Groupes, corps et extensions de Polya : une question de capitulation

Amandine Leriche

UNIVERSITÉ DE PICARDIE JULES VERNE
U.F.R DES SCIENCES
ÉCOLE DOCTORALE EN SCIENCES ET SANTÉ E.D. 368

THÈSE

présentée pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE PICARDIE JULES VERNE

Spécialité : Mathématiques

par

Amandine LERICHE

sous la direction du Pr. Jean-Luc CHABERT

Titre :

GROUPES, CORPS ET EXTENSIONS DE PÓLYA : UNE QUESTION DE CAPITULATION

soutenue publiquement le 1er décembre 2010

JURY

M. Paul-Jean CAHEN	Professeur, Université Paul Cezanne	Rapporteur
M. Jean-Luc CHABERT	Professeur, Université de Picardie Jules Verne	Directeur
M. Hedi DABOUSSI	Professeur Émerite, Université de Picardie Jules Verne	Examinateur
M. Fabien DURAND	Professeur, Université de Picardie Jules Verne	Examinateur
Mme Sophie FRISCH	Professeur, Technische Universität Graz	Examinateur
M. Keith JOHNSON	Professeur, Dalhousie University	Examinateur
M. Christian MAIRE	Professeur, Université de Franche-Comté	Rapporteur

Résumé

Dans cette thèse, nous nous intéressons à l'ensemble $Int(\mathcal{O}_K)$ des polynômes à valeurs entières sur l'anneau $\mathcal{O}_K$ des entiers d'un corps de nombres K. Selon Pólya, une base $(f_n)_{n\in\mathbb{N}}$ du $\mathcal{O}_K$-module $Int(\mathcal{O}_K)$ est dite régulière si pour tout $n \in \mathbb{N}$, $\deg(f_n) = n$. Un corps K tel que $Int(\mathcal{O}_K)$ possède une base régulière est dit de Pólya et le groupe de Pólya d'un corps de nombres K est un sous-groupe du groupe de classes de K qui peut être considéré comme une mesure de l'écart pour un corps au fait d'être de Pólya.

Nous étudions le groupe de Pólya d'un compositum $L = K_1K_2$ de corps de nombres galoisiens et établissons des liens avec la ramification des nombres premiers dans chacune des extensions $K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$. Nous appliquons ces résultats aux corps de nombres de petit degré afin d'élargir la famille des corps de Pólya quadratiques déjà caractérisés.

Par ailleurs, une condition pour qu'un corps de nombres K soit de Pólya est que tous les produits d'idéaux de K de même norme soient principaux. Par analogie avec le problème classique du plongement, on peut se poser la question suivante : tout corps de nombres K peut-il être plongé dans un corps de Pólya ? Nous donnons une réponse positive à cette question : pour tout corps K, le corps de classes de Hilbert H_K de K est un corps de Pólya .

Toujours par analogie avec le problème de plongement où l'on sait que les idéaux de $\mathcal{O}_K$ deviennent principaux dans $\mathcal{O}_{H_K}$, on peut définir la notion d'extension de Pólya d'un corps K : il s'agit de corps L contenant K dans lesquels le groupe de Pólya de K devient trivial par extensions des idéaux, ce sont aussi des corps L tels que le $\mathcal{O}_L$-module engendré par $Int(\mathcal{O}_K)$ possède une base régulière. Outre H_K dans le cas général, dans le cas où K est une extension abélienne, la capitulation des idéaux ambiges de K montre que le corps de genre de K en est une extension de Pólya. Ceci nous amène à des questions de minimalité et d'unicité concernant les corps et extensions de Pólya.

Abstract

In this thesis, we focus on the set $Int(\mathcal{O}_K)$ of integer-valued polynomials over $\mathcal{O}_K$, the ring of integers of a number field K. According to G. Pólya, a basis $(f_n)_{n\in\mathbb{N}}$ of the $\mathcal{O}_K$-module $Int(\mathcal{O}_K)$ is said to be regular if for each $n \in \mathbb{N}$, $\deg(f_n) = n$. A field K such that $Int(\mathcal{O}_K)$ has a regular basis is said to be a Pólya field and the Pólya group of number field K is a subgroup of the class group of K which can be considered as a measure of the obstruction for a field being a Pólya field.

We study the Pólya group of a compositum $L = K_1K_2$ of two galoisian extensions $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ and we link it to the behaviour of the ramification of primes in $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$. We apply these results to number fields with small degree in order to enlarge the well known family of quadratic Pólya fields.

Furthermore, a field K is a Pólya field if the products of all maximal ideals of $\mathcal{O}_K$ with the same norm are principal. Analogously to the classical embedding problem, we can set the following problem : is every number field contained in a Pólya field ? We give a positive answer to this question : for each number field K, the Hilbert class field H_K of K is a Pólya field.

We know also that every ideal of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_{H_K}$. This leads us to introduce the notion of Pólya extension : it is a field L containing K such that the Pólya group of K becomes trivial by extension of ideals, it is also a field L such that the $\mathcal{O}_L$-module generated by $Int(\mathcal{O}_K)$ has a regular basis. Consequently, H_K is a Pólya extension of K in the general case. Moreover, when K is abelian, capitulation of ambigeous ideals of K proves that the genus field of K is a Pólya extension. This leads us to consider minimality and unicity questions for Pólya fields and Pólya extensions.

Remerciements

Je tiens tout d'abord à exprimer ma gratitude envers celui qui a dirigé mes recherches durant ces trois années : Jean-Luc Chabert. Sa patience, sa sollicitude et ses connaissances ont été pour moi d'une valeur inestimable. Il a su me donner goût à la recherche en mathématiques, m'a plongé dans la très vaste et belle théorie des polynômes à valeurs entières. J'ai beaucoup appris à son contact et j'espère pouvoir travailler encore longtemps au sein du GTATN. Je tiens à en remercier chaque membre en qui j'ai trouvé un soutien constant durant ma thèse : David, notre base polynésienne (à valeurs entières) qui m'a souvent débloquée et aidée à résoudre mes problèmes, Jacques qui porte toujours un oeil vif et intéressé lors de chacun des exposés et à qui je dois un certain nombre de coups de pouce, Sabine, une complice avec qui j'ai partagé de très bons moments à Amiens mais aussi lors des colloques auxquels nous avons assisté, enfin Youssef, sans cesse en émulation, la source dynamique de notre groupe.

Je remercie Paul-Jean Cahen et Christian Maire qui ont accepté d'être les rapporteurs de ma thèse et qui m'ont prodigué de précieux conseils utiles pour la poursuite de mon travail. Je remercie également Hedi Daboussi, Fabien Durand, Sophie Frisch et Keith Johnson de me faire l'honneur de participer à mon jury de thèse.

Je souhaite également remercier tous les membres du LAMFA au sein duquel j'ai pu travailler dans d'excellentes conditions et dans une ambiance amicale. Un grand merci à Olivier Goubet, directeur du LAMFA, qui est toujours à l'écoute et prend grand soin de ses doctorants : il m'a permis de participer à de nombreux colloques en France comme à l'étranger où j'ai pu faire de très belles rencontres mathématiques. Je remercie tous les collègues doctorants avec qui j'ai pu travailler et échanger, un merci particulier à Guillaume qui a souvent été présent quand j'en avais besoin.

Enfin, je remercie chaleureusement ma famille : mes parents et grands-parents pour leur soutien constant dans ma vie et mes études. J'ai une pensée particulière pour mon grand-père qui aurait été très fier de voir ce projet

aboutir. Pour finir, je remercie infiniment Romain qui m'a aidée, supportée (surtout) durant ces trois années et qui a su créer autour de moi une atmosphère propice à l'élaboration de cette thèse.

Table des matières

Introduction

Dans les années 1910, Georg Pólya et Alexander Ostrowski ont introduit la notion de polynôme à valeurs entières sur un corps de nombres K. Il s'agit des polynômes $f(X)$ à coefficients dans K qui prennent des valeurs entières sur l'ensemble $\mathcal{O}_K$ des entiers de K. Pólya [33] s'est alors intéressé aux corps de nombres K pour lesquels l'ensemble $\mathrm{Int}(\mathcal{O}_K)$ des polynômes à valeurs entières sur $\mathcal{O}_K$ possède, en tant que $\mathcal{O}_K$-module, une base $(f_n)_{n\in\mathbb{N}}$ telle que $\deg(f_n) = n$ pour tout n. En 1982, Zantema [42] donna à ces corps le nom de corps de Pólya. Dans son article de 1919, Pólya remarqua qu'un corps de nombres est un corps de Pólya si et seulement si pour tout $n \geq 0$, l'idéal fractionnaire formé de 0 et des coefficients dominants des polynômes de $\mathrm{Int}(\mathcal{O}_K)$ de degré $\leq n$ est principal. Puis, en réponse à l'article de Pólya, Ostrowski [32] montre qu'un corps K est de Pólya si et seulement si, pour tout q puissance d'un nombre premier, les idéaux

$$\Pi_q(K) = \prod_{\substack{\mathfrak{m}\in Max(\mathcal{O}_K)\\ N(\mathfrak{m})=q}} \mathfrak{m}$$

sont principaux. Le groupe de Pólya $Po(K)$ est le sous-groupe du groupe des classes de K engendré par les classes des idéaux $\Pi_q(K)$. C'est en fait une mesure de l'obstruction pour un corps au fait d'être de Pólya. En effet, K est un corps de Pólya si et seulement si $Po(K) = \{1\}$.

Peu de travaux ont été réalisés sur le calcul du groupe de Pólya d'un corps de nombres quelconque et il reste beaucoup de questions, même dans le cas où $K/\mathbb{Q}$ est galoisienne et où $Po(K)$ correspond au groupe des classes des idéaux ambiges de K. Après un premier chapitre introductif aux notions abordées dans cette thèse, le deuxième chapitre est consacré à l'étude du groupe de Pólya d'un corps de nombres galoisien et plus particulièrement au compositum de deux corps de nombres galoisiens. Nous verrons que le comportement du groupe de Pólya est intimement lié à la ramification des premiers dans ce corps de nombres. Zantema [42] montre que le compositum de deux corps de Pólya galoisiens dont les degrés sont premiers entre eux est

encore un corps de Pólya. En fait, dans ces mêmes conditions, le groupe de Pólya du compositum est le produit direct du groupe de Pólya des deux corps composés. Nous obtenons au cours du second chapitre, des résultats similaires mais avec des conditions plus faibles sur les indices de ramification. Nous montrerons également que le nombre de premiers ramifiés dans un corps K de Pólya galoisien est majoré par une fonction du degré de l'extension $K/\mathbb{Q}$.

Au cours du troisième chapitre, les résultats obtenus lors du chapitre précédent sont appliqués aux corps de Pólya de petit degré. Nous parvenons à caractériser les corps de Pólya cycliques cubiques et quartiques. Nous étudions également les corps sextiques galoisiens, clôture galoisienne d'un corps cubique pur. Nous nous intéressons au compositum de deux corps quadratiques de Pólya qui est, sauf exceptions que l'on précisera, un corps biquadratique de Pólya.

Bien sûr, un corps dont l'anneau des entiers est principal est un corps de Pólya mais la réciproque est, en général, fausse : l'hypothèse K est un corps de Pólya est plus faible que l'hypothèse $\mathcal{O}_K$ est principal. On connaît le problème de plongement classique d'un corps de nombres K dans un corps L dont l'anneau des entiers est principal. En 1964, Golod et Schafarevitch ont donné une réponse négative à ce problème. En affaiblissant les hypothèses, on peut reformuler le problème de la manière suivante :

Est-ce que tout corps de nombres peut être plongé dans un corps de Pólya ?

Le contre-exemple donné par Golod et Schafarevitch, à savoir un corps quadratique imaginaire $K = \mathbb{Q}[\sqrt{d}]$ où d possède au moins six diviseurs premiers, n'en est pas un pour notre problème puisque tout corps quadratique est contenu dans un corps cylotomique qui, d'après Zantema, est un corps de Pólya. C'est en introduisant la notion d'extension de Pólya que nous parviendrons à répondre à cette question. Notre problème est, de façon évidente, équivalent au suivant :

Existe-t-il un corps L contenant K tel que pour tout $q \geq 2$,
les idéaux $\Pi_q(L)$ de l'anneau $\mathcal{O}_L$ soient principaux ?

Considérons le corps de classes de Hilbert H_K de K, les idéaux $\Pi_q(K)$ capitulent, c'est-à-dire deviennent principaux dans $\mathcal{O}_{H_K}$ mais on ignore, sans une étude préalable, si les idéaux $\Pi_q(H_K)$ sont principaux. Par analogie avec cette propriété, on introduit la notion d'extension de Pólya : l'extension L/K est de Pólya si, pour tout q puissance d'un nombre premier, l'idéal étendu $\Pi_q(K)\mathcal{O}_L$ est principal. Le corps de classes de Hilbert H_K de K est donc une

extension de Pólya. Le degré d'une extension de Pólya minimale de K est une nouvelle mesure de l'obstruction au fait que K soit un corps de Pólya.

On sait qu'une réponse positive au problème de plongement classique est équivalente, pour tout corps K, à une tour de corps de classes finie. Ayant défini la notion d'extension de Pólya par analogie avec les propriétés du corps de classes, on pourrait penser que notre problème est équivalent à une tour d'extensions de Pólya finie. Or, nous parvenons à construire explicitement, au cours du dernier chapitre, une tour d'extensions de Pólya $L_0 \subset L_1 \subset \dots L_i \subset \dots$ infinie telle que L_i ne soit jamais un corps de Pólya. Et pourtant, après l'étude des liens entre corps et extensions de Pólya dans le cas d'extensions non ramifiées, nous serons en mesure de donner une réponse positive au problème de plongement : tout corps de nombres est inclus dans un corps de Pólya, à savoir son corps de classes de Hilbert.

Si l'on souhaite raffiner ce résultat, en cherchant un corps de Pólya contenant K de degré minimal, on peut penser au corps de genre dans le cas abélien. En effet, il résulte des travaux de Furuya [15] que le corps de genre de K est une extension de Pólya de K, et par suite également un corps de Pólya. Mais même dans le cas quadratique, nous verrons que le corps de genre est loin d'être une réponse optimale au plongement dans un corps de Pólya. Enfin, nous montrons pour terminer qu'il n'y a pas unicité des extensions de Pólya non ramifiées minimales.

Chapitre 1

Groupes, corps et extensions de Pólya : une question de capitulation

Dans ce travail, K désigne un corps de nombres et $\mathcal{O}_K$ l'anneau des entiers de K.

1.1 Corps de Pólya et problème de plongement

1.1.1 Le problème des bases régulières

On rappelle la définition des polynômes à valeurs entières et celle des bases régulières, définitions introduites par Pólya [33] :

Définition 1.1. [33] On appelle *polynôme à valeurs entières* sur $\mathcal{O}_K$ tout polynôme $P \in K[X]$ tel que $P(\mathcal{O}_K) \subseteq \mathcal{O}_K$.

Notations. L'ensemble des polynômes à valeurs entières sur $\mathcal{O}_K$ est une $\mathcal{O}_K$-algèbre notée $\mathrm{Int}(\mathcal{O}_K)$. Ainsi,

$$\mathrm{Int}(\mathcal{O}_K) = \{P \in K[X] \,|\, P(\mathcal{O}_K) \subseteq \mathcal{O}_K\}.$$

Pour tout $n \in \mathbb{N}$, on note également

$$\mathrm{Int}_n(\mathcal{O}_K) = \{P \in \mathrm{Int}(\mathcal{O}_K) \mid \deg(P) \leq n\}$$

et $\mathfrak{I}_n(\mathcal{O}_K)$ le sous-ensemble de K formé de 0 et des coefficients dominants des polynômes de $\mathrm{Int}_n(\mathcal{O}_K)$.

Proposition 1.2. [10, Prop I.3.1] *Pour tout entier $n \geq 0$, $\mathfrak{I}_n(\mathcal{O}_K)$ est un idéal fractionnaire de $\mathcal{O}_K$. On appelle ces idéaux* idéaux caractéristiques *de l'anneau $\mathcal{O}_K$.*

Preuve. Soit $f = \alpha_0 + \alpha_1 X + \ldots + \alpha_n X^n \in K[X]$ et soient $x_0, \ldots, x_n$ des éléments distincts de $\mathcal{O}_K$. Alors, en écrivant que les $f(x_i)$ sont dans $\mathcal{O}_K$, les α_j vérifient un système de $n+1$ équations linéaires à coefficients dans $\mathcal{O}_K$ dont le déterminant est le déterminant de Vandermonde $d = \prod_{0 \leq i < j \leq n}(x_i - x_j)$. D'après la règle de résolution d'un système de Cramer, il vient, pour tout $i \in \{0, \ldots, n\}$, $d\alpha_i \in \mathcal{O}_K$.

□

Rappelons aussi :

Proposition 1.3. [10, Cor II.3.6] *Le $\mathcal{O}_K$-module $\mathrm{Int}_n(\mathcal{O}_K)$ est un module projectif de rang $n+1$. De plus,*

$$\mathrm{Int}_n(\mathcal{O}_K) \simeq \mathfrak{I}_0(\mathcal{O}_K) \oplus \mathfrak{I}_1(\mathcal{O}_K) \oplus \ldots \oplus \mathfrak{I}_n(\mathcal{O}_K).$$

Corollaire 1.4. [10, Rem II.3.7] *Le $\mathcal{O}_K$-module $\mathrm{Int}(\mathcal{O}_K)$ est un module libre.*

Preuve. Il existe un isomorphisme de $\mathcal{O}_K$-module de $\mathrm{Int}(\mathcal{O}_K)$ sur la somme $\oplus_{n=0}^{\infty}\mathfrak{I}_n(\mathcal{O}_K)$. Ainsi $\mathrm{Int}(\mathcal{O}_K)$ est un $\mathcal{O}_K$-module projectif qui n'est pas de type fini ; cela implique, selon un résultat de Bass [5], qu'il s'agit d'un module libre. □

Pólya a cherché à caractériser les corps pour lesquels $\mathrm{Int}(\mathcal{O}_K)$ possède ce qu'il appelle une base régulière :

Définition 1.5. [33] Une base $(f_n)_{n\in\mathbb{N}}$ du $\mathcal{O}_K$-module $\mathrm{Int}(\mathcal{O}_K)$ est dite *régulière* si pour tout $n \in \mathbb{N}$, $deg(f_n) = n$.

Remarque 1.6. Toutefois, il existe des corps K pour lesquels $\mathrm{Int}(\mathcal{O}_K)$ ne possède pas de base régulière, il n'est alors pas toujours facile d'exhiber une base. On trouve un tel exemple dans [18] avec le corps $K = \mathbb{Q}\left[\sqrt{-5}\right]$.

Zantema a introduit la définition suivante :

Définition 1.7. [42] Un corps de nombres K est dit *corps de Pólya* si son anneau des entiers $\mathcal{O}_K$ est tel que $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière.

Proposition 1.8. [10, Prop. II.1.4] *Une suite $\{f_n\}_{n\in\mathbb{N}}$ d'éléments de $\mathrm{Int}(\mathcal{O}_K)$ est une base régulière de $\mathrm{Int}(\mathcal{O}_K)$ si et seulement si, pour tout n, f_n est un polynôme de degré n dont le coefficient dominant engendre $\mathfrak{I}_n(\mathcal{O}_K)$ en tant que $\mathcal{O}_K$-module. En particulier, $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière si, et seulement si, les $\mathcal{O}_K$-modules $\mathfrak{I}_n(\mathcal{O}_K)$ sont des idéaux fractionnaires principaux de $\mathcal{O}_K$.*

Preuve. Soit $\{f_n\}_{n\in\mathbb{N}}$ une suite d'éléments de $\mathrm{Int}(\mathcal{O}_K)$ tels que $\deg(f_n) = n$. Notons a_n le coefficient dominant de f_n. Montrons que si $\{f_n\}_{n\in\mathbb{N}}$ est une base de $\mathrm{Int}(\mathcal{O}_K)$ alors, pour tout entier n, $\mathfrak{I}_n(\mathcal{O}_K) = a_n\mathcal{O}_K$. Pour tout $a \in \mathcal{O}_K$, $af_n \in \mathrm{Int}(\mathcal{O}_K)$ donc $a_n\mathcal{O}_K \subseteq \mathfrak{I}_n(\mathcal{O}_K)$. Par ailleurs, tout polynôme $g \in \mathrm{Int}(\mathcal{O}_K)$ de degré n s'écrit suivant cette base $g = \lambda_0 f_0 + \lambda_1 f_1 + \cdots + \lambda_n f_n$, où $\lambda_k \in \mathcal{O}_K$. En particulier, le coefficient dominant de g qui est $\lambda_n a_n$, appartient à $a_n\mathcal{O}_K$. On en déduit que $\mathfrak{I}_n(\mathcal{O}_K) = a_n\mathcal{O}_K$.

Réciproquement, supposons que, pour tout n, $\mathfrak{I}_n(\mathcal{O}_K) = a_n\mathcal{O}_K$. Si $f \in \mathrm{Int}(\mathcal{O}_K)$ est un polynôme de degré n dont le coefficient dominant est a alors $a = \lambda a_n$, où $\lambda \in \mathcal{O}_K$. En posant $g = f - \lambda f_n$, on a $g \in \mathrm{Int}(\mathcal{O}_K)$ et $\deg(g) < n$. On montre ainsi par récurrence que f est une combinaison linéaire dans $\mathcal{O}_K$ des polynômes f_k où $0 \leq k \leq n$. □

Remarque 1.9. Si $\mathcal{O}_K$ est principal, alors $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière. Par exemple, $\mathrm{Int}(\mathbb{Z})$ possède une base régulière [10, Prop. I.1.1] : il s'agit de la famille de polynômes binomiaux

$$\binom{X}{n} = \frac{X(X-1)\dots(X-n+1)}{n!}.$$

De même, $\mathrm{Int}(\mathbb{Z}[i])$ possède une base régulière. G. Gerboud [19] explicite un algorithme de construction d'une telle base régulière dont voici les premiers éléments :

$$G_0 = 1,\ G_1 = X,\ G_2 = \frac{1}{1+i}(X^2 - X),$$

$$G_3 = \frac{1}{1+i}(X^3 - X^2),\ G_4 = \frac{1}{(1+i)^3}(X^4 - 2X^3 - iX^2 + (1+i)X)$$

1.1.2 Un nouveau problème de plongement ?

Nous venons de voir que si $\mathcal{O}_K$ est principal, alors $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière. Cependant, il existe des anneaux d'entiers $\mathcal{O}_K$ non principaux tels que $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière. Par exemple, le corps $\mathbb{Q}[\sqrt{-23}]$ possède un nombre de classes égal à 3. L'anneau de ses entiers n'est donc pas principal mais on verra ultérieurement qu'il s'agit d'un corps de Pólya (cf. proposition 1.38) : l'hypothèse "K est de Pólya" est plus faible que l'hypothèse "$\mathcal{O}_K$ est principal".

On connaît le problème de plongement :

Est-ce que tout corps de nombres peut être plongé dans un corps L tel que $\mathcal{O}_L$ soit principal ?

En 1964, Golod et Shafarevitch [20] ont donné une réponse négative à cette question. Mais en reformulant le problème avec une hypothèse plus faible, il nous vient la question :

Est-ce que tout corps de nombres peut être plongé dans un corps de Pólya ?

On remarque que le contre-exemple donné par Golod et Schafarevitch au problème de plongement dans un corps de nombres de classe 1, à savoir un corps quadratique imaginaire $K = [\sqrt{d}]$ où d possède au moins six diviseurs premiers, n'est pas un contre-exemple pour le problème du plongement dans un corps de Pólya puisque tout corps quadratique est contenu dans un corps cyclotomique qui, on le verra, est toujours de Pólya (cf proposition 1.40).
Afin de tenter de répondre à cette question, nous allons considérer la notion de *groupe des idéaux factoriels* et étudier ses propriétés.

1.2 Groupe des idéaux factoriels

1.2.1 Idéaux factoriels de Bhargava

Rappelons que, dans $\mathcal{O}_K$, qui est un anneau de Dedekind, tout idéal fractionnaire non nul est inversible. Cela signifie que pour tout idéal fractionnaire non nul $\mathfrak{I}$, $\mathfrak{I}.\mathfrak{I}^{-1} = \mathcal{O}_K$ où $\mathfrak{I}^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}$. L'ensemble de ces idéaux fractionnaires non nuls de $\mathcal{O}_K$ forme un groupe, appelé groupe des idéaux fractionnaires que l'on notera $I(K)$. Pour simplifier, souvent, on appellera idéal de K (resp. idéal premier de K) un idéal de $\mathcal{O}_K$ (resp. un idéal maximal de $\mathcal{O}_K$).

C'est justement dans les anneaux de Dedekind que Bhargava ([3], [4]) a généralisé la notion de factorielle par la notion d'idéal factoriel. On peut définir ces idéaux de la façon suivante

Définition 1.10. Le *n-ième idéal factoriel de $\mathcal{O}_K$* est l'idéal :

$$(n!)_{\mathcal{O}_K} = \mathfrak{I}_n(\mathcal{O}_K)^{-1} = \{a \in \mathcal{O}_K \mid a\mathfrak{I}_n(\mathcal{O}_K) \subseteq \mathcal{O}_K\}.$$

Remarque 1.11.
1. Pour $K = \mathbb{Q}$, $(n!)_{\mathbb{Z}} = n!\mathbb{Z}$.
2. Pour tous m, $n \in \mathbb{N}$, l'idéal $(n!)_{\mathcal{O}_K}(m!)_{\mathcal{O}_K}$ divise l'idéal $((n+m)!)_{\mathcal{O}_K}$.

Rappels et notations. Comme $\mathcal{O}_K$ est de Dedekind, pour tout idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$, le localisé $(\mathcal{O}_K)_{\mathfrak{m}}$ est un anneau de valuation discrète. Pour chaque idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$, notons $v_{\mathfrak{m}}$ la valuation correspondante, $N(\mathfrak{m})$

la norme de $\mathfrak{m}$ (le cardinal du corps résiduel $\mathcal{O}_K/\mathfrak{m}$) et $w_\mathfrak{m}$ la fonction arithmétique définie par

$$w_\mathfrak{m}(n) = w_{N(\mathfrak{m})}(n) = \sum_{k=1}^{\infty} \left[\frac{n}{N(\mathfrak{m})^k} \right].$$

Remarque 1.12. Pour $K = \mathbb{Q}$ et $\mathfrak{m} = p\mathbb{Z}$ on a

$$w_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right] = v_p(n!).$$

C'est la formule de Legendre.

Comme un anneau d'entiers est noethérien, l'ensemble des polynômes à valeurs entières se comporte bien par localisation :

Proposition 1.13. *Pour tout idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$, on a :*

$$\mathrm{Int}\,(\mathcal{O}_K)_\mathfrak{m} = \mathrm{Int}\,((\mathcal{O}_K)_\mathfrak{m}).$$

Preuve. Soit $\mathfrak{m}$ un idéal maximal de $\mathcal{O}_K$. Montrons d'abord l'inclusion $\mathrm{Int}\,(\mathcal{O}_K)_\mathfrak{m} \subset \mathrm{Int}\,((\mathcal{O}_K)_\mathfrak{m})$. Soit $P \in \mathrm{Int}\,(\mathcal{O}_K)$. L'application polynomiale définie par P étant une application uniformément continue, on peut la prolonger par continuité au complété $\widehat{\mathcal{O}_K}$ de $\mathcal{O}_K$ relativement à la topologie $\mathfrak{m}$-adique en une application

$$\tilde{P} : \widehat{\mathcal{O}_K} \to \widehat{\mathcal{O}_K}.$$

Par ailleurs, comme $\widehat{\mathcal{O}_K} \cap K = (\mathcal{O}_K)_\mathfrak{m}$, en considérant la restriction de $\tilde{P}$ à $\widehat{\mathcal{O}_K} \cap K$, on obtient que $P \in \mathrm{Int}\,((\mathcal{O}_K)_\mathfrak{m})$.
Montrons l'inclusion inverse. Soit $P \in \mathrm{Int}\,((\mathcal{O}_K)_\mathfrak{m}))$, on a

$$\langle P\,(\mathcal{O}_K)\rangle \subseteq (\mathcal{O}_K)_\mathfrak{m} \cap C(P)$$

où $\langle P\,(\mathcal{O}_K)\rangle$ désigne le $\mathcal{O}_K$-module engendré par $P\,(\mathcal{O}_K)$ et où $C(P)$ désigne le $\mathcal{O}_K$-module engendré par les coefficients de P. Comme $\mathcal{O}_K$ est noethérien, $\langle P\,(\mathcal{O}_K)\rangle$ est un $\mathcal{O}_K$-module de type fini, donc engendré par un nombre fini d'éléments qui ont un dénominateur commun $d \in \mathcal{O}_K \setminus \mathfrak{m}$. Il vient $dP\,(\mathcal{O}_K) \subseteq \mathcal{O}_K$, d'où $P\,(\mathcal{O}_K) \subseteq (\mathcal{O}_K)_\mathfrak{m}$. □

Remarque 1.14. En fait, on sait [10, Théorème I.2.3] que, plus généralement, pour tout anneau intègre A et pour toute partie multiplicative S de A, on a

$$S^{-1}\mathrm{Int}(A) \subset \mathrm{Int}(S^{-1}A)$$

et, lorque A est noethérien, on a l'égalité

$$S^{-1}\mathrm{Int}(A) = \mathrm{Int}(S^{-1}A.)$$

Corollaire 1.15. *Pour tout $n \in \mathbb{N}$ et pour tout idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$,*

$$\mathfrak{I}_n\left(\mathcal{O}_K\right)_{\mathfrak{m}} = \mathfrak{I}_n\left(\left(\mathcal{O}_K\right)_{\mathfrak{m}}\right) \text{ et } \left((n!)_{\mathcal{O}_K}\right)_{\mathfrak{m}} = (n!)_{(\mathcal{O}_K)_{\mathfrak{m}}}$$

Preuve. Il est immédiat, d'après l'égalité précédente des $\left(\mathcal{O}_K\right)_{\mathfrak{m}}$-modules, que

$$\mathfrak{I}_n\left(\mathcal{O}_K\right)_{\mathfrak{m}} = \mathfrak{I}_n\left(\left(\mathcal{O}_K\right)_{\mathfrak{m}}\right).$$

Si $\mathfrak{I}^{-1}$ désigne l'inverse d'un idéal fractionnaire $\mathfrak{I}$ de $\mathcal{O}_K$, et si S est une partie multiplicative de $\mathcal{O}_K$, alors $S^{-1}\mathfrak{I}^{-1} = (S^{-1}\mathfrak{I})^{-1}$. Autrement dit l'inverse de l'ideal localisé est le localisé de l'idéal inverse. □

On obtient la décomposition des idéaux caractéristiques en produit d'idéaux maximaux :

Proposition 1.16. [33, Pólya] *Pour tout $n \in \mathbb{N}$ et pour tout idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$,*

$$v_{\mathfrak{m}}\left(\mathfrak{I}_n\left(\mathcal{O}_K\right)\right) = -w_{\mathfrak{m}}(n).$$

Autrement dit,

$$\mathfrak{I}_n\left(\mathcal{O}_K\right) = \prod_{\mathfrak{m} \in Max(\mathcal{O}_K)} \mathfrak{m}^{-w_{\mathfrak{m}}(n)}$$

1.2.2 Présentation du groupe des idéaux factoriels

Définition 1.17. Le *groupe des idéaux factoriels* de K est le sous-groupe du groupe $I(K)$ des idéaux fractionnaires non nuls de $\mathcal{O}_K$ engendré par les idéaux factoriels de $\mathcal{O}_K$. On le note $Fact\left(K\right)$.

Remarque 1.18. Le groupe des idéaux factoriels est, autrement dit, le sous-groupe de $I(K)$ engendré par les idéaux caractéristiques de $\mathcal{O}_K$.

Notations. Pour tout entier $q \geq 2$, notons $\Pi_q\left(K\right)$ ou plus simplement Π_q le produit de tous les idéaux maximaux de $\mathcal{O}_K$ de norme q. Autrement dit :

$$\Pi_q\left(K\right) = \prod_{\substack{\mathfrak{m} \in Max(\mathcal{O}_K) \\ N(\mathfrak{m}) = q}} \mathfrak{m}.$$

Si q n'est la norme d'aucun idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$, on pose

$$\Pi_q\left(K\right) = \mathcal{O}_K.$$

Proposition 1.19. [10, Prop. II.3.9] *Le groupe $Fact\left(K\right)$ est le sous-groupe abélien libre de $I\left(K\right)$ de base les idéaux $\prod_q\left(K\right)$ non triviaux.*

Preuve. Le sous-groupe $Fact\,(K)$ est contenu dans le sous-groupe des idéaux fractionnaires engendré par les $\Pi_q\,(K)$. En effet,

$$(n!)_{\mathcal{O}_K} = \prod_{\mathfrak{m}\in Max(\mathcal{O}_K)} \mathfrak{m}^{w_{\mathfrak{m}}(n)}.$$

Dans cette égalité, chaque idéal maximal $\mathfrak{m}$ de norme q apparait avec un exposant égal à $w_{\mathfrak{m}}(n) = w_q(n)$, il vient :

$$\prod_{2\leq q\leq n} \left(\prod_{N(\mathfrak{m})=q} \mathfrak{m} \right)^{w_q(n)} = \prod_{2\leq q\leq n} \Pi_q^{w_q(n)}.$$

On a l'inclusion inverse car $\Pi_2 = (2!)_{\mathcal{O}_K}$ et, comme $w_n(n) = 1$, on obtient

$$(n!)_{\mathcal{O}_K} = \Pi_n \times \prod_{2\leq q<n} \Pi_q^{w_q(n)},$$

et on peut donc vérifier par récurrence que, si les Π_q sont dans $Fact\,(\mathcal{O}_K)$ pour $q < n$, alors Π_n aussi. De plus, il n'y a pas de relations entre les idéaux Π_q, si l'on excepte ceux égaux à $\mathcal{O}_K$, car les idéaux maximaux intervenant dans deux Π_q distincts sont eux-mêmes distincts. □

Corollaire 1.20. *Le $\mathcal{O}_K$-module* $\mathrm{Int}\,(\mathcal{O}_K)$ *possède une base régulière si et seulement si, pour tout entier $q \geq 2$, Π_q est un idéal principal.*

Exemple 1.21. Cas des corps quadratiques : pour tout $p \in \mathbb{P}$, on a de façon immédiate :

- $p\mathcal{O}_K = \Pi_p$, si p est décomposé,
- $p\mathcal{O}_K = \Pi_{p^2}$ si p est inerte et,
- $p\mathcal{O}_K = \Pi_p^2$ si p est ramifié.

Les seuls idéaux Π_q éventuellement non principaux sont les idéaux Π_p où p est ramifié. Cependant, leur carré est principal. Ainsi, le groupe des idéaux factoriels de K possède au plus s_K générateurs non principaux, où s_K désigne le nombre de premiers ramifiés dans $K/\mathbb{Q}$.

1.3 Groupe de Pólya

On a vu que si $\mathcal{O}_K$ est principal alors $\mathrm{Int}\,(\mathcal{O}_K)$ possède une base régulière, autrement dit K est un corps de Pólya. Mais la principalité de $\mathcal{O}_K$ n'est pas nécessaire : à cet effet, on introduit un groupe qui peut être considéré comme une mesure de l'obstruction à ce que K soit de Pólya.

