Université Paris 13
École Normale Supérieure de Rennes

Théorème de densité de Chebotarev

Gabriel Lepetit

Mémoire de stage de Licence 3 réalisé sous la direction de Cédric Pépin *au LAGA, Université Paris 13*

Magistère 1 2014-2015

Ce stage a été effectué du 19 mai au 20 juin 2015 au :

Laboratoire Analyse, Géométrie et Applications (LAGA)
Université Paris 13
99 avenue Jean-Baptiste Clément
93430 Villetaneuse

Mon maître de stage était Cédric Pépin (`http://www.math.univ-paris13.fr/~cpepin/`), maître de conférences au sein de l'équipe Arithmétique et Géométrie Algébrique.

Table des matières

****

INTRODUCTION

Le théorème de densité de Chebotarev, démontré par Nikolaï Chebotarev [1] en 1922, est une généralisation du théorème de Dirichlet qui affirme que l'ensemble des nombres premiers en progression arithmétique de raison m a une densité naturelle parmi les nombres premiers de $\frac{1}{\varphi(m)}$ où φ est la fonction indicatrice d'Euler. Il fournit au passage une démonstration plus profonde de ce théorème, qui peut être péniblement démontré de manière élémentaire : on montrera en effet que c'est un cas particulier du théorème de Chebotarev, précisément le cas où il est appliqué à une *extension cyclotomique* $\mathbb{Q}[\zeta]$ de $\mathbb{Q}$, où ζ est une racine primitive de l'unité.

Ce fait est révélateur d'un état d'esprit général de la théorie des nombres, qui veut que l'on prenne de la hauteur et que l'on introduise des concepts très généraux, comme le sont les extensions de corps, les anneaux de Dedekind, l'étude de la ramification ou la théorie de Galois, pour prouver des énoncés simplement compréhensibles.

Dans ce mémoire, on s'attachera d'abord à présenter des outils généraux de la théorie des nombres (en s'appuyant essentiellement sur [4]) à travers la présentation des extensions algébriques de corps et des anneaux de Dedekind, puis on fera un traitement succint de la théorie de Galois ; enfin, nous tâcherons de comprendre un des énoncés principaux de la théorie du corps de classe : la loi de réciprocité d'Artin, qui sera au cœur de la démonstration du théorème de Chebotarev, que nous finirons par effectuer en utilisant des techniques d'analyse complexe.

1. en transcription cyrillique standard, Nikolaï TCHEBOTARIOV (1894-1947), mathématicien soviétique, connu aussi pour un théorème sur les racines de l'unité.

Chapitre 1

Généralités sur les extensions algébriques

1.1 Extension finies

Définition 1.1.1

Soient A et B des anneaux tels que $A \subset B$. On dit que B est une extension finie de A si c'est un A-module de type fini.

En particulier, cela donne dans le cas des corps :

Définition 1.1.2

Soit K un corps. On dit que L est une extension finie de K si c'est un corps contenant K et que sa dimension en tant que K-espace vectoriel, notée $[L : K]$ est finie. On appelle $[L : K]$ le degré de L sur K.

Proposition 1.1.3 (*formule des degrés*)

Soient $K \subset L \subset M$ une suite d'extensions finies de corps. Alors

$$[M : K] = [M : L][L : K]$$

Démonstration. Soit $n = [L : K], m = [M : L]$, $(x_1, \dots, x_n)$ une base de L sur K, $(y_1, \dots, y_m)$ une base de M sur L.

Alors, en notant $\forall 1 \leqslant i \leqslant n, \forall 1 \leqslant j \leqslant m, z_{i,j} = x_i y_j$, on peut affirmer que $(z_{i,j})$ est une base à mn éléments de M sur K.

En effet, si $z \in M$, il existe $(a_j) \in L^m$ tel que $z = \sum_{j=1}^{m} a_j y_j$.

