac{U_2}{8}\right)^4.$$

Des résultats analogues au corollaire précédent sont obtenus pour les autres valeurs du coefficient a_1.

Pour améliorer les bornes des autres coefficients aussi bien dans le cas de la ramification en $p = 2$, en $p = 5$ et en $p = 7$, nous allons faire intervenir dans ce qui suit les fonctions $\mathcal{T}_m(\theta) = \sum_{i=0}^{8} |\theta_i|^m$ pour $m \in \mathbb{Z} - \{0, 2\}$.

3.5.2 Utilisation des fonctions $\mathcal{T}_m(\theta) = \sum_{i=0}^{8} |\theta_i|^m$

Une fois les coefficients a_1, a_2, a_3 et a_8 fixés, nous déterminons les autres coefficients en calculant des majorations pour les fonctions $\mathcal{T}_m(\theta) = \sum_{i=0}^{8} |\theta_i|^m$ pour $m \in \mathbb{Z} - \{0, 2\}$ où les θ_i sont les conjugués de θ. L'énoncé suivant dû à Pohst **[23]**, indique une manière de trouver ces majorations.

Théorème 3.5.11
Soit T et N deux constantes positives vérifiant

$$(T/n)^{n/2} \geq N.$$

Alors la fonction

$$\mathcal{T}_m(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^m$$

$m \in \mathbb{Z} - \{0, 2\}$ possède un maximum absolu sur le compact

$$S = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | \sum_{i=1}^{n} x_i^2 \leq T; \ \prod_{i=1}^{n} x_i = N; x_i \geq 0 \quad pour \quad i = 1, \ldots, n\}.$$

Ce maximum est atteint en un point $(y_1, \ldots, y_n) \in S$ ayant deux coordonnées différentes au plus.

La manière de calculer effectivement ces maxima pour les fonctions $\mathcal{T}_m(\theta), m \in \mathbb{Z} - \{0, 2\}$ est décrite dans **[23]**.

Pour chaque valeur entière de t où $(1 \leq t < n)$, on cherche la plus petite racine positive (notée y_1) de l'équation

$$t(y^{t-n}N)^{2/t} + (n-t)y^2 - T = 0;$$

alors, pour chaque $m \in \mathbb{Z} - \{0, 2\}$ on a :

$$\mathcal{T}_m(\theta) \leq \ \max_{1 \leq t < n}\{t(y_1^{t-n}N)^{m/t} + (n-t)y_1^m\}.$$

Nous mettrons en place un programme permettant de calculer ces majorations. Notons $\mathcal{T}_m$, la partie entière de ces majorations. On a

$$|S_m| \leq \mathcal{T}_m \quad pour \quad m \in \mathbb{Z} - \{0, 2\}.$$

Une fois les valeurs de $\mathcal{T}_m$ connues, à partir de la relation de Newton

$$S_k + \sum_{i=1}^{k-1} a_i S_{k-i} + k a_k = 0 \quad 1 \leq k \leq n$$

nous pouvons dans le cas où $a_1 = 0$, donner de meilleures bornes pour les autres coefficients a_k du polynôme f_θ :

i) $|a_3| = |S_3/3| \leq \mathcal{T}_3/3$;

ii) $|a_4| = |\frac{1}{4}(2a_2^2 - S_4)| \leq \frac{2a_2^2 + \mathcal{T}_4}{4}$;

iii) $|a_7| = |a_8 S_{-1}| \leq |a_8|\mathcal{T}_{-1}$.

Des résultats analogues donnent des bornes de ces coefficients pour les autres valeurs de a_1. On obtient les coefficients a_5 et a_6 (ausi bien pour a_1 non nul) à partir du résultat suivant, meilleur que celui obtenu par utilisation de la relation de Newton .
Soit $f_\theta(x) = \prod_{i=1}^{8}(x - \theta_i)$; on remarque que $f_\theta(\pm 1)$ est une norme. En utilisant l'inégalité entre moyennes arithmétique et géométrique on obtient

$$|f_\theta(1)| = |N(1-\theta)| = \prod_{i=1}^{8} |1 - \theta_i| \leq (\mathcal{T}_2(1-\theta)/8)^4.$$

Or,

$$(\mathcal{T}_2(1-\theta)/8)^4 = (1 + (\mathcal{T}_2(\theta) - 2S_1)/8)^4;$$

on a donc

$$|f_\theta(1)| \leq (1 + (\mathcal{T}_2(\theta) - 2S_1)/8)^4.$$

De même on montre que

$$|f_\theta(-1)| \leq (1 + (\mathcal{T}_2(\theta) + 2S_1)/8)^4.$$

Dans le cas où $a_1 = 0$ on a

$$|f_\theta(\pm 1)| \leq (1 + \mathcal{T}_2(\theta)/8)^4.$$

En posant

$$f_\theta(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_5x^3 + a_6x^2 + a_7x + a_8,$$

on obtient

$$a_5 = \frac{f_\theta(1) - f_\theta(-1)}{2} - (a_1 + a_3 + a_7),$$
$$a_6 = \frac{f_\theta(1) + f_\theta(-1)}{2} - (1 + a_2 + a_4 + a_8).$$

On termine cette partie par la notion de corrections locales qui interviennent dans la minoration des discriminants, et qui conduisent à des simplifications considérables dans les calculs.

3.5.3 Utilisation des corrections locales de Serre, Odlyzko et Poitou

Tous les tableaux de ce paragraphe ont été extraits de **[24]** et **[25]**.
On peut améliorer la table dans **[8]** donnant la minoration en valeur absolue du discriminant d'un corps de nombres de degré 8 si l'on connait la décomposition en idéaux premiers (de ce corps) des petits nombres premiers. Il suffit de faire intervenir dans le calcul de la minoration la contribution correspondant aux corrections locales. Ces résultats vont nous permettre d'éliminer un bon nombre de discriminants en fonction de la signature du corps K.

Cas où K est totalement imaginaire :

Supposons que le nombre premier p soit divisible par un idéal premier $\wp$ de K de norme $q = p^f$ où f est le degré résiduel de $\wp$ dans $K/\mathbb{Q}$. On obtient alors les minorations suivantes de façon inconditionnelle pour les valeurs de p et q indiquées.

p	q	Minoration
2	2	3 379 344
2	4	1 930 702
3	3	2 403 757
3	9	1 221 236
5	5	1 656 110
7	7	1 361 652

Nous avons déjà vérifié que les corps K recherchés contiennent un idéal premier $\wp$ qui divise 2 (resp. 7) et de norme 2 ou 4 (resp. 7) dans le cas de la ramification en 2 (resp. en 7).

Proposition 3.5.12
Si le discriminant $d_K = \pm 2^{21}$ alors on a $2\mathbb{Z}_K = \wp^4$, et le corps K ne peut donc contenir des idéaux premiers de norme 2.

Preuve :
Il découle du tableau ci-dessus. □

Cas où K est de signature (2,3) :

La contribution des corrections locales permet d'améliorer les minorations de Diaz y Diaz. Les résultats (sans GRH) sont donnés dans le tableau ci-dessous pour les valeurs de p et q indiquées comme précédemment.

p	q	Minoration
2	2	11 725 962
2	4	6 688 609
3	3	8 336 752
3	9	4 160 401
5	5	5 726 300
7	7	4 682 933

Proposition 3.5.13
Si K est ramifié seulement en 2 et de signature $(2,3)$ alors son discriminant d_K ne peut prendre les valeurs suivantes :

$$\pm 2^{21}, \pm 2^{22}.$$

Preuve :
Il découle du tableau ci-dessus. □

Cas où K est de signature (4,2) :

La contribution des corrections locales sans GRH donne les résultats suivants :

p	q	Minoration
2	2	42 765 015
2	4	24 363 884
3	3	30 393 069
3	9	14 972 957
5	5	20 829 049
7	7	16 957 023

Proposition 3.5.14
Si K est ramifié seulement en 2 et de signature $(4,2)$ alors son discriminant d_K ne peut prendre les valeurs suivantes :

$$\pm 2^{21}, \pm 2^{22}, \pm 2^{24}.$$

Dans le cas de la ramification en 7, on obtient ces résultats analogues :

Proposition 3.5.15
Si K est ramifié seulement en 7 et de signature $(4,2)$ alors son discriminant d_K ne peut prendre la valeur 7^8.

Lemme 3.5.16
Soit K un corps de nombres de degré 8, de signature $(4,2)$ et de discriminant $d_K = -7^9$. Si y est un entier de K de norme absolue a, alors :
$v_2(a) = 0$ ou $v_2(a) \geq 2$.

Preuve :
Ce résultat découle du tableau ci-dessus donnant la minoration du discriminant en tenant compte de la contribution correspondant aux corrections locales et du fait que si y est entier dans K alors :

$$|N(y)| = |\mathbb{Z}_K/y\mathbb{Z}_K| = |\mathbb{Z}_K/\prod_i {\wp_i}^{r_i}| = \prod_i |\mathbb{Z}_K/{\wp_i}^{r_i}| = \prod_i N({\wp_i}^{r_i}) = \prod_i p_i^{f_i r_i}. \quad \square$$

Ce lemme permet d'éliminer un nombre assez important de valeurs du terme constant a_8.

Cas où K est de signature (6,1) :

La contribution des corrections locales sans GRH donnent :

p	q	Minoration
2	2	162 569 966
2	4	92 810 082
3	3	115 852 707
3	9	52 529 001
5	5	79 259 702
7	7	64 309 248

Proposition 3.5.17
Si K est ramifié seulement en 2 et de signature $(6,1)$ alors son discriminant d_K ne peut prendre les valeurs suivantes :

$$\pm 2^{21}, \pm 2^{22}, \pm 2^{24}, \pm 2^{25}, \pm 2^{26}.$$

Dans le cas de la ramification en 7, on a le lemme suivant qui découle du tableau ci-dessus

Lemme 3.5.18
Soit K un corps de nombres de degré 8, de signature $(6,1)$ et de discriminant $d_K = -7^9$. Si y est un entier de K de norme absolue a alors :

i) $v_2(a) = 0$ *ou* $v_2(a) \geq 3$,

ii) $v_3(a) = 0$ *ou* $v_3(a) \geq 3$,

iii) $v_5(a) = 0$ *ou* $v_5(a) \geq 2$,

iv) $v_7(a) = 0$ *ou* $v_7(a) \geq 2$.

Proposition 3.5.19
Si le corps K est de signature $(6,1)$ alors son discriminant d_K ne peut prendre les valeurs 7^8 et -7^9.

Preuve :
Il découle du tableau ci-dessus. □

Cas où K est totalement réel :

Ce cas est plus intéressant dans la mesure où on peut éliminer un grand nombre de discriminants. Mais avant cela, rappelons d'abord ce théorème établi par J. Kluners et G. Malle dans **[20]**.

Théorème 3.5.20
La valeur minimale en valeur absolue prise par le discriminant d'un corps de nombre primitif totalement réel de degré 8 est 483345053. Le corps correspondant est unique à isomorphisme près, un polynôme générateur est :

$$x^8 - x^7 - 7x^6 + 4x^5 + 15x^4 - 3x^3 - 9x^2 + 1,$$

et son groupe de Galois est T_{50}.

Le tableau ci-dessous donnant les minorations des discriminants en degré 8 de façon inconditionnelle, en tenant compte de la contribution des corrections locales nous donne de meilleures bornes :

p	q	Minoration
2	2	646 844 001
2	4	367 892 401
3	3	459 467 465
3	9	222 553 383
5	5	254 052 210
7	7	203 776 319

De ces résultats, nous allons énoncer les propositions suivantes :

Proposition 3.5.21
Si K est primitif, ramifié seulement en 2 et totalement réel, alors son discriminant d_K ne peut prendre les valeurs suivantes :

$$\pm 2^{21}, \pm 2^{22}, \pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{27}, \pm 2^{28}.$$

Preuve :
Elle découle du tableau ci-dessus. □

Proposition 3.5.22
Si K est primitif, ramifié seulement en 7 et totalement réel, alors son discriminant d_K ne peut prendre les valeurs suivantes :

$$7^8, -7^9, 7^{10}.$$

Preuve :
Elle découle du théorème de Kluners et Malle. □

L'étude menée dans ce paragraphe permet d'énoncer le théorème suivant :

Théorème 3.5.23
Si K est un corps de nombres de degré 8 de discriminant égal à $\pm 2^{21}$ ou $\pm 2^{22}$ alors il ne peut être que totalement imaginaire. Dans le cas où le discriminant est égal à $\pm 2^{21}$, alors le corps K ne peut contenir que des idéaux premiers de norme 4.

Voyons maintenant ce qu'il en est de cette étude dans le cas des corps de nombres de degré 9.

3.6 Amélioration des bornes des coefficients de f_θ en degré 9

On pose :

$$f_\theta(x) = x^9 + a_1x^8 + a_2x^7 + a_3x^6 + a_4x^5 + a_5x^4 + a_6x^3 + a_7x^2 + a_8x + a_9$$

le polynôme minimal de l'élément primitif θ en degré 9.

$$\text{Soit } \mathcal{T}_2 = \mathcal{T}_2(\theta) = \sum_{i=1}^{9} |\theta_i|^2 \text{ et } U_2 = \frac{1}{9}(Tr(\theta))^2 + \gamma_8\left(\frac{m^2|d_K|}{9l^2}\right)^{1/8}$$

où les θ_i désignent les conjugués de θ, et $S_k = \sum_{i=1}^{9} \theta_i^k$ avec $k \in \mathbb{Z}$.

En appliquant les résultats du paragraphe 3.3 au cas $n = 9$, on obtient :

i) $|a_k| \leq C_9^k {U_2}^{k/2} \quad 1 \leq k \leq 9.$

ii) $\dfrac{a_1^2 - U_2}{2} \leq a_2 \leq \dfrac{\frac{7}{9}a_1^2 + U_2}{2}.$

iii) En posant $\mathcal{T}_k = \sum_{j=1}^{9} |\theta_j|^k$ on a
$\dfrac{-\sum_{i=1}^{k-1} a_i S_{k-i} - \mathcal{T}_k}{k} \leq a_k \leq \dfrac{-\sum_{j=1}^{k-1} a_i S_{k-i} + \mathcal{T}_k}{k}.$
Cette inégalité donne un encadrement par récurrence des coefficients a_k en fonction de $\mathcal{T}_k$ pour $3 \leq k \leq 9$.

iv) En prenant $k = -1$ dans la somme S_k des puissances k-ième des θ_i, on a

$$S_{-1} = -\frac{a_8}{a_9}.$$

v) A partir des inégalités entre moyennes arithmétique et géométrique on déduit :

$$1 \leq |a_9| \leq \left(\frac{\mathcal{T}_2}{9}\right)^{4.5} \leq \left(\frac{U_2}{9}\right)^{4.5}.$$

3.6.1 Utilisation du théorème de Jones et Roberts

Le cas de la ramification en $p = 2$:

Nous avons vu au chapitre précédent que la seule décomposition possible dans ce cas est $2\mathbb{Z}_K = \wp_1^8\wp_2$. Nous déterminons les différents polynômes générateurs en fonction de cette décomposition. On en déduit le corollaire suivant qui découle du théorème de Jones et Roberts :

Corollaire 3.6.1
Soit K un corps de nombres primitif de degré 9 ramifié seulement en 2 ($d_K = \pm 2^r$), I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus de 2 . Alors il existe $\theta \in I \backslash \mathbb{Z}$ tel que si :

i) $\mathcal{T}_2(\theta) \leq U_2$ *où* $U_2 = \frac{a_1^2}{9} + (\frac{2^{10+r}}{9})^{1/8}$;

ii) $0 \leq a_1 \leq 9$.

Preuve :
Elle découle directement du théorème de Jones et Roberts en degré $n = 9$. □

Appliquons ce corollaire aux différents discriminants obtenus. Le coefficient $a_1 = 0, 2, 4, 6$ ou 8. On calcule aisément les valeurs respectives de U_2 et les autres coefficients du polynôme générateur f_θ.