1.3.1 Définition

Rappels et notations. On rappelle que le groupe de classes de $\mathcal{O}_K$ est le quotient $Cl(K) = I(K)/P(K)$ du groupe $I(K)$ des idéaux fractionnaires non nuls de $\mathcal{O}_K$ par le groupe $P(K)$ des idéaux principaux non nuls.

Définition 1.22. On appelle *groupe de Pólya-Ostrowski* ou plus simplement *groupe de Pólya* de $\mathcal{O}_K$ l'image $Po(K)$ du groupe factoriel $Fact(K)$ dans le groupe des classes $Cl(K)$.

$$Po(K) = Fact(K)/P(K) \cap Fact(K)$$

Autrement dit : le groupe de Pólya de $\mathcal{O}_K$ est le sous-groupe de $Cl(K)$ engendré par les classes des idéaux factoriels $(n!)_{\mathcal{O}_K}$.

Remarque 1.23. $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière (ou encore K est de Pólya) si et seulement si $Po(K) = \{1\}$.

Proposition 1.24. *$Po(K)$ est engendré par les classes des idéaux Π_q.*

Exemple 1.25. Cas des corps quadratiques

Proposition 1.26. *Soit $K = \mathbb{Q}[\sqrt{d}]$ un corps quadratique où d désigne un entier sans facteurs carrés. Si le groupe $Po(K)$ n'est pas trivial, il a pour exposant 2. Si s_K désigne le nombre de diviseurs premiers du discriminant D_K de K, alors $Po(K)$ a au plus $s_K - 1$ générateurs et donc au plus 2^{s_K-1} éléments.*

Preuve. On rappelle que $D_K = d$ si $d \equiv 1 \pmod 4$ et $D_K = 4d$ si $d \equiv 2$ ou $3 \pmod 4$ et qu'un nombre premier est ramifié si, et seulement si, il divise D_K. On a vu que le groupe abélien $Po(K)$ est à priori engendrable par au plus s_K éléments et ceux-ci sont d'ordre au plus 2. Mais, si $p_1, \ldots, p_{s_K}$ sont les diviseurs de d et si $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s_K}$ désignent les idéaux premiers de $\mathcal{O}_K$ qui les relèvent, alors $\mathfrak{p}_1 \ldots \mathfrak{p}_{s_K} = \sqrt{d}\mathcal{O}_K$ est principal. Le groupe $Po(K)$ est ainsi engendré par au plus $s_K - 1$ générateurs. Donc le cardinal de $Po(K)$ divise 2^{s_K-1}.

□

La notion d'idéal ambige au sens de Hilbert permet de calculer le cardinal du groupe de Pólya.

1.3.2 Idéaux ambiges et groupe de Pólya

Faisons le lien entre groupe de Pólya et idéaux ambiges. Rappelons que si l'extension $K/\mathbb{Q}$ est galoisienne, un idéal $\mathfrak{a}$ de K est dit *ambige* si $\mathfrak{a}$ est globalement invariant par tous les éléments σ de $Gal(K/\mathbb{Q})$.

Proposition 1.27. *Soit $K/\mathbb{Q}$ une extension galoisienne.*

1. *Le groupe des idéaux factoriels de K est le groupe des idéaux ambiges de K.*
2. *Le groupe de Pólya de K est le sous-groupe du groupe des classes d'idéaux de $\mathcal{O}_K$ engendré par les classes des idéaux ambiges de K.*

Preuve. Dans le cas où $K/\mathbb{Q}$ est galoisienne, les idéaux de $\mathcal{O}_K$ stables sous l'action du groupe de Galois $G = Gal(K/\mathbb{Q})$ forment un sous-groupe $I(K)^G$ de $I(K)$. Ce sous-groupe n'est autre que le groupe engendré par les idéaux $\Pi_q(K)$ où q est une puissance d'un nombre premier p. En effet, les idéaux $\Pi_q(K)$ étant le produit des conjugués d'un idéal maximal divisant p, ils sont ambiges.
Réciproquement, soit $\mathfrak{A}$ un idéal ambige de $\mathcal{O}_K$. Soit $\mathfrak{Q}$ un idéal maximal de $\mathcal{O}_K$ divisant $\mathfrak{A}$, l'idéal $\mathfrak{Q}$ est au-dessus d'un nombre premier p, soit f le degré résiduel de $\mathfrak{Q}$. Posons $q = p^f$. Comme $\mathfrak{Q}$ divise $\mathfrak{A}$, pour tout $\sigma \in G$, $\sigma(\mathfrak{Q})$ divise $\sigma(\mathfrak{A}) = \mathfrak{A}$. Le produit des $\sigma(\mathfrak{Q})$ distincts quand σ décrit G est égal à $\Pi_q(K)$. Si on écrit $\mathfrak{A} = \Pi_q(K)\,\mathfrak{B}$, alors $\mathfrak{B}$ est ambige et par récurrence descendante, on voit que $\mathfrak{A}$ est engendré par les $\Pi_q(K)$.
Ainsi, $Po(K)$ est le sous-groupe de $Cl(K)$ formé des classes des idéaux ambiges de K. □

Rappelons la notion historique d'idéal ambige.

Définition 1.28. [24] Soit K une extension galoisienne de $\mathbb{Q}$ de degré premier l. Son groupe de Galois est donc cyclique engendré par un élément σ. Un idéal $\mathcal{I}$ de K est *ambige au sens de Hilbert* s'il est inaltéré par l'action de σ et s'il n'est contenu dans aucun idéal principal de la forme $q\mathcal{O}_K$, où $q \in \mathbb{Z}$, $q \geq 2$.

Proposition 1.29. *Soit K une extension galoisienne de $\mathbb{Q}$ de degré premier l. Les idéaux premiers ambiges de K au sens de Hilbert sont exactement ceux qui sont au-dessus des nombres premiers ramifiés dans $K/\mathbb{Q}$.*

Preuve. Soit p un nombre premier et soit $\mathfrak{P}$ un idéal premier de K au dessus de p. On note e l'indice de ramification de p dans $K/\mathbb{Q}$, f son degré résiduel et g l'indice de décomposition. On a la relation $efg = l$, où l est un nombre premier. Trois cas se présentent :

– Soit $e = l$. Dans ce cas, $p\mathcal{O}_K = \mathfrak{P}^l$. Le nombre p est totalement ramifié.

– Soit $f = l$. Dans ce cas, $p\mathcal{O}_K = \mathfrak{P}$. Le nombre p est inerte.
– Soit $g = l$. Dans ce cas, $p\mathcal{O}_K = \mathfrak{P}\mathfrak{P}_1 \dots \mathfrak{P}_{l-1}$. Le nombre p est totalement décomposé.

Si p est totalement décomposé dans $\mathcal{O}_K$, $\sigma(\mathfrak{P}) \neq \mathfrak{P}$ car les idéaux $\mathfrak{P}_i$ sont deux à deux conjugués. Puis, si p est inerte, $\mathfrak{P}$ est contenu dans $p\mathcal{O}_K$. Ainsi, si $\mathfrak{P}$ est ambige au sens de Hilbert, il est au dessus d'un nombre premier ramifié. Réciproquement, supposons que p se ramifie dans l'extension $K/\mathbb{Q}$. On a $\sigma(\mathfrak{P})^l = \sigma\left(\mathfrak{P}^l\right) = \sigma(p\mathcal{O}_K) = p\mathcal{O}_K = \mathfrak{P}^l$. D'où $\sigma(\mathfrak{P}) = \mathfrak{P}$. De plus, $\mathfrak{P}$ ne peut être contenu dans un idéal $q\mathcal{O}_K$, $q \in \mathbb{Z}$, $q \geq 2$. En effet, si c'était le cas, q^l diviserait $\mathfrak{P}^l$, donc p. □

Remarque 1.30. Dans toute la suite lorsque l'on parlera d'idéal ambige sans précision, il s'agira d'idéal ambige au sens actuel.

Soit $\mathfrak{a}$ un idéal de K. Notons A sa classe dans le groupe de classes de K. Soit $\sigma(A)$ la classe de $\sigma(\mathfrak{a})$ dans $Cl(K)$. On vérifie aisément que $\sigma(A)$ ne dépend pas du choix du représentant de la classe de $\mathfrak{a}$.

Définition 1.31. On dit que la *classe* A est *ambige* lorsque $\sigma(A) = A$.

Notons qu'une classe ambige n'est pas toujours la classe d'un idéal ambige. Afin de déterminer le groupe de Pólya d'un corps K, nous allons nous intéresser aux classes ambiges déterminées par les idéaux ambiges de K.

1.3.3 Groupe de Pólya d'un corps quadratique

Dans la suite $K/\mathbb{Q}$ est une extension quadratique et le groupe de Galois de cette extension est engendré par σ. On note s_K ou plus simplement s le nombre de diviseurs premiers du discriminant D_K de K.

On a vu que les idéaux premiers ambiges au sens de Hilbert de $\mathcal{O}_K$ sont ceux qui étaient au-dessus des nombres premiers ramifiés dans $K/\mathbb{Q}$. Ainsi :

Théorème 1.32. [24, Hilbert,§73] *Si K est un corps quadratique, les s idéaux premiers $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ au dessus des nombres premiers $p_1, \dots, p_s$ divisant le discriminant de K sont ambiges et il n'y a pas d'autres idéaux premiers ambiges au sens de Hilbert que ceux-ci. Les 2^s idéaux*

$$\mathcal{O}_K, \mathfrak{P}_1, \dots, \mathfrak{P}_s, \mathfrak{P}_1\mathfrak{P}_2, \dots, \mathfrak{P}_1\mathfrak{P}_2 \dots \mathfrak{P}_s$$

forment l'ensemble de tous les idéaux ambiges au sens de Hilbert de $\mathcal{O}_K$.

Preuve. Le fait qu'il n'y ait pas d'autres idéaux premiers ambiges que $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ résulte de la proposition 1.29. Considérons $\mathfrak{A}$ un idéal ambige de

$\mathcal{O}_K$ et soit $\mathfrak{A} = \mathfrak{Q}_1^{\alpha_1}, \ldots, \mathfrak{Q}_r^{\alpha_r}$ sa décomposition en idéaux premiers. Comme $\mathfrak{A} = \sigma(\mathfrak{A})$, $\sigma(\mathfrak{Q}_i) = \mathfrak{Q}_j$, $i, j \in \{1, \ldots, r\}$. Si $i \neq j$, alors $\mathfrak{A}_i$ serait au dessus d'un permier q décomposé. Or $\mathfrak{A}$ est contenu dans $\mathfrak{Q}_i\mathfrak{Q}_j$ et serait donc contenu dans $\sigma(\mathfrak{Q}_i)\,\mathfrak{Q}_i = q\mathcal{O}_K$ mais alors $\mathfrak{A}$ ne serait pas ambige au sens de Hilbert. Ainsi $\sigma(\mathfrak{Q}_i) = \mathfrak{Q}_i$. Donc les $\mathfrak{Q}_i$ sont ambiges au sens de Hilbert puisque si $\mathfrak{Q}_i$ était contenu dans un idéal de la forme $q\mathcal{O}_K$ où $q \in \mathbb{Z}$, $q \geq 2$, $\mathfrak{A}$ le serait a fortiori, puisque $\mathfrak{A}$ est contenu dans $\mathfrak{Q}_i$ pour tout i. Par ailleurs, comme le carré des idéaux $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ est divisible par un entier, les entiers α_i sont égaux à 1. □

Cherchons les classes ambiges qui résultent des 2^s idéaux ambiges. Pour cela rappelons la définition de Hilbert concernant les classes d'idéaux indépendantes.

Définition 1.33. [24] Plusieurs *classes d'idéaux* sont *indépendantes* lorsqu'aucune d'elle n'est égale à la classe de $\mathcal{O}_K$, c'est-à-dire à la classe principale et lorsqu'aucune classe n'est engendrée par les autres classes.

Théorème 1.34. [24, §75] *Si K est un corps quadratique, les s idéaux premiers ambiges au sens de Hilbert déterminent toujours $s-1$ classes indépendantes dans le cas d'un corps quadratique imaginaire. Dans le cas réel, ils déterminent $s-1$ (resp. $s-2$) classes indépendantes si la norme de l'unité fondamentale est égale -1 (resp. $+1$). Autrement dit, $|Po(K)| = 2^{s-1}$ ou 2^{s-2}.*

Compte tenu de l'importance pour nous de cet énoncé, nous en redonnons la preuve selon Hilbert.

Preuve. Débarrassons-nous du cas de $\mathbb{Q}[i]$ et $\mathbb{Q}[\sqrt{-3}]$. Dans l'extension, $\mathbb{Q}[i]/\mathbb{Q}$, seul 2 est ramifié, l'idéal premier au-dessus de 2 est principal car engendré par $(1+i)$. Dans l'extension $\mathbb{Q}[\sqrt{-3}]/\mathbb{Q}$, seul 3 est ramifié, l'idéal premier au-dessus de 3 est principal, il s'agit de $\sqrt{-3}\mathcal{O}_K$. D'ailleurs, on sait bien que dans les deux cas, l'anneau des entiers est principal.

Nous cherchons des relations entre les idéaux ambiges. Plus précisement, nous recherchons des indices $i_1, \ldots, i_k$ et des exposants $\alpha_1, \ldots, \alpha_k$ tels que $\mathfrak{P}_{i_1}^{\alpha_1} \ldots \mathfrak{P}_{i_k}^{\alpha_k}$ appartient à la classe principale ; c'est-à-dire qu'il existe $\alpha \in \mathcal{O}_K$ tel que $\mathfrak{P}_{i_1}^{\alpha_1} \cdot \ldots \cdot \mathfrak{P}_{i_k}^{\alpha_1} = \alpha\mathcal{O}_K$.

Comme les idéaux $\mathfrak{P}_{i_j}$, $j \in \{1, \ldots, k\}$, sont ambiges, $\sigma(\alpha) = \alpha$. On exclut les puissances paires des $\mathfrak{P}_{i_j}$, $j \in \{1, \ldots, k\}$ car celles-ci sont dans la classe principale. On est ramené à étudier des relations du type $\mathfrak{P}_{i_1} \ldots \mathfrak{P}_{i_k} = \alpha\mathcal{O}_K$ où $\alpha\mathcal{O}_K$ est ambige. La connaissance de la forme des idéaux principaux ambiges au sens de Hilbert permettra de déterminer le nombre de classes indépendantes (cf propositions 1.35 et 1.37). □

Proposition 1.35. *Si K est un corps quadratique imaginaire, les s idéaux premiers ambiges au sens de Hilbert déterminent $s-1$ classes indépendantes.*

Preuve. Les unités de $\mathcal{O}_K$ sont 1 et -1. Notons D_K le discriminant de K. Pour $i \in \{1, \ldots, s\}$, les idéaux premiers ambiges sont les $\mathfrak{Q}_i$ au dessus des nombres premiers q_i divsant D_K

1. Tout d'abord, étudions le cas où $m \equiv 1 \pmod 4$. Nous savons que $D_K = m = q_1 \ldots q_s$ (m est sans facteurs carrés), et donc $\mathfrak{Q}_1 \ldots \mathfrak{Q}_s = \sqrt{m}\mathcal{O}_K$, ce qui donne une relation entre les classes des idéaux premiers ambiges. En revanche, pour $k < s$, aucun produit de k idéaux parmi les $\mathfrak{Q}_i$ n'est principal. En effet si, quitte à renuméroter, il existait $\alpha \in \mathcal{O}_K$ tel que $\mathfrak{Q}_1 \ldots \mathfrak{Q}_k = \alpha\mathcal{O}_K$, on aurait $\alpha^2 = \pm q_1 \ldots q_k$, donc $K = \mathbb{Q}(\sqrt{m})$ contiendrait soit $\sqrt{q_1 \ldots q_k}$ soit $\sqrt{-q_1 \ldots q_k}$ et on aboutit à une contradiction. Notons que ceci implique en particulier que pour $s \geq 2$, aucun idéal $\mathfrak{Q}_i$ n'est principal.
2. Traitons ensuite le cas où $m \equiv 2, 3 \pmod 4$. Il est bien connu que $D_K = 4m$. Convenons que $q_1 = 2$. Si $m = -2$, alors $s = 1$ et $\mathfrak{Q}_1 = \sqrt{m}\mathcal{O}_K$. Sinon, $s \geq 2$ et $\mathfrak{Q}_2 \ldots \mathfrak{Q}_s = \sqrt{m}\mathcal{O}_K$, ce qui donne une relation entre les classes des $\mathfrak{Q}_i$ et c'est la seule. En effet, si un autre produit d'idéaux $\mathfrak{Q}_i$ était principal, de la forme $\alpha\mathcal{O}_K$, on aurait alors soit $\alpha^2 = \pm 2d$ ou $\alpha^2 = \pm d$, pour un diviseur d de m (suivant que le facteur $\mathfrak{Q}_1$ apparaisse ou non dans ce produit). Dans tous les cas, $K = \mathbb{Q}(\sqrt{m})$ contiendrait la racine carrée $\sqrt{n}$ d'un entier n sans facteur carré distinct de m et on aurait une contradiction.

Ainsi, on exprime l'un des s idéaux premiers ambiges au sens de Hilbert au moyen de $\sqrt{m}\mathcal{O}_K$ et des $s-1$ autres. □

Déterminons ensuite la forme des idéaux ambiges principaux d'un corps quadratique réel.

Lemme 1.36. *Soit $K = \mathbb{Q}(\sqrt{m})$ où m est un entier ≥ 2 sans facteurs carrés. Notons ϵ l'unité fondamentale de K.*

1. *Si $N(\epsilon) = -1$, les seuls idéaux principaux ambiges au sens de Hilbert sont $\mathcal{O}_K$ et $\sqrt{m}\mathcal{O}_K$.*
2. *Si $N(\epsilon) = +1$, il existe alors $\alpha \in \mathcal{O}_K$, non divisible par un entier ≥ 2 tel que $\frac{\alpha}{\sigma(\alpha)} = \epsilon$ et*
   - *les idéaux $\mathcal{O}_K$, $\sqrt{m}\mathcal{O}_K$ et $\alpha\mathcal{O}_K$ sont trois idéaux distincts ambiges au sens de Hilbert*
   - *le seul autre idéal principal ambige au sens de Hilbert est celui obtenu en débarrassant $\alpha\sqrt{m}$ de tout facteur entier ≥ 2.*

Preuve. **1er cas :** $N(\epsilon) = -1$**.** Soit $\beta \in \mathcal{O}_K$ tel que $\beta\mathcal{O}_K$ soit ambige au sens de Hilbert. Alors en particulier, $\sigma(\beta)$ et β engendrent le même idéal, donc $f \in \mathbb{Z}$ tel que $\sigma(\beta) = \pm\epsilon^f\beta$. Prenant les normes, comme β et $\sigma(\beta)$ ont même norme et $N(\epsilon) = -1$, on voit que f doit être pair, soit $f = 2f'$.
Considérons $\gamma = \epsilon^{f'}\beta$. De la relation $N(\epsilon) = \epsilon\sigma(\epsilon) = -1$, on tire $\sigma(\epsilon) = -\epsilon^{-1}$ et donc

$$\sigma(\gamma) = \pm\epsilon^{-f'}\sigma(\beta) = (\pm\epsilon^{-f'})(\pm\epsilon^f\beta) = \pm\epsilon^{-f'}\beta = \pm\gamma.$$

Si $\sigma(\gamma) = \gamma$, alors $\gamma \in \mathbb{Z}$ et si $\sigma(\gamma) = -\gamma$, alors $\gamma \in \sqrt{m}\mathbb{Z}$. Par ailleurs, $\beta\mathcal{O}_K = \gamma\mathcal{O}_K$ (puisque γ est le produit de β par unité). Comme l'idéal est ambige au sens de Hilbert, il en résulte que $\beta\mathcal{O}_K = \mathcal{O}_K$ ou bien $\beta\mathcal{O}_K = \sqrt{m}\mathcal{O}_K$.
2nd cas : $N(\epsilon) = +1$**.** D'après le théorème 90 de Hilbert, il existe $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$ tel que $\frac{\alpha}{\sigma(\alpha)} = \epsilon$ et, bien sûr, $\alpha\mathcal{O}_K$ est ambige. Les trois idéaux $\mathcal{O}_K$, $\sqrt{m}\mathcal{O}_K$ et $\alpha\mathcal{O}_K$ sont distincts, car sinon il existe $e \in \{0, 1\}$ et $f \in \mathbb{Z}$ tels que $\alpha = (-1)^e\epsilon^f$ ou $\alpha = (-1)^e\epsilon^f\sqrt{m}$, d'où $\frac{\alpha}{\sigma(\alpha)} = \epsilon^{2f}$; or, $\epsilon^{2f} \neq \epsilon$.
Soit $\beta\mathcal{O}_K$ un idéal ambige. Alors, il existe $e \in \{0, 1\}$ et $f \in \mathbb{Z}$ tels que $\beta = (-1)^e\epsilon^f\sigma(\beta)$. D'où

$$\frac{\beta}{\sigma(\beta)} = \left(\frac{\sqrt{m}}{\sigma(\sqrt{m})}\right)^e \left(\frac{\alpha}{\sigma(\alpha)}\right)^f.$$

Ainsi $\gamma = \frac{\beta}{(\sqrt{m})^e\alpha^f}$ vérifie $\frac{\gamma}{\sigma(\gamma)} = 1$, donc $\gamma = r \in \mathbb{Z}$ et $\beta = r\sqrt{m}^e\alpha^f$. Si $\beta\mathcal{O}_K$ est ambige au sens de Hilbert, $r = \pm 1$, $e = 0$ ou 1, $f = 0$ ou 1. On trouve quatre idéaux principaux ambiges : $\mathcal{O}_K$, $\sqrt{m}\mathcal{O}_K$, $\alpha\mathcal{O}_K$ et $\beta\mathcal{O}_K$ où $\sqrt{m}\alpha$ est débarrassé de tout facteur entier ≥ 2.

□

Proposition 1.37. *Soit K un corps quadratique réel, les s idéaux premiers ambiges au sens de Hilbert déterminent $s-1$ (resp. $s-2$) classes indépendantes si la norme de l'unité fondamentale est égale -1 (resp. $+1$).*

Preuve. On exprime l'un des s idéaux premiers ambiges au moyen de $\sqrt{m}\mathcal{O}_K$ et des $s-1$ autres idéaux premiers ambiges et lorsque le corps K est réel et que $N(\epsilon) = 1$, on choisira parmi ces $s-1$ idéaux premiers ambiges un idéal particulier que nous exprimerons au moyen de α et des $s-2$ autres (compte tenu du théorème 1.32). □

On obtient ainsi une caractérisation des corps quadratiques de Pólya.

Proposition 1.38. [10, Cor. II.4.5] *Un corps quadratique $\mathbb{Q}\left[\sqrt{d}\right]$ est un corps de Pólya si et seulement si d satisfait l'une des conditions suivantes :*

1. $d = -1$, $d = -2$,
2. $d = -p$ *où* p *est un nombre premier et* $p \equiv 3 \pmod 4$,
3. $d = p$ *où* p *est un nombre premier,*
4. $d = 2p$ *où* p *est un nombre premier et soit*
   - *soit* $p \equiv 3 \pmod 4$
   - *soit* $p \equiv 1 \pmod 4$ *et l'unité fondamentale a pour norme* $+1$
5. $d = pq$ *où* p *et* q *sont des premiers tels que :*
   - *soit* $p, q \equiv 3$*(mod 4)*
   - *soit* $p, q \equiv 1$*(mod 4) et l'unité fondamentale a pour norme* $+1$

1.4 Corps et extensions de Pólya.

1.4.1 Corps de Pólya

On rappelle qu'un corps de nombres K est un corps de Pólya si $\mathrm{Int}(\mathcal{O}_K)$ possède une base régulière. On peut reformuler ceci de plusieurs façons :

Proposition 1.39. *Le corps* K *est de Pólya s'il vérifie l'une des assertions équivalentes suivantes :*

1. $\mathrm{Int}(\mathcal{O}_K)$ *possède une base régulière,*
2. *pour tout* $n \in \mathbb{N}$, *les idéaux* $(n!)_{\mathcal{O}_K}$ *sont principaux,*
3. *pour tout* $q \geq 2$, *les idéaux* $\Pi_q(K)$, *produits des idéaux maximaux de* $\mathcal{O}_K$ *de même norme* q, *sont principaux,*
4. *le groupe* $Po(K)$ *est trivial.*

Proposition 1.40. [42, Zantema] *Tout corps cyclotomique est de Pólya.*

Preuve. Soit $K = \mathbb{Q}[\mu_m]$ où μ_m est une racine primitive m-ième de l'unité. On rappelle que $\mathcal{O}_K = \mathbb{Z}[\mu_m]$ et que les nombres premiers ramifiés dans l'extension $K/\mathbb{Q}$ sont exactement les diviseurs de m. Soit p un nombre premier divisant m. Notons $r = v_p(m)$, $e = (p-1)p^{r-1}$, ζ une racine primitive p^r-ième de l'unité, $K_1 = \mathbb{Q}[\zeta]$ et $\mathcal{O}_{K_1} = \mathbb{Z}[\zeta]$. Alors p est le seul nombre premier ramifié dans l'extension $K_1/\mathbb{Q}$ et on a :

$$p\mathcal{O}_{K_1} = (\zeta - 1)^e \mathcal{O}_{K_1}.$$

Comme $(\zeta - 1)^e \mathcal{O}_{K_1}$ n'est pas ramifié dans l'extension K/K_1, le produit des idéaux maximaux de $\mathcal{O}_K$ au-dessus de p est égal au produit des idéaux maximaux de $\mathcal{O}_K$ au-dessus de l'idéal $(\zeta - 1)\mathcal{O}_{K_1}$ et c'est donc l'idéal principal $(\zeta - 1)\mathcal{O}_K$. □

Il est possible d'expliciter un générateur des idéaux $(n!)_{\mathcal{O}_K}$ lorsque K est un corps cyclotomique. Rappelons tout d'abord la manière dont se décompose un nombre premier dans un corps cyclotomique.

Proposition 1.41. [28] *Soit μ_m une racine primitive m-ième de l'unité et $K = \mathbb{Q}[\mu_m]$. Pour tout nombre premier p, le degré résiduel f_p et l'indice de ramfication e_p de p dans $K/\mathbb{Q}$ vérifient les égalités*

$$f_p = \min\left\{ f \geq 1 \mid p^f \equiv 1 \pmod{\frac{m}{p^{v_p(m)}}} \right\} \text{ et } e_p = \varphi\left(p^{v_p(m)}\right)$$

où φ désigne l'indicatrice d'Euler.

Proposition 1.42. *Soit μ_m une racine primitive m-ième de l'unité et $K = \mathbb{Q}[\mu_m]$. Pour tout $n \in \mathbb{N}$, on a*

$$(n!)_{\mathcal{O}_K} = \prod_{p \nmid m} p^{w_{p^{f_p}}(n)} \times \prod_{p \mid m} \left(1 - \mu_m^{\left(\frac{m}{p^{v_p(m)}}\right)}\right)^{w_{p^{f_p}}(n)} \mathbb{Z}[\mu_m].$$

Preuve. Soit p un nombre premier diviseur de m et $r = v_p(m)$. Nous avons les inclusions suivantes :

$$\begin{array}{c} \mathbb{Q}[\mu_m] \\ | \\ \mathbb{Q}[\mu_{p^r}] \\ | \\ \mathbb{Q} \end{array}$$

Dans ce cas, p est totalement ramifié dans $\mathbb{Q}[\mu_{p^r}]/\mathbb{Q}$ et il existe un unique idéal premier au dessus de p qui est $(1-\mu_{p^r})\mathbb{Z}[\mu_{p^r}]$. Par ailleurs, μ_m^{m/p^r} étant une racine primitive p^r-ième de l'unité, si $p \mid m$,

$$\Pi_{p^{f_p}}(K) = \left(1 - \mu_m^{\left(\frac{m}{p^{v_p(m)}}\right)}\right) \mathbb{Z}[\mu_m].$$

Soit p un premier ne divisant pas m. Le nombre p n'est donc pas ramifié dans $K/\mathbb{Q}$, il vient :

$$\Pi_{p^{f_p}}(K) = p\mathbb{Z}[\mu_m].$$

La décomposition des idéaux factoriels en produit d'idéaux $\Pi_q(K)$,

$$(n!)_{\mathcal{O}_K} = \prod_{2 \leq q \leq n} \Pi_q^{w_q(n)},$$

nous permet de conclure.

□

Proposition 1.43. [42] *Le sous-corps réel maximal $K = \mathbb{Q}[\mu_m + \mu_m^{-1}]$ du corps cyclotomique $\mathbb{Q}[\mu_m]$ est un corps de Pólya.*

Preuve. Si m est une puissance d'un nombre premier, seul un nombre premier est ramifié dans l'extension $K/\mathbb{Q}$. Comme nous le verrons dans la Proposition 2.8, le corps K est un corps de Pólya. Supposons que m ne soit pas une puissance d'un nombre premier. De plus, on suppose que si m est pair alors m est divisible par 4 ($\mu_{2m'} = -\mu_{m'}$) . Soit p un premier divisant m. Posons $m = qp^r$ où $r = v_p(m)$, $\zeta = \mu_m^q$ est une racine primitive p^r-ième de l'unité. Posons

$$a_p = (1-\zeta)(1+\mu_m)^{-\frac{m}{2}-q} \text{ si m est pair, et}$$

$$a_p = (1-\zeta)(1-\mu_m^{\frac{m+1}{2}})^{-m-2q} \text{ si m est impair.}$$

Comme $a_p = \bar{a_p}$ ($\bar{a_p}$ désignant le conjugué complexe de a_p), a_p appartient à K.
Par ailleurs, si m est pair, $(1+\mu_m)$ et, si m est impair, $(1-\mu_m^{\frac{m+1}{2}})$ sont des unités de $L = \mathbb{Q}[\mu_m]$. En effet, $N_{L/\mathbb{Q}}(1+\mu_m) = \Phi_m(-1)$ et $N_{L/\mathbb{Q}}(1-\mu_m^{\frac{m+1}{2}}) = \Phi_m(1)$. Or, si n est un entier > 0 et p un premier, on dispose des relations suivantes entre polynômes cyclotomiques

$$\Phi_{pn}(X) = \Phi_n(X^p) \text{ si } p \mid n$$
$$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)} \text{ si } p \not| n$$

En l'occurence, comme m n'est pas une puissance d'un nombre premier, on a $\Phi_m(1) = 1$ et, comme m est divisible par 4 lorsqu'il est pair, on a alors $\Phi_m(-1) = 1$.
On sait que

$$p\mathcal{O}_L = (1-\zeta)^e\mathcal{O}_L \text{ où } e = \varphi(p^r).$$

Par conséquent,

$$p\mathcal{O}_L = a_p^e\mathcal{O}_L.$$

En faisant appel au morphisme injectif j_K^L d'extension des idéaux que nous présentons au chapitre suivant, on obtient :

$$j_K^L(p\mathcal{O}_K) = j_K^L(a_p^e\mathcal{O}_K).$$

Par injectivité $p\mathcal{O}_K = a_p^e\mathcal{O}_K$. Ici $e = e_p(L/\mathbb{Q})$, or $e_p(K/\mathbb{Q}) \leq e_p(L/\mathbb{Q})$ et l'égalité précédente montre que $e_p(K/\mathbb{Q}) \leq e$. On en conclut que $e_p(K/\mathbb{Q}) = e_p(L/\mathbb{Q}) = e$ et

$$\Pi_{p^r}(K) = a_p\mathcal{O}_K.$$

□

On rappelle le théorème de Kronecker-Weber :

Théorème 1.44 (Kronecker, Weber)**.** *Tout corps de nombres abélien est contenu dans un corps cyclotomique* $\mathbb{Q}[\zeta_m]$ *(*$m \in \mathbb{N}$*).*

Corollaire 1.45. *Toute extension abélienne de* $\mathbb{Q}$ *est contenue dans un corps de Pólya.*

Par conséquent, dans le cas abélien nous avons une réponse positive au problème de plongement d'un corps de nombres dans un corps de Pólya. Deux questions naturelles se posent alors :

Dans le cas non abélien, cela est-il encore vrai ?

Dans le cas où K *est contenu dans un corps de Pólya, comment décrire une extension* L *de* K *de degré minimal telle que* L *soit un corps de Pólya ?*

Nous avons montré que le groupe de Pólya $Po(K)$ d'un corps de nombres K était une mesure de l'obstruction pour ce corps au fait d'être de Pólya, mesure donnée notamment par l'entier $|Po(K)|$. La question précédente nous conduit à introduire une autre mesure de cette obstruction.

Définition 1.46. Soit K un corps de nombres.

1. On appelle *corps de Pólya minimal au-dessus de* K toute extension L de K qui est un corps de Pólya et telle qu'aucune extension intermédiaire $K \subseteq M \subsetneq L$ ne soit un corps de Pólya.
2. On pose :

$$po_{corps}(K) = \inf_{K \subseteq L} \{\ [L : K] \mid L \text{ corps de Pólya}\}.$$

La question du problème de plongement d'un corps de nombres dans un corps de Pólya est donc équivalente a la question :

Pour tout corps de nombres K*, la quantité* $po_{corps}(K)$ *est-elle finie ?*

Si pour toute extension abélienne $K/\mathbb{Q}$, on note f_K le *conducteur* de K, à savoir le plus petit entier m tel que $K \subset \mathbb{Q}[\zeta_m]$, alors le corollaire 1.45 implique :

Pour toute extension abélienne K de $\mathbb{Q}$, on a l'inégalité :

$$po_{corps}(K) \quad \leq \quad \frac{\varphi(f_K)}{[K : \mathbb{Q}]}. \tag{1.1}$$

lorsque K est une extension abélienne réelle, d'après la proposition 1.43 on peut affiner cette majoration :

$$po_{corps}(K) \quad \leq \quad \frac{\varphi(f_K)}{2[K:\mathbb{Q}]}. \tag{1.2}$$

On peut ensuite se poser les deux questions suivantes :

1. Pour un corps de nombres K, y a-t-il un unique corps de Pólya minimal au dessus de K ?
2. Sinon, deux corps de Pólya minimaux au dessus d'un même corps K ont-ils même degré ?

1.4.2 Extensions de Pólya

On rappelle le problème de plongement classique :

Peut-on plonger un corps K dans un corps L tel que $\mathcal{O}_L$ soit principal ?

Le problème de plongement d'un corps K dans un corps L de Pólya est équivalent au problème suivant :

Existe-t-il un corps L tel que pour tout $q \geq 2$,
les idéaux $\Pi_q(L)$ de l'anneau $\mathcal{O}_L$ soient principaux ?

On sait que pour tout corps de nombres K, il existe une extension abélienne qui possède des qualités de principalité.

Définition 1.47. On appelle *corps de classes de Hilbert* (resp. *au sens restreint*) d'un corps de nombres K et on note H_K (resp. H_K^{res}), l'extension abélienne non ramifiée (resp. aux seules places finies) maximale de K.

Théorème 1.48. [34] *Le groupe de Galois de l'extension H_K/K est isomorphe à $Cl(K)$, le groupe de classes de K. Le degré de l'extension $[H_K : K]$ est donc égal à h_K, le nombre de classes de K.*

$$Gal(H_K/K) \simeq Cl(K), \;\; [H_K : K] = h_K.$$

Dans la suite de ce travail, pour un certain nombre premier p, nous serons amenés à travailler avec le p-corps de classes de Hilbert d'un corps de nombres.

Définition 1.49. On appelle *p-corps de classes de Hilbert* du corps K la p-extension maximale contenue dans H_K. On le note $H_K^{(p)}$.