De plus, $\forall j \in [\![1; m]\!]$, comme $a_j \in L$, on peut trouver $u_{i,j} \in K$ tel que $a_j = \sum_{i=1}^{n} u_{i,j} x_i$.

Donc $z = \sum_{j=1}^{m} \sum_{i=1}^{n} u_{i,j} x_i y_j$ donc $(z_{i,j})$ est génératrice.

La liberté est claire car si $u_{i,j} \in K$ et $\sum_{i,j} u_{i,j} x_i y_j = 0$, alors par liberté de (y_j) dans le L-espace vectoriel M, $\forall j \in [\![1; m]\!], \sum_{i=1}^{n}, u_{i,j} x_i = 0$ donc $\forall i, j, u_{i,j} = 0$ par liberté de (x_i). □

Dans le cas d'un corps fini K, le cardinal de K s'exprime en fonction de sa caractéristique p et de son degré sur un sous-corps isomorphe à $\mathbb{F}_p$:

Proposition 1.1.4

Soit K un corps fini. Alors

- *la caractéristique de K est un nombre premier p et il existe $n \in N$ tel que K a $q = p^n$ éléments.*
- *Le groupe des inversibles de K noté $K^\times$ est un groupe cyclique à $q-1$ éléments.*

1.2 Extensions algébriques

1.2.1 Cas des anneaux

Définition 1.2.1

Soit B un anneau et A un sous-anneau de B. On dit que $x \in B$ est entier sur A si il est racine d'un polynôme unitaire à coefficients dans A. Une équation du type $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ est alors appelée équation de dépendance intégrale de x sur A.

B est dit entier sur A si tout élément de B est entier sur A.

Théorème 1.2.2

Si B est un anneau, A un sous-anneau de B et $x \in B$, il y a équivalence entre

1. *x est entier.*
2. *$A[x]$ est un A-module de type fini.*
3. *Il existe un sous-anneau C de B, contenant A et x, qui est un A-module de type fini.*

Proposition 1.2.3

Soient B un anneau, A un sous-anneau de B, et $(x_1, \ldots, x_n) \in B^n$. Si chacun des x_i est entier sur $A[x_1, \ldots, x_{i-1}]$, alors $A[x_1, \ldots, x_n]$ est un A-module de type fini.

Par conséquent, si A' est l'ensemble des éléments de B qui sont entiers sur A, A' est un sous-anneau de B.

Définition 1.2.4

Avec les notations de la proposition précédente, l'ensemble A' est appelé fermeture intégrale de A dans B.

Démonstration. La première assertion se démontre par récurrence sur n. Elle est évidente au rang 1.

Soit $n \in \mathbb{N}^*$, supposons le résultat vrai au rang $n-1$. Alors si $C = A[x_1, \ldots, x_{n-1}]$, c'est un A-module de type fini par hypothèse de récurrence. Donc on peut trouver $c_1, \ldots, c_p \in C$: $C = \sum_{j=1}^{p} Ac_j$. Comme de plus, $A[x_1, \ldots, x_n] = C[x_n]$ et x_n entier sur C, c'est un C-module de type fini, donc $\exists d_1, \ldots, d_q : A[x_1, \ldots, x_n] = \sum_{k=1}^{q} Cd_k = \sum_{k=1}^{q} \left(\sum_{j=1}^{p} Ac_j \right) d_k = \sum_{j,k} Ac_j d_k$.

Une fois ce premier point prouvé, le reste en découle facilement. Soient $x, y \in B$ entiers sur A. Alors $x+y$ et xy sont dans $A[x,y]$ qui est un A-module de type fini selon ce qui précède. Il en va donc de même de $A[x+y]$ et $A[xy]$ ce qui montre selon le théorème 1.2.2 que $x+y, xy \in A'$. □

Avec ce théorème, la proposition suivante se montre sans difficultés.

Proposition 1.2.5 (*transitivité du caractère entier*)

Si $A \subset B \subset C$ est une suite de sous-anneaux, et si B est entier sur A et C est entier sur B, alors C est entier sur A.