Le cas de la ramification en p=3 :
Nous avons vu que le seul cas possible est la ramification totale en 3, c'est-à-dire $3\mathbb{Z}_K = \wp^9$. Du théorème de Jones et Roberts et des exposants de Newton-Ore, découlent les résultats suivants.

Corollaire 3.6.2
Soit K un corps de nombres primitif de degré 9 ramifié seulement en 3 ($d_K = \pm 3^\beta$), I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus de 3 . Alors il existe $\theta \in I \backslash \mathbb{Z}$ tel que :

i) $\mathcal{T}_2(\theta) \leq U_2$ *où* $U_2 = \frac{a_1^2}{9} + 2 \times 3^{\frac{\beta-2}{8}}$;

ii) $0 \leq a_1 \leq 13$.

Corollaire 3.6.3
i) Si $d_K = 3^{26}$ alors $a_1 = 0$;

ii) Si $d_K \in \{3^{18}, -3^{19}, 3^{20}, -3^{21}, 3^{22}, -3^{23}, 3^{24}, -3^{25}\}$ alors $a_1 = 0$ ou 9.

Preuve :

i) Si $d_K = 3^{26}$ alors l'exposant de Newton-Ore du coefficient a_1 est 3 ; cela veut dire que la plus petite puissance de 3 divisant a_1 est 27. Comme $0 \leq a_1 \leq 13$ alors $a_1 = 0$.

ii) Si $d_K \in \{3^{18}, -3^{19}, 3^{20}, -3^{21}, 3^{22}, -3^{23}, 3^{24}, -3^{25}\}$, l'exposant de Newton-Ore est 2 et on montre de façon analogue que $a_1 = 0$ ou 9. □

Une fois la valeur de a_1 fixée, en fonction du discriminant on calule facilement U_2 et partant de là, les autres coefficients de f_θ.

Le cas de la ramification en p=5 sans GRH :
Dans le cas de la ramification en 5, on a montré que les décompositions possibles sont : $5\mathbb{Z}_K = \wp_1^5\wp_2^4$, $5\mathbb{Z}_K = \wp_1^5\wp_2^3\wp_3$, $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3^2$ ou $5\mathbb{Z}_K = \wp_1^5\wp_2$. En fonction de ces décompositions, nous obtenons les corollaires suivants qui découlent du théorème de Jones et Roberts.

Corollaire 3.6.4
Soit K un corps de nombres primitif de degré 9 de discriminant $d_K = 5^b$, I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus de 5 . Alors il existe $\theta \in I\backslash\mathbb{Z}$ tel que :

i) si $5\mathbb{Z}_K = \wp_1^5\wp_2^4$ alors $\mathcal{T}_2(\theta) \leq U_2$ où $U_2 = \frac{a_1^2}{9} + 2 \times (5^{b+2}/9)^{\frac{1}{8}}$;

ii) si $5\mathbb{Z}_K = \wp_1^5\wp_2^3\wp_3$, $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3^2$ ou $5\mathbb{Z}_K = \wp_1^5\wp_2^2$ alors $\mathcal{T}_2(\theta) \leq U_2$ où $U_2 = \frac{a_1^2}{9} + 2 \times (5^{b+4}/9)^{\frac{1}{8}}$.

De plus $0 \leq a_1 \leq 22$.

Les exposants de Newton-Ore montrent que $a_1 = 0, 5, 10, 15$ ou 20. Pour chaque valeur de a_1 fixée, on calcule la valeur de U_2 respective. On détermine comme précédemment les autres coefficients de f_θ.

Le cas de la ramification en p=7 :

Dans le cas de la ramification en 7, les différentes décompositions possibles de l'idéal engendré par 7 dans $\mathbb{Z}_K$ sont $7\mathbb{Z}_K = \wp_1^7\wp_2^2$, $7\mathbb{Z}_K = \wp_1^7\wp_2\wp_3$ ou $7\mathbb{Z}_K = \wp_1^7\wp_2$. Cela nous amène aux résultats suivants qui découlent du théorème de Jones et Roberts.

Corollaire 3.6.5
Soit K un corps de nombres primitif de degré 9 ramifié seulement en 7 ($d_K = \pm 7^s$), I le produit de tous les idéaux premiers non nuls de $\mathbb{Z}_K$ au-dessus de 7 . Alors il existe $\theta \in I\backslash\mathbb{Z}$ tel que :

i) Si $7\mathbb{Z}_K = \wp_1^7\wp_2$ alors $\mathcal{T}_2(\theta) \leq U_2$ où $U_2 = \frac{a_1^2}{9} + 2 \times (7^{s+2}/9)^{1/8}$;

ii) Si $7\mathbb{Z}_K = \wp_1^7\wp_2\wp_3$ ou $7\mathbb{Z}_K = \wp_1^7\wp_2$ alors $\mathcal{T}_2(\theta) \leq U_2$ où $U_2 = \frac{a_1^2}{9} + 2 \times (7^{s+4}/9)^{1/8}$;

iii) De plus on a : $0 \leq a_1 \leq 28$.

Proposition 3.6.6
Si le corps K est ramifié seulement en 7 alors le coefficient a_1 du polynôme générateur f_θ appartient à l'ensemble

$$\{0, 7, 14, 21, 28\}.$$

Preuve :
Il découle du corollaire précédent et du tableau des exposants de Newton-Ore. □

Une fois les valeurs de a_1 connues, on calcule facilement les valeurs respectives de U_2. Le calcul des autres coefficients en découle aisément.

Pour améliorer les bornes des coefficients aussi bien dans le cas de la ramification en $p = 2$, $p = 3$, $p = 5$ ou en $p = 7$, nous allons utiliser dans ce qui suit les fonctions $\mathcal{T}_m(\theta) = \sum_{i=0}^{9} |\theta_i|^m$ pour $m \in \mathbb{Z} - \{0, 2\}$.

3.6.2 Utilisation des fonctions $\mathcal{T}_m(\theta) = \sum_{i=0}^{9} |\theta_i|^m$

Une fois les coefficients a_1, a_2, a_3 et a_9 fixés, nous allons maintenant déterminer les autres coefficients en calculant des majorations pour les fonctions $\mathcal{T}_m(\theta) = \sum_{i=0}^{9} |\theta_i|^m$ pour $m \in \mathbb{Z} - \{0, 2\}$ où les θ_i sont les conjugués de θ. Nous utiliserons la même méthode que celle vue dans le théorème 3.5.11. Nous mettrons en place un programme permettant de calculer ces majorations comme dans le cas des corps de degré 8. Notons aussi $\mathcal{T}_m$, la partie entière de ces majorations. On a

$$|S_m| \leq \mathcal{T}_m \quad pour \quad m \in \mathbb{Z} - \{0, 2\}.$$

Une fois les valeurs de $\mathcal{T}_m$ connues, à partir de la relation de Newton

$$S_k + \sum_{i=1}^{k-1} a_i S_{k-i} + k a_k = 0 \quad 1 \leq k \leq n$$

nous pouvons dans le cas où $a_1 = 0$, donner de meilleures bornes pour les autres coefficients a_k du polynôme f_θ :

i) $|a_3| = |S_3/3| \leq \mathcal{T}_3/3$;

ii) $|a_4| = |\frac{1}{4}(2a_2^2 - S_4)| \leq \frac{2a_2^2 + \mathcal{T}_4}{4}$;

iii) $|a_5| = |\frac{1}{5}(5a_2a_3 - S_5)| \leq \frac{1}{5}(5|a_2a_3| + \mathcal{T}_5)$;

iv) $|a_8| = |a_9 S_{-1}| \leq |a_9| \mathcal{T}_{-1}$.

Des résultats analogues donnent des bornes pour les autres valeurs de a_1. On obtient les coefficients a_6 et a_7 à partir du résultat suivant.
Soit $f_\theta(x) = \prod_{i=1}^{9}(x - \theta_i)$; on remarque que $f_\theta(\pm 1)$ est une norme. En utilisant l'inégalité entre moyennes arithmétique et géométrique on obtient

$$|f_\theta(1)| = |N(1-\theta)| = \prod_{i=1}^{9} |1 - \theta_i| \leq (\mathcal{T}_2(1-\theta)/9)^{4.5}.$$

Or,

$$(\mathcal{T}_2(1-\theta)/9)^{4.5} = (1 + (\mathcal{T}_2(\theta) - 2S_1)/9)^{4.5};$$

on a donc

$$|f_\theta(1)| \leq (1 + (\mathcal{T}_2(\theta) - 2S_1)/9)^{4.5}.$$

De même on montre que

$$|f_\theta(-1)| \leq (1 + (\mathcal{T}_2(\theta) + 2S_1)/9)^{4.5}.$$

Dans le cas où $a_1 = 0$ on a

$$|f_\theta(\pm 1)| \leq (1 + \mathcal{T}_2(\theta)/9)^{4.5}.$$

En posant

$$f_\theta(x) = x^9 + a_1x^8 + a_2x^7 + a_3x^6 + a_4x^5 + a_5x^4 + a_6x^3 + a_7x^2 + a_8x + a_9,$$

on obtient

$$a_6 = \frac{f_\theta(1) - f_\theta(-1)}{2} - (1 + a_2 + a_4 + a_8),$$

$$a_7 = \frac{f_\theta(1) + f_\theta(-1)}{2} - (a_1 + a_3 + a_5 + a_9).$$

Remarque :

Il faut noter que plus l'exposant de Newton-Ore d'un coefficient est grand, moins nous avons de valeurs pour ce coefficient. Cette restriction des valeurs des coefficients permet d'avoir nos résultats numériques dans un temps (délai) assez raisonnable.

Voyons maintenant dans le paragraphe qui suit comment l'utilisation des minorations de discriminanats avec corrections locales peut conduire à des simplifications dans les calculs.

3.6.3 Utilisation des corrections locales de Serre, Odlyzko et Poitou

Tous les tableaux de ce paragraphe ont été extraits de **[24]** et **[25]**.
Comme on l'a vu dans le cas des corps de nombres de degré 8, on peut améliorer la table dans **[8]** donnant la minoration en valeur absolue du discriminant d'un corps de nombres de degré 9 si l'on connait la décomposition en idéaux premiers des petits nombres premiers. Ces résultats permettront d'éliminer un certain nombre de discriminants de corps en fonction des signatures.

Cas où K est de signature (1,4) :

Supposons que le nombre premier p soit divisible par un idéal premier $\wp$ de K de norme $q = p^f$. On obtient alors les minorations suivantes de façon inconditionnelle pour les valeurs de p et q indiquées.

p	q	Minoration
2	2	81 295 503
2	4	46 348 905
2	8	30 249 458
2	16, 32	24 397 331
3	3	57 789 564
3	9	28 685 778
3	27	28 685 778
5	5	39 657 567
5	25	23 235 622
7	7	32 371 194
11	11	26 604 281
13	13	91 837 308

Dans le cas de la ramification en 2 (resp. en 3), nous avons déjà vérifié que les corps K recherchés contiennent des idéaux premiers de norme 2 (resp. 3). Le tableau ci-dessus montre que le discriminant d_K ne peut prendre les valeurs $\pm 2^{25}$ et $\pm 2^{26}$. On vérifie aisément que d_K ne peut aussi prendre la valeur 3^{16} et par conséquent la décomposition $3\mathbb{Z}_K = \wp_1^6 \wp_2^3$ ne peut être possible.

Cas où K est de signature (3,3) :

La contribution des corrections locales permet d'améliorer les minorations de Diaz y Diaz. Les résultats (sans GRH) sont donnés dans le tableau ci-dessous pour les valeurs de p et q indiquées comme précédemment :

p	q	Minoration
2	2	301 476 861
2	4	171 694 369
2	8	111 192 502
2	16, 32	88 341 844
3	3	214 235 487
3	9	105 151 850
3	27	81 777 838
5	5	146 723 989
5	25	82 205 903
7	7	119 294 245
11	11	96 946 913
13	13	91 837 308

A la lecture de ce tableau, on remarque que si le corps K est ramifié en 2, de discriminant $\pm 2^{27}$ et $\pm 2^{28}$ alors il est nécessairement de signature $(1, 4)$, et donc le discriminant d_K ne peut prendre les valeurs -2^{27} et -2^{28}. Ce tableau montre aussi que le corps K de discriminant 5^{11} serait nécessairement de signature $(1, 4)$. On montre de plus que le discriminant d_K ne peut prendre la valeur -7^9 si le corps K ne contient que des idéaux premiers de norme 7.

Cas où K est de signature (5,2) :

La contribution des corrections locales sans GRH donne les résultats suivants :

p	q	Minoration
2	2	1 165 733 328
2	4	663 330 211
2	8	427 071 142
2	16, 32	336 805 639
3	3	828 171 818
3	9	403 025 243
3	27	303 876 441
5	5	566 314 065
5	25	306 080 997
7	7	459 066 093
11	11	369 919 117
13	13	348 840 194

Ce tableau montre que si $d_K \in \{\pm 2^{29}, \pm 2^{30}\}$ alors le corps K est de signature $(1,4)$ ou $(3,3)$. Si $d_K = 3^{18}$ alors le corps K est de signature $(1,4)$. De même si $d_K = 5^{11}$ ou 5^{12} alors le corps K est nécessairement de signature $(1,4)$.

Lemme 3.6.7
Soit K un corps de nombres de degré 9, de signature $(5,2)$ et de discriminant $d_K = 7^{10}$. Si y est un entier de K de norme absolue a, alors :
$v_7(a) = 0$ *ou* $v_7(a) \geq 2$.

Ce lemme permet d'éliminer un nombre assez important de valeurs du terme constant a_9.

Cas où K est de signature (7,1) :

La contribution des corrections locales sans GRH donnent :

p	q	Minoration
2	2	4 679 375 344
2	4	2 660 850 796
2	8	1 705 336 411
2	16, 32	1 341 973 338
3	3	3 323 648 034
3	9	1 606 721 182
3	27	1 181 154 862
5	5	2 269 966 179
5	25	1 191 894 258
7	7	1 835 806 268
11	11	1 469 648 592
13	13	1 381 026 625

On remarque bien que cette signature ne peut être possible dans le cas de la ramification en 2. Si $d_K = -3^{19}$ alors K est de signature $(3,3)$.

Cas où K est totalement réel :

Ce cas est plus intéressant dans la mesure où on peut éliminer un grand nombre de discriminants. Mais avant cela, rappelons d'abord quelques résultats.
Le discriminant minimum pour un corps totalement réel imprimitif de degré 9 a été déterminé par F. Diaz y Diaz et M. Olivier **[12]**. Il s'agit du discriminant 16240385609, atteint pour une extension du corps cubique de discriminant 49. Le théorème suivant dû à K. Takeuchi **[28]** donne le discriminant minimum dans le cas général (primitif et imprimitif).

Théorème 3.6.8
La valeur minimale en valeur absolue prise par le discriminant d'un corps de nombres totalement réel de degré 9 est 9685993193. Le corps correspondant est unique à isomorphisme près; un polynôme générateur est :

$$x^9 - 9x^7 + 24x^5 + 2x^4 - 20x^3 - 3x^2 + 5x + 1.$$

Il s'agit d'un corps primitif de groupe de Galois T_{34}.

Le tableau ci-dessous donne les minorations des discriminants en degré 9 en tenant compte de la contribution des corrections locales de façon inconditionnelle.

p	q	Minoration
2	2	19 422 125 230
2	4	11 037 907 072
2	8	7 048 615 040
2	16, 32	5 553 588 743
3	3	13 792 616 428
3	9	6 632 556 137
3	27	4 775 745 111
5	5	9 410 697 938
5	25	4 826 869 699
7	7	7 596 741 549
11	11	6 050 186 436
13	13	5 669 479 611

Grâce à ces résultats, nous énonçons les propositions suivantes :

Proposition 3.6.9
Soit K un corps de nombres de degré 9 totalement réel.
Si K est ramifié seulement en 2 alors tout idéal premier $\wp$ de K au-dessus de 2 est de degré $f_\wp$ supérieur ou égal à 6.
Si $d_K = 3^{20}$ tout idéal premier $\wp$ de K au-dessus de 3 est de degré $f_\wp$ supérieur ou égal à 4.