Rappelons que pour un nombre premier p fixé, une extension K'/K est dite p-extension si elle est galoisienne et si son groupe de Galois est un p-groupe. Par conséquent, l'extension $H_K^{(p)}/K$ possède un groupe de Galois isomorphe au p-sous-groupe de Sylow du groupe des classes.

Théorème 1.50. [14, Capitulation, Fürtwangler] *Les idéaux de $\mathcal{O}_K$ deviennent principaux par extension à $\mathcal{O}_{H_K}$. Autrement dit, ces idéaux capitulent dans $\mathcal{O}_{H_K}$.*

Pour tout $q \geq 2$, l'idéal $\Pi_q(K)$ capitule dans $\mathcal{O}_{H_K}$. Mais $\Pi_q(H_K)$ n'est, à priori, pas nécessairement principal. Par analogie avec la propriété de H_K, définissons les extensions de Pólya :

Définition 1.51. Une extension de corps de nombres L/K est dite *extension de Pólya* si tous les idéaux $\Pi_q(K)$ capitulent dans $\mathcal{O}_L$.

Faisons le lien avec les polynômes à valeurs entières afin de justifier la terminologie.

Définition 1.52. Soit L une extension de K.

1. L'*ensemble des polynômes à valeurs entières sur $\mathcal{O}_K$ relativement à $\mathcal{O}_L$* est l'ensemble :
$$\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L) = \{P \in K[X] \,|\, P(\mathcal{O}_K) \subset \mathcal{O}_L\}.$$
2. Le *n-ième idéal factoriel de $\mathcal{O}_K$ relativement à $\mathcal{O}_L$* est l'idéal de $\mathcal{O}_L$ noté $n!_{\mathcal{O}_K}^{\mathcal{O}_L}$, inverse de l'idéal fractionnaire formé des coefficients dominants des polynômes de $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ de degré $\leq n$.
3. Si $Cl(\mathcal{O}_L)$ désigne le groupe des classes d'idéaux de $\mathcal{O}_L$, le *groupe de Pólya-Ostrowski* de $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ est le sous-groupe de $Cl(\mathcal{O}_L)$ engendré par les classes d'idéaux factoriels $n!_{\mathcal{O}_K}^{\mathcal{O}_L}$. On le note $Po(\mathcal{O}_K, \mathcal{O}_L)$.

Proposition 1.53. *Le $\mathcal{O}_L$-module engendré par* $\mathrm{Int}(\mathcal{O}_K)$ *est égal à l'anneau* $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$. *En particulier,*
$$n!_{\mathcal{O}_K}\mathcal{O}_L = n!_{\mathcal{O}_K}^{\mathcal{O}_L}.$$

Preuve. L'inclusion $\mathrm{Int}(\mathcal{O}_K) \subset \mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ entraîne que le $\mathcal{O}_L$ module engendré par $\mathrm{Int}(\mathcal{O}_K)$ est contenu dans $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$.

Montrons l'inclusion inverse. Posons pour simplifier $A = \mathcal{O}_K$ et $B = \mathcal{O}_L$. Soit $f \in \mathrm{Int}(A, B)$ de degré d. Soit $\mathfrak{m}$ un idéal maximal de A. On sait [10, Th. II.2.7] que comme $A_{\mathfrak{m}}$ est un anneau de valuation discrète à corps résiduel

fini de cardinal q, il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de K telle que les polynômes $(f_n)_{n\in\mathbb{N}}$ suivants forment une base régulière de $\mathrm{Int}(A_\mathfrak{m})$ qui est aussi égal à $\mathrm{Int}(A)_\mathfrak{m}$ (cf. proposition 1.13) :

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}.$$

Explicitons une telle suite $(a_n)_{n\in\mathbb{N}}$. En suivant [10, Prop. II.2.3], considérons un système complet de représentants $\{a_0, \ldots, a_{q-1}\}$ modulo $\mathfrak{m}$ et t une uniformisante. En décomposant n en base q, $n = n_r q^r + \ldots + n_1 q_1 + n_0$ où $0 \leq n_i < q$ pour tout i et en posant $a_n = a_{n_r} t^r + \ldots + a_{n_1} t + a_{n_0}$, la suite $(a_n)_{n\in\mathbb{N}}$ fournit une base régulière $(f_n)_{n\in\mathbb{N}}$ de $\mathrm{Int}(A_\mathfrak{m})$. La suite $(f_n)_{n\in\mathbb{N}}$ est en particulier une base de $L[X]$, donc il existe $\alpha_0, \ldots, \alpha_d$ dans L tels que

$$f(X) = \sum_{k=0}^{d} \alpha_k f_k(X).$$

Comme

$$f_k(a_j) \in A_\mathfrak{m} \text{ pour } 0 \leq j, k \leq d,$$

$$f_k(a_j) = 0 \text{ pour } 0 \leq j \leq d,$$

$$f_k(a_k) = 1,$$

$$f(a_j) \in B \text{ pour } 0 \leq j \leq d,$$

les $d+1$ coefficients α_k vérifient un système de $d+1$ équations linéaires dont la matrice est triangulaire, unimodulaire à coefficients dans $A_\mathfrak{m}$ et dont tous les seconds membres sont dans B. Par suite, les α_k sont dans $B_\mathfrak{m}$ et donc le B-module $\mathrm{Int}(A, B)$ est contenu dans le $B_\mathfrak{m}$-module engendré par $\mathrm{Int}(A)$. Ceci ayant lieu pour tout idéal $\mathfrak{m}$, $\mathrm{Int}(A, B)$ est contenu dans le B-module engendré par $\mathrm{Int}(A)$.

La suite de la proposition est prouvée par le fait que l'idéal $n!_{\mathcal{O}_K}\mathcal{O}_L$ est l'idéal inverse de l'idéal formé par les coefficients dominants de l'ensemble $\langle \mathrm{Int}_n(\mathcal{O}_K)\rangle_{(\mathcal{O}_L)}$ qui est égal à $\mathrm{Int}_n(\mathcal{O}_K, \mathcal{O}_L)$; mais l'idéal inverse formé par l'ensemble des coefficients dominants de $\mathrm{Int}_n(\mathcal{O}_K, \mathcal{O}_L)$ n'est autre que $n!_{\mathcal{O}_K}^{\mathcal{O}_L}$. □

On généralise alors toutes les propriétés obtenues sur $\mathrm{Int}(\mathcal{O}_K)$. En particulier :

Proposition 1.54. *Les assertions suivantes sont équivalentes :*

1. *Le $\mathcal{O}_L$-module $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ possède une base régulière.*

2. *Pour tout* $n \in \mathbb{N}$*, l'idéal* $n!_{\mathcal{O}_K}^{\mathcal{O}_L}$ *de* $\mathcal{O}_L$ *est principal.*
3. *Le groupe* $Po(\mathcal{O}_K, \mathcal{O}_L)$ *est trivial.*

Preuve. L'équivalence de 2 et 3 est évidente. L'équivalence de 1 et 2 se montre de façon analogue à celle de la proposition 1.8. □

Ces deux dernières propositions permettent de montrer :

Proposition 1.55. *L'extension* L/K *est une extension de Pólya si et seulement si le* $\mathcal{O}_L$*-module* $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ *possède une base régulière.*

Preuve. Supposons que L/K soit une extension de Pólya. Par définition, les idéaux étendus $\Pi_q(\mathcal{O}_K)\mathcal{O}_L$ sont principaux. Par ailleurs, les idéaux $n!_{\mathcal{O}_K}$ sont engendrés par les idéaux $\Pi_q(\mathcal{O}_K)$ et réciproquement. Les idéaux étendus $\Pi_q(\mathcal{O}_K)\mathcal{O}_L$ sont principaux si et seulement si les idéaux $n!_{\mathcal{O}_K}^{\mathcal{O}_L} = n!_{\mathcal{O}_K}\mathcal{O}_L$ sont principaux, d'après la proposition précédente, ceci est équivalent à dire que, $\mathrm{Int}(\mathcal{O}_K, \mathcal{O}_L)$ possède une base régulière.

□

Exemple 1.56.
1. Si K est un corps de Pólya, alors toute extension L/K est une extension de Pólya.
2. Tout corps de nombres K possède une extension de Pólya, à savoir H_K, le corps de classes de Hilbert de K.

Lemme 1.57. *Soit* I *un idéal de* $\mathcal{O}_K$ *dont la classe est d'ordre* r *dans* $Cl(K)$*. Écrivant* $I^r = \alpha\mathcal{O}_K$ *et notant* β *une racine* r*-ième de* I *alors* I *capitule dans* $K(\beta)$*.*

Preuve. En posant $L = K(\beta)$:

$$(I\mathcal{O}_L)^r = I^r\mathcal{O}_L = \alpha\mathcal{O}_L = \beta^r\mathcal{O}_L = (\beta\mathcal{O}_L)^r .$$

□

A fortiori, I capitule dans toute extension plus grande. Bien evidemment, $[K(\beta) : K] \leq r$. En fait, on verra plus loin que $[K(\beta) : K] = r$

Proposition 1.58. *Il existe une extension de Pólya de* K *dont le degré est inférieur au produit des ordres des classes des* $\Pi_q(K)$ *formant un système générateur de* $Po(K)$*.*

Preuve. Ayant choisi $\Pi_{q_1}, \ldots, \Pi_{q_l}$ dont les classes engengrent le groupe $Po(K)$, la classe de chaque Π_{q_i} est d'ordre r_i fini dans ce groupe. Il existe α_i tel que $\Pi_{q_i}^{r_i} = \alpha_i\mathcal{O}_K$. Pour tout entier i, soit $\beta_i \in \mathbb{C}$ tel que $\beta_i^{r_i} = u\alpha_i$ où $u \in \mathcal{O}_K^\times$.

D'après le lemme précédent, l'extension $L = K(\beta_1, \cdots, \beta_s)$ est une extension de Pólya de K. Ainsi les Π_{q_i} capitulent dans $\mathcal{O}_L$ et donc aussi tous les Π_q puisque les classes des Π_{q_i} engendrent $Po(K)$. Enfin, pour tout entier i, $[K(\beta_i) : K] \leq r_i$. □

Exemple 1.59. Soit $K = \mathbb{Q}\left(\sqrt{-d}\right)$ où d est un entier positif sans facteurs carrés possédant au moins 2 diviseurs premiers distincts (ceci nous assurant que K n'est pas un corps de Pólya). Soient $p_1, \ldots, p_s$ les diviseurs premiers du discriminant D_K de K. Seuls les idéaux Π_{p_i} sont susceptibles d'être non principaux dans $\mathcal{O}_K$. Pour tout $i \in \{1, \ldots, s\}$, $p_i\mathcal{O}_K = \Pi_{p_i}^2$ et l'ordre de la classe de Π_{p_i} dans $Po(K)$ est au plus égal à 2. La proposition précédente nous donne une extension de Pólya de K : $K\left(\sqrt{p_1}, \ldots, \sqrt{p_s}\right)$.

Remarque 1.60. Le type d'extension fournie par la proposition 1.58 n'est pas toujours incluse dans H_K. En effet, considérons $K = \mathbb{Q}\left(\sqrt{-15}\right)$. Le corps $L = K\left(\sqrt{-5}, \sqrt{3}\right)$ est une extension de Pólya de K et le nombre 2 est ramifié dans l'extension $\mathbb{Q}\left(\sqrt{-15}\right) \subset \mathbb{Q}\left(\sqrt{-5}, \sqrt{3}\right)$.

Remarque 1.61. Même si les idéaux d'un corps K capitulent dans son corps de classes de Hilbert H_K, il se peut que les idéaux de $\mathcal{O}_{H_K}$ ne soient pas tous principaux. De façon analogue, bien que les deux notions soient proches, une extension de Pólya n'est pas, en général, un corps de Pólya. En effet, au chapitre suivant, nous verrons que l'extension $\mathbb{Q}[\sqrt{-5}, \sqrt{2}]/\mathbb{Q}[\sqrt{-10}]$ est une extension de Pólya mais que le corps $\mathbb{Q}[\sqrt{-5}, \sqrt{2}]$ n'est pas un corps de Pólya.

Si une extension L/K est de Pólya, alors toute extension M de L est une extension de Pólya de K. D'où l'intérêt de trouver des extensions de Pólya de K minimales :

Définition 1.62. Soit K un corps de nombres.

1. On appelle *extension de Pólya minimale de K* toute extension de Pólya L de K telle qu'aucune extension intermédiaire $K \subseteq M \subsetneq L$ ne soit une extension de Pólya.
2. On pose :

$$po_{ext}(K) = \min_{K \subseteq L}\{\ [L : K] \mid L/K \text{ extension de Pólya}\}.$$

D'après l'exemple 1.56 et la proposition 1.58, pour tout corps de nombres K, on a les inégalités :

$$po_{ext}(K) \quad \leq \quad h_K \tag{1.3}$$

et

$$po_{ext}(K) \quad \leq \quad \prod_{\Pi_q(K)} \text{ ordre de la classe de } \Pi_q(K). \tag{1.4}$$

Bien sûr,

$$K \text{ de Pólya } \Leftrightarrow \ |Po(K)| = 1 \ \Leftrightarrow \ po_{corps}(K) = 1 \ \Leftrightarrow \ po_{ext}(K) = 1.$$

Si L/K est une extension de Pólya de degré minimal parmi les extensions de Pólya de K alors, bien sûr, L/K est une extension de Pólya minimale.

S'intéressant aux extensions de Pólya minimales, on peut d'abord chercher les extensions minimales pour la capitulation d'un idéal donné. De façon générale, soit K un corps de nombres et soit I un idéal de $\mathcal{O}_K$, une extension minimale de K pour la capitulation de I est une extension L/K dans laquelle I capitule et telle que I ne capitule dans aucune autre extension intermédiaire $K \subseteq M \subsetneq L$.

Lemme 1.63. *Soit M/K une extension de corps de nombres dont le degré vérifie $[M : K] = m$ et soit I un idéal de $\mathcal{O}_K$ qui capitule dans $\mathcal{O}_M$. Alors I^m est principal dans $\mathcal{O}_K$.*

Preuve. Comme I capitule dans $\mathcal{O}_M$, il existe $\alpha \in \mathcal{O}_M$ tel que $I\mathcal{O}_M = \alpha\mathcal{O}_M$. En appliquant à cette égalité la norme relative de l'extension M/K, dont on rappelera les propriétés au chapitre suivant, on obtient :

$$N_{M/K}(I\mathcal{O}_M) = N_{M/K}(\alpha)\mathcal{O}_K.$$

Or I est un idéal de $\mathcal{O}_K$, donc $N_{M/K}(I\mathcal{O}_K) = I^m$. □

Proposition 1.64. *Soit I un idéal de $\mathcal{O}_K$ dont la classe est d'ordre r dans $Cl(K)$. Écrivant $I^r = \alpha\mathcal{O}_K$ et notant β une racine r-ième de I, alors $K(\beta)$ est une extension minimale de K pour la capitulation de I. En outre $[K(\beta) : K] = r$.*

Preuve. Supposons qu'il existe une extension intermédiaire M entre K et $K(\beta)$ dans laquelle I capitule. Tout d'abord notons $m := [M : K]$. Il vient $m \leq r$. D'après le lemme précédent, I^m est principal dans $\mathcal{O}_K$ donc r divise m. On en déduit que $m = r$ et par conséquent $M = K(\beta)$. □

Corollaire 1.65. *Soient K un corps de nombres, p un nombre premier, $q = p^f$ tels que seul l'idéal $\Pi_q(K)$ ne soit pas principal dans $\mathcal{O}_K$. Soit d_q l'ordre de $\Pi_q(K)$ dans $Cl(K)$ et soit α tel que $\Pi_q(K)^{d_q} = \alpha\mathcal{O}_K$. Soit $\beta \in \mathbb{C}$ tel que $\beta^{d_q} = \alpha$. Il n'existe pas d'extension de Pólya intermédiaire entre K et $K(\beta)$.*

Exemple 1.66. Considérons le corps $K = \mathbb{Q}\left(\sqrt[3]{7}, j\right)$, grâce à un résultat qui sera donné ultérieurement à la proposition 3.7, seul $\Pi_3(K)$ n'est pas principal. En posant $L = \mathbb{Q}\left(\sqrt[3]{7}, \sqrt[3]{3}, j\right)$, l'extension L/K est une extension de Pólya minimale.

On peut alors se poser les questions suivantes :

1. Quelles relations a-t-on entre extensions de Pólya et corps de Pólya ?
2. Existe-t-il une unique extension de Pólya minimale ?
3. Deux extensions de Pólya minimales contenues dans $H(K)$ sont-elles isomorphes ?
4. Deux extensions de Pólya minimales ont-elles même degré ?
5. Quel lien peut on faire entre corps de Pólya minimal au dessus de K et extension de Pólya minimale de K ?

Chapitre 2

Groupe de Pólya dans le cas galoisien

Notations. Soit L/K une extension finie de corps de nombres. On note j_K^L le morphisme injectif d'extension des idéaux :

$$j_K^L : \mathcal{I} \in I(K) \mapsto \mathcal{I}\mathcal{O}_L \in I(L)$$

qui induit le morphisme

$$\epsilon_K^L : \overline{\mathcal{I}} \in Cl(K) \mapsto \overline{\mathcal{I}\mathcal{O}_L} \in Cl(L).$$

On note N_L^K le morphisme norme suivant [37, Chap I. §5] :

$$N_L^K : I(L) \mapsto I(K)$$

qui est déterminé par les valeurs qu'il prend sur chaque idéal maximal $\mathcal{N}$ de $\mathcal{O}_L$

$$N_L^K(\mathcal{N}) = \mathcal{M}^{f_{\mathcal{N}}(L/K)}$$

où $\mathcal{M} = \mathcal{N} \cap \mathcal{O}_K$ et $f_{\mathcal{N}}(L/K) = [\mathcal{O}_L/\mathcal{N} : \mathcal{O}_K/\mathcal{M}]$. On sait que ce morphisme norme généralise la notion de norme $N_{L/K}$ d'un élément x dans une extension L/K et celle de norme absolue d'un idéal à savoir :

$$N_L^K(x\mathcal{O}_L) = N_{L/K}(x)\mathcal{O}_K \text{ et } \left|N_{K/\mathbb{Q}}(I)\right| = Card(\mathcal{O}_K/I),$$

pour tout idéal entier I de K.

On rappelle que, puisque l'extension L/K est séparable, pour tout idéal $\mathcal{I}$ de $I(K)$ [37, Chap I. §5] :

$$N_L^K \circ j_K^L(\mathcal{I}) = \mathcal{I}^{[L:K]}.$$

Ce morphisme norme induit un morphisme

$$\nu_L^K : \overline{\mathcal{I}} \in Cl\,(L) \mapsto \overline{N_L^K\,(\mathcal{I})} \in Cl\,(K)\,.$$

Remarque 2.1. 1. La proposition 1.53 nous permet de souligner que l'image $\epsilon_K^L\,(Po(K))$ est le sous-groupe de $Cl(L)$ que nous avons noté $Po(K,L)$ (cf. définition 1.52).
2. En général, le morphisme ϵ_K^L n'est pas injectif, toutefois on a le résultat suivant :

Proposition 2.2. *Soit $n = [L : K]$ et soit $Cl(K)_{\hat{n}}$ le sous-groupe de $Cl(K)$ formé des éléments d'ordre premier à n. Alors, la restriction du morphisme ϵ_K^L au sous-groupe $Cl(K)_{\hat{n}}$ est injective.*

Preuve. L'application composée suivante est clairement injective :

$$\nu_L^K \circ \epsilon_{K\ |Cl(K)_{\hat{\mathrm{n}}}}^L : \overline{I} \in Cl(K)_{\hat{\mathrm{n}}} \mapsto \overline{I^n} \in Cl(K).$$

□

2.1 Groupe de Pólya d'une extension galoisienne de $\mathbb{Q}$

Dans ce paragraphe, nous étudions le groupe de Pólya d'un corps de nombres K extension galoisienne de $\mathbb{Q}$.

Rappels. Si K est une extension galoisienne de $\mathbb{Q}$, pour tout nombre premier p, les g_p idéaux maximaux de $\mathcal{O}_K$ au dessus de p ont le même indice de ramification $e_p = e_p\,(K/\mathbb{Q})$ et le même degré résiduel $f_p = f_p\,(K/\mathbb{Q})$ et l'on obtient

$$e_p f_p g_p = [K : \mathbb{Q}]\,.$$

De plus,

$$p\mathcal{O}_K = \prod_{\mathcal{M}|p} \mathcal{M}^{e_p} = \Pi_q\,(K)^{e_p} \text{ où } q = p^{f_p}$$

Par conséquent, on obtient

Proposition 2.3. [10] *Soit K une extension galoisienne finie de $\mathbb{Q}$.*

1. *Si $q = p^f$ où le nombre premier p n'est pas ramifié dans l'extension $K/\mathbb{Q}$, alors $\Pi_q\,(K)$ est principal.*

2. *Le groupe de Pólya de K est engendré par les classes des $\Pi_q(K)$ où $q = p^f$ et le nombre premier p est ramifié dans l'extension $K/\mathbb{Q}$*

Corollaire 2.4. *Soit K une extension galoisienne finie de $\mathbb{Q}$. Le morphisme naturel de $Fact(K)$ sur $Po(K)$ se factorise de la manière suivante :*

$$Fact(K) \overset{\psi}{\to} \oplus_{p\in\mathbb{P}}\mathbb{Z}/e_p\mathbb{Z} \overset{\phi}{\to} Po(K).$$

Preuve. $Fact(K)$ est le groupe abélien libre de base les idéaux $\Pi_q(K)$ non triviaux où $q = p^{f_p}$ et où p décrit l'ensemble $\mathbb{P}$ des nombres premiers. Tout idéal $\mathfrak{I}$ de $Fact(K)$ s'écrit de façon unique sous la forme $\prod_p \left(\prod_{p^{f_p}}(K)\right)^{k_p}$. On a donc un isomorphisme ψ tel que :

$$\begin{array}{ccc} Fact(K) & \overset{\psi}{\to} & \oplus_{p\in\mathbb{P}}\mathbb{Z} \\ \mathfrak{I} = \prod_p \left(\prod_{p^{f_p}}(K)\right)^{k_p} & \mapsto & (\ldots, k_p, \ldots) \end{array}$$

où $(\ldots, k_p, \ldots)$ est l'élément de $\oplus_{p\in\mathbb{P}}\mathbb{Z}$ dont la composante relative à p est k_p. Comme l'idéal $\left(\prod_{p^{f_p}}(K)\right)^{e_p}$ est principal, le morphisme de $Fact(K)$ vers $Po(K)$ se factorise à travers $\oplus_{p\in\mathbb{P}}\mathbb{Z}/e_p\mathbb{Z}$. Par conséquent, celui de $\oplus_{p\in\mathbb{P}}\mathbb{Z}$ vers $Po(K)$ également. □

Corollaire 2.5. *Soit K une extension galoisienne finie de $\mathbb{Q}$,*
- *l'exposant de $Po(K)$ divise $[K : \mathbb{Q}]$,*
- *l'ordre de $Po(K)$ divise le produit $\prod_p e_p$.*

Preuve. La première assertion résulte de ce que $Po(K)$ est engendré par les classes des idéaux $\Pi_{p^{f_p}}$, pour p ramifié. L'ordre de la classe de $\Pi_{p^{f_p}}$ divise l'indice de ramification e_p donc divise $[K : \mathbb{Q}]$ pour tout p ramifié. La seconde assertion résulte de la surjectivité du morphisme ϕ dans le corollaire précédent. □

Corollaire 2.6. *Soient q un nombre premier, $n \geq 1$ et $K/\mathbb{Q}$ une extension galoisienne telle que $[K : \mathbb{Q}] = q^n$. Soit $Cl_q(K)$ le q-groupe de classes de K. Nous avons l'inclusion $Po(K) \subset Cl_q(K)$.*

Preuve. D'après le corollaire précédent, l'exposant de $Po(K)$ est un diviseur de $[K : \mathbb{Q}]$. Si $[K : \mathbb{Q}] = q^n$, alors $Po(K)$ est un q-groupe. On en conclut que $Po(K) \subset Cl_q(K)$. □

Corollaire 2.7. *Soit K une extension galoisienne de $\mathbb{Q}$ de degré n et de nombre de classes h_K. Si n et h_K sont premiers entre eux, alors K est un corps de Pólya.*

Preuve. D'après le corollaire 2.5, on sait que l'exposant de $|Po(K)|$ divise n. De plus, $|Po(K)|$ divise $|Cl(K)| = h_K$. Comme n et h_K sont premiers entre eux, il en résulte que $Po(K)$ est d'exposant 1, donc trivial. □

Proposition 2.8. [42] *Soit $K/\mathbb{Q}$ une extension abélienne finie. Si un seul nombre premier p y est ramifié alors K est un corps de Pólya.*

Preuve. L'extension $K/\mathbb{Q}$ étant une extension abélienne, K est contenue dans un corps cyclotomique $L = \mathbb{Q}[\mu]$ où μ est une racine p^r-ième de l'unité. Posons $\zeta = N_{L/K}(\mu - 1)$. On a [36] :

$$p\mathcal{O}_L = (\mu - 1)^{[L:\mathbb{Q}]}\,\mathcal{O}_L,$$

et on obtient en appliquant N_L^K :

$$p\mathcal{O}_K = (\zeta\mathcal{O}_K)^{[K:\mathbb{Q}]}.$$

Ainsi, $\mathcal{O}_K$ possède un seul idéal maximal au-dessus de p, il s'agit de $\zeta\mathcal{O}_K$. □

Lorsqu'on est en présence d'extensions galoisiennes de $\mathbb{Q}$, les groupes de Pólya de K et L se comportent bien vis à vis des morphismes j, ϵ, N et ν introduits en début de chapitre :

Proposition 2.9. [11] *Si K et L sont deux extensions galoisiennes de $\mathbb{Q}$ telles que $K \subset L$ alors*

1. $$j_K^L(Fact(K)) \subseteq Fact(L) \;\; et\; \epsilon_K^L(Po(K)) \subseteq Po(L)$$
2. $$N_L^K(Fact(L)) \subseteq Fact(K) \;\; et\; \nu_L^K(Po(L)) \subseteq Po(K)$$

La vérification est immédiate.

Corollaire 2.10. *Soient K et L deux extensions galoisiennes de $\mathbb{Q}$ telles que $K \subset L$. L'extension L/K est de Pólya si et seulement si l'image $\epsilon_K^L(Po(K))$ est triviale dans $Po(L)$.*

En effet, l'extension L/K est de Pólya si et seulement si les idéaux étendus $\Pi_q(K)\mathcal{O}_L$ sont principaux.

Corollaire 2.11. *Dans l'hypothèse où K et L sont deux extensions galoisiennes de $\mathbb{Q}$ telles que $K \subset L$, si L est de Pólya alors L/K est une extension de Pólya.*

Preuve. Si L est de Pólya, $Po(L)$ est trivial, il en est de même pour l'image $\epsilon_K^L\left(Po\left(K\right)\right)$. □

Remarque 2.12. Si L est un corps de Pólya extension galoisienne de $\mathbb{Q}$, alors L est extension de Pólya de toutes ses sous-extensions K qui sont des extensions galoisiennes de $\mathbb{Q}$. Qu'en est-il pour les autres sous-extensions ? Qu'en est-il de la réciproque de cette assertion ? L'exemple 3.39 que nous étudierons au chapitre suivant montre qu'il existe un corps L qui n'est pas un corps de Pólya mais qui est une extension de Pólya pour tous ses sous-corps.

2.2 Groupe de Pólya du compositum de deux extensions galoisiennes de $\mathbb{Q}$

Dans [11], il est prouvé le résultat suivant :

Proposition 2.13. *Soient K_1 et K_2 deux extensions galoisiennes de $\mathbb{Q}$ et soit $L = K_1K_2$. Si $[K_1 : \mathbb{Q}]$ et $[K_2 : \mathbb{Q}]$ sont premiers entre eux, alors*

$$j_{K_1}^L\left(Fact\left(K_1\right)\right).j_{K_2}^L\left(Fact\left(K_2\right)\right) = Fact\left(L\right).$$

Nous allons tenter d'énoncer ce résultat avec des hypothèses plus faibles en notant que la condition sur le degré des extensions implique que :

1. K_1 et K_2 sont linéairement disjointes sur $\mathbb{Q}$.
2. Pour tout $p \in \mathbb{P}$, $e_p(K_1/\mathbb{Q})$ et $e_p(K_2/\mathbb{Q})$ sont premiers entre eux.

Commençons par rappeler d'abord quelques propriétés des extensions linéairement disjointes, puis des propriétés de multiplicativité des indices de ramification.

2.2.1 Extensions linéairement disjointes

Dans ce paragraphe, on rappelle la définition d'extensions linéairement disjointes et on donne uniquement les propriétés qui seront utilisées par la suite.

Définition 2.14. [6, Chap.V, §2, n°5] Soient K un corps quelconque et K_1, K_2 deux extensions finies de K. On dit que K_1 et K_2 sont *linéairement disjointes* sur K si il existe une base de K_2 sur K libre par rapport à K_1.

Notation. On note K_1K_2 le corps engendré par K_1 et K_2.

Proposition 2.15. *Soient K_1 et K_2 deux extensions finies de K,*

1. *K_1 et K_2 sont linéairement disjointes sur K si et seulement si*

$$[K_1K_2 : K_1] = [K_2 : K]$$

ou encore si et seulement si

$$[K_1K_2 : K] = [K_1 : K]\,[K_2 : K]\,.$$

2. *Si K_1 et K_2 sont linéairement disjointes sur K, alors $K_1 \cap K_2 = K$.*

La réciproque de cette dernière assertion est fausse. Toutefois,

Proposition 2.16. *Si K_1/K est galoisienne et si $K_1 \cap K_2 = K$ alors K_1 et K_2 sont linéairement disjointes sur K.*

En effet, si l'extension K_1/K est galoisienne, l'extension K_1K_2/K_2 est galoisienne et $Gal(K_1K_2/K_2) \simeq Gal(K_1/K_1 \cap K_2)$.

Corollaire 2.17. *Supposons que K_1/K_0 et K_2/K_0 soient galoisiennes et que $K_1 \cap K_2 = K$. Alors K_1K_2/K_0 est une extension galoisienne et on a l'isomorphisme $Gal\,(K_1K_2/K) \simeq Gal\,(K_1/K) \times Gal\,(K_2/K)$.*

2.2.2 Sur l'indice de ramification dans un compositum

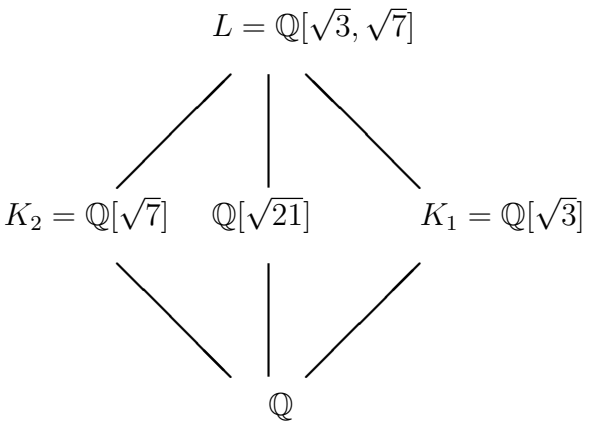
Notations. Soient K_1 et K_2 deux corps de nombres. Posons $K_1 \cap K_2 = K$ et $L = K_1K_2$. Pour tout idéal maximal $\mathfrak{M}$ de L, posons

$$\mathfrak{P}_1 = \mathfrak{M} \cap K_1, \mathfrak{P}_2 = \mathfrak{M} \cap K_2 \text{ et } \mathfrak{p} = \mathfrak{M} \cap K$$

Lorsque les extensions $K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$ sont galoisiennes et lorsque les degrés $[K_1 : K]$ et $[K_2 : K]$ sont premiers entre eux, il est aisé d'obtenir les égalités suivantes portant sur les indices de ramifications :

$$e(\mathfrak{M}/\mathfrak{p}) = e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p}). \tag{2.1}$$

Les degrés résiduels et nombres de décomposition vérifient une égalité semblable. Sans l'hypothèse "$[K_1 : K]$ et $[K_2 : K]$ premiers entre eux", cette égalité n'est, en général, pas vérifiée comme le montre le contre-exemple suivant.



On a donc $K = K_1 \cap K_2 = \mathbb{Q}$. Étudions la ramification de l'idéal premier $\mathfrak{p} = 2\mathbb{Z}$. On obtient $e(\mathfrak{p}_1/\mathfrak{p}) = e(\mathfrak{p}_2/\mathfrak{p}) = 2$ mais l'idéal $\mathfrak{p} = 2\mathbb{Z}$ n'étant pas ramifié dans la sous-extension $\mathbb{Q}[\sqrt{21}]$ de $L = \mathbb{Q}[\sqrt{3}, \sqrt{7}]$, $e(\mathfrak{M}/\mathfrak{p}) = 2 \neq e(\mathfrak{p}_1/\mathfrak{p})e(\mathfrak{p}_2/\mathfrak{p})$.

Remarque 2.18. La proposition 14.1.E de [34] est en contradiction avec cet exemple. En effet, elle affirme que lorsque K_1 et K_2 sont deux extensions galoisiennes de K telles que $K_1 \cap K_2 = K$ et $L = K_1K_2$ alors :

$$I_{\mathfrak{M}}(L/K) \simeq I_{\mathfrak{P}_1}(K_1/K) \times I_{\mathfrak{P}_2}(K_2/K), \tag{2.2}$$

où $I_{\mathfrak{M}}(L/K)$ (resp. $I_{\mathfrak{P}_1}(K_1/K)$, $I_{\mathfrak{P}_2}(K_2/K)$) désigne le groupe d'inertie de l'idéal $\mathfrak{M}$ (resp. $\mathfrak{P}_1$, $\mathfrak{P}_2$) dans l'extension L/K (resp. K_1/K, K_2/K).

Il est vrai que sous ces hypothèses $Gal\,(L/K) \simeq Gal\,(K_1/K) \times Gal\,(K_2/K)$ et que les images par restriction du sous-groupe $I_{\mathfrak{M}}(L/K)$ est le sous-groupe $I_{\mathfrak{P}_1}(K_1/K)$ de $Gal\,(K_1/K)$ et le sous-groupe $I_{\mathfrak{P}_2}(K_2/K)$ de $Gal\,(K_2/K)$ respectivement. Toutefois, nous ne pouvons en déduire l'égalité 2.2. Dans l'exemple précédent, $I_{\mathfrak{P}_1}(K_1/K) = I_{\mathfrak{P}_2}(K_2/K) \simeq \mathbb{Z}/2\mathbb{Z}$. Le groupe d'inertie $I_{\mathfrak{M}}(L/K)$ est en fait le troisième sous-groupe d'ordre 2 de $Gal\,(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et non le produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Rappelons donc quelques relations de divisibilité qui s'obtiennent de façon immédiate :

Lemme 2.19. *Soit K un corps de nombres et soient K_1 et K_2 deux extensions finies de K telles que $K_1 \cap K_2 = K$, $L = K_1K_2$.*

1. *L'indice $e(\mathfrak{M}/\mathfrak{p})$ est divisible par le ppcm de $e(\mathfrak{P}_1/\mathfrak{p})$ et de $e(\mathfrak{P}_2/\mathfrak{p})$.*
2. *Si $K_1/\mathbb{Q}$ ou $K_2/\mathbb{Q}$ est galoisienne, $e(\mathfrak{M}/\mathfrak{p})$ divise $e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p})$.*

3. Si $K_1/\mathbb{Q}$ ou $K_2/\mathbb{Q}$ est galoisienne et si $(e(\mathfrak{P}_1/\mathfrak{p}), e(\mathfrak{P}_2/\mathfrak{p})) = 1$ alors

$$e(\mathfrak{M}/\mathfrak{p}) = e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p}). \tag{2.3}$$

Preuve. 1. De façon générale, on a la relation immédiate :

$$e(\mathfrak{M}/\mathfrak{p}) = e(\mathfrak{M}/\mathfrak{P}_1)e(\mathfrak{P}_1/\mathfrak{p}). \tag{2.4}$$

Par suite, le ppcm de $e(\mathfrak{P}_1/\mathfrak{p})$ et de $e(\mathfrak{P}_2/\mathfrak{p})$ divise $e(\mathfrak{M}/\mathfrak{p})$.
2. Si l'extension K_2/K est galoisienne, L/K_1 l'est aussi. On a un isomorphisme induit par la restriction :

$$\sigma \in Gal(L/K_1) \mapsto \sigma_{|K_2} \in Gal(K_2/K).$$

L'image du groupe d'inertie $I_{\mathfrak{M}}(L/K_1)$ par σ est un sous-groupe du groupe d'inertie $I_{\mathfrak{P}_2}(K_2/K)$. Par suite,

$$e(\mathfrak{M}/\mathfrak{P}_1) \text{ divise } e(\mathfrak{P}_2/\mathfrak{p}). \tag{2.5}$$

On obtient ainsi que $e(\mathfrak{M}/\mathfrak{p})$ divise $e(\mathfrak{P}_1/\mathfrak{p})e(\mathfrak{P}_2/\mathfrak{p})$.
3. Cette assertion résulte des deux premières.