Définition 1.2.6

Si A est un anneau intègre et K est son corps des fractions, la fermeture intégrale de A dans K est appelée clôture intégrale de A. Si cette clôture est A lui-même, on dit que A est intégralement clos.

Proposition 1.2.7

Un anneau principal est intégralement clos.

Démonstration. Soit A anneau principal, $K = \mathrm{Frac}(A)$. Si $x = \dfrac{a}{b} \in K$, où a et b sont premiers entre eux, est entier sur A, alors on peut fixer $a_0, \ldots, a_{n-1} \in A$ tels que

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_1\left(\frac{a}{b}\right) + a_0 = 0$$

Donc en multipliant par b^n, $a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0$, soit

$$a^n = -b\left(a_{n-1}a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}\right)$$

Donc $b|a^n$, donc comme a et b sont premiers entre eux, selon le lemme de Gauss, $b|a$, donc $b = 1$ et $x \in A$. □

1.2.2 Cas des corps

Définition 1.2.8

Soit K un corps et L une extension de K. On dit que $x \in L$ est algébrique sur K si il est racine d'un polynôme (pas nécessairement unitaire) à coefficients dans K.

L est dite extension algébrique de K si tout élément de L est algébrique sur K.

Remarque. Il est immédiat que toute extension finie L de K est algébrique sur K. En effet, si $x \in L$, $[K[x] : K] \leqslant [L : K]$ qui est fini.

Soient K un corps et L une extension de K. Si $x \in L$, on peut considérer

$$\begin{array}{rccc} \varphi_x : & K[X] & \longrightarrow & L \\ & P & \longmapsto & P(x) \end{array}$$

le morphisme d'évaluation en x. Son noyau est un idéal de $K[X]$ qui est un anneau principal.

Deux cas se présentent :

- Ou bien cet idéal est nul, on dit que x est *transcendant*, il n'est racine d'aucun polynôme à coefficients dans K et $K[x]$ n'est pas une extension algébrique de K.
- Ou bien, il est de la forme (Π) où Π est polynôme unitaire, et alors x est algébrique. Π est appelé *polynôme minimal* de x. Dans ce cas, selon le théorème 1.2.2, $K[x]$ est une extension finie de K donc une extension algébrique de K.

Par définition du polynôme minimal, on a $\forall P \in K[X], P(x) = 0 \iff \Pi | P$ dans $K[X]$.

De plus, φ_x étant surjectif, $K[X]/(\Pi) \simeq K[x]$. Donc $K[x]$ est un corps si et seulement si Π est irréductible.

$K[x]$ est un anneau intègre car contenu dans le corps L donc Π est un élément premier de $K[X]$, donc Π est irréductible.

Remarque. Soit K un corps et P un polynôme irréductible de $K[X]$. Alors $L = K[X]/(P)$ est un corps et en notant $x = \overline{X}$ la classe de X modulo P, et $\psi_{X\to x}$ le morphisme d'évaluation en x, on a $\psi_{X\to x}(P) = \overline{P} = 0$ donc P admet x pour racine dans L.

De plus, $L = K[x]$ est de degré fini sur K puisque x admet P pour polynôme minimal.

Cette remarque constitue l'argument principal du théorème suivant :

Théorème 1.2.9

Soit K un corps, $P \in K[X]$ non constant. Il existe une extension finie L de K tel que P se décompose en produits de facteurs de degré 1 dans $L[X]$.

Démonstration. On procède par récurrence sur d, degré de P. Le théorème est évident pour $d = 1$.

Soit P de degré $d \geqslant 2$, supposons l'assertion vraie jusqu'au degré $d-1$. Comme $K[X]$ est factoriel, P se divise en produits d'irréductibles sur K, on peut prendre F un de ces facteurs. Selon la remarque, il existe une extension finie K' de K et $a \in K'$ tel que $X - a | F(X)$ dans $K'[X]$. Donc $P(X) = (X-a)P_1(X)$ où P_1 est un polynôme de degré $d-1$ dans $K'[X]$. Selon l'hypothèse de récurrence, il existe une extension finie L de K' dans laquelle P_1 se décompose en facteurs de degré 1, ce qui montre le résultat. □

A l'aide du lemme de Zorn et de ce théorème, il est possible de montrer que tout corps est contenu dans un corps algébriquement clos, appelé sa clôture algébrique.