Tout idéal premier $\wp$ de K au-dessus de 5 est de degré $f_\wp$ supérieur ou égal à 3.

Preuve :
Elle découle du tableau ci-dessus. □

On a le corollaire suivant :

Corollaire 3.6.10
Soit K un corps de nombres de degré 9 totalement réel. Si y est un entier de K de norme absolue a, alors :
i) $v_2(a) = 0$ *ou* $v_2(a) \geq 6$
iii) Si $d_K = 3^{20}$ *alors* $v_3(a) = 0$ *ou* $v_3(a) \geq 4$
iv) $v_5(a) = 0$ *ou* $v_2(a) \geq 3$.

On obtient des résultats analogues pour les autres signatures. Ceci permet de réduire de façon considérable les valeurs du terme constant a_9.

Proposition 3.6.11
Si K est ramifié seulement en 7 et totalement réel, alors son discriminant $d_K = 7^{12}$ ou 7^{14}.

L'étude menée dans ce paragraphe sur les discriminants se résume à travers le théorème suivant :

Théorème 3.6.12
Si K est un corps de nombres de degré 9 ramifié seulement en 2 alors son discriminant d_K ne peut prendre les valeurs $\pm 2^{25}$, $\pm 2^{26}$, -2^{27} et -2^{28}. De même si le corps K est ramifié seulement en 3 alors il est totalement ramifié et son discriminant d_K ne peut prendre la valeur 3^{16}. Si K est ramifié seulement en 5 alors il est nécessairement de signature $(1, 4)$.

Ces résultats permettent de réduire de façon assez considérable le nombre de polynômes à prendre en considération dans les programmes que nous allons mettre en place dans le chapitre suivant. La recherche numérique se montrant très coûteux en temps CPU, des astuces pour réduire les polynômes à étudier s'avèrent nécessaires si nous voulons les résultats de nos recherches numériques en temps raisonnable.

Chapitre 4

Tables et résultats

4.1 Commentaires

Des bornes pour les coefficients a_i des polynômes susceptibles d'engendrer les différents corps de nombres K ayant été déterminées, nous allons maintenant commencer nos recherches numériques. Les programmes mis en place ont été écrits en langage C ; nous avons utilisé le système de calcul Pari **[22]**. Il faut signaler que nos recherches portent au départ sur des milliards de polynômes. Des astuces pour accélérer le programme s'imposent si nous voulons avoir les résultats escomptés dans un délai acceptable. Nous avons remarqué que les polynômes sur lesquels nous menons nos recherches sont en général tous irréductibles, et pour cette raison nous évitons de faire intervenir le test d'irréductibilité au début dans le programme.

Les discriminants et les signatures des différents corps recherchés étant déjà fixés, on arrive dans une première étape à éliminer plus de la moitié des polynômes à étudier car n'ayant pas le bon signe du discriminant. Cette étape est très importante car elle nous fait gagner un temps considérable. La condition $d_{f_\theta} = d_K a^2$ (où $a = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$) permet d'éliminer tous les polynômes dont le discriminant d_{f_θ} n'a pas la bonne p-partie, et aussi tous les polynômes tels que le rapport $\frac{d_{f_\theta}}{d_K}$ n'est pas un carré parfait. Ces deux conditions sont très importantes car elles constituent un véritable "*filtre*" pour les polynômes ayant le bon signe du discriminant. En effet en degré 8, dans le cas de la ramification en 2 très peu de polynômes vérifient ces conditions (moins de 0.003%) et presqu'aucun dans le cas de la ramification en 5 ou en 7. En degré 9, moins de 0.005% de polynômes vérifient ces conditions dans le cas de la ramification en 3 et presqu'aucun pour $p = 2, 5$ ou 7.

A l'étape suivante, on impose maintenant la condition d'irréductibilité aux polynômes ayant traversé le "*filtre*", et ils sont pour la plupart irréductibles (avec en général un nombre important de polynômes d'Eisenstein).

A la suite de cette étape nous ne prenons en compte que les polynômes ayant vérifié le test du discriminant du corps. Il faut signaler que la valeur du discriminant du corps étant connue, nous l'imposons dans le programme afin d'écarter tous les corps dont le discriminant ne correspond pas à cette valeur. On remarque dans nos résultats que moins de 0.002% des polynômes ayant le bon discriminant vérifient ce test du discriminant du corps dans le cas de la ramification en 2 en degré 8 (resp. en 3 en degré 9). Nos calculs ne donnent aucun corps vérifiant ce test dans le cas de la ramification en 5 ou en 7 en degré 8 (resp. en 2, 5 ou 7 en degré 9).

Enfin pour terminer, on applique le test d'isomorphisme aux polynômes ayant vérifié tous ces tests imposés précédemment : il s'agit de tester si deux corps ayant le même discriminant sont $\mathbb{Q}$-isomorphes ou non. La commande spéciale mise en place dans Pari pour ce test est "polredabs". Une fois ce travail effectué, on calcule le groupe de Galois de la clôture galoisienne des différents corps obtenus. La commande spéciale utilisée alors est "polgalois".

Les étapes de l'algorithme :

Nous rappelons ici les grandes étapes de l'algorithme mis en place pour déterminer les différents corps.
Etape 1. On construit les polynômes f_θ susceptibles d'engendrer les corps de nombres fixés en donnant les différentes valeurs obtenues des coefficients a_i.
Etape 2. En fixant la signature du corps, on calcule dans cette deuxième étape le discriminant d_{f_θ} du polynôme.
Etape 3. On teste si le discriminant du polynôme vérifie la relation $d_{f_\theta} = d_K a^2$. On fait intervenir ici la notion de valuation du discriminant en un unique premier p.
Etape 4. On teste l'irréductibilité du polynôme f_θ.
Etape 5. Dans cette dernière étape, on garde les polynômes f_θ donnant la valeur fixée du discriminant du corps.

L'ordre de ces vérifications est primordial, car ces tests vont être répétés un grand nombre de fois; il permet ainsi d'accélérer nos programmes mis en place.

4.2 Résultats

La grande partie de notre étude est consacrée à la recherche numériques des corps en question. Après environ huit mois de calcul pour chaque degré sur les machines "entiers" et "node" à l'université de Bordeaux 1, nous obtenons tous nos résultats. Nous donnons à travers les tables qui suivent ces différents résultats : on choisit parmi les polynômes générateurs f_θ du même corps de nombres de degré 8 (resp. de degré 9), celui donnant le plus petit indice de $\mathbb{Z}[\theta]$ dans l'anneau $\mathbb{Z}_K$ des entiers pour représenter le corps de nombres K.

4.2.1 Résultats numériques en degré 8

À isomorphisme près, on obtient 38 différents corps de nombres et 14 différents groupes de Galois de degré 8. Tous les corps obtenus sont ramifiés seulement en 2. La recherche numérique montre que la ramification seulement en 7 n'est pas possible. Nous avons montré dans le chapitre 2 que sous G.R.H la ramification en 5 n'est pas possible. La recherche numérique sans G.R.H montre aussi qu'il n'existe pas de corps de nombres de degré 8 ramifiés seulement en 5. Les tables qui suivent donnent en détail les résultats de nos recherches numériques des corps de degré 8. On note a l'indice de $\mathbb{Z}[\theta]$ dans l'anneau $\mathbb{Z}_K$. L'utilisation de Pari permet de donner d'autres polynômes générateurs et aussi une base d'entiers du corps K.

$d_K = 2^{22}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 + 6x^4 + 1$	$(0, 4)$	T_4^+	128

$d_K = 2^{24}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 + 1$	$(0, 4)$	T_2^+	1
$x^8 + 4x^6 + 8x^4 + 4x^2 + 1$	$(0, 4)$	T_4^+	9

$d_K = 2^{25}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 - 4x^6 + 6x^4 - 4x^2 + 2$	$(0, 4)$	T_{21}	1

$d_K = 2^{26}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 - 4x^6 - 2x^4 - 4x^2 + 1$	$(4, 2)$	T_{10}^+	128
$x^8 + 4x^6 - 2x^4 + 4x^2 + 1$	$(0, 4)$	T_{10}^+	128
$x^8 + 4x^4 - 4x^2 + 1$	$(0, 4)$	T_{19}^+	1

$d_K = 2^{27}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 + 2x^4 + 2$	$(0, 4)$	T_{17}	1
$x^8 - 2x^4 + 2$	$(0, 4)$	T_{17}	1
$x^8 - 4x^6 + 10x^4 - 8x^2 + 2$	$(0, 4)$	T_6	1

$d_K = \pm 2^{28}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 - 4x^6 - 2x^4 + 12x^2 + 1$	$(4, 2)$	T_{20}^+	128
$x^8 + 4x^6 - 2x^4 - 12x^2 + 1$	$(4, 2)$	T_{20}^+	128
$x^8 - 6x^4 - 8x^2 - 1$	$(2, 3)$	T_6	25
$x^8 - 2x^4 - 1$	$(2, 3)$	T_8	1
$x^8 + 2x^4 - 1$	$(2, 3)$	T_8	1
$x^8 - 4x^6 + 10x^4 + 4x^2 + 1$	$(0, 4)$	T_{19}^+	128

$d_K = \pm 2^{29}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 - 4x^6 + 8x^4 - 8x^2 + 2$	$(4, 2)$	T_{28}	1
$x^8 + 4x^6 + 8x^4 + 8x^2 + 2$	$(0, 4)$	T_{28}	1
$x^8 - 4x^6 + 4x^4 - 2$	$(2, 3)$	T_{30}	1
$x^8 + 4x^6 + 4x^4 - 2$	$(2, 3)$	T_{30}	1

$d_K = -2^{30}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 - 4x^6 + 2x^4 + 4x^2 - 1$	$(6, 1)$	T_{27}	1
$x^8 + 4x^6 + 2x^4 - 4x^2 - 1$	$(2, 3)$	T_{27}	1
$x^8 - 4x^6 + 6x^4 - 4x^2 - 1$	$(2, 3)$	T_{30}	1
$x^8 + 4x^6 + 6x^4 + 4x^2 - 1$	$(2, 3)$	T_{30}	1

$d_K = \pm 2^{31}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^8 - 8x^4 + 8x^2 - 2$	$(6,1)$	T_{27}	1
$x^8 - 8x^4 - 8x^2 - 2$	$(2,3)$	T_{27}	1
$x^8 - 2$	$(2,3)$	T_8	1
$x^8 + 8x^4 - 2$	$(2,3)$	T_6	81
$x^8 + 2$	$(0,4)$	T_6	1
$x^8 + 8x^6 + 20x^4 + 16x^2 + 2$	$(0,4)$	T_1	1
$x^8 - 8x^6 + 20x^4 - 16x^2 + 2$	$(8,0)$	T_1	1
$x^8 - 4x^4 + 2$	$(4,2)$	T_{16}	1
$x^8 + 4x^4 + 2$	$(0,4)$	T_{16}	1
$x^8 + 8x^6 + 24x^4 + 32x^2 + 18$	$(0,4)$	T_{17}	3
$x^8 - 8x^6 + 24x^4 - 32x^2 + 18$	$(0,4)$	T_{17}	3
$x^8 + 8x^6 - 12x^4 + 2$	$(4,2)$	T_7	289
$x^8 - 4x^4 - 8x^2 + 2$	$(4,2)$	T_{28}	81
$x^8 - 4x^4 + 8x^2 + 2$	$(0,4)$	T_{28}	81

À la lecture des tables, on remarque que certains discriminants ne peuvent être réalisés. Les groupes de Galois obtenus sont tous résolubles, et même tous imprimitifs. Ce résultat nous amène à énoncer le théorème suivant :

Théorème 4.2.1
Il n'existe pas de corps de nombres primitif de degré 8 ramifié seulement en p, pour $p = 2, 3, 5$ et 7.

4.2.2 Résultats numériques en degré 9

À isomorphisme près, on obtient 13 différents corps de nombres et 8 différents groupes de Galois de degré 9. Tous les corps obtenus sont ramifiés seulement en 3. La recherche numérique montre que la ramification seulement en 7 n'est pas possible. Nous avons montré dans le chapitre 2 que sous G.R.H la ramification seulement en 5 des corps de nombres de degré 9 n'est pas possible. La recherche numérique sans G.R.H aboutit aussi à ce même résultat. Les tables qui suivent donnent en détail les résultats de nos recherches numériques des corps de degré 9. On note a l'indice de $\mathbb{Z}[\theta]$ dans l'anneau $\mathbb{Z}_K$. L'utilisation de Pari permet de donner d'autres polynômes générateurs et aussi une base d'entiers du corps K.

$d_K = -3^{19}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^9 - 3x^6 - 6x^3 - 1$	$(3,3)$	T_4	81

$d_K = -3^{21}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^9 - 3x^6 + 1$	$(3,3)$	T_{13}	1

$d_K = 3^{22}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^9 - 6x^6 + 12x^3 + 1$	$(1,4)$	T_{11}^+	81
$x^9 - 9x^7 + 27x^5 - 30x^3 + 9x - 1$	$(9,0)$	T_1^+	1

$d_K = -3^{23}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^9 - 6x^6 + 9x^3 - 3$	$(3,3)$	T_{22}	1
$x^9 - 3x^6 + 3$	$(3,3)$	T_{22}	1
$x^9 - 3x^6 - 9x^3 + 3$	$(3,3)$	T_{22}	512

$d_K = -3^{25}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^9 - 9x^7 - 3x^6 + 27x^5 + 18x^4 - 24x^3 - 27x^2 - 9x + 23$	$(3,3)$	T_{20}	2560
$x^9 - 9x^7 - 6x^6 + 27x^5 + 36x^4 - 24x^3 - 54x^2 - 9x + 22$	$(3,3)$	T_{20}	64
$x^9 - 9x^7 - 3x^6 + 27x^5 + 18x^4 - 15x^3 - 27x^2 - 36x - 4$	$(3,3)$	T_{20}	1024

$d_K = 3^{26}$

polynômes $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$	a
$x^9 - 9x^6 + 27x^3 - 3$	$(1,4)$	T_3^+	512
$x^9 - 3$	$(1,4)$	T_{10}^+	1
$x^9 - 9x^6 + 27x^3 - 24$	$(1,4)$	T_{10}^+	8

À la lecture des tables, on remarque que certains discriminants ne peuvent être réalisés. Les groupes de Galois obtenus sont tous résolubles, et même tous imprimitifs. Ce résultat nous amène à énoncer le théorème suivant :

Théorème 4.2.2

Il n'existe pas de corps de nombres primitif de degré 9 ramifié seulement en p, pour $p = 2, 3, 5$ et 7.

4.3 Conclusion

Les travaux de J. Jones **[17]** ont montré qu'il n'existe pas de corps de nombres de degré 5 ou de degré 6 ramifiés en un unique premier petit et de groupe de Galois non résoluble.

Dans le cas du degré 7, S. Brueggeman **[1]** a montré aussi que de tels corps de nombres ne peuvent exister. En nous inspirant des travaux des auteurs précédents, nous avons mené l'étude dans le cas des corps de nombres de degré 8 et de degré 9. Au terme de notre étude, nous arrivons au même résultat que précédemment. Nous pouvons donc affirmer que la conjecture de B. Gross **[15]** relative à l'existence de corps de nombres de degré n ramifiés en un unique premier $p < 11$ et ayant un groupe de Galois non résoluble n'est pas vérifiée pour $n \leq 9$. Le théorème suivant résume les résultats de nos recherches.

Théorème 4.3.1
Soit K un corps de nombres de degré $n \leq 9$ et ramifié en un unique premier $p < 11$. Alors le groupe de Galois de sa clôture galoisienne est résoluble.