□

En fait, il existe un résultat beaucoup plus général énoncé chez [39] pour les corps de fonctions mais qui s'applique également aux corps de nombres :

Lemme 2.20. [39, Lemme d'Abhyankar] *Soit K un corps de nombres, K_1 et K_2 deux extensions finies de K. Soit $\mathfrak{M}$, un idéal maximal de $L = K_1K_2$. Soient $\mathfrak{P}_1 = \mathfrak{M} \cap K_1$, $\mathfrak{P}_2 = \mathfrak{M} \cap K_2$ et $\mathfrak{p} = \mathfrak{M} \cap K$. L'idéal premier $\mathfrak{p}$ est au-dessus d'un premier p. Si p ne divise pas $e(\mathfrak{P}_1/\mathfrak{p})$ ou bien $e(\mathfrak{P}_2/\mathfrak{p})$ alors l'indice de ramification $e(\mathfrak{M}/\mathfrak{p})$ vérifie*

$$e(\mathfrak{M}/\mathfrak{p}) = ppcm\left(e(\mathfrak{P}_1/\mathfrak{p}), e(\mathfrak{P}_2/\mathfrak{p})\right).$$

2.2.3 Groupe des idéaux factoriels et groupe de Pólya du compositum de deux extensions galoisiennes de $\mathbb{Q}$

Dans cette section, K_1 et K_2 désignent deux corps de nombres extensions galoisiennes de $\mathbb{Q}$. On sait que $L = K_1K_2$ est une extension galoisienne de $\mathbb{Q}$, on fait l'hypothèse que $K = K_1 \cap K_2$ est une extension galoisienne de $\mathbb{Q}$.

Proposition 2.21. *Soient K, K_1 et K_2 des extensions galoisiennes de $\mathbb{Q}$ telles que $K_1 \cap K_2 = K$. Soit $L = K_1K_2$. Pour que*

$$j_{K_1}^L\left(Fact\left(K_1\right)\right).j_{K_2}^L\left(Fact\left(K_2\right)\right) = Fact\left(L\right),$$

il faut et il suffit que pour tout idéal maximal $\mathfrak{p}$ de K,

$$e_{L/K}(\mathfrak{p}) = \mathrm{ppcm}(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})).$$

Cette égalité est en particulier vérifiée lorsque $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$.

Preuve. Fixons un idéal premier $\mathfrak{p}$ de K. Supposons que $N(\mathfrak{p}) = p^\alpha$ et simplifions les notations. On note $e_i = e_{K_i/K}(\mathfrak{p})$, $\epsilon_i = e_{L/K_i}(\mathfrak{p})$ $f_i = f_{K_i/K}(\mathfrak{p})$ et $\varphi_i = f_{L/K_i}(\mathfrak{p})$ pour $i \in 1, 2$. Posons $e = e_{L/K}(\mathfrak{p})$. L'extension L/K étant galoisienne, $f_{L/K}(\mathfrak{p}) = f_1\varphi_1 = f_2\varphi_2$ et $e = e_1\epsilon_1 = e_2\epsilon_2$.

On note également $\Pi_i = \Pi_{p^{\alpha f_i}}\left(K_i\right)$ et $\Pi = \Pi_{p^{\alpha f_i\varphi_i}}\left(L\right)$. Il vient

$$\Pi_{p^\alpha}(K)\mathcal{O}_{K_i} = \Pi_i^{e_i}, \Pi_{p^\alpha}(K)\mathcal{O}_L = \Pi^e, \Pi_i\mathcal{O}_L = \Pi^{\epsilon_i}\ (i = 1, 2)\,.$$

On obtient

$$\langle \Pi_1\mathcal{O}_L, \Pi_2\mathcal{O}_L\rangle = \langle \Pi^{\epsilon_1}, \Pi^{\epsilon_2}\rangle = \left\langle \Pi^{(\epsilon_1,\epsilon_2)}\right\rangle.$$

De $e = e_1\epsilon_1 = e_2\epsilon_2$, on déduit

$$(\epsilon_1, \epsilon_2) = \frac{e}{\mathrm{ppcm}(e_1, e_2)}.$$

D'où $\langle \Pi_1\mathcal{O}_L, \Pi_2\mathcal{O}_L\rangle = \langle \Pi\rangle$ si et seulement si $e = \mathrm{ppcm}(e_1, e_2)$. □

Remarque 2.22. La preuve précédente montre que, avec les mêmes notations, si pour un idéal $\mathfrak{p}$ de K on a $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$, l'idéal Π de $\mathcal{O}_L$ correspondant est principal si et seulement si les idéaux étendus $\Pi_i\mathcal{O}_L$ sont également principaux.

Clairement :

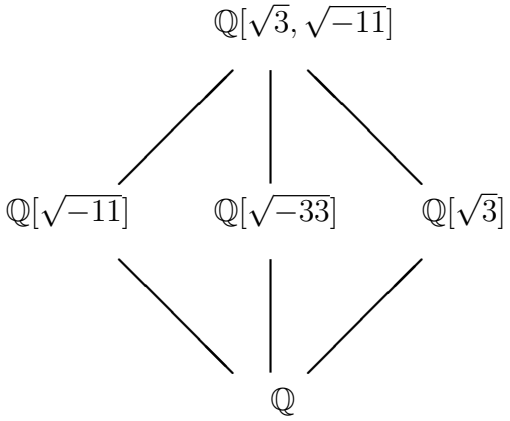
Corollaire 2.23. *Soient K, K_1 et K_2 des extensions galoisiennes de $\mathbb{Q}$ telles que $K_1 \cap K_2 = K$ et soit $L = K_1K_2$. Si, pour tout idéal premier $\mathfrak{p}$ de K, on a l'égalité $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$, alors :*

1. $$\epsilon_{K_1}^L\left(Po\left(K_1\right)\right).\epsilon_{K_2}^L\left(Po\left(K_2\right)\right) = Po\left(L\right)$$
2. *Par suite, L est un corps de Pólya si et seulement si L/K_1 et L/K_2 sont des extensions de Pólya.*

3. *En particulier, si K_1 et K_2 sont des corps de Pólya, L est aussi un corps de Pólya.*

Rappelons que cette dernière assertion est obtenue par Zantema [42, Thm 3.4] sous l'hypothèse plus forte que les degrés des extensions $K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$ sont premiers entre eux.

Application. Cette proposition permet de montrer que certains types de corps sont de Pólya. En particulier certains corps biquadratiques. En effet, posons $K_1 = \mathbb{Q}[\sqrt{3}]$ et $K_2 = \mathbb{Q}[\sqrt{-11}]$. Considérons le corps $L = K_1K_2 = \mathbb{Q}[\sqrt{3}, \sqrt{-11}]$ ($h_L = 2$). Nous sommes dans la situation suivante :



Les extensions $K_1/\mathbb{Q}$ et $K_2/\mathbb{Q}$ sont galoisiennes. On vérifie que les premiers ramifiés dans $K_1/\mathbb{Q}$ ne sont pas les mêmes qui sont ramifiés dans $K_2/\mathbb{Q}$ donc $(e_p(K_1/\mathbb{Q}), e_p(K_2/\mathbb{Q})) = 1$ pour tout $p \in \mathbb{P}$. On en conclut que $L = \mathbb{Q}[\sqrt{3}, \sqrt{-11}]$ est un corps de Pólya. On utilisera ultérieurement cette propriété à plusieurs reprises afin de construire des corps de Pólya particuliers.

Il est intéressant d'étudier l'intersection $j_{K_1}^L(Fact(K_1)) \cap j_{K_2}^L(Fact(K_2))$.

Proposition 2.24. *Soient K, K_1 et K_2 des extensions galoisiennes de $\mathbb{Q}$ telles que $K_1 \cap K_2 = K$. Soit $L = K_1K_2$. Si, pour tout idéal premier $\mathfrak{p}$ de K, on a $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$ alors*

$$j_{K_1}^L(Fact(K_1)) \cap j_{K_2}^L(Fact(K_2)) = j_K^L(Fact(K)).$$

Preuve. Reprenons les notations de la preuve de la proposition 2.21. Soit $I \in j_{K_1}^L(Fact(K_1)) \cap j_{K_2}^L(Fact(K_2))$. Sans perte de généralité, on se restreint

au cas où I est de la forme $\Pi_{p^{\alpha f_i}}(K_i)^{k_i}\mathcal{O}_L \in j_{K_i}^L(Fact(K_i))$, c'est-à-dire $I = \Pi_i^{k_i}\mathcal{O}_L$, $k_i \in \mathbb{Z}$ pour $i \in \{1,2\}$, $p \in \mathbb{P}$. Il vient

$$I = \Pi_1^{k_1}\mathcal{O}_L = \Pi_2^{k_2}\mathcal{O}_L$$

c'est-à-dire

$$\Pi^{k_1 e_2} = \Pi^{k_2 e_1}$$

d'où

$$k_1 e_2 = k_2 e_1.$$

On remarque alors que

$$I \in \left\langle \Pi^{ppcm(e_1,e_2)} \right\rangle.$$

Dans le cas où $(e_1, e_2) = 1$,

$$I \in \left\langle \Pi^{ppcm(e_1,e_2)} \right\rangle = \langle \Pi^{e_1 e_2} \rangle = \langle \Pi_{p^\alpha}(K)\mathcal{O}_L \rangle.$$

□

On sait que, pour $i \in 1,2$ les morphismes $\nu_L^{K_i}$ et $\epsilon_{K_i}^L$ envoient respectivement $Po(L)$ sur $Po(K_i)$ et $Po(K_i)$ sur $Po(L)$. On ignore si, sous les hypothèses précédentes, $\nu_{K_i}^L$ est surjectif ou si $\epsilon_{K_i}^L$ est injectif. Cependant, il est possible d'obtenir ces propriétés sous des hypothèses plus faibles que dans [11], à savoir $([K_1 : \mathbb{Q}], [K_2 : \mathbb{Q}]) = 1$, mais plus fortes que les précédentes, c'est-à-dire $(e_p(K_1/\mathbb{Q}), e_p(K_2/\mathbb{Q})) = 1$ pour tout $p \in \mathbb{P}$.

Proposition 2.25. *Soient K, K_1 et K_2 des extensions galoisiennes de $\mathbb{Q}$ telles que $K_1 \cap K_2 = K$. Soit $L = K_1K_2$. Supposons que pour tout $p \in \mathbb{P}$, $(e_p(K_1/\mathbb{Q}), [K_2 : K]) = 1$, alors*

$$\nu_L^{K_1}(Po(L)) = Po(K_1).$$

Preuve. On pose ici $e_1 = (e_p(K_1/\mathbb{Q}))$ et $n_2 = [K_2 : K]$. Soient u et v deux entiers tels que $ue_1 + vn_2 = 1$. Il vient $N_L^{K_1}(\Pi)^{ve_2} = N_L^{K_1}(\Pi^{e_2})^v = N_L^{K_1}(\Pi_1\mathcal{O}_L)^v = (\Pi_1^{n_2})^v = \Pi_1^{1-e_1u} = \Pi_1 \times (\Pi_1^{e_1})^{-u} = \Pi_1 \times (p\mathcal{O}_{K_1})^{-u}$. En quotientant par le groupe des idéaux principaux de K_1, on obtient bien l'égalité voulue. □

Remarquons que la preuve utilise $e_p(K_1/\mathbb{Q})$ et non pas $e_p(K_1/K)$

Proposition 2.26. *Soient K, K_1 et K_2 des extensions galoisiennes de $\mathbb{Q}$ telles que $K_1 \cap K_2 = K$. Soit $L = K_1K_2$. Si les indices de ramification dans l'extension $K_1/\mathbb{Q}$ sont premiers avec $[K_2 : K]$, alors le morphisme $\epsilon_{K_1}^L : Po(K_1) \to Po(L)$ est injectif, autrement dit $Po(K_1) \simeq Po(K_1, L)$.*

Preuve. Nous savons que $|Po(K_1)|$ divise $\prod_p e_p(K_1/\mathbb{Q})$. Comme pour tout premier p, $(e_p(K_1/\mathbb{Q}), [K_2 : K]) = 1$, on a :

$$(|Po(K_1)|, [K_2 : K]) = 1.$$

L'ordre d'un élément $\overline{\mathcal{I}}$ de $Po(K_1)$ divisant $|Po(K_1)|$, celui-ci est premier avec $[K_2 : K]$. Par conséquent, le morphisme

$$\nu_L^{K_1} \circ \epsilon_{K_1}^L : \overline{\mathcal{I}} \in Po(K_1) \mapsto \overline{\mathcal{I}}^{[K_2:K]} \in Po(K_1)$$

est injectif et de ce fait $\epsilon_{K_1}^L$ l'est également. □

Proposition 2.27. *Soient K_1 et K_2 deux extensions galoisiennes de $\mathbb{Q}$ telles que $K_1 \cap K_2 = \mathbb{Q}$ et soit $L = K_1K_2$. Si les indices de ramification dans $K_1/\mathbb{Q}$ sont premiers avec $[K_2 : \mathbb{Q}]$ et symétriquement alors :*

1. *Les morphismes $\epsilon_{K_1}^L$ et $\epsilon_{K_2}^L$ sont injectifs.*
2. *Le groupe $Po(L)$ est produit direct de ses sous-groupes $\epsilon_{K_i}^L(Po(K_i))$.*
3. *On a l'isomorphisme $Po(L) \simeq Po(K_1) \times Po(K_2)$.*

Preuve. 1. On renvoie à la proposition précédente en remplaçant K par $\mathbb{Q}$. 2. Il est possible d'appliquer le corollaire 2.23. En effet, pour tout $p \in \mathbb{P}$, $(e_p(K_1/\mathbb{Q}), [K_2 : \mathbb{Q}]) = 1$ et $(e_p(K_2/\mathbb{Q}))$ divise n_2. On en déduit que $(e_p(K_1/\mathbb{Q}), e_p(K_2/\mathbb{Q})) = 1$. Cela nous donne :

$$\epsilon_{K_1}^L Po(K_1) \cdot \epsilon_{K_2}^L Po(K_2) = Po(L).$$

De plus, considérons un élément $\overline{\mathcal{I}} \in \epsilon_{K_1}^L Po(K_1) \cap \epsilon_{K_2}^L Po(K_2)$. D'après le corollaire 2.5, son ordre l divise n_2 mais comme l divise également $\prod_p e_p(K_1/\mathbb{Q})$ et que $(e_p(K_1/\mathbb{Q}), n_2) = 1$ pour tout p premier, l est premier avec n_2 : la seule possibilité est $l = 1$. Ainsi, $\epsilon_{K_1}^L Po(K_1) \cap \epsilon_{K_2}^L Po(K_2) = 1$.

3. Les assertions 1 et 2 nous donnent facilement 3.

□

Soit $K/\mathbb{Q}$ une extension abélienne de degré n. Pour tout p divisant n, notons K_p l'unique sous-extension de K telle que $[K_p : \mathbb{Q}]$ est la plus grande puissance de p qui divise n, soit $p^{v_p(n)}$. Rappelons que K_p est le sous-corps de K laissé fixe par le sous-groupe de $Gal(K/\mathbb{Q})$ formé des éléments dont l'ordre est premier à p. La proposition précédente nous donne :

Corollaire 2.28. [42] *Supposons que l'extension $K/\mathbb{Q}$ soit abélienne de degré n. Alors*

$$Po(K) \simeq \prod_{p|n} Po(K_p, K).$$

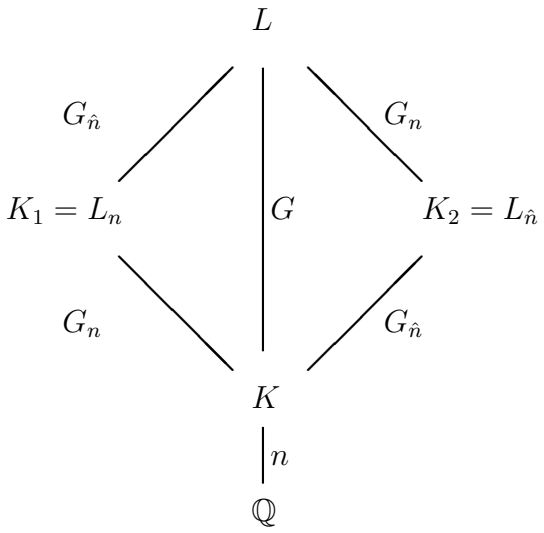
Corollaire 2.29. *Avec les hypothèses et notations du corollaire précédent, K est un corps de Pólya si et seulement si pour tout p premier divisant n, K/K_p est une extension de Pólya.*

Application.

Proposition 2.30. *Soient $K \subset L$ deux extensions galoisiennes de $\mathbb{Q}$ telles que l'extension L/K soit abélienne. Soit $n = [K : \mathbb{Q}]$. Notons $G = Gal(L/K)$, G étant un groupe abélien fini :*

$$G \simeq G_n \times G_{\hat{n}}$$

où G_n (resp. $G_{\hat{n}}$) est le sous-groupe de G formé des éléments dont l'ordre divise une puissance de n (resp. dont l'ordre est premier avec n). On note $L_n = L^{G_{\hat{n}}}$ (resp. $L_{\hat{n}} = L^{G_n}$) le sous-corps de L laissé fixe par G_n (resp. $G_{\hat{n}}$). Si les corps L_n et $L_{\hat{n}}$ sont des extensions galoisiennes de $\mathbb{Q}$, alors $Po(L_n)$ s'injecte dans $Po(L)$.



Preuve. Appliquons la proposition 2.26 avec $K_1 = L_n$, $K_2 = L_{\hat{n}}$ et $K_1 \cap K_2 = K$. Ces deux extensions sont bien linéairement disjointes sur K. Par ailleurs, les indices de ramification dans l'extension $K_1/\mathbb{Q}$ sont premiers avec $[K_2 : K]$. En effet, les indices de ramification dans l'extension galoisienne $K_1/\mathbb{Q}$ divisent $[K_1 : \mathbb{Q}] = [K_1 : K][K : \mathbb{Q}] = n \times |G_n|$ qui est un diviseur d'une puissance de n, alors que $[K_2 : K]$ est premier avec n. D'après la proposition 2.26, le morphisme $\epsilon_{K_1}^{K_1K_2}$, autrement dit $\epsilon_{L_n}^{L}$, est injectif.

□

2.3 Une approche du cas non-galoisien

Lorsque les extensions $K/\mathbb{Q}$ et $L/\mathbb{Q}$ ne sont pas galoisiennes, on ne dispose pas toujours des inclusions relatives aux groupes $Fact(K)$ et $Po(K)$.

Proposition 2.31. *Soit L une extension finie de K. Les inclusions*

$$j_K^L\left(Fact\left(K\right)\right) \subseteq Fact\left(L\right) \text{ et}$$

$$\epsilon_K^L\left(Po\left(K\right)\right) \subseteq Po\left(L\right)$$

sont fausses en général lorsque :

1. *$L/\mathbb{Q}$ est non galoisienne même si $K/\mathbb{Q}$ est galoisienne.*
2. *$K/\mathbb{Q}$ est non galoisienne même si $L/\mathbb{Q}$ est galoisienne.*

Preuve. La première assertion résulte du contre-exemple 2.33 ci-dessous et la deuxième du contre-exemple 2.34 ci-après. □

Ces contre-exemples utilisent des extensions cubiques pures $K = \mathbb{Q}\left[\sqrt[3]{m}\right]$ où m est un entier ≥ 2. Rappelons la décomposition d'un nombre premier dans un tel corps. D'après [12, Cor 6.4.15, Cor 6.4.16], on a :

Proposition 2.32. *Soit $K = \mathbb{Q}[\sqrt[3]{m}]$ où m est un entier ≥ 2 sans facteurs cubiques. Posons $m = ab^2$ où a et b sont premiers entre eux. Soit p un nombre premier. La décomposition de $p\mathcal{O}_K$ en idéaux premiers est la suivante :*

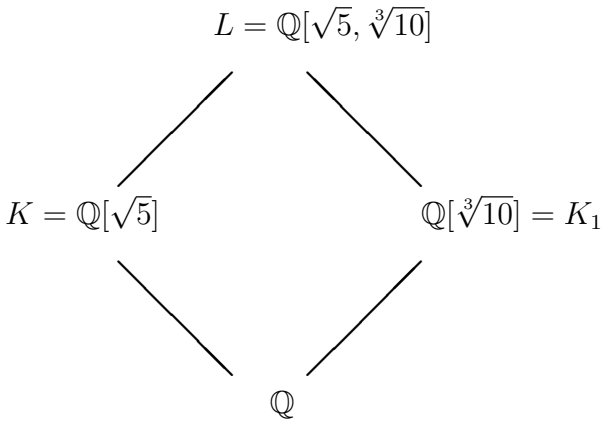
1. *Supposons que $p = 3$. Si $a^2 \equiv b^2 \pmod 9$ alors 3 est partiellement ramifié, c'est-à-dire $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2$. Sinon $3\mathcal{O}_K = \mathfrak{p}^3$.*

On suppose désormais $p \neq 3$.

2. *Si $p|ab$ alors $p\mathcal{O}_K = \mathfrak{p}^3$*
3. *Si $p \nmid ab$ et $p \equiv 2 \pmod 3$ alors $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ où $\mathfrak{p}_1$ possède un degré d'inertie égal à 1 alors que celui de $\mathfrak{p}_2$ est égal à 2.*
4. *Si $p \nmid ab$, $p \equiv 1 \pmod 3$ et $m^{\frac{p-1}{3}} \equiv 1 \pmod p$ alors $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.*
5. *Si $p \nmid ab$, $p \equiv 1 \pmod 3$ et $m^{\frac{p-1}{3}} \not\equiv 1 \pmod p$ alors $p\mathcal{O}_K$ est inerte.*

Exemple 2.33. Etudions le comportement du groupe des idéaux factoriels de $\mathbb{Q}[\sqrt{5}]$ dans l'extension $\mathbb{Q}[\sqrt{5}, \sqrt[3]{10}]/\mathbb{Q}[\sqrt{5}]$

Posons $K_1 = \mathbb{Q}[\sqrt[3]{10}]$. Dans ce cas, on a $a = 10$ et $b = 1$ et ainsi $a^2 \equiv b^2 \pmod 9$. Le nombre 3 est donc partiellement ramifié. Considérons ensuite le corps quadratique $K = \mathbb{Q}[\sqrt{5}]$ dans lequel 3 est inerte (5 n'est pas un carré dans $\mathbb{F}_3$). Puis, posons $L = K_1K$. Nous sommes dans la situation suivante :



Comme nous l'avons évoqué plus haut,

$$3\mathcal{O}_K = \mathfrak{m} \text{ où } N(\mathfrak{m}) = 3^2.$$

Ensuite

$$3\mathcal{O}_{K_1} = \mathfrak{m}_1\mathfrak{m}_2^2 \text{ où } N(\mathfrak{m}_i) = 3.$$

La multiplicativité des indices de ramification et des degrés résiduels indique que $3\mathcal{O}_L$ se décompose en un produit d'au moins deux idéaux maximaux dont le degré résiduel est au moins égal à 2. De plus l'un de ces deux idéaux possède un indice de ramification égal à deux. On en déduit alors l'unique décomposition possible dans $L = K_1K$.

$$3\mathcal{O}_L = \mathfrak{n}_1\mathfrak{n}_2^2 \text{ où } N(\mathfrak{n}_i) = 3^2.$$

On obtient

$$\Pi_9(L) = \mathfrak{n}_1\mathfrak{n}_2.$$

Considérons $\Pi_9(K)\mathcal{O}_L$.
D'après les égalités ci-dessus,

$$\Pi_9(K)\mathcal{O}_L = \mathfrak{m}\mathcal{O}_L = 3\mathcal{O}_L = \mathfrak{n}_1\mathfrak{n}_2^2.$$

Si nous avions l'inclusion $j_K^L\left(Fact\left(K\right)\right) \subseteq Fact\left(L\right)$, on aurait $\mathfrak{n}_2 \in Fact\left(L\right)$. Comme $N(\mathfrak{n}_2) = 3^2$, $\mathfrak{n}_2$, de norme 9, serait une puissance de $\Pi_9(L)$ ($N(\Pi_9(L)) = 81$). Ceci est impossible.
De la même manière si nous avions l'inclusion $\epsilon_K^L\left(Po\left(K\right)\right) \subseteq Po\left(L\right)$, la classe $\bar{\mathfrak{n}_2}$ de $\mathfrak{n}_2$ dans $Cl(L)$ vérifierait $\bar{\mathfrak{n}_2} \in Po(L)$. Toutefois, on rappelle que $Po\left(L\right) = Fact\left(L\right)/P(L) \cap Fact\left(L\right)$, donc $\mathfrak{n}_2$ serait encore une fois une puissance de $\Pi_9(L)$.

Exemple 2.34. Posons $K = \mathbb{Q}[\sqrt[3]{m}]$, où $m \in \mathbb{Z}$ et $L = \mathbb{Q}[j, \sqrt[3]{m}]$ et $K_1 = \mathbb{Q}[j]$. Soit $p \in \mathbb{P}$ tel que $p\mathcal{O}_K = \mathfrak{m}_1\mathfrak{m}_2$ où $N(\mathfrak{m}_1) = p$ et $N(\mathfrak{m}_2) = p^2$ (ce cas se présente lorsque $m = 5$ et $p = 2$ par exemple). Le nombre p n'étant pas ramifié dans $K/\mathbb{Q}$, $p \neq 3$. Il n'est donc pas ramifié dans $K_1/\mathbb{Q}$.
L'extension $L/\mathbb{Q}$ étant galoisienne, $2 \mid f_p(L/\mathbb{Q})$ donc, $2 \geq f_p(L/\mathbb{Q})$. De plus, $g_p(L/\mathbb{Q}) \geq 2$. Sachant que $e_p(L/\mathbb{Q})f_p(L/\mathbb{Q})g_p(L/\mathbb{Q}) = 6$, $f_p(L/\mathbb{Q}) = 2$ et $g_p(L/\mathbb{Q}) = 3$. Ainsi,

$$p\mathcal{O}_L = \mathfrak{n}_1\mathfrak{n}_2\mathfrak{n}_3, \text{ où } N(\mathfrak{n}_i) = p^2, \ i = 1, 2, 3.$$

Avec les notations habituelles,

$$p\mathcal{O}_K = \Pi_p(K)\Pi_{p^2}(K),$$

$$\Pi_p(K)\mathcal{O}_L = \mathfrak{n}_1, \ \Pi_{p^2}(K)\mathcal{O}_L = \mathfrak{n}_1\mathfrak{n}_2.$$

Cependant, ni $\Pi_p(K)\mathcal{O}_L \notin Fact(L)$, ni $\Pi_{p^2}(K)\mathcal{O}_L \notin Fact(L)$.

Si nous avions l'inclusion $\epsilon_K^L(Po(K)) \subseteq Po(L)$, la classe $\bar{\mathfrak{n}_1}$ de $\mathfrak{n}_1$ dans $Cl(L)$ vérifierait $\bar{\mathfrak{n}_1} \in Po(L)$, et, comme dans le contre-exemple précédent, $\mathfrak{n}_1$ ($N(\mathfrak{n}_1) = p^2$) serait une puissance de $\Pi_{p^2}(L)$ ($N(\Pi_{p^2}(L)) = p^4$).

Dans le contre-exemple 2.33, $L/\mathbb{Q}$ n'est pas galoisienne, mais L/K non plus. Aussi, pourrait-on se demander s'il ne suffirait pas que $K/\mathbb{Q}$ et L/K soient galoisiennes. Il n'en n'est rien :

Exemple 2.35. Considérons un corps biquadratique $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ où $(m, n) = 1$. Posons $K_1 = \mathbb{Q}[\sqrt{m}]$ et $K_2 = \mathbb{Q}[\sqrt{n}]$. Supposons qu'il existe un nombre premier p tel que $p\mathcal{O}_{K_1} = \mathfrak{p}^2$ et $p\mathcal{O}_{K_2} = \mathfrak{q}_1\mathfrak{q}_2$. Dans ce cas,

$$\Pi_p(K_1) = \mathfrak{p} \text{ et } \Pi_p(K_2) = \mathfrak{q}_1\mathfrak{q}_2.$$

Comme $p\mathcal{O}_K = \mathfrak{P}^2\mathfrak{Q}^2$, $\Pi_p(K) = \mathfrak{P}\mathfrak{Q}$. Soit L une extension quadratique de K telle que

$$\mathfrak{P}\mathcal{O}_K = \mathfrak{M}^2, \ \mathfrak{M} \text{ non principal et,}$$
$$\mathfrak{Q}\mathcal{O}_K = \mathfrak{N}_1\mathfrak{N}_2.$$

Nous avons $\Pi_p(L) = \mathfrak{M}\mathfrak{N}_1\mathfrak{N}_2$, $p\mathcal{O}_L = \mathfrak{M}^4\mathfrak{N}_1^2\mathfrak{N}_2^2$, d'où

$$\Pi_p(K)\mathcal{O}_L = \mathfrak{M}^2\mathfrak{N}_1\mathfrak{N}_2.$$

Si l'inclusion $\epsilon_K^L(Po(K)) \subseteq Po(L)$ était vérifiée, l'idéal $\mathfrak{M}$ serait principal. A l'aide du logiciel Kash, on vérifie que cette situation est celle de l'extension L/K et du nombre premier 2 lorsque $K = \mathbb{Q}[\sqrt{-2}, \sqrt{-15}]$ et $L = \mathbb{Q}[\sqrt{-2}, \sqrt[4]{-15}]$.

Malgré tout cela, il existe une condition nécessaire et suffisante pour laquelle nous avons toujours l'inclusion relative à $Fact(K)$, que l'extension L/K soit galoisienne ou non.

Proposition 2.36. *Soit $K/\mathbb{Q}$ une extension galoisienne et soit L une extension de K. Pour que*

$$j_K^L\left(Fact\left(K\right)\right) \subseteq Fact\left(L\right)$$

il faut et il suffit que pour tous $\mathfrak{p}_1, \mathfrak{p}_2$ idéaux premiers de $\mathcal{O}_L$ au dessus d'un même nombre premier,

$$f_{\mathfrak{p}_1}\left(L/K\right) = f_{\mathfrak{p}_2}\left(L/K\right) \Rightarrow e_{\mathfrak{p}_1}\left(L/K\right) = e_{\mathfrak{p}_2}\left(L/K\right)$$

Preuve. Soit p un nombre premier. Notons $e = e_p(K/\mathbb{Q})$ et $f = f_p(K/\mathbb{Q})$. On a

$$p\mathcal{O}_K = \Pi_{p^f}\left(K\right)^e.$$

Supposons que pour tous $\mathfrak{p}_1, \mathfrak{p}_2$ idéaux premiers de $\mathcal{O}_L$ au dessus de p, $f_{\mathfrak{p}_1}\left(L/K\right) = f_{\mathfrak{p}_2}\left(L/K\right) \Rightarrow e_{\mathfrak{p}_1}\left(L/K\right) = e_{\mathfrak{p}_2}\left(L/K\right)$. Notons $f_1, \ldots, f_r$ les différents degrés résiduels des idéaux premiers de $\mathcal{O}_L$ dans l'extension L/K et $e_1, \ldots, e_r$ les indices de ramification correspondants. D'après les hypothèses,

$$\Pi_{p^f}\left(K\right)\mathcal{O}_L = \left(\Pi_{p^{ff_1}}\left(L\right)\right)^{e_1} \ldots \left(\Pi_{p^{ff_r}}\left(L\right)\right)^{e_r}.$$

Ainsi, $\Pi_{p^f}\left(K\right)\mathcal{O}_L \in Fact\left(L\right)$. On en déduit que $j_K^L\left(Fact\left(K\right)\right) \subseteq Fact\left(L\right)$.

Réciproquement, on suppose que $j_K^L\left(Fact\left(K\right)\right) \subseteq Fact\left(L\right)$. Considérons $\Pi_{p^f}\left(K\right) \in Fact\left(K\right)$, il existe $\alpha_1, \ldots, \alpha_s \in \mathbb{Z}$ et $f_1, \ldots, f_s \in \mathbb{N}$ tels que

$$\Pi_{p^f}\left(K\right)\mathcal{O}_L = \left(\Pi_{p^{ff_1}}\left(L\right)\right)^{\alpha_1} \ldots \left(\Pi_{p^{ff_s}}\left(L\right)\right)^{\alpha_s}.$$

Clairement, cette décomposition est celle de $\Pi_{p^f}\left(K\right)\mathcal{O}_L$ en produit d'idéaux maximaux. Les idéaux de L au dessus de p sont tous présents dans cette décomposition. On en déduit que pour tous $\mathfrak{p}_1, \mathfrak{p}_2$ idéaux premiers de $\mathcal{O}_L$ au dessus de p, $f_{\mathfrak{p}_1}\left(L/K\right) = f_{\mathfrak{p}_2}\left(L/K\right) \Rightarrow e_{\mathfrak{p}_1}\left(L/K\right) = e_{\mathfrak{p}_2}\left(L/K\right)$. □

Corollaire 2.37. *Supposons que $m = ab^2$ où a et b sont premiers entre eux et sans facteurs carrés. Soit $K_1 = \mathbb{Q}[\sqrt[3]{m}]$ un corps cubique pur tel que $a^2 \not\equiv b^2 \pmod 9$. Pour toute extension galoisienne $K/\mathbb{Q}$ on a :*

$$j_K^{KK_1}\left(Fact\left(K\right)\right) \subseteq Fact\left(KK_1\right).$$

Preuve. En se référant à la décomposition donnée par la proposition 2.32 d'un nombre premier dans un corps cubique pur, aucun nombre premier p n'est partiellement ramifié. Par suite, tous les $\mathfrak{p}_1, \mathfrak{p}_2$ idéaux premiers de $\mathcal{O}_{KK_1}$ au dessus d'un même nombre premier p vérifient la condition de la proposition précédente. □

2.4 Majoration du nombre de premiers ramifiés dans un corps de Pólya

Le corollaire 2.23 permet de construire des corps de Pólya possédant un nombre de premiers ramifiés aussi grand qu'on le souhaite. En effet, un corps $\mathbb{Q}[\sqrt{p_1},\ldots,\sqrt{p_r}]$, où $r \in \mathbb{N}^*$ et p_i est un nombre premier tel que $p_i \equiv 1 \pmod 4$ est le compositum de r corps quadratiques $K_1 = \mathbb{Q}[\sqrt{p_1}],\ldots,$ $K_r = \mathbb{Q}[\sqrt{p_r}]$ de Pólya d'après le corollaire 1.38. Par ailleurs, les indices de ramifications dans les extensions $K_i/\mathbb{Q}$ des nombres premiers p_i sont premiers entre eux deux à deux puisque ce ne sont pas les mêmes premiers qui sont ramifiés dans chacune des extensions quadratiques. Il est alors possible d'appliquer la proposition 2.23 pour prouver que $L := \prod_{i=1}^{r} K_i = \mathbb{Q}[\sqrt{p_1},\ldots,\sqrt{p_r}]$ est un corps de Pólya et possède r premiers ramifiés. Avec cette construction, pour obtenir r premiers ramifiés, il faut ici considérer une extension de degré au moins égal à 2^r.