1.3 K-isomorphismes et éléments conjugués

Cette section est un préliminaire à la théorie de Galois qui sera traitée dans le chapitre 4.

Définition 1.3.1

Soient K un corps, L et L' des extensions finies de K.Un K-isomorphisme de L dans L' est un morphisme de corps φ tel que $\varphi_{|K} = \mathrm{id}$.

Remarque. Un morphisme de corps est toujours injectif.

Définition 1.3.2

Soit K un corps, L une extension de K et $x, y \in L$. On dit que x et y sont conjugués s'il existe un K-isomorphisme de $K[x]$ dans $K[y]$.

Le lemme suivant lie la notion de K-isomorphisme et de racines d'un polynôme, ce qui est historiquement dans l'esprit de la théorie de Galois.

Lemme 1.3.3

Les racines d'un polynôme irréductible $P \in K[X]$ dans une clôture algébrique C de K sont deux à deux conjuguées.

Démonstration. En effet, si x, y sont deux racines de P, elles ont le même polynôme minimal P donc $K[x] \simeq K[X]/(P) \simeq K[y]$ et la composition des deux isomorphismes donne un K-isomorphisme de $K[x]$ dans $K[y]$.

Réciproquement, si φ est un K-isomorphisme de L dans L' et $x \in L$, $\varphi(x)$ a le même polynôme minimal Π que x. En effet, si $P \in K[X]$, alors $P(x) = 0 \iff P(\varphi(x)) = \varphi(P(x)) = 0$ puisque φ est un K-morphisme injectif.

Donc $\varphi(x)$ est une racine de Π dans un corps algébriquement clos contenant K.

□

On va dégager une classe de corps K pour lesquels, pour toute extension finie L de degré n de K, il existe exactement n K-isomorphismes de L dans K, ce qui corrrespond à la notion de corps parfait.

Définition 1.3.4

Un corps parfait est un corps de caractéristique 0, ou un corps de caractéristique $p > 0$ tel que le morphisme de Frobenius $x \mapsto x^p$ soit surjectif.

On rappelle le résultat suivant :

Proposition 1.3.5

Si K est un corps fini de caractéristique p, le morphisme de Frobenius $\varphi_p : x \longmapsto x^p$ est un automorphisme de K. Par conséquent, un corps fini est un corps parfait.

Proposition 1.3.6

Si K est un corps parfait, si P est un polynôme irréductible à coefficients dans K inclus dans un corps algébriquement clos C, alors toutes les racines de P dans C sont simples.

Démonstration. Supposons que P de degré $n \geqslant 2$ admette une racine multiple u dans C. C'est alors une racine de P'.

Soit Q le polynôme minimal de u dans K. On a $Q|P$ et P est unitaire irréductible, d'où $P = Q$. De plus, u est racine de P' donc $P|P'$. Par suite $P' = 0$ puisque P' est de degré $n-1$ s'il est non nul.

Notons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. $P'(X) = nX^{n-1} + \sum_{j=1}^{n-1} j a_j X^{j-1}$ donc en particulier $n.1_K = 0$: cela est impossible si $\mathrm{car}(K) = 0$.

Maintenant, si K est un corps de caractéristique p premier tel que $x \longmapsto x^p$ soit surjectif, on a $p|n$ et $\forall 1 \leqslant j \leqslant n-1, p \nmid j \Rightarrow a_j = 0$, ce qui nous assure que P est de la forme $X^{pq} + b_{q-1}X^{(q-1)p} + \cdots + b_1X^p + b_0$.

