Le théorème de Kronecker-Weber

Pascal Molin et Sylvain Rairat
sujet proposé par Gaëtan Chenevier

Juin 2004

Table des matières

1 Introduction

L'objet de ce mémoire est la démonstration du théorème de Kronecker-Weber qui affirme que toute extension normale de $\mathbf{Q}$ de groupe de Galois abélien est incluse dans une extension cyclotomique de $\mathbf{Q}$.

Ce théorème nous permet par exemple d'affirmer que la formule de Gauss

$$\sqrt{n} = \sum_{k=0}^{n-1} e^{\frac{2ik^2\pi}{n}} \text{ si } n \equiv 1 \mod 4$$

n'a rien de fortuit, mais illustre élégamment une telle inclusion.

La preuve que nous donnons ici de ce théorème est celle que suggère Marcus, sous la forme d'une suite d'exercices guidés. La présentation donnée des différentes notions doit également beaucoup à son ouvrage.

Nous commencerons par introduire quelques résultats de théorie de la ramification qui seront nécessaires à la démonstration. En conséquence, les premières parties de ce mémoire sont consacrées à la définition et aux propriétés des anneaux d'entiers qui sont, comme nous le verrons des exemples d'anneaux de Dedekind. Cette caractéristique leur confère la remarquable propriété de décomposition unique des idéaux en idéaux premier. Nous pourrons alors étudier ces décompositions à l'aide de la théorie de la ramification, qui conjuguée à la théorie de Galois fournit en retour des renseignements sur la structure du corps. En particulier l'étude des contraintes auxquelles doit se plier la ramification dans les corps abéliens nous permettra de démontrer le théorème.

2 Anneaux d'entiers

Dans cette partie, nous allons définir et développer les premières propriétés des anneaux d'entiers. En particulier, nous allons montrer que les anneaux d'entiers sont des anneaux de Dedekind.

2.1 Quelques définitions

Définition 2.1.1. *Quelques rappels :*
- *Un corps de nombres* $\mathbf{K}$ *est un sous-corps de* $\mathbf{C}$ *de degré fini sur* $\mathbf{Q}$.
- *Un nombre algébrique est dit entier algébrique s'il est racine d'un polynôme unitaire à coefficients entiers. On note* $\mathcal{O}$*, l'ensemble des entiers algébriques.*
- *L'anneau des entiers d'un corps de nombre* $\mathbf{K}$ *est* $\mathcal{O} \cap \mathbf{K}$*. On le note* $\mathcal{O}_{\mathbf{K}}$

Définition 2.1.2. *On a aussi des corps particuliers :*
- *Un corps de nombres* $\mathbf{K}$ *est dit quadratique si* $[\mathbf{K} : \mathbf{Q}] = 2$*, on peut alors l'écrire sous la forme* $\mathbf{K} = \mathbf{Q}[\sqrt{d}]$ *où* d *est un entier relatif sans facteur carré.*
- *Un corps de nombres* $\mathbf{K}$ *est dit cyclotomique si il est engendré par une racine* $m-$*ième de l'unité.*

Remarque 2.1.1. *En fait, un nombre est entier algébrique si son polynôme minimal est à coefficients entiers. De plus, un anneau d'entiers est bien un anneau en tant qu'intersection de deux anneaux.*

Remarque 2.1.2. *L'anneau des entiers de* $\mathbf{Q}$ *est* $\mathbf{Z}$ *, donc la définition est bien cohérente avec la notion usuelle d'entier.*

Proposition 2.1.1. $\forall \alpha \in \mathbf{K}, \exists m \in \mathbf{Z}$ *non nul,* $m\alpha \in \mathcal{O}_{\mathbf{K}}$

Conséquence 2.1.2. *Il existe une base de* $\mathbf{K}$ *sur* $\mathbf{Q}$ *constituée d'éléments de* $\mathcal{O}_{\mathbf{K}}$*.*

Définition 2.1.3. *On appelle anneau de Dedekind un anneau* R *vérifiant :*
- R *est intègre*
- R *est noetherien*
- *Tout idéal premier non nul est maximal*
- R *est intégralement clos*

2.2 Trace et Norme

Définition 2.2.1. *Soient* $\mathbf{K} \subset \mathbf{L}$ *deux corps de nombres. Soient* $\sigma_1, \ldots, \sigma_n$ *les* n $\mathbf{K}$*-plongements de* $\mathbf{L}$ *dans* $\mathbf{C}$*.*

Pour $\alpha \in \mathbf{L}$*, on considère l'endomorphisme* M_α *de multiplication par* α *dans le* $\mathbf{K}$*-espace vectoriel* $\mathbf{L}$*. On définit alors :*
- *la trace de* α *:*
$$\mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\alpha) = \mathrm{Tr}(M_\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$
- *la norme de* α *:*
$$\mathrm{N}_{\mathbf{K}}^{\mathbf{L}}(\alpha) = \det(M_\alpha) = \sigma_1(\alpha) \times \cdots \times \sigma_n(\alpha)$$

Proposition 2.2.1. $\mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}$ *est additive, et* $\mathrm{N}_{\mathbf{K}}^{\mathbf{L}}$ *multiplicative.*

Proposition 2.2.2. *Soit* $\alpha \in \mathbf{L}$*, alors* $\mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\alpha)$ *et* $\mathrm{N}_{\mathbf{K}}^{\mathbf{L}}(\alpha)$ *sont dans* $\mathbf{K}$*. De plus, si* $\alpha \in \mathcal{O}_{\mathbf{L}}$*, alors* $\mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\alpha)$ *et* $\mathrm{N}_{\mathbf{K}}^{\mathbf{L}}(\alpha)$ *sont dans* $\mathcal{O}_{\mathbf{K}}$*.*

Proposition 2.2.3. *Si on a* $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M}$*, trois corps de nombres, alors pour tout* $\alpha \in \mathbf{M}$*, on a :*

- $\mathrm{Tr}_{\mathbf{K}}^{\mathbf{M}}(\alpha) = \mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\mathrm{Tr}_{\mathbf{L}}^{\mathbf{M}}(\alpha))$
- $\mathrm{N}_{\mathbf{K}}^{\mathbf{M}}(\alpha) = \mathrm{N}_{\mathbf{K}}^{\mathbf{L}}(\mathrm{N}_{\mathbf{L}}^{\mathbf{M}}(\alpha))$

Démonstration : Il s'agit d'étendre les plongements de $\mathbf{L}$ dans $\mathbf{C}$ à $\mathbf{M}$, et on trouve le résultat. □

Proposition 2.2.4. *Soit* $\mathbf{K}$ *un corps quadratique, alors*

$$\forall \alpha \in \mathbf{K}, \alpha \in \mathcal{O}_{\mathbf{K}} \Leftrightarrow \mathrm{Tr}^{\mathbf{K}}(\alpha) \in \mathbf{Z} \text{ et } \mathrm{N}^{\mathbf{K}}(\alpha) \in \mathbf{Z}$$

Démonstration : Si $\alpha \in \mathbf{Q}$, alors c'est clair, et si $\alpha \in \mathbf{K} \setminus \mathbf{Q}$, alors son polynôme minimal est de degré 2, et ses coefficients sont au signe près la norme et la trace de α, d'où le résultat. □

2.3 Discriminant

Soit $\mathbf{K}$ un corps de nombres de degré n sur $\mathbf{Q}$. Soient $\alpha_1, \ldots, \alpha_n \in \mathbf{K}$, et $\sigma_1, \ldots, \sigma_n$ les n plongements de $\mathbf{K}$ dans C.

Définition 2.3.1. *On définit le discriminant de* $\alpha_1, \ldots, \alpha_n$ *par :*

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}^{\mathbf{K}}(\alpha_i \alpha_j))$$

Notation : Si $\mathbf{K} = \mathbf{Q}[\alpha]$, alors on note $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{disc}(\alpha)$.

Proposition 2.3.1. *On a les appartenances :*

$$\forall \alpha_1, \ldots, \alpha_n \in \mathbf{K}, \mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbf{Q}$$
$$\forall \alpha_1, \ldots, \alpha_n \in \mathcal{O}_{\mathbf{K}}, \mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}$$

Théorème 2.3.2.

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$$

Démonstration : Ceci est la conséquence immédiate de l'égalité matricielle :

$$[\sigma_j(\alpha_i)] \times [\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)] = [\mathrm{Tr}^{\mathbf{K}}(\alpha_i\alpha_j)]$$

□

Remarque 2.3.1. *Le carré fait que le déterminant ne dépend pas de l'ordre des* σ *ou des* α.

Proposition 2.3.3. *Si* $[\alpha_i] = M \times [\beta_i]$, *avec* M *matrice* $n \times n$ *à coefficents dans* $\mathbf{Q}$ *, alors :*

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(M)^2 \, \mathrm{disc}(\beta_1, \ldots, \beta_n)$$

Démonstration : On a

$$\forall j, [\sigma_j(\alpha_i)]_i = M \times [\sigma_j(\beta_i)]_i$$

On en déduit donc que

$$[\sigma_j(\alpha_i)]_{i,j} = M \times [\sigma_j(\beta_i)]_{j,i}$$

On obtient donc le résultat en passant au déterminant et en mettant au carré. □

Théorème 2.3.4. $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0 \Leftrightarrow \alpha_1, \ldots, \alpha_n$ *sont linéairement dépendants sur* $\mathbf{Q}$.

Démonstration : Si $\alpha_1, \ldots, \alpha_n$ sont linéairement dépendants, alors les colonnes de la matrice $[\sigma_i(\alpha_j)]$ aussi, et donc $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$.

Inversement, si $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$, alors les lignes R_i de la matrice $[\mathrm{Tr}^{\mathbf{K}}(\alpha_i\alpha_j)]$ sont liées. Supposons que les $\alpha_1, \ldots, \alpha_n$ sont linéairement indépendants sur $\mathbf{Q}$. Soient $a_1, \ldots, a_n \in \mathbf{Q}$ non tous nuls tels que $a_1R_1 + \cdots + a_nR_n = 0$. Soit $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$. Nécessairement, $\alpha \neq 0$. De plus, en regardant les coordonnées de chaque ligne, on obtient : $\mathrm{Tr}^{\mathbf{K}}(\alpha\alpha_j) = 0$, pour chaque j. Comme $\alpha \neq 0$, et les $\alpha_1, \ldots, \alpha_n$ sont linéairement indépendant, ils forment donc une base de $\mathbf{K}$ sur $\mathbf{Q}$, et de même pour les $\alpha\alpha_1, \ldots, \alpha\alpha_n$. Mais alors, $\forall \beta \in \mathbf{K}$ $\mathrm{Tr}^{\mathbf{K}}(\beta) = 0$, ce qui est une contradiction car $\mathrm{Tr}^{\mathbf{K}}(1) = n$. □

Théorème 2.3.5. *Si* $\mathbf{K} = \mathbf{Q}[\alpha]$, *soient* $\alpha_1, \ldots \alpha_n$ *les conjugués de* α *sur* $\mathbf{Q}$, *et* f *le polynôme minimal de* α *sur* $\mathbf{Q}$ *; alors*

$$\mathrm{disc}(\alpha) = \prod_{r \neq s} (\alpha_r - \alpha_s)^2 = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}^{\mathbf{K}}(f'(\alpha))$$

Démonstration : On a :

$$\det(\sigma_i(\alpha^{j-1})) = \det((\sigma_i(\alpha))^{j-1}) = \det(\alpha_i^{j-1})$$

si les σ_i sont dans le bon ordre. On a donc un déterminant de Vandermonde, d'où la première égalité. Enfin, comme $f(X) = \prod_{1 \leq i \leq n}(X - \alpha_i)$, on a :

$$\begin{aligned}
(-1)^{\frac{n(n-1)}{2}} \prod_{r<s} (\alpha_r - \alpha_s)^2 &= \prod_{1 \leq r \leq n} \prod_{s \neq r} (\alpha_r - \alpha_s) \\
&= \prod_{1 \leq r \leq n} f'(\alpha_r) \\
&= \prod_{1 \leq r \leq n} \sigma_r(f'(\alpha)) \\
&= \mathrm{N}^{\mathbf{K}}(f'(\alpha))
\end{aligned}$$

□

2.4 Structure additive de l'anneau des entiers

Définition 2.4.1. *Un groupe abélien libre de rang* n *est un groupe qui est isomorphe à* $\mathbf{Z}^n$.

Remarque 2.4.1. *Le rang est bien déterminé car les* $\mathbf{Z}^n$ *ne sont pas isomorphes deux à deux.*

Proposition 2.4.1. *Un sous-groupe d'un groupe abélien libre de rang* n *est encore un groupe abélien libre de rang inférieur ou égal à* n.

Théorème 2.4.2. *Soit* $\mathfrak{a}$ *un idéal de* $\mathcal{O}_{\mathbf{K}}$ *et* $\{\alpha_1, \ldots, \alpha_n\}$ *une base de* $\mathbf{K}$ *sur* $\mathbf{Q}$ *constituée d'éléments de* $\mathfrak{a}$, *et* $d = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$. *Alors tout* $\alpha \in \mathfrak{a}$ *peut s'exprimer sous la forme :*

$$\alpha = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d} \quad \text{avec } m_j \in \mathbf{Z} \text{ et } d | m_j^2.$$

Démonstration : Soit $\alpha \in \mathfrak{a}$, on écrit $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$, avec $x_i \in \mathbf{Q}$. On multiplie chaque côté par α_i et on prend la trace.

$$\mathrm{Tr}^{\mathbf{K}}(\alpha\alpha_j) = \sum x_i \,\mathrm{Tr}^{\mathbf{K}}(\alpha_i\alpha_j)$$

Les éléments $\mathrm{Tr}^{\mathbf{K}}(\alpha\alpha_j)$ et $\mathrm{Tr}^{\mathbf{K}}(\alpha_i\alpha_j)$ sont dans $\mathbf{Z}$, donc en résolvant le système obtenu par les règles de Cramer, les x_i sont tous des entiers divisés par $d = \det(\mathrm{Tr}^{\mathbf{K}}(\alpha_i\alpha_j))$. □

Proposition 2.4.3. *Tout idéal $\mathfrak{a}$ non nul de $\mathcal{O}_{\mathbf{K}}$ contient une base de $\mathbf{K}$ sur $\mathbf{Q}$.*

Démonstration : Soit $\beta_1, \ldots, \beta_n$ une base de $\mathbf{K}$ sur $\mathbf{Q}$, alors il existe $b \in \mathbf{Z}$ (il suffit de prendre le ppcm des m_i de la proposition 2.1.1) tel que $\forall i\ b\beta_i \in \mathcal{O}_{\mathbf{K}}$. Soit $\alpha \in \mathfrak{a}$ non nul, alors les éléments $b\alpha\beta_1, \ldots, b\alpha\beta_n$ forment une base de $\mathbf{K}$ sur $\mathbf{Q}$ et sont dans $\mathfrak{a}$. □

Corollaire 2.4.4. *$\mathfrak{a}$ est un groupe libre abélien de rang n.*

Démonstration : Soit $\{\alpha_1, \ldots, \alpha_n\}$, comme dans le théorème (il en existe, d'après la proposition 2.4.3) , et $A = \mathbf{Z}\alpha_1 \oplus \cdots \oplus \mathbf{Z}\alpha_n$. Alors d'après le théorème, on a :

$$A \subset \mathfrak{a} \subset \frac{1}{d}A$$

Ce qui permet de conclure grâce a la propriété 2.4.1. □

Conséquence 2.4.5. *$\mathcal{O}_{\mathbf{K}}$ est un groupe abélien libre de rang n.*

Définition 2.4.2. *Si $\{\alpha_1, \ldots, \alpha_n\}$ est une base de $\mathfrak{a}$ en tant que $\mathbf{Z}$-module, alors on l'appelle base intégrale de $\mathfrak{a}$.*

Remarque 2.4.2. *Une base intégrale de $\mathfrak{a}$ est aussi une base de $\mathbf{K}$ sur $\mathbf{Q}$.*

Théorème 2.4.6. *Soient $\alpha_1, \ldots, \alpha_n$ et $\beta_1, \ldots, \beta_n$, deux bases intégrales de $\mathfrak{a}$. Alors*

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\beta_1, \ldots, \beta_n)$$

Démonstration : On écrit les β en fonction des α :

$$[\beta_i] = M \times [\alpha_i]$$

M est une matrice $n \times n$ à coefficients dans $\mathbf{Z}$. En appliquant la proposition 2.3.3, on obtient :

$$\mathrm{disc}(\beta_1, \ldots, \beta_n) = \det(M)^2 \times \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$$

Comme $\det(M) \in \mathbf{Z}$, on a $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) | \,\mathrm{disc}(\beta_1, \ldots, \beta_n)$, et ils ont le même signe. De la même manière, on montre que $\mathrm{disc}(\beta_1, \ldots, \beta_n) | \,\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$, et qu'ils sont donc égaux. □

Remarque 2.4.3. *Le discriminant d'une base intégrale de $\mathcal{O}_{\mathbf{K}}$ ne dépend donc pas de la base choisie, mais que de l'anneau considéré. On peut donc le noter* $\mathrm{disc}(\mathcal{O}_{\mathbf{K}})$.

Théorème 2.4.7. *Soit $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$ une base de $\mathbf{K}$ sur $\mathbf{Q}$ avec $|\operatorname{disc}(\alpha_1, \ldots, \alpha_n)|$ minimal. Alors $\alpha_1, \ldots, \alpha_n$ est une base intégrale de $\mathfrak{a}$.*

Démonstration : Comme la valeur absolue du déterminant d'une base est un entier strictement positif, il existe une telle base.

Soit $\alpha \in \mathfrak{a}$, alors $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n$, avec $\gamma_i \in \mathbf{Q}$. Nous devons donc montrer que $\gamma_i \in \mathbf{Z}$; supposons le contraire. Alors, on peut supposer que $\gamma_1 \notin \mathbf{Z}$, quitte à réindexer les éléments de la base. $\gamma_1 = m + \theta$, avec $m \in \mathbf{Z}$ and $0 < \theta < 1$. Soit $\beta_1 = \alpha - m\alpha_1, \beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n$. Alors, $\beta_1, \ldots, \beta_n \in \mathfrak{a}$ et forment une base de $\mathbf{K}$ sur $\mathbf{Q}$ car $\beta_1 = \theta\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n$. La matrice de transition entre ces bases est donc :

$$\begin{pmatrix} \theta & \gamma_2 & \ldots & \gamma_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

Donc, par la définition du discriminant, on a : $\operatorname{disc}(\beta_1, \ldots, \beta_n) = \theta^2 \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ ce qui est absurde par choix de $\alpha_1, \ldots, \alpha_n$. □

Théorème 2.4.8. *Soit $\mathbf{K}$ un corps de nombres, alors $\mathcal{O}_\mathbf{K}$ est un anneau de Dedekind.*

Lemme 2.4.9. *Soit $\mathfrak{a}$ un idéal non nul $\mathcal{O}_\mathbf{K}$, alors $\mathcal{O}_\mathbf{K}/\mathfrak{a}$ est fini. On appelle norme de $\mathfrak{a}$ et on note $\|\mathfrak{a}\|$ son cardinal.*

Démontrons le lemme :

Démonstration : Soient $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, et $m = \mathrm{N}^\mathbf{K}(\alpha) \in \mathbf{Z}$. $m \neq 0$, et on a $m \in \mathfrak{a}$ car $m/\alpha \in \mathbf{K}$ et m/α est un produit de conjugués de α (pas nécessairement dans $\mathbf{K}$) , qui est donc entier algébrique. $\mathcal{O}_\mathbf{K}/(m)$ est fini de cardinal m^n car si $\mathcal{O}_\mathbf{K} = \bigoplus \alpha_i\mathbf{Z}$, alors $\mathcal{O}_\mathbf{K}/(m) = \bigoplus \alpha_i \frac{\mathbf{Z}}{m\mathbf{Z}}$, donc, comme $(m) \subset \mathfrak{a}$, $\mathcal{O}_\mathbf{K}/\mathfrak{a}$ est fini, de cardinal divisant m^n. □

Démonstration : Il est clair que $\mathcal{O}_\mathbf{K}$ est intègre et intégralement clos.

Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_\mathbf{K}$, alors $\mathfrak{a}$ est un sous-groupe de $\mathcal{O}_\mathbf{K}$, c'est donc un sous-groupe d'un groupe abélien libre de rang n, donc $\mathfrak{a}$ est aussi un groupe abélien libre de rang inférieur ou égal à n, il est donc finiment engendré. Donc $\mathcal{O}_\mathbf{K}$ est un anneau noethérien.

Soit $\mathfrak{p}$ un idéal non nul, premier. Alors $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ est un anneau intègre fini, c'est donc un corps, et $\mathfrak{p}$ est maximal. □

Théorème 2.4.10. *Soient $\mathbf{K}$ et $\mathbf{L}$ deux corps de nombres de degrés respectifs m et n sur $\mathbf{Q}$. Soit $d = m \wedge n$. Si $[\mathbf{KL} : \mathbf{Q}] = mn$, alors $\mathcal{O}_\mathbf{K}\mathcal{O}_\mathbf{L} \subset \mathcal{O}_\mathbf{KL} \subset \frac{1}{d}\mathcal{O}_\mathbf{K}\mathcal{O}_\mathbf{L}$.*

Démonstration : La première inclusion est claire. Soit $\alpha_1, \ldots, \alpha_m$ et $\beta_1, \ldots, \beta_n$ des bases intégrales de $\mathcal{O}_\mathbf{K}$ et $\mathcal{O}_\mathbf{L}$. Alors la famille des $\alpha_i\beta_j$ forme une $\mathbf{Z}$-base de $\mathcal{O}_\mathbf{K}\mathcal{O}_\mathbf{L}$, et une base de $\mathbf{KL}$ sur $\mathbf{Q}$. Tout α dans $\mathcal{O}_\mathbf{KL}$ peut se mettre sous la forme :

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r(\alpha)} \alpha_i\beta_j$$

où les m_{ij} et $r(\alpha)$ sont dans $\mathbf{Z}$, et $\{r, m_{ij}\}$ premiers dans leur ensemble.

Nous devons donc montrer que $\forall \alpha, r(\alpha)|d$. Tout plongement σ de $\mathbf{K}$ dans $\mathbf{C}$ peut être étendu à $\mathbf{KL}$, par l'identité sur $\mathbf{L}$, car puisque par hypothèse $[\mathbf{KL} : \mathbf{L}] = m$, les m plongements de $\mathbf{KL}$ dans $\mathbf{C}$ induisant l'identité sur $\mathbf{L}$ parcourent tous les plongements de $\mathbf{K}$ dans $\mathbf{C}$, par restriction. Donc pour tout σ, on a :

$$\sigma(\alpha) = \sum_{i,j} \frac{m_{ij}}{r(\alpha)} \sigma(\alpha_i)\beta_j$$

Soit

$$x_i = \sum_j \frac{m_{ij}}{r(\alpha)} \beta_j \in \mathbf{L}$$

On obtient un système d'équations, pour k entre 1 et m :

$$\sigma_k(\alpha) = \sum_i \sigma_k(\alpha_i) x_i$$

On résoud le système d'inconnues x_i par les règles de Cramer : $x_i = \gamma_i/\delta$, où $\delta = \det(\sigma_j(\alpha_i))_{i,j}$, et γ_i est obtenu en remplaçant la i-ème colonne par les $\sigma_j(\alpha)$. $\delta^2 = \mathrm{disc}(\mathcal{O}_\mathbf{K}) = e \neq 0$, et de plus tous les $\sigma_j(\alpha_i)$ et les $\sigma_j(\alpha)$ sont des entiers algébriques, donc les γ_i et δ aussi. On a $ex_i = \delta\gamma_i \in \mathcal{O}_\mathbf{L}$. Comme les β_j forment une base intégrale de $\mathcal{O}_\mathbf{L}$, on a $em_{i,j}/r(\alpha) \in \mathbf{Z}$, donc $r(\alpha)|e = \mathrm{disc}(\mathcal{O}_\mathbf{K})$, car il est premier au pgcd des $m_{i,j}$. Par symétrie de $\mathbf{K}$ et $\mathbf{L}$, on a aussi $r(\alpha)|\,\mathrm{disc}(\mathcal{O}_\mathbf{L})$, et donc $r(\alpha)|d$, d'où le résultat. □

Conséquence 2.4.11. *Si* $[\mathbf{KL} : \mathbf{Q}] = [\mathbf{K} : \mathbf{Q}][\mathbf{L} : \mathbf{Q}]$ *et* $\mathrm{disc}(\mathcal{O}_\mathbf{K}) \wedge \mathrm{disc}(\mathcal{O}_\mathbf{L}) = 1$, *alors* $\mathcal{O}_\mathbf{KL} = \mathcal{O}_\mathbf{K}\mathcal{O}_\mathbf{L}$.

2.5 Exemple : les corps quadratiques

Soit $\mathbf{K}$ un corps quadratique. Alors $\exists m \in \mathbf{Z}$, m sans facteur carré, tel que $\mathbf{K} = \mathbf{Q}[\sqrt{m}]$.