Il serait assez intéressant de poursuivre cette étude dans le cas des degrés $n \geq 10$ mais malheureusement la méthode que nous avons utilisée devient moins efficace au niveau de la recherche numérique car très coûteuse en temps CPU pour être raisonnablement faite. Pour ces degrés, les coefficients a_i du polynômes générateur f_θ explosent très rapidement !

On remarque particulièrement que la méthode développée dans cette thèse ne suffit pas pour résoudre entièrement le cas du degré 10 car les groupes de Galois non résolubles ne sont pas tous primitifs. Les résultats de cette remarque sont donnés en Annexe A. Ceci montre bien les limites de ladite méthode dans le cas où le degré n est supérieur ou égal à 10.

Bibliographie

[1] S. Brueggeman, Septic Number Fields Which are Ramified Only at One Small Prime. Departement of Mathematics. The Ohio State University, Columbus, Ohio 43210, USA.
J. Symbolic Computation (2001) **31**, 549 – 555
doi : 10.1006/jsco. 2001.0440.
http ://www.idealibrary.com on **IDE.**

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

[3] G. Butler et J. Mckay, The transitive groups of degree up to eleven. Comm. Algebra, **11(8)** : 863 – 911, 1983.

[4] H. Cohen, A Course in Computational Algebraic Number Theory. Berlin, Springer-Verlag (1993).

[5] H. Cohen, Advanced Topics in Computational Number Theory. New York, Springer-Verlag (2000).

[6] H. Cohen, F. Diaz Y Diaz et M. Olivier, Imprimitive octic fields with small discriminants. Université Bordeaux 1, laboratoire $A2X$, 351 Cours de la Libération, 33405 Talence, France.

[7] R. Descombes, Eléments de théorie des nombres. PUF, 1986.

[8] F. Diaz Y Diaz, Tables minorant la racine n-ième du discriminant d'un corps de nombres de degré n. Publications Mathématiques d'Orsay **80.06**, 1980..

[9] F. Diaz Y Diaz, Petits discriminants des corps de nombres totalement imaginaires de degré 8. Journal of Number Theory **25**, 34 – 52 (1987).

[10] F. Diaz Y Diaz, Discriminant minimal et petits discriminants des corps de nombres de degré 7 avec cinq places réelles. J. London Math. Soc.**(2) 38**, (1988)33 – 46.

[11] F. Diaz Y Diaz, J. Martinet et M. Pohst, The minimum discriminant of totally real octic fields. Journal of Number Theory **36**, 145 – 159 (1990).

[12] F. Diaz Y Diaz et M. Olivier, Imprimitive octic fields with small discriminants. Mathematics of computation, volume **64**, number 209, January 1995, page 305 – 321.

[13] Y. Eichenlaub, Problèmes effectifs de théorie de Galois en degré 8 à 11. Thèse soutenue à l'université de Bordeaux 1, 1996.

[14] I. Gozard, Théorie de Galois. Ellipses (1997).

[15] B. Gross, Modular forms (mod p) and galois representation. Internat. Math. Res. Notices, **16**, 865 – 875 (1998).

[16] D. Harbater, Galois groups with prescribed ramification. Contemporary Mathematics, Volume **174**, 1994.

[17] J. Jones, Table of number fields with prescribed ramification, (1998). **http ://math.la.asu.edu./˜ jj/numberfields.**

[18] J. Jones, D. Roberts, Timming analysis for targeted hunter searches. In Buhler, J. P., ed., Algorithmic Number Theory (ANTS-III). LNCS **1423**, pp. $412-423$. Springer-Verlag (1998).

[19] J. Jones, D. Roberts, Sextic number fields with discriminant $(-1)^j 2^a 3^b$. In Number Theory : Fifth Conference of the Canadian Number Theory Association, CRM Proceedings and Lecture Notes, **19**, pp. $141-172$. American Mathematical Society (1999).

[20] J. Kluners et G. Malle, **http ://www.mathematik.univ.kassel.de/Malle/minimum/database/node** 13.

[21] J. Martinet, Petits discriminants des corps de nombres. London Mathematical Society Lecture Note Series **56** pp. $151-193$.

[22] PARI/GP, version 2.1.5, Bordeaux, 2004, 2005, **http ://pari.math.u-bordeaux1.fr/**.

[23] M. Pohst, On the computation of number fields of small discriminants including the mininum discriminants of sixth degree fields. J. Number Theory , **14**, $99-117$ (1982).

[24] G. Poitou, Sur les petits discriminants. Seminaire Delange-Pisot-Poitou, **18**, $6-01-6-18$ (1976).

[25] S. Selmane, Odlyzko-Poitou-Serre lower bounds for discriminants for number fields. Maghreb Math. Rev., Vol. **8** No 18.2 (1999).

[26] J.P. Serre, Corps locaux. Hermann, Paris, (1962).

[27] J.P. Serre, Oeuvres, vol. 3. Springer-Verlag, Berlin/New York, 1986.

[28] K. Takeuchi, Totally real algebraic number fields of degree 9 with small discriminants. Saitama Math. J. Vol. **17** (1999), $63-85$.

[29] J. Tate, The non-existence of certain Galois extension of $\mathbb{Q}$ unramified outside 2. Contemp. Math. **174** (1994) $153-156$.

[30] R. Thompson, On the possible forms of discriminants of algebraic fields I. American J. of Mathematics (**53**) 1931 pp. $81-90$.

[31] R. Thompson, On the possible forms of discriminants of algebraic fields II. American J. of Mathematics (**55**) 1933 pp. $110-118$.

Annexe A

Les groupes transitifs

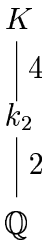
A.1 En degré 8

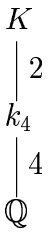
Groupes G	Ordres	Parité	$K \supset k_4$	$K \supset k_2$
T_1	8		oui	oui
T_2	8	+	oui	oui
T_3	8	+	oui	oui
T_4	8	+	oui	oui
T_5	8	+	oui	oui
T_6	16		oui	oui
T_7	16		oui	oui
T_8	16		oui	oui
T_9	16	+	oui	oui
T_{10}	16	+	oui	oui
T_{11}	16	+	oui	oui
T_{12}	24	+	oui	oui
T_{13}	24	+	oui	oui
T_{14}	24	+	oui	oui
T_{15}	32		oui	oui
T_{16}	32		oui	oui
T_{17}	32		oui	oui
T_{18}	32	+	oui	oui
T_{19}	32	+	oui	oui
T_{20}	32	+	oui	oui
T_{21}	32		oui	oui
T_{22}	32	+	oui	oui
T_{23}	48		oui	non
T_{24}	48	+	oui	oui
T_{25}	56	+	non	non

Groupes G	Ordres	Parité	$K \supset k_4$	$K \supset k_2$
T_{26}	64		oui	oui
T_{27}	64		oui	oui
T_{28}	64		oui	oui
T_{29}	64	+	oui	oui
T_{30}	64		oui	oui
T_{31}	64		oui	oui
T_{32}	96	+	oui	non
T_{33}	96	+	non	oui
T_{34}	96	+	non	oui
T_{35}	128		oui	oui
T_{36}	168	+	non	non
T_{37}	168	+	non	non
T_{38}	192		oui	non
T_{39}	192	+	oui	non
T_{40}	192		oui	non
T_{41}	192	+	non	oui
T_{42}	288	+	non	oui
T_{43}	336		non	non
T_{44}	384		oui	non
T_{45}	576	+	non	oui
T_{46}	576		non	oui
T_{47}	1152		non	oui
T_{48}	1344	+	non	non
T_{49}	20160	+	non	non
T_{50}	40320		non	non

Dans les tableaux ci-dessus, K désigne un corps de nombres de degré 8, k_2 un sous-corps quadratique, k_4 un sous-corps quartique et G le groupe de Galois de la clôture galoisienne de K. On

utilise le symbôle "+" pour indiquer que le groupe est pair.





Groupes de Galois de degré 8 non résolubles :

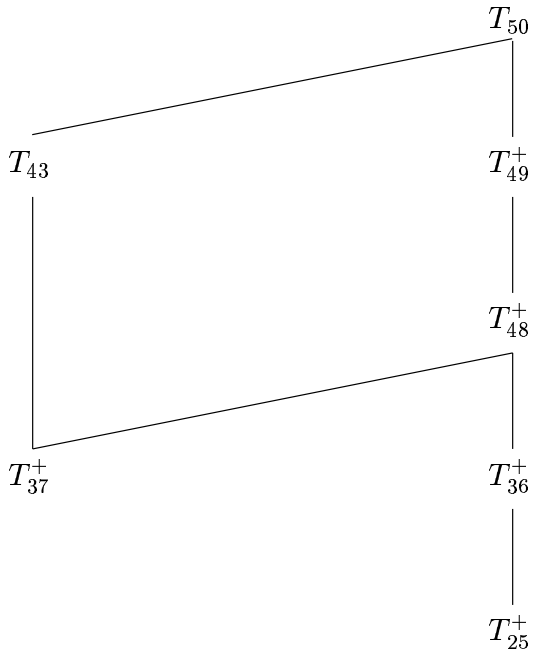
$$T_{37}^+, T_{43}, T_{48}^+, T_{49}^+ \text{ et } T_{50}.$$

Groupes de Galois primitifs de degré 8 :

$$T_{25}^+, T_{36}^+, T_{37}^+, T_{43}, T_{48}^+, T_{49}^+ \text{ et } T_{50}.$$

On remarque bien que tous les groupes de Galois non résolubles sont primitifs.

Graphe des inclusions des sous-groupes de Galois primitifs de degré 8 **:**

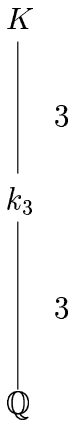


A.2 En degré 9

Groupes G	Ordres	Parité	$K \supset k_3$
T_1	9	+	oui
T_2	9	+	oui
T_3	18	+	oui
T_4	18		oui
T_5	18	+	oui
T_6	27	+	oui
T_7	27	+	oui
T_8	36		oui
T_9	36	+	non
T_{10}	54	+	oui
T_{11}	54	+	oui
T_{12}	54		oui
T_{13}	54		oui
T_{14}	72	+	non
T_{15}	72		non
T_{16}	72		non
T_{17}	81	+	oui

Groupes G	Ordres	Parité	$K \supset k_3$
T_{18}	108		oui
T_{19}	144		non
T_{20}	162		oui
T_{21}	162	+	oui
T_{22}	162		oui
T_{23}	216	+	non
T_{24}	324		oui
T_{25}	324	+	oui
T_{26}	432		non
T_{27}	504	+	non
T_{28}	648		oui
T_{29}	648		oui
T_{30}	648	+	oui
T_{31}	1296		oui
T_{32}	1512	+	non
T_{33}	181440	+	non
T_{34}	362880		non

Dans les tableaux ci-dessus, K désigne un corps de nombres de degré 9, k_3 un sous-corps cubic et G le groupe de Galois de la clôture galoisienne de K.



Groupes de Galois de degré 9 non résolubles :

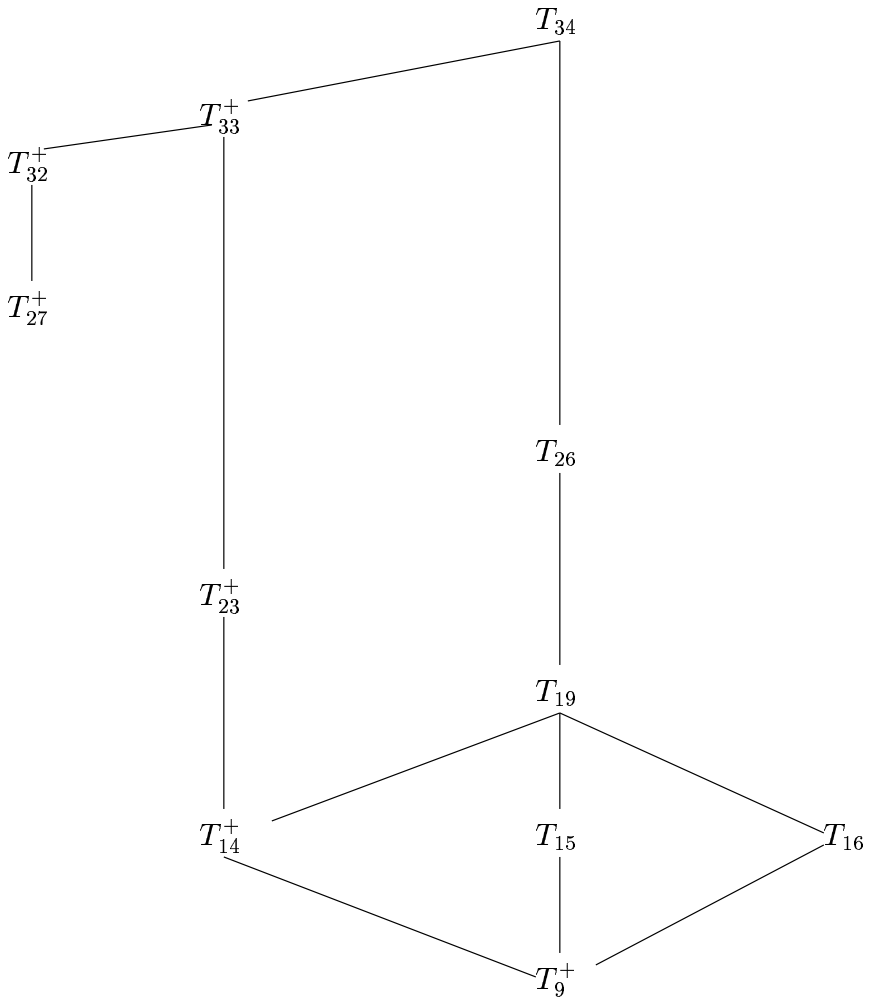
$$T_{27}^+, T_{32}^+, T_{33}^+ \text{ et } T_{34}.$$

Groupes de Galois primitifs de degré 9 :

$$T_9^+, T_{14}^+, T_{15}, T_{16}, T_{19}, T_{23}^+, T_{26}, T_{27}^+, T_{32}^+, T_{33}^+ \text{ et } T_{34}.$$

On remarque aussi que tous les groupes de Galois non résolubles sont primitifs.

Graphe des inclusions des groupes de Galois primitifs de degré 9 :

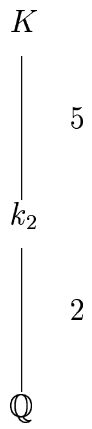


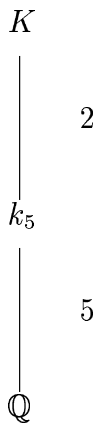
A.3 En degré 10

Groupes G	Ordres	Parité	$K \supset k_5$	$K \supset k_2$
T_1	10		oui	oui
T_2	10		oui	oui
T_3	20		oui	oui
T_4	20		oui	oui
T_5	40		oui	oui
T_6	50		non	oui
T_7	60	+	non	non
T_8	80	+	oui	non
T_9	100		non	oui
T_{10}	100		non	oui
T_{11}	120		oui	oui
T_{12}	120		oui	oui
T_{13}	120		non	non
T_{14}	160		non	oui
T_{15}	160	+	oui	non
T_{16}	160		oui	non
T_{17}	200		non	oui
T_{18}	200	+	non	oui
T_{19}	200		non	oui
T_{20}	200		non	oui
T_{21}	200		non	oui
T_{22}	240		oui	oui
T_{23}	320	+	oui	non

Groupes G	Ordres	Parité	$K \supset k_5$	$K \supset k_2$
T_{24}	320	+	oui	non
T_{25}	320		oui	non
T_{26}	360	+	non	non
T_{27}	400		non	oui
T_{28}	400	+	non	oui
T_{29}	640		oui	non
T_{30}	720		non	non
T_{31}	720	+	non	non
T_{32}	720		non	non
T_{33}	800		non	oui
T_{34}	960	+	oui	non
T_{35}	1440		non	non
T_{36}	1920		oui	non
T_{37}	1920	+	oui	non
T_{38}	1920		oui	non
T_{39}	3840		oui	non
T_{40}	7200		non	oui
T_{41}	14400		non	oui
T_{42}	14400	+	non	oui
T_{43}	28800		non	oui
T_{44}	1814400	+	non	non
T_{45}	3628800		non	non

Dans les tableaux ci-dessus, K désigne un corps de nombres de degré 10, k_2 un sous-corps quadratique, k_5 un sous-corps de degré 5 et G le groupe de Galois de la clôture galoisienne de K.