Cependant, par surjectivité du morphisme de Frobenius, $\forall i \in [\![0; q-1]\!], \exists c_i \in K : b_i = c_i^p$, donc

$$P(X) = \left(X^q + c_{q-1}X^{q-1} + \cdots + c_0\right)^p$$

donc P n'est pas irréductible, ce qui est absurde. Donc toutes les racines de F sont simples dans les deux cas. □

Lemme 1.3.7

Soient K un corps et L une extension finie de K. Alors si φ est isomorphisme de K dans K', on peut prolonger φ en un isomorphisme de L dans L' où L' est une extension finie de K'.

Démonstration. On raisonne par récurrence sur le degré $n = [L : K]$. Pour $n = 1$, il n'y a rien à démontrer.

Supposons $n = [L : K] \geqslant 2$ et faisons l'hypothèse que le résultat est vrai pour toute extension de degré inférieur à $n-1$.

Soit $x \in L, x \notin K$. On a $K \subset K[x] \subset L$. De plus, on peut prolonger φ à $K[x]$. En effet, si P est le polynôme minimal de x, on peut considérer le morphisme d'évaluation $\psi = \varphi_{X \to X}$ prolongeant φ. Si y est une racine de $\psi(P) \in K'[X]$ dans une extension finie de K' (cf théorème 1.2.9), on peut définir

$$\begin{array}{rccc} \varphi' : & K[x] & \to & K'[y] \\ & x & \longmapsto & y \\ & z \in K & \longmapsto & \varphi(z) \end{array}$$

De plus, par hypothèse de récurrence, comme $[L : K[x]] < [L : K]$, on peut trouver une extension finie L' de K' et un isomorphisme φ'' de L dans L' tels que $\varphi''_{|K} = \varphi$.

□

Théorème 1.3.8

Soit K un corps parfait, L une extension finie n de K et C un corps algébriquement clos contenant K. Alors il existe n K-isomorphismes distincts de L dans C.

Remarquons que si C est algébriquement clos et contient K, toutes les racines de polynômes à coefficients dans K sont dans C, ce qui assure en particulier que C contient toute extension finie de K.

Démonstration. On distingue deux cas :

- **Premier cas** : $L = K[x]$. Le polynôme minimal P de x sur K est alors clairement de de degré n, et on sait qu'il est irréductible. Donc il a n racines simples dans C selon la proposition précédente.

  Par suite, ses racines étant deux à deux conjuguées, on obtient n K-isomorphismes distincts de $K[x]$ dans C qui envoient x sur chacune de ces racines.

- **Second cas** : cas général. On raisonne par récurrence sur $n = [L : K]$. Si $x \in L, x \notin K$, on a $K \subset K[x] \subset L$, et $q := [K[x] : K] > 1$. Par hypothèse de récurrence, on peut trouver q K-isomorphismes distincts $\sigma_1, \ldots, \sigma_q$ de $K[x]$ dans C.

  Pour $i \in [\![1; q]\!]$, $\sigma_i(K[x]) = K[\sigma_i(x)]$ donc $K[x]$ et $K[\sigma_i(x)]$ sont isomorphes via σ_i. On peut donc, selon le lemme précédent, construire une extension L_i de $K[\sigma_i(x)]$ et un isomorphisme $\tau_i L \to L_i$ prolongeant σ_i.

  Or, $K[\sigma_i[x]]$ est un corps parfait, et $[L_i : K[\sigma_i(x)]] = [L : K[x]] = \dfrac{n}{q} < n$ donc par hypothèse de récurrence, on peut trouver $\dfrac{n}{q}$ $K[\sigma_i[x]]$-isomorphismes distincts θ_{ij} de L_i dans C.

  Les morphismes $\theta_{ij} \circ \tau_i$ fournissent alors n K-isomorphismes distincts de K' dans C. Pour s'en convaincre, il suffit de calculer l'image de x.

□

Théorème 1.3.9 (*de l'élément primitif*)

Soit K un corps parfait, L une extension finie de K. Alors il existe un $x \in L$ appelé élément primitif tel que $L = K[x]$.