Théorème 2.5.1. *On peut calculer l'anneau des entier d'un corps quadratique :*
- *Si* $m \equiv 2, 3 \mod 4$, *alors* $\mathcal{O}_\mathbf{K} = \mathbf{Z} \oplus \sqrt{m}\mathbf{Z}$
- *Si* $m \equiv 1 \mod 4$, *alors* $\mathcal{O}_\mathbf{K} = \mathbf{Z} \oplus (\frac{1+\sqrt{m}}{2})\mathbf{Z}$

Démonstration : D'après la proposition 2.2.4, soit $x = r + s\sqrt{m} \in \mathbf{K}$, avec $r, s \in \mathbf{Q}$, alors :

$$\begin{aligned} x \in \mathcal{O}_\mathbf{K} &\Leftrightarrow \mathrm{Tr}^\mathbf{K}(x) \in \mathbf{Z} \text{ et } \mathrm{N}^\mathbf{K}(x) \in \mathbf{Z} \\ &\Leftrightarrow 2r \in \mathbf{Z} \text{ et } r^2 - ms^2 \in \mathbf{Z} \end{aligned}$$

Si $x \in \mathcal{O}_\mathbf{K}$, alors $2r \in \mathbf{Z}$, et par conséquent $4s^2m \in \mathbf{Z}$, or m est sans facteur carré, donc $2s \in \mathbf{Z}$. Soit $x = \frac{u+v\sqrt{m}}{2}$, avec $u, v \in \mathbf{Z}$.

Si $m \equiv 2, 3 \mod 4$, alors $u^2 - mv^2 \equiv u^2 + v^2 \mod 4$ ou $u^2 + 2v^2 \mod 4$. De plus, cette quantité doit être congrue à $0 \mod 4$, pour que la norme soit dans $\mathbf{Z}$. La seule possiblité dans les deux cas est que m et n soient pairs, ce qui démontre le premier cas (l'autre inclusion est claire).

Si $m \equiv 1 \mod 4$, alors $u^2 - mv^2 \equiv u^2 - v^2 \mod 4$; pour que $x \in \mathcal{O}_\mathbf{K}$ il faut que u et v aient même parité. On a donc une inclusion car

$$\mathbf{Z} \oplus (\frac{1+\sqrt{m}}{2})\mathbf{Z} = \{\frac{u+v\sqrt{m}}{2} \in \mathbf{K}, u \equiv v \mod 2\}$$

L'autre inclusion se vérifie aisément. □

Théorème 2.5.2. *Soit $d = \mathrm{disc}(\mathcal{O}_\mathbf{K})$, alors :*
- *$d = 4m$ si $m \equiv 2, 3 \mod 4$*
- *$d = m$ si $m \equiv 1 \mod 4$*

Démonstration : D'après le théorème précédent, on dispose de bases intégrales (α_1, α_2) de $\mathcal{O}_\mathbf{K}$. On utilise la définition du discriminant, et on a alors :
- Si $m \equiv 2, 3 \mod 4$, alors

$$d = \det(\mathrm{Tr}^\mathbf{K}(\alpha_i\alpha_j)) = \begin{vmatrix} 2 & 0 \\ 0 & 2m \end{vmatrix} = 4m$$

- Si $m \equiv 1 \mod 4$, alors

$$d = \det(\mathrm{Tr}^\mathbf{K}(\alpha_i\alpha_j)) = \begin{vmatrix} 2 & -1 \\ -1 & (1+m)/2 \end{vmatrix} = m$$

□

2.6 Exemple : les corps cyclotomiques

Soit m un entier plus grand que 3, $\omega = e^{2i\pi/m}$ et $\mathbf{K} = \mathbf{Q}[\omega]$, un corps cyclotomique.

Proposition 2.6.1. $\mathrm{disc}(\omega) | m^{\phi(m)}$.

Démonstration : Soit $\Phi_m \in \mathbf{Z}[X]$ le polynôme minimal (unitaire) de ω (le m-ième polynôme cyclotomique). Alors $X^m - 1 = \Phi_m(X)Q(X)$, pour un certain $Q \in \mathbf{Z}[X]$. En dérivant, et en évaluant en ω, on obtient que $m = \omega\Phi'_m(\omega)Q(\omega)$, donc en passant aux normes, on a $m^{\phi(m)} = \pm\,\mathrm{disc}(\omega)\,\mathrm{N}^\mathbf{K}(\omega Q(\omega))$ (théorème 2.3.5). Or $\mathrm{N}^\mathbf{K}(\omega Q(\omega)) \in \mathbf{Z}$, car c'est un polynôme à coefficients dans $\mathbf{Z}$ en ω qui est un entier algébrique. D'où le résultat. □

Théorème 2.6.2. *Si $m = p^r$, avec p un nombre premier. Alors $\mathcal{O}_\mathbf{K} = \mathbf{Z}[\omega]$.*

Lemme 2.6.3.

$$\prod_{k=1, p\nmid k}^{m} (1 - \omega^k) = p$$

Démonstration : Soit $P(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}$. On a $P(1) = p$, et tous les ω^k, $p \nmid k$, sont racines de P, car ils sont racines de $X^{p^r} - 1$, mais pas de $X^{p^{r-1}} - 1$, donc

$$P(X) = \prod_{k=1, p\nmid k}^{m} (X - \omega^k)$$

En prenant $X = 1$, on obtient le résultat. □

Démonstration : D'après le théorème 2.4.2, comme $\mathbf{Q}[\omega] = \mathbf{Q}[1 - \omega]$, tout $\alpha \in \mathcal{O}_\mathbf{K}$ peut se mettre sous la forme :

$$\alpha = \frac{m_1 + m_2(1-\omega) + \cdots + m_n(1-\omega)^{n-1}}{d}$$

où $n = \phi(p^r)$, $m_i \in \mathbf{Z}$, et $d = \mathrm{disc}(\omega) = \mathrm{disc}(1-\omega)$. En effet,

$$\mathrm{disc}(\omega) = \prod_{r<s}(\omega_r - \omega_s)^2 = \prod_{r<s}((1-\omega_r) - (1-\omega_s))^2 = \mathrm{disc}(1-\omega)$$

où les ω_r sont les conjugués de ω, ce qui implique que les conjugués de $1-\omega$ sont les $1-\omega_r$.

D'après la proposition 2.6.1, d est une puissance de p. Nous allons montrer que $\mathcal{O}_{\mathbf{K}} = \mathbf{Z}[1-\omega]$, ce qui impliquera le résultat car $\mathbf{Z}[1-\omega] = \mathbf{Z}[\omega]$.

Supposons que $\mathcal{O}_{\mathbf{K}} \neq \mathbf{Z}[1-\omega]$, alors il existe un élément non nul

$$\alpha = \frac{m_1 + m_2(1-\omega) + \cdots + m_n(1-\omega)^{n-1}}{p^k}$$

pour lequel aucun des m_i n'est divisible par $d = p^k$. On considère alors le premier indice i pour lequel la valuation v_i de m_i en p est minimale (pour tout j, $p^{v_i} | m_j$ et $p^{v_i+1} \nmid m_i$), et on pose

$$\beta = p^{k-v_i-1}\alpha - \sum_{j<i} \frac{m_j(1-\omega)^{j-1}}{p^{v_i+1}}$$

Alors $\beta \in \mathcal{O}_{\mathbf{K}}$ car par définition de i les $\frac{m_j(1-\omega)^{j-1}}{p^{v_i+1}}$ sont entiers algébriques. On peut alors écrire :

$$\beta = \frac{m_i(1-\omega)^{i-1} + m_{i+1}(1-\omega)^i + \cdots + m_n(1-\omega)^{n-1}}{p}, p \nmid m_i$$

Or d'après le lemme, $p/(1-\omega)^n \in \mathbf{Z}[\omega]$, car $(1-\omega)$ divise $(1-\omega^k)$ dans $\mathbf{Z}[\omega]$, et on a $\phi(m) = n$ tels facteurs. Donc $\frac{p}{(1-\omega)^i} \in \mathbf{Z}[\omega]$, d'où

$$\frac{\beta p}{(1-\omega)^i} = \frac{m_i}{1-\omega} + \sum_{j>i} m_j(1-\omega)^{j-i} \in \mathcal{O}_{\mathbf{K}}$$

Dans ce nombre, tous les termes d'indice supérieur à i sont dans $\mathcal{O}_{\mathbf{K}}$, donc par soustraction, $\frac{m_i}{1-\omega} \in \mathcal{O}_{\mathbf{K}}$. Ce qui implique que $\mathrm{N}^{\mathbf{K}}(1-\omega) | \mathrm{N}^{\mathbf{K}}(m_i)$, mais c'est impossible, car $\mathrm{N}^{\mathbf{K}}(m_i) = m_i^n$, et le lemme montre que $\mathrm{N}^{\mathbf{K}}(1-\omega) = p$. □

Théorème 2.6.4. *On ne suppose plus rien sur m, alors $\mathcal{O}_{\mathbf{K}} = \mathbf{Z}[\omega]$.*

Démonstration : Nous allons montrer le résultat par récurrence sur le nombre de facteurs premiers de m. Si m est une puissance d'un nombre premier, alors on a déjà établi le résultat. Supposons maintenant que $m = m_1 m_2$, avec $m_1 \wedge m_2 = 1$ et $m_1, m_2 > 1$. On a donc le résultat sur m_1 et m_2, par hypothèse de récurrence. Soient :

$$\omega_1 = e^{2i\pi/m_1}, \omega_2 = e^{2i\pi/m_2}$$

$$\mathbf{K}_1 = \mathbf{Q}[\omega_1], \mathbf{K}_2 = \mathbf{Q}[\omega_2]$$

Nous allons utiliser la conséquence 2.4.11, et on aura alors $\mathcal{O}_{\mathbf{K}} = \mathcal{O}_{\mathbf{K}_1}\mathcal{O}_{\mathbf{K}_2} = \mathbf{Z}[\omega_1]\mathbf{Z}[\omega_2] = \mathbf{Z}[\omega]$, car $m_1 \wedge m_2 = 1$ (alors $um_1 + vm_2 = 1$ pour deux entiers u et v, d'où $\omega = \omega_1^v \omega_2^u$). On a bien $\mathbf{K} = \mathbf{K}_1\mathbf{K}_2$, $[\mathbf{K} : \mathbf{Q}] = \phi(m) = \phi(m_1)\phi(m_2) = [\mathbf{K}_1 : \mathbf{Q}][\mathbf{K}_2 : \mathbf{Q}]$, car $m_1 \wedge m_2 = 1$. Il ne reste qu'à vérifier la condition du discriminant, qui est claire d'après 2.6.1. On a donc le résultat. □

3 Idéaux dans les anneaux de Dedekind

Dans cette partie, nous allons considérer un anneau de Dedekind R, quelconque, de corps de fractions $\mathbf{K}$, et allons montrer qu'on peut décomposer les idéaux en produit d'idéaux premiers, de la même manière que l'on décompose les entiers en produits de nombres premiers.

3.1 Le groupe des classes d'idéaux

Lemme 3.1.1. *Tout idéal* $\mathfrak{i}$ *non nul contient un produit fini d'idéaux premiers non nuls.*

Démonstration : Supposons que non, considérons l'ensemble des idéaux non nuls qui ne contiennent pas de produit d'idéaux premiers. Il est non vide, et admet donc un élément maximal $\mathfrak{m}$, car R est noethérien. $\mathfrak{m}$ n'est pas un idéal premier, par définition. Donc $\exists r, s \in R \setminus \mathfrak{m},\ rs \in \mathfrak{m}$. Les idéaux $\mathfrak{m} + (r)$ et $\mathfrak{m} + (s)$ sont strictement plus grand que $\mathfrak{m}$, et doivent donc contenir un produit de nombres premiers, donc $(\mathfrak{m} + (r))(\mathfrak{m} + (s))$ aussi, qui est contenu dans $\mathfrak{m}$, contradiction. □

Théorème 3.1.2. *Soit* $\mathfrak{i}$ *un idéal non nul de* R*. Alors, il existe un idéal* $\mathfrak{j}$ *non nul tel que* $\mathfrak{ij}$ *soit principal.*

Lemme 3.1.3. *Soit* $\mathfrak{a}$ *un idéal propre de* R*, de corps de fractions* $\mathbf{K}$*. Alors* $\exists \gamma \in \mathbf{K} \setminus R, \gamma\mathfrak{a} \subset R$*.*

Démonstration : Soit $a \in \mathfrak{a}$ $a \neq 0$, alors $\exists \mathfrak{p}_1, \ldots, \mathfrak{p}_r$, des idéaux premiers tels que $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset (a)$, avec r minimal. (d'après le lemme précedent). De plus, $\mathfrak{a}$ est contenu dans un idéal maximal $\mathfrak{p}$ qui est donc premier. Donc $\mathfrak{p}$ contient $\mathfrak{p}_1 \ldots \mathfrak{p}_r$. Il s'en suit donc que $\mathfrak{p}$ contient un $\mathfrak{p}_i$, par primalité de $\mathfrak{p}$. On peut supposer que $\mathfrak{p}_1 \subset \mathfrak{p}$. Comme R est un anneau de Dedekind, on doit donc avoir que $\mathfrak{p}_1 = \mathfrak{p}$.

Finalement, comme (a) ne peut pas contenir un produit de moins de r idéaux premiers, $\mathfrak{p}_2 \ldots \mathfrak{p}_r \nsubseteq (a)$ et, en particulier, $\exists b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r \setminus (a)$. Donc $\gamma = b/a \in \mathbf{K} \setminus R$ convient. □

Revenons à la démonstration du théorème :

Démonstration : Soit α un élément non nul de $\mathfrak{i}$ et $\mathfrak{j} = \{\beta \in R, \beta\mathfrak{i} \subset (\alpha)\}$. Alors $\mathfrak{j}$ est clairement un idéal non nul car $\alpha \in \mathfrak{j}$ et on a $\mathfrak{ij} \subset (\alpha)$. Soit $\mathfrak{a} = \frac{1}{\alpha}\mathfrak{ij} \subset R$. $\mathfrak{a}$ est un idéal. Si $\mathfrak{a} = R$, alors $\mathfrak{ij} = (\alpha)$, et on a terminé. Sinon, $\mathfrak{a}$ est un idéal propre et on peut appliquer le deuxième lemme. Ainsi $\gamma\mathfrak{a} \subset R, \gamma \in \mathbf{K} \setminus R$. Nous allons obtenir une contradiction de ce fait. Comme R est intégralement clos, il suffit de montrer que γ est racine d'un polynôme unitaire de $R[X]$.

Comme $\alpha \in \mathfrak{i}$, alors $\mathfrak{j} \subset \mathfrak{a}$, ainsi $\gamma\mathfrak{j} \subset \gamma\mathfrak{a} \subset R$. On en déduit que $\gamma\mathfrak{j} \subset \mathfrak{j}$, grâce à la définition de $\mathfrak{j}$.

Finalement, soit $\alpha_1, \ldots, \alpha_m$ un ensemble générateur de $\mathfrak{j}$: grâce à la relation $\gamma\mathfrak{j} \subset \mathfrak{j}$, on a une relation matricielle : $\gamma[\alpha_i] = M \times [\alpha_i]$; où M est une matrice $n \times n$ à coefficients dans R. On obtient donc un polynôme unitaire à coefficients dans R grâce au determinant ; ce qui termine la preuve. □

On peut tirer de ce théorème, trois conséquences :

Conséquence 3.1.4 (Loi de simplification). *Si* $\mathfrak{a}$*,* $\mathfrak{b}$ *et* $\mathfrak{c}$ *sont des idéaux non nuls de* R*, et* $\mathfrak{ab} = \mathfrak{ac}$*, alors* $\mathfrak{b} = \mathfrak{c}$*.*

Démonstration : Il existe un idéal $\mathfrak{j}$ tel que $\mathfrak{aj} = (\alpha)$. Donc $\alpha\mathfrak{b} = \alpha\mathfrak{c}$, d'où le résultat. □

Définition 3.1.1. *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux non nuls de R, alors on définit la relation $|$ par : $\mathfrak{a}|\mathfrak{b} \Leftrightarrow \exists \mathfrak{c}\ \mathfrak{b} = \mathfrak{ac}$. On dit alors que $\mathfrak{a}$ divise $\mathfrak{b}$.*

Remarque 3.1.1. *La relation de divisibilité des idéaux est une relation réflexive transitive. Elle devient antisymétrique dans l'ensemble des classes d'idéaux défini ci-après.*

Conséquence 3.1.5. *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux non nuls de R, alors $\mathfrak{a}|\mathfrak{b}$ si et seulement si $\mathfrak{a} \supset \mathfrak{b}$*

Démonstration : Une implication est triviale : si $\mathfrak{a}|\mathfrak{b}$ alors $\mathfrak{a} \supset \mathfrak{b}$. Réciproquement, si $\mathfrak{a} \supset \mathfrak{b}$, alors $\exists \mathfrak{j} \exists \alpha\ \mathfrak{aj} = (\alpha)$. Soit $\mathfrak{c} = \frac{1}{\alpha}\mathfrak{jb}$. C'est un idéal de R. Et on a $\mathfrak{ac} = \mathfrak{b}$. □

Définition 3.1.2. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de R, un anneau de Dedekind. On définit la relation $\sim$ par :*

$$\mathfrak{a} \sim \mathfrak{b} \Longleftrightarrow \exists \alpha, \beta \in R,\ \alpha\mathfrak{a} = \beta\mathfrak{b}$$

Proposition 3.1.6. *La relation $\sim$ est une relation d'équivalence compatible avec la multiplication des idéaux. On définit alors l'ensemble des classes comme l'ensemble des idéaux de R quotienté par cette relation.*

Conséquence 3.1.7. *L'ensemble des classes d'idéaux dans un anneau de Dedekind forme un groupe pour la loi de multiplication des idéaux.*

Démonstration : Le neutre est la classe de R, c'est à dire l'ensemble des idéaux principaux. L'associativité et la commutativité découlent de celle de la multiplication entre idéaux ; enfin le théorème 3.1.2 affirme l'existence d'un inverse. □

3.2 Théorème de décomposition des idéaux

Théorème 3.2.1. *Tout idéal non nul de R se décompose de manière unique comme produit d'idéaux premiers.*

Démonstration : Existence : Supposons le contraire, alors l'ensemble des idéaux qui ne vérifient pas le théorème est non vide, et a donc un élément maximal $\mathfrak{m}$ car R est noethérien. $\mathfrak{m} \neq R$ car R est par convention le produit vide d'idéaux, car il est l'unité du semi-groupe des idéaux de R. Donc $\mathfrak{m}$ est inclus dans un idéal premier $\mathfrak{p}$. Donc $\mathfrak{m} = \mathfrak{pi}$ pour un certain idéal $\mathfrak{i}$. Donc $\mathfrak{i}$ contient $\mathfrak{m}$. Si $\mathfrak{i} = \mathfrak{m}$, alors $\mathfrak{m} = \mathfrak{pm}$, et on a donc $\mathfrak{p} = R$, ce qui est absurde. Ainsi, $\mathfrak{i}$ est strictement plus gros que $\mathfrak{m}$, et est donc produit d'idéaux premiers, et par conséquent $\mathfrak{m}$ aussi, ce qui est absurde.

Unicité : Supposons que $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, où les $\mathfrak{p}_i$ et $\mathfrak{q}_i$ sont des idéaux premiers non nécessairement distincts. Donc $\mathfrak{p}_1 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$, ce qui implique que $\mathfrak{p}_1 \supset \mathfrak{q}_i$, pour un certain i (regarder la preuve du lemme du théorème concernant l'existence d'un inverse pour les idéaux). On peut donc supposer, quitte à réindexer que $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Donc $\mathfrak{p}_1 = \mathfrak{q}_1$, par maximalité des idéaux premiers. Grâce à la loi de simplification 3.1.4, on a $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Ce qui nous permet de déduire en itérant que $r = s$ et $\mathfrak{p}_i = \mathfrak{q}_i$ pour tout i quitte à réindexer. □

Corollaire 3.2.2. *Les idéaux d'un anneau d'entiers $\mathcal{O}_\mathbf{K}$ se décomposent de manière unique en produit d'idéaux premiers.*

Théorème 3.2.3. *Un anneau de Dedekind est principal si, et seulement si, il est factoriel.*

Démonstration : On sait que principal implique factoriel. Supposons que l'anneau de Dedekind R n'est pas principal. Soit $\mathfrak{p}$ un premier non principal (il en existe d'après le théorème 3.2.1 ; sinon tout idéal serait principal). On considère alors l'ensemble des idéaux $\mathfrak{i}$ tels que $\mathfrak{pi}$ est principal ; le théorème 3.1.2 montre que cet ensemble est non vide, on peut donc fixer un élément maximal $\mathfrak{m}$. $\mathfrak{pm} = (\alpha)$. Donc α est un élément irréductible, car sinon, si $\alpha = \beta\gamma$, alors soit (β), soit (γ) serait de la forme $\mathfrak{pj}$ pour un certain $\mathfrak{j}$. La maximalité de $\mathfrak{m}$ implique donc $\mathfrak{j} = \mathfrak{m}$, ainsi, soit β, soit γ est une unité.

Soient donc $\delta \in \mathfrak{p} \setminus (\alpha)$ et $\epsilon \in \mathfrak{m} \setminus (\alpha)$ (car $\mathfrak{p}$ et $\mathfrak{m}$ ne sont pas principaux). Donc $\delta\epsilon \in (\alpha)$, mais $\alpha \nmid \delta$ et $\alpha \nmid \epsilon$, ce qui implique que R n'est pas factoriel. □

3.3 Idéaux fractionnaires

Définition 3.3.1. *Un idéal fractionnaire de* $\mathbf{K}$ *est un ensemble de la forme* $\alpha\mathfrak{i}$*, où* $\alpha \in \mathbf{K}$ *et* $\mathfrak{i}$ *est un idéal de* R*.*

Remarque 3.3.1. *La multiplication des idéaux fractionnaires est bien définie par :* $(\alpha\mathfrak{a})(\beta\mathfrak{b}) = \alpha\beta\mathfrak{ab}$ *et ne dépend pas de la représentation choisie.*

Définition 3.3.2. *Soit* $\mathfrak{a}$ *un idéal fractionnaire de* $\mathbf{K}$*, alors on définit* $\mathfrak{a}^{-1}$ *comme* $\{\alpha \in \mathbf{K}/\alpha\mathfrak{a} \subset R\}$*.*

Proposition 3.3.1. *Un sous-ensemble de* $\mathbf{K}$ *est un idéal fractionnaire si, et seulement si c'est un* R*-module de type fini.*

Démonstration : $\mathfrak{i}$, idéal de R, est un $\mathbf{Z}$-module de type fini, c'est donc un R-module de type fini, et $\mathfrak{a} = \alpha\mathfrak{i}$ aussi.

Inversement, si $\mathfrak{a}$ est un R-module de type fini, alors $\exists\alpha_1, \ldots, \alpha_n \in \mathbf{K}$ tels que $\mathfrak{a} = \alpha_1 R + \cdots + \alpha_n R$. En écrivant les α_i sous forme de fractions d'éléments de R, et en multipliant par le produit des dénominateurs $\beta \in R$, on trouve que $\mathfrak{a} = \frac{1}{\beta}(\alpha_1\beta R + \cdots + \alpha_n\beta R)$, avec $\alpha_i\beta \in R$. D'où le résultat. □

Proposition 3.3.2. *On a* $\mathfrak{a}\mathfrak{a}^{-1} = R$*, et* $\mathfrak{a}^{-1}$ *est un idéal fractionnaire de* $\mathbf{K}$*. C'est de plus l'unique idéal fractionnaire ayant cette propriété, on l'appelle inverse de* $\mathfrak{a}$*.*

Démonstration : $\mathfrak{a} = \alpha\mathfrak{i}$. Or il existe $\mathfrak{j}, \beta$ tels que $\mathfrak{ij} = (\beta)$.(voir le théorème 3.1.2). De plus $\mathfrak{j} = \{\gamma \in R/\gamma\mathfrak{i} \subset (\beta)\}$. Donc $\mathfrak{a}^{-1} = \frac{1}{\alpha\beta}\mathfrak{j}$, et par conséquent $\mathfrak{a}\mathfrak{a}^{-1} = R$, et c'est bien un idéal fractionnaire.

Si $\mathfrak{ab} = R$, alors en multipliant par $\mathfrak{a}^{-1}$ on obtient que $\mathfrak{a}^{-1} = \mathfrak{b}$. □

Théorème 3.3.3. *Tout idéal fractionnaire de* $\mathbf{K}$ *s'écrit de manière unique sous la forme* $\mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r}$ *où les* $\mathfrak{p}_i$ *sont des idéaux premiers de* R *et* $m_i \in \mathbf{Z}$*.*

Démonstration : On écrit $\mathfrak{a} = \frac{1}{\alpha}\mathfrak{i}$, avec $\alpha \in R$. Si $\mathfrak{i} = \mathfrak{p}_1^{n_1} \ldots \mathfrak{p}_k^{n_k}$ et $(\alpha) = \mathfrak{p}_1^{l_1} \ldots \mathfrak{p}_k^{l_k}$, avec les n_i et les l_j dans $\mathbf{N}$; alors on vérifie facilement que $\mathfrak{a} = \mathfrak{p}_1^{n_1 - l_1} \ldots \mathfrak{p}_k^{n_k - l_k}$. □

Remarque 3.3.2. *Cela permet de définir l'inverse d'un idéal fractionnaire, et la définition coïncide avec la définition pour un idéal normal.*

4 Théorie de la ramification

4.1 Décomposition des idéaux premiers dans les extensions

Dans cette partie, $\mathbf{K}$ et $\mathbf{L}$ seront des corps de nombres, avec $\mathbf{K} \subset \mathbf{L}$. De plus $\mathcal{O}_\mathbf{K}$ et $\mathcal{O}_\mathbf{L}$ désigneront les anneaux des entiers de $\mathbf{K}$ et $\mathbf{L}$. Le terme idéal premier désignera un idéal premier non nul.