Groupes de Galois non résolubles en degré 10 :

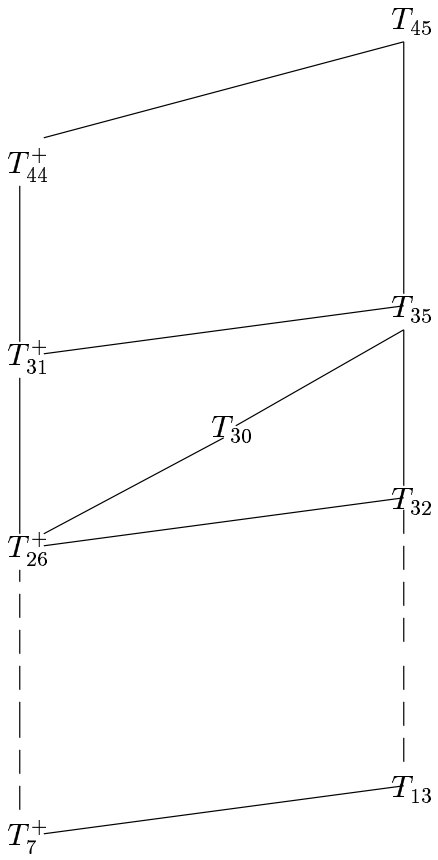
$T_7^+, T_{11}, T_{12}, T_{13}, T_{22}, T_{26}^+, T_{30}, T_{31}^+, T_{32}, T_{34}^+, T_{35}, T_{36}, T_{37}^+, T_{38}, T_{39}, T_{40}, T_{41}, T_{42}^+, T_{43}, T_{44}^+$ et T_{45}.

Groupes de Galois primitifs de degré 10 :

$$T_7^+, T_{13}, T_{26}^+, T_{30}, T_{31}^+, T_{32}, T_{35}, T_{44}^+ \text{ et } T_{45}.$$

Contrairement aux deux cas précédents, on remarque ici que tous les groupes de Galois primitifs sont non résolubles. Mais par contre, on constate qu'il existe des groupes de Galois non résolubles qui ne sont pas primitifs.
Les groupes de Galois non résolubles pour lesquels le corps K est une extension quadratique d'un sous-corps quintique k_5 sont : $T_{11}, T_{12}, T_{22}, T_{34}, T_{36}, T_{37}^+, T_{38}$ et T_{39}.
Les groupes de Galois non résolubles pour lesquels le corps K est une extension de degré 5 d'un sous-corps quadratique k_2 sont : $T_{11}, T_{12}, T_{22}, T_{40}, T_{41}, T_{42}^+$ et T_{43}.

Graphe des inclusions des groupes de Galois primitifs de degré 10 **:**



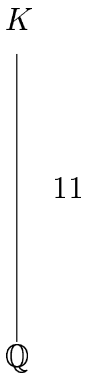
Inclusions non directes :

$$T_{32}/T_{13} \text{ et } T_{26}^+/T_7^+.$$

A.4 En degré 11

Groupes G	Ordres	Parité
T_1	11	+
T_2	22	
T_3	55	+
T_4	110	
T_5	660	+
T_6	7920	+
T_7	$(\frac{1}{2})11!$	+
T_8	11!	

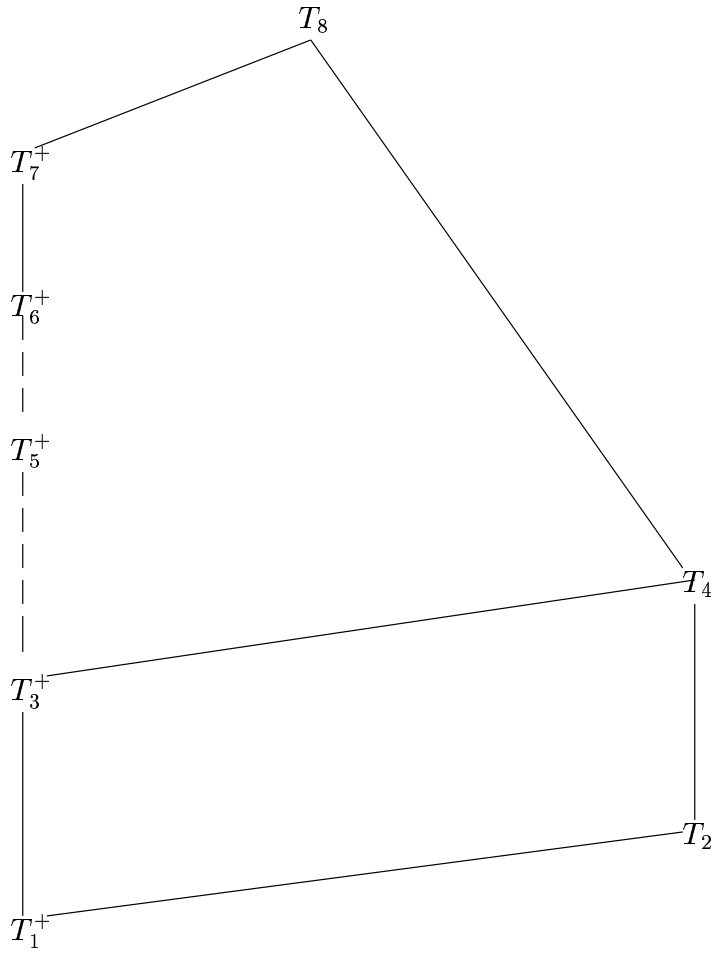
Dans le tableau ci-dessus, K désigne un corps de nombres de degré 11. Les corps de nombres K en question sont tous primitifs.



Groupes de Galois de degré 11 non résolubles :

$$T_5, T_6, T_7^+ \text{ et } T_8.$$

Graphe des inclusions des groupes de Galois de degré 11 **:**



Inclusions non directes :

$$T_6^+/T_5^+ \text{ et } T_5^+/T_3^+.$$

Annexe B

Tables des minorations des discriminants de corps de nombres avec corrections locales

Dans les tableaux suivants, on donne des minorations des valeurs absolues des discriminants sous l'hypothèse que ce corps contienne un idéal premier de norme indiquée avec ou sans G.R.H. Le cas "Sans" correspond aux valeurs des minorations sans corrections locales et r_1 désigne le nombre de places réelles.

B.1 En degré 7

$r_1 = 1$

Normes	Sous G.R.H	Sans G.R.H
Sans	177 523	161 815
2	579 113	501 984
4	331 477	287 038
8,16	222 826	197 864
3	412 579	357 155
9	204 690	183 287
5	284 955	246 473
7	231 950	203 548
11	190 493	173 001

$r_1 = 3$

Normes	Sous G.R.H	Sans G.R.H
Sans	579 508	508 757
2	2 063 528	1 703 785
4	1 178 349	972 420
8,16	813 084	678 911
3	1 468 393	1 211 545
9	716 695	608 519
5	1 009 387	833 090
7	819 992	682 829
11	657 749	567 939

$r_1 = 5$

Normes	Sous G.R.H	Sans G.R.H
Sans	2 032 227	1 702 525
2	7 834 382	6 101 052
4	4 467 574	3 477 291
8,16	3 187 488	2 474 956
3	5 570 643	4 336 562
9	2 690 366	2 145 635
5	3 815 532	2 974 198
7	3 093 048	2 424 966
11	2 447 559	1 986 692

$r_1 = 7$

Normes	Sous G.R.H	Sans G.R.H
Sans	7 611 004	6 024 813
2	31 512 798	22 911 544
4	17 950 357	13 044 622
8,16	13 270 850	9 489 089
3	22 396 983	16 279 941
9	10 733 502	7 967 687
5	15 300 987	11 143 859
7	12 365 406	9 051 399
11	9 712 280	7 335 183

B.2 En degré 8

$r_1 = 0$

Normes	Sous G.R.H	Sans G.R.H
Sans	1 174 862	1 052 302
2	3 982 120	3 369 529
4	2 276 712	1 926 221
8,32	1 477 923	1 281 382
3	2 835 493	2 397 211
9	1 396 063	1 221 237
5	1 954 403	1 653 297
7	1 589 376	1 362 411
11	1 290 742	1 146 560

$r_1 = 2$

Normes	Sous G.R.H	Sans G.R.H
Sans	3 957 866	3 403 708
2	14 549 091	11 725 967
4	8 303 321	6 688 612
8,32	5 347 417	4 404 589
3	10 349 684	8 336 756
9	5 029 339	4 160 403
5	7 104 060	5 726 303
25	3 964 454	3 425 371
7	5 767 138	4 682 936
11	4 598 215	3 869 548

$r_1 = 4$

Normes	Sous G.R.H	Sans G.R.H
Sans	14 252 378	11 660 853
2	56 418 857	42 765 062
4	32 160 483	24 363 905
8,32	20 731 327	16 023 170
3	40 109 239	30 393 088
9	19 315 119	14 972 969
5	27 445 073	20 829 067
25	14 393 415	11 852 202
7	22 226 635	16 957 037
11	17 533 637	13 831 813

$r_1 = 6$

Normes	Sous G.R.H	Sans G.R.H
Sans	54 578 395	42 071 532
2	231 027 708	163 060 305
4	131 552 095	92 810 025
8,32	85 275 143	61 237 254
16	71 142 011	52 183 744
3	164 181 558	115 852 633
9	78 514 952	56 528 978
5	112 092 169	79 259 652
25	55 974 938	43 337 703
7	90 488 352	64 309 209
11	70 957 234	51 958 143

$r_1 = 8$

Normes	Sous G.R.H	Sans G.R.H
Sans	221 081 193	158 960 873
2	994 069 586	646 843 393
4	565 425 881	367 892 054
8,32	370 218 652	244 247 200
16	313 114 263	208 609 666
3	706 280 884	459 467 032
9	335 795 458	222 553 178
5	481 468 126	313 918 266
25	231 479 421	166 284 241
7	387 431 755	254 051 972
11	302 671 160	203 776 133

B.3 En degré 9

$r_1 = 1$

Normes	Sous G.R.H	Sans G.R.H
Sans	27 336 198	23 007 468
2	103 415 809	81 295 503
4	58 993 192	46 348 905
8	37 903 228	30 249 458
16, 32	28 894 944	24 397 331
3	73 547 113	57 789 564
9	35 611 093	28 685 778
27	27 384 664	23 162 204
5	50 420 440	39 657 567
25	27 444 772	23 235 622
7	40 901 188	32 371 194
11	32 461 075	26 604 281
13	30 521 075	25 351 143

$r_1 = 3$

Normes	Sous G.R.H	Sans G.R.H
Sans	100 826 742	80 499 455
2	408 896 565	301 476 861
4	233 000 135	171 694 369
8	148 878 228	111 192 502
16, 32	111 152 277	88 341 844
3	290 649 571	214 235 487
9	139 615 164	105 151 850
27	101 755 234	81 777 838
5	198 712 762	146 723 989
25	102 315 643	82 205 903
7	160 763 465	119 294 245
11	126 516 059	96 946 913
13	118 084 813	91 837 308

$r_1 = 5$

Normes	Sous G.R.H	Sans G.R.H
Sans	394 044 797	295 584 269
2	1 702 316 508	1 165 733 328
4	969 002 763	663 330 211
8	616 204 541	427 071 142
16, 32	456 946 740	336 805 639
3	1 209 671 082	828 171 818
9	577 374 510	403 025 243
27	403 094 446	303 876 441
5	825 432 210	566 314 065
25	406 743 930	306 080 997
7	665 653 806	459 066 093
11	521 276 677	369 919 117
13	484 054 703	348 840 194

$r_1 = 7$

Normes	Sous G.R.H	Sans G.R.H
Sans	1 624 004 131	1 133 345 245
2	7 429 487 899	4 679 375 344
4	4 224 562 286	2 660 850 796
8	2 675 012 621	1 705 336 411
16, 32	1 989 763 412	1 341 973 338
3	5 278 216 390	3 323 648 034
9	2 505 505 269	1 606 721 182
27	1 691 823 903	1 181 154 862
5	3 596 905 746	2 269 966 179
25	1 712 660 012	1 191 894 258
7	2 891 853 456	1 835 806 268
11	2 257 145 378	1 469 648 592
13	2 088 578 822	1 381 026 625

$r_1 = 9$

Normes	Sous G.R.H	Sans G.R.H
Sans	7 026 037 714	4 516 673 541
2	33 855 860 645	19 422 125 230
4	19 232 807 627	11 037 907 072
8	12 132 809 631	7 048 615 040
16, 32	9 107 161 514	5 553 588 743
3	24 045 270 132	12 792 616 428
9	11 358 116 411	6 632 556 137
27	7 475 603 559	4 775 745 111
5	16 371 452 597	9 410 697 938
25	7 588 771 600	4 826 869 699
7	13 128 739 277	7 596 741 549
11	10 219 961 472	6 050 186 436
13	9 433 946 286	5 669 479 611
17	8 460 451 744	5 218 144 751

B.4 En degré 10

$r_1 = 0$

Normes	Sous G.R.H	Sans G.R.H
Sans	190 6638 83	156 914 890
2	740 426 539	567 293 498
4	422 205 776	323 292 357
8	270 711 490	210 342 194
16	204 013 840	167 315 382
3	526 465 800	403 212 252
9	254 137 136	199 244 537
27	191 394 867	158 469 056
5	360 539 227	276 482 027
25	192 039 183	159 097 773
7	292 227 407	225 326 599
11	231 100 600	184 343 302
13	216 652 665	175 238 619
17	201 305 572	165 591 519

$r_1 = 2$

Normes	Sous G.R.H	Sans G.R.H
Sans	718 803 925	559 597 103
2	2 980 613 031	2 136 241 097
4	1 697 854 424	1 216 227 849
8	1 083 093 771	785 917 566
16	797 858 884	612 742 365
3	2 118 414 413	1 517 906 031
9	1 015 327 688	742 632 841
27	728 419 086	570 817 409
5	1 447 294 935	1 038 973 400
25	733 338 150	574 232 812
7	1 169 678 719	843 790 455
11	918 756 440	683 523 067
13	855 889 837	646 382 134
17	784 697 517	605 131 856

$r_1 = 4$

Normes	Sous G.R.H	Sans G.R.H
Sans	2 862 348 932	2 088 070 162
2	12 601 769 759	8 368 219 605
4	7 170 867 388	4 760 575 727
8	4 553 806 893	3 060 049 825
16	3 302 214 317	2 348 646 396
3	8 954 258 943	5 944 584 603
9	4 266 295 554	2 886 094 070
27	2 944 353 793	2 156 454 132
5	6 107 197 047	4 063 229 959
25	2 974 244 636	2 173 500 758
7	4 920 215 652	3 291 028 528
11	3 848 653 623	2 645 746 264
13	3 569 385 711	2 491 832 782
17	3 239 439 525	2 315 406 950

$r_1 = 6$

Normes	Sous G.R.H	Sans G.R.H
Sans	11 987 990 462	8 115 526 398
2	55 737 261 086	33 963 988 326
4	31 684 080 429	19 309 484 505
8	20 039 430 064	12 360 386 570
16	14 373 721 674	9 369 713 899
3	39 594 812 715	24 122 383 952
9	18 767 216 112	11 640 607 782
27	12 566 954 734	8 497 375 213
5	26 974 529 535	16 469 538 205
25	12 733 072 445	8 579 262 582
7	21 669 637 402	13 311 273 832
11	16 899 675 558	10 637 690 795
13	15 624 929 011	9 986 739 884
17	14 072 608 176	9 223 907 327

$r_1 = 8$

Normes	Sous G.R.H	Sans G.R.H
Sans	52 587 162 637	32 716 460 257
2	256 953 999 072	142 309 471 117
4	145 935 780 488	80 864 912 511
8	91 974 989 703	51 590 490 567
16	65 449 889 461	38 719 289 018
3	182 478 812 038	101 056 293 132
9	86 086 961 948	48 529 248 771
27	56 314 478 103	34 750 385 085
5	124 216 754 266	68 932 900 841
25	57 207 781 730	35 138 033 732
7	99 552 057 759	55 619 147 085
11	77 441 418 970	44 236 815 013
13	71 448 258 146	41 423 005 626
17	63 981 042 810	38 072 174 744

$r_1 = 10$

Normes	Sous G.R.H	Sans G.R.H
Sans	240 678 113 824	136 283 580 755
2	1 230 495 953 669 102	613 589 454 748
4	698 345 783 618	348 510 760 012
8	438 792 999 213	221 737 878 999
16	310 365 182 346	165 066 518 589
3	873 595 261 507	435 659 433 146
9	410 420 276 724	208 381 740 887
27	263 599 785 878	146 849 343 591
5	594 257 715 290	296 948 683 359
25	268 371 215 704	148 680 767 372
7	475 394 440 096	239 262 416 755
11	368 908 290 884	189 562 717 350
13	339 876 772 761	177 132 879 226
17	303 041 995 478	162 150 961 588

Annexe C

Quelques exemples de polynômes générateurs

On donne dans cet appendice quelques polynômes générateurs obtenus à partir des programmes mis en place pour déterminer les différents corps de nombres de discriminant fixé. La technique des exposants de Newton-Ore est très efficace dans la construction de ces polynômes.