On utilisera le lemme suivant :

Lemme 1.3.10

Soit K un corps infini, E un K-espace vectoriel. Alors E ne peut s'écrire comme une réunion finie de sous-espaces stricts.

Démonstration. Supposons que $E = \bigcup_{j=1}^{p} E_j$ où p est pris minimal. Soit $a \in E \setminus (E_1 \cup \cdots \cup E_{p-1}), b \in E \setminus E_p$.

Si D est la droite affine passant par a et b, on a $\forall j, D \not\subset E_j$ par construction donc $D \cap E_j$ a au plus un point donc, comme E est la réunion des E_j, D a au plus p points, ce qui contredit que K est infini.

□

Démonstration (du théorème)**.** Dans le cas où K est fini, L l'est aussi donc $L^\times$ est cyclique de générateur x donc $L = K[x]$.

Dans le cas où K est infini, on a n K-isomorphismes σ_i de L dans C clôture algébrique de K.

Pour $i \neq j, V_{ij} = \{y \in L : \sigma_i(y) = \sigma_j(y)\} = \ker(\sigma_i - \sigma_j)$ est un K-sous-espace vectoriel de L distinct de L car $\sigma_i \neq \sigma_j$.

On a $L \neq \bigcup_{i,j} V_{ij}$ donc selon le lemme, on peut prendre $x \in L$ tel que $x \notin \bigcup_{i,j} V_{ij}$. Donc $x \in \bigcap_{i,j} V_{ij}^C$ et les $\sigma_i(x)$ sont deux à deux distincts. Or, ce sont des racines du polynôme minimal Π de x dans C donc $\deg \Pi \geqslant n$ soit $[K[x] : K] \geqslant n$. Ainsi, $L = K[x]$. □

En conséquence de ce théorème, il y a *exactement* n K-isomorphismes de L dans C. En effet, le polynôme minimal de l'élément primitif x est de degré $n = [L : K]$ donc il admet n racines distinctes selon la proposition 1.3.6. De plus, un K-isomorphisme de L dans C est entièrement déterminé par l'image de x, qui est nécessairement une racine du polynôme minimal de x, donc il y a autant de K-isomorphismes que de racines de ce polynôme, c'est-à-dire n.

1.4 Norme, trace, discriminant

Soit A un anneau et B un anneau contenant A. On suppose que B est un A-module libre de rang n.

Si $x \in B$, on peut considérer l'application A-linéaire $m_x : \begin{array}{ccc} B & \longrightarrow & B \\ b & \longmapsto & bx \end{array}$.

Définition 1.4.1

La trace (resp. norme, polynôme caractéristique) de x est la trace (resp. déterminant, polynôme caractéristique) de x. On la note $\mathrm{Tr}_{B/A}(x)$ *(resp.* $N_{B/A}(x), \chi_x$*).*

Remarque. Cette définition s'étend à B et A des anneaux tels que A soit un sous-anneau de B et B soit un A-module libre de type fini.

On a les propriétés immédiates suivantes :

- Si $a \in A$, la matrice de m_a est diagonale dans toute base donc $\mathrm{Tr}(a) = na, N(a) = a^n, \chi_a = (X - a)^n$.
- $x \longmapsto m_x$ est un morphisme de A-algèbres de B dans $\mathscr{L}_A(B)$ (ensemble des applications A-linéaires de B dans B).

Proposition 1.4.2

Soient K un corps et L une extension finie de K.

Si K est un corps parfait, si $x \in L$ et $x_1, \ldots, x_n$ sont les racines du polynôme minimal Π_x de x sur K dans une clôture algébrique C de K, chacune répétée $[L : K[x]]$ fois, alors $\mathrm{Tr}(x) = x_1 + \cdots + x_n$, $N_{L/K}(x) = x_1 \ldots x_n$ *et* $\chi_x = (X - x_1) \ldots (X - x_n) = \Pi_x^{[L:K[x]]}$.