Théorème 4.1.1. *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_\mathbf{K}$ et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_\mathbf{L}$. Les conditions suivantes sont équivalentes :*

1. $\mathfrak{P}|\mathfrak{p}\mathcal{O}_\mathbf{L}$
2. $\mathfrak{P} \supset \mathfrak{p}\mathcal{O}_\mathbf{L}$
3. $\mathfrak{P} \supset \mathfrak{p}$
4. $\mathfrak{P} \cap \mathcal{O}_\mathbf{K} = \mathfrak{p}$
5. $\mathfrak{P} \cap \mathbf{K} = \mathfrak{p}$

Définition 4.1.1. *Quand les conditions équivalentes du théorème sont remplies, on dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$.*

Démonstration : On a $1 \Leftrightarrow 2$ d'après la conséquence 3.1.5 (équivalence entre diviser et contenir). $2 \Leftrightarrow 3$, trivialement car $\mathfrak{P}$ est un idéal de $\mathcal{O}_\mathbf{L}$. $4 \Rightarrow 3$ est clair ; et $4 \Leftrightarrow 5$ car $\mathfrak{P} \subset \mathcal{O}$, où $\mathcal{O}$ désigne l'ensemble des nombres entiers algébriques dans $\mathbf{C}$. Il ne reste plus que $3 \Rightarrow 4$: $\mathfrak{P} \cap \mathcal{O}_\mathbf{K}$ contient $\mathfrak{p}$ et est un idéal de $\mathcal{O}_\mathbf{K}$, donc $\mathfrak{P} \cap \mathcal{O}_\mathbf{K} = \mathcal{O}_\mathbf{K}$ ou $\mathfrak{p}$ car premier équivaut à maximal dans un anneau de Dedekind. Si $\mathfrak{P} \cap \mathcal{O}_\mathbf{K} = \mathcal{O}_\mathbf{K}$, alors $1 \in \mathfrak{P}$, et alors $\mathfrak{P} = \mathcal{O}_\mathbf{L}$, contradiction. □

Théorème 4.1.2. *Tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_\mathbf{L}$ est au-dessus d'un unique idéal premier $\mathfrak{p}$ de $\mathcal{O}_\mathbf{K}$. Tout idéal premier $\mathfrak{p}$ est en-dessous d'au moins un idéal premier $\mathfrak{P}$ de $\mathcal{O}_\mathbf{L}$.*

Démonstration : Montrons que $\mathfrak{P} \cap \mathcal{O}_\mathbf{K}$ est un idéal premier non nul. Il est non nul car il contient la norme de chacun des éléments de $\mathfrak{P}$. De plus, il est premier, car si a et b sont dans $\mathcal{O}_\mathbf{K}$ et $ab \in \mathfrak{P} \cap \mathcal{O}_\mathbf{K}$, alors $a \in \mathfrak{P} \cap \mathcal{O}_\mathbf{K}$ ou $b \in \mathfrak{P} \cap \mathcal{O}_\mathbf{K}$. Enfin il ne contient pas 1, et est donc différent de $\mathcal{O}_\mathbf{K}$. Pour la seconde partie, les idéaux premiers au-dessus de $\mathfrak{p}$ sont les diviseurs de $\mathfrak{p}\mathcal{O}_\mathbf{L}$. Montrons que $\mathfrak{p}\mathcal{O}_\mathbf{L} \neq \mathcal{O}_\mathbf{L}$, et a donc au moins un diviseur. De manière équivalente, nous devons montrer que $1 \notin \mathfrak{p}\mathcal{O}_\mathbf{L}$. D'après le lemme 3.1.3, $\exists \gamma \in \mathbf{K} \setminus \mathcal{O}_\mathbf{K}$ tel que $\gamma\mathfrak{p} \subset \mathcal{O}_\mathbf{K}$. Ainsi $\gamma\mathfrak{p}\mathcal{O}_\mathbf{L} \subset \mathcal{O}_\mathbf{K}\mathcal{O}_\mathbf{L} = \mathcal{O}_\mathbf{L}$. Si $1 \in \mathfrak{p}\mathcal{O}_\mathbf{L}$, alors $\gamma \in \mathcal{O}_\mathbf{L}$, et est donc un entier algébrique, ce qui contredit le choix de γ. □

Remarque 4.1.1. *Les idéaux premiers au-dessus de $\mathfrak{p}$ sont les diviseurs de $\mathfrak{p}\mathcal{O}_\mathbf{L}$.*

Définition 4.1.2. *On appelle indice de ramification de $\mathfrak{P}$ sur $\mathfrak{p}$, la puissance exacte $\mathfrak{P}^e$ de $\mathfrak{P}$ qui divise $\mathfrak{p}\mathcal{O}_\mathbf{L}$, noté $e(\mathfrak{P}|\mathfrak{p})$.*

Proposition 4.1.3. *Soit $\mathfrak{P}$ un idéal premier au-dessus de $\mathfrak{p}$, alors $\mathcal{O}_\mathbf{L}/\mathfrak{P}$ et $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ sont des corps finis, et $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ s'injecte canoniquement dans $\mathcal{O}_\mathbf{L}/\mathfrak{P}$. On appelle degré d'inertie de $\mathfrak{P}$ et on note $f(\mathfrak{P}|\mathfrak{p})$ l'entier $[\mathcal{O}_\mathbf{L}/\mathfrak{P} : \mathcal{O}_\mathbf{K}/\mathfrak{p}]$, .*

Démonstration : $\mathfrak{p}$ et $\mathfrak{P}$ sont maximaux, donc $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ et $\mathcal{O}_\mathbf{L}/\mathfrak{P}$ sont des corps. Ils sont finis, d'après le lemme 2.4.9. On a donc le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_\mathbf{K} & \xrightarrow{i} & \mathcal{O}_\mathbf{L} \\ & & \downarrow \pi \\ & & \mathcal{O}_\mathbf{L}/\mathfrak{P} \end{array}$$

Le noyau de $\pi \circ i$ est $\mathcal{O}_\mathbf{K} \cap \mathfrak{P} = \mathfrak{p}$, d'après le théorème 4.1.1. Il se factorise donc en :

$$\begin{array}{ccc} \mathcal{O}_\mathbf{K} & \xrightarrow{i} & \mathcal{O}_\mathbf{L} \\ \downarrow & & \downarrow \pi \\ \mathcal{O}_\mathbf{K}/\mathfrak{p} & \xrightarrow{i'} & \mathcal{O}_\mathbf{L}/\mathfrak{P} \end{array}$$

Or i' est un morphisme d'anneaux entre corps et est donc injective. □

Proposition 4.1.4. *Si on a trois corps de nombres $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M}$, d'anneaux d'entiers respectifs $\mathcal{O}_\mathbf{K} \subset \mathcal{O}_\mathbf{L} \subset \mathcal{O}_\mathbf{M}$, et des idéaux premiers $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{r}$, alors :*
- $e(\mathfrak{r}|\mathfrak{p}) = e(\mathfrak{r}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p})$
- $f(\mathfrak{r}|\mathfrak{p}) = f(\mathfrak{r}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p})$

Démonstration : On a $\mathfrak{p}\mathcal{O}_\mathbf{L} = \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}\mathfrak{q}_2...\mathfrak{q}_k$. De même : $\mathfrak{q}\mathcal{O}_\mathbf{M} = \mathfrak{r}^{e(\mathfrak{r}|\mathfrak{q})}\mathfrak{r}_2...\mathfrak{r}_n$, donc $\mathfrak{p}\mathcal{O}_\mathbf{M} = (\mathfrak{q}\mathcal{O}_\mathbf{M})^{e(\mathfrak{q}|\mathfrak{p})}(\mathfrak{q}_2\mathcal{O}_\mathbf{M})...(\mathfrak{q}_k\mathcal{O}_\mathbf{M}) = \mathfrak{r}^{e(\mathfrak{q}|\mathfrak{p})e(\mathfrak{r}|\mathfrak{q})}\mathfrak{r}'_{2,1}...\mathfrak{r}'_{k,n_k}$, avec $\mathfrak{r}'_{i,j}$ au-dessus de $\mathfrak{q}_i$, et donc différents de $\mathfrak{r}$. D'où la première égalité par unicité de la décomposition. La deuxième vient du diagramme suivant et de la formule de multiplicativité des degrés (base téléscopique) :

$$\begin{array}{ccccc} \mathcal{O}_\mathbf{K} & \longrightarrow & \mathcal{O}_\mathbf{L} & \longrightarrow & \mathcal{O}_\mathbf{M} \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{O}_\mathbf{K}/\mathfrak{p} & \longrightarrow & \mathcal{O}_\mathbf{L}/\mathfrak{q} & \longrightarrow & \mathcal{O}_\mathbf{M}/\mathfrak{r} \end{array}$$

□

Remarque 4.1.2. *On sait que si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_\mathbf{K}$, alors $\mathfrak{p}$ est au-dessus d'un unique nombre premier $p \in \mathbf{Q}$. Alors $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ est une extension de corps de $\mathbf{Z}/p\mathbf{Z}$, donc $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ est un corps de cardinal p^f où $f = f(\mathfrak{p}|p)$. On sait que $\mathfrak{p}$ contient $p\mathcal{O}_\mathbf{K}$, donc p^f est au plus $|\mathcal{O}_\mathbf{K}/p\mathcal{O}_\mathbf{K}| = p^n$; où $n = [\mathbf{K} : \mathbf{Q}]$ ($\mathcal{O}_\mathbf{K}$ est un groupe abélien libre de rang n). On a donc la relation $f \leq n$. En fait, on a mieux :*

Théorème 4.1.5. *Soit $n = [\mathbf{L} : \mathbf{K}]$ et soient $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, les idéaux premiers de $\mathcal{O}_\mathbf{L}$ au-dessus d'un idéal premier $\mathfrak{p}$ de $\mathcal{O}_\mathbf{K}$. Soient $e_1, \ldots, e_r$ et $f_1, \ldots, f_r$ leurs degrés de ramification et d'inertie respectifs. Alors :*

$$\sum_{i=1}^{r} e_i f_i = n$$

Nous allons démontrer ce théorème en même temps que le suivant. Pour un idéal $\mathfrak{i}$ de $\mathcal{O}_\mathbf{K}$, on rappelle que $|\mathcal{O}_\mathbf{K}/\mathfrak{i}|$ est fini et se note $\|\mathfrak{i}\|$.

Théorème 4.1.6. *Soit $n = [\mathbf{L} : \mathbf{K}]$. Alors :*

1. *Pour les idéaux $\mathfrak{i}$ et $\mathfrak{j}$ de $\mathcal{O}_\mathbf{K}$, on a :*
$$\|\mathfrak{ij}\| = \|\mathfrak{i}\|\|\mathfrak{j}\|$$
2. *Soit $\mathfrak{i}$ un idéal de $\mathcal{O}_\mathbf{K}$, alors :*
$$\|\mathfrak{i}\mathcal{O}_\mathbf{L}\| = \|\mathfrak{i}\|^n$$
3. *Soit $\alpha \in \mathcal{O}_\mathbf{K}$, non nul. Alors :*
$$\|(\alpha)\| = |\,\mathrm{N}_\mathbf{Q}^\mathbf{K}(\alpha)|$$

Démonstration : Nous allons montrer 1 dans le cas où $\mathfrak{i}$ et $\mathfrak{j}$ sont premiers entre eux, puis que $\|\mathfrak{p}^m\| = \|\mathfrak{p}\|^m$ pour tout idéal premier $\mathfrak{p}$. Ce qui impliquera que $\|\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r}\| = \|\mathfrak{p}_1\|^{m_1} \dots \|\mathfrak{p}_r\|^{m_r}$. Le résultat découlera du théorème 3.2.1.

Supposons que $\mathfrak{i}$ et $\mathfrak{j}$ sont premiers entre eux. Alors $\mathfrak{i}+\mathfrak{j} = \mathcal{O}_\mathbf{K}$ et $\mathfrak{i}\cap\mathfrak{j} = \mathfrak{ij}$. D'après le théorème des restes chinois, on a donc un isomorphisme :

$$\mathcal{O}_\mathbf{K}/\mathfrak{ij} \longrightarrow \mathcal{O}_\mathbf{K}/\mathfrak{i} \times \mathcal{O}_\mathbf{K}/\mathfrak{j}$$

On a donc $\|\mathfrak{ij}\| = \|\mathfrak{i}\|\|\mathfrak{j}\|$.

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_\mathbf{K}$. On a une chaîne d'idéaux : $\mathcal{O}_\mathbf{K} \supset \mathfrak{p} \supset \dots \supset \mathfrak{p}^m$. Il suffit donc de montrer que $\|\mathfrak{p}\| = |\mathfrak{p}^k/\mathfrak{p}^{k+1}|$, pour tout k, où les $\mathfrak{p}^k$ sont considérés comme des groupes additifs. Soit $\alpha \in \mathfrak{p}^k \smallsetminus \mathfrak{p}^{k+1}$. On a un isomorphisme clair :

$$\mathcal{O}_\mathbf{K}/\mathfrak{p} \longrightarrow \alpha\mathcal{O}_\mathbf{K}/\alpha\mathfrak{p}$$

Or on a l'inclusion $\alpha\mathcal{O}_\mathbf{K} \subset \mathfrak{p}^k$, ce qui induit :

$$\alpha\mathcal{O}_\mathbf{K} \longrightarrow \mathfrak{p}^k/\mathfrak{p}^{k+1}$$

Le noyau de ce morphisme est $(\alpha\mathcal{O}_\mathbf{K}) \cap \mathfrak{p}^{k+1}$, et l'image $((\alpha\mathcal{O}_\mathbf{K}) + \mathfrak{p}^{k+1})/\mathfrak{p}^{k+1}$. $\mathfrak{p}^k$ est l'exacte puissance de $\mathfrak{p}$ qui divise $\alpha\mathcal{O}_\mathbf{K}$, d'où $(\alpha\mathcal{O}_\mathbf{K}) + \mathfrak{p}^{k+1} = \mathfrak{p}^k$, car c'est le plus grand commun diviseur. $(\alpha\mathcal{O}_\mathbf{K}) \cap \mathfrak{p}^{k+1} = \alpha\mathfrak{p}$ car c'est le plus petit commun multiple de $\alpha\mathcal{O}_\mathbf{K} = \mathfrak{p}^k\mathfrak{q}_1 \cdots \mathfrak{q}_r$ et $\mathfrak{p}^{k+1}$. □

Nous allons ensuite démontrer un cas particulier du théorème 4.1.5 ; dans le cas où $\mathbf{K} = \mathbf{Q}$ et $\mathfrak{p} = p\mathbf{Z}$, pour un nombre premier p.

Démonstration : On a :

$$p\mathcal{O}_\mathbf{L} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

Donc :

$$\|p\mathcal{O}_\mathbf{L}\| = \prod_{i=1}^{r} \|\mathfrak{P}_i\|^{e_i} = \prod_{i=1}^{r} (p^{f_i})^{e_i}$$

On sait de plus que : $\|p\mathcal{O}_\mathbf{L}\| = p^n$, ce qui établit le résultat. □

Pour démontrer le 2 du théorème 4.1.6, nous avons besoin du lemme suivant :

Lemme 4.1.7. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls d'un anneau de Dedekind $\mathbf{R}$, tels que $\mathfrak{b} \subset \mathfrak{a}$ et $\mathfrak{a} \neq \mathbf{R}$. Alors il existe un $\gamma \in \mathbf{K}$, l'anneau des fractions de $\mathbf{R}$, tel que $\gamma\mathfrak{b} \subset \mathbf{R}$ et $\gamma\mathfrak{b} \nsubseteq \mathfrak{a}$.*

Démonstration : Par le théorème 3.1.2, il existe un idéal non nul $\mathfrak{c}$ tel que $\mathfrak{bc} = (\alpha)$. Alors $\mathfrak{bc} \nsubseteq \alpha\mathfrak{a}$, soit $\beta \in \mathfrak{c}$ tel que $\beta\mathfrak{b} \nsubseteq \alpha\mathfrak{a}$. Alors $\gamma = \beta/\alpha$ convient. □

Nous pouvons démontrer le 2 du théorème 4.1.6 :

Démonstration : Il suffit de le démontrer pour $\mathfrak{p}$ idéal premier, et d'appliquer le 1, et le théorème de décomposition en idéaux premiers.

Remarquons que $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$ est un espace vectoriel sur le corps $\mathcal{O}_\mathbf{K}/\mathfrak{p}$, car c'est un anneau qui contient $\mathcal{O}_\mathbf{K}/\mathfrak{p}$. Il faut démontrer que sa dimension est n. Elle est au plus n : en effet, si $\alpha_1, \ldots, \alpha_{n+1} \in \mathcal{O}_\mathbf{L}$, ils sont linéairement dépendants sur $\mathbf{K}$, et donc sur $\mathcal{O}_\mathbf{K}$. Donc il existe $\beta_1, \ldots, \beta_{n+1} \in \mathcal{O}_\mathbf{K}$ non tous nuls tels que $\sum_{i=1}^{n+1} \beta_i\alpha_i = 0$. Il faut réduire l'équation modulo $\mathfrak{p}$. Mais si tous les β_i sont dans $\mathfrak{p}$, alors il faut appliquer le lemme à $\mathfrak{a} = \mathfrak{p}$, et $\mathfrak{b} = (\beta_1, \ldots, \beta_{n+1})$, et on obtient alors le résultat.

Il faut montrer qu'on a bien l'égalité. Soit $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, et considérons les idéaux premiers $\mathfrak{p}_i$ de $\mathcal{O}_\mathbf{K}$ au-dessus de p. Soit $n_i = Dim_{\mathcal{O}_\mathbf{K}/\mathfrak{p}_i}(\mathcal{O}_\mathbf{L}/\mathfrak{p}_i\mathcal{O}_\mathbf{L}) \leq n$. Nous allons montrer l'égalité pour tout i. Soit $e_i = e(\mathfrak{p}_i|p)$ et $f_i = f(\mathfrak{p}_i|p)$. Alors $\sum_i e_i f_i = [\mathbf{K} : \mathbf{Q}] = m$, d'après le cas particulier du théorème 4.1.5. On a $p\mathcal{O}_\mathbf{K} = \prod_i \mathfrak{p}_i^{e_i}$, donc $p\mathcal{O}_\mathbf{L} = \prod_i (\mathfrak{p}_i\mathcal{O}_\mathbf{L})^{e_i}$, d'après le 1, on a $\|p\mathcal{O}_\mathbf{L}\| = \prod_i \|\mathfrak{p}_i\mathcal{O}_\mathbf{L}\|^{e_i} = \prod_i \|\mathfrak{p}_\mathfrak{i}\|^{n_i e_i} = \prod_i (p^{f_i})^{n_i e_i} = p^{mn}$. Donc $mn = \sum e_i f_i n_i$. Comme pour tout i, $n_i \leq n$, et $\sum_i e_i f_i = m$, on a l'égalité pour tout i. □

Démonstration : (cas général du théorème 4.1.5) On a $\mathfrak{p}\mathcal{O}_\mathbf{L} = \prod \mathfrak{P}_i^{e_i}$, d'où :

$$\|\mathfrak{p}\mathcal{O}_\mathbf{L}\| = \prod \|\mathfrak{P}_i\|^{e_i} = \prod \|\mathfrak{p}\|^{f_i e_i} = \|\mathfrak{p}\|^n$$

D'après le théorème 4.1.6 1 et 2 ; et la définition des f_i. D'où le résultat. □

Démonstration : (3 du théorème 4.1.6) Soit $\mathbf{M}$ une extension normale de $\mathbf{Q}$ qui contient $\mathbf{K}$. Pour tout plongement σ de $\mathbf{K}$ dans $\mathbf{C}$, on a $\|\sigma(\alpha)\mathcal{O}_\mathbf{M}\| = \|\alpha\mathcal{O}_\mathbf{M}\|$. En effet, il suffit d'étendre σ en un automorphisme de $\mathbf{M}$, et de constater que $\sigma(\mathcal{O}_\mathbf{M}) = \mathcal{O}_\mathbf{M}$. On a alors le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_\mathbf{M} & \xrightarrow{\sigma} & \mathcal{O}_\mathbf{M} \\ \downarrow & & \downarrow \\ \frac{\mathcal{O}_\mathbf{M}}{\alpha\mathcal{O}_\mathbf{M}} & \xrightarrow{\tau} & \frac{\mathcal{O}_\mathbf{M}}{\sigma(\alpha)\mathcal{O}_\mathbf{M}} \end{array}$$

τ est bijectif (surjectif est clair, et injectif car on a factorisé par le noyau). Soit $N = \mathrm{N}^\mathbf{K}(\alpha)$. On a donc

$$\|N\mathcal{O}_\mathbf{M}\| = \prod_\sigma \|\sigma(\alpha)\mathcal{O}_\mathbf{M}\| = \|\alpha\mathcal{O}_\mathbf{M}\|^n$$

De plus $\|N\mathcal{O}_\mathbf{M}\| = |N|^{nm}$, où $m = [M : K]$, et $\|\alpha\mathcal{O}_\mathbf{M}\| = \|\alpha\mathcal{O}_\mathbf{K}\|^m$, d'après le 2. Donc on en déduit que $\|\alpha\mathcal{O}_\mathbf{K}\| = |N|$. □

Remarque 4.1.3. *Les formules du théorème 4.1.6 sont encore vraies pour les idéaux fractionnaires, en posant pour un idéal fractionnaire* $\mathfrak{a} = \mathfrak{ij}^{-1}$ *:* $\|\mathfrak{a}\| = \frac{\|\mathfrak{i}\|}{\|\mathfrak{j}\|}$.

Théorème 4.1.8. *Soit* $\mathbf{L}$ *une extension normale de* $\mathbf{K}$*,* $\mathfrak{P}_1$ *et* $\mathfrak{P}_2$*, deux idéaux premiers au-dessus de* $\mathfrak{p}$*, idéal premier de* $\mathcal{O}_\mathbf{K}$*. Alors il existe* $\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K})$ *tel que* $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

Démonstration : Supposons que $\sigma(\mathfrak{P}_1) \neq \mathfrak{P}_2$ pour tout $\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K})$. Alors, d'après le théorème des restes chinois, on a une solution du système de congruences :

$$\begin{cases} x \equiv 0 & \mod \mathfrak{P}_2 \\ x \equiv 1 & \mod \sigma(\mathfrak{P}_1) \text{ pour tout } \sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K}) \end{cases}$$

Soit $\alpha \in \mathcal{O}_\mathbf{L}$ une telle solution, nous avons $\mathrm{N}_\mathbf{K}^\mathbf{L}(\alpha) \in \mathcal{O}_\mathbf{K} \cap \mathfrak{P}_2 = \mathfrak{p}$. D'un autre côté, on a $\alpha \notin \sigma(\mathfrak{P}_1)$, ainsi $\sigma^{-1}(\alpha) \notin \mathfrak{P}_1$. Comme $\mathrm{N}_\mathbf{K}^\mathbf{L}(\alpha)$ est le produit des $\sigma^{-1}(\alpha)$, et aucun n'est dans l'idéal premier $\mathfrak{P}_1$, alors $\mathrm{N}_\mathbf{K}^\mathbf{L}(\alpha) \notin \mathfrak{P}_1$, ce qui est une contradiction. □

Corollaire 4.1.9. *Si* $\mathbf{L}$ *est normale sur* $\mathbf{K}$*, et* $\mathfrak{P}_1$,$\mathfrak{P}_2$ *sont deux idéaux premiers au-dessus de* $\mathfrak{p}$*, idéal premier de* $\mathcal{O}_\mathbf{K}$ *; alors* $e(\mathfrak{P}_1|\mathfrak{p}) = e(\mathfrak{P}_2|\mathfrak{p}) = e$ *et* $f(\mathfrak{P}_1|\mathfrak{p}) = f(\mathfrak{P}_2|\mathfrak{p}) = f$*. De plus, si* r *est le nombre d'idéaux premier distincts de* $\mathcal{O}_\mathbf{L}$ *au-dessus de* $\mathfrak{p}$*, alors* $ref = [\mathbf{L} : \mathbf{K}]$*.*

Démonstration : L'égalité des degrés de ramification provient du théorème d'unicité de la décomposition en idéaux premiers ; en effet les $\mathfrak{P}_i$ au-dessus de $\mathfrak{p}$ sont conjugués deux-à-deux dans $\mathbf{L}$ galoisienne. Quant à l'égalité des degrés d'inertie, elle provient de l'isomorphisme induit par un tel σ entre $\mathcal{O}_\mathbf{L}/\mathfrak{P}_1$ et $\mathcal{O}_\mathbf{L}/\mathfrak{P}_2$. La formule en découle directement. □

Définition 4.1.3. *On dit que :*
- $\mathfrak{p}$ *est ramifié si* $e(\mathfrak{P}|\mathfrak{p}) > 1$ *pour un certain* $\mathfrak{P}$ *au-dessus de* $\mathfrak{p}$*.*
- $\mathfrak{p}$ *se ramifie totalement si* $e(\mathfrak{P}|\mathfrak{p}) = n$*. (et donc* $r = 1$ *et* $f(\mathfrak{P}|\mathfrak{p}) = 1$*)*
- $\mathfrak{p}$ *se décompose complètement si* $r = n$*. (et donc* $e_i = f_i = 1$ *pour tout* i*)*
- $\mathfrak{p}$ *est inerte si* $r = e_1 = 1$ *(c-à-d.* $\mathfrak{p}\mathcal{O}_\mathbf{L}$ *est premier)*

Théorème 4.1.10. *Si* $\mathfrak{p}$ *se décompose complètement dans* $\mathbf{L}$*, alors il se décompose aussi complètement dans toutes les extensions intermédiaires.*

Démonstration : Soient $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ dans $\mathbf{L}$ et $\mathfrak{p}' = \mathfrak{P} \cap \mathbf{K}'$, avec $\mathbf{K}'$ une extension intermédiaire. Alors $e(\mathfrak{p}'|p) = f(\mathfrak{p}'|p) = 1$, par multiplicativité dans les tours, et ce pour tout $\mathfrak{P}$, donc pour tout $\mathfrak{p}'$, car il ya toujours un idéal premier au-dessus. Donc $\mathfrak{p}$ se décompose complètement dans $\mathbf{K}'$. □

Théorème 4.1.11. *Soit* p *un nombre premier de* $\mathbf{Z}$*, on suppose que* p *est ramifié dans un anneau d'entiers* $\mathcal{O}_\mathbf{K}$*, alors* $p|\operatorname{disc}(\mathcal{O}_\mathbf{K})$*.*

Démonstration : Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_\mathbf{K}$ tel que $e(\mathfrak{p}|p) > 1$. $p\mathcal{O}_\mathbf{K} = \mathfrak{p}\mathfrak{i}$, où $\mathfrak{i}$ est un idéal divisible par tous les idéaux premiers au-dessus de p.