C.1 En degré 8

Pour $d_K = 2^{22}$

$$x^8 - 4x^7 + 4x^6 - 8x^5 + 34x^4 - 24x^3 + 12x^2 + 8x + 2$$

$$x^8 - 4x^7 + 4x^6 + 2x^4 - 8x^3 + 12x^2 - 8x + 2$$

$$x^8 - 4x^7 + 4x^6 + 16x^5 - 14x^4 - 16x^3 + 20x^2 - 8x + 2$$

$$x^8 - 4x^7 + 8x^6 - 16x^5 + 38x^4 - 16x^3 + 28x^2 + 2$$

$$x^8 - 4x^7 + 8x^6 - 8x^5 + 6x^4 - 8x^3 + 4x^2 + 2$$

$$x^8 - 4x^7 + 8x^6 - 8x^5 + 6x^4 - 4x^2 + 2$$

$$x^8 - 4x^7 + 8x^6 - 26x^4 + 8x^3 + 36x^2 + 16x + 2$$

$$x^8 - 4x^7 + 12x^6 - 24x^5 + 34x^4 - 32x^3 + 20x^2 - 8x + 2$$

$$x^8 - 4x^7 + 12x^6 - 16x^5 + 2x^4 + 16x^3 + 20x^2 - 8x + 2$$

$$x^8 - 4x^7 + 12x^6 - 8x^5 + 18x^4 + 8x^3 + 12x^2 + 8x + 2$$

$$x^8 + 4x^4 + 32x^2 + 4$$

$$x^8 + 4x^7 + 4x^6 + 8x^5 + 34x^4 + 24x^3 + 12x^2 - 8x + 2$$

$$x^8 + 4x^7 + 4x^6 + 2x^4 + 8x^3 + 12x^2 + 8x + 2$$

$$x^8 + 4x^7 + 4x^6 - 16x^5 - 14x^4 + 16x^3 + 20x^2 + 8x + 2$$

$$x^8 + 4x^7 + 8x^6 + 16x^5 + 38x^4 + 16x^3 + 28x^2 + 2$$

$$x^8 + 4x^7 + 8x^6 + 8x^5 + 6x^4 + 8x^3 + 4x^2 + 2$$

$$x^8 + 4x^7 + 8x^6 + 8x^5 + 6x^4 - 4x^2 + 2$$

$$x^8 + 4x^7 + 8x^6 - 26x^4 - 8x^3 + 36x^2 - 16x + 2$$
$$x^8 + 4x^7 + 12x^6 + 24x^5 + 34x^4 + 32x^3 + 20x^2 + 8x + 2$$
$$x^8 + 4x^7 + 12x^6 + 16x^5 + 2x^4 - 16x^3 + 20x^2 + 8x + 2$$
$$x^8 + 4x^7 + 12x^6 + 8x^5 + 18x^4 - 8x^3 + 12x^2 - 8x + 2$$

Pour $d_K = 2^{24}$

$$x^8 - 8x^5 + 2x^4 + 12x^2 + 8x + 2$$
$$x^8 + 2x^4 - 16x^3 + 20x^2 - 8x + 2$$
$$x^8 + 2x^4 + 16x^3 + 20x^2 + 8x + 2$$
$$x^8 + 12x^4 + 4$$
$$x^8 + 8x^5 + 2x^4 + 12x^2 - 8x + 2$$
$$x^8 + 4x^6 + 6x^4 - 8x^3 + 4x^2 + 8x + 2$$
$$x^8 + 4x^6 + 6x^4 + 8x^3 + 4x^2 - 8x + 2$$

Pour $d_K = 2^{25}$

$$x^8 - 8x^6 + 18x^4 + 4x^2 + 2$$
$$x^8 - 4x^6 + 4x^4 + 8$$
$$x^8 - 4x^6 + 6x^4 - 4x^2 + 2$$
$$x^8 - 4x^6 + 12x^4 - 16x^2 + 8$$
$$x^8 - 4x^6 + 22x^4 - 12x^2 + 2$$
$$x^8 - 4x^6 + 36x^4 + 32x^2 + 8$$
$$x^8 - 8x^5 + 34x^4 - 56x^3 + 52x^2 + 2$$
$$x^8 + 2x^4 - 4x^2 + 2$$
$$x^8 + 2x^4 + 4x^2 + 2$$
$$x^8 + 8x^5 + 34x^4 + 56x^3 + 52x^2 + 2$$
$$x^8 + 4x^6 - 26x^4 - 8x^3 + 52x^2 + 16x + 2$$
$$x^8 + 4x^6 - 26x^4 + 8x^3 + 52x^2 - 16x + 2$$
$$x^8 - 4x^6 + 36x^4 + 32x^2 + 8$$
$$x^8 + 4x^6 + 4x^4 + 8$$
$$x^8 + 4x^6 + 6x^4 + 4x^2 + 2$$
$$x^8 + 4x^6 + 12x^4 + 16x^2 + 8$$
$$x^8 + 4x^6 + 22x^4 + 12x^2 + 2$$
$$x^8 - 4x^6 + 36x^4 - 32x^2 + 8$$
$$x^8 + 8x^6 - 8x^5 - 20x^4 + 32x^3 + 48x^2 + 16x + 4$$

$$x^8 + 8x^6 + 18x^4 - 4x^2 + 2$$
$$x^8 + 8x^6 + 8x^5 - 20x^4 - 32x^3 + 48x^2 - 16x + 4$$

Pour $d_K = 2^{26}$

$$x^8 - 8x^6 - 44x^4 - 144x^2 + 4$$
$$x^8 - 8x^6 - 44x^4 + 48x^2 + 4$$
$$x^8 - 4x^6 - 8x^5 - 4x^4 + 8x^3 + 8x^2 - 2$$
$$x^8 - 4x^6 - 8x^5 + 8x^3 + 16x^2 + 16x + 2$$
$$x^8 - 4x^6 + 4x^4 + 8x^2 + 4$$
$$x^8 - 4x^6 + 8x^4 - 8x^3 + 8x^2 + 2$$
$$x^8 - 4x^6 + 8x^4 + 8x^3 + 8x^2 + 2$$
$$x^8 - 4x^6 + 12x^4 - 24x^3 + 16x^2 - 2$$
$$x^8 - 4x^6 + 12x^4 - 8x^2 + 4$$
$$x^8 - 4x^6 + 12x^4 + 24x^3 + 16x^2 - 2$$
$$x^8 - 4x^6 + 8x^5 - 4x^4 - 8x^3 + 8x^2 - 2$$
$$x^8 - 4x^6 - 8x^5 - 4x^4 + 8x^3 + 8x^2 - 2$$
$$x^8 - 4x^6 + 8x^5 - 8x^3 + 16x^2 - 16x + 2$$
$$x^8 - 4x^6 - 8x^5 + 8x^3 + 16x^2 + 16x + 2$$
$$x^8 - 28x^4 - 64x^3 - 64x^2 - 32x - 4$$
$$x^8 - 28x^4 + 64x^3 - 64x^2 + 32x - 4$$
$$x^8 + 4x^6 - 8x^5 + 8x^3 + 2$$
$$x^8 + 4x^6 - 8x^5 + 10x^4 - 24x^3 + 16x^2 + 2$$
$$x^8 + 4x^6 + 8x^5 + 10x^4 + 24x^3 + 16x^2 + 2$$
$$x^8 + 4x^6 - 8x^5 + 32x^4 + 56x^3 + 48x^2 + 16x + 2$$
$$x^8 + 4x^6 + 8x^5 + 32x^4 - 56x^3 + 48x^2 - 16x + 2$$
$$x^8 + 4x^6 + 4x^4 - 8x^2 + 4$$
$$x^8 + 4x^6 + 12x^4 + 8x^2 + 4$$
$$x^8 + 4x^6 + 8x^5 - 8x^3 + 2$$
$$x^8 - 8x^6 + 16x^4 - 32x^3 - 80x^2 - 32x + 8$$
$$x^8 - 8x^6 + 16x^4 + 32x^3 - 80x^2 + 32x + 8$$
$$x^8 - 8x^6 + 36x^4 - 64x^3 + 64x^2 - 32x + 8$$
$$x^8 - 8x^6 + 36x^4 + 64x^3 + 64x^2 + 32x + 8$$
$$x^8 - 8x^5 + 26x^4 + 72x^3 + 80x^2 + 16x + 10$$
$$x^8 + 6x^4 - 8x^3 + 16x^2 + 16x + 10$$

$$x^8 + 6x^4 + 8x^3 + 16x^2 - 16x + 10$$
$$x^8 + 20x^4 - 64x^3 + 80x^2 - 32x + 8$$
$$x^8 + 20x^4 + 64x^3 + 80x^2 + 32x + 8$$
$$x^8 + 8x^5 + 26x^4 - 72x^3 + 80x^2 - 16x + 10$$
$$x^8 + 4x^6 - 8x^5 + 10x^4 - 8x^3 + 8x^2 - 16x + 10$$
$$x^8 + 4x^6 + 38x^4 - 72x^3 + 64x^2 - 16x + 10$$
$$x^8 + 4x^6 + 38x^4 + 72x^3 + 64x^2 + 16x + 10$$
$$x^8 + 4x^6 + 8x^5 + 10x^4 + 8x^3 + 8x^2 + 16x + 10$$
$$x^8 - 8x^6 - 8x^4 - 32x^2 + 16$$
$$x^8 - 8x^6 + 16x^4 + 16$$
$$x^8 - 8x^6 + 40x^4 - 96x^2 + 16$$
$$x^8 + 16x^4 - 32x^2 + 16$$
$$x^8 + 16x^4 + 32x^2 + 16$$
$$x^8 + 4x^6 - 8x^5 - 4x^4 + 8x^3 + 120x^2 - 32x + 14$$
$$x^8 + 4x^6 + 8x^5 - 4x^4 - 8x^3 + 120x^2 + 32x + 14$$

Pour $d_K = 2^{27}$

$$x^8 - 8x^6 - 8x^5 + 30x^4 + 64x^3 + 48x^2 + 16x + 2$$
$$x^8 - 8x^6 + 30x^4 + 2$$
$$x^8 - 8x^6 + 34x^4 - 16x^2 + 2$$
$$x^8 - 8x^6 + 8x^5 + 30x^4 - 64x^3 + 48x^2 - 16x + 2$$
$$x^8 - 4x^6 - 8x^5 + 6x^4 + 32x^3 + 32x^2 + 2$$
$$x^8 - 4x^6 + 6x^4 + 2$$
$$x^8 - 4x^6 + 10x^4 - 8x^2 + 2$$
$$x^8 - 4x^6 + 12x^4 - 32x^3 + 56x^2 + 4$$
$$x^8 - 4x^6 + 12x^4 + 32x^3 + 56x^2 + 4$$
$$x^8 - 4x^6 + 8x^5 + 6x^4 - 32x^3 + 32x^2 + 2$$
$$x^8 - 2x^4 + 2$$
$$x^8 + 2x^4 + 2$$
$$x^8 + 4x^6 - 16x^5 + 12x^4 - 32x^3 + 72x^2 - 32x + 4$$
$$x^8 + 4x^6 - 8x^5 + 6x^4 + 32x^2 + 16x + 2$$
$$x^8 + 4x^6 + 6x^4 + 2$$
$$x^8 + 4x^6 + 10x^4 + 8x^2 + 2$$
$$x^8 + 4x^6 + 8x^5 + 6x^4 + 32x^2 - 16x + 2$$

$$x^8 + 4x^6 + 16x^5 + 12x^4 + 32x^3 + 72x^2 + 32x + 4$$
$$x^8 + 8x^6 - 8x^5 + 30x^4 + 16x^2 + 2$$
$$x^8 + 8x^6 + 30x^4 + 2$$
$$x^8 + 8x^6 + 34x^4 + 16x^2 + 2$$
$$x^8 + 8x^6 + 8x^5 + 30x^4 + 16x^2 + 2$$
$$x^8 - 8x^6 - 8x^5 + 10x^4 + 32x^3 + 56x^2 + 32x + 10$$
$$x^8 - 8x^6 + 20x^4 - 16x^2 + 8$$
$$x^8 - 8x^6 + 8x^5 + 10x^4 - 32x^3 + 56x^2 - 32x + 10$$
$$x^8 - 4x^6 - 8x^5 + 10x^4 + 16x^2 + 16x + 10$$
$$x^8 - 4x^6 + 8x^5 + 10x^4 + 16x^2 - 16x + 10$$
$$x^8 - 8x^5 + 10x^4 + 96x^3 + 168x^2 + 48x + 10$$
$$x^8 - 4x^6 + 8$$
$$x^8 + 4x^6 + 8$$
$$x^8 + 12x^4 - 16x^2 + 8$$
$$x^8 + 12x^4 + 16x^2 + 8$$
$$x^8 + 60x^4 - 32x^2 + 8$$
$$x^8 + 60x^4 + 32x^2 + 8$$
$$x^8 + 8x^5 + 10x^4 - 96x^3 + 168x^2 - 48x + 10$$
$$x^8 + 4x^6 - 8x^5 + 10x^4 - 32x^3 + 48x^2 - 32x + 10$$
$$x^8 + 4x^6 + 8x^5 + 10x^4 + 32x^3 + 48x^2 + 32x + 10$$