Dans cette section, nous nous appuyons sur des résultats généraux rappelés dans [11]. Soit K une extension galoisienne de $\mathbb{Q}$ et soit G son groupe de Galois. Le groupe G agit sur les groupes K, K^*, $\mathcal{O}_K$, $\mathcal{O}_K^\times$, $P(K)$, $I(K)$ (où $\mathcal{O}_K^\times$ est le groupe des unités de $\mathcal{O}_K$, $I(K)$ est l'ensemble des idéaux fractionnaires de $\mathcal{O}_K$ et $P(K)$ désigne l'ensemble des idéaux principaux de $\mathcal{O}_K$). D'après la proposition 1.27, $Fact(K)$ est le groupe des idéaux ambiges de K donc

$$Fact(K) = I(K)^G$$

où $I(K)^G$ désigne le sous-groupe $I(K)$ des idéaux de K invariants par G. On obtient que

$$Po(K) = I(K)^G / P(K)^G.$$

Par ailleurs la suite exacte courte

$$1 \to \mathcal{O}_K^\times \to K^* \to P(K) \to 1$$

permet d'établir, grâce au théorème 90 de Hilbert, que :

Lemme 2.38. [9, Lemme 2.1] *La suite de groupes abéliens suivante est exacte*

$$1 \to \mathbb{Q}^*/\{\pm 1\} \to P(K)^G \to H^1\left(G, \mathcal{O}_K^\times\right) \to 1.$$

Une conséquence de ce lemme est un résultat de Zantema [42] :

Proposition 2.39. [11] *Si $K/\mathbb{Q}$ est galoisienne de groupe de Galois G alors la suite de groupes abéliens suivante est exacte :*

$$1 \to H^1\left(G, \mathcal{O}_K^\times\right) \to \oplus_{p\in\mathbb{P}}\mathbb{Z}/e_p\mathbb{Z} \to Po(K) \to 1$$

En particulier,

$$|Po\,(K)| \times \left|H^1\left(G, \mathcal{O}_K^\times\right)\right| = \prod_{p\in\mathbb{P}} e_p.$$

De ce fait, si $K/\mathbb{Q}$ est une extension galoisienne, K est un corps de Pólya si et seulement si $\left|H^1\left(G, \mathcal{O}_K^\times\right)\right| = \prod_{p\in\mathbb{P}} e_p$.

Nous pouvons traiter le cas particulier des extensions cycliques :

Corollaire 2.40. [11] *Soit $K/\mathbb{Q}$ une extension cyclique de degré n.*

1. *Si K est réel et si $N(\mathcal{O}_K^\times) = \{1\}$, alors*

$$|Po(K)| = \frac{1}{2n}\prod_{p\in\mathbb{P}} e_p.$$

2. *Sinon,*

$$|Po(K)| = \frac{1}{n}\prod_{p\in\mathbb{P}} e_p.$$

Preuve. Supposons que G soit un groupe cyclique engendré par σ, d'après [31, IV.3.7] :

$$H^1\left(G, \mathcal{O}_K^\times\right) \simeq H^{-1}\left(G, \mathcal{O}_K^\times\right) = \frac{\left\{a \in \mathcal{O}_K^\times \mid N_{K/\mathbb{Q}}(a) = 1\right\}}{\left\{\sigma\,(a)\,/a \mid a \in \mathcal{O}_K^\times\right\}}.$$

Ce groupe est de cardinal $2[K : \mathbb{Q}]$ si K est réel et si $N(\mathcal{O}_K^\times) = \{1\}$. Il est de cardinal $[K : \mathbb{Q}]$ sinon.

□

Corollaire 2.41. *Soit $K/\mathbb{Q}$ une extension cyclique de degré premier q. Si $q \neq 2$, $|Po(K)| = q^{s-1}$ où s désigne le nombre de premiers ramifiés dans l'extension $K/\mathbb{Q}$.*

Preuve. Un nombre premier ramifié dans une extension cyclique de degré premier q y est totalement ramifié. Ainsi, le cardinal $|Po(K)|$ étant entier, lorsque $q \neq 2$, d'après le corollaire 2.40, $|Po(K)| = q^{s-1}$. □

Remarquons que si $q = 2$, la situation est différente et conforme au théorème 1.34.

Dans le cas d'une extension galoisienne $K/\mathbb{Q}$ non nécessairement cyclique, nous allons également pouvoir majorer le nombres de premiers ramifiés dans cette extension lorsque K est un corps de Pólya. Pour cela nous utilisons un résultat de Brumer et Rosen [9].

Proposition 2.42. [9] *Soit $K/\mathbb{Q}$ une extension galoisienne de groupe de Galois G d'ordre n. Soit $n = \prod_p p^{v_p(n)}$ la décomposition de n en facteurs premiers. Alors $\left|H^1\left(G, \mathcal{O}_K^\times\right)\right|$ divise $\prod_{p|n} p^{R_p(n)}$ où*

$$R_p(n) = n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{v_p(n)}}\right) + v_p(n).$$

Corollaire 2.43. *Il existe une fonction $g : \mathbb{N} \to \mathbb{N}$ telle que, pour tout corps de Pólya K extension galoisienne de $\mathbb{Q}$ de degré n sur $\mathbb{Q}$, le nombre s_K de premiers ramifiés dans l'extension $K/\mathbb{Q}$ soit majoré par $g(n)$. Plus précisément, le nombre de premiers ramifiés dans un corps de Pólya extension galoisienne de $\mathbb{Q}$ de degré n est majoré par $\sum_{p|n} R_p(n)$ où $R_p(n) = n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{v_p(n)}}\right) + v_p(n)$.*

Preuve. On suppose K de Pólya. D'après la proposition 2.39, $\left|H^1\left(G, \mathcal{O}_K^\times\right)\right| = \prod_{p\in\mathbb{P}} e_p$. Soit p un nombre premier ramifié dans l'extension $K/\mathbb{Q}$, son indice de ramification e_p dans $K/\mathbb{Q}$ est donc non trivial et d'après la proposition précédente on obtient $\prod_{p\in\mathbb{P}} e_p \mid \prod_{p|n} p^{R_p(n)}$. Le nombre de facteurs irréductibles de $\prod_{p\in\mathbb{P}} e_p$ étant minoré par s et celui de $\prod_{p|n} p^{R_p(n)}$ étant $\sum_{p|n} R_p(n)$, on a $s \leq \sum_{p|n} R_p(n)$. □

Exemple 2.44. Cas des corps cubiques et sextiques.
D'après le corollaire 2.41, un corps cubique cyclique K est de de Pólya si et seulement si un seul premier est ramifié dans l'extension $K/\mathbb{Q}$. Cependant les extensions de degré 3 sur $\mathbb{Q}$ ne sont pas toutes galoisiennes, leur clôture galoisienne L est alors de degré 6. Si L est un corps de Pólya, le nombre de ramifiés dans l'extension $L/\mathbb{Q}$ de degré 6 est majoré par $\sum_{p|n} R_p(n) = R_2(6) + R_2(3) = 4 + 3 = 7$.

Exemple 2.45. Cas des extensions de degré p^a, p premier, $a \in \mathbb{N}^*$.
Pour conclure, nous avons exhibé au début de ce paragraphe une famille de corps de Pólya dans laquelle il est possible de trouver un corps avec un nombre de premiers ramifiés aussi grand que l'on veut. Il s'agit de corps de degré 2^a sur $\mathbb{Q}$ où $a \in \mathbb{N}$. Déterminons dans un cadre plus général, le nombre de premier ramifiés dans le cas où K est un corps de Pólya extension galoisienne de $\mathbb{Q}$ de degré p^a avec $a \in \mathbb{N}$. Le corollaire 2.43 montre que ce nombre est majoré par $R_p(n) = \frac{p^a-1}{p-1} + a$. Par exemple, les corps quartiques de Pólya extensions galoisiennes de $\mathbb{Q}$, que nous étudions au chapitre suivant, possèdent au plus 5 premiers ramifiés. Soulignons que pour $p = 2$, le nombre de premiers ramifiés est majoré par $2^{a-1} + a$ alors que l'exemple construit au début de ce paragraphe n'a que a premiers ramifiés. On peut donc se poser la question de l'effectivité de la borne.

Chapitre 3

Applications aux corps de Pólya cubiques, quartiques et sextiques

De même que la proposition 1.38 caractérise les corps quadratiques de Pólya, nous allons tenter de caractériser dans ce chapitre les corps de nombres K de petit degré qui sont aussi des corps de Pólya. La proposition 2.3 montre qu'il est, à priori, plus aisé d'obtenir une telle caractérisation dans le cas où K est un corps de nombres galoisien. Là encore, la simplicité de la caractérisation est fonction des propriétés du groupe de Galois $G(K/\mathbb{Q})$ mais également de la ramification dans l'extension $K/\mathbb{Q}$.

La situation la plus simple est celle où $G(K/\mathbb{Q})$ est cyclique d'ordre un nombre premier p impair. En effet, le corollaire 2.41 permet alors d'affirmer qu'un corps K est de Pólya si et seulement si un seul premier est ramifié dans l'extension $K/\mathbb{Q}$. Nous expliciterons au §3.1 la forme de tous les corps cubiques cycliques qui sont de Pólya.

Vient ensuite le cas où $G(K/\mathbb{Q})$ est cyclique mais non d'ordre premier. La proposition 2.27 nous ramène aisément au cas d'un groupe de Galois cyclique d'ordre une puissance d'un nombre premier. Nous caractériserons au §3.3 les extensions quartiques cycliques.

On rencontre ensuite le cas où $G(K/\mathbb{Q})$ n'est pas cyclique mais est abélien. La proposition 2.27 nous ramène de nouveau au cas où l'ordre du groupe est une puissance d'un nombre premier. Nous étudierons au §3.4 les corps biquadratiques obtenus comme compositum de corps quadratiques de Pólya.

Enfin, nous nous intéresserons au cas où $G(K/\mathbb{Q})$ n'est pas abélien. Une telle situation n'apparaît pas avant le degré 6 pour un groupe de Galois isomorphe au groupe symétrique S_3. De telles extensions sextiques sont les clôtures galoisiennes de corps cubiques non cycliques. Nous caractérisons au §3.2 les extensions sextiques qui sont la clôture galoisienne d'un corps cubique pur, donc de la forme $\mathbb{Q}[j, \sqrt[3]{m}]$.

Quant au cas non galoisien, le plus délicat, il apparaît dès le degré 3 avec les corps cubiques non cycliques. Nous l'évoquerons très brièvement au début du §3.1.

3.1 Corps cubiques cycliques

Pour commencer, soit K un corps cubique quelconque. Ecrivons son discrimant sous la forme

$$D_K = df^2 \quad \text{où} \quad d \text{ est sans facteurs carrés.}$$

L'extension $K/\mathbb{Q}$ est galoisienne si et seulement si $d = 1$, c'est-à-dire, si et seulement si D_K est un carré parfait, et c'est alors une extension cyclique. Dans le cas général non galoisien, il est difficile d'obtenir des résultats simples. Toutefois, la seule considération des décompositions possibles des nombres premiers conduit à la proposition générale suivante :

Proposition 3.1. *Un corps cubique est de Pólya si et seulement si, pour tout nombre premier p non totalement décomposé, tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_K$ au dessus de p est principal.*

Preuve. Dans une extension de degré 3, un nombre premier p peut se décomposer suivant l'une des écritures suivantes. On exhibe également les idéaux $\Pi_q(K)$ correspondant :

- $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ où $N(\mathfrak{P}_i) = p$ pour $i = 1, 2, 3$; $\Pi_p(\mathcal{O}_K) = p\mathcal{O}_K$
- $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ où $N(\mathfrak{P}_1) = p$ et $N(\mathfrak{P}_1) = p^2$; $\Pi_p(\mathcal{O}_K) = \mathfrak{P}_1$ et $\Pi_{p^2}(\mathcal{O}_K) = \mathfrak{P}_2$
- $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2^2$ où $N(\mathfrak{P}_i) = p$ pour $i = 1, 2$; $\Pi_p(\mathcal{O}_K) = \mathfrak{P}_1\mathfrak{P}_2$
- $p\mathcal{O}_K = \mathfrak{P}^3$ où $N(\mathfrak{P}) = p$; $\Pi_p(\mathcal{O}_K) = \mathfrak{P}$
- $p\mathcal{O}_K = \mathfrak{P}$ où $N(\mathfrak{P}) = p^3$; $\Pi_{p^3}(\mathcal{O}_K) = \mathfrak{P} = p\mathcal{O}_K$

□

Parmi les corps cubiques non galoisiens (ceux pour lesquels $d \neq 1$), nous avons déjà considéré le cas particulier des corps purs $\mathbb{Q}[\sqrt[3]{m}]$ (ceux pour lesquels $d = -3$) avec la proposition 2.32 qui fournit, dans ce cas, la décomposition des nombres premiers. La juxtapposition avec la proposition précédente conduit à l'énoncé (peu utilisable) suivant :

Proposition 3.2. *Soit $K = \mathbb{Q}[\sqrt[3]{m}]$ un corps cubique pur où m est un entier ≥ 2 sans facteurs cubiques. Posons $m = ab^2$ où a et b sont premiers entre eux. Le corps K est de Pólya si et seulement si*

1. *pour tout p divisant m et pour $p = 3$ lorsque $a^2 \not\equiv b^2 \pmod 9$, il existe un entier de K de norme p,*
2. *pour tout $p \equiv 2 \pmod 3$ et ne divisant pas m et pour $p = 3$ lorsque $a^2 \equiv b^2 \pmod 9$, les idéaux premiers $\mathfrak{P}$ de $\mathcal{O}_K$ au-dessus de p sont principaux.*

Revenons au cas galoisien, donc cyclique, lorsque D_K est un carré parfait. Rappelons la description des corps cubiques cycliques donnée dans [12] :

Proposition 3.3. [12, Lem 6.4.5] *Pour tout corps cubique cyclique K, il existe une unique paire d'entiers (e, u) telle que e est un produit de premiers distincts tous congrus à $1 \pmod 3$, $u \equiv 2 \pmod 3$ et $K = \mathbb{Q}[\theta]$ où θ est une racine du polynôme $P(X) = X^3 - 3eX - eu$. De plus $e = \frac{u^2+3v^2}{4}$, $v \in \mathbb{N}^*$ et le discriminant de P est $81e^2v^2$. Réciproquement, un corps K de ce type est un corps cubique cyclique. En outre, si $3 \not| v$, $D_K = 81e^2v^2$ et si $3|v$, $D_K = e^2$.*

Proposition 3.4. *Un corps cubique cyclique K est de Pólya si et seulement si $K = \mathbb{Q}[\theta]$ où θ est racine d'un polynôme P à coefficients entiers de la forme*

$$X^3 - 3X + 1 \text{ ou bien}$$

$$X^3 - 3pX - pu$$

où p est un nombre premier tel que $p = \frac{u^2+27w^2}{4}$ avec $u \equiv 2 \pmod 3$ et $w > 0$.

Preuve. D'après le corollaire 2.41, K étant un corps cyclique de degré 3 sur $\mathbb{Q}$, $|Po(K)| = 3^{s_K - 1}$ où s_K désigne le nombre de premiers ramifiés dans l'extension $K/\mathbb{Q}$. En particulier, K est un corps de Pólya si et seulement si $s_K = 1$. En reprenant les notations de la proposition 3.3, si 3 est ramifié dans $K/\mathbb{Q}$, 3 est le seul diviseur premier éventuel de e. Or, $e \equiv 1 \pmod 3$, d'où $e = 1$, $u = \pm 1$, $v = 1$. Mais $u \equiv 2 \pmod 3$, donc $u = -1$ et $P(X) = X^3 - 3X + 1$. Si 3 n'est pas ramifié, $3|v$ et $D_K = e^2$. Ainsi $e = p$ où p est un nombre premier $\equiv 1 \pmod 3$. On en conclut que

$$P(X) = X^3 - 3pX - pu$$

où $p = \frac{u^2+27w^2}{4}$ avec $u \equiv 2 \pmod 3$ et $w > 0$.

□

Exemple 3.5. Avec $p = 13$, $u = 5$, $w = 1$. Le corps $K = \mathbb{Q}[\theta]$ où θ est racine de $X^3 - 39X - 65$ est un corps cubique cyclique de Pólya.

3.2 Corps sextiques galoisiens

Les différents types de corps sextiques sont trop nombreux pour être étudiés en détail. Nous nous limitons aux corps sextiques galoisiens. Il y a alors deux type de corps selon que le groupe de Galois est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ (et donc cyclique) ou à S_3 (donc non abélien). Le cas sextique cyclique se traite facilement :

Proposition 3.6. *Les corps de Pólya sextiques cycliques sont exactement les corps obtenus comme compositum d'un corps de Pólya quadratique et d'un corps de Pólya cubique cyclique.*

Preuve. Soit K un corps sextique cyclique. Il est clair que K contient exactement deux sous-corps non triviaux : un sous-corps quadratique K_1 et un sous-corps cubique K_2 et ce dernier est cyclique. La proposition 2.27 s'applique : le corps K est de Pólya si et seulement si K_1 et K_2 sont de Pólya. □

Reste le cas des corps K sextiques non abéliens. Le groupe S_3 contient un seul sous-groupe d'ordre 3 et 3 sous-groupes d'ordre 2, donc le corps K contient un seul sous-corps quadratique $K_1 = \mathbb{Q}[\sqrt{d}]$ et 3 sous-corps cubiques $K_{2,k}$ $(1 \leq k \leq 3)$ conjugués sur $\mathbb{Q}$. Le corps K est le compositum de K_1 et de n'importe lequel des $K_{2,k}$. Le corps sextique K est aussi la clôture galoisienne de chacun de ces corps cubiques non cycliques, et réciproquement, la clôture galoisienne de tout corps cubique non cyclique est un corps sextique de groupe de Galois isomorphe à S_3. Afin d'utiliser ce que nous avons vu précédemment, nous allons nous limiter à l'étude de ces corps sextiques K qui contiennent un corps cubique pur, ce qui se produit si et seulement si le sous-corps quadratique K_1 de K est le corps $\mathbb{Q}[j]$ des racines cubiques de l'unité. Autrement dit, nous allons essayer de caractériser les corps de Pólya de la forme $\mathbb{Q}[j, \sqrt[3]{m}]$.

Proposition 3.7. *Soit $m = ab^2$ où m est un entier ≥ 2, a et b sont sans facteurs carrés et premiers entre eux. Soit $L = \mathbb{Q}[j, \sqrt[3]{m}]$. Soit $K_1 = \mathbb{Q}[j]$ et $K = \mathbb{Q}[\sqrt[3]{m}]$. Le corps L est un corps de Pólya si et seulement si*

- *lorsque $a^2 \not\equiv b^2 \pmod 9$, pour tout premier $p \mid 3m$, il existe un élément $\alpha \in K$ tel que $N_{K/\mathbb{Q}}(\alpha) = \pm p$.*
- *lorsque $a^2 \equiv b^2 \pmod 9$, pour tout premier p diviseur de m, il existe un élément $\alpha \in K$ tel que $N_{K/\mathbb{Q}}(\alpha) = \pm p$.*

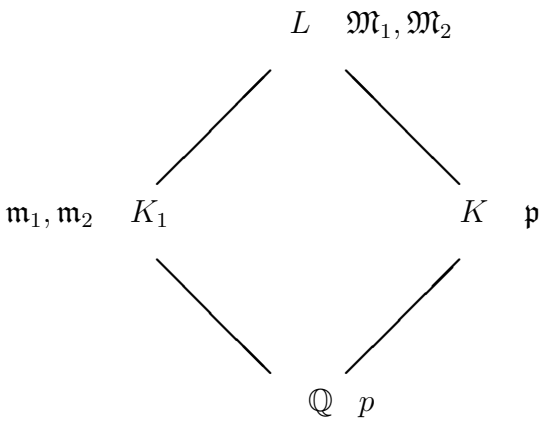
Montrons d'abord deux lemmes :

Lemme 3.8. *Soient m un entier ≥ 2 sans facteurs cubiques, $K = \mathbb{Q}[\sqrt[3]{m}]$ et $L = \mathbb{Q}[j, \sqrt[3]{m}]$. Pour tout p divisant m, $p \neq 3$, on a :*

1. $\Pi_p(K)\mathcal{O}_L = \Pi_p(L)$ *ou bien* $\Pi_{p^2}(L)$,
2. $\Pi_p(K)$ *est principal si et seulement si* $\Pi_p(L)$ *(resp.* $\Pi_{p^2}(L)$*) est principal.*

Preuve. D'après le théorème 1.41 de décomposition d'un premier dans un corps cyclotomique on obtient en posant $K_1 = \mathbb{Q}[j]$:
- Si $p \equiv 1 \pmod 3$, $p\mathcal{O}_{K_1} = \mathfrak{m}_1\mathfrak{m}_2$ et $N(\mathfrak{m}_i) = p$.
- Si $p \equiv 2 \pmod 3$, $p\mathcal{O}_{K_1} = \mathfrak{m}$ et $N(\mathfrak{m}) = p^2$.

Si $p \mid m$ et $p \neq 3$, alors p est totalement ramifié dans $K/\mathbb{Q}$, $p\mathcal{O}_K = \mathfrak{p}^3$ et $N(\mathfrak{p}) = p$ d'après la décomposition d'un nombre premier dans un corps cubique pur (proposition 2.32). Par exemple lorsque $p \equiv 1 \pmod 3$, $p \mid m$ et $p \neq 3$ la situation est la suivante :



Ainsi,
- Si $p \equiv 1 \pmod 3$, $p\mathcal{O}_L = \Pi_p(L)^3$.
- Si $p \equiv 2 \pmod 3$, $p\mathcal{O}_L = \Pi_{p^2}(L)^3$.

Dans le cas $p \mid m$, $p \neq 3$ et $p \equiv 1 \pmod 3$ (resp. $p \equiv 2 \pmod 3$), nous obtenons l'égalité $\Pi_p(K)\mathcal{O}_L = \Pi_p(L)$ (resp. $\Pi_p(K)\mathcal{O}_L = \Pi_{p^2}(L)$). Par conséquent, si les idéaux $\Pi_p(K)$ sont principaux, les idéaux $\Pi_p(L)$ (resp. $\Pi_{p^2}(L)$) le sont également. Réciproquement, si les idéaux $\Pi_p(L)$ (resp. $\Pi_{p^2}(L)$) sont principaux, en appliquant le morphisme norme N_L^K, on obtient, lorsque $p \equiv 1 \pmod 3$:

$$N_L^K(\Pi_p(L)) = \Pi_p(K)^2.$$

Ainsi, $\Pi_p(L) = \mathfrak{M}_1\mathfrak{M}_2$ et $N_L^K(\Pi_p(L)) = \mathfrak{p}^2$.

De même, si $p \equiv 2 \pmod 3$, $N_L^K(\Pi_{p^2}(L)) = \Pi_p(K)^2$. Ainsi, dans les deux cas, $\Pi_p(K)^2$ est principal. Ceci signifie que l'image de $\Pi_p(K)$ est dans le sous-

groupe $Cl(K)_{\hat{3}}$ de $Cl(K)$ formé des éléments d'ordre premier à 3. D'après la proposition 2.2, ceci implique que $\Pi_p(K)$ est principal. □

Lemme 3.9. *Soient $m = ab^2$ un entier ≥ 2 sans facteurs cubiques où a et b sont premiers entre eux, $K = \mathbb{Q}[\sqrt[3]{m}]$ et $L = \mathbb{Q}[j, \sqrt[3]{m}]$.*

1. *Lorsque $a^2 \equiv b^2 \pmod 9$, l'idéal $\Pi_3(L)$ est principal.*
2. *Sinon, $\Pi_3(K)$ est principal si et seulement si $\Pi_3(L)$ est principal.*

Preuve. On sait qu'il existe un unique idéal maximal $\mathfrak{m}$ de norme 3 tel que $3\mathcal{O}_{K_1} = \mathfrak{m}^2 = \Pi_3(K_1)^2$.
Dans un premier temps, supposons que $3\mathcal{O}_K = \mathfrak{m}_1\mathfrak{m}_2^2$ où $N(\mathfrak{m}_i) = 3$. Cela se produit lorsque $a^2 \equiv b^2 \pmod 9$. L'extension $L/\mathbb{Q}$ étant galoisienne de degré 6, l'unique décomposition possible en produit d'idéaux maximaux pour 3 est la suivante :

$$3\mathcal{O}_L = (\mathfrak{n}_1\mathfrak{n}_2\mathfrak{n}_3)^2 \text{ où } N(\mathfrak{n}_i) = 3.$$

L'extension L/K_1 étant galoisienne, nous avons

$$\mathfrak{m}\mathcal{O}_L = \Pi_3(K_1)\mathcal{O}_L = \Pi_3(L) = \mathfrak{n}_1\mathfrak{n}_2\mathfrak{n}_3.$$

Le corps K_1 étant un corps cyclotomique, il est de Pólya (cf. proposition 1.40), $\Pi_3(K_1)$ est donc principal, il en de même pour $\Pi_3(L)$.
Supposons maintenant que l'on ait $3\mathcal{O}_K = \mathfrak{p}^3 = \Pi_3(K)^3$. Cela se produit lorsque $a^2 \not\equiv b^2 \pmod 9$. Dans ce cas, $3\mathcal{O}_L = \mathfrak{n}^6$. Les extensions L/K et L/K_1 étant galoisiennes, on obtient :

$$\mathfrak{m}\mathcal{O}_L = \Pi_3(K_1)\mathcal{O}_L = \Pi_3(L)^3 = \mathfrak{n}^3,$$

$$\mathfrak{p}\mathcal{O}_L = \Pi_3(K)\mathcal{O}_L = \Pi_3(L)^2 = \mathfrak{n}^2.$$

Or, $\Pi_3(K_1)$ étant principal, $\Pi_3(L)^3$ l'est également. De ce fait, $\Pi_3(L)$ est principal si et seulement si $\Pi_3(L)^2$ l'est. Or, si $\Pi_3(K)$ est principal, comme $\Pi_3(K)\mathcal{O}_L = \Pi_3(L)^2$, l'idéal $\Pi_3(L)^2$ l'est également. Réciproquement, supposons $\Pi_3(L)^2$ principal, l'idéal $N_L^K(\Pi_3(L)^2) = N_L^K(\Pi_3(K)\mathcal{O}_L) = \Pi_3(K)^2$ est alors principal et la relation $3\mathcal{O}_K = \Pi_3(K)^3$ nous permet d'affirmer que $\Pi_3(K)$ est effectivement principal. Ainsi, $\Pi_3(L)^2$ est principal si et seulement si $\Pi_3(K)$ est principal. □

Preuve de la proposition 3.7. Le seul premier ramifié dans $K_1/\mathbb{Q}$ est 3, les ramifiés dans $K_2/\mathbb{Q}$ sont 3 et les diviseurs premiers de m. Leur cas est traité dans les deux lemmes précédents. Les premiers différents de 3 et des diviseurs de m ne sont donc ramifiés ni dans $K_1/\mathbb{Q}$, ni dans $K_2/\mathbb{Q}$, ni, a fortiori (lemme 2.19), dans $L = K_1K_2$. L'extension $L/\mathbb{Q}$ étant galoisienne, les idéaux $\Pi_q(L)$ au dessus de ces premiers sont principaux (cf. proposition 2.3). □

Corollaire 3.10. *Soit p un nombre premier, le corps $\mathbb{Q}[j, \sqrt[3]{p}]$ est un corps de Pólya si et seulement si*

- *ou bien $p^2 \equiv 1 \pmod 9$,*
- *ou bien il existe un élément entier de $\mathbb{Q}[\sqrt[3]{p}]$ de norme ± 3.*

Preuve. Le premier p est totalement ramifié dans $\mathbb{Q}[\sqrt[3]{p}]/\mathbb{Q}$ et :

- si $p \equiv 1 \pmod 3$, $p\mathcal{O}_L = \Pi_p(L)^3$, d'où $\Pi_p(L) = \sqrt[3]{p}\mathcal{O}_L$.
- si $p \equiv 2 \pmod 3$, $p\mathcal{O}_L = \Pi_{p^2}(L)^3$, d'où $\Pi_{p^2}(L) = \sqrt[3]{p}\mathcal{O}_L$.

Ainsi $\mathbb{Q}[j, \sqrt[3]{p}]$ est un corps de Pólya si et seulement si lorsque $p^2 \not\equiv 1 \pmod 9$, l'idéal $\Pi_3(K_2)$ est principal, ce qui est équivalent à l'existence d'un élément entier de $\mathbb{Q}[\sqrt[3]{p}]$ de norme ± 3.

□

On connait précisément une base de l'anneau des entiers d'un corps cubique :

Proposition 3.11. [12, Thm 6.4.13] *Soit $K = \mathbb{Q}[\sqrt[3]{m}]$ un corps cubique pur, où $m \geq 2$ est sans facteurs cubiques. Posons $m = ab^2$ où a et b sont sans facteurs carrés et premiers entre eux. Soit $\theta = \sqrt[3]{m}$.*

1. *Si $a^2 \not\equiv b^2 \pmod 9$, alors $\left(1, \theta, \frac{\theta^2}{b}\right)$ est une base de $\mathcal{O}_K$.*
2. *Si $a^2 \equiv b^2 \pmod 9$, alors $\left(1, \theta, \frac{\theta^2+m\theta+b^2}{3b}\right)$ est une base de $\mathcal{O}_K$*

Lorsque $m = p$, p premier, et $p^2 \not\equiv 1 \pmod 9$, une base de l'anneau des entiers de $\mathbb{Q}[\sqrt[3]{p}]$ est $\left(1, \sqrt[3]{p}, (\sqrt[3]{p})^2\right)$. Un entier $\alpha = a + b\sqrt[3]{p} + c(\sqrt[3]{p})^2$ a pour norme $N(\alpha) = a^3 + p(b^3 + pc^3 - 3abc)$. Ainsi, si $\mathcal{O}_K$ admet un élément de norme 3, alors 3 est un cube modulo p.

Exemple 3.12. Pour $p = 7$, on vérifie facilement que ± 3 n'est pas un cube modulo 7, $\Pi_3(K_2)$ n'est donc pas principal. De plus le nombre de classes de $K = \mathbb{Q}[\sqrt[3]{7}]$ étant égal à 3, $Po(K) = Cl(K) \simeq \mathbb{Z}/3\mathbb{Z}$. Ainsi, $\mathbb{Q}[j, \sqrt[3]{7}]$, possède un groupe de Pólya isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Exemple 3.13. Pour $p = 17$, $17^2 \equiv 1 \pmod 9$, le corps $\mathbb{Q}[j, \sqrt[3]{17}]$ est donc un corps de Pólya.

3.3 Corps de Pólya quartiques cycliques

Rappelons quelques résultats obtenus à propos des corps quartiques cycliques. Tout d'abord, dans [22], on dispose d'une description complète des corps quartiques cycliques :

Théorème 3.14. *Si K est un corps quartique cyclique alors il s'écrit de manière unique sous la forme*

$$K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right) \tag{3.1}$$

où A, B, C et D sont des entiers tels que :

$$\begin{cases} A \text{ est impair sans facteurs carrés,} \\ D = B^2 + C^2,\ B > 0,\ C > 0,\ D \text{ sans facteurs carrés,} \\ (A, D) = 1 \end{cases} \tag{3.2}$$

Notations. Dans cette section, nous conserverons les notations utlisées dans ce théorème.

Remarque 3.15. Le corps $k = \mathbb{Q}\left(\sqrt{D}\right)$ est l'unique sous-corps quadratique de K. Le corps K est réel si $A > 0$ et imaginaire si $A < 0$.

Lemme 3.16. *Soit $K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right)$ un corps quartique cyclique et $k = \mathbb{Q}\left(\sqrt{D}\right)$ son unique sous-corps quadratique. Si un nombre premier p est ramifié dans l'extension $k/\mathbb{Q}$ alors il est totalement ramifié dans l'extension $K/\mathbb{Q}$.*

Preuve. Le corps $k = \mathbb{Q}\left(\sqrt{D}\right)$ est l'unique sous-corps quadratique de K. Ainsi si un premier est ramifié dans $k/\mathbb{Q}$, il est ramifié dans toutes les sous-extensions minimales de $K/\mathbb{Q}$. D'après le lemme 3.29, il est totalement ramifié dans $K/\mathbb{Q}$. □

Afin d'étudier la ramification dans l'extension $K/\mathbb{Q}$, on donne le discriminant de K.

Proposition 3.17. [25] *Soit $K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right)$ un corps quartique cyclique son discriminant D_K vérifie*

$D_K = 2^8 A^2 D^3$ *si* $D \equiv 0 \pmod 2$
$D_K = 2^6 A^2 D^3$ *si* $D \equiv 1 \pmod 2$ *et* $B \equiv 1 \pmod 2$
$D_K = 2^4 A^2 D^3$ *si* $D \equiv 1 \pmod 2$ *et* $B \equiv 0 \pmod 2, A + B \equiv 3 \pmod 4$
$D_K = A^2 D^3$ *si* $D \equiv 1 \pmod 2$ *et* $B \equiv 0 \pmod 2, A + B \equiv 1 \pmod 4$

On rappelle le résultat concernant le cardinal du groupe de Pólya d'un corps cyclique. Ici, $K/\mathbb{Q}$ est une extension cyclique de degré 4, d'après le corollaire 2.40 :

1. Si K est réel et si $N(\mathcal{O}_K^\times) = 1$, alors

$$|Po(K)| = \frac{1}{8}\prod_{p\in\mathbb{P}} e_p.$$

2. Sinon,

$$|Po(K)| = \frac{1}{4}\prod_{p\in\mathbb{P}} e_p.$$

Notations. Pour tout entier n, notons $\omega(n)$ le nombre de diviseurs premiers distincts de n. Considérons l'entier α_K défini de la manière suivante

$$\begin{cases} \alpha_K = 1 \text{ si } K \text{ est réel et si } N(\mathcal{O}_K^\times) = 1 \\ \alpha_K = 0 \text{ sinon,} \end{cases} \tag{3.3}$$

Proposition 3.18. *Soit $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$ un corps quartique cyclique. L'ordre $|Po(K)|$ de son groupe de Pólya est donné par :*

1. $|Po(K)| = 4^{\omega(D)-1}2^{\omega(A)-\alpha_K}$ *si* $D \equiv 0 \pmod 2$ *ou* $A+B \equiv 1 \pmod 4$
2. $|Po(K)| = 4^{\omega(D)-1}2^{\omega(A)-\alpha_K+1}$ *sinon .*

Preuve. L'entier D étant une somme de deux carrés, $D \equiv 1, 2 \pmod 4$. Si $D \equiv 2 \pmod 4$, le nombre de diviseurs du discrimant de $k = \mathbb{Q}[\sqrt{D}]$ est également celui de D. On en déduit que $s_k = \omega(D)$. Sachant que A est un nombre impair premier à D, qu'un premier ramifié dans $k/\mathbb{Q}$ est totalement ramifié dans $K/\mathbb{Q}$ (cf. proposition 3.16), on déduit facilement du cardinal du groupe de Pólya et du discriminant de K les égalités de la proposition. Le second cas correspond au fait que 2 peut diviser D_K sans diviser D. □

Proposition 3.19. *Un corps quartique cyclique $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$ est de Pólya si et seulement si il vérifie l'une des conditions suivantes où p et q désignent des nombres premiers impairs distincts :*

1. $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}})\right)$ *ou* $K = \mathbb{Q}\left(i\sqrt{2+\sqrt{2}})\right)$.
2. $K = \mathbb{Q}\left(\sqrt{q(2+\sqrt{2})}\right)$ *où* $N(\mathcal{O}_K^\times) = 1$.
3. $K = \mathbb{Q}\left(\sqrt{p+B\sqrt{p}}\right)$ *où* $p \equiv 1 \pmod 4$, $B \equiv 0 \pmod 4$, $p = B^2 + C^2$.
4. $K = \mathbb{Q}\left(i\sqrt{p+B\sqrt{p}}\right)$ *où* $p \equiv 1 \pmod 4$, $B \equiv 2 \pmod 4$, $p = B^2 + C^2$.
5. $K = \mathbb{Q}\left(\sqrt{p+B\sqrt{p}}\right)$ *avec* $p \equiv 1 \pmod 4$, $B \equiv 1, 2, 3 \pmod 4$, $p = B^2 + C^2$ *et* $N(\mathcal{O}_K^\times) = 1$.