Soient $\sigma_1, \ldots, \sigma_n$, les plongements de $\mathbf{K}$ dans $\mathbf{C}$, étendus en automorphismes de $\mathbf{L}$, clôture normale de $\mathbf{K}$.

Soit $\alpha_1, \ldots, \alpha_n$ une base intégrale de $\mathcal{O}_\mathbf{K}$. Soit $\alpha \in \mathfrak{i} \setminus p\mathcal{O}_\mathbf{K} \neq \varnothing$ que l'on écrit $\alpha = \sum m_i\alpha_i$, avec $m_i \in \mathbf{Z}$. Comme $\alpha \notin p\mathcal{O}_\mathbf{K}$, alors il y a au moins un des m_i qui n'est pas divisible par p. On peut supposer que $p \nmid m_1$.

Soit $d = \operatorname{disc}(\mathcal{O}_\mathbf{K}) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$; alors il est facile de voir que $\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n) = m_1^2 d$. Il suffit donc de montrer que $p|\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$.

Comme α est dans tous les idéaux premiers de $\mathcal{O}_\mathbf{K}$ au-dessus de p, il est dans tous les idéaux premiers de $\mathcal{O}_\mathbf{L}$ au-dessus de p. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_\mathbf{L}$ au-dessus de p. Alors $\sigma^{-1}(\mathfrak{P})$

est aussi un idéal premier au-dessus de p, et donc $\sigma(\alpha) \in \mathfrak{P}$, pour tout σ. Donc $\mathfrak{P}$ contient $\mathrm{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$. Comme le déterminant est dans $\mathbf{Z}$, il est donc dans $\mathbf{Z} \cap \mathfrak{P} = p\mathbf{Z}$. □

Corollaire 4.1.12. *Il n'y a qu'un nombre fini de nombres premiers ramifiés dans $\mathcal{O}_\mathbf{K}$.*

Corollaire 4.1.13. *Il n'y a qu'un nombre fini d'idéaux premiers de $\mathcal{O}_\mathbf{K}$ qui se ramifient dans $\mathcal{O}_\mathbf{L}$.*

Démonstration : Si $\mathfrak{p}$ est un idéal premier qui se ramifie dans $\mathcal{O}_\mathbf{L}$, alors $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ donc p est un nombre premier qui se ramifie dans $\mathcal{O}_\mathbf{L}$, or ils sont en nombre fini, et il n'y a qu'un nombre fini d'idéaux premiers dans $\mathcal{O}_\mathbf{K}$ au-dessus de chacun d'eux. □

4.2 Ramification dans les corps quadratiques et cyclotomiques

Théorème 4.2.1 (Ramification dans les corps quadratiques). *Soit $\mathbf{K}$ un corps quadratique, $\mathbf{K} = \mathbf{Q}(\sqrt{d})$ avec d sans facteur carré, et soit p un nombre premier. Alors la décomposition de p est donnée par :*

- *si $p|d$, $(p) = (p, \sqrt{d})^2$*
- *si $p = 2$ et d est impair,*

$$(2) = \begin{cases} (2, 1+\sqrt{d})^2 & \text{si } d \equiv 3 \mod 4 \\ (2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2}) & \text{si } d \equiv 1 \mod 8 \\ (2) \text{ (c-à-d. reste premier)} & \text{si } d \equiv 5 \mod 8 \end{cases}$$

- *si p est impair, $p \nmid d$,*

$$(p) = \begin{cases} (p, n+\sqrt{d})(p, n-\sqrt{d}) & \text{si } d \equiv n^2 \mod p \\ (p) \text{ (c-à-d. reste premier)} & \text{si } d \text{ n'est pas un carré modulo } p. \end{cases}$$

Démonstration : $\mathbf{K}$ est une extension normale de $\mathbf{Q}$, $ref = 2$.

Dans le cas où p se décompose, il suffit de vérifier la décomposition : on factorise le produit par p et on montre que l'autre facteur est $\mathcal{O}_\mathbf{K}$ en écrivant 1.

Montrer que p reste premier est équivalent au fait que $f = 2$, c-à-d. que le corps quotient n'est pas réduit à $\mathbf{Z}/p\mathbf{Z}$. Or le polynôme $X^2 - d$ a une racine dans $\mathcal{O}_\mathbf{K}$, donc dans $\mathcal{O}_\mathbf{K}/\mathfrak{p}$, et n'en a pas dans $\mathbf{Z}/p\mathbf{Z}$ si d n'est pas un carré modulo p, donc $\mathcal{O}_\mathbf{K}/\mathfrak{p}$ et $\mathbf{Z}/p\mathbf{Z}$ ne sont pas isomorphes.

De même pour $p = 2$, en considérant $X^2 - X + \frac{1-d}{4}$. En effet, les racines de ce polynôme sont $\frac{\pm\sqrt{d}+1}{2} \in \mathcal{O}_\mathbf{K}$, et il se réduit en $X^2 + X + 1$ dans $\mathbf{Z}/2\mathbf{Z}[X]$, qui n'a pas de racine dans $\mathbf{Z}/2\mathbf{Z}$, mais en a dans $\mathcal{O}_\mathbf{K}/\mathfrak{p}$. □

Théorème 4.2.2 (décomposition dans les corps cyclotomiques). *Soit $\mathbf{K} = \mathbf{Q}(\zeta)$, $\zeta = e^{\frac{2i\pi}{m}}$ une extension cyclotomique, et soit p premier. On écrit $m = p^k n, p \wedge n = 1$. Alors dans la décomposition de p dans $\mathcal{O}_\mathbf{K}$, $e = \varphi(p^k)$ et f est l'ordre (multiplicatif) de p modulo n.*

Démonstration : On sait que l'extension est normale et que $ref = \varphi(m)$.

Posons $\alpha = \zeta^n$ et $\beta = \zeta^{p^k}$ qui sont des racines respectivement p^k-ième et n-ième de l'unité. Le résultat découle immédiatement de la décomposition de p dans $\mathbf{Q}(\alpha)$ et $\mathbf{Q}(\beta)$ en prenant l'extension composée.

Dans $\mathbf{Q}(\alpha)$. On sait que $p = \prod_{i=1,p\nmid i}^{p^k}(1-\alpha^i)$ (lemme 2.6.3). Or si $p \nmid i$, en écrivant $1 = ui + vp$, on a $\frac{1-\alpha}{(1-\alpha^i)} = \sum_{j=0}^{u-1}(\alpha^i)^j \in \mathbf{Z}[\alpha]$, et son inverse est également entier, donc c'est une unité. On peut donc écrire $p = \prod_{i=1,p\nmid i}^{p^k} u_i(1-\alpha) = u(1-\alpha)^{\varphi(p^k)}$, où u est une unité. Donc p est la puissance $\varphi(p^k)$-ième de l'idéal $(1-\alpha)$, et comme $\varphi(p^k) = [\mathbf{Q}(\alpha) : \mathbf{Q}]$, nous avons là la factorisation en idéaux premiers de (p).

On se place désormais dans $\mathbf{Q}(\beta)$, qui est le n-ième corps cyclotomique, et on cherche à calculer le degré d'inertie f.

Montrons tout d'abord que p est non ramifié dans $\mathbf{Q}(\beta)$, par un argument de discriminant. On sait en effet que $\mathcal{O}_{\mathbf{Q}(\beta)} = \mathbf{Z}[\beta]$ (théorème 2.6.4), et d'après la proposition 2.6.1,

$$\mathrm{disc}(\mathbf{Z}[\beta]) = \mathrm{disc}(\beta) \mid n^{\varphi(n)}$$

On sait donc que p se ramifie dans $\mathbf{Q}(\beta)$ si et seulement si il divise $\mathrm{disc}(\mathcal{O}_{\mathbf{Q}(\beta)})$. Donc comme $p \wedge n = 1$, $p \nmid \mathrm{disc}(\mathcal{O}_{\mathbf{Q}(\beta)})$ donc p est non ramifié dans $\mathbf{Q}(\beta)$.

On peut donc écrire $p\mathbf{Z}[\beta] = \mathfrak{p}_1 \dots \mathfrak{p}_r$, et $rf = \varphi(n)$. Montrons que f est l'ordre de p modulo n. Nous disposons d'un isomorphisme :

$$\begin{cases} (\mathbf{Z}/n\mathbf{Z})* & \to & \mathrm{Gal}(\mathbf{Q}(\beta)/\mathbf{Q}) \\ k & \mapsto & \sigma_k : \beta \mapsto \beta^k \end{cases}$$

Donc l'ordre de p est celui de σ_p. Soit $\mathfrak{p}$ au dessus de p, par définition $f = [\mathbf{Z}[\beta]/\mathfrak{p} : \mathbf{Z}/p\mathbf{Z}]$, extension dont le groupe de Galois est cyclique d'ordre f, engendré par le Froebenius $\phi : x \mapsto x^p$. Montrons donc que σ_p et ϕ ont le même ordre.

Or pour tout $k \in \mathbf{Z}$, on a d'une part $\sigma_p^k = id \Leftrightarrow \beta^{p^k} = \beta \Leftrightarrow p^k \equiv 1 \mod n$, et d'autre part $\phi^k = id \Leftrightarrow \beta^{p^k} \equiv \beta \mod \mathfrak{p}$. Soit $l \in [|1..n|]$ tel que $p^k \equiv l \mod n$, $\beta^{p^k} = \beta^l \equiv \beta \mod \mathfrak{p}$, donc $\beta^{l-1} \equiv 1 \mod \mathfrak{p}$, car β est une unité. Or on sait que $(1-\beta)\dots(1-\beta^{n-1}) = n$ (en prenant la dérivée de $X^n - 1$ en 1), donc la condition $n \wedge p = 1$ impose $l = 1$. Ainsi, $\forall k \in \mathbf{Z}, \beta^{p^k} \equiv \beta \mod \mathfrak{p} \Leftrightarrow p^k \equiv 1 \mod n$ c-à-d. $\sigma_p^k = id \Leftrightarrow \phi^k = id$, donc σ_p et ϕ ont le même ordre, f.

On peut maintenant combiner les résultats obtenus dans $\mathbf{Q}(\alpha)$ et $\mathbf{Q}(\beta)$: On considère des premiers $\mathfrak{P}_1 \dots \mathfrak{P}_r$ au dessus de $\mathfrak{p}_1 \dots \mathfrak{p}_r$ respectivement. Alors chaque $\mathfrak{P}_i$ est au dessus de p, donc de $(1-\alpha)$, puisque $p\mathbf{Z}[\alpha] = (1-\alpha)^{\varphi(p^k)}$. On a donc :

$$\begin{aligned} e(\mathfrak{P}_i|p) \geq e(1-\alpha|p) &= \varphi(p^k) \\ f(\mathfrak{P}_i|p) \geq f(\mathfrak{p}_i|p) &= f \end{aligned}$$

Or $rf = \varphi(n)$, donc $\varphi(p^k)rf = \varphi(m)$ et les inégalités ci-dessus sont des égalités. Ainsi, les $\mathfrak{P}_i$ sont les seuls premiers au-dessus de p, et on a bien le résultat sur e et f. □

4.3 Différente

Nous avons vu que le discriminant nous renseigne sur les éventuels nombres premiers ramifiés. Nous verrons avec le théorème 4.4.13 que la réciproque est vraie, cependant ce nombre seul ne permet pas de déterminer la manière dont a lieu la ramification (on voudrait en particulier avoir une idée du degré de ramification). Nous introduisons ici un autre invariant d'une extension, appelé différente, qui nous renseigne avec plus d'acuité à ce sujet. Il s'agit en effet d'un idéal divisible par les seuls idéaux ramifiés, et ce avec une puissance liée à la structure de la ramification, par la formule dite de Hilbert que nous verrons dans la section 4.6. Auparavant, il nous faut définir la différente et montrer comment la calculer.

Définition 4.3.1. *Soient* $\mathbf{K} \subset \mathbf{L}$ *deux corps de nombres. On appelle codifférente de* $\mathcal{O}_\mathbf{L}$ *sur* $\mathcal{O}_\mathbf{K}$ *l'idéal fractionnaire* $\operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K}) = \{x \in \mathbf{L}, \operatorname{Tr}^\mathbf{L}_\mathbf{K}(x\mathcal{O}_\mathbf{L}) \subset \mathcal{O}_\mathbf{K}\}$.

On a $\mathcal{O}_\mathbf{K} \subset \operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$. Justifions le fait que l'on a affaire à un idéal fractionnaire :

Soit (e_i) une $\mathbf{K}$-base entière de $\mathbf{L}$, pour $x = \sum \lambda_i e_i \in \operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$, $\operatorname{Tr}^\mathbf{L}_\mathbf{K}(xe_j) \in \mathcal{O}_\mathbf{K}$ pour tout j. Or $(\operatorname{Tr}^\mathbf{L}_\mathbf{K}(xe_j)) = (\operatorname{Tr}^\mathbf{L}_\mathbf{K}(e_ie_j))(\lambda_i)$, donc (en inversant la matrice), on a $\lambda_i \in \frac{\mathcal{O}_\mathbf{K}}{d}$, où $d = \operatorname{disc}(e_1, \dots e_n) = \det(\operatorname{Tr}^\mathbf{L}_\mathbf{K}(e_ie_j))$. Donc la codifférente est un $\mathcal{O}_\mathbf{K}$module de type fini, de base $\frac{e_i}{d}$, donc un idéal fractionnaire.

Définition 4.3.2. *On appelle différente de* $\mathcal{O}_\mathbf{L}$ *sur* $\mathcal{O}_\mathbf{K}$ *l'idéal*

$$\operatorname{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K}) = \operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})^{-1}$$

Lemme 4.3.1. *Soient* $\mathfrak{a} \subset \mathbf{K}$ *et* $\mathfrak{b} \subset \mathbf{L}$ *des idéaux fractionnaires, alors*

$$\operatorname{Tr}^\mathbf{L}_\mathbf{K}(\mathfrak{b}) \subset \mathfrak{a} \Leftrightarrow \mathfrak{b} \subset \mathfrak{a}\mathcal{O}_\mathbf{L} \operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$$

Démonstration :

$$\begin{aligned}
\operatorname{Tr}^\mathbf{L}_\mathbf{K}(\mathfrak{b}) \subset \mathfrak{a} &\Leftrightarrow \mathfrak{a}^{-1} \operatorname{Tr}^\mathbf{L}_\mathbf{K}(\mathfrak{b}) \subset \mathcal{O}_\mathbf{K} \\
&\Leftrightarrow \operatorname{Tr}^\mathbf{L}_\mathbf{K}(\mathfrak{a}^{-1}\mathfrak{b}) \subset \mathcal{O}_\mathbf{K}, \text{car } \mathfrak{a}^{-1} \subset \mathbf{K}, \text{ et la trace est } \mathbf{K}\text{-linéaire} \\
&\Leftrightarrow \mathfrak{a}^{-1}\mathfrak{b} \subset \operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})
\end{aligned}$$

□

Proposition 4.3.2. *La différente est multiplicative dans les tours d'extensions.*

$$\operatorname{diff}(\mathcal{O}_\mathbf{M}|\mathcal{O}_\mathbf{K}) = \operatorname{diff}(\mathcal{O}_\mathbf{M}|\mathcal{O}_\mathbf{L})(\operatorname{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})\mathcal{O}_\mathbf{M})$$

Démonstration : On considère des extensions $\mathbf{K} \subset \mathcal{O}_\mathbf{L} \subset \mathbf{M}$.

$$\begin{aligned}
x \in \operatorname{codiff}(\mathcal{O}_\mathbf{M}|\mathcal{O}_\mathbf{L}) &\Leftrightarrow \operatorname{Tr}^\mathbf{M}_\mathbf{K}(x\mathcal{O}_\mathbf{M}) \subset \mathcal{O}_\mathbf{K} \\
&\Leftrightarrow \operatorname{Tr}^\mathbf{L}_\mathbf{K}(\operatorname{Tr}^\mathbf{M}_\mathbf{L}(x\mathcal{O}_\mathbf{M})) \subset \mathcal{O}_\mathbf{K} \\
&\Leftrightarrow \operatorname{Tr}^\mathbf{M}_\mathbf{L}(x\mathcal{O}_\mathbf{M}) \subset \operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K}) \text{ par définition} \\
&\Leftrightarrow x\mathcal{O}_\mathbf{M} \subset \operatorname{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K}) \operatorname{codiff}(\mathcal{O}_\mathbf{M}|\mathcal{O}_\mathbf{L}) \text{ d'après le lemme.}
\end{aligned}$$

Ainsi, en prenant l'inverse,

$$\operatorname{diff}(\mathcal{O}_\mathbf{M}|\mathcal{O}_\mathbf{K}) = \operatorname{diff}(\mathcal{O}_\mathbf{M}|\mathcal{O}_\mathbf{L})(\operatorname{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})\mathcal{O}_\mathbf{M})$$

□

Théorème 4.3.3. *Soit* $\mathfrak{P}$ *un idéal premier de* $\mathcal{O}_\mathbf{L}$ *au-dessus de* $\mathfrak{p}$. *Alors,* $\mathfrak{P}$ *ramifié* $\Leftrightarrow \mathfrak{P} \mid \operatorname{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$.

Nous allons avoir besoin de deux lemmes pour démontrer ce théorème :

Lemme 4.3.4.

1. *Le* $\mathcal{O}_\mathbf{K}/\mathfrak{p}$*-espace vectoriel* $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$ *est de dimension* $[\mathbf{L} : \mathbf{K}]$.

2. *Si (e_i) est une famille d'éléments de $\mathcal{O}_\mathbf{L}$ dont l'image dans $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$ est $\mathcal{O}_\mathbf{K}/\mathfrak{p}$-libre, alors les e_i forment une famille libre de $\mathbf{L}/\mathbf{K}$.*
3. *De plus, si $\mathfrak{P}$ divise $\mathfrak{p}\mathcal{O}_\mathbf{L}$ et si les e_i forment une base de $\mathbf{L}/\mathbf{K}$, alors $\mathrm{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$ a même valuation en $\mathfrak{P}$ que l'idéal engendré par la différente de $\sum_{i=1}^n \mathcal{O}_\mathbf{K} e_i$.*
4. *Si $x \in \mathcal{O}_\mathbf{L}$, alors $\mathrm{Tr}_\mathbf{K}^\mathbf{L}(x) \mod \mathfrak{p}$ est la trace de l'endomorphisme $\mathcal{O}_\mathbf{K}/\mathfrak{p}$-linéaire de mutliplication par $\bar{x}$ dans $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$.*

Démonstration : On a vu dans la démonstration du théorème 4.1.6 que $|\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}| = |\mathcal{O}_\mathbf{K}/\mathfrak{p}|^n$ avec $n = [\mathbf{L} : \mathbf{K}]$. Cela conclut la première assertion.

Vérifions maintenant le 2. Soit (e_i) une famille d'éléments de $\mathcal{O}_\mathbf{L}$ dont l'image dans $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$ est libre sur $\mathcal{O}_\mathbf{K}/\mathfrak{p}$, montrons qu'elle est libre dans $\mathcal{O}_\mathbf{L}/\mathfrak{p}^r\mathcal{O}_\mathbf{L}$ pour tout r. Supposons donc que

$$\sum x_i e_i \in \mathfrak{p}^r \mathcal{O}_\mathbf{L} \Rightarrow x_i \in \mathfrak{p}^r$$

et montrons le pour $r+1$ par induction (c'est l'hypothèse pour $r = 1$). Considérons donc la relation

$$\sum_i x_i e_i = 0 \mod \mathfrak{p}^{r+1}\mathcal{O}_\mathbf{L}$$

avec les x_i dans $\mathcal{O}_\mathbf{K}$. En particulier la somme est nulle modulo $\mathfrak{p}^r$, donc par hypothèse de récurrence tous les x_i sont dans $\mathfrak{p}^r$. Mais $\mathfrak{p}^r/\mathfrak{p}^{r+1}$ est un $\mathcal{O}_\mathbf{K}/\mathfrak{p}$-espace vectoriel de dimension 1, car $|\mathfrak{p}^r/\mathfrak{p}^{r+1}| = |(\mathcal{O}_\mathbf{K}/\mathfrak{p}^{r+1})/(\mathcal{O}_\mathbf{K}/\mathfrak{p}^r)| = \|\mathfrak{p}\|^{r+1}/\|\mathfrak{p}\|^r = \|\mathfrak{p}\|$. Fixons $t \in \mathfrak{p}^r$ un générateur, on peut écrire $x_i = a_i t \mod \mathfrak{p}^r$, $a_i \in \mathcal{O}_\mathbf{K}/\mathfrak{p}$. On en déduit que $t(\sum_i a_i \overline{e_i}) = 0$ dans $\mathfrak{p}^r\mathcal{O}_\mathbf{L}/\mathfrak{p}^{r+1}\mathcal{O}_\mathbf{L}$. Mais on montre de la même manière que la multiplication par t induit un isomorphisme de $\mathcal{O}_\mathbf{K}/\mathfrak{p}$-espaces vectoriels $\mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L} \to \mathfrak{p}^r\mathcal{O}_\mathbf{L}/\mathfrak{p}^{r+1}\mathcal{O}_\mathbf{L}$. On en déduit que $\sum_i a_i \overline{e_i} = 0 \in \mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$, puis que $a_i = 0$ pour tout i par l'hypothèse ($r = 1$). Ce qui prouve la récurrence. Pour prouver 2, supposons que $\sum_i x_i e_i = 0$, avec $x_i \in \mathbf{K}$. On peut supposer que les x_i sont dans $\mathcal{O}_\mathbf{K}$ en multipliant cette relation par un dénominateur commun. La récurrence implique alors que chaque x_i est dans $\cap_{r\geq 1}\mathfrak{p}^r = \{0\}$, d'où le résultat.

Vérifions maintenant 3. Soit (e_i) une famille de éléments de $\mathcal{O}_\mathbf{L}$ comme dans 2, qui est de plus une $\mathcal{O}_\mathbf{K}/\mathfrak{p}$-base modulo $\mathfrak{p}\mathcal{O}_\mathbf{L}$. C'est donc une base de $\mathbf{L}/\mathbf{K}$ d'après 1. Considérons le $\mathcal{O}_\mathbf{K}$-module $S = \oplus_{i=1}^n \mathcal{O}_\mathbf{K} e_i$. Par construction $\mathfrak{p}\mathcal{O}_\mathbf{L} + S = \mathcal{O}_\mathbf{L}$. Ainsi, le $\mathcal{O}_\mathbf{K}$-module $N = \mathcal{O}_\mathbf{L}/S$ (de type fini car $\mathcal{O}_\mathbf{L}$ l'est) satisfait $N/\mathfrak{p}N = 0$, c-à-d. $N = \mathfrak{p}N$. En particulier, si $\mathfrak{A}\mathfrak{p}N = 0$ pour un idéal $\mathfrak{A}$ de $\mathcal{O}_\mathbf{L}$, alors $\mathfrak{A}N = 0$. Comme (e_i) est une $\mathbf{K}$-base de $\mathbf{L}$, N est de torsion et donc $\mathfrak{I} = \{x \in \mathcal{O}_\mathbf{K}, x\mathcal{O}_\mathbf{L} \subset S\} = \mathrm{Ann}_{\mathcal{O}_\mathbf{K}}(\mathrm{N})$ est un idéal non nul de $\mathcal{O}_\mathbf{K}$. De plus, $\mathfrak{p}$ ne divise pas $\mathfrak{I}$, car si l'on écrit $\mathfrak{I} = \mathfrak{p}\mathfrak{A}$, on aurait $\mathfrak{p}\mathfrak{A}N = 0$ d'où $\mathfrak{A}\mathbf{N} = 0$, absurde car $\mathfrak{I} \subsetneq \mathfrak{A}$. L'inclusion $\mathfrak{I}\mathcal{O}_\mathbf{L} \subset S \subset \mathcal{O}_\mathbf{L}$ montre que* $\mathrm{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K}) \subset \mathrm{codiff}(S) \subset \mathfrak{I}^{-1}\,\mathrm{codiff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$, puis $\mathfrak{I}\,\mathrm{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K}) \subset \mathrm{diff}(S) \subset \mathrm{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$. Comme $\mathfrak{I}$ est premier à $\mathfrak{p}$, $\mathrm{diff}(S)\mathcal{O}_\mathbf{L}$ a même valuation en $\mathfrak{P}$ que $\mathrm{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$.