Pour $d_K = \pm 2^{28}$

$$x^8 - 8x^6 - 16x^5 + 4x^4 + 128x^3 - 112x^2 - 32x + 4$$
$$x^8 - 8x^6 - 8x^5 + 4x^4 - 8x^2 + 2$$
$$x^8 - 8x^6 - 8x^5 + 16x^4 + 32x^3 + 16x^2 - 2$$
$$x^8 - 8x^6 - 8x^5 + 80x^4 - 80x^3 - 16x^2 + 16x - 2$$
$$x^8 - 8x^6 - 60x^4 + 80x^2 + 4$$
$$x^8 - 8x^6 - 20x^4 - 16x^2 - 4$$
$$x^8 - 8x^6 + 4x^4 + 16x^2 + 4$$
$$x^8 - 8x^6 + 12x^4 + 48x^2 - 4$$
$$x^8 - 8x^6 + 20x^4 - 32x^3 - 80x^2 - 64x - 4$$
$$x^8 - 8x^6 + 20x^4 - 16x^2 - 4$$
$$x^8 - 8x^6 + 20x^4 + 32x^3 - 80x^2 + 64x - 4$$
$$x^8 - 8x^6 + 28x^4 - 16x^2 + 4$$

$$x^8 - 8x^6 + 8x^5 + 4x^4 - 8x^2 + 2$$

$$x^8 - 8x^6 + 8x^5 + 16x^4 - 32x^3 + 16x^2 - 2$$

$$x^8 - 8x^6 + 8x^5 + 80x^4 + 80x^3 - 16x^2 - 16x - 2$$

$$x^8 - 8x^6 + 16x^5 + 4x^4 - 128x^3 - 112x^2 + 32x + 4$$

$$x^8 - 4x^6 - 8x^5 - 28x^4 - 48x^3 - 32x^2 - 16x - 2$$

$$x^8 - 4x^6 - 8x^5 - 16x^3 - 16x^2 + 2$$

$$x^8 - 4x^6 + 8x^5 - 28x^4 + 48x^3 - 32x^2 + 16x - 2$$

$$x^8 - 4x^6 + 8x^5 + 16x^3 - 16x^2 + 2$$

$$x^8 - 8x^5 - 4x^4 + 16x^2 + 16x + 6$$

$$x^8 - 8x^5 - 4x^4 + 24x^2 - 16x + 2$$

$$x^8 - 8x^5 + 8x^4 - 16x^2 + 16x - 2$$

$$x^8 - 8x^5 + 8x^4 + 8x^2 + 2$$

$$x^8 - 28x^4 - 4$$

$$x^8 - 20x^4 - 32x^2 + 4$$

$$x^8 - 20x^4 + 32x^2 + 4$$

$$x^8 - 4x^4 - 4$$

$$x^8 + 4x^4 - 4$$

$$x^8 + 28x^4 - 4$$

$$x^8 + 8x^5 - 4x^4 + 16x^2 - 16x + 6$$

$$x^8 + 8x^5 - 4x^4 + 24x^2 + 16x + 2$$

$$x^8 + 8x^5 + 8x^4 - 16x^2 - 16x - 2$$

$$x^8 + 8x^5 + 8x^4 + 8x^2 + 2$$

$$x^8 + 4x^6 - 8x^5 - 76x^4 - 112x^3 - 104x^2 - 16x - 2$$

$$x^8 + 4x^6 - 8x^5 - 28x^4 - 16x^3 - 2$$

$$x^8 + 4x^6 - 8x^5 + 4x^4 + 16x^3 - 24x^2 + 16x - 2$$

$$x^8 + 4x^6 + 8x^5 - 76x^4 + 112x^3 - 104x^2 + 16x - 2$$

$$x^8 + 4x^6 + 8x^5 - 28x^4 + 16x^3 - 2$$

$$x^8 + 4x^6 + 8x^5 + 4x^4 - 16x^3 - 24x^2 - 16x - 2$$

$$x^8 + 8x^6 - 16x^5 + 28x^4 - 128x^3 + 144x^2 + 32x + 4$$

$$x^8 + 8x^6 - 60x^4 - 80x^2 + 4$$

$$x^8 + 8x^6 - 20x^4 + 16x^2 - 4$$

$$x^8 + 8x^6 + 4x^4 - 16x^2 + 4$$

$$x^8 + 8x^6 + 12x^4 - 48x^2 - 4$$

Pour $d_K = \pm 2^{29}$

$$x^8 - 4x^6 - 24x^4 - 24x^2 + 2$$

$$x^8 - 4x^6 - 12x^4 - 8x^2 - 2$$

$$x^8 - 4x^6 + 2$$

$$x^8 - 4x^6 + 4x^4 - 40x^2 - 2$$

$$x^8 - 4x^6 + 4x^4 - 2$$

$$x^8 - 4x^6 + 4x^4 + 8x^2 - 2$$

$$x^8 - 4x^6 + 8x^4 - 8x^2 + 2$$

$$x^8 - 4x^6 + 16x^4 + 16x^2 + 2$$

$$x^8 - 4x^6 + 52x^4 - 96x^2 - 2$$

$$x^8 + 4x^6 - 24x^4 + 24x^2 + 2$$

$$x^8 + 4x^6 - 12x^4 + 8x^2 - 2$$

$$x^8 + 4x^6 + 2$$

$$x^8 + 4x^6 + 4x^4 - 8x^2 - 2$$

$$x^8 + 4x^6 + 4x^4 - 2$$

$$x^8 + 4x^6 + 4x^4 + 40x^2 - 2$$

$$x^8 + 4x^6 + 8x^4 + 8x^2 + 2$$

$$x^8 + 4x^6 + 16x^4 - 16x^2 + 2$$

$$x^8 + 4x^6 + 52x^4 + 96x^2 - 2$$

$$x^8 - 8x^6 - 16x^5 - 48x^4 - 128x^3 - 48x^2 + 8$$

$$x^8 - 8x^6 - 16x^5 + 16x^4 + 96x^3 + 16x^2 + 8$$

$$x^8 - 8x^6 - 16x^5 + 24x^4 + 32x^3 + 80x^2 - 64x - 8$$

$$x^8 - 8x^6 - 16x^4 + 176x^2 + 8$$

$$x^8 - 8x^6 - 8x^4 + 16x^2 - 8$$

$$x^8 - 8x^6 + 16x^4 - 16x^2 + 8$$

$$x^8 - 8x^6 + 24x^4 - 112x^2 - 8$$

$$x^8 - 8x^6 + 24x^4 - 16x^2 - 8$$

$$x^8 - 8x^6 + 48x^4 - 48x^2 + 8$$

$$x^8 - 8x^6 + 16x^5 - 48x^4 + 128x^3 - 48x^2 + 8$$

$$x^8 - 8x^6 + 16x^5 + 16x^4 - 96x^3 + 16x^2 + 8$$

$$x^8 - 8x^6 + 16x^5 + 24x^4 - 32x^3 + 80x^2 + 64x - 8$$

$$x^8 - 8x^4 - 16x^2 - 8$$

$$x^8 - 8x^4 + 16x^2 - 8$$

$$x^8 + 88x^4 - 272x^2 - 8$$
$$x^8 + 88x^4 + 272x^2 - 8$$
$$x^8 + 8x^6 - 16x^4 - 176x^2 + 8$$
$$x^8 + 8x^6 - 16x^5 - 40x^4 + 128x^3 - 144x^2 + 64x - 8$$
$$x^8 + 8x^6 - 16x^4 - 176x^2 + 8$$
$$x^8 + 8x^6 - 8x^4 - 16x^2 - 8$$
$$x^8 + 8x^6 + 16x^4 + 16x^2 + 8$$
$$x^8 + 8x^6 + 24x^4 + 16x^2 - 8$$
$$x^8 + 8x^6 + 24x^4 + 112x^2 - 8$$
$$x^8 + 8x^6 + 48x^4 + 48x^2 + 8$$
$$x^8 + 8x^6 + 16x^5 - 40x^4 - 128x^3 - 144x^2 - 64x - 8$$
$$x^8 - 4x^6 - 16x^5 + 4x^4 - 32x^3 + 144x^2 - 80x + 14$$
$$x^8 - 4x^6 - 16x^5 + 4x^4 + 112x^3 - 120x^2 + 16x + 14$$
$$x^8 - 4x^6 + 16x^5 + 4x^4 - 112x^3 - 120x^2 - 16x + 14$$
$$x^8 - 4x^6 + 16x^5 + 4x^4 + 32x^3 + 144x^2 + 80x + 14$$
$$x^8 + 4x^6 - 16x^5 + 8x^4 + 32x^3 - 104x^2 - 80x - 14$$
$$x^8 + 4x^6 + 16x^5 + 8x^4 - 32x^3 - 104x^2 + 80x - 14$$
$$x^8 - 8x^6 - 48x^4 - 64x^2 - 32$$
$$x^8 - 8x^6 + 32$$
$$x^8 - 8x^6 + 16x^4 - 320x^2 - 32$$
$$x^8 - 8x^6 + 16x^4 - 32$$
$$x^8 - 8x^6 + 16x^4 + 64x^2 - 32$$
$$x^8 - 8x^6 + 32x^4 - 64x^2 + 32$$
$$x^8 - 8x^6 + 64x^4 + 128x^2 + 32$$
$$x^8 + 8x^6 - 48x^4 + 64x^2 - 32$$
$$x^8 + 8x^6 + 32$$
$$x^8 + 8x^6 + 16x^4 - 64x^2 - 32$$
$$x^8 + 8x^6 + 16x^4 - 32$$
$$x^8 + 8x^6 + 16x^4 + 320x^2 - 32$$
$$x^8 + 8x^6 + 32x^4 + 64x^2 + 32$$
$$x^8 + 8x^6 + 64x^4 - 128x^2 + 32$$
$$x^8 - 4x^6 + 20x^4 - 16x^3 - 64x^2 - 48x + 62$$
$$x^8 - 4x^6 + 20x^4 + 16x^3 - 64x^2 + 48x + 62$$

Pour $d_K = -2^{30}$

$$x^8 - 8x^6 - 32x^5 + 20x^4 + 256x^3 - 336x^2 + 64x + 4$$
$$x^8 - 8x^6 - 16x^5 + 12x^4 + 96x^3 - 32x^2 - 32x - 4$$
$$x^8 - 8x^6 - 52x^4 - 64x^2 - 4$$
$$x^8 - 8x^6 - 20x^4 + 32x^2 - 4$$
$$x^8 - 8x^6 + 4x^4 - 4$$
$$x^8 - 8x^6 + 12x^4 - 4$$
$$x^8 - 8x^6 + 36x^4 - 32x^2 - 4$$
$$x^8 - 8x^6 + 16x^5 + 12x^4 - 96x^3 - 32x^2 + 32x - 4$$
$$x^8 - 8x^6 + 32x^5 + 20x^4 - 256x^3 - 336x^2 - 64x + 4$$
$$x^8 - 76x^4 - 48x^2 - 4$$
$$x^8 - 76x^4 + 48x^2 - 4$$
$$x^8 - 68x^4 - 192x^3 - 176x^2 - 64x - 4$$
$$x^8 - 68x^4 + 192x^3 - 176x^2 + 64x - 4$$
$$x^8 - 12x^4 - 16x^2 - 4$$
$$x^8 - 12x^4 + 16x^2 - 4$$
$$x^8 - 4x^4 - 16x^2 - 4$$
$$x^8 - 4x^4 + 16x^2 - 4$$
$$x^8 + 8x^6 - 32x^5 - 60x^4 - 320x^3 + 64x^2 - 4$$
$$x^8 + 8x^6 - 52x^4 + 64x^2 - 4$$
$$x^8 + 8x^6 - 20x^4 - 32x^2 - 4$$
$$x^8 + 8x^6 + 4x^4 - 4$$
$$x^8 + 8x^6 + 12x^4 - 4$$
$$x^8 + 8x^6 + 36x^4 + 32x^2 - 4$$
$$x^8 + 8x^6 + 32x^5 - 60x^4 + 320x^3 + 64x^2 - 4$$
$$x^8 - 8x^6 - 16x^5 - 16x^4 - 64x^3 - 96x^2 - 64x - 8$$
$$x^8 - 8x^6 - 16x^5 - 16x^4 + 64x^3 + 96x^2 - 8$$
$$x^8 - 8x^6 - 16x^5 + 32x^4 + 64x^3 - 128x^2 + 64x - 8$$
$$x^8 - 8x^6 - 16x^5 + 56x^4 + 64x^3 - 224x^2 + 128x + 8$$
$$x^8 - 8x^6 + 16x^5 - 16x^4 + 64x^3 - 96x^2 + 64x - 8$$
$$x^8 - 8x^6 + 16x^5 + 32x^4 - 64x^3 - 128x^2 - 64x - 8$$
$$x^8 - 8x^6 + 16x^5 + 56x^4 - 64x^3 - 224x^2 - 128x + 8$$
$$x^8 - 16x^5 - 120x^4 + 256x^3 - 128x^2 + 8$$
$$x^8 - 16x^5 - 32x^4 + 32x^2 - 8$$
$$x^8 - 16x^5 + 40x^4 - 64x^2 + 128x + 8$$
$$x^8 + 16x^5 - 120x^4 - 256x^3 - 128x^2 + 8$$
$$x^8 + 16x^5 - 32x^4 + 32x^2 - 8$$
$$x^8 + 16x^5 + 40x^4 - 64x^2 - 128x + 8$$

$$x^8 + 8x^6 - 16x^5 + 24x^4 - 64x^3 - 32x^2 + 8$$
$$x^8 + 8x^6 + 16x^5 + 24x^4 + 64x^3 - 32x^2 + 8$$
$$x^8 - 8x^6 - 72x^4 - 96x^2 - 16$$
$$x^8 - 8x^6 - 56x^4 + 416x^2 - 16$$
$$x^8 - 8x^6 - 24x^4 - 32x^2 - 16$$
$$x^8 - 8x^6 - 8x^4 + 32x^2 - 16$$
$$x^8 - 8x^6 + 8x^4 + 32x^2 - 16$$
$$x^8 - 8x^6 + 40x^4 + 96x^2 - 16$$
$$x^8 + 8x^6 - 72x^4 + 96x^2 - 16$$
$$x^8 + 8x^6 - 56x^4 - 416x^2 - 16$$
$$x^8 + 8x^6 - 24x^4 + 32x^2 - 16$$
$$x^8 + 8x^6 - 8x^4 - 32x^2 - 16$$
$$x^8 + 8x^6 + 8x^4 - 32x^2 - 16$$
$$x^8 + 8x^6 + 24x^4 + 32x^2 - 16$$
$$x^8 + 8x^6 + 40x^4 - 96x^2 - 16$$
$$x^8 - 8x^6 - 16x^5 + 20x^4 + 32x^3 + 32x^2 - 96x - 36$$
$$x^8 - 8x^6 + 16x^5 + 20x^4 - 32x^3 + 32x^2 + 96x - 36$$
$$x^8 + 8x^6 + 20x^4 - 64x^3 - 80x^2 + 36$$
$$x^8 + 8x^6 + 20x^4 + 64x^3 - 80x^2 + 36$$