6. $K = \mathbb{Q}\left(\sqrt{q(p+B\sqrt{p})}\right)$ *avec* $p \equiv 1 \pmod 4$, $p = B^2 + C^2$, $q + B \equiv 1 \pmod 4$ *et* $N(\mathcal{O}_K^\times) = 1$.

Preuve. Supposons K de Pólya. D'après la proposition 3.18, $\omega(D) = 1$ et $\omega(A) = 0$ ou 1 . Comme $D \equiv 1, 2 \pmod 4$, $D = 2$ ou $D = p$ où $p \equiv 1 \pmod 4$.

Traitons le cas $D = 2$. Alors $\omega(A) = \alpha_K$. Si $\alpha_K = 0$, $A = \pm 1$, d'où les corps $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}})\right)$ et $K = \mathbb{Q}\left(i\sqrt{2+\sqrt{2}})\right)$. Réciproquement, on vérifie que ces deux corps sont de Pólya puisque un seul premier y est ramifié, à savoir 2. Si $\alpha_K = 1$, alors $A > 0$, $\omega(A) = 1$ donc $A = q$ où q est un nombre premier. D'où un corps de la forme $\mathbb{Q}\left(\sqrt{q(2+\sqrt{2})}\right)$. Un tel corps est de Pólya sous réserve que $N(\mathcal{O}_K^\times) = 1$.

Traitons le cas $D = p \equiv 1 \pmod 4$. Lorsque $A + B \equiv 1 \pmod 4$, $\omega(A) = \alpha_K$. Si $\alpha_K = 0$, $A = \pm 1$, d'où les corps $K = \mathbb{Q}\left(\sqrt{p+B\sqrt{p}}\right)$ ($A = 1$, $B \equiv 0 \pmod 4$) et $K = \mathbb{Q}\left(i\sqrt{p+B\sqrt{p}}\right)$ ($A = -1$ et $B \equiv 2 \pmod 4$). Réciproquement ces deux corps sont de Pólya puisque seul le nombre premier p y est ramifié. Si $\alpha_K = 1$, alors $A > 0$, $\omega(A) = 1$ donc $A = q$ où q est un nombre premier impair. D'où un corps de la forme $\mathbb{Q}\left(\sqrt{q(p+B\sqrt{p})}\right)$. Un tel corps est de Pólya sous réserve que $N(\mathcal{O}_K^\times) = 1$.
Supposons que $A + B \not\equiv 1 \pmod 4$. On obtient $\omega(A) = \alpha_K - 1 = 0$. Donc $\alpha_K = 1$ et $A = 1$ ($B \not\equiv 0 \pmod 4$). On obtient un corps de la forme $\mathbb{Q}\left(\sqrt{(p+B\sqrt{p})}\right)$. Un tel corps est de Pólya sous réserve que $N(\mathcal{O}_K^\times) = 1$. □

Dans certains cas, il est possible de préciser la proposition précédente grâce au théorème suivant :

Proposition 3.20. [16] *Soit K un corps de nombres réel galoisien. Supposons que le conducteur f de K soit un entier composé. Soit M_f le sous-corps réel maximal de $\mathbb{Q}\left(e^{\frac{2i\pi}{f}}\right)$. Si le degré $[M_f : K]$ est impair, autrement dit, si $\frac{\varphi(f)}{2[K:\mathbb{Q}]}$ est impair, alors $N(\mathcal{O}_K^\times) = 1$.*

Suivant par exemple [38], rappelons comment nous est donné le conducteur d'un corps quartique cyclique, avec les mêmes notations que le théorème 3.14.

Proposition 3.21. [38] *Le conducteur f d'un corps quartique cyclique $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$ est $f = 2^l|A|D$ où*

$$l = \begin{cases} 3, \ \textit{si } D \equiv 2 \pmod 4 \ \textit{ou } D \equiv 1 \pmod 4, B \equiv 1 \pmod 2 \\ 2, \ \textit{si } D \equiv 1 \pmod 4, B \equiv 0 \pmod 2, A + B \equiv 3 \pmod 4 \\ 0, \ \textit{si } D \equiv 1 \pmod 4, B \equiv 0 \pmod 2, A + B \equiv 1 \pmod 4 \end{cases}$$

Nous pouvons alors raffiner les points 5 et 6 de la proposition 3.19

Corollaire 3.22. *1. Soit $K = \mathbb{Q}\left(\sqrt{p+B\sqrt{p}}\right)$ un corps quartique cyclique tel que $p \equiv 1 \pmod 4$ et $B \equiv 2 \pmod 4$, $p = B^2 + C^2$. Si $p \equiv 5 \pmod 8$, alors K est un corps de Pólya.*

2. Soit $K = \mathbb{Q}\left(\sqrt{q(p+B\sqrt{p})}\right)$ un corps quartique cyclique tel que avec $p \equiv 1 \pmod 4$, $B \equiv 0 \pmod 2$, $p = B^2 + C^2$, $q + B \equiv 1 \pmod 4$. Si $p \equiv 5 \pmod 8$ et $q \equiv 3 \pmod 4$, alors K est un corps de Pólya.

Preuve. 1. Le conducteur f de K vérifie $f = 2^2 p$. Si $p \equiv 5 \pmod 8$, $\frac{\varphi(f)}{2[K:\mathbb{Q}]} = \frac{p-1}{4}$ est impair puis on applique la proposition 3.20

2. Le conducteur f de K vérifie $f = qp$. Si $p \equiv 5 \pmod 8$ et $q \equiv 3 \pmod 4$, alors $\frac{\varphi(f)}{2[K:\mathbb{Q}]} = \frac{(p-1)(q-1)}{8}$ est impair et on conclut avec la proposition 3.20

□

3.4 Corps biquadratiques

Dans cette section, nous allons prouver qu'à quelques exceptions près, le compositum de deux corps quadratiques de Pólya est un corps biquadratique de Pólya. Plus précisément,

Théorème 3.23. *Soient m et n deux entiers distincts sans facteurs carrés tels que $\mathbb{Q}[\sqrt{m}]$ et $\mathbb{Q}[\sqrt{n}]$ soient deux corps quadratiques de Pólya. Alors le corps biquadratique $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ est un corps de Pólya à l'exception des corps suivants où p et q désignent des nombres premiers impairs distincts et où $p \equiv 3 \pmod 4$:*

1. *$\mathbb{Q}[i\sqrt{2}, \sqrt{p}]$ qui n'est pas un corps de Pólya.*
2. *$\mathbb{Q}[i, \sqrt{2q}]$ qui n'est pas un corps de Pólya.*
3. *Si $\mathbb{Q}[\sqrt{p}, \sqrt{2q}]$ est un corps de Pólya, alors :*
   (a) *soit $p \equiv -1 \pmod 8$ et $q \equiv 1, -1 \pmod 8$*
   (b) *soit $p \equiv 3 \pmod 8$ et $q \equiv 1, 3 \pmod 8$*

3.4.1 Rappels sur les discriminants et les bases entières des corps biquadratiques

Soient m et n deux entiers distincts sans facteurs carrés. Notons $l = pgcd(m, n)$ et m_1 et n_1 les entiers définis par $m = lm_1$ et $n = ln_1$. Le corps $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ possède alors trois sous-corps quadratiques distincts

qui sont $\mathbb{Q}[\sqrt{m}]$, $\mathbb{Q}[\sqrt{n}]$, $\mathbb{Q}[\sqrt{m_1 n_1}]$. Son groupe de Galois est isomorphe au groupe de Klein. K.S. Williams [41] fournit une formule explicite du discriminant D_K et d'une base $\mathcal{B}$ de l'anneau des entiers de K en fonction de m, n, l, m_1, n_1 suivant leurs congruences modulo 4 :

Cas n°1. $(m,n) \equiv (m_1,n_1) \equiv (1,1) \pmod 4$:

$$D_K = (l m_1 n_1)^2 \text{ et } \mathcal{B} = \left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1 n_1}}{4}\right\}.$$

Cas n°2. $(m,n) \equiv (1,1) \pmod 4$, $(m_1,n_1) \equiv (3,3) \pmod 4$:

$$D_K = (l m_1 n_1)^2 \text{ et } \mathcal{B} = \left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1 n_1}}{4}\right\}.$$

Cas n°3. $(m,n) \equiv (1,2) \pmod 4$:

$$D_K = (4 l m_1 n_1)^2 \text{ et } \mathcal{B} = \left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{m_1 n_1}}{2}\right\}.$$

Cas n°4. $(m,n) \equiv (2,3) \pmod 4$:

$$D_K = (8 l m_1 n_1)^2 \text{ et } \mathcal{B} = \left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_1 n_1}}{2}\right\}.$$

Cas n°5. $(m,n) \equiv (3,3) \pmod 4$:

$$D_K = (4 l m_1 n_1)^2 \text{ et } \mathcal{B} = \left\{1, \sqrt{m}, \frac{\sqrt{n}+\sqrt{m}}{2}, \frac{1+\sqrt{m_1 n_1}}{2}\right\}.$$

3.4.2 Compositum de deux corps quadratiques de Pólya

Pour essayer de montrer que le compositum de deux corps quadratiques de Pólya est un corps biquadratique de Pólya, nous nous appuyons sur la remarque qui suit la proposition 2.21 et qui permet de raffiner le corollaire 2.23 de la manière suivante :

Proposition 3.24. *Soit $K \subseteq L$ deux extensions galoisiennes de $\mathbb{Q}$. Si pour tout idéal premier $\mathfrak{p}$ of K, il existe deux extensions galoisiennes K_1 and K_2 de $\mathbb{Q}$ telles que :*

1. *K_1 et K_2 sont linéairement disjoints sur K et $L = K_1 K_2$,*
2. *$(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$,*

3. K_1 et K_2 sont des corps de Pólya,

alors L est un corps de Pólya.

Soient K_1 et K_2 deux corps quadratiques et soit $L = K_1K_2$. Notons D_{K_i} le discriminant de K_i. L'hypothèse "pour tout $\mathfrak{p}$ de K $(e_{K_1/K}(\mathfrak{p}), e_{K_2/K}(\mathfrak{p})) = 1$" est, de façon évidente, équivalente à " $(D_{K_1}, D_{K_2}) = 1$". Toutefois même si cette condition n'est pas satisfaite, la proposition précédente nous conduit à considérer le troisième sous-corps quadratique de L :

Proposition 3.25. *Si $K_1 = \mathbb{Q}[\sqrt{m}]$ et $K_2 = \mathbb{Q}[\sqrt{n}]$ sont deux corps quadratiques de Pólya distincts tels que 2 est ramifié dans au plus deux des trois extensions $\mathbb{Q}[\sqrt{m}]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$ et $\mathbb{Q}[\sqrt{m_1n_1}]/\mathbb{Q}$, alors le corps $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ est un corps de Pólya.*

Preuve. Considérons un nombre premier p impair ramifié à la fois dans $\mathbb{Q}[\sqrt{m}]/\mathbb{Q}$ et $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$, p divise D_{K_i} pour $i = 1, 2$ donc p divise (D_{K_1}, D_{K_2}). Or, $D_{K_1} = m$ ou $4m$ et $D_{K_2} = n$ ou $4n$. On en conclut que $p|4l$. Ainsi, p n'est pas ramifié dans $\mathbb{Q}[\sqrt{m_1n_1}]$. Il suffit ensuite d'appliquer la proposition précédente. □

Ainsi, lorsque $\mathbb{Q}[\sqrt{m}]$ et $\mathbb{Q}[\sqrt{n}]$ sont des corps quadratiques de Pólya, il est possible que $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ ne soit pas de Pólya lorsque 2 est ramifé dans toutes les extensions quadratiques $\mathbb{Q}[\sqrt{m}]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$ et $\mathbb{Q}[\sqrt{m_1n_1}]/\mathbb{Q}$.

Lemme 3.26. *Le premier 2 est ramifé dans toutes les extensions quadratiques $\mathbb{Q}[\sqrt{m}]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$ et $\mathbb{Q}[\sqrt{m_1n_1}]/\mathbb{Q}$ si et seulement si deux des trois entiers m, n, m_1n_1 sont congrus à 2 (mod 4) et que le troisième est congru à 3 (mod 4).*

Preuve. Pour que 2 soit ramifié dans les extensions quadratiques $\mathbb{Q}[\sqrt{m}]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}]/\mathbb{Q}$ et $\mathbb{Q}[\sqrt{m_1n_1}]/\mathbb{Q}$ il faut et il suffit que m, n, $m_1n_1 \equiv 2, 3 \pmod 4$. Raisonnons sur les congruences modulo 4 du couple (m, n).

- Si $m, n \equiv 3 \pmod 4$, alors $mn \equiv 1 \pmod 4$. Si ce produit mn est sans facteurs carrés, $mn = m_1n_1 \equiv 1 \pmod 4$, et dans ce cas 2 n'est pas ramifié dans $\mathbb{Q}[\sqrt{m_1n_1}]/\mathbb{Q}$. Si le produit mn possède un facteur carré q^2, $q^2 \equiv 1 \pmod 4$. Donc en débarrassant mn de tous ses facteurs carrés, $m_1n_1 \equiv 1 \pmod 4$.
- Supposons que $m, n \equiv 2 \pmod 4$. On ne peut pas avoir $m_1n_1 \equiv 2 \pmod 4$ sinon 4 diviserait m ou bien n, or ils sont supposés sans facteurs carrés. Pour que 2 soit ramifié dans $\mathbb{Q}[\sqrt{m_1n_1}]/\mathbb{Q}$, il faut et il suffit que $m_1n_1 \equiv 3 \pmod 4$
- Si $m \equiv 2 \pmod 4$ et $n \equiv 3 \pmod 4$, 2 n'est pas un facteur carré de mn donc $2|m_1n_1$. Ainsi $m_1n_1 \equiv 2 \pmod 4$.

□

En utilisant la caractérisation des corps quadratiques de Pólya (cf. proposition 1.38), nous pouvons donner la liste des corps biquadratiques, compositum de corps quadratiques de Pólya, dans lesquels 2 est ramifié dans chaque sous-extension quadratique :

Lemme 3.27. *Soient $\mathbb{Q}[\sqrt{m}]$ et $\mathbb{Q}[\sqrt{n}]$ deux corps quadratiques de Pólya. Le nombre premier 2 est ramifié dans chacune des sous-extensions quadratiques de $L = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ si et seulement si $(m, n) = (-1, 2)$, $(-1, 2q)$, $(2, p)$, $(-2, p)$, $(p, 2q)$ où p et q sont deux premiers impairs distincts tels que $p \equiv 3 \pmod 4$.*

Un corps biquadratique $L = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ de l'une des 5 formes données dans le lemme 3.27 est de Pólya si et seulement si $\Pi_2(L)$ est principal. Le lemme qui suit nous dit que 2 est totalement ramifié dans ces corps biquadratiques. Ainsi l'idéal $\Pi_2(L)$ sera principal si et seulement si L possède un entier de norme ± 2.

Définition 3.28. Soit L/K une extension finie non triviale de corps de nombres. On dit que L est une *extension minimale* de K si, pour tout corps M tel que $K \subset M \subset L$, $M = L$ ou $M = K$.

Lemme 3.29. *Soit L/K une extension galoisienne. Un idéal premier $\mathfrak{p}$ de K est totalement ramifiée dans l'extension L/K si et seulement si il est ramifié dans toutes les extensions minimales de K contenues dans L.*

Preuve. Une implication est immédiate, montrons l'autre. Supposons que $\mathfrak{p}$ ne soit pas totalement ramifié dans l'extension L/K. Soit $\mathfrak{P}$ un idéal premier de L au dessus de $\mathfrak{p}$, le groupe I d'inertie de $\mathfrak{P}$ dans L/K est un sous groupe strict de $Gal(L/K)$. On considére L^I, le sous corps de L laissé fixe par I. L'idéal premier $\mathfrak{p}$ est alors non ramifié dans l'extension L^I/K et L^I/K contient une extension minimale dans laquelle $\mathfrak{p}$ est non ramifié. □

Lemme 3.30. *Soit $L = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ un corps biquadratique de l'une des 5 formes données dans le lemme 3.27. Pour que L soit un corps de Pólya, il faut que chacune des 3 sous-extensions quadratiques de L contienne un entier de norme ± 2.*

C'est une conséquence du lemme 3.31 ci-dessous :

Lemme 3.31. *Soient L et K deux corps de nombres tels que $K \subset L$. Soit $\mathfrak{N} \in Max(\mathcal{O}_L)$ et posons $\mathfrak{M} = \mathfrak{N} \cap \mathcal{O}_K$. Si $\mathfrak{N}$ est principal et si $e(\mathfrak{N}/\mathfrak{M}) = [L : K]$, alors $\mathfrak{M}$ est également principal.*

En effet, si $\mathfrak{N} = \alpha\mathcal{O}_L$ alors $N_L^K(\mathfrak{N}) = \mathfrak{M} = N_{L/K}(\alpha)\mathcal{O}_K$.

3.4.3 Les 5 cas particuliers

Nous allons considérer les 5 corps biquadratiques L du lemme 3.27 et chercher s'il existe un générateur de l'idéal $\Pi_2(L)$. L'idéal $\Pi_2(L)$ étant maximal, $\mathcal{O}_L/\Pi_2(L) \simeq \mathbb{F}_2$. Soit ψ le morphisme de $\mathcal{O}_L$ vers $\mathbb{F}_2$ ayant pour noyau $\Pi_2(L)$.

Proposition 3.32. *Le corps $L = \mathbb{Q}[\sqrt{2}, i]$ est un corps de Pólya et l'idéal $\Pi_2(L)$ est engendré par $\frac{\sqrt{2}+i\sqrt{2}}{2} - 1$.*

Preuve. L'extension $L/\mathbb{Q}$ étant galoisienne et ne possédant qu'un seul premier ramifié à savoir 2, d'après la proposition 2.8, le corps L est un corps de Pólya. Nous avons donc répondu à la question mais nous allons tout de même déterminer un générateur de $\Pi_2(L)$.
Une base de $\mathcal{O}_L$ est $\mathcal{B} = \left\{1, \sqrt{2}, i, \frac{\sqrt{2}+i\sqrt{2}}{2}\right\}$. Comme $\psi(2) = 0$ et $\psi(-1) = 1$, $\psi(\sqrt{2}) = 0$ et $\psi(i) = 1$. Par ailleurs, $\left(\frac{\sqrt{2}+i\sqrt{2}}{2}\right)^2 = i$ donc $\psi\left(\frac{\sqrt{2}+i\sqrt{2}}{2}\right) = 1$. Décrivons le morphisme ψ. Soit $x = a + b\sqrt{2} + ci + d\frac{\sqrt{2}+i\sqrt{2}}{2} \in \Pi_2(L)$. Dans $\mathbb{F}_2$,

$$\bar{0} = \psi(x) = \bar{a} + \bar{c} + \bar{d}.$$

Ainsi,

$$\exists k \in \mathbb{Z}, a + c + d = 2k$$

$$\exists k \in \mathbb{Z}, x = 2k + b\sqrt{2} + c(i-1) + d(\frac{\sqrt{2}+i\sqrt{2}}{2} - 1).$$

Ceci montre que

$$\Pi_2(L) = 2.\mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus (i-1)\mathbb{Z} \oplus \left(\frac{\sqrt{2}+i\sqrt{2}}{2} - 1\right)\mathbb{Z}.$$

Comme $i-1 = i\sqrt{2}\left(\frac{\sqrt{2}+i\sqrt{2}}{2}\right)$, $\Pi_2(L)$ est l'idéal engendré par $\sqrt{2}$ et $\frac{\sqrt{2}+i\sqrt{2}}{2}-1$. On note que

$$\sqrt{2} = \left(-i - \frac{\sqrt{2}+i\sqrt{2}}{2}\right)\left(\frac{\sqrt{2}+i\sqrt{2}}{2} - 1\right).$$

Donc $\Pi_2(L)$ est l'idéal engendré par $\left(\frac{\sqrt{2}+i\sqrt{2}}{2} - 1\right)$. Bien sûr, on vérifie :

$$\begin{aligned} N_{L/\mathbb{Q}}\left(\tfrac{\sqrt{2}+i\sqrt{2}}{2} - 1\right) &= \left(\tfrac{\sqrt{2}+i\sqrt{2}}{2} - 1\right)\left(\tfrac{-\sqrt{2}-i\sqrt{2}}{2} - 1\right) \\ &\quad \left(\tfrac{\sqrt{2}-i\sqrt{2}}{2} - 1\right)\left(\tfrac{-\sqrt{2}+i\sqrt{2}}{2} - 1\right) \\ &= 2 \end{aligned}$$

□

Traitons le cas des corps biquadratiques imaginaires $\mathbb{Q}[\sqrt{-2}, \sqrt{p}]$ et $\mathbb{Q}[i, \sqrt{2q}]$.

Proposition 3.33. *Pour tout p premier tel que $p \equiv 3 \pmod 4$, le corps $L = \mathbb{Q}[\sqrt{-2}, \sqrt{p}]$ n'est pas de Pólya.*

Preuve. Si l'idéal $\Pi_2(L)$ était principal, d'après le lemme 3.31, en posant $K = \mathbb{Q}[\sqrt{-2p}]$, l'idéal $\Pi_2(K)$ serait lui aussi principal. Comme le nombre 2 est ramifié dans $K/\mathbb{Q}$, il existerait un élément de norme ± 2 dans $\mathcal{O}_K$. Toutefois l'équation $a^2 + 2pb^2 = \pm 2$ n'admet pas de solutions entières. □

De la même manière, comme il n'existe aucun idéal de norme 2 dans $K = \mathbb{Q}[i, \sqrt{2q}]$, on montre que :

Proposition 3.34. *Pour tout q premier impair, le corps $L = \mathbb{Q}[i, \sqrt{2q}]$ n'est pas de Pólya.*

Traitons le cas incertain des corps du type $L = \mathbb{Q}[\sqrt{2}, \sqrt{p}]$ où $p \equiv 3 \pmod 4$. Une base de $\mathcal{O}_L$ est $\mathcal{B} = \left\{1, \sqrt{2}, \sqrt{p}, \frac{\sqrt{2}+\sqrt{2p}}{2}\right\}$. Comme $\psi(2) = 0$ et $\psi(p) = 1$, $\psi(\sqrt{2}) = 0$ et $\psi(\sqrt{p}) = 1$. De plus $\left(\frac{\sqrt{2}+\sqrt{2p}}{2}\right)^2 = \frac{p+1}{2} + \sqrt{p}$. Donc $\psi\left(\frac{\sqrt{2}+\sqrt{2p}}{2}\right) = 1$. Soit $x = a + b\sqrt{2} + c\sqrt{p} + d\frac{\sqrt{2}+\sqrt{2p}}{2} \in \Pi_2(L)$, $\bar{0} = \psi(x) = \bar{a} + \bar{c} + \bar{d}$. Il existe $k \in \mathbb{Z}$ tel que $a + c + d = 2k$. D'où $x = 2k + b\sqrt{2} + c(\sqrt{p} - 1) + d\left(\frac{\sqrt{2}+\sqrt{2p}}{2} - 1\right)$. Ceci montre que

$$\Pi_2(L) = 2.\mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus (\sqrt{p} - 1)\mathbb{Z} \oplus \left(\frac{\sqrt{2} + \sqrt{2p}}{2} - 1\right)\mathbb{Z}.$$

Or,

$$\sqrt{p} - 1 = \sqrt{2}\left(\frac{-\sqrt{2} + \sqrt{2p}}{2}\right)$$

et $\frac{-\sqrt{2}+\sqrt{2p}}{2} \in \mathcal{O}_L$ car il s'agit d'un conjuqué de $\frac{\sqrt{2}+\sqrt{2p}}{2}$. L'idéal $\Pi_2(L)$ est donc engendré par $\sqrt{2}$ et $\frac{\sqrt{2}+\sqrt{2p}}{2} - 1$ dans $\mathcal{O}_L$.

Notons $\alpha_p = \frac{\sqrt{2}+\sqrt{2p}}{2} - 1$, $N(\alpha_p) = \left(\frac{p-1}{2}\right)^2 - p$. Notons que $\left(\frac{p-1}{2}\right)^2 - p = \pm 2$ si $p = 3$ ou $p = 7$. Ainsi $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ et $\mathbb{Q}[\sqrt{2}, \sqrt{7}]$ possèdant tous deux un élément de norme 2, à savoir respectivement α_3 et α_7, ils sont tous deux des corps de Pólya.

Pour $p \geq 11$, $N(\alpha_p) \geq 14$ et $N(\sqrt{2}) = 4$ donc $\sqrt{2} \notin \alpha_p\mathcal{O}_L$. De plus, une égalité du type $\alpha_p = \sqrt{2}\beta$ où $\beta \in \mathcal{O}_L$ aboutit à une absurdité.

S'il est difficile de touver un générateur de $\Pi_2(L)$ à partir de ces deux générateurs, on peut se référer à [1]. A. Azizi et A. Mouhib s'intéressent aux corps biquadratiques réels du type $K = \mathbb{Q}[\sqrt{m}, \sqrt{d}]$ tels que $m = 2$ ou bien m est un nombre premier tel que $m \equiv 1 \pmod 4$ et d un entier naturel sans facteurs carrés. Rappelons la partie de leur théorème 1 correspondant à $m = 2$:

Proposition 3.35. [1, Thm. 1] *Soient $k = \mathbb{Q}\left(\sqrt{2}\right)$ et $K = k\left(\sqrt{d}\right)$ où d est un entier sans facteurs carrés. Notons r le nombre d'idéaux premiers de $k = \mathbb{Q}[\sqrt{2}]$ qui se ramifient dans K et posons $2^e = [\mathcal{O}_k^\times : N_{K/k}(K^*) \cap \mathcal{O}_k^\times]$. Alors,*

1. *Le rang du 2-groupe des classes $Cl_2(K)$ de K est égal à $r - 1 - e$.*
2. *S'il existe un premier impair q divisant d tel que $q \equiv 3 \pmod 4$, alors $e = 1$ ou $e = 2$.*
3. *Le rang de $Cl_2(K)$ est $r-2$ si et seulement si, pour tout nombre premier impair q divisant d, $\left(\frac{2}{q}\right) = 1 \Rightarrow \left(\frac{-1}{q}\right) = 1$*

Corollaire 3.36. *Les corps biquadratiques du type $L = \mathbb{Q}[\sqrt{2}, \sqrt{p}]$ où $p \equiv 3 \pmod 4$ sont des corps de Pólya.*

Preuve. Nous allons appliquer la proposition précédente avec $d = p \equiv 3 \pmod 4$. Le rang de $Cl_2(K)$ est ici égal à $r - 2$ ou $r - 3$.

Lorsque $\left(\frac{2}{p}\right) = -1$, il y a exactement $r = 2$ idéaux premiers ramifiés dans l'extension $L/\mathbb{Q}[\sqrt{2}]$, il s'agit des idéaux premiers au dessus de 2 et p dans $\mathbb{Q}[\sqrt{2}]$. Le rang du 2-groupe de classes de L est donc nul, autrement dit, le 2-groupe de classes de L est trivial. Par ailleurs, on sait que $2\mathcal{O}_L = \Pi_2(L)^4$, $\Pi_2(L)$ est donc principal.
Lorsque $\left(\frac{2}{p}\right) = 1$, il y a exactement $r = 3$ idéaux premiers ramifiés dans l'extension $L/\mathbb{Q}[\sqrt{2}]$, à savoir 2 idéaux premiers dans $\mathbb{Q}[\sqrt{2}]$ au dessus de 2 et le dernier au dessus de p. Comme $p \equiv 3 \pmod 4$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$. D'après la 3ème assertion de la proposition précédente, le rang de $Cl_2(K)$ n'est pas égal à $r - 2$ donc est égal à $r - 3 = 0$. Le 2-groupe de classes de L est de nouveau trivial. □

Pour finir, nous nous intéressons au dernier cas particulier : le corps $L = \mathbb{Q}[\sqrt{2q}, \sqrt{p}]$ où p et q sont deux premiers distincts tels que $p \equiv 3 \pmod 4$. La considération des équations aux normes dans $\mathbb{Q}(\sqrt{2pq})$ nous permet d'obtenir la condition nécessaire suivante :

Proposition 3.37. *Soient p et q des nombres premiers impairs distincts tels que $p \equiv 3 \pmod 4$. Si $\mathbb{Q}[\sqrt{p}, \sqrt{2q}]$ est un corps de Pólya, alors :*

1. *soit $p \equiv -1 \pmod 8$ et $q \equiv 1, -1 \pmod 8$*
2. *soit $p \equiv 3 \pmod 8$ et $q \equiv 1, 3 \pmod 8$*

Preuve. Supposons que L soit un corps de Pólya. L'idéal $\Pi_2(L)$ est alors principal. D'après le lemme 3.31, en posant $K = \mathbb{Q}[\sqrt{2pq}]$, l'idéal $\Pi_2(K)$ serait lui aussi principal. Comme le nombre 2 est ramifié dans $K/\mathbb{Q}$, il existerait un élément de norme ± 2 dans $\mathcal{O}_K$: l'équation $a^2 - 2pqb^2 = \pm 2$ admet un couple solution $(a, b) \in \mathbb{Z}^2$. On obtient :

$$\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = 1 \text{ ou } \left(\frac{-2}{p}\right) = \left(\frac{-2}{q}\right) = 1.$$

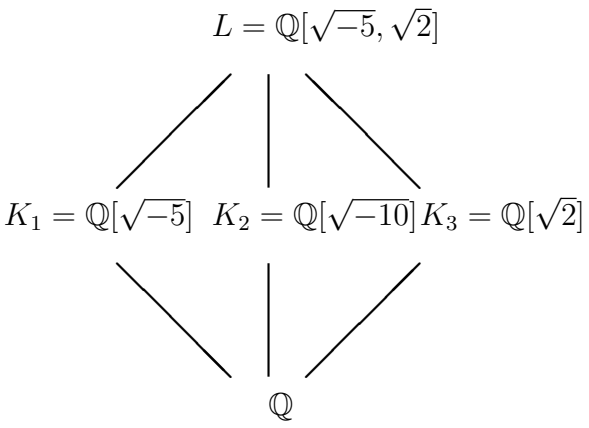
Or, $p \equiv 3 \pmod 4$ donc $p \equiv -1 \pmod 8$ ou $p \equiv 3 \pmod 8$. Les règles de calculs pour le symbole de Legendre nous donnent facilement les conditions sur q de la proposition. □

Remarque 3.38. Lorsque $p, q \equiv 3 \pmod 8$, les calculs effectués avec KASH montrent que, pour $p, q < 100$, $\mathbb{Q}[\sqrt{p}, \sqrt{2q}]$ est toujours un corps de Pólya. Cependant, dans tous les autres cas, la condition précédente apparait comme non suffisante puisque l'on dispose, pour chaque condition précitée sur p et q, d'un couple (p, q) tel que $\mathbb{Q}[\sqrt{p}, \sqrt{2q}]$ n'est pas un corps de Pólya. Par exemple, les corps $\mathbb{Q}[\sqrt{7}, \sqrt{34}]$, $\mathbb{Q}[\sqrt{7}, \sqrt{46}]$, $\mathbb{Q}[\sqrt{3}, \sqrt{66}]$ sont de Pólya mais ce n'est pas le cas de $\mathbb{Q}[\sqrt{7}, \sqrt{82}]$, $\mathbb{Q}[\sqrt{7}, \sqrt{62}]$, $\mathbb{Q}[\sqrt{3}, \sqrt{34}]$.

3.5 Un contre-exemple important

Relativement aux notions de corps de Pólya et d'extensions de Pólya, nous avons noté d'emblée à propos du nouveau problème de plongement étudié qu'une extension de Pólya n'est pas nécessairement un corps de Pólya. Nous donnons maintenant un exemple d'*un corps galoisien qui est extension de Pólya de tous ses sous-corps et qui pourtant n'est pas un corps de Pólya.*

Exemple 3.39. Le corps $L = \mathbb{Q}[\sqrt{-5}, \sqrt{2}]$ est une extension de Pólya de tous ses sous-corps et pourtant n'est pas un corps de Pólya.



La classification des corps quadratiques de Pólya (cf. proposition 1.38) nous permet d'affirmer que, contrairement à $\mathbb{Q}[\sqrt{2}]$, les corps $\mathbb{Q}[\sqrt{-10}]$ et $\mathbb{Q}[\sqrt{-5}]$ ne sont pas des corps de Pólya. Nous pouvons d'ores et déja affirmer que l'extension $\mathbb{Q}[\sqrt{-5}, \sqrt{2}]/\mathbb{Q}[\sqrt{2}]$ est une extension de Pólya. Etudions ensuite l'extension $\mathbb{Q}[\sqrt{-5}, \sqrt{2}]/\mathbb{Q}[\sqrt{-10}]$. Les seuls premiers ramifiés dans $\mathbb{Q}[\sqrt{-10}]/\mathbb{Q}$ sont 2 et 5. D'après l'exemple 1.59, $\mathbb{Q}[\sqrt{-5}, \sqrt{2}]/\mathbb{Q}[\sqrt{-10}]$ est une extension de Pólya. De même, l'extension L/K_1 est une extension de Pólya.