Terminons par le 4. On peut donc trouver $s \in \mathfrak{I} \subset \mathcal{O}_\mathbf{K}$ tel que $s \equiv 1 \mod \mathfrak{p}$ par les restes chinois. Si x est dans $\mathcal{O}_\mathbf{L}$, $\mathrm{Tr}_\mathbf{K}^\mathbf{L}(sx) = s\,\mathrm{Tr}_\mathbf{K}^\mathbf{L}(x) \equiv \mathrm{Tr}_\mathbf{K}^\mathbf{L}(x) \mod \mathfrak{p}$, de sorte que la trace est celle de la multiplication par sx définie de S à valeurs dans S (car $s\mathcal{O}_\mathbf{L} \subset S$). Mais S étant libre, cette trace modulo $\mathfrak{p}$ est aussi la trace de l'endomorphisme de multiplication par $\overline{sx}$ dans $S/\mathfrak{p}S = \mathcal{O}_\mathbf{L}/\mathfrak{p}\mathcal{O}_\mathbf{L}$. En effet on a une injection de l'un dans l'autre car $\mathfrak{p}\mathcal{O}_\mathbf{L} \cap S = \mathfrak{p}S$, d'après 2, et ils ont même dimension par 1. On conclut car $s \equiv 1 \mod \mathfrak{p}$. □

Lemme 4.3.5. *Si $\mathbf{k}'/\mathbf{k}$ est une extension finie de corps fini, alors il existe $x \in \mathbf{k}'$ de trace 1 sur $\mathbf{k}$.*

*On utilise ici la codifférente du $\mathcal{O}_\mathbf{K}$-module S, dont la définition est évidente : on remplace $\mathcal{O}_\mathbf{L}$par S.

Démonstration : Disons que $\mathbf{k}'/\mathbf{k}$ est $\mathbf{F}_{q^n}/\mathbf{F}_q$, alors $\mathrm{Tr}_{\mathbf{k}}^{\mathbf{k}'}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}$ est une forme $\mathbf{F}_q$-linéaire. Elle n'est pas identiquement nulle car c'est un polynôme sur $\mathbf{k}'$ de degré $< q^n$, et a donc au plus q^{n-1} racines. Elle prend donc la valeur 1. □

Revenons à la démonstration du théorème :

Démonstration : Tout d'abord, notons que

$$\begin{aligned} \mathfrak{P}|\operatorname{diff}(\mathcal{O}_{\mathbf{L}}|\mathcal{O}_{\mathbf{K}}) &\Leftrightarrow \mathfrak{P}^{-1} \subset \operatorname{codiff}(\mathcal{O}_{\mathbf{L}}|\mathcal{O}_{\mathbf{K}}) \\ &\Leftrightarrow \mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\mathfrak{P}^{-1}) \subset \mathcal{O}_{\mathbf{K}} \text{ par définition} \\ &\Leftrightarrow \mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\mathfrak{p}\mathfrak{P}^{-1}) \subset \mathfrak{p} \\ &\Leftrightarrow \mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\mathfrak{P}^{e-1}\mathfrak{I}) \subset \mathfrak{p} \end{aligned}$$

Une difficulté technique parasite la preuve du théorème, venant de ce que $\mathcal{O}_{\mathbf{K}}$ n'est pas toujours principal (en particulier c'est vrai si $\mathbf{K} = \mathbf{Q}$, mais nous en aurons besoin dans un cadre plus général). Si $\mathcal{O}_{\mathbf{K}}$ est principal, $\mathcal{O}_{\mathbf{L}}$ est un $\mathcal{O}_{\mathbf{K}}$-module libre (donc de rang $[\mathbf{L} : \mathbf{K}]$), mais cela ne tient plus *a priori*. Le lemme des restes chinois et le fait que $\mathfrak{I} + \mathfrak{P}^e = \mathcal{O}_{\mathbf{L}}$ impliquent que la projection canonique

$$\mathcal{O}_{\mathbf{L}}/\mathfrak{p}\mathcal{O}_{\mathbf{L}} \to \mathcal{O}_{\mathbf{L}}/\mathfrak{P}^e \times \mathcal{O}_{\mathbf{L}}/\mathfrak{I},$$

est un isomorphisme d'anneaux. En particulier, d'après le 4 du lemme 4.3.4 il vient que pour tout $z \in \mathcal{O}_{\mathbf{L}}$:

$$\mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(z) \mod \mathfrak{p} = \mathrm{Tr}_{\mathcal{O}_{\mathbf{K}}/\mathfrak{p}}^{\mathcal{O}_{\mathbf{L}}/\mathfrak{p}\mathcal{O}_{\mathbf{L}}}(M_{\bar{z}}) = \mathrm{Tr}_{\mathcal{O}_{\mathbf{K}}/\mathfrak{p}}^{\mathcal{O}_{\mathbf{L}}/\mathfrak{P}^e}(M_a) + \mathrm{Tr}_{\mathcal{O}_{\mathbf{K}}/\mathfrak{p}}^{\mathcal{O}_{\mathbf{L}}/\mathfrak{I}}(M_b), \text{ où } \bar{z} = (a, b)$$

Supposons que $e > 1$. Si $z \in \mathfrak{P}^{e-1}\mathfrak{I} \subset \mathfrak{P}$, alors son image dans $\mathcal{O}_{\mathbf{L}}/\mathfrak{p}\mathcal{O}_{\mathbf{L}}$ est de la forme $(a, 0)$ avec $a \in \bar{\mathfrak{P}}$, donc nilpotent, puis de trace nulle. Ainsi, $\mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(z) \mod \mathfrak{p} = \mathrm{Tr}_{\mathcal{O}_{\mathbf{K}}/\mathfrak{p}}^{\mathcal{O}_{\mathbf{L}}/\mathfrak{p}\mathcal{O}_{\mathbf{L}}}(M_{\bar{x}}) = 0$, et donc $\mathfrak{P}|\operatorname{diff}(\mathcal{O}_{\mathbf{L}}|\mathcal{O}_{\mathbf{K}})$ d'après la première ligne de la démonstration.

De même, si $e = 1$, $\mathcal{O}_{\mathbf{L}}/\mathfrak{P}$ est un corps fini. Soit x comme dans le deuxième lemme. D'après les restes chinois plus haut, on peut trouver $z \in \mathfrak{I}$ tel que $z \equiv x \mod \mathfrak{P}$. Il vient que $\mathrm{Tr}(z) \equiv 1 \mod \mathfrak{p}$, puis $\mathfrak{P}$ ne divise pas $\operatorname{diff}(\mathcal{O}_{\mathbf{L}}|\mathcal{O}_{\mathbf{K}})$. □

Théorème 4.3.6. *Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_{\mathbf{L}}$ au-dessus de $\mathfrak{p}$, totalement ramifié ($e(\mathfrak{P}|\mathfrak{p}) = [\mathbf{L} : \mathbf{K}]$), et $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, de polynôme minimal $f \in \mathbf{K}[X]$. Alors pour tout entier k, on a :*

$$\mathfrak{P}^k \mid \operatorname{diff}(\mathcal{O}_{\mathbf{L}}|\mathcal{O}_{\mathbf{K}}) \Leftrightarrow \mathfrak{P}^k \mid (f'(\pi)) \Leftrightarrow f'(\pi) \in \mathfrak{P}^k$$

Démonstration : Soient π comme dans l'énoncé et $n = [\mathbf{L} : \mathbf{K}]$. D'après l'assertion 3 du lemme précédent, il suffit de voir d'une part que les images de $1, \pi, \ldots, \pi^{n-1}$ sont libres dans $\mathcal{O}_{\mathbf{L}}/\mathfrak{p}\mathcal{O}_{\mathbf{L}}$, et d'autre part que la codifférente de $S = \oplus_{i=0}^{n-1}\mathcal{O}_{\mathbf{K}}\pi^i$ est $f'(\pi)^{-1}S$. Vérifions le premier point. Comme $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, on a montré dans la preuve du théorème 4.1.6 que $\mathfrak{P}^r = \mathcal{O}_{\mathbf{K}}\pi^r + \mathfrak{P}^{r+1}$. Supposons $\sum_{i=0}^{n-1} a_i\pi^i \in \mathfrak{p}\mathcal{O}_{\mathbf{L}}$ avec les $a_i \in \mathcal{O}_{\mathbf{K}}$, $\mathfrak{p}\mathcal{O}_{\mathbf{L}} = \mathfrak{P}^e$. En réduisant cette équation successivement modulo $\mathfrak{P}$, $\mathfrak{P}^2$, etc... il vient que a_0,a_1, etc... sont dans $\mathfrak{p}$, ce que l'on voulait.

Il ne reste qu'à montrer que $\operatorname{codiff}(S) = \{x \in \mathbf{L}, \forall i, \mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(x\pi^i) \subset \mathcal{O}_{\mathbf{K}}\}$ vaut $f'(\pi)^{-1}S$. Si (f_i) est la $\mathbf{K}$-base de $\mathbf{L}$ duale de $1, \pi, \ldots, \pi^{n-1}$ relativement à la forme trace (non dégénérée d'après le théorème 2.3.4), alors il est immédiat que $\operatorname{codiff}(S) = \oplus_{i=1}^{n}\mathcal{O}_{\mathbf{K}}f_i$. Notons $f(X) = \prod_{k=1}^{n}(X - \pi_k)$ le polynôme minimal de π sur $\mathbf{K}$, et montrons que cette base est $\{f_i = \frac{\pi^{n-i-1}}{f'(\pi)}\}$, c'est-à-dire que $\mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\frac{\pi^i}{f'(\pi)}) = \delta_{i,n-1}$.

Par décomposition en éléments simples,

$$\frac{1}{f(X)} = \sum_{k=1}^{n} \frac{1}{f'(\pi_k)(X-\pi_k)}$$

Si l'on considère le développement de $\frac{1}{f(X)}$ en puissances de $\frac{1}{X}$, le terme de plus bas degré est $\frac{1}{X^n}$ car f est unitaire de degré n, ce qui impose sur le membre de droite que :

$$\forall i < n-1, \sum_{k=1}^{n} \frac{\pi_k^i}{f'(\pi_k)} = 0 = \mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\frac{\pi^i}{f'(\pi)}), \text{ et } \sum_{k=1}^{n} \frac{\pi_k^{n-1}}{f'(\pi_k)} = 1 = \mathrm{Tr}_{\mathbf{K}}^{\mathbf{L}}(\frac{\pi^{n-1}}{f'(\pi)})$$

ce qui est bien la relation cherchée. Ainsi, $\mathrm{codiff}(S) = \oplus_{i=1}^{n} \mathcal{O}_{\mathbf{K}} \frac{\pi^{n-i-1}}{f'(\pi)} = \frac{1}{f'(\pi)} S$, et nous avons le résultat par le lemme 4.3.4. □

4.4 Théorie de Galois appliquée à la décomposition des idéaux premiers

Dans cette partie et les deux suivantes, $\mathbf{L}$ est une extension normale de $\mathbf{K}$. G sera le groupe de Galois $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$; son ordre est $n = [\mathbf{L} : \mathbf{K}]$. On fixe $\mathfrak{p}$ un idéal premier de $\mathcal{O}_{\mathbf{K}}$ et $\mathfrak{P}$ un idéal premier de $\mathcal{O}_{\mathbf{L}}$ au dessus de $\mathfrak{p}$. L'indice de ramification et le degré d'inertie ne dépendent pas de $\mathfrak{P}$ choisi, donc on les note e et f. Si il y a r premiers au dessus de $\mathfrak{p}$, alors on a la formule $n = ref$.

Définition 4.4.1. *On définit deux sous-groupes de G importants pour la suite :*
- *Le groupe de décomposition $D = D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G, \sigma\mathfrak{P} = \mathfrak{P}\}$*
- *Le groupe d'inertie $E = E(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G, \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}, \forall \alpha \in \mathcal{O}_{\mathbf{L}}\}$*

Proposition 4.4.1. *Il est clair que D et E sont des sous-groupes de G, et que $E \subset D$.*

Proposition 4.4.2. *Si $\sigma \in G$, alors on a :*

$$D(\sigma\mathfrak{P}|\mathfrak{p}) = \sigma D(\mathfrak{P}|\mathfrak{p})\sigma^{-1}, \text{ et } E(\sigma\mathfrak{P}|\mathfrak{p}) = \sigma E(\mathfrak{P}|\mathfrak{p})\sigma^{-1}$$

Démonstration : On a de manière évidente les inclusions

$$\sigma D(\mathfrak{P}|\mathfrak{p})\sigma^{-1} \subset D(\sigma\mathfrak{P}|\mathfrak{p}) \text{ et } \sigma E(\mathfrak{P}|\mathfrak{p})\sigma^{-1} \subset E(\sigma\mathfrak{P}|\mathfrak{p})$$

En appliquant ce résultat avec σ^{-1} et $\sigma\mathfrak{P}$, on trouve le résultat. □

Remarque 4.4.1. *Si G est abélien, alors E et D ne dépendent que de $\mathfrak{p}$, pas de $\mathfrak{P}$.*

Proposition 4.4.3. *Si $\sigma \in D$ et $\alpha \in \mathfrak{P}^k \setminus \mathfrak{P}^{k+1}$, alors $\sigma(\alpha) \in \mathfrak{P}^k \setminus \mathfrak{P}^{k+1}$.*

Démonstration : Si $\alpha = p_1 \dots p_k$, avec $p_i \in \mathfrak{P}$ alors $\sigma(\alpha) = \sigma(p_1) \dots \sigma(p_k) \in \mathfrak{P}^k$, par définition de D. Donc $\sigma(\mathfrak{P}^k) \subset \mathfrak{P}^k$. Maintenant, si $\exists \alpha \in \mathfrak{P}^k \setminus \mathfrak{P}^{k+1}, \sigma(\alpha) \in \mathfrak{P}^{k+1}$, alors $\alpha = \sigma^n(\alpha) = \sigma^{n-1}(\sigma(\alpha)) \in \mathfrak{P}^{k+1}$, ce qui est une contradiction, d'où le résultat. □

Proposition 4.4.4. *Soit $\sigma \in D$, nous avons alors le diagramme commutatif suivant :*

$$\begin{array}{ccc} \mathcal{O}_{\mathbf{L}} & \xrightarrow{\sigma} & \mathcal{O}_{\mathbf{L}} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{O}_{\mathbf{L}}/\mathfrak{P} & \xrightarrow{\bar{\sigma}} & \mathcal{O}_{\mathbf{L}}/\mathfrak{P} \end{array}$$

avec $\bar{\sigma} \in \mathrm{Gal}(\mathcal{O}_{\mathbf{L}}/\mathfrak{P}/\mathcal{O}_{\mathbf{K}}/\mathfrak{p}) = \bar{G}$.

Démonstration : $\pi \circ \sigma$ est un morphisme d'anneau de noyau $\sigma^{-1}(\mathfrak{P}) = \mathfrak{P}$, donc il se factorise en un morphisme $\bar{\sigma}$ de $\mathcal{O}_{\mathbf{L}}/\mathfrak{P}$ dans lui-même. Ce sont des corps car $\mathfrak{P}$ est premier donc maximal, car $\mathcal{O}_{\mathbf{L}}$ est un anneau de Dedekind, donc le morphisme est injectif, et comme ils sont finis (lemme 2.4.9), c'est un automorphisme. De plus σ fixe point par point $\mathcal{O}_{\mathbf{K}}$, et $\mathfrak{P} \cap \mathcal{O}_{\mathbf{K}} = \mathfrak{p}$, donc $\bar{\sigma}$ fixe $\mathcal{O}_{\mathbf{K}}/p$ point par point. □

Conséquence 4.4.5. *On a un morphisme de groupe :*

$$\Psi : \left\{ \begin{array}{ccc} D & \longrightarrow & \bar{G} \\ \sigma & \longmapsto & \bar{\sigma} \end{array} \right.$$

Son noyau est E et donc :
- $E \triangleleft D$
- $Im(\Psi) \simeq D/E$

Démonstration : clair, par définition de E. □

Remarque 4.4.2. *Nous allons bientôt voir que Ψ est en fait surjectif, et donc que $\bar{G} \simeq D/E$. De plus, on sait que $\bar{G}$ est cyclique d'ordre f, donc D/E le sera aussi.*

Notation : Si H est un sous-groupe de G, nous noterons L^H le sous-corps de $\mathbf{L}$ des invariant par H. Si X est une partie de $\mathbf{L}$, alors X^H sera $X \cap L^H$, donc $\mathcal{O}_{\mathbf{L}}^H$ sera l'anneau des entiers de L^H, et $\mathfrak{P}^H$, l'unique idéal premier de $\mathcal{O}_{\mathbf{L}}^H$, en dessous de $\mathfrak{P}$. De plus $\mathfrak{P}^H$ est au-dessus de $\mathfrak{p}$, et donc $\mathcal{O}_{\mathbf{L}}^H/\mathfrak{P}^H$ est un corps intermédiaire entre $\mathcal{O}_{\mathbf{L}}/\mathfrak{P}$ et $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$.

Théorème 4.4.6. *Nous avons le diagramme suivant :*

Degrés	$\mathbf{L}$	$\mathfrak{P}$	*Indices de ramification*	*Degré d'inertie*
e	|	|	e	1
	$\mathbf{L}^E$	$\mathfrak{P}^E$		
f	|	|	1	f
	$\mathbf{L}^D$	$\mathfrak{P}^D$		
r	|	|	1	1
	$\mathbf{K}$	$\mathfrak{p}$		

$\mathbf{L}^D$ *s'appelle le corps de décomposition, et* $\mathbf{L}^E$*, le corps d'inertie.*

Démonstration : Commençons par montrer que $[\mathbf{L}^D : \mathbf{K}] = r$. D'après la théorie de Galois, on sait que $[\mathbf{L}^D : \mathbf{K}] = [G : D]$. Or chaque classe à droite σD envoie $\mathfrak{P}$ sur $\sigma\mathfrak{P}$, et il est clair que $\sigma D = \tau D \Leftrightarrow \sigma\mathfrak{P} = \tau\mathfrak{P}$. Nous avons donc une bijection entre les classes à droite de D et les $\sigma\mathfrak{P}$. D'après le théorème 4.1.8, cela inclut tout ceux de la décomposition de $\mathfrak{p}\mathcal{O}_{\mathbf{L}}$, et il ne peux y avoir que ceux-là. Comme il y en a r, on a bien le résultat.

Montrons que $e(\mathfrak{P}^D|\mathfrak{p}) = f(\mathfrak{P}^D|\mathfrak{p}) = 1$. Comme L est une extension normale de $\mathbf{L}^D$, et que son groupe de Galois est D, $\mathfrak{P}$ est le seul idéal premier de $\mathcal{O}_{\mathbf{L}}$ au-dessus de $\mathfrak{P}^D$, car ils sont necessairement permutés de manière transitive par D. D'après le théorème 4.1.5 : $[\mathbf{L} : \mathbf{L}^D] = e(\mathfrak{P}|\mathfrak{P}^D)f(\mathfrak{P}|\mathfrak{P}^D)$. Le nombre de gauche est ef, car on a déja vu que $[\mathbf{L}^D : \mathbf{K}] = r$ et $ref = n$. D'après la multiplicativité de e et f (cf proposition 4.1.4), donc on a bien le résultat souhaité.

Montrons que $f(\mathfrak{P}|\mathfrak{P}^E) = 1$, ce qui équivaut à montrer que $\mathcal{O}_{\mathbf{L}}/\mathfrak{P} = \mathcal{O}_{\mathbf{L}}^E/\mathfrak{P}^E$. Il suffit donc de montrer que $\mathrm{Gal}((\mathcal{O}_{\mathbf{L}}/\mathfrak{P})/(\mathcal{O}_{\mathbf{L}}^E/\mathfrak{P}^E))$ est trivial. Soit $\theta \in \mathcal{O}_{\mathbf{L}}/\mathfrak{P}$, il faut montrer que $\theta \in \mathcal{O}_{\mathbf{L}}^E/\mathfrak{P}^E$.

Nous allons montrer pour cela que le polynôme $(X-\theta)^m$ est à coefficients dans $\mathcal{O}_{\mathbf{L}}^E/\mathfrak{P}^E$, pour un certain $m>0$. Dans ce cas le groupe de Galois envoie θ sur un de ses conjugués qui ne pourra être que θ, et on aura le résultat souhaité. Soit $\alpha \in \mathcal{O}_{\mathbf{L}}$ correspondant à $\theta \in \mathcal{O}_{\mathbf{L}}/\mathfrak{P}$, par la projection canonique. Alors

$$P(X) = \prod_{\sigma \in E} (X - \sigma(\alpha))$$

est à coefficients dans $\mathcal{O}_{\mathbf{L}}^E$; en réduisant modulo $\mathfrak{P}$, on trouve $\bar{P} \in (\mathcal{O}_{\mathbf{L}}/\mathfrak{P})[X]$, qui a ses coefficients dans $\mathcal{O}_{\mathbf{L}}^E/\mathfrak{P}^E$. Mais tous les $\sigma(\alpha)$ se réduisent en θ, par définition de E. Donc $\bar{P}(X) = (X-\theta)^{|E|}$.

Ainsi, $\forall \theta \in \mathcal{O}_{\mathbf{L}}/PP, \forall \sigma \in \mathrm{Gal}((\mathcal{O}_{\mathbf{L}}/\mathfrak{P})/(\mathcal{O}_{\mathbf{L}}^E/\mathfrak{P}^E)), \sigma(\theta) = \theta$ c-à-d. $\sigma = id$, ce qui prouve $f(\mathfrak{P}|\mathfrak{P}^E) = 1$.

Avec $f(\mathfrak{P}^D|\mathfrak{p}) = 1$, on a $f(\mathfrak{P}^E|\mathfrak{P}^D) = f(\mathfrak{P}|\mathfrak{p}) = f$. Donc, d'après le théorème 4.1.5, $[\mathbf{L}^E : \mathbf{L}^D] \geq f$. Mais nous avons vu que $E \lhd D$, et que D/E se plonge dans $\bar{G}$, de cardinal f. Donc $\mathbf{L}^D \subset \mathbf{L}^E$ est normale, de groupe de Galois D/E, et donc $[\mathbf{L}^E : \mathbf{L}^D] = |D/E| \leq f$, donc on a l'égalité. Donc on en déduit que $e(\mathfrak{P}^E|\mathfrak{P}^D) = 1$. Finalement, on en déduit facilement que $[\mathbf{L} : \mathbf{L}^E] = e$, et que $e(\mathfrak{P}|\mathfrak{P}^E) = e$. □

Corollaire 4.4.7. *D/E est cyclique d'ordre f.*

Démonstration : On a déja vu que D/E se plonge dans $\bar{G}$ qui est cyclique d'ordre f. De plus, les deux groupes ont même cardinal f car $|D/E| = [\mathbf{L}^E : \mathbf{L}^D]$, d'où le résultat. □

Corollaire 4.4.8. *Supposons que D est distingué dans G, alors $\mathfrak{p}$ se décompose en r facteurs premiers distincts dans $\mathbf{L}^D$; si de plus E est aussi distingué dans G, alors chacun d'eux est inerte dans $\mathbf{L}^E$. Finalement, chacun devient une puissance $e-$ième d'un idéal premier dans $\mathbf{L}$.*

Démonstration : Si $D \lhd G$, alors $\mathbf{L}^D$ est une extension normale de $\mathbf{K}$, et donc comme $\mathfrak{P}^D$ à un indice de ramification et un degré d'inertie égaux à 1, tous ses conjugués aussi, et donc $r = n$, d'après le corollaire du théorème 4.1.5. Donc, il y a exactement r idéaux premiers au-dessus de $\mathfrak{p}$ dans $\mathbf{L}^E$, car c'est vrai dans $\mathbf{L}$ et dans $\mathbf{L}^E$, donc chaque idéal premier $\bar{\mathfrak{p}}$ au-dessus de $\mathfrak{p}$, dans $\mathbf{L}^D$, est en-dessous d'exactement un idéal premier $\tilde{\mathfrak{p}}$ de $\mathbf{L}^E$. Si, de plus $E \lhd G$, alors $\mathbf{L}^E$ est une extension normale de $\mathbf{K}$, et donc $e(\tilde{\mathfrak{p}}|\mathfrak{p}) = e(\mathfrak{P}^E|\mathfrak{p}) = 1$. Donc $e(\tilde{\mathfrak{p}}|\bar{\mathfrak{p}}) = 1$. Donc $\bar{\mathfrak{p}}$ est inerte dans $\mathbf{L}^E$, $\tilde{\mathfrak{p}} = \bar{\mathfrak{p}}\mathcal{O}_{\mathbf{L}}^E$. Enfin, il n'y a forcément qu'un seul idéal premier dans $\mathbf{L}$ au-dessus de $\tilde{\mathfrak{p}}$, et par multiplicativité dans les tours, $\tilde{\mathfrak{p}}$ devient une puissance $e-$ième. □

Soit $\mathbf{K}'$, un corps intermédiaire entre $\mathbf{K}$ et $\mathbf{L}$. Il existe H un sous-groupe de G tel que $\mathbf{K}' = \mathbf{L}^H$. L'anneau des entiers de $\mathbf{K}'$ est $\mathcal{O}_{\mathbf{L}}^H$. Soit $\mathfrak{p}' = \mathfrak{P} \cap \mathcal{O}_{\mathbf{K}'}$, l'unique idéal premier de $\mathcal{O}_{\mathbf{K}'}$ en dessous de $\mathfrak{P}$, alors $\mathfrak{p}'$ est au-dessus de $\mathfrak{p}$. $\mathbf{L}$ est une extension normale de $\mathbf{K}'$, et on a :

$$D(\mathfrak{P}|\mathfrak{p}') = D \cap H$$

$$E(\mathfrak{P}|\mathfrak{p}') = E \cap H$$

On en déduit, de par la théorie de Galois, que $\mathbf{L}^D\mathbf{K}'$ et $\mathbf{L}^E\mathbf{K}'$ sont les corps de décomposition et d'inertie pour $\mathfrak{P}$ sur $\mathfrak{p}'$. De plus, on a les caractérisations :

Théorème 4.4.9. *Avec les notations ci-dessus :*

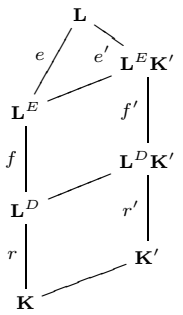
1. *$\mathbf{L}^D$ est le plus grand corps intermédiaire $\mathbf{K}'$ tel que $e(\mathfrak{p}'|\mathfrak{p}) = f(\mathfrak{p}'|\mathfrak{p}) = 1$*

2. $\mathbf{L}^D$ *est le plus petit corps intermédiaire* $\mathbf{K}'$ *tel que* $\mathfrak{P}$ *est le seul idéal premier de* $\mathcal{O}_\mathbf{L}$ *au-dessus de* $\mathfrak{p}'$.
3. $\mathbf{L}^E$ *est le plus grand corps intermédiaire* $\mathbf{K}'$ *tel que* $e(\mathfrak{p}'|\mathfrak{p}) = 1$
4. $\mathbf{L}^E$ *est le plus petit corps intermédiaire* $\mathbf{K}'$ *tel que* $\mathfrak{p}'$ *est totalement ramifié dans* $\mathbf{L}$ *(c-à-d.* $e(\mathfrak{P}|\mathfrak{p}') = [\mathbf{L} : \mathbf{K}']$*)*

Démonstration : On a déja démontré que $\mathbf{L}^E$ et $\mathbf{L}^D$ ont ces propriètés.