Pour $d_K = \pm 2^{31}$

$$x^8 - 8x^6 - 32x^5 - 64x^4 + 32x^3 + 184x^2 + 80x - 2$$
$$x^8 - 8x^6 - 32x^5 + 32x^3 - 24x^2 - 16x - 2$$
$$x^8 - 8x^6 - 32x^5 + 160x^3 + 224x^2 + 64x - 8$$
$$x^8 - 8x^6 - 32x^5 + 4x^4 + 64x^3 + 144x^2 + 64x + 4$$
$$x^8 - 8x^6 - 16x^5 - 60x^4 - 128x^3 - 96x^2 - 32x - 4$$
$$x^8 - 8x^6 - 16x^5 - 52x^4 + 64x^3 - 32x - 4$$
$$x^8 - 8x^6 - 16x^5 - 36x^4 + 256x^3 - 312x^2 + 64x + 2$$
$$x^8 - 8x^6 - 16x^5 + 12x^4 - 64x^2 + 32x - 4$$
$$x^8 - 8x^6 - 16x^5 + 16x^4 + 32x^3 + 24x^2 - 16x - 2$$
$$x^8 - 8x^6 - 36x^4 - 248x^2 + 2$$
$$x^8 - 8x^6 - 12x^4 + 2$$
$$x^8 - {}^6_x + 4x^4 + 32x^2 + 2$$
$$x^8 - 8x^6 + 12x^4 - 8x^2 + 2$$

$$x^8 - 8x^6 + 16x^4 - 32x^3 - 128x^2 - 64x - 8$$

$$x^8 - 8x^6 + 16x^4 + 2$$

$$x^8 - 8x^6 + 16x^4 + 32x^3 - 128x^2 + 64x - 8$$

$$x^8 - 8x^6 + 20x^4 - 16x^3 - 80x^2 - 32x + 2$$

$$x^8 - 8x^6 + 20x^4 - 16x^2 + 2$$

$$x^8 - 8x^6 + 20x^4 + 16x^3 - 80x^2 + 32x + 2$$

$$x^8 - 8x^6 + 28x^4 - 24x^2 + 2$$

$$x^8 - 8x^6 + 16x^5 - 60x^4 + 128x^3 - 96x^2 + 32x - 4$$

$$x^8 - 8x^6 + 16x^5 - 52x^4 - 64x^3 + 32x - 4$$

$$x^8 - 8x^6 + 16x^5 - 36x^4 - 256x^3 - 312x^2 - 64x + 2$$

$$x^8 - 8x^6 + 16x^5 + 12x^4 - 64x^2 - 32x - 4$$

$$x^8 - 8x^6 + 16x^5 + 16x^4 - 32x^3 + 24x^2 + 16x - 2$$

$$x^8 - 8x^6 + 32x^5 - 64x^4 - 32x^3 + 184x^2 - 80x - 2$$

$$x^8 - 8x^6 + 32x^5 - 160x^3 + 224x^2 - 64x - 8$$

$$x^8 - 8x^6 + 24x^4 - 32x^2 + 18$$

$$x^8 - 32x^5 + 16x^4 + 192x^3 - 304x^2 + 48x - 2$$

$$x^8 - 32x^5 + 40x^4 + 96x^3 - 168x^2 + 48x - 2$$

$$x^8 - 16x^5 - 68x^4 + 40x^2 - 32x + 2$$

$$x^8 - 116x^4 + 2$$

$$x^8 - 36x^4 - 16x^2 + 2$$

$$x^8 - 36x^4 + 16x^2 + 2$$

$$x^8 - 32x^4 - 64x^3 - 48x^2 - 16x - 2$$

$$x^8 - 32x^4 + 64x^3 - 48x^2 + 16x - 2$$

$$x^8 - 20x^4 + 2$$

$$x^8 - 8x^4 + 8x^2 - 2$$

$$x^8 - 8x^4 - 8x^2 - 2$$

$$x^8 - 4x^4 - 8x^2 + 2$$

$$x^8 - 4x^4 + 2$$

$$x^8 - 4x^4 + 8x^2 + 2$$

$$x^8 - 2$$

$$x^8 + 2$$

$$x^8 + 4x^4 + 2$$

$$x^8 + 8x^4 - 2$$

$$x^8 + 8x^6 + 24x^4 + 32x^2 + 18$$

$$x^8 + 20x^4 + 2$$

$$x^8 + 116x^4 + 2$$

$$x^8 + 16x^5 - 68x^4 + 40x^2 + 32x + 2$$

$$x^8 + 32x^5 + 16x^4 - 192x^3 - 304x^2 - 48x - 2$$

$$x^8 + 32x^5 + 40x^4 - 96x^3 - 168x^2 - 48x - 2$$

$$x^8 + 8x^6 - 16x^5 - 28x^4 + 128x^3 - 192x^2 + 96x - 4$$

$$x^8 + 8x^6 - 36x^4 + 248x^2 + 2$$

$$x^8 + 8x^6 - 12x^4 + 2$$

$$x^8 + 8x^6 + 4x^4 - 32x^2 + 2$$

$$x^8 + 8x^6 + 12x^4 + 8x^2 + 2$$

$$x^8 + 8x^6 + 16x^4 + 2$$

$$x^8 + 8x^6 + 20x^4 + 16x^2 + 2$$

$$x^8 + 8x^6 + 28x^4 + 24x^2 + 2$$

$$x^8 + 8x^6 + 16x^5 - 28x^4 - 128x^3 - 192x^2 - 96x - 4$$

C.2 En degré 9

Pour $d_K = -3^{19}$

$$x^9 - 9x^7 - 15x^6 - 9x^5 + 9x^3 + 9x^2 - 3$$
$$x^9 - 15x^6 + 54x^4 - 18x^3 - 72x^2 + 54x - 3$$
$$x^9 - 12x^6 + 18x^4 - 9x^3 - 9x^2 + 3$$
$$x^9 - 12x^6 + 36x^5 + 18x^4 - 117x^3 + 126x^2 - 54x + 3$$
$$x^9 - 9x^7 - 6x^6 + 27x^5 + 27x^4 - 18x^3 - 18x^2 - 3$$
$$x^9 - 9x^7 - 3x^6 - 27x^5 + 54x^4 + 9x^3 + 45x^2 + 3$$
$$x^9 - 9x^7 - 3x^6 + 27x^5 + 18x^4 - 36x^3 + 45x^2 + 27x + 3$$
$$x^9 - 9x^7 - 3x^6 + 36x^5 - 27x^4 + 9x^3 - 9x^2 + 3$$
$$x^9 - 9x^6 + 3x^6 - 27x^5 - 54x^4 + 9x^3 - 45x^2 - 3$$
$$x^9 - 9x^7 + 3x^6 + 27x^5 - 18x^4 - 36x^3 - 45x^2 + 27x - 3$$
$$x^9 - 9x^7 + 3x^6 + 36x^5 + 27x^4 + 9x^3 + 9x^2 - 3$$
$$x^9 - 6x^6 - 9x^5 - 9x^4 + 9x^2 - 3$$
$$x^9 - 6x^6 + 18x^4 + 27x^3 + 36x^2 - 3$$
$$x^9 + 9x^7 - 6x^6 - 18x^5 + 27x^4 + 9x^3 - 45x^2 - 27x - 3$$
$$x^9 + 9x^7 - 3x^6 - 72x^4 + 72x^2 - 27x + 3$$
$$x^9 + 9x^7 + 3x^6 + 72x^4 - 72x^2 - 27x - 3$$
$$x^9 - 9x^7 + 6x^6 + 27x^5 - 27x^4 - 18x^3 + 18x^2 + 3$$
$$x^9 - 9x^7 + 15x^6 - 9x^5 + 9x^3 - 9x^2 + 3$$
$$x^9 + 6x^6 - 18x^4 + 27x^3 - 36x^2 + 3$$
$$x^9 + 12x^6 - 18x^4 - 9x^3 + 9x^2 - 3$$
$$x^9 + 12x^6 + 36x^5 - 18x^4 - 117x^3 - 126x^2 - 54x - 3$$
$$x^9 + 15x^6 - 54x^4 - 18x^3 + 72x^2 + 54x + 3$$
$$x^9 - 9x^7 - 6x^6 - 27x^5 - 9x^4 + 243x^3 + 198x^2 - 108x + 24$$
$$x^9 - 9x^7 + 6x^6 - 27x^5 + 9x^4 + 243x^3 - 198x^2 - 108x - 24$$
$$x^9 - 9x^6 - 216x^3 - 27$$
$$x^9 - 9x^6 - 54x^3 - 27$$
$$x^9 + 9x^6 - 216x^3 + 27$$
$$x^9 + 9x^6 - 54x^3 + 27$$

Pour $d_K = -3^{21}$

$$x^9 - 6x^6 - 27x^5 - 9x^4 + 36x^3 + 27x^2 - 3$$
$$x^9 + 9x^7 - 3x^6 + 27x^5 - 18x^4 + 27x^3 - 27x^2 + 3$$

$$x^9 + 9x^7 + 3x^6 + 27x^5 + 18x^4 + 27x^3 + 27x^2 - 3$$
$$x^9 + 6x^6 - 27x^5 + 9x^4 + 36x^3 - 27x^2 + 3$$

Pour $d_K = 3^{22}$

$$x^9 + 9x^8 - 39x^6 - 9x^5 + 54x^4 + 9x^3 - 27x^2 + 3$$
$$x^9 - 9x^6 - 9x^5 - 27x^4 - 9x^3 - 27x^2 - 12$$
$$x^9 + 9x^6 - 9x^5 + 27x^4 - 9x^3 + 27x^2 + 12$$
$$x^9 - 9x^8 + 39x^6 - 9x^5 - 54x^4 + 9x^3 + 27x^2 - 3$$
$$x^9 - 9x^6 - 9x^5 + 27x^3 + 54x^2 + 27x + 30$$
$$x^9 + 9x^6 - 9x^5 + 27x^3 - 54x^2 + 27x - 30$$

Pour $d_K = -3^{23}$

$$x^9 - 6x^6 + 9x^3 - 3$$
$$x^9 + 3x^6 - 3$$
$$x^9 + 3x^6 - 9x^3 - 3$$
$$x^9 + 6x^6 + 9x^3 + 3$$
$$x^9 - 3x^6 + 3$$
$$x^9 - 3x^6 - 9x^3 + 3$$
$$x^9 - 27x^6 + 99x^3 - 9$$
$$x^9 - 9x^6 - 9x^3 + 9$$
$$x^9 + 9x^6 - 9x^3 - 9$$
$$x^9 - 9x^6 + 81$$
$$x^9 + 9x^6 - 81$$
$$x^9 - 9x^6 + 18x^3 + 9$$
$$x^9 + 9x^6 + 18x^3 - 9$$
$$x^9 - 3x^6 - 18x^3 + 3$$
$$x^9 + 3x^6 - 18x^3 - 3$$
$$x^9 - 81x^3 - 243$$
$$x^9 - 81x^3 + 243$$
$$x^9 - 15x^6 + 18x^3 - 3$$
$$x^9 - 6x^6 - 9x^3 - 3$$
$$x^9 - 63x^3 - 9$$
$$x^9 - 9x^3 - 9$$
$$x^9 + 27x^6 + 99x^3 + 9$$
$$x^9 + 15x^6 + 18x^3 + 3$$

$$x^9 + 6x^6 - 9x^3 + 3$$
$$x^9 + 6x^6 - 9x^3 + 3$$
$$x^9 - 63x^3 + 9$$
$$x^9 - 9x^3 + 9$$
$$x^9 - 18x^6 - 9x^3 + 9$$
$$x^9 - 15x^6 + 54x^3 - 3$$
$$x^9 - 12x^6 + 27x^3 + 3$$
$$x^9 - 9x^6 - 36x^3 - 9$$
$$x^9 - 9x^6 + 18x^3 - 9$$
$$x^9 + 18x^6 - 9x^3 - 9$$
$$x^9 + 12x^6 + 27x^3 - 3$$
$$x^9 + 9x^6 - 36x^3 + 9$$
$$x^9 + 9x^6 + 18x^3 + 9$$

Pour $d_K = -3^{25}$

$$x^9 + 9x^8 + 27x^7 + 18x^6 - 54x^5 - 81x^4 + 27x^3 + 81x^2 - 3$$
$$x^9 + 9x^8 + 27x^7 + 18x^6 - 54x^5 - 81x^4 + 36x^3 + 108x^2 - 48$$
$$x^9 + 9x^8 + 27x^7 + 27x^6 - 81x^3 - 81x^2 - 27x - 3$$
$$x^9 + 9x^8 + 27x^7 + 27x^6 - 9x^3 - 27x^2 - 12$$
$$x^9 - 9x^8 + 27x^7 - 18x^6 - 54x^5 + 81x^4 + 27x^3 - 81x^2 + 3$$
$$x^9 - 9x^8 + 27x^7 - 18x^6 - 54x^5 + 81x^4 + 36x^3 - 108x^2 + 48$$
$$x^9 - 9x^8 + 27x^7 - 27x^6 - 81x^3 + 81x^2 - 27x + 3$$
$$x^9 - 9x^8 + 27x^7 - 27x^6 - 9x^3 + 27x^2 + 12$$
$$x^9 - 9x^6 + 54x^4 - 54x^3 - 162x + 45$$
$$x^9 + 9x^6 - 54x^4 - 54x^3 - 162x - 45$$
$$x^9 - 9x^6 + 27x^4 - 81x^3 + 243x^2 - 324x + 144$$
$$x^9 + 9x^6 - 27x^4 - 81x^3 - 243x^2 - 324x - 144$$

Pour $d_K = 3^{26}$

$$x^9 - 9x^6 + 27x^3 - 3$$
$$x^9 - 3$$
$$x^9 - 9$$
$$x^9 + 3$$
$$x^9 + 9$$
$$x^9 - 9x^6 + 27x^3 - 24$$

$$x^9 + 9x^6 + 27x^3 + 24$$

$$x^9 + 9x^6 + 27x^3 + 3$$

$$x^9 - 27x^6 + 27x^3 - 9$$

$$x^9 + 27x^6 + 27x^3 + 9$$

$$x^9 - 27x^6 + 432x^3 + 576$$

$$x^9 + 27x^6 + 432x^3 - 576$$

$$x^9 - 18x^6 - 27x^3 - 24$$

$$x^9 + 18x^6 - 27x^3 + 24$$

$$x^9 - 18x^6 + 81x^3 + 192$$

$$x^9 + 18x^6 + 81x^3 - 192$$

$$x^9 + 27x^3 - 72$$

$$x^9 + 27x^3 + 72$$

$$x^9 - 81$$

$$x^9 + 81$$

$$x^9 - 243$$

$$x^9 + 243$$

$$x^9 - 2187$$

$$x^9 + 2187$$

$$x^9 - 6561$$

$$x^9 + 6561$$

$$x^9 - 27x^6 - 27x^3 - 72$$

$$x^9 + 27x^6 - 27x^3 + 72$$

$$x^9 - 27x^6 + 297x^3 - 576$$

$$x^9 + 27x^6 + 297x^3 + 576$$

$$x^9 - 18x^6 - 3$$

$$x^9 + 18x^6 + 3$$

$$x^9 - 9x^6 + 216x^3 + 192$$

$$x^9 + 9x^6 + 216x^3 - 192$$

$$x^9 + 54x^3 - 9$$

Résumé : La présente étude vise à vérifier la conjecture faite par B. Gross relative à l'existence de corps de nombres de groupe de Galois non résoluble et ramifiés en un unique premier $p < 11$. À travers ce travail, nous nous intéressons au cas des corps de nombres de degré $n \leq 9$. Après quelques rappels généraux sur les outils utilisés, on présente les méthodes pratiques permettant de vérifier cette conjecture. Les travaux de J. Jones ont montré que les corps de nombres de degré 5 et 6 vérifiant ces types de ramification ont tous un groupe de Galois résoluble. Dans le cas du degré 7, S. Brueggeman a abouti au même résultat que le travail sus-cité.

Nos travaux dans le cas des degrés 8 et 9 montrent que sous GRH ou de façon inconditionnelle, la ramification en 5 n'est pas possible. À l'issue des recherches numériques, les seules tables obtenues sont celles de la ramification en $p = 2$ en degré 8 et celles de la ramification en $p = 3$ en degré 9. Les corps obtenus ont tous un groupe de Galois résoluble, montrant ainsi que cette conjecture de B. Gross n'est pas vérifiée pour les corps de nombres de degré $n \leq 9$.

Mots clefs : Groupe de Galois, Corps de nombres, Discriminant, Polynôme générateur, Exposant de Newton-Ore, Résoluble, Ramification.

Abstract : The current research examines the conjecture made by B. Gross on the existence of several number fields with a nonsolvable Galois group and which are ramified at exactly one prime p less than 11. The study concerns the number fields of degree $n \leq 9$. First of all, we focus on the instruments of the analysis, before presenting the methods that we used to solve the problem. The work of J. Jones showed that quintic and sextic number fields ramified only at one small prime are always solvable. Also, S. Brueggeman showed that septic number fields ramified only at one small prime are always solvable.

We eliminate octic and nonic number fields ramified only at 5 by using a method which depend on GRH or inconditionally by computer search. Our computer search also shows that only the ramification at $p = 2$ for the octic number fields and the ramification at $p = 3$ for the nonic number fields are possible. Note that all of these fields found have a solvable Galois group. We conclude that Gross's question has a negative answer for nonsolvable Galois group inside S_n, for $n \leq 9$.

Key words : Galois group, Number field, Discriminant, Generating polynomial, Newton-Ore exponent, Solvable, Ramification.

Thèse de **MATHEMATIQUES PURES**

Laboratoire A2X, Université Bordeaux 1,
351, Cours de la Libération 33405 Talence cedex.