Montrons que L n'est pas un corps de Pólya. Pour cela, montrons que $\Pi_2(L)$ n'est pas un idéal principal. Comme 2 est ramifié dans chacune des extensions K_i, d'après le lemme 3.29 il existe un unique idéal maximal $\mathfrak{N}$ au dessus de 2 dans $\mathcal{O}_L$:

$$2\mathcal{O}_L = \mathfrak{N}^4 = \Pi_2(L)^4.$$

Si $\Pi_2(L)$ était principal, il existerait $\alpha \in \mathcal{O}_L$ tel que $\Pi_2(L) = \alpha\mathcal{O}_L$. Appliquons le morphisme norme $N_{K_1}^L$,

$$N_{K_1}^L(\Pi_2(L)) = N_{K_1}^L(\alpha\mathcal{O}_L) = N_{L/K_1}(\alpha)\mathcal{O}_{K_1}.$$

Or, $N_{K_1}^L(\Pi_2(L)) = \Pi_2(K_1)$ car l'extension $L/\mathbb{Q}$ est complètement ramifiée en 2. L'équation $a^2 + 5b^2 = 2$, n'admettant pas de solution entière, $\Pi_2(K_1)$ n'est pas principal. Aboutissant à une contradiction, $\Pi_2(L)$ n'est pas un idéal principal.

On obtient alors :

$$Po(K_1) \simeq \mathbb{Z}/2\mathbb{Z},\ Po(K_2) \simeq \mathbb{Z}/2\mathbb{Z},\ Po(K_3) = \{1\} \text{ et } Po(L) \simeq \mathbb{Z}/2\mathbb{Z}.$$

En effet, l'extension $L/\mathbb{Q}$ est galoisienne et les premiers ramifiés dans cette extension sont 2 et 5. Or, $\Pi_5(L) = \sqrt{-5}\mathcal{O}_L$. Ainsi, $Po(L)$ est engendré par

la classe de $\Pi_2(L)$ dans $Cl(K)$. L'étude de la ramification dans $L/\mathbb{Q}$ nous montre que $\sqrt{2}\mathcal{O}_{K_3} = \Pi_2(K_3)$ et que $\Pi_2(K_3)\mathcal{O}_L = \Pi_2(L)^2$. Ainsi, $\Pi_2(L)^2$ est principal. Nous en concluons que $Po(L) \simeq \mathbb{Z}/2\mathbb{Z}$. L'extension L/K_2 étant de Pólya, $Po(K_2, L) = \{1\}$.

Chapitre 4

Le corps de genre : une réponse ambiguë au problème de plongement

Au cours du premier chapitre, nous avons vu que le corps de classes de Hilbert H_K d'un corps de nombres K était une extension de Pólya de K (cf. théorème 1.50). Cependant, un exemple simple montre que H_K n'est pas une extension de Pólya minimale. En effet considérons l'extension de corps $\mathbb{Q}\left(\sqrt{-95}\right) \subset \mathbb{Q}\left(\sqrt{5}, \sqrt{-19}\right)$. On vérifie à l'aide de l'exemple 1.59 qu'il s'agit d'une extension de Pólya et que cette extension est non ramifiée. Elle est donc contenue dans le corps de classes de Hilbert de $\mathbb{Q}\left(\sqrt{-95}\right)$. Or, le nombre de classes de $\mathbb{Q}\left(\sqrt{-95}\right)$ est 8. On a donc un exemple d'extension de Polya d'un corps K incluse strictement dans H_K : H_K n'est donc pas une extension de Pólya minimale. Le corps $\mathbb{Q}\left(\sqrt{5}, \sqrt{-19}\right)$ est en fait ce qu'on appelle le corps de genre de $\mathbb{Q}\left(\sqrt{-95}\right)$.

4.1 Présentation du corps de genre

Dans ce paragraphe, en suivant l'ouvrage de M. Ishida [26], nous rappelons comment a été défini le corps de genre. Dans le cas où K est un corps de nombres abélien, Leopoldt [29] a défini la notion de corps de genre au sens restreint :

Définition 4.1. Soit K un corps de nombres abélien. Le *corps de genre au sens restreint* $\Gamma_K^{'}$ de K est l'extension abélienne maximale de $\mathbb{Q}$ contenant K et telle que $\Gamma_K^{'}/K$ est non ramifiée aux places finies.

A. Fröhlich [13] a généralisé cette définition :

Définition 4.2. Soit K un corps de nombres quelconque. Le *corps de genre au sens restreint* $\Gamma_K^{'}$ de K est l'extension maximale non ramifiée aux places finies de K obtenue en composant K avec une extension abélienne de $\mathbb{Q}$.

Tout comme pour le corps de classes, on distingue le corps de genre au sens large Γ_K, qui impose que toutes les places finies ou infinies de K soient non ramifiées dans Γ_K/K, du corps de genre au sens restreint $\Gamma_K^{'}$ qui lui, impose que seulement les places finies soient non ramifiées.

Définition 4.3. Soit K un corps de nombres abélien. Le *corps de genre* Γ_K *de* K *au sens large* de K, ou plus simplement corps de genre de K est l'extension abélienne maximale de $\mathbb{Q}$ contenant K et telle que Γ_K/K est non ramifiée en toutes les places.

La définition de corps de genre au sens restreint a été initialement donnée par Hasse [23] pour les corps quadratiques. Pour un corps de nombres quelconque, on dispose de la définition plus générale qui suit :

Définition 4.4. [21, Chap. 4, §4] Soit K un corps de nombres quelconque. Le *corps de genre de* K est la sous-extension maximale de H_K égale au compositum de K avec une extension abélienne de $\mathbb{Q}$.

Le théorème suivant donne une définition explicite du corps de genre au sens restreint et au sens large d'un corps quadratique. Une preuve est donnée dans [26], mais on la trouve également dans [21].

Proposition 4.5. [21, §4.2.9] *Soit* $K = \mathbb{Q}\left(\sqrt{d}\right)$ *un corps quadratique où* d *est un entier sans facteurs carrés. En écrivant* d *sous la forme*

$$d := s2^{\delta}.\prod_{i=1}^{t} s_i p_i$$

où les p_i *sont les diviseurs impairs de* d, $\delta \in \{0,1\}$, $s_i := (-1)^{\frac{p_i-1}{2}}$, $s \in \{-1,1\}$. *Le corps de genre au sens restreint de* $K = \mathbb{Q}\left(\sqrt{d}\right)$ *est*

$$\Gamma_K^{'} = \mathbb{Q}\left(\sqrt{s2^{\delta}}, \sqrt{s_1 p_1}, \ldots, \sqrt{s_t p_t}\right).$$

Le corps de genre au sens large est obtenu de la manière suivante :

1. *Si* $d < 0$, $\Gamma_K = \Gamma_K^{'}$. *Lorsque* $d > 0$, $\Gamma_K = \Gamma_K^{'}$ *si et seulement si* $s_1 = s_2 = \ldots = s_t = 1$.
2. *Sinon,* Γ_K *est le sous-corps réel maximal de* $\Gamma_K^{'}$.

4.2 Capitulation des idéaux ambiges

Dans toute cette partie K est un corps de nombres abélien. Nous suivons un travail d'Hisako Furuya [15] dans lequel il prouve que les idéaux ambiges de $\mathcal{O}_K$ capitulent dans Γ_K' et Γ_K.

Précisons le théorème de Konecker-Weber énoncé au premier chapitre :

Théorème 4.6. [26, Chap.1][Kronecker, Weber] *Tout corps de nombres abélien K est contenu dans un corps cyclotomique $\mathbb{Q}[\zeta_m]$ ($m \in \mathbb{N}$). Le plus petit entier m tel que $K \subset \mathbb{Q}[\zeta_m]$ est le conducteur de K que l'on a déjà noté f_K. De plus, un nombre premier p est ramifié dans K si et seulement si $p \mid f_K$.*

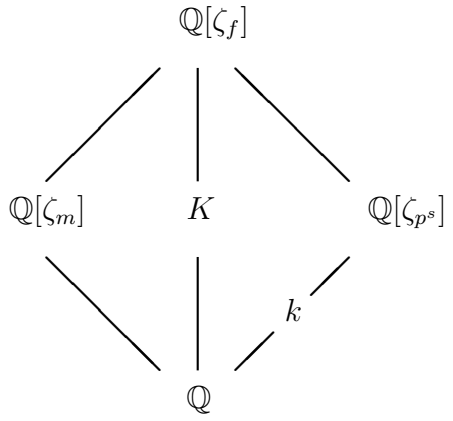
Compte tenu de l'importance de cette notion de corps de genre, nous réécrivons la preuve du résultat de Furuya (Thm 4.8 ci-après) tout comme, nous avons dans une certaine mesure repris la preuve de Hilbert à propos des idéaux ambiges d'un corps quadratique.

Proposition 4.7. *Soit K un corps de nombres abélien. Soit f tel que $K \subset \mathbb{Q}[\zeta_f]$ et soit p un diviseur de f. Ecrivons $f = p^s m$ où $p \nmid m$ et posons*

$$k = K\mathbb{Q}[\zeta_m] \cap \mathbb{Q}[\zeta_{p^s}].$$

On a l'égalité suivante :

$$[k : \mathbb{Q}] = e_p(K/\mathbb{Q}).$$



Preuve. L'extension $\mathbb{Q}[\zeta_{p^s}]/\mathbb{Q}$ étant totalement ramifiée, $[k : \mathbb{Q}] = e_p(k/\mathbb{Q})$. Montrons que $e_p(K/\mathbb{Q}) = e_p(k/\mathbb{Q})$. Montrons tout d'abord que pour tout corps de nombres N tel que $N \subset \mathbb{Q}[\zeta_f]$,

$$e_p(\mathbb{Q}[\zeta_f]/N) = [\mathbb{Q}[\zeta_f] : N\mathbb{Q}[\zeta_m]]$$

Dans l'extension $\mathbb{Q}[\zeta_f]/\mathbb{Q}$, le groupe d'inertie relatif à p est le groupe de Galois $G\left(\mathbb{Q}[\zeta_f]/\mathbb{Q}[\zeta_m]\right)$. Le groupe d'inertie relatif à p dans l'extension $\mathbb{Q}[\zeta_f]/N$ est donc

$$G\left(\mathbb{Q}[\zeta_f]/\mathbb{Q}[\zeta_m]\right) \cap G\left(\mathbb{Q}[\zeta_f]/N\right) = G\left(\mathbb{Q}[\zeta_f]/N\mathbb{Q}[\zeta_m]\right).$$

D'où

$$e_p(\mathbb{Q}[\zeta_f]/N) = [\mathbb{Q}[\zeta_f] : N\mathbb{Q}[\zeta_m]].$$

De ce fait,

$$e_p(\mathbb{Q}[\zeta_f]/K) = [\mathbb{Q}[\zeta_f] : K\mathbb{Q}[\zeta_m]],$$
$$e_p(\mathbb{Q}[\zeta_f]/k) = [\mathbb{Q}[\zeta_f] : k\mathbb{Q}[\zeta_m]].$$

Montrer que

$$[k : \mathbb{Q}] = e_p(K/\mathbb{Q})$$

revient à prouver que

$$e_p(\mathbb{Q}[\zeta_f]/K) = e_p(\mathbb{Q}[\zeta_f]/k)$$

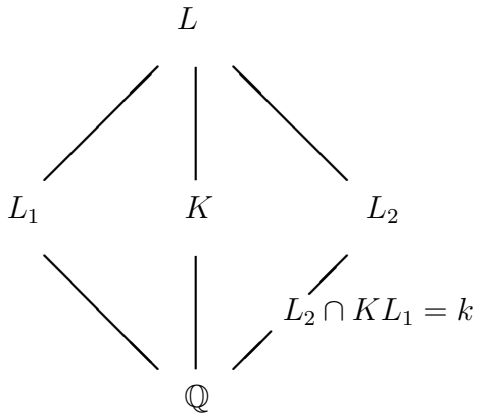
ou encore que

$$[\mathbb{Q}[\zeta_f] : K\mathbb{Q}[\zeta_m]] = [\mathbb{Q}[\zeta_f] : k\mathbb{Q}[\zeta_m]].$$

D'après la définition de k, $k\mathbb{Q}[\zeta_m] \subset K\mathbb{Q}[\zeta_m]$. Montrons que

$$k\mathbb{Q}[\zeta_m] = K\mathbb{Q}[\zeta_m].$$

Cela revient à prouver que $G\left(\mathbb{Q}[\zeta_f]/K\mathbb{Q}[\zeta_m]\right) = G\left(\mathbb{Q}[\zeta_f]/k\mathbb{Q}[\zeta_m]\right)$. Un diagramme simplifié sera utile :



Montrons que $G\left(L/KL_1\right) = G\left(L/kL_1\right)$. Tout d'abord,

$$G\left(L/kL_1\right) = G\left(L/k\right) \cap G\left(L/L_1\right),$$

et,

$$G\left(L/k\right) = G\left(L/L_2 \cap KL_1\right) = G\left(L/KL_1\right) \times G\left(L/L_2\right).$$

D'où

$$G\left(L/kL_1\right) = \left(G\left(L/KL_1\right) \times G\left(L/L_2\right)\right) \cap G\left(L/L_1\right).$$

Or, $G\left(L/KL_1\right) \subset G\left(L/L_1\right)$, il vient

$$G\left(L/kL_1\right) = G\left(L/KL_1\right) \times \left(G\left(L/L_2\right) \cap G\left(L/L_1\right)\right)$$

Mais

$$G\left(L/L_2\right) \cap G\left(L/L_1\right) = G\left(L/L_2L_1\right) = G\left(L/L\right) = Id,$$

on peut alors conclure :

$$G\left(L/KL_1\right) = G\left(L/kL_1\right).$$

□

Théorème 4.8. [15, Furuya] *Soit $f = p_1^{r_1} \dots p_t^{r_t}$ une factorisation du conducteur de K. Soit e_i l'indice de ramification de p_i dans $K/\mathbb{Q}$. Pour tout p_i impair, soit le sous-corps k_i de $\mathbb{Q}[\zeta_{p_i^{r_i}}]$ tel que $[k_i : \mathbb{Q}] = e_i$, celui-ci est déterminé de façon unique. Lorsque $p_i = 2$, on choisit parmi les sous-corps de $\mathbb{Q}[\zeta_{2_i^{r_i}}]$ un corps k_i adequat tel que $[k_i : \mathbb{Q}] = e_i$. Alors $\Gamma_K^{'} = k_1k_2 \dots k_t$.*

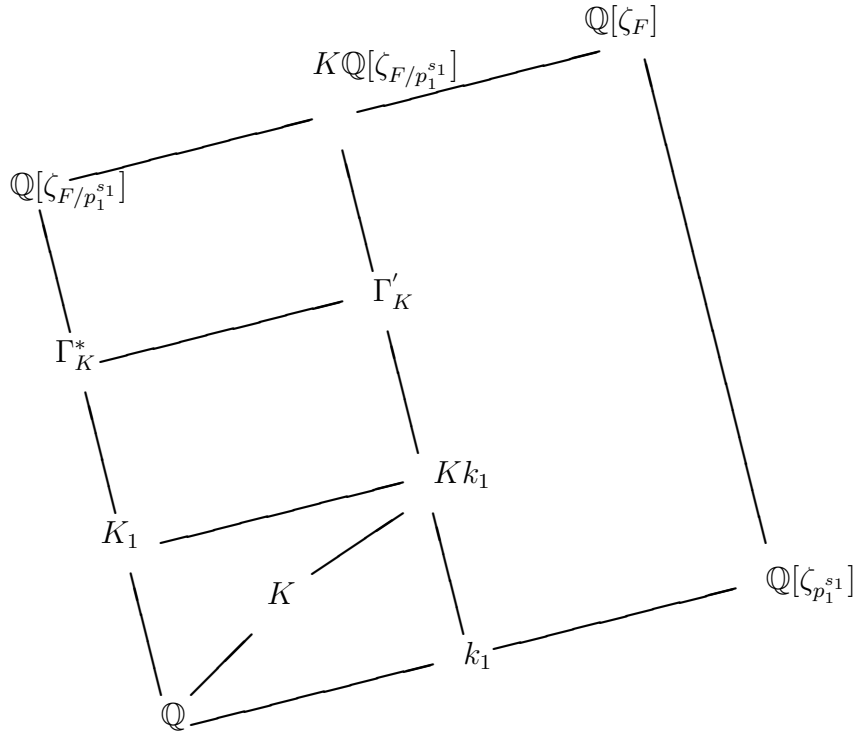
Preuve. Soit F le conducteur de $\Gamma_K^{'}$. Montrons que $f = F$.

Comme $K \subset \Gamma_K^{'} \subset \mathbb{Q}[\zeta_F]$, $f \leq F$. Comme $\Gamma_K^{'}/K$ est non ramifiée, les nombres premiers ramifiées dans $\Gamma_K^{'}/\mathbb{Q}$ sont exactement ceux qui sont ramifiées dans $K/\mathbb{Q}$. D'après le théorème de Kronecker-Weber, $f \mid F$ de sorte que $F = p_1^{s_1} \dots p_t^{s_t}$ où $r_i \leq s_i$.
Posons

$$k_1 = K\mathbb{Q}[\zeta_{F/p_1^{s_1}}] \cap \mathbb{Q}[\zeta_{p_1^{s_1}}]$$

et

$$K_1 = \mathbb{Q}[\zeta_{F/p_1^{s_1}}] \cap Kk_1.$$



Il vient $Kk_1 = KK_1$. Comme $k_1 \subset \mathbb{Q}[\zeta_{p_1^{s_1}}]$, $p_2, \ldots, p_t$ ne sont pas ramifiées dans $k_1/\mathbb{Q}$, ils ne sont donc pas ramifiés dans Kk_1/K. Comme p_1 n'est pas ramifié dans $K_1/\mathbb{Q}$ car $K_1 \subset \mathbb{Q}[\zeta_{F/p_1^{s_1}}]$, p_1 n'est pas ramifié dans KK_1/K donc dans Kk_1/K. Aucun idéal premier n'est alors ramifié dans Kk_1/K. De plus $Kk_1/\mathbb{Q}$ est abélienne. On en déduit que

$$Kk_1 \subset \Gamma'_K.$$

Montrons que $K\mathbb{Q}[\zeta_{F/p_1^{s_1}}] = \Gamma'_K\mathbb{Q}[\zeta_{F/p_1^{s_1}}]$. Supposons que $K\mathbb{Q}[\zeta_{F/p_1^{s_1}}] \subset \Gamma'_K\mathbb{Q}[\zeta_{F/p_1^{s_1}}]$. Comme p_1 est totalement ramifié dans $\mathbb{Q}[\zeta_F]/\mathbb{Q}[\zeta_{F/p_1^{s_1}}]$, p_1 est totalement ramifié dans les extensions intermédiares

$$\mathbb{Q}[\zeta_{F/p_1^{s_1}}] \subset K\mathbb{Q}[\zeta_{F/p_1^{s_1}}] \subset \Gamma'_K\mathbb{Q}[\zeta_{F/p_1^{s_1}}] \subset \mathbb{Q}[\zeta_F].$$

Or, p_1 n'est pas ramifié dans Γ'_K/K et ne l'est pas non plus dans l'extension $K\mathbb{Q}[\zeta_{F/p_1^{s_1}}]/K$. Il n'est donc pas ramifié dans l'extension $\Gamma'_K\mathbb{Q}[\zeta_{F/p_1^{s_1}}]/K$, a fortiori, il n'est pas non plus ramifié dans l'extension $\Gamma'_K\mathbb{Q}[\zeta_{F/p_1^{s_1}}]/K\mathbb{Q}[\zeta_{F/p_1^{s_1}}]$. Ainsi, $K\mathbb{Q}[\zeta_{F/p_1^{s_1}}] = \Gamma'_K\mathbb{Q}[\zeta_{F/p_1^{s_1}}]$. On en conclut que

$$\Gamma'_K \subset \mathbb{Q}[\zeta_{F/p_1^{s_1}}].$$

Comme $K \subset \mathbb{Q}[\zeta_{p_1^{r_1}\ldots p_t^{r_t}}]$, on a $\Gamma_K^{'} \subset \mathbb{Q}[\zeta_{p_1^{r_1}p_2^{s_2}\ldots p_t^{s_t}}]$, il vient $s_1 \leq r_1$. De la même façon, on montre que pour tout $i \in \{2, \ldots, t\}$, $s_i \leq r_i$. D'où

$$f = F.$$

Posons $\Gamma_K^* = \mathbb{Q}[\zeta_{f/p_1^{s_1}}] \cap \Gamma_K^{'}$ et montrons qu'il s'agit du corps de genre au sens restreint de K_1. Comme $Kk_1 \subset \Gamma_K^{'}$, $Kk_1 \cap \Gamma_K^{'} = Kk_1$, il vient $K_1 = \Gamma_K^* \cap Kk_1$. Par ailleurs, on montre facilement que $\Gamma_K^{'} = \Gamma_K^* Kk_1$.
Introduisons $\Gamma_K^{''}$ le corps de genre de K_1. Comme $\Gamma_K^{'}/K$ est non ramifiée et que $K \subset Kk_1 \subset \Gamma_K^{'}$, on conclut que $\Gamma_K^{'}/Kk_1$ est non ramifiée. Par ailleurs, les extensions $\mathbb{Q} \subset k_1 \subset \mathbb{Q}[\zeta_{p_1^{s_1}}]$ sont totalement ramifiées uniquement en p_1, on en conclut qu'aucun idéal au dessus de p_i, $i \neq 1$ n'est ramifié dans l'extension Kk_1/K_1. De ce fait, aucun idéal premier ne se ramifie dans Γ_K^*/K_1. Il vient $K_1 \subset \Gamma_K^* \subset \Gamma_K^{''}$.
Par ailleurs $\Gamma_K^{''}\Gamma_K^*/\mathbb{Q}$ est abélienne ; de plus, $\Gamma_K^{'}/K$ et Γ_K^*/K_1 étant non ramifiées, l'extension $\Gamma_K^{'}\Gamma_K^*/K$ est non ramifiée également. Ainsi, $\Gamma_K^{'}\Gamma_K^* \subset \Gamma_K^{'}$. Il vient $\Gamma_K^* \subset \Gamma_K^{'}$. Mais p_1 est totalement ramifié dans $\Gamma_K^{'}/\Gamma_K^*$, comme $K_1 \subset \Gamma_K^* \subset \Gamma_K^{''} \subset \Gamma_K^{'}$ et que $\Gamma_K^{''}/K_1$ est non ramifiée, on en déduit que $\Gamma_K^{''} = \Gamma_K^*$

On obtient $\Gamma_K^{'} = \Gamma_K^* k_1$, le conducteur de K_1 est $f/p_1^{r_1}$. On montre par récurence que $\Gamma_K^{'} = k_1 k_2 \ldots k_t$, le lemme précédent nous donne $[k_i : \mathbb{Q}] = e_i$. □

Corollaire 4.9. [Furuya] *Soit K une extension abélienne de $\mathbb{Q}$, les idéaux ambiges de $\mathcal{O}_K$ capitulent dans le corps de genre au sens restreint $\Gamma_K^{'}$ de K.*

Preuve. Rappelons que les idéaux premiers ambiges de $\mathcal{O}_K$ sont exactement les idéaux premiers au-dessus des nombres premiers ramifiés dans l'extension $K/\mathbb{Q}$. Il est bien connu que, pour tout nombre premier p_i,

$$\left(1 - \zeta_{p_i^{r_i}}\right)^{\varphi(p_i^{r_i})} = p\mathbb{Z}[\zeta_{p_i^{r_i}}].$$

Considérons la norme $N := N_{\mathbb{Q}[\zeta_{p_i^{r_i}}]/k_i}$. Comme l'extension $\mathbb{Q}[\zeta_{p_i^{r_i}}]/k_i$ est totalement ramifiée, $N\left(1 - \zeta_{p_i^{r_i}}\right)$ est un idéal maximal principal de $\mathcal{O}_{k_i}$ et on a $p\mathcal{O}_{k_i} = N\left(1 - \zeta_{p_i^{r_i}}\right)^{e_i} \mathcal{O}_{k_i}$. Par ailleurs, $p_i\mathcal{O}_K = \mathfrak{A}_i^{e_i}$ où $\mathfrak{A}_i$ est ambige. Il vient $p_i\mathcal{O}_{Kk_i} = (\mathfrak{A}_i\mathcal{O}_{Kk_i})^{e_i}$ et $p\mathcal{O}_{Kk_i} = N\left(1 - \zeta_{p_i^{r_i}}\right)^{e_i} \mathcal{O}_{Kk_i}$. On en déduit que

$$\mathfrak{A}_i\mathcal{O}_{Kk_i} = N\left(1 - \zeta_{p_i^{r_i}}\right)\mathcal{O}_{Kk_i}.$$

□

Remarque 4.10. C. Thiebaud généralise ce résultat de capitulation [40]. Elle prouve que si k est un corps quadratique imaginaire de discriminant $d_k < -4$ et K une extension abélienne de k de conducteur premier à 2, alors tout idéal ambige de K capitule dans Γ_K.

Corollaire 4.11. *Le corps de genre au sens restreint Γ'_K d'une extension abélienne K de $\mathbb{Q}$ est une extension de Pólya de K.*

Dans [15], H. Furuya montre ensuite que les idéaux ambiges d'un corps abélien K capitulent déjà dans le corps de genre au sens large de K. D'où l'énoncé plus fort :

Proposition 4.12. *Le corps de genre au sens large Γ_K d'une extension abélienne K de $\mathbb{Q}$ est une extension de Pólya de K.*

Ainsi si l'on note g_K le nombre de genre du corps K à savoir $g_K = [\Gamma_K : K]$, on a l'inégalité suivante pour tout corps abélien K :

$$po_{ext}(K) \leq g_K.$$

Il est alors naturel de se demander si le corps de genre est encore une extension de Pólya dans le cas où K est galoisien, mais non abélien.

4.3 Corps de Pólya, extensions de Pólya et ramification

Une autre question naturelle se pose :

Le corps de genre d'un corps de nombres abélien est-il un corps de Pólya ?

De façon plus générale :

Soit K un corps de nombres et soit L/K une extension de Pólya non ramifiée, L est-il un corps de Pólya ?

Proposition 4.13. *Soit K et L deux extensions galoisiennes de $\mathbb{Q}$ telles que $K \subset L$. Si L/K est une extension de Pólya non ramifiée aux places finies alors L est un corps de Polya.*

Preuve. Soit p un nombre premier. On pose $f = f_p(K/\mathbb{Q})$ et $F = f_p(L/K)$. L'extension L/K étant non ramifiée, on a

$$\Pi_{p^f}(K)\mathcal{O}_L = \Pi_{p^F}(L).$$

Cependant, l'extension L/K étant une extension de Pólya, $\Pi_{p^f}(K)\mathcal{O}_L$ est un idéal principal de L, il en de même pour $\Pi_{p^F}(L)$. □

Corollaire 4.14. *Le corps de genre (resp. au sens restreint) d'une extension abélienne de $\mathbb{Q}$ est un un corps de Pólya.*

Ainsi, pour toute extension abélienne K de $\mathbb{Q}$,

$$po_{corps}(K) \leq g_K.$$

Exemple 4.15. Dans le cas non galoisien, le corps de genre ne nous donne pas les résultats attendus. Considérons le corps cubique $\mathbb{Q}\left(\sqrt[3]{20}\right)$. Les tables de calculs nous donnent $h_K = 3$. Rappelons :

Proposition 4.16. [21, §4.2.6] *Soit*

$$L := \mathbb{Q}\left(\sqrt[3]{3^{n_0} p_1^{n_1} \cdots p_t^{n_t}}\right),$$

où $t \geq 0$, $n_0 \in \{0, 1\}$, $n_i \in \{1, 2\}$ pour $1 \leq i \leq t$, où les p_i sont des nombres premiers distincts différents de 3. Le corps de genre au sens restreint Γ_L' de L a pour degré sur L

$$\left[\Gamma_L' : L\right] = 3^{\gamma}$$

où γ est le nombre de p_i congrus à 1 modulo 3.

Dans le cas qui nous intéresse, $20 = 2^2.5$. Ainsi, $p_1 = 2$ et $p_2 = 5$. Aucun des p_i n'est congru à 1 modulo 3. On en déduit que $\left[\Gamma_K' : K\right] = 1$, donc $\Gamma_K' = K$. A fortiori, le corps de genre au sens large de K est K lui même.

Montrons que K n'est pas un corps de Pólya.

Il s'avère que 2 est ramifié dans l'extension $K/\mathbb{Q}$ car il divise le discrimant $D_K = -27.20^2$ de K. Si l'idéal premier $\mathfrak{P}$ au-dessus de 2 était principal, il existerait un élément $\alpha \in \mathcal{O}_K$ de norme 2. Or, la fonction "OrderNormEquation" du logiciel Kash nous indique qu'il n'existe aucun élément de $\mathcal{O}_K$ de norme égale à 2. De ce fait, K n'est pas un corps de Pólya. Comme $h_K = 3$, $Po(K) = Cl(K)$. Ainsi :

Proposition 4.17. *Dans le cas où le corps de nombres K n'est pas galoisien, le corps de genre (resp. au sens restreint) n'est pas nécessairement un corps de Pólya, ni une extension de Pólya de K.*

Exemple 4.18. Considérons le corps sextique $K = \mathbb{Q}\left(\sqrt[3]{20}, j\right)$ galoisien mais non abélien. Montrons que le corps de genre au sens restreint de K est le corps K lui-même. Rappelons :

Proposition 4.19. [26, Chap IV, Prop. 2] *Si K est le compositum de deux sous-corps K_1 et K_2 tels que $([K_1 : \mathbb{Q}], [K_2 : \mathbb{Q}]) = 1$ alors $\Gamma_K' = \Gamma_{K_1}' \Gamma_{K_2}'$.*

En posant $K_1 = \mathbb{Q}[j]$, vu le degré du corps de genre au sens restreint d'un corps quadratique (cf. proposition 4.5), $\Gamma'_{K_1} = K_1$. En posant, $K_2 = \mathbb{Q}\left(\sqrt[3]{20}\right)$, on vient de montrer que $\Gamma'_{K_2} = K_2$. Ainsi Le corps de genre de $K = \mathbb{Q}\left(\sqrt[3]{20}, j\right)$ est K lui même. D'après la proposition 3.7, comme il n'existe aucun entier de norme 2 dans $K = \mathbb{Q}\left(\sqrt[3]{20}\right)$, $\mathbb{Q}\left(\sqrt[3]{20}, j\right)$ n'est pas un corps de Pólya.

Proposition 4.20. *Dans le cas où le corps de nombres K est galoisien mais non abélien, le corps de genre Γ_K n'est pas nécessairement un corps de Pólya ni une extension de Pólya de K.*

La preuve de la proposition 4.13 peut être adaptée sous des hypothèses plus faibles et permet d'obtenir le résultat suivant :

Théorème 4.21. *Soit K un corps de nombres quelconque, le corps de classes de Hilbert H_K de K est un corps de Pólya.*

Preuve. Soit q une puissance d'un nombre premier p. Par définition,

$$\Pi_q\left(H_K\right) = \prod_{\substack{\mathfrak{m}\in Max\left(\mathcal{O}_{H_K}\right)\\ N(\mathfrak{m})=q}} \mathfrak{m}.$$

Posons $\mathfrak{p}_i = \mathfrak{m}_i \cap K$. Soient $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_s}$ les traces des $\mathfrak{m}_i$ toutes distinctes entre elles. Ainsi, pour tout $j \in \{1, \ldots, s\}$,

$$\mathfrak{p}_{i_j}\mathcal{O}_{H_K} = \prod_{\mathfrak{m}\cap K=\mathfrak{p}_{i_j}} \mathfrak{m}$$

car l'extension H_K/K n'est pas ramifiée. On obtient

$$\prod_{j=1}^{s} \mathfrak{p}_{i_j}\mathcal{O}_{H_K} = \prod_{\substack{\mathfrak{m}\in Max\left(\mathcal{O}_{H_K}\right)\\ N(\mathfrak{m})=q}} \mathfrak{m} = \Pi_q\left(H_K\right).$$

Comme $\prod_{j=1}^{s} \mathfrak{p}_{i_j}$ est un idéal de $\mathcal{O}_K$ et que les idéaux de $\mathcal{O}_K$ capitulent dans H_K, $\prod_{j=1}^{s} \mathfrak{p}_{i_j}\mathcal{O}_{H_K}$ est principal donc $\Pi_q\left(H_K\right)$ également. □

La question du problème d'inclusion d'un corps de nombres dans un corps de Pólya possède donc une réponse positive.

Proposition 4.22. *Tout corps de nombres K peut être plongé dans un corps de Pólya, à savoir son corps de classes de Hilbert H_K.*

4.4 A propos de la finitude d'une tour d'extensions de Pólya

Une réponse positive au problème de plongement classique d'un corps de nombres K dans un corps de nombres L tel que $h_L = 1$ est équivalent à la finitude de la tour de corps de classes de Hilbert de K [35]. Dans le paragraphe précédent, nous avons donné une réponse positive au problème de plongement d'un corps K dans un corps de Pólya (cf. Thm 4.21). Ayant défini la notion d'extension de Pólya par analogie avec la propriété remarquable du corps de classes de Hilbert d'un corps de nombres, à savoir la capitulation, il est alors naturel de se poser la question suivante :

Est-ce que, pour tout corps de nombres, une tour d'extensions de Pólya telle que chacune de ses extensions ne soit pas un corps de Pólya est nécessairement finie ?

Toutefois, paradoxalement au problème de plongement classique, nous allons construire une tour infinie d'extensions de Pólya d'un corps de nombres dans laquelle ces extensions ne sont pas des corps de Pólya. Pour cela montrons tout d'abord :

Proposition 4.23. *Pour tout nombre premier $p > 2$, il existe un corps K cyclique de degré p^α (où $\alpha \geq 1$) qui n'est pas un corps de Pólya.*

Preuve. Soit p un nombre premier impair. Le théorème de Dirichlet nous garantit l'existence de 2 nombres premiers distincts q_1 et q_2 tels que $q_i \equiv 1 \pmod{p}$. Soit $n = q_1 q_2$ et ζ_n une racine primitive n-ième de l'unité. On a les égalités suivantes :

$$[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n) = (q_1 - 1)(q_2 - 1) = p^\alpha m \text{ où } (p, m) = 1 \text{ et } \alpha \geq 2.$$

Il existe un unique sous-corps K de $\mathbb{Q}[\zeta_n]$ cyclique de degré p^α sur $\mathbb{Q}$. Montrons que q_1 et q_2 sont ramifiés dans $K/\mathbb{Q}$. On a :

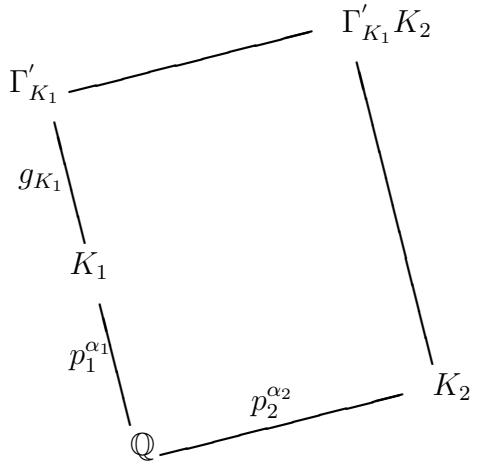
$$e_{q_i}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) = q_i - 1 = e_{q_i}(\mathbb{Q}[\zeta_n]/K) e_{q_i}(K/\mathbb{Q}).$$

On sait que $e_{q_i}(\mathbb{Q}[\zeta_n]/K) \mid m$, mais comme $p \mid q_i - 1$ et $(p, m) = 1$, on obtient $p \mid e_{q_i}(K)/\mathbb{Q})$.
Le corollaire 2.41 affirme que si $K/\mathbb{Q}$ est une extension cyclique de degré premier $p > 2$, le corps K est de Pólya si et seulement s'il y a exactement un nombre premier ramifié dans $K/\mathbb{Q}$. Or, le corps K ainsi construit possède deux premiers ramifiés. □

Remarque 4.24. Remarquons que selon le thèorème 4.8 de Furuya, si K est une extension cyclique degré p^α où $\alpha \geq 1$, alors $g'_K = \left[\Gamma'_K : K\right]$ est nécessairement de la forme p^β où $\beta \geq 0$ puisque compositum d'extensions cycliques de $\mathbb{Q}$ de degré une puissance de p. De plus, si K n'est pas de Pólya, alors $g'_K = p^\beta$ où $\beta \geq 1$.