Si $\mathbf{K}' = \mathbf{L}^H$ est un corps intermédiaire dans lequel $\mathfrak{P}$ est le seul premier au-dessus de $\mathfrak{p}'$. On sait que $\sigma \in H$ envoie $\mathfrak{P}$ sur un autre idéal premier au-dessus de $\mathfrak{p}'$, donc on doit avoir $H \subset D$, ce qui démontre 2.

Supposons maintenant que $e(\mathfrak{p}'|p) = f(\mathfrak{p}'|p) = 1$, alors $e = e'$ et $f = f'$, par multiplicativité dans les tours. Considérons le diagramme suivant :



Nous avons donc $\mathbf{L}^D$ et $\mathbf{L}^D\mathbf{K}'$ qui ont le même indice dans $\mathbf{L}$, et comme on a une inclusion, alors on a l'égalité, et $\mathbf{K}' \subset \mathbf{L}^D$, donc 1 est démontré.

On obtient 3 de la même manière, car on a alors $e = e'$, et donc $\mathbf{K}' \subset \mathbf{L}^E$.

Finalement, si $\mathfrak{p}'$ est totalement ramifié dans $\mathbf{L}$, $[\mathbf{L}^E : \mathbf{K}'] = e'$, et donc d'après le diagramme, $\mathbf{K}' = \mathbf{L}^E\mathbf{K}'$, et donc $\mathbf{L}^E \subset \mathbf{K}'$. □

Corollaire 4.4.10. *Si* $D \triangleleft G$ *(pour un* $\mathfrak{P}$ *au-dessus de* $\mathfrak{p}$*), alors* $\mathfrak{p}$ *se décompose totalement dans* $\mathbf{K}'$ *si et seulement si* $\mathbf{K}' \subset \mathbf{L}^D$.

Démonstration : Si $\mathfrak{p}$ se décompose totalement dans $\mathbf{K}'$, alors si $\mathfrak{p}' = \mathfrak{P} \cap \mathbf{K}'$, alors $e(\mathfrak{p}'|\mathfrak{p}) = f(\mathfrak{p}'|p) = 1$ et donc $\mathbf{L}^D \subset \mathbf{K}'$, d'après le théorème précédent. Inversement, si $\mathbf{K}' \subset \mathbf{L}^D$, le deuxième corollaire du théorème 4.4.6, montre que $\mathfrak{p}$ se décompose totalement dans $\mathbf{L}^D$, et donc aussi dans $\mathbf{K}'$. □

Théorème 4.4.11. *Soit* $\mathbf{K}$ *un corps de nombres, et* $\mathbf{L}$ *et* $\mathbf{M}$ *deux extensions finies de* $\mathbf{K}$. *Soit* $\mathfrak{p}$ *un idéal premier de* $\mathcal{O}_\mathbf{K}$. *Alors :*

- *Si* $\mathfrak{p}$ *est non ramifié dans* $\mathbf{L}$ *et* $\mathbf{M}$*, alors il n'est pas ramifié dans* $\mathbf{LM}$.
- *Si* $\mathfrak{p}$ *se décompose complètement dans* $\mathbf{L}$ *et* $\mathbf{M}$*, alors il se décompose complètement dans* $\mathbf{LM}$.

Démonstration : Soit $\mathbf{F}$ la clôture normale de $\mathbf{LM}$, $\mathfrak{p}'$ un idéal premier au-dessus de $\mathfrak{p}$ dans $\mathcal{O}_\mathbf{LM}$, et $\mathfrak{q}$ un idéal premier de $\mathcal{O}_\mathbf{F}$, au-dessus de $\mathfrak{p}'$. $\mathfrak{q}$ est donc au-dessus de $\mathfrak{p}$.

Si $\mathfrak{p}$ n'est pas ramifié dans $\mathbf{L}$ et dans $\mathbf{M}$, alors si $E = E(\mathfrak{q}|\mathfrak{p})$, alors le corps d'inertie $\mathbf{F}^E$ contient donc $\mathbf{L}$ et $\mathbf{M}$; d'après le théorème 4.4.9. Donc il contient $\mathbf{LM}$, et donc $\mathfrak{p}$ n'est pas ramifié dans $\mathbf{F}$,

et donc pas non plus dans $\mathbf{LM}$.

Si $\mathfrak{p}$ se décompose totalement dans $\mathbf{L}$ et $\mathbf{M}$, alors si $D = D(\mathfrak{q}|\mathfrak{p})$, le corps de décomposition $\mathbf{F}^D$ contient $\mathbf{L}$ et $\mathbf{M}$, donc $\mathbf{LM}$, d'où le résultat. □

Corollaire 4.4.12. *Soient $\mathbf{K} \subset \mathbf{L}$ deux corps de nombres, et $\mathfrak{p}$ un premier dans $\mathcal{O}_\mathbf{K}$. Si $\mathfrak{p}$ est non ramifié ou se décompose complètement dans $\mathbf{L}$, alors c'est aussi vrai dans la clôture galoisienne de $\mathbf{L}$ sur $\mathbf{K}$.*

Démonstration : Si $\mathfrak{p}$ est non ramifié ou se décompose complètement dans $\mathbf{L}$, alors c'est aussi vrai dans $\sigma(L)$, où σ est un $\mathbf{K}-$plongement de $\mathbf{L}$ dans $\mathbf{C}$, et donc d'après le théorème précédent, c'est encore vrai dans la clôture galoisienne. □

Théorème 4.4.13. *Soit $\mathbf{K}$ un corps de nombres, p un premier de $\mathbf{Z}$ qui divise $\operatorname{disc}\mathcal{O}_\mathbf{K}$. Alors p se ramifie dans K.*

Démonstration : Soit $\alpha_1, \dots, \alpha_n$ une base intégrale de $\mathcal{O}_\mathbf{K}$. $\operatorname{disc}\mathcal{O}_\mathbf{K} = \det(\operatorname{Tr}^\mathbf{K}(\alpha_i\alpha_j))$. En réduisant modulo p, on obtient que les lignes de la matrices sont liées dans $\mathbf{Z}/p\mathbf{Z}$, car $p|\operatorname{disc}\mathcal{O}_\mathbf{K}$. Il existe des entiers $m_1, \dots, m_n$, qui ne sont pas tous divisibles par p, tels que :

$$\forall j, \sum_{i=1}^{n} m_i \operatorname{Tr}^\mathbf{K}(\alpha_i\alpha_j) \in p\mathbf{Z}$$

Soit $\alpha = \sum m_i\alpha_i$. On a $\operatorname{Tr}^\mathbf{K}(\alpha\mathcal{O}_\mathbf{K}) \in p\mathbf{Z}$. De plus $\alpha \notin p\mathcal{O}_\mathbf{K}$ parce que les m_i ne sont pas tous divisibles par p. En effet, $\mathcal{O}_\mathbf{K} = p\alpha_1\mathbf{Z} \oplus \cdots \oplus p\alpha_n\mathbf{Z}$.

Supposons que p n'est pas ramifié dans $\mathbf{K}$, $p\mathcal{O}_\mathbf{K}$ est donc produit d'idéaux premiers. Donc un de ces idéaux ne contient pas α (car sinon, il serait dans l'intersection qui est leur ppcm, et donc leur produit $p\mathcal{O}_\mathbf{K}$). Ainsi $\alpha \notin \mathfrak{p}$ pour un $\mathfrak{p}$, idéal premier au-dessus de p.

Soit $\mathbf{L}$, la clôture normale de $\mathbf{K}$ sur $\mathbf{Q}$. p n'est pas ramifié dans $\mathbf{L}$, par le théorème précédent. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_\mathbf{L}$ au-dessus de $\mathfrak{p}$, on a $\alpha \notin \mathfrak{P}$, car sinon $\alpha \in \mathfrak{P} \cap \mathbf{K} = \mathfrak{p}$.

On a : $\operatorname{Tr}^\mathbf{L}(\alpha\mathcal{O}_\mathbf{L}) = \operatorname{Tr}^\mathbf{K}(\operatorname{Tr}^\mathbf{L}_\mathbf{K}(\alpha\mathcal{O}_\mathbf{L})) = \operatorname{Tr}^\mathbf{K}(\alpha \operatorname{Tr}^\mathbf{L}_\mathbf{K}(\mathcal{O}_\mathbf{L})) \subset \operatorname{Tr}^K(\alpha\mathcal{O}_\mathbf{K}) \subset p\mathbf{Z}$.

Soit $\beta \in \mathcal{O}_\mathbf{L}$ tel que $\beta \notin \mathfrak{P}$ et β dans tous les autres idéaux premiers au-dessus de p (il en existe par le théorème des restes chinois). Alors $\forall\gamma \in \mathcal{O}_\mathbf{L}$ on a :

1. $\operatorname{Tr}^\mathbf{L}(\alpha\beta\gamma) \in \mathfrak{P}$
2. $\forall\sigma \in \operatorname{Gal}(\mathbf{L}|\mathbf{Q}) \setminus D(\mathfrak{P}|p), \sigma(\alpha\beta\gamma) \in \mathfrak{P}$

La première assertion découle du fait que $\operatorname{Tr}^\mathbf{L}(\alpha\mathcal{O}_\mathbf{L}) \subset p\mathbf{Z} \subset \mathfrak{P}$. Ensuite, on a $\beta \in \sigma^{-1}(\mathfrak{P}) \neq \mathfrak{P}$, d'où $\sigma(\beta) \in \mathfrak{P}$, d'où la deuxième affirmation.

On en déduit que

$$\forall\gamma \in \mathcal{O}_\mathbf{L}, \sum_{\sigma \in D(\mathfrak{P}|p)} \sigma(\alpha\beta\gamma) \in \mathfrak{P}$$

On sait que les éléments de D induisent un automorphisme de $\mathcal{O}_\mathbf{L}/\mathfrak{P}$, on peut donc réduire modulo $\mathfrak{P}$. On a alors :

$$\forall\gamma \in \mathcal{O}_\mathbf{L}, \sum_{\sigma \in D} \bar{\sigma}(\bar{\alpha}\bar{\beta}\bar{\gamma}) = 0$$

Or $\bar{\alpha}\bar{\beta} \neq 0$, on en déduit que $\forall x \in \mathcal{O}_\mathbf{L}/\mathfrak{P}, \sum_{\sigma\in D} \bar{\sigma}(x) = 0$, mais les $\bar{\sigma}$ sont des automorphismes distincts, car $D/E \simeq D \simeq \bar{G} = \operatorname{Gal}(\mathcal{O}_\mathbf{L}/\mathfrak{P}/\mathbf{Q})$. D'après le lemme d'indépendance de Dedekind, une somme d'automorphismes distincts est non nulle, donc on a une contradiction, et p se ramifie. □

4.5 L'automorphisme de Froebenius

On rappelle le morphisme :

$$\Psi : \left\{ \begin{array}{ccc} D(\mathfrak{P}|\mathfrak{p}) & \longrightarrow & \bar{G} = \mathrm{Gal}((\mathcal{O}_{\mathbf{L}}/\mathfrak{P})/(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})) \\ \sigma & \longmapsto & \bar{\sigma} \end{array} \right.$$

Ce morphisme est surjectif, son noyau est $E(\mathfrak{P}|\mathfrak{p})$, et son image $\bar{G}$ est cyclique d'ordre f.

Définition 4.5.1. *On appelle automorphisme de Froebenius tout élément $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ tel que $\forall x \in \mathcal{O}_{\mathbf{L}}/\mathfrak{P}, \Psi(\sigma)(x) = x^{\|\mathfrak{p}\|}$, qui est un générateur de $\bar{G}$. On a alors :*

$$\forall x \in \mathcal{O}_{\mathbf{L}}, \sigma(x) \equiv x^{\|\mathfrak{p}\|} \mod \mathfrak{P}$$

Remarque 4.5.1. *Si $\sigma \in D$ est un Froebenius, alors σE est l'ensemble de tous les Froebenius de D. Et donc, si E est trivial (ce qui équivaut à $\mathfrak{p}$ non ramifié), il n'y a alors qu'un seul Froebenius, noté $\Phi(\mathfrak{P}|\mathfrak{p})$.*

On suppose que $\mathfrak{p}$ est non ramifié,

Proposition 4.5.1. *$\Phi(\sigma\mathfrak{P}|\mathfrak{p}) = \sigma\Phi(\mathfrak{P}|\mathfrak{p})\sigma^{-1}$, pour tout $\sigma \in G$. Et de plus, $\Phi(\mathfrak{P}|\mathfrak{p})$ est d'ordre f, car on a $\bar{G} \simeq D/E \simeq D$.*

Proposition 4.5.2. *Si G est abélien, alors Φ ne dépend que de $\mathfrak{p}$, et on a*

$$\forall x \in \mathcal{O}_{\mathbf{L}}, \Phi(x) \equiv x^{\|\mathfrak{p}\|} \mod \mathfrak{p}\mathcal{O}_{\mathbf{L}}$$

Démonstration : Cela vient de la proposition précédente (les conjugués de Φ sont encore Φ), et du fait que $\mathfrak{p}\mathcal{O}_{\mathbf{L}} = \prod_{\sigma \in G} \sigma(\mathfrak{p})$. □

4.6 Groupes de ramification

Nous avons vu que les groupes de décomposition et d'inertie D et E de $\mathfrak{P}$ sur $\mathfrak{p}$ nous renseignent sur la structure de l'extension $\mathbf{L}/\mathbf{K}$. Nous allons ici poursuivre cette démarche en résolvant complètement ces groupes, à l'aide de la suite des groupes de ramification V_m.

Définition 4.6.1. *Pour $m \geq 0$, on définit*

$$V_m = \{\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K}), \forall \alpha \in \mathcal{O}_{\mathbf{L}}, \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}^{m+1}\}$$

Proposition 4.6.1. *Les V_m vérifient les propriétés élémentaires suivantes :*
- *$V_0 = E$.*
- *$\forall m, V_{m+1} \subset V_m$ et $V_m \lhd D$.*
- *$V_m = \{id\}$ pour m suffisamment grand.*

Démonstration :
- $V_m \lhd D$: soit $(\sigma, \sigma') \in V_m \times D$, $\forall \alpha \in \mathcal{O}_{\mathbf{L}}, \sigma(\sigma'^{-1}(\alpha)) = \sigma'^{-1}(\alpha) + \beta$ avec $\beta \in \mathfrak{P}^{m+1}$ par définition de V_m, et comme $\sigma \in D$ laisse $\mathfrak{P}$ stable, $\sigma' \circ \sigma \circ \sigma'^{-1}(\alpha) = \alpha + \sigma'(\beta) \equiv \alpha \mod \mathfrak{P}^{m+1}$. Ainsi $V_m \lhd D$.
- Pour montrer que la suite stationne à $\{id\}$, il suffit de voir que $\bigcap V_m = \{id\}$. Or si $\sigma \in \bigcap V_m$, $\forall \alpha \in \mathcal{O}_{\mathbf{L}}, \sigma(\alpha) - \alpha \in \bigcap \mathfrak{P}^m$. Or $\bigcap \mathfrak{P}^m$ est divisible par tous les $\mathfrak{P}^n$ donc est nul (décomposition unique des idéaux). Donc $\sigma = id$.

□

Nous établissons maintenant dans la proposition 4.6.3 un critère d'appartenance aux V_m. Mais commençons par un lemme technique qui nous sera bien utile.

Lemme 4.6.2. *Soient $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, $\gamma \in \mathcal{O}_\mathbf{L}$ et $\sigma \in V_{m-1}, m \geq 1$ tel que $\sigma(\pi) \equiv \gamma\pi \mod \mathfrak{P}^{m+1}$. Alors $\forall \beta \in \mathfrak{P}, \sigma(\beta) \equiv \gamma\beta \mod \mathfrak{P}^{m+1}$.*

Démonstration :
- Soit $\alpha = \pi s \in \pi\mathcal{O}_\mathbf{L}$, alors $\sigma(\alpha) = (\gamma\pi + p_{m+1})(s + p_m)$ avec $p_{m+1} \in \mathfrak{P}^{m+1}$ et $p_m \in \mathfrak{P}^m$, car $\sigma \in V_{m-1}$. Donc $\sigma(\alpha) \equiv \gamma\pi s \equiv \gamma\alpha \mod \mathfrak{P}^{m+1}$ car $\pi \in \mathfrak{P}$.
- Soit maintenant $\alpha \in \mathfrak{P}$. Par définition de π, on a $\pi\mathcal{O}_\mathbf{L} = \mathfrak{P}\mathfrak{M}$ avec $\mathfrak{P} \wedge \mathfrak{M} = 1$, d'où l'existence de $\beta \in \mathfrak{M} \setminus \mathfrak{P}$ tel que $\alpha\beta \in \pi\mathcal{O}_\mathbf{L}$. On peut donc écrire $\sigma(\alpha\beta) = \gamma\alpha\beta + p_{m+1}, p_{m+1} \in \mathfrak{P}^{m+1}$. Or $\sigma(\beta) = \beta + p_m, p_m \in \mathfrak{P}^m$, donc en reportant : $\beta\sigma(\alpha) = \gamma\beta\alpha + p_{m+1} - p_m\sigma(\alpha)$. Or $\alpha, \sigma(\alpha) \in \mathfrak{P}$, donc $\beta\sigma(\alpha) \equiv \gamma\beta\alpha \mod \mathfrak{P}^{m+1}$. Et comme $\beta \notin \mathfrak{P}$, on obtient bien $\forall \alpha \in \mathfrak{P}, \sigma(\alpha) \equiv \gamma\alpha \mod \mathfrak{P}^{m+1}$.

□

Proposition 4.6.3. *Soit $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, alors :*

$$\forall \sigma \in E, \sigma \in V_m \Leftrightarrow \sigma(\pi) \equiv \pi \mod \mathfrak{P}^{m+1}$$

Démonstration : Le sens direct est la définition. Dans l'autre sens, raisonnons par récurrence sur m. Le cas $m = 0$ est trivial. Soit $\sigma \in E$ vérifiant l'hypothèse pour $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, alors par récurrence, $\sigma \in V_{m-1}$. D'après le lemme précédent, appliqué pour $\gamma = 1$, on sait que $\forall \alpha \in \mathfrak{P}, \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}^{m+1}$. De plus, comme $f(\mathfrak{P}|\mathfrak{P}^E) = 1$, on a $\mathcal{O}_\mathbf{L}/\mathfrak{P} \simeq \mathcal{O}_\mathbf{L}^E/\mathfrak{P}^E$, donc $\mathcal{O}_\mathbf{L} = \mathcal{O}_\mathbf{L}^E + \mathfrak{P}$. Or $\mathcal{O}_\mathbf{L}^E$ est stable par $\sigma \in E$, donc $\forall \alpha \in \mathcal{O}_\mathbf{L}, \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}^{m+1}$, donc par définition $\sigma \in V_m$. □

Ce critère nous permet d'établir les résultats de structure suivants :

Proposition 4.6.4. *On a les plongements suivants :*
- *E/V_1 se plonge dans le groupe multiplicatif $(\mathcal{O}_\mathbf{L}/\mathfrak{P})^*$. En particulier, E/V_1 est cyclique d'ordre divisant $\|\mathfrak{P}\| - 1$.*
- *Pour $m \geq 2$, V_{m-1}/V_m se plonge dans le groupe additif $\mathcal{O}_\mathbf{L}/\mathfrak{P}$. On peut donc l'écrire comme somme de groupes cycliques d'ordre p tel que $p = \mathfrak{P} \cap \mathbf{Z}$.*

Corollaire 4.6.5. *V_1 est le p-groupe de Sylow de E. Donc V_1 est non trivial si et seulement si p divise $e(\mathfrak{P}|\mathfrak{p})$.*

Démonstration :
- Construisons le plongement cherché : Soit $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Alors $\pi\mathcal{O}_\mathbf{L} = \mathfrak{P}\mathfrak{M}$ avec $\mathfrak{P} \wedge \mathfrak{M} = 1$, donc par le théorème chinois, il existe $y \in \mathcal{O}_\mathbf{L}$ satisfaisant $\begin{cases} y \equiv 1 \mod \mathfrak{P} \\ y \equiv 0 \mod \mathfrak{M} \end{cases}$
  Soit $\sigma \in E$. On considère $x = \sigma(\pi)y$, qui vérifie alors $\begin{cases} x \equiv \sigma(\pi) \mod \mathfrak{P}^2 \\ x \equiv 0 \mod \mathfrak{M} \end{cases}$ car $\sigma(\pi) \in \mathfrak{P}$, et donc $x \in \mathfrak{P}\mathfrak{M} = \pi\mathcal{O}_\mathbf{L}$.
  Donc il existe $\alpha \in \mathcal{O}_\mathbf{L}$, donné par $x = \pi\alpha$, tel que $\sigma(\pi) \equiv \alpha\pi \mod \mathfrak{P}^2$. De plus α est bien déterminé modulo $\mathfrak{P}$, car si $\pi\alpha \equiv \pi\alpha' \mod \mathfrak{P}^2$, $\alpha \equiv \alpha' \mod \mathfrak{P}$ car $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. Et $\alpha \notin \mathfrak{P}$ car $\sigma(\pi) \notin \mathfrak{P}^2$.

Ceci permet donc de définir une application :

$$\Phi \left\{ \begin{array}{ccc} E & \to & (\mathcal{O}_{\mathbf{L}}/\mathfrak{P})^* \\ \sigma & \mapsto & \alpha_\sigma \end{array} \right.$$

Φ est un morphisme, car :

$$\begin{aligned} \sigma \circ \tau(\pi) &\equiv \sigma(\alpha_\tau \pi) \mod \mathfrak{P}^2 \\ &\equiv \underbrace{\sigma(\alpha_\tau)}_{\equiv \alpha_\tau [\mathfrak{P}]} \underbrace{\alpha_\sigma \pi}_{\in \mathfrak{P}} \mod \mathfrak{P}^2 \\ &\equiv \alpha_\tau \alpha_\sigma \pi \mod \mathfrak{P}^2 \end{aligned}$$

Donc $\alpha_{\sigma\tau} \equiv \alpha_\sigma \alpha_\tau \mod \mathfrak{P}$.
Son noyau est $\{\sigma, \sigma(\pi) \equiv \pi \mod \mathfrak{P}^2\} = V_1$ d'après la proposition 4.6.3. Ainsi en factorisant, on a bien le plongement voulu.

– Soient maintenant $m \geq 2$, $\sigma \in V_{m-1}$, et $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. $\pi\mathcal{O}_{\mathbf{L}} = \mathfrak{P}\mathfrak{M}$, donc $\pi^m = \mathfrak{P}^m\mathfrak{M}^m$ avec $\mathfrak{P} \nmid \mathfrak{M}^m$, donc $\pi^m \in \mathfrak{P}^m \setminus \mathfrak{P}^{m+1}$. Comme précédemment, on construit grâce au théorème chinois y et $x = (\sigma(\pi) - \pi)y$ vérifiant

$$\left\{ \begin{array}{lll} y \equiv 1 \mod \mathfrak{P}^{m+1}, & x \equiv 0 \mod \mathfrak{P}^m \\ y \equiv 0 \mod \mathfrak{M}^m, & x \equiv 0 \mod \mathfrak{M}^m \end{array} \right.$$

Donc $x \in \pi^m\mathcal{O}_{\mathbf{L}}$ s'écrit $\pi^m\alpha$, avec α vérifiant $\sigma(\pi) \equiv \pi + \alpha\pi^m \mod \mathfrak{P}^{m+1}$. De plus cette relation qui le détermine modulo $\mathfrak{P}$, car si α' vérifie la même formule, on a $(\alpha - \alpha')\pi^m \equiv \sigma(\pi) - \pi \mod \mathfrak{P}^{m+1}$, d'où $\alpha - \alpha' \equiv 0 \mod \mathfrak{P}$ car $\sigma(\pi) - \pi \in \mathfrak{P}^m \setminus \mathfrak{P}^{m+1}$, car $\sigma \in V_{m-1}$ et $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$.
Ceci permet de définir

$$\Psi \left\{ \begin{array}{ccc} V_{m-1} & \to & \mathcal{O}_{\mathbf{L}}/\mathfrak{P} \\ \sigma & \mapsto & \alpha_\sigma \end{array} \right.$$

qui est un morphisme :

$$\begin{aligned} \sigma \circ \tau(\pi) &\equiv \sigma(\pi + \alpha_\tau \pi^m) \mod \mathfrak{P}^{m+1} \\ &\equiv \sigma(\pi) + \sigma(\alpha_\tau)\sigma(\pi)^m \mod \mathfrak{P}^{m+1} \\ &\equiv \pi + \alpha_\sigma \pi^m + \alpha_\tau \pi^m \mod \mathfrak{P}^{m+1} \end{aligned}$$

Donc $\alpha_{\sigma\tau} = \alpha_\sigma + \alpha_\tau$, toujours modulo $\mathfrak{P}$.
De plus, d'après la proposition 4.6.3, $\ker \Psi = V_m$, d'où le plongement

$$V_{m-1}/V_m \hookrightarrow (\mathcal{O}_{\mathbf{L}}/\mathfrak{P}, +) \simeq (\mathbf{Z}/p\mathbf{Z})^{f(\mathfrak{P}|p)}$$

□

Nous pouvons être plus précis dans les cas abéliens qui vont nous intéresser.