Proposition 4.25. *Il existe une tour de corps de nombres $\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n \subset \ldots$ infinie telle que pour tout entier $i \geq 0$, L_{i+1}/L_i est une extension de Pólya et L_i n'est jamais un corps de Pólya.*

Preuve. La proposition 4.23 nous garantit, pour tout nombre premier $p_i > 2$, $(i > 0)$, l'existence d'un corps cyclique K_i de degré $p_i^{\alpha_i}$ qui n'est pas un corps de Pólya. Pour tout $i > 0$, soit Γ'_{K_i} le corps de genre au sens restreint de K_i. La remarque 4.24 nous donne $[\Gamma'_{K_i} : \mathbb{Q}] = p_i^{\beta_i}$ où $\beta_i > 0$. Soit $p_1 \in \mathbb{P}$, $p \neq 2$, et K_1 un corps cyclique de degré $p_1^{\alpha_1}$ qui n'est pas de Pólya. Soit p_2 un premier impair tel que $p_2 \neq p_1$ et K_2 un corps cyclique de degré $p_2^{\alpha_2}$ qui n'est pas de Pólya. Nous sommes dans la situation suivante :



Les extensions $\Gamma'_{K_1}/\mathbb{Q}$ et $K_2/\mathbb{Q}$ sont galoisiennes et leurs degrés sont premiers entre eux. L'extension $\Gamma'_{K_1}K_2/\mathbb{Q}$ est galoisienne et, d'après la proposition 2.26, le morphisme $\epsilon_{K_2}^{\Gamma'_{K_1}K_2}$ est injectif. Le corps K_2 n'étant pas de Pólya, $\Gamma'_{K_1}K_2$ ne l'est pas non plus. Montrons que $\Gamma'_{K_1}K_2/K_2$ est une extension de Pólya. D'après le corollaire 4.14, Γ'_{K_1} est un corps de Pólya. De plus les extensions $\Gamma'_{K_1}/\mathbb{Q}$ et $K_1/\mathbb{Q}$ sont galoisiennes, le corollaire 2.11 affirme que Γ'_{K_1}/K_1 est une extension de Pólya. A fortiori, $\Gamma'_{K_1}K_2/K_1$ est également une extension de Pólya. En posant $L_1 = K_1$, $L_2 = \Gamma'_{K_1}K_2$, nous construisons les

deux premières extensions de notre tour. On construit ensuite cette tour de la manière suivante :

$$\begin{array}{c} \Gamma'_{K_1}\Gamma'_{K_2}K_3 \\ | \\ \Gamma'_{K_1}\Gamma'_{K_2} \\ | \\ \Gamma'_{K_1}K_2 \\ | \\ \mathbb{Q} \end{array}$$

Soit $p_3 \in \mathbb{P}$, $p_3 \neq p_1, p_2$ et K_3 un corps cyclique de degré $p_3^{\alpha_3}$ qui n'est pas de Pólya. D'après le théorème 2.23, comme Γ'_{K_1} et Γ'_{K_2} sont des corps de Pólya galoisiens, $\Gamma'_{K_1}\Gamma'_{K_2}$ est un corps de Pólya galoisien. Les extensions $\Gamma'_{K_1}\Gamma'_{K_2}/\mathbb{Q}$ et $K_3/\mathbb{Q}$ sont galoisiennes et leur degré sont premiers entre eux. L'extension $\Gamma'_{K_1}\Gamma'_{K_2}K_3/\mathbb{Q}$ est galoisienne et d'après la proposition 2.26 le morphisme $\epsilon_{K_3}^{\Gamma'_{K_1}\Gamma'_{K_2}K_3}$ est injectif. Le corps K_3 n'étant pas de Pólya, $\Gamma'_{K_1}\Gamma'_{K_2}K_3$ ne l'est pas non plus. Les extensions $\Gamma'_{K_1}\Gamma'_{K_2}/\mathbb{Q}$ et $\Gamma'_{K_1}K_2/\mathbb{Q}$ sont galoisiennes, le corollaire 2.11 affirme que $\Gamma'_{K_1}\Gamma'_{K_2}/\Gamma'_{K_1}K_2$ est une extension de Pólya. Par conséquent, $\Gamma'_{K_1}\Gamma'_{K_2}K_3/\Gamma'_{K_1}K_2$ est également une extension de Pólya. On pose alors $L_3 = \Gamma'_{K_1}\Gamma'_{K_2}K_3$ et on poursuit la construction de sorte que pour $i > 1$, $L_i = \Gamma'_{K_1} \ldots \Gamma'_{K_{i-1}}K_i$. □

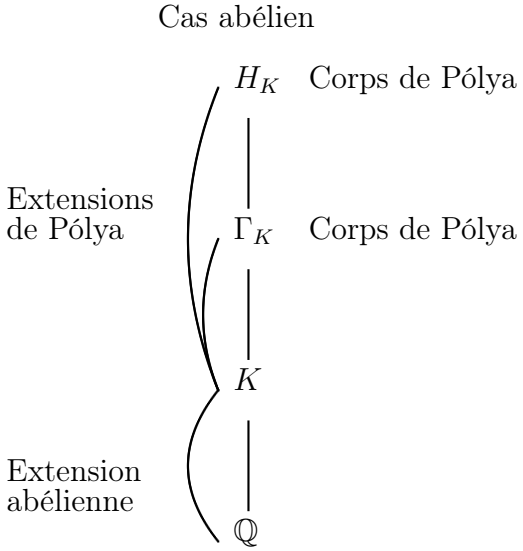
4.5 Questions de minimalités et d'unicité

Lorsqu'un corps K n'est pas un corps de Pólya, on essaie de le plonger dans un corps qui lui est de Pólya, ou dans un corps qui est une extension de Pólya de K. Il existe des corps pour lesquels on obtient une extension de Pólya minimale explicite comme le montre le corollaire 1.65. Dans les autres cas, on cherchera à majorer, le degré d'un corps de Pólya minimal au dessus de K (resp. d'une extension de Pólya minimale de K).

4.5.1 Etat des lieux

Dans les paragraphes précédents nous avons vu qu'il existait toujours, pour tout corps de nombres K, un corps de Pólya qui le contient à savoir son corps de classe de Hilbert H_K, qu'il soit au sens large ou au sens restreint. Le théorème de capitulation nous indique que H_K est également une extension de Pólya de K. Dans le cas où K est une extension abélienne de $\mathbb{Q}$, le corps de genre de K (au sens large ou au sens restreint) était à la fois une extension

de Pólya de K et un corps de Pólya. Nous sommes donc dans la situation suivante :



On peut se poser les questions suivantes :

1. *Le corps de genre est-il une extension de Pólya minimale de K (resp. un corps de Pólya minimal au dessus de K) d'un corps de nombres abélien ?*
2. *Sinon, y a-t-il une extension de Pólya minimale contenue dans H_K, dans Γ_K ?*
3. *Quel lien existe-t-il entre le nombre de premiers ramifiés dans l'extension $K/\mathbb{Q}$ et le degré d'une extension minimale de Pólya de K(resp. d'un corps de Pólya minimal au dessus de K) ?*

La construction d'une tour d'extensions de Pólya infinie met en évidence le fait qu'il existe plusieurs extensions de Pólya ramifiées pour un corps de nombres.

4. *Y a t-il unicité d'une extension de Pólya minimale de K (resp. d'un corps de Pólya minimal au-dessus de K) non ramifiée ?*

4.5.2 Majoration de $po_{corps}(K)$ dans le cas abélien

Supposons tout d'abord que K soit corps de nombres abélien. Comme nous l'avons déjà évoqué au §1.4.1, d'après le théorème de Kronecker Weber,

K est contenu dans un corps cyclotomique $\mathbb{Q}[\zeta_f]$ où f est le conducteur de K. On obtient une première majoration :

$$po_{corps}(K) \leq \frac{\varphi(f)}{[K:\mathbb{Q}]} \text{ et}$$

$$po_{corps}(K) \leq \frac{\varphi(f)}{2[K:\mathbb{Q}]} \text{ si } K \text{ est réel.}$$

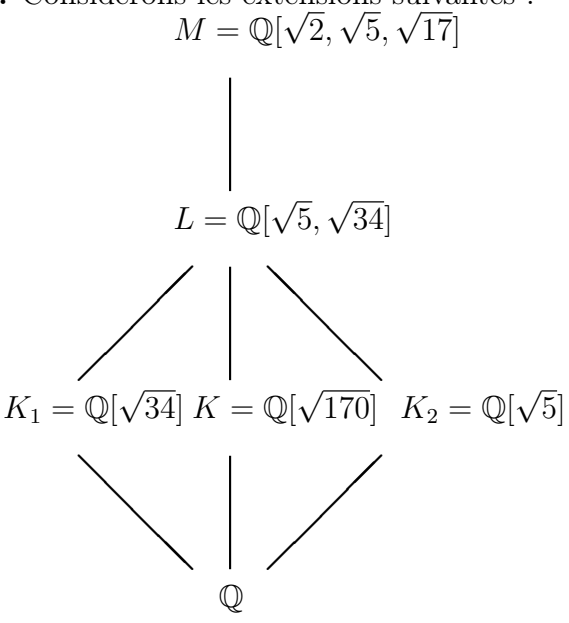
où φ désigne l'indicatrice d'Euler. Par exemple, le conducteur d'un corps quadratique est la valeur absolue de son discriminant.

Le corps de genre de K étant un corps de Pólya on peut alors majorer $po_{corps}(K)$ par le nombre de genre g_K de K qui est le degré de $[\Gamma_K : K]$:

$$po_{corps}(K) \leq g_K.$$

Toutefois, l'exemple suivant montre que le corps de genre n'est pas un corps de Pólya minimal au-dessus d'un corps K abélien.

Exemple 4.26. Considérons les extensions suivantes :



D'après la proposition 4.5, le corps de genre au sens restreint de $K = \mathbb{Q}[\sqrt{170}]$ est $\Gamma'_K = M$ et dans ce cas précis, d'après cette même proposition, le corps de genre au sens large est le même que le corps de genre au sens restreint. En se référant à la classification des corps quadratiques de Pólya (proposition 1.38), les corps K_1 et K_2 sont tous deux des corps de Pólya. Par ailleurs,

le premier 2 n'étant pas ramifié dans $K_2/\mathbb{Q}$, la proposition 3.25 affirme que $K_1K_2 = L$ est un corps de Pólya. Le corps de genre de K n'est donc pas un corps de Pólya minimal au-dessus de K.

On peut également se demander si le corps de genre de K est une extension de Pólya minimale de K. Comme L est un corps de Pólya, et que les extensions $L/\mathbb{Q}$ et $K/\mathbb{Q}$ sont des extensions galoisiennes, d'après la proposition 2.11, l'extension L/K est bien une extension de Pólya. Le corps de genre de K n'est pas non plus une extension de Pólya minimale de K. Ainsi,

Proposition 4.27. *Le corps de genre Γ_K d'une extension abélienne K de $\mathbb{Q}$ n'est pas toujours un corps de Pólya minimal au-dessus de K, ni une extension de Pólya minimale de K.*

En fait, comme le montre la proposition suivante, le corps de genre d'un corps K est en fait assez loin, en fonction du nombre de premiers ramifiés dans $K/\mathbb{Q}$, d'être un corps de Pólya minimal au-dessus de K.

Proposition 4.28. *Soit $K = \mathbb{Q}[\sqrt{d}]$ ($d \in \mathbb{Z}$ sans facteurs carrés) un corps quadratique. Soit σ (resp. τ) le nombre de diviseurs premiers impairs de d congrus à 3 (mod 4) (resp. 1 (mod 4)). On a les majorations :*

1. *Si $d \equiv 1 \pmod 4$, $po_{corps}(K) \leq 2^{\frac{\sigma}{2}+\tau-1}$ si $d > 0$ et $2^{\frac{\sigma-1}{2}+\tau}$ si $d < 0$.*
2. *Si $d \equiv 3 \pmod 4$, $po_{corps}(K) \leq 2^{\frac{\sigma-1}{2}+\tau}$ si $d > 0$ et $2^{\frac{\sigma}{2}+\tau}$ si $d < 0$.*
3. *Si $d \equiv 2 \pmod 8$, $po_{corps}(K) \leq 2^{\frac{\sigma}{2}+\tau}$ si $d > 0$ et $2^{\frac{\sigma-1}{2}+\tau+1}$ si $d < 0$.*
4. *Si $d \equiv 6 \pmod 8$, $po_{corps}(K) \leq 2^{\frac{\sigma-1}{2}+\tau}$ si $d > 0$ et $2^{\frac{\sigma}{2}+\tau}$ si $d < 0$.*

Preuve. Posons $d = (-1)^e 2^\gamma p_1 \dots p_\sigma q_1 \dots q_\tau$ où $p_i \equiv 3 \pmod 4$ et $q_j \equiv 1 \pmod 4$, $e = 0$ ou 1, $\gamma = 0$ ou 1. Rappelons que les corps quadratiques $\mathbb{Q}[\sqrt{\delta}]$ suivants sont des corps de Pólya : $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{-2}]$, et pour p et q premiers impairs distincts $\mathbb{Q}[\sqrt{p}]$, $\mathbb{Q}[\sqrt{-p}]$ lorsque $p \equiv 3 \pmod 4$, $\mathbb{Q}[\sqrt{2p}]$ lorsque $p \equiv 3 \pmod 4$ et $\mathbb{Q}[\sqrt{pq}]$ lorsque p et $q \equiv 3 \pmod 4$. Dans chaque cas, les premiers ramifiés dans $\mathbb{Q}[\sqrt{\delta}]/\mathbb{Q}$ sont les diviseurs premiers de δ sauf pour $\mathbb{Q}[i]$ où 2 est ramifié. Suivant les congruences de d modulo 8, nous allons composer ces corps quadratiques de Pólya en respectant les hypothèses de la proposition 2.23 pour obtenir un corps de Pólya contenant K de degré sur K le petit possible.

Commençons par les cas où σ est pair. Si $d > 0$ et impair, $d \equiv 1 \pmod 4$. En appliquant la proposition 2.23, on obtient que $\mathbb{Q}[\sqrt{p_1p_2}, \dots, \sqrt{p_{\sigma-1}p_\sigma}]$ est un corps de Pólya où seuls les p_i sont ramifiés. De plus, les corps du type $\mathbb{Q}\left(\sqrt{q_j}\right)$ étant des corps de Pólya où seuls les q_j sont ramifiés, en appliquant de nouveau la proposition 2.23, on montre que le corps $\mathbb{Q}[\sqrt{q_1}, \dots, \sqrt{q_\tau}]$ est

un corps de Pólya. En appliquant une dernière fois cette proposition, on voit que le corps

$$L = \mathbb{Q}[\sqrt{q_1}, \ldots, \sqrt{q_\tau}, \sqrt{p_1 p_2}, \ldots, \sqrt{p_{\sigma-1} p_\sigma}]$$

est un corps de Pólya de degré $\sigma/2 + \tau$ sur $\mathbb{Q}$ contenant K. Donc

$$po_{corps}(K) \leq 2^{\frac{\sigma}{2}+\tau-1}.$$

Supposons $d < 0$ et impair. Dans ce cas, $d \equiv 3 \pmod 4$. Pour obtenir un corps de Pólya contenant K, il suffit d'adjoindre i au corps L obtenu dans le cas $d > 0$, c'est un corps de degré $\sigma/2 + \tau + 1$ sur $\mathbb{Q}$. D'où

$$po_{corps}(K) \leq 2^{\frac{\sigma}{2}+\tau}.$$

Supposons d pair et $d > 0$ (resp. $d < 0$). Dans ce cas, $d \equiv 2 \pmod 8$ (resp. $d \equiv 6 \pmod 8$), le corps $L(\sqrt{2})$ (resp. $L(\sqrt{-2})$) est un corps de Pólya contenant K. D'où, encore :

$$po_{corps}(K) \leq 2^{\frac{\sigma}{2}+\tau}.$$

Continuons avec le cas où σ est impair. Si $d > 0$ et impair, $d \equiv 3 \pmod 4$. Le corps M suivant est un corps de Pólya contenant K :

$$M = \mathbb{Q}\left(\sqrt{p_1 p_2}, \ldots, \sqrt{p_{\sigma-2} p_{\sigma-1}}, \sqrt{p_\sigma}, \sqrt{q_1}, \ldots, \sqrt{q_\tau}\right).$$

Si $d < 0$ et impair, $d \equiv 1 \pmod 4$. En substituant $\sqrt{-p_\sigma}$ à $\sqrt{p_\sigma}$ dans M, on obtient de nouveau un corps de Pólya contenant K. Enfin si $d > 0$ (resp. $d < 0$) et pair, en substituant $\sqrt{2p_\sigma}$ à $\sqrt{p_\sigma}$ dans M, le corps M ainsi construit (resp. $M(\sqrt{-2})$) est un corps de Pólya contenant K. □

Corollaire 4.29. *Si σ désigne le nombre de premiers $p \equiv 3 \pmod 4$ ramifiés dans le corps quadratique K, on a la minoration :*

$$\frac{g_K}{po_{corps}(K)} \geq 2^{\frac{\sigma}{2}-2} \text{ si } d \text{ est pair,}$$

$$\frac{g_K}{po_{corps}(K)} \geq 2^{\frac{\sigma+1}{2}-2} \text{ si } d \text{ est impair .}$$

Dès que $\sigma \geq 4$, Γ_K n'est pas un corps de Pólya minimal au dessus de K.

Preuve. D'après la proposition 4.5, $g_K = [\Gamma_K : K] \geq \frac{g'_K}{2} = \frac{[\Gamma'_K : K]}{2}$. En effet, si l'on écrit $\Gamma'_K = \mathbb{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_v}, \sqrt{-q_1}, \ldots, \sqrt{-q_w}\right)$ alors $L = \Gamma'_K \cap \mathbb{R} = \mathbb{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_v}, \sqrt{q_1 q_2}, \sqrt{q_1 q_3}, \ldots, \sqrt{q_1 q_w}\right)$ et $\Gamma'_K = L(\sqrt{-q_1})$. D'où $g_K \geq$

$2^{\sigma+\tau-2}$ si d est impair et $\geq 2^{\sigma+\tau-1}$ si d est pair. Par ailleurs, la proposition précédente montre que $po_{corps}(K) \leq 2^{\frac{\sigma}{2}+\tau}$ si d est impair et $\leq 2^{\frac{\sigma-1}{2}+\tau+1}$. Donc si d est pair,

$$\frac{g_K}{po_{corps}(K)} \geq 2^{\frac{\sigma}{2}-2}$$

et si d est impair,

$$\frac{g_K}{po_{corps}(K)} \geq 2^{\frac{\sigma+1}{2}-2}.$$

Le membre de droite est > 1 dès que $\sigma \geq 4$.

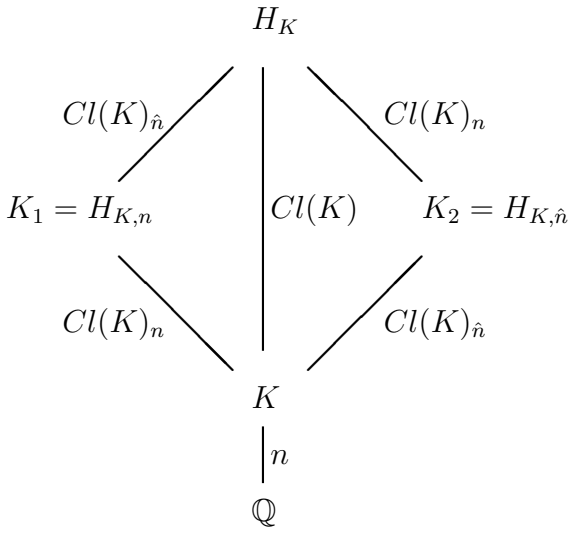
□

4.5.3 Majoration de $po_{corps}(K)$ dans le cas galoisien

L'exemple 4.18 nous fournit un corps K extension galoisienne de $\mathbb{Q}$ non abélien dont le corps de genre n'est pas un corps de Pólya. La majoration du paragraphe précédent n'est donc plus valable. Dans le cas d'un corps de nombres quelconque, on ne peut, à priori, majorer $po_{corps}(K)$ que par h_K (cf proposition 4.21). Toutefois, si K est une extension galoisienne (non nécessairement abélienne), on dispose tout de même d'une majoration plus fine que celle donnée par h_K.

Proposition 4.30. *Soit K une extension galoisienne de $\mathbb{Q}$. Soit $n = [K : \mathbb{Q}]$ et soit $H_{K,n}$ le sous-corps de H_K laissé fixe sous l'action des éléments de $Gal(H_K/K) \simeq Cl(K)$ dont l'ordre est premier à n. Le corps $H_{K,n}$ est un corps de Pólya.*

Preuve. Comme dans la proposition 2.30, on note $Cl(K)_n$ (resp. $Cl(K)_{\hat{n}}$) le sous-groupe de $Cl(K)$ formé des éléments dont l'ordre divise une puisance de n (resp. dont l'ordre est premier avec n). Ainsi, en faisant l'abus de notation d'identification de $Gal(H_K/K)$ avec $Cl(K)$, $H_{K,n} = H_K^{Cl(K)_{\hat{n}}}$ (resp. $H_{K,\hat{n}} = H_K^{Cl(K)_n}$) est le sous-corps de H_K laissé fixe par $Cl(K)_{\hat{n}}$ (resp. $Cl(K)_n$).



L'extension $H_K/\mathbb{Q}$ est une extension galoisienne. En effet, soit σ un morphisme de H_K sur un corps L. L'extension $\sigma(H_K)/\sigma(K)$ est abélienne et non ramifiée. Comme $K/\mathbb{Q}$ est galoisienne, $\sigma(K) = K$. L'extension $\sigma(H_K)/K$ est abélienne et non-ramifiée, par maximalité de H_K, $\sigma(H_K) \subset H_K$. De même les extensions $H_{K,n}/\mathbb{Q}$ et $H_{K,\hat{n}}/\mathbb{Q}$ sont galoisiennes. D'après la proposition 2.30, $Po(H_{K,n})$ s'injecte dans $Po(H_K)$. Or, H_K étant un corps de Pólya, $Po(H_K)$ est trivial. Ainsi, $H_{K,n}$ est un corps de Pólya.

□

Corollaire 4.31. *Soit $K/\mathbb{Q}$ une extension galoisienne de degré n, on a la majoration :*

$$po_{corps}(K) \leq |Cl(K)_n| = \prod_{p|n} p^{v_p(h_K)}.$$

Compte tenu de la proposition 1.50, on a aussi

$$po_{ext}(K) \leq \prod_{p|n} p^{v_p(h_K)}.$$

4.5.4 Non-unicité d'une extension de Pólya minimale non ramifiée

Considérons l'extension $\mathbb{Q}\left(\sqrt{-15}\right) \subset \mathbb{Q}\left(\sqrt{-5}, \sqrt{3}\right)$. C'est une extension de Pólya minimale où le nombre 2 est ramifié. Cependant le corps de genre de $\mathbb{Q}\left(\sqrt{-15}\right)$ est $\mathbb{Q}\left(\sqrt{5}, \sqrt{-3}\right)$: l'extension $\mathbb{Q}\left(\sqrt{-15}\right) \subset \mathbb{Q}\left(\sqrt{5}, \sqrt{-3}\right)$ est non ramifiée et il s'agit d'une extension de Pólya minimale. Nous sommes en présence de deux extensions de Pólya minimales, l'une ramifiée et l'autre

non. Toutefois, on peut se demander s'il y a unicité pour les extensions de Pólya non ramifiées minimales.

Dans cette section, nous allons prouver qu'il peut exister, dans le cas d'un corps de nombres K abélien, plusieurs extensions de Pólya de K minimales non ramifiées et de même degré. Pour cela nous faisons appel à un résultat d'A. Azizi et M. Talbi [2].

Notations. Soit $k = \mathbb{Q}[\sqrt{l}]$ où l est un nombre premier tel que $l = 2$ ou $l \equiv 5 \pmod 8$. Soit p un nombre premier tel que $p \equiv 1 \pmod 4$ et $\left(\frac{p}{l}\right)_4 = -1$ ou $\left(\frac{\cdot}{\cdot}\right)_4$ désigne le symbole biquadratique. Désignons par ϵ l'unité fondamentale de k. On considère le corps quartique cyclique $K = k\left(\sqrt{-p\epsilon\sqrt{l}}\right)$.

L'extension $K/\mathbb{Q}$ étant galoisienne de degré 4, d'après la proposition 2.6, $Po(K) \subseteq Cl_2(K)$ où $Cl_2(K)$ désigne le 2-groupe de classes de K. Or, à propos de $Cl_2(K)$, on a le résultat suivant de Brown et Parry (cf. [7] pour $l \equiv 3 \pmod 8$ et [8] pour $l = 2$) :

Proposition 4.32. *Avec les hypothèses précédentes, si $H_K^{(2)}$ désigne le 2-corps de classes de Hilbert de K, on a :*

$$Gal\left(H_K^{(2)}/K\right) \simeq Cl_2(K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Précisons ces éléments de $Cl_2(K)$. Comme $\left(\frac{p}{l}\right) = 1$, il existe deux idéaux $\mathfrak{p}_1$ et $\mathfrak{p}_2$ de k tels que

$$p\mathcal{O}_k = \mathfrak{p}_1\mathfrak{p}_2$$

et donc deux idéaux premiers $\mathfrak{m}_1$ et $\mathfrak{m}_2$ de K tels que

$$\mathfrak{p}_i\mathcal{O}_K = \mathfrak{m}_i^2 \ (i = 1, 2).$$

Par suite, $Po(K)$ est le sous groupe d'ordre 2 engendré par la classe de $\Pi_2(K) = \mathfrak{m}_1\mathfrak{m}_2$. Les deux autres éléments non triviaux de $Cl_2(K)$ étant les classes de $\mathfrak{m}_1$ et de $\mathfrak{m}_2$.

La proposition 4.32 montre qu'il existe 3 corps F_1, F_2, F_3 intermédiaires entre K et $H_K^{(2)}$. A. Azizi et M. Talbi étudient la capitulation des 2-classes d'idéaux dans les corps F_i. A cet effet, ils ontroduisent les élements π_1 et π_2 de k conjugués sur $\mathbb{Q}$ tels que :

$$\mathfrak{p}_i^{h_k} = \pi_i\mathcal{O}_k \ (i = 1, 2)$$

où h_k désigne le nombres de classes de k. Ils montrent alors :

Proposition 4.33. [2] *Soient* $K = k\left(\sqrt{-p\epsilon\sqrt{l}}\right)$ *où* l *est un nombre premier tel que* $l = 2$ *ou* $l \equiv 5 \mod 8$, ϵ *l'unité fondamentale de* $k = \mathbb{Q}[\sqrt{l}]$, p *un nombre premier tel que* $p \equiv 1 \mod 4$ *et* $\left(\frac{p}{l}\right)_4 = -1$. *Soient* π_1 *et* π_2 *définis comme ci-dessus, alors* $H_K^{(2)}$ *possède 3 sous-corps quadratiques* F_1, F_2, F_3 *sur* K *tels que :*

1. *Si* $\left(\frac{l}{p}\right)_4 = 1$ *alors* $F_1 = K(\sqrt{-\pi_1})$, $F_2 = K(\sqrt{-\pi_2})$ *et* $F_3 = K(\sqrt{p}) = \Gamma_K$. *Les quatres classes de* $Cl_2(K)$ *capitulent dans chacune des extensions* F_i *pour* $i \in 1, 2, 3$
2. *Si* $\left(\frac{l}{p}\right)_4 = -1$ *alors* $F_1 = K(\sqrt{\pi_1})$, $F_2 = K(\sqrt{\pi_2})$ *et* $F_3 = K(\sqrt{p}) = \Gamma_K$. *Dans chacune des extensions* F_i, $i \in 1, 2, 3$, *il existe exactement deux classes de* $Cl_2(K)$ *qui capitulent.*

Ainsi dans le 2ème cas de la proposition 4.33, seule l'extension $F_3 = \Gamma_K$ est de Pólya, en revanche :

Proposition 4.34. *Soit* K *un corps quartique cyclique vérifiant les hypothèses de la proposition 4.33. Si de plus* $\left(\frac{l}{p}\right)_4 = 1$, *alors les 3 extensions quadratiques de* K *contenues dans le 2-corps de classes de Hilbert* $H_K^{(2)}$ *de* K *sont des extensions de Pólya minimales, et aussi des corps de Pólya minimaux au-dessus de* K.

La dernière partie de la proposition résulte de ce que K n'est pas un corps de Pólya et que les 3 extensions en question sont non ramifiées (cf. proposition 4.13). Reprenons un contre-exemple donné dans [2] :

Exemple 4.35. On considère le corps $K = \mathbb{Q}\left(\sqrt{-89(2+\sqrt{2})}\right)$. D'après la proposition 3.19, le corps K est un corps quartique cyclique qui n'est pas un corps de Pólya. Il s'avère que $89 \equiv 9 \mod 16$ et que $\left(\frac{2}{89}\right)_4 = 1$. Ainsi $F_1 = K\left(\sqrt{-(11+4\sqrt{2})}\right)$, $F_2 = K\left(\sqrt{-(11-4\sqrt{2})}\right)$ et $F_3 = K\left(\sqrt{89}\right)$. D'après la proposition précédente, chacune des extensions F_i est une extension de Pólya de K quadratique, donc minimale. Comme K n'est pas un corps de Pólya, les extension F_i/K étant des extensions de Pólya galoisiennes non ramifiées, d'après la proposition 4.13, les corps F_i sont également des corps de Pólya.

Ainsi à la question :

Deux extensions de Pólya minimales contenue dans $H(K)$ sont-elles isomorphes ?

posée à la fin du premier chapitre, nous pouvons apporter la réponse suivante :

Proposition 4.36. *Soit K un corps de nombres. Deux extensions de Pólya de K minimales (resp. deux corps de Pólya minimaux au-dessus de K) contenues dans H_K ne sont pas isomorphes en général.*

Index des notations

Bibliographie

[1] A. Azizi, A. Mouhib, Sur le rang du 2-groupe de classes de $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ où $m = 2$ ou un premier $p \equiv 1 \pmod 4$, *Transactions of the A.M.S.*, **353** (2001), 2741-2752.

[2] A. Azizi, M. Talbi, Capitulation dans certaines extensions non ramifiées de corps quartiques cycliques, *Arch. Mat.* **44** (2008), 271-284.

[3] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490** (1997), 101-127.

[4] M. Bhargava, Generalized factorials and fixed divisors over subsets of a Dedekind domain, *J. Number Theory* **72** (1998), 67-75.

[5] H. Bass, Big projective modules are free, *Illinois J. Math.* **7** (1963), 24-31.

[6] N. Bourbaki, *Algèbre*, Chapitre V, Masson, Paris, 1981.

[7] E. Brown, C.J. Parry, The 2-class group of certain biquadratic number fields I, *J. reine angew. Math.* **295** (1977), 61-71.

[8] E. Brown, C.J. Parry, The 2-class group of certain biquadratic number fields II, *Pacific J. Math.* **78** (1978), 11-26.

[9] A. Brumer et M. Rosen, Class number and ramification in number fields, *Nagoya Math. J.* **23** (1963), 97-101.

[10] P.J. Cahen, J.L. Chabert, *Integer-valued polynomials*, Mathematical Surveys and Monographs, vol **48**, Amer. Math. Soc., Providence (1997).

[11] J.L Chabert, Factorial Groups and Pólya groups in Galoisian Extension of $\mathbb{Q}$, *Lecture Notes in Pure and Applied Mathematics*, vol **231**, pp 77-86, Marcel Dekker, New-York, 2003

[12] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 2000.

[13] A. Frölich, The genus field and the genus group in finite number fields, *Mathematika* **6** (1959), 40-46.

[14] Ph. Furtwängler, Beweis des Hauptidealsatzes fur Klassenkörper algebraischer Zahlkörper, *Abh. Math. Sem. Hamburg* **7** (1930), 379-387.

[15] H. Furuya, Principal ideal theorem in the genus field for absolutely abelian extensions, *J. Number Theory* **9** (1977), 4-15.

[16] D. A. Garbanati, Units with norm -1 and signatures of units, *J. Reine Angew. Math.* **283/284** (1976), 164-175.

[17] R. Gilmer, *Multiplicative Ideal Theory*, Dekker, 1972.

[18] G. Gerboud, Bases of integer-valued polynomials, *Commutative ring theory* **149** (1991), 97-116.

[19] G. Gerboud, Polynômes à valeurs entières sur l'anneau des entiers de Gauss, *C.R. Acad. Sc. Paris, Sér A*, **307** (1988), 375-378.

[20] E. S. Golod, I.R. Shafarevich, On the class field tower, *Izv. Akad. Nauk* **28** (1964), 261-272.

[21] G. Gras, *Class Field Theory*, Springer, 2005.

[22] K. Hardy, R.H. Hudson, D. Richman, K.S. Williams and N.M. Holtz, Calculation of Class Numbers of Imaginary Cyclic Quartic Fields, *Carleton-Ottawa Mathematical Lecture Note Series* **7** (1986), 201 pp.

[23] H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlenkörpern, *J. Math. Soc. Japan* **3** (1951), 45-51.

[24] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, **4** (1894-95), 175-546.

[25] R.H Hudson and K.S Williams, The Integers of a Cyclic Quartic Field, *Rocky Mountain Journal of Mathematics* **20** (1990), 145-150.

[26] M. Ishida, *The Genus Fields of Algebraic Number Fields*, Springer, 1976.

[27] M. Ishida, On the genus field of an algebraic number field of odd prime degree, *J. Reine Angew. Math.* **268/269** (1974), 165-173.

[28] H. Koch, *Number Theory*, Graduate Studies in Mathematics, A.M.S. (2000).

[29] H. W. Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, *Math. Nachr.* **9** (1953), 350-362.

[30] Minkowski, Zur Theorie der quadratischen Formen, *J. Reine Angew. Math.* **101** (1887), 196-202.

[31] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[32] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpren, *J. reine angew. Math.* **149** (1919), 117-124.

[33] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. Reine Angew. Math.* **149** (1919), 97-116.

[34] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2000.

[35] P. Roquette, On class field towers, in Cassels and Fröhlich, *Algebraic number theory* (Proc. Instructional Conf., Brighton, 1965), Academic Press, London, and Thompson Book, Washington DC, (1967) 231-249.

[36] P. Samuel, *Théorie Algébrique des Nombres*, Hermann, 1970.

[37] J.P Serre, *Corps Locaux*, Hermann, Paris, 1962.

[38] B.K. Spearman, K.S. Williams, The conductor of a cyclic quartic field using Gauss sums, *Czech. Math. J.* **47** (1997), 453-462.

[39] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, 1993.

[40] C. Thiebaud, Sur la capitulation dans les corps de genres d'une extension abélienne d'un corps quadratique imaginaire, *J. Number Theory* **85** (2000), 92-107.

[41] K.S. Williams, Integers of biquadratic fields, *Canad. Math. Bull.* **13** (1970), 519-526.

[42] H. Zantema, Integer valued polynomials over a number field, *Manusc. Math.* **40** (1982), 155-203.