Proposition 4.6.6. *Si D/V_1 est abélien, alors*[†]

$$E/V_1 \hookrightarrow (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^*$$

En particulier, E/V_1 est cyclique d'ordre divisant $\|\mathfrak{p}\| - 1$.

[†]On remarquera bien la différence avec la proposition 4.6.4, il s'agit ici de $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$, sous-corps de $\mathcal{O}_{\mathbf{L}}/\mathfrak{P}$.

Démonstration : Soit $\phi : x \mapsto x^{\|\mathfrak{p}\|}$ un générateur (appelé automorphisme de Froebenius) de $\mathrm{Gal}(\mathcal{O}_\mathbf{L}/\mathfrak{P}/\mathcal{O}_\mathbf{K}/\mathfrak{p})$. Pour montrer que l'image de Φ est dans $(\mathcal{O}_\mathbf{K}/\mathfrak{p})^*$, il suffit de montrer qu'elle est invariante par ϕ, c'est à dire que $\forall \sigma \in E, \alpha_\sigma \equiv \phi(\alpha_\sigma) \mod \mathfrak{P}$.

Or $\mathrm{Gal}(\mathcal{O}_\mathbf{L}/\mathfrak{P}/\mathcal{O}_\mathbf{K}/\mathfrak{p}) \simeq D/E$, donc en notant encore ϕ un automorphisme de D qui lui correspond (défini modulo E), on a $\forall \alpha \in \mathcal{O}_\mathbf{L}, \phi(\alpha) \equiv \alpha^{\|\mathfrak{P}\|} \mod \mathfrak{P}$, et l'on se ramène donc à montrer que $\forall \sigma \in E, \alpha_\sigma \equiv \alpha_\sigma^{\|\mathfrak{p}\|} \mod \mathfrak{P}$.

Soit comme toujours $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, $\sigma(\pi) \equiv \alpha_\sigma \pi \mod \mathfrak{P}^2$. Si D/V_1 est abélien, alors les commutateurs de D sont dans V_1, donc on peut écrire $\phi\sigma\phi^{-1}\sigma^{-1} = v_1 \in V_1$. Alors $\phi\sigma\phi^{-1}(\pi) \equiv v_1(\alpha_\sigma\pi) \mod \mathfrak{P}^2 \equiv \alpha_\sigma \pi \mod \mathfrak{P}^2$. Or en notant $\beta = \phi^{-1}(\pi) \in \mathfrak{P}$,

$$\begin{aligned}
\sigma(\beta) &\equiv \alpha_\sigma \beta \mod \mathfrak{P}^2 \text{ d'après le lemme 4.6.2,} \\
\text{donc } \phi\sigma\phi^{-1}(\pi) &\equiv (\alpha_\sigma^{\|\mathfrak{p}\|} + q1)\pi \mod \mathfrak{P}^2, q_1 \in \mathfrak{P}, \\
&\equiv \alpha_\sigma^{\|\mathfrak{p}\|}\pi \mod \mathfrak{P}^2 \text{ car } \pi \in \mathfrak{P}. \\
\text{Donc } \alpha_\sigma^{\|\mathfrak{p}\|} &\equiv \alpha_\sigma \mod \mathfrak{P} \text{ car } \pi \in \mathfrak{P} \setminus \mathfrak{P}^2.
\end{aligned}$$

Ainsi, on a bien $\forall \sigma, \alpha_\sigma = \phi(\alpha_\sigma)$ dans $\mathcal{O}_\mathbf{L}/\mathfrak{P}$, soit $\alpha_\sigma \in \mathcal{O}_\mathbf{K}/\mathfrak{p}$. □

Proposition 4.6.7 (formule de Hilbert). *Soit $\mathfrak{P}^k$ la plus grande puissance de $\mathfrak{P}$ divisant* $\mathrm{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K})$. *Alors*

$$k = \sum_{m \geq 0} (|V_m| - 1)$$

Remarque 4.6.1. *En particulier, si $\mathfrak{p}$ est non ramifié, $k = 0$.*

Démonstration : On se place tout d'abord dans L^E, ce qui revient à considérer le cas où $\mathfrak{p}$ est totalement ramifié, ou de manière équivalente que $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K}) = D = E$. Soit $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, de polynôme minimal $f \in \mathbf{K}[X]$. D'après le théorème 4.3.6, $\mathfrak{P}^k$ est de manière équivalente la plus grande puissance de $\mathfrak{P}$ divisant $f'(\pi)$.

Or $f(X) = \prod_{\sigma \in E}(X - \sigma(\pi))$, car $E = G$, et comme $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, on a bien des racines distinctes, car si $\sigma(\pi) = \sigma'(\pi)$, alors $\sigma\sigma'^{-1} \in V_m$ pour tout m, donc $\sigma\sigma'^{-1} = id$. Donc

$$f'(\pi) = \prod_{\sigma \neq 1}(\pi - \sigma(\pi)) = \prod_{m \geq 1} \prod_{\sigma \in V_{m-1} \setminus V_m} (\pi - \sigma(\pi))$$

Or pour $\sigma \in V_{m-1} \setminus V_m$, d'après le critère de la proposition 4.6.3, $\mathfrak{P}^m$ est la plus grande puissance de $\mathfrak{P}$ qui divise $\pi - \sigma(\pi)$. Donc en passant aux valuations sur $\mathfrak{P}$,

$$\begin{aligned}
k &= \sum_{m \geq 1} m|V_{m-1} \setminus V_m| \\
&= \sum_{m \geq 1}^{N} m|V_{m-1}| - \sum_{m \geq 1}^{N} m|V_m| \text{ pour N tel que } V_N = \{id\} \\
&= \sum_{m \geq 0}^{N-1} (m+1)|V_m| - \sum_{m \geq 0}^{N} m|V_m| \\
&= \sum_{m \geq 0}^{N-1} |V_m| - N|V_N| \\
&= \sum_{m \geq 0} (|V_m| - 1)
\end{aligned}$$

Dans le cas général ($\mathbf{K} \neq \mathbf{L}^E$), On sait, d'après la proposition 4.3.2, que $\mathrm{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_\mathbf{K}) = \mathrm{diff}(\mathcal{O}_\mathbf{L}|\mathcal{O}_{L^E})(\mathrm{diff}(\mathcal{O}_{\mathbf{L}^E}|\mathcal{O}_\mathbf{K})\mathcal{O}_\mathbf{L})$. Or

$$\begin{aligned}
\mathfrak{P} \mid \mathrm{diff}(\mathcal{O}_{\mathbf{L}^E}|\mathcal{O}_\mathbf{K})\mathcal{O}_\mathbf{L} &\Leftrightarrow \mathrm{diff}(\mathcal{O}_{\mathbf{L}^E}|\mathcal{O}_\mathbf{K})\mathcal{O}_\mathbf{L} \subset \mathfrak{P} \\
&\Leftrightarrow \mathrm{diff}(\mathcal{O}_{\mathbf{L}^E}|\mathcal{O}_\mathbf{K})\mathcal{O}_\mathbf{L} \cap \mathcal{O}_{\mathbf{L}^E} \subset \mathfrak{P} \cap \mathcal{O}_{\mathbf{L}^E} \\
&\Leftrightarrow \mathrm{diff}(\mathcal{O}_{\mathbf{L}^E}|\mathcal{O}_\mathbf{K}) \subset \mathfrak{P}^E \\
&\Leftrightarrow \mathfrak{P}^E \mid \mathrm{diff}(\mathcal{O}_{\mathbf{L}^E}|\mathcal{O}_\mathbf{K})
\end{aligned}$$

On sait de plus, que $\mathfrak{P}^E$ est non ramifié dans $\mathbf{L}^E$, par définition. Donc $\mathfrak{P}^E \nmid \mathrm{diff}(\mathcal{O}_{\mathbf{L}^E}|\mathcal{O}_\mathbf{K})$, par le théorème 4.3.3. Donc $k = \sum_{m\geq 0}(|V_m(\mathfrak{P}/\mathfrak{P}^E)| - 1)$ or pour tout $m \geq 0$,

$$\begin{aligned}
V_m(\mathfrak{P}/\mathfrak{P}^E) &= \{\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{L}^E) = E(\mathfrak{P}|\mathfrak{p}), \forall \alpha \in \mathcal{O}_\mathbf{L}, \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}^{m+1}\} \\
&= \{\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{K}), \forall \alpha \in \mathcal{O}_\mathbf{L}, \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}^{m+1}\} \cap E(\mathfrak{P}|\mathfrak{p}) \\
&= V_m(\mathfrak{P}/\mathfrak{p}) \cap E(\mathfrak{P}|\mathfrak{p}) \\
&= V_m(\mathfrak{P}/\mathfrak{p})
\end{aligned}$$

D'où le résultat. □

4.7 Exemple de ramification

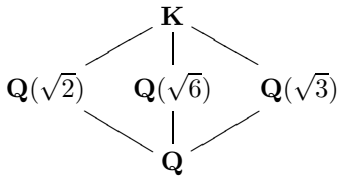
Nous allons ici appliquer les connaissances acquises jusqu'ici pour étudier la ramification dans l'extension galoisienne $\mathbf{K} = \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

Ce corps a été choisi de sorte qu'on ait un nombre premier totalement ramifié, et que la structure soit suffisamment simple pour que les calculs le soient aussi, et les phénomènes bien visibles. Puisque nous connaissons la ramification dans les corps quadratiques, nous avons cherché $\mathbf{K}$ sous la forme d'une extension composée de deux tels corps $\mathbf{Q}(\sqrt{d})$ et $\mathbf{Q}(\sqrt{d'})$. Le fait qu'un premier p soit totalement ramifié dans tous les sous-corps de $\mathbf{K}$ impose qu'il le soit dans $\mathbf{K}$ (car p n'est pas ramifié dans $\mathbf{K}^E$). En examinant la classification, des corps quadratiques, l'existence d'un même premier ramifié dans $\mathbf{Q}(\sqrt{d}), \mathbf{Q}(\sqrt{d'})$ et $\mathbf{Q}(\sqrt{dd'})$ impose

$$p|d, p = 2 \text{ et } d' \equiv 3 \mod 4, p|dd'$$

D'où le choix de $\mathbf{K} = \mathbf{Q}(\sqrt{2}, \sqrt{3})$, dans lequel 2 est totalement ramifié par construction. Nous voyons que 3 est également ramifié, car $3 = (\sqrt{3})^2$. Nous allons montrer que ce sont les seuls, et calculer explicitement leur ramification dans $\mathbf{K}$.

La première chose à faire est de calculer l'anneau $\mathcal{O}_\mathbf{K}$. Nous utilisons pour cela les propriétés de compatibilité de la norme avec les extensions intermédiaires, en considérant les sous-corps de $\mathbf{K}$.



Nous savons en effet que la norme et la trace de tout élément de $\mathbf{K}$ relative à l'un de ses sous-corps est dans l'anneau des entiers de ce sous-corps. Or nous avons calculé ces anneaux d'entiers dans la section 2.5, et l'on a :

$$\mathcal{O}_{\mathbf{Q}(\sqrt{2})} = \mathbf{Z}[\sqrt{2}], \mathcal{O}_{\mathbf{Q}(\sqrt{3})} = \mathbf{Z}[\sqrt{3}], \mathcal{O}_{\mathbf{Q}(\sqrt{6})} = \mathbf{Z}[\sqrt{6}],$$

Notons σ_2, σ_3 et σ_6 les $\mathbf{Q}$ -automorphismes de corps respectifs de $\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{3})$ et $\mathbf{Q}(\sqrt{6})$. Ainsi, $\mathbf{Q}(\sqrt{2})$ est le sous-corps de $\mathbf{K}$ fixé par σ_3.

$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ est une $\mathbf{Q}$ -base de $\mathbf{K}$. Soit $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \mathcal{O}_{\mathbf{K}}$, alors

$$\mathrm{Tr}^{\mathbf{K}}_{\mathbf{Q}(\sqrt{2})}(\alpha) = \alpha + \sigma_3(\alpha) = 2a + 2b\sqrt{2} \in \mathbf{Z}[\sqrt{2}]$$

De même en considérant la trace dans $\mathbf{Q}(\sqrt{3})$ et $\mathbf{Q}(\sqrt{6})$. On obtient alors

$$a, b, c, d \in \frac{1}{2}\mathbf{Z}$$

C'est encore insuffisant, tous les éléments de cette forme ne sont pas entiers. Mais de même, en considérant la norme relative :

$$\mathrm{N}^{\mathbf{K}}_{\mathbf{Q}(\sqrt{2})}(\alpha) = \alpha\sigma_3(\alpha) = (a + b\sqrt{2})^2 - (c\sqrt{3} + d\sqrt{6})^2 \in \mathbf{Z}[\sqrt{2}]$$

et celles correspondant aux autres corps, on obtient les conditions suivantes :

$$\left.\begin{array}{l} a^2 + 2b^2 - 3c^2 - 6d^2 \\ 2ab - 6cd \\ a^2 + 3c^2 - 2b^2 - 6d^2 \\ 2ac - 4bd \\ a^2 + 6d^2 - 2b^2 - 3c^2 \\ 2ad - 2bc \end{array}\right\} \in \mathbf{Z}$$

On en déduit que $2a^2 - 12d^2 \in \mathbf{Z}$, donc $2a^2 \in \mathbf{Z}$ et la même chose pour c, c'est-à-dire $a, c \in \mathbf{Z}$. Les autres équations ne nous apprennent rien de plus.

Nous n'avons pas encore suffisemment de contraintes sur les coefficients, mais il nous reste à utiliser la norme absolue de $\mathbf{K}$ sur $\mathbf{Q}$. La formule obtenue devrait être volumineuse, mais on peut en supprimer au fur-et-à-mesure tous les termes clairement entiers d'après les conditions précédentes, ce qui ne laisse finalement que la contrainte :

$$4b^4 + 36d^4 \in \mathbf{Z}$$

Ainsi, b et d sont soit tous deux entiers, soit tous deux demi-entiers.

Toutes ces conditions permettent d'écrire que tout entier de $\mathcal{O}_{\mathbf{K}}$est de la forme :

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} + e\frac{\sqrt{2} + \sqrt{6}}{2}, a, b, c, d, e \in \mathbf{Z}$$

Réciproquement, comme $\frac{\sqrt{2}+\sqrt{6}}{2}$ est entier (car racine de $X^2 - 1 - 2\sqrt{3}$, $\sqrt{3}$ entier), on a ici exactement l'anneau des entiers. On remarquera également que $\frac{\sqrt{2}+\sqrt{6}}{2}$ est une unité de $\mathcal{O}_{\mathbf{K}}$, que nous noterons u.

Ainsi, en supprimant la redondance,

$$\mathcal{O}_{\mathbf{K}} = \mathbf{Z} + \sqrt{2}\mathbf{Z} + \sqrt{3}\mathbf{Z} + u\mathbf{Z}, u = \frac{\sqrt{2} + \sqrt{6}}{2}$$

De plus, on a ici la chance d'avoir obtenu une $\mathbf{Z}$ -base de $\mathcal{O}_{\mathbf{K}}$, ce qui nous permet de calculer son discriminant :

$$\mathrm{disc}(\mathcal{O}_{\mathbf{K}}) = \begin{vmatrix} 1 & \sqrt{2} & \sqrt{3} & \frac{\sqrt{2}+\sqrt{6}}{2} \\ 1 & -\sqrt{2} & \sqrt{3} & \frac{-\sqrt{2}-\sqrt{6}}{2} \\ 1 & \sqrt{2} & -\sqrt{3} & \frac{\sqrt{2}-\sqrt{6}}{2} \\ 1 & -\sqrt{2} & -\sqrt{3} & \frac{-\sqrt{2}+\sqrt{6}}{2} \end{vmatrix}^2 = (\frac{\sqrt{2}\sqrt{3}\sqrt{6}}{2})^2 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix}^2 = (3.2^4)^2$$

D'après le théorème 4.1.11, on sait donc que 2 et 3 sont les seuls premiers ramifiés dans $\mathbf{K}$.

Nous voulons maintenant calculer les idéaux premiers qui sont au-dessus. Commençons par le faire pour les corps quadratiques intermédiaires, grâce à la classification de la section 4.2.

Commençons par le cas le plus simple, $p = 3$. On trouve alors :

$$(3) = \begin{cases} (3) & \text{dans } \mathbf{Q}(\sqrt{2}) \\ (\sqrt{3})^2 & \text{dans } \mathbf{Q}(\sqrt{3}) \\ (3, \sqrt{6})^2 & \text{dans } \mathbf{Q}(\sqrt{6}) \end{cases}$$

Donc dans $\mathbf{K}$, par multiplicativité de e et f, on a $e \geq 2, f \geq 2$ avec $ref = 4$, donc il existe un unique idéal $\mathfrak{p}_3$ de $\mathcal{O}_\mathbf{K}$ au-dessus de 3, ramifié d'indice 2 et de degré d'inertie 2. Nous considérons l'idéal $\mathfrak{p}_3 = (\sqrt{3})\mathcal{O}_\mathbf{K}$, qui contient 3, et vérifie bien $\mathfrak{p}_3^2 = (3)$. Donc cet idéal est nécessairement l'idéal premier $\mathfrak{p}_3$ cherché (s'il n'était pas premier, cela impliquerait $e > 2$ ou $r > 1$, impossible), et nous savons donc qu'il est de degré d'inertie 2. Nous pouvons le vérifier :

$$\begin{aligned} \mathcal{O}_\mathbf{K}/\mathfrak{p}_3 &= \mathcal{O}_\mathbf{K}/(\sqrt{3}, \sqrt{6}) \text{ car } \sqrt{6} \in (\sqrt{3}) \\ &= (\mathbf{Z} + \frac{\sqrt{2}+\sqrt{6}}{2}\mathbf{Z})/(\sqrt{3}, \sqrt{6}) \\ &= (\mathbf{Z} + \sqrt{2}\mathbf{Z})/(\sqrt{3}) \text{ car } \frac{1}{2} = 2 \text{ car } 3 = 0 \\ &= \mathbf{Z}[X]/(X^2 - 2, \sqrt{3}) \\ &= \mathbf{Z}/3\mathbf{Z}[X]/(X^2 + 1) = \mathbf{F}_9 \end{aligned}$$

Examinons maintenant le cas $p = 2$, qui est par construction totalement ramifié.

$$(2) = \begin{cases} (\sqrt{2})^2 & \text{dans } \mathbf{Q}(\sqrt{2}) \\ (2, 1 + \sqrt{3})^2 & \text{dans } \mathbf{Q}(\sqrt{3}) \\ (2, \sqrt{6})^2 & \text{dans } \mathbf{Q}(\sqrt{6}) \end{cases}$$

Nous cherchons désormais un idéal $\mathfrak{p}_2$ tel que $\mathfrak{p}_2^4 = (2)$ où de manière équivalente $\mathfrak{p}_2^2 = (\sqrt{2}) = (2, 1+\sqrt{3}) = (2, \sqrt{6})$ (ces idéaux sont égaux dans $\mathcal{O}_\mathbf{K}$). On considère l'idéal $\mathfrak{p}_2 = (\sqrt{2}, 1+u), u = \frac{\sqrt{2}+\sqrt{6}}{2}$.

$$\begin{aligned} \mathfrak{p}_2^2 &= (2, 1 + (2 + \sqrt{3}) + 2u, \sqrt{2}(1 + u)) \\ &= (\sqrt{2})(\sqrt{2}, 1 + \sqrt{2}(1 + u), 1 + u) \text{ car } 1 + \sqrt{3} = \sqrt{2}u \\ &= (\sqrt{2})\mathcal{O}_\mathbf{K} \end{aligned}$$

Nous sommes donc en présence de l'idéal recherché, et

$$(2) = (\sqrt{2}, 1 + u)^4 = \mathfrak{p}_2^4$$

Le fait d'avoir pour $\mathbf{K}$ une extension composée de corps quadratiques simplifie bien sûr considérablement les choses, puisque nous connaissons bien toutes les extensions intermédiaires ; mais nous voyons ici la très grande puissance des résultats théoriques (formule $n = ref$, comportements dans les extensions composées...), qui nous ont permis de connaître la ramification sans faire aucun calcul, et en évitant en particulier celui de l'anneau des entiers, en général très complexe.

Nous pouvons également sans peine exhiber les autres types de décomposition de premiers dans $\mathbf{K}$. En raisonnant simplement sur l'étude des corps quadratiques, on voit par exemple que :

$$(7) = \begin{cases} (7, 3 + \sqrt{2})(7, 3 - \sqrt{2}) & \text{dans } \mathbf{Q}(\sqrt{2}) \\ (7) & \text{dans } \mathbf{Q}(\sqrt{3}) \\ (7) & \text{dans } \mathbf{Q}(\sqrt{6}) \end{cases}$$

et que donc $(7) = (7, 3+\sqrt{2})(7, 3-\sqrt{2})$ dans $\mathcal{O}_{\mathbf{K}}$, chaque idéal étant de degré d'inertie 2. De même, 5 et 19 sont inertes dans $\mathbf{K}$ car ils le sont dans tous les corps intermédiaires.

Nous allons maintenant calculer la suite des groupes de ramification pour les premiers ramifiés, 2 et 3 :

Pour $p = 3$, $|E(\mathfrak{p}_3|3)| = 2$, et $E = \{id, \sigma_3\}$ (en effet $\sqrt{2} - \sigma_2(\sqrt{2}) = 2\sqrt{2} \notin \mathfrak{p}_3$, donc $\sigma_2 \notin E$, et de même pour σ_6). D'après le corollaire 4.6.5, son 3-Sylow $V_1(\mathfrak{p}_3|3) = \{id\}$, ce que nous pouvons vérifier à la main : comme $\sqrt{3} \in \mathfrak{p}_3 \smallsetminus \mathfrak{p}_3^2$, en utilisant le critère 4.6.3,

$$\sqrt{3} - \sigma_3(\sqrt{3}) = 2\sqrt{3} \in \mathfrak{p}_3 \smallsetminus \mathfrak{p}_3^2$$

donc $\sigma_3 \in E, \sigma_3 \notin V_1(\mathfrak{p}_3|3)$. Ainsi,

$$E_3 = V_0(\mathfrak{p}_3|3) \simeq \mathbf{Z}/2\mathbf{Z} \text{ et pour } m \geq 1, V_m(\mathfrak{p}_3|3) = \{1\}$$

Passons maintenant au cas $p = 2$, pour lequel la suite sera plus intéressante. 2 est totalement ramifié, donc $E(\mathfrak{p}_2|2) = G = (\mathbf{Z}/2\mathbf{Z})^2$, et son 2-Sylow $V_1(\mathfrak{p}_2|2) = (\mathbf{Z}/2\mathbf{Z})^2$.

Pour connaître les groupes suivants, nous utilisons le critère 4.6.3. Nous cherchons donc un élément $\pi \in \mathfrak{p}_2 \smallsetminus \mathfrak{p}_2^2$: $1 + u$ convient[‡]. Nous avons alors :

$$1 + u - \sigma_2(1 + u) = 2u \in \mathfrak{p}_2^4 \smallsetminus \mathfrak{p}_2^5$$
$$1 + u - \sigma_3(1 + u) = \sqrt{6} \in (\sqrt{3})\mathfrak{p}_2^2 \subset \mathfrak{p}_2^2 \smallsetminus \mathfrak{p}_2^3$$

en effet, $\sqrt{3} \notin \mathfrak{p}_2$ car sinon $\sqrt{2}(1 + u) - \sqrt{3} = 1 + \sqrt{2} \in \mathfrak{p}_2$, donc $1 \in \mathfrak{p}_2$.

Ainsi,

$$\sigma_2 \in V_m(\mathfrak{p}_2|2) \Leftrightarrow m \leq 3 \text{ et } \sigma_3 \in V_m(\mathfrak{p}_2|2) \Leftrightarrow m \leq 1$$

Cela suffit pour connaître la suite des groupes de ramification pour $p = 2$:

$$V_0 = V_1 = (\mathbf{Z}/2\mathbf{Z})^2, V_2 = V_3 = \mathbf{Z}/2\mathbf{Z}, \text{et pour } m \geq 4, v_m = \{1\}$$

[‡]en réalité, la vraie démarche est inverse : nous avons trouvé l'idéal $\mathfrak{p}_2$ en adjoignant un élément de $\mathfrak{p}_2 \smallsetminus \mathfrak{p}_2^2$ à l'idéal $(\sqrt{2})$. Trouver un tel élément se fait par conditions nécessaires sur des congruences.

5 Preuve du théorème de Kronecker-Weber

Nous possédons désormais l'outillage théorique requis pour établir le théorème de Kronecker-Weber, à l'exception d'un résultat dû à Minkowski, permettant d'affirmer l'existence de premiers ramifiés dans un corps de nombres, et dont nous n'énonçons ici qu'un corollaire :

Théorème 5.0.1. *Si* $\mathbf{K} \neq \mathbf{Q}$*, alors* $|\operatorname{disc}(\mathcal{O}_{\mathbf{K}})| > 1$.

Nous n'en ferons pas la démonstration, qui repose sur des considérations géométriques de volume et aurait conduit à un développement trop long et éloigné de notre sujet.

Ce théorème implique bien l'existence de nombres premiers ramifiés sur $\mathbf{K}$, du fait de l'équivalence p ramifié $\Leftrightarrow p|\operatorname{disc}(\mathcal{O}_{\mathbf{K}})$.

Nous énonçons maintenant le théorème de Kronecker-Weber :

Théorème 5.0.2. *Toute extension abélienne de* $\mathbf{Q}$ *est incluse dans une extension cyclotomique.*

5.1 Réduction des cas

Nous établissons dans un premier temps plusieurs lemmes qui permettent de restreindre l'étude à des corps de nombres les plus simples possibles.

Remarque 5.1.1. *Tout d'abord, pour un corps de nombres* $\mathbf{K}$ *de groupe de Galois* G *abélien, on peut écrire* $G = \bigoplus \mathbf{Z}/p_i^{m_i}\mathbf{Z}$*, donc* $\mathbf{K}$ *est l'extension composée de corps de nombres abéliens d'ordre puissance d'un nombre premier. Comme la propriété de cyclomicité passe aux extensions composées, on peut donc se restreindre au cas où* $G = \mathbf{Z}/p^m\mathbf{Z}$*.*

On considère donc désormais une extension abélienne $\mathbf{K}$ de $\mathbf{Q}$ de degré puissance d'un nombre premier. On pourrait même supposer son groupe de Galois cyclique, mais la réduction suivante nous fait perdre cette caractéristique.

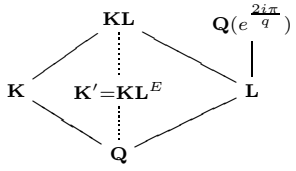
Lemme 5.1.1. *Soit* $\mathbf{K}$ *extension abélienne de* $\mathbf{Q}$ *de degré* p^m*. Si il existe* $q \neq p$ *premier ramifié dans* $\mathbf{K}$ *, alors il existe un corps de nombre* $\mathbf{K}'$ *abélien de degré sur* $\mathbf{Q}$ *une puissance de* p*, dans lequel* q *et tous les premiers non ramifiés de* $\mathbf{K}$ *sont non ramifiés, et qui est contenu dans une extension cyclotomique si et seulement si* $\mathbf{K}$ *l'est.*

Remarque 5.1.2. *Comme seuls un nombre fini de nombres premiers se ramifient dans* $\mathbf{K}$ *, ce lemme permet de se ramener au cas où* p *est le seul, en éliminant les autres un par un.*

Démonstration : L'idée de la démonstration est d'inclure la ramification en q dans un corps $\mathbf{L}$ contenu dans une extension cyclotomique, puis de considérer un corps $\mathbf{K}'$ dans lequel on supprime cette ramification, et qui ne diffère de $\mathbf{K}$ que d'une composante cyclotomique, en l'occurence $\mathbf{L}$.

Soit $\mathfrak{q}$ premier de $\mathcal{O}_{\mathbf{K}}$ au-dessus de q. Comme $e(\mathfrak{q}|q)$ divise $[\mathbf{K} : \mathbf{Q}] = p^m$, il est premier avec q, donc d'après le corollaire 4.6.5, son q-Sylow $V_1(\mathfrak{q}|q) = \{1\}$. Donc $e = |E/V_1|$ divise $\|q\| - 1 = q - 1$ d'après la proposition 4.6.6.

Donc le q-ième corps cyclotomique possède un sous corps $\mathbf{L}$ de degré e sur $\mathbf{Q}$, unique. De plus on sait que q est totalement ramifié dans son corps cyclotomique, donc dans $\mathbf{L}$ (d'après l'étude de la ramification dans les extensions cyclotomiques, théorème 4.2.2).

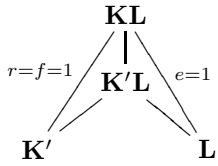


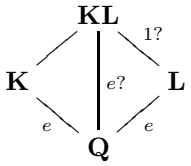
On considère alors un premier $\mathfrak{Q}$ de l'extension $\mathbf{KL}$ au-dessus de $\mathfrak{q}$, et le sous corps $\mathbf{K}' = \mathbf{KL}^{E(\mathfrak{Q}|q)}$. Alors par définition du corps d'inertie q est non ramifié dans $\mathbf{K}'$, et tout r premier non ramifié dans $\mathbf{K}$ ne l'est pas non plus dans $\mathbf{L}$ car $r \neq q$, et donc ne l'est pas dans $\mathbf{KL}$ (théorème 4.4.11) et a fortiori dans $\mathbf{K}'$.

De plus,le groupe de Galois de $\mathbf{KL}$ est un sous-groupe de $\mathrm{Gal}(\mathbf{K}/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{L}/\mathbf{Q})$, donc abélien d'ordre une puissance de p, et donc $\mathbf{K}'$ est également une extension galoisienne de degré puissance de p.

Enfin, pour avoir l'équivalence $\mathbf{K}$ inclus dans un corps cyclotomique $\Leftrightarrow$ $\mathbf{K}'$ inclus dans un corps cyclotomique, nous allons montrer en fait que $\mathbf{KL} = \mathbf{K}'\mathbf{L}$, ce qui est suffisant car $\mathbf{L}$ est cyclotomique.[§]

Pour cela, montrons les égalités présentes sur le premier diagramme, qui impliqueront $[\mathbf{KL} : \mathbf{K}'\mathbf{L}] = ref = 1$ par croissance de r, e et f.





Comme $\mathbf{K}' = \mathbf{KL}^E$, on a bien $r(\mathbf{KL}|\mathbf{K}') = f(\mathbf{KL}|\mathbf{K}') = 1$.

D'autre part, on veut montrer que $\mathfrak{Q}$ est non ramifié sur $\mathbf{L}$. Or si $\mathfrak{q}_\mathbf{L}$ est l'idéal premier de $\mathbf{L}$ au-dessus de q, on a $e(\mathfrak{Q}|\mathfrak{q}_\mathbf{L}) = \frac{e(\mathfrak{Q}|q)}{e(\mathfrak{q}_L|q)} = \frac{e(\mathfrak{Q}|q)}{e(\mathfrak{q}|q)}$, car $\mathfrak{q}_\mathbf{L}$ totalement ramifié sur $\mathbf{L}$ de degré $e(\mathfrak{q}|q)$. Donc on veut montrer que $e(\mathfrak{Q}|q) = e(\mathfrak{q}|q)$, ce qui nous ramène à $\mathbf{K}$ que l'on connaît mieux.

Comme $[\mathbf{KL} : \mathbf{Q}]|[\mathbf{K} : \mathbf{Q}] \times [\mathbf{L} : \mathbf{Q}]$ est une puissance de p (car $e(\mathfrak{q}|q)$ en est une), $e(\mathfrak{Q}|q)$ est également puissance de p, donc le q-Sylow $V_1(\mathfrak{Q}|q)$ est réduit à $\{id\}$ (corollaire 4.6.5). Donc $E(\mathfrak{Q}|q) = E(\mathfrak{Q}|q)/V_1$ est cyclique d'après la proposition 4.6.6.

D'autre part en considérant le plongement :

$$\mathrm{Gal}(\mathbf{KL}/\mathbf{Q}) \hookrightarrow \mathrm{Gal}(\mathbf{K}/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{L}/\mathbf{Q})$$

on obtient par restriction :

$$E(\mathbf{KL}/\mathbf{Q}) \hookrightarrow E(\mathbf{K}/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{L}/\mathbf{Q})$$

car si $\sigma \in E(\mathbf{KL}/\mathbf{Q})$, pour $\alpha \in \mathcal{O}_\mathbf{K}, \sigma(\alpha) = \alpha + q$, où $q \in \mathfrak{Q} \cap \mathcal{O}_\mathbf{K} = \mathfrak{q}$, donc $\sigma_{|\mathbf{K}} \in E(\mathbf{K}/\mathbf{Q})$.

Donc le générateur de $E(\mathbf{KL}/\mathbf{Q})$ a un ordre divisant le ppcm des cardinaux des groupes images qui sont tous deux égaux à $e(\mathfrak{q}|q)$. Comme réciproquement $e(\mathfrak{Q}|q) \geq e(\mathfrak{q}|q)$, on a donc bien le résultat $e(\mathfrak{Q}|q) = e(\mathfrak{q}|q)$.

Ainsi :

$$\begin{aligned} [\mathbf{KL} : \mathbf{K}'\mathbf{L}] &= r(\mathbf{KL}|\mathbf{K}'\mathbf{L})\ e(\mathbf{KL}|\mathbf{K}'\mathbf{L})\ f(\mathbf{KL}|\mathbf{K}'\mathbf{L}) \\ &\leq r(\mathbf{KL}|\mathbf{K}')\ e(\mathbf{KL}|\mathbf{L})\ f(\mathbf{KL}|\mathbf{K}') \\ &= 1 \end{aligned}$$

Donc $\mathbf{KL} = \mathbf{K}'\mathbf{L}$, ce qui achève la démonstration. □

Nous considérons donc désormais le cas où $\mathbf{K}$ est d'ordre p^m, et tel que p soit le seul premier ramifié dans $\mathbf{K}$. Nous allons traiter séparément les cas $p = 2$ et p impair.

[§]Il est légitime d'espérer cette égalité, puisque l'on a construit $\mathbf{L}$ de sorte qu'il contienne la ramification de q, tandis que $\mathbf{K}'$ est obtenu en enlevant cette ramification. On retrouve $\mathbf{KL}$ en combinant les deux.

5.2 Démonstration dans le cas $p = 2$

Proposition 5.2.1. *Toute extension abélienne de* $\mathbf{Q}$ *de degré* 2^m *telle que* 2 *soit le seul premier ramifié est contenue dans l'extension cyclotomique* $\mathbf{Q}(e^{\frac{2i\pi}{2^{m+2}}})$.

Démonstration : Si $m = 1$, $\mathbf{K} = \mathbf{Q}(\sqrt{d})$ et l'étude de la ramification dans les corps quadratiques impose que d soit au plus divisible par 2 (sinon d'autres nombres se ramifient). Réciproquement, $d = 2, -2, -1$ conviennent. Donc pour $m = 1$, $\mathbf{K} = \mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{-2})$ ou $\mathbf{Q}(\sqrt{-1})$, qui sont bien incluses dans l'extension cyclotomique $\mathbf{Q}(e^{\frac{i\pi}{4}}) = \mathbf{Q}(\frac{\sqrt{2}}{2}(1+i))$.

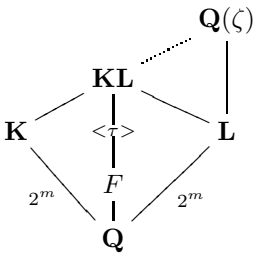
Soit maintenant $m \geq 2$. $\mathbf{K} \cap \mathbf{R} = \mathbf{K}^{<\varsigma>}$ où ς est la conjugaison complexe, d'ordre au plus 2, est une extension normale de degré $[\mathbf{K} \cap \mathbf{R} : \mathbf{Q}] \geq 2^{m-1} > 1$. Donc un sous-corps quadratique de $\mathbf{K} \cap \mathbf{R}$ est nécessairement $\mathbf{Q}(\sqrt{2})$, (car seul 2 peut se ramifier dans $\mathbf{K} \cap \mathbf{R}$) et donc $\mathbf{Q}(\sqrt{2}) \subset \mathbf{K}$ pour $m \geq 2$.

Posons $\mathbf{L} = \mathbf{Q}(\zeta) \cap \mathbf{R}$, où $\zeta = e^{\frac{2i\pi}{2^{m+2}}}$. Comme son groupe de Galois G est isomorphe à $(\mathbf{Z}/2^{m+2}\mathbf{Z})^*/(\pm 1)$, donc cyclique, $\mathbf{Q}(\sqrt{2})$ est l'unique sous corps quadratique de $\mathbf{L}$ (même argument). Et comme $\mathbf{Q}(\zeta)$ contient i, $\mathbf{Q}(\zeta)$ contient également les deux autres corps quadratiques $\mathbf{Q}(\sqrt{-1})$ et $\mathbf{Q}(\sqrt{-2})$.

Écrivons $G =< \sigma >$ et considérons $\tau \in \mathrm{Gal}(\mathbf{KL}/\mathbf{Q})$ tel que $\tau_{|L} = \sigma$. Posons $F = \mathbf{KL}^{<\tau>}$. $[F : \mathbf{Q}] \mid [\mathbf{KL} : \mathbf{Q}] \mid [\mathbf{K} : \mathbf{Q}][\mathbf{L} : \mathbf{Q}]$, donc $[F : \mathbf{Q}]$ est de la forme 2^k. Or $\mathbf{KL}^{<\tau>} \cap \mathbf{L} \subset \mathbf{L}^{<\tau>} \subset \mathbf{L}^{<\sigma>} = \mathbf{Q}$, donc $F \cap \mathbf{L} = \mathbf{Q}$, d'où $k \leq 1$ (sinon $\mathbf{Q}(\sqrt{2}) \subset F \cap \mathbf{L}$, car seul 2 peut se ramifier dans F, d'après le théorème 4.4.11). Donc $F = \mathbf{Q}, \mathbf{Q}(\sqrt{-2})$ ou $\mathbf{Q}(\sqrt{-1})$. En particulier $F \subset \mathbf{Q}(\zeta)$.

Montrons maintenant que $\mathbf{KL} = F\mathbf{L}$, ce qui permettra de conclure.

Comme on a un plongement $\mathrm{Gal}(\mathbf{KL}/\mathbf{Q}) \hookrightarrow \mathrm{Gal}(\mathbf{K}/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{L}/\mathbf{Q})$, et que les deux groupes à l'arrivée sont d'ordre 2^m, $\tau \in \mathrm{Gal}(\mathbf{KL}/\mathbf{Q})$ est d'ordre inférieur à 2^m. Mais comme σ est d'ordre 2^m, τ l'est également. On a donc :



$$\begin{cases} F\mathbf{L} \subset \mathbf{KL} \\ [\mathbf{KL} : F] = |<\tau>| = 2^m \\ [F\mathbf{L} : F] = [\mathbf{L} : F \cap \mathbf{L}] = [\mathbf{L} : \mathbf{Q}] = 2^m \end{cases}$$

Donc $F\mathbf{L} = \mathbf{KL}$, et comme $F \subset \mathbf{Q}(\zeta)$, on a l'inclusion voulue $\mathbf{K} \subset \mathbf{KL} = F\mathbf{L} \subset \mathbf{Q}(\zeta)$. □

5.3 Démonstration pour p impair

Le théorème est donc prouvé dans le cas particulier $p = 2$. Nous considérons donc désormais une extension de degré p^m, où p est impair, et dans laquelle p est toujours le seul premier ramifié.

Lemme 5.3.1. *Si* $m = 1$, *alors pour* $\mathfrak{p}$ *premier au-dessus de* p, *on a* $\mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathbf{Z}) = \mathfrak{p}^{2(p-1)}$.

Démonstration : $\mathfrak{p}$ est ramifié sur p (car sinon, il n'y aurait pas de premier ramifié, ce qui contredirait le corollaire du théorème de Minkowski), donc l'est totalement car $e(\mathfrak{p}|p)|p = [\mathbf{K} : \mathbf{Q}]$. Comme de plus p est le seul premier ramifié, $\mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathbf{Z})$ n'est divisible que par $\mathfrak{p}$. Donc $\mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathbf{Z}) = \mathfrak{p}^k$.

Il nous reste à montrer que cette puissance k qui intervient est égale à $2(p-1)$; nous disposons de deux résultats pour y parvenir : la formule de Hilbert (proposion 4.6.7) et le théorème 4.3.6.

Puisque $|E| = p$, les V_i sont soit E tout entier, soit réduits à $\{id\}$. La formule de Hilbert $k = \sum_{i\geq 0}(|V_i| - 1)$ est donc une somme de $p-1$. Ainsi, $p-1|k$.

Utilisons maintenant le théorème 4.3.6 : soit donc $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, alors nécessairement $\pi \notin \mathbf{Q}$ (car $\mathcal{O}_\mathbf{K} p = \mathfrak{p}^p \subset \mathfrak{p}^2 \subset \mathfrak{p}$, donc $p\mathbf{Z} = \mathcal{O}_\mathbf{K} p \cap \mathbf{Q} = \mathfrak{p}^2 \cap \mathbf{Q} = \mathfrak{p} \cap \mathbf{Q} = p\mathbf{Z}$), donc π est de degré p sur $\mathbf{Q}$.

Soit f son polynôme minimal, $f(X) = X^p + a_1 X^{p-1} + \dots a_p, a_i \in \mathbf{Z}$. k est la plus grande puissance de $\mathfrak{p}$ qui divise $f'(\pi)$.

On considère la plus grande puissance de $\mathfrak{p}$ qui divise chacun des termes de $f'(\pi) = p\pi^{p-1} + \dots a_1$. Les ia_i sont dans $\mathbf{Z}$, donc la puissance de $\mathfrak{p}$ qui divise chacun d'eux est multiple de $e = p$, car si $\mathfrak{p}$ divise a_i, $a_i \in \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, donc $a_i = pa_i'$, et on recommence jusqu'à ce que $a_i^{(n)} \notin \mathfrak{p}$. Comme $p\mathcal{O}_\mathbf{K} = \mathfrak{p}^p$, la puissance obtenue est bien multiple de p.

Comme $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, la plus grande puissance de $\mathfrak{p}$ qui divise $ia_i\pi^{i-1}$ est donc congrue à $i-1$ modulo p, donc ces puissances sont en particulier toutes distinctes, et k est nécessairement la plus petite d'entre elles.

En considérant le premier terme, on a $k \leq 2p-1$. D'autre part, si on plonge la relation $\pi^p + a_1\pi^{p-1} + \dots a_p = 0$ dans le $\mathbf{Z}/p\mathbf{Z}$ espace vectoriel $\mathcal{O}_\mathbf{K}/\mathfrak{p}$, les π^i étant indépendants sur $\mathbf{Z}/p\mathbf{Z}$ (en utilisant à nouveau l'argument de congruence), on a nécessairement $\forall i, p|a_i$. Donc $\mathfrak{p}^p$ divise chaque terme, d'où $k \geq p$.

Or k est multiple de $p-1$, donc ces deux conditions imposent $k = 2(p-1)$.

Ainsi, $\mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathbf{Z}) = \mathfrak{p}^{2(p-1)}$. □

Lemme 5.3.2. *Si $m = 2$, alors $G = \mathrm{Gal}(\mathbf{K}/\mathbf{Q})$ est cyclique.*

Démonstration : Nous allons pour cela montrer que G possède un unique sous groupe d'ordre p.

Existence : elle est évidente car G est un p-groupe, mais nous allons en fait exhiber ce sous-groupe. Puisque p est par hypothèse le seul premier qui se ramifie et qu'il ne se ramifie plus dans $\mathbf{K}^E$, le théorème de Minkowski 5.0.1 impose $[\mathbf{K}^E : \mathbf{Q}] = 1$, donc $\mathfrak{p}$ est totalement ramifié sur p, et E est d'ordre p^2. D'après le théorème 4.6.5, son p-Sylow V_1 est également d'ordre p^2 ¶. Soit V_r le premier groupe de ramification d'ordre inférieur à p^2 : comme $r \geq 2$, V_{r-1}/V_r se plonge dans $\mathcal{O}_\mathbf{K}/\mathfrak{p}$, qui est de dimension $f = 1$ sur $\mathbf{Z}/p\mathbf{Z}$ car $\mathfrak{p}$ est totalement ramifié, donc $|V_r| \geq \frac{|V_{r-1}|}{p}$. Ainsi, V_r est un sous-groupe d'ordre p.

Unicité : soit H un sous-groupe d'ordre p de G, alors $\mathbf{K}^H$ est une extension d'ordre p de $\mathbf{Q}$, dans laquelle p est encore le seul premier ramifié. Donc d'après le lemme 5.3.1, $\mathrm{diff}(\mathcal{O}_{\mathbf{K}^H}|\mathbf{Z}) = \mathfrak{p}^{2(p-1)}$. Par multiplicativité de la différente, (théorème 4.3.2), $\mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathbf{Z}) = \mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathcal{O}_{\mathbf{K}^H})\mathfrak{p}^{2(p-1)}$, donc $\mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathcal{O}_{\mathbf{K}^H})$ est indépendante du groupe H choisi. Or si l'on écrit la formule de Hilbert pour l'exposant k de $\mathfrak{p}$ (qui ne dépend pas de H) dans $\mathrm{diff}(\mathcal{O}_\mathbf{K}|\mathcal{O}_{\mathbf{K}^H})$, comme $V_i(\mathfrak{p}|\mathfrak{p}_H) = V_i(\mathfrak{p}|p) \cap H$, on a :

$$k = \sum_{i\geq 0}(|V_i(\mathfrak{p}|p) \cap H| - 1)$$

Tant que $|V_i| = p^2$, alors $|V_i \cap H| = |H| = p$. Mais pour $i = r$, si $H \neq V_r$, alors $|V_i \cap H| = 1$ pour $i \geq r$, d'où $\sum_{i\geq r}(|V_i \cap H| - 1) = 0$; mais si $H = V_r$, cette même somme est strictement positive. Comme la somme ne peut dépendre de H, on a un unique H possible : $H = V_r$.

Ainsi G possède un unique sous-groupe d'ordre p, donc il existe un élément d'ordre p^2, et G est cyclique. □

Nous pouvons maintenant démontrer le théorème pour p impair :

¶De manière générale, le théorème de Minkowski permet d'affirmer que si p est le seul premier ramifié, alors il l'est totalement.

Théorème 5.3.3. *Soit* $\mathbf{K}$ *une extension abélienne de* $\mathbf{Q}$ *de degré* p^m *(*p *premier impair), dans laquelle seul* p *se ramifie. Alors* $\mathbf{K}$ *est l'unique sous-corps d'indice* $p-1$ *du* p^{m+1}*-ième corps cyclotomique.*

Démonstration : Si $m = 1$, et supposons l'existence de deux extensions $\mathbf{K}$ et $\mathbf{K}'$ distinctes vérifiant ces hypothèses. Alors $\mathbf{KK}'$ est une extension de degré p^2 de $\mathbf{Q}$, dans laquelle p est toujours le seul premier qui se ramifie, donc d'après le lemme 5.3.2, $\mathrm{Gal}(\mathbf{KK}'/\mathbf{Q})$ est cyclique, et donc $\mathbf{KK}'$ possède une unique extension intermédiaire d'indice p, absurde car $\mathbf{K} \neq \mathbf{K}'$. Donc $\mathbf{K}$ est unique et est l'unique sous-corps de $\mathbf{Q}(e^{\frac{2i\pi}{p^2}})$ de degré p sur $\mathbf{Q}$.

Si $m \geq 1$, soit $\mathbf{L}$ l'unique sous-corps de $\mathbf{Q}(e^{\frac{2i\pi}{p^{m+1}}})$ de degré p^m sur $\mathbf{Q}$ (comme $p \neq 2$, $(\mathbf{Z}/p^{m+1}\mathbf{Z})^*$ est en effet cyclique, ce qui assure l'unicité de $\mathbf{L}$). De manière analogue à ce qui avait été fait dans le cas $p = 2$, soit σ un générateur de $\mathrm{Gal}(\mathbf{L}/\mathbf{Q})$, que l'on étend en un automorphisme τ de $\mathbf{KL}$, et soit $F = (\mathbf{KL})^{<\tau>}$. On a encore $F \cap \mathbf{L} \subset \mathbf{L}^{<\sigma>} = \mathbf{Q}$. Supposons par l'absurde que $F \neq \mathbf{Q}$. Comme $[F : \mathbf{Q}]|(p^m)^2$ est de la forme p^k, on peut considérer un sous-corps de F de degré p sur $\mathbf{Q}$ (d'après le théorème de Sylow, $\mathrm{Gal}(F/\mathbf{Q})$ contient un sous-groupe de cardinal p^{k-1}), qui est unique en appliquant le cas $m = 1$ (p est bien le seul premier ramifié dans $\mathbf{KL}$ (d'après le théorème 4.4.11) donc dans F). Or $\mathbf{L}$ contient également ce sous-corps, donc on ne peut avoir $F \cap \mathbf{L} = \mathbf{Q}$, absurde.

Ainsi, $[\mathbf{KL} : \mathbf{Q}] = [\mathbf{KL} : F]$ est l'ordre de τ. Or du fait du plongement

$$\mathrm{Gal}(\mathbf{KL}/\mathbf{Q}) \hookrightarrow \mathrm{Gal}(\mathbf{K}/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{L}/\mathbf{Q})$$

l'ordre de τ divise p^m, mais est supérieur à l'ordre de σ qui vaut encore p^m. Donc $[\mathbf{KL} : \mathbf{Q}] = [\mathbf{K} : \mathbf{Q}]$, c'est à dire $\mathbf{K} = \mathbf{L}$. □

6 Bibliographie

– Daniel A. Marcus, Number Fields, Springer Universitext.
– Kenneth Ireland & Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate texts in mathematics 84.