Démonstration. Traitons d'abord le cas particulier où $L = K[x]$. Si P est le polynôme minimal de x sur K et $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ est de degré n, $(1, x, \ldots, x^{n-1})$ est une base de L sur K.

De plus, la matrice de m_x dans cette base est $\begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ (0) & & 1 & -a_{n-1} \end{pmatrix}$ matrice compagnon de P de polynôme caractéristique $P = (X-x_1)\ldots(X-x_n)$ donc de trace $\mathrm{Tr}(x) = x_1 + \cdots + x_n$ et de norme $x_1 \ldots x_n$.

Pour le cas général, notons $r = [L : K[x]]$. Soit Π le polynôme minimal de x sur K, et P son polynôme caractéristique relativement à L/K.

Si $(y_1, \ldots, y_q)$ est une base de $K[x]$ sur K, et $(z_1, \ldots, z_r)$ une base de L sur $K[x]$, on sait selon la démonstration de la formule des degrés que $\mathscr{B} = (y_i z_j)_{i,j}$ est une base de L sur K, et $n = qr$.

On note $A = (a_{ih})_{i,h}$ la matrice dans (y_i) de m_x. On a $\forall i, x y_i = \sum_{h=1}^{q} a_{ih} y_h$, donc $\forall i, j, x(y_i z_j) = \sum_{h=1}^{q} a_{ih}(y_h z_j)$. En ordonnant $(y_i z_j)$ dans l'ordre lexicographique en triant d'abord selon j puis selon i, on obtient que la matrice M de m_x dans $\mathscr{B}$ est $\begin{pmatrix} A & & (0) \\ & \ldots & \\ (0) & & A \end{pmatrix}$, donc $\chi_M = (\chi_A)^r$, ce qui montre le résultat.

□

Remarque. En d'autres termes, au vu de la manière dont on a construit les n K-isomorphismes $\sigma_1, \ldots, \sigma_n$ de L dans C, $\mathrm{Tr}(x) = \sum_{i=1}^{n} \sigma_i(x), N(x) = \prod_{i=1}^{n} \sigma_i(x), \chi_x = \prod_{i=1}^{n} (X - \sigma_i(x))$.

Proposition 1.4.3

Soient A un anneau intègre de corps des fractions K, qu'on suppose de caractéristique nulle, et L une extension finie de K. Si x est entier sur A, les coefficients de χ_x polynôme caractéristique de x par rapport à L/K sont entiers sur A. En particulier, $\mathrm{Tr}(x)$ et $N(x)$ sont entiers.

Démonstration. Si $\sigma_1, \ldots, \sigma_n$ sont les n K-isomorphismes de L dans une clôture algébrique de K, $x_i = \sigma_i(x)$ et il suffit d'appliquer σ_i à une équation de dépendance intégrale de x sur A. □

Définition 1.4.4

Si B est un anneau et A un sous-anneau de B tel que B soit un A-module libre de rang fini n. Si $(x_1, \ldots, x_n) \in B^n$, le discriminant de $(x_1, \ldots, x_n)$ est $D(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{B/A}((x_i x_j)_{i,j}))$.

Proposition 1.4.5

Si $(y_1, \ldots, y_n) \in B^n$ est tel que $\forall i \in [\![1; n]\!], y_i = \sum_{j=1}^{n} a_{ij} x_j, a_{ij} \in A$, alors si $A = (a_{ij})_{i,j}$ $D(y_1, \ldots, y_n) = \det(A)^2 D(x_1, \ldots, x_n)$.

Démonstration. En effet, pour $1 \leqslant p, q \leqslant n$:

$$\mathrm{Tr}(y_p y_q) = \mathrm{Tr}\left(\sum_{1\leqslant i,j\leqslant n} a_{pi}a_{qj}x_i x_j\right) = \sum_{1\leqslant i,j\leqslant n} a_{pi}a_{qj}\mathrm{Tr}(x_i x_j)$$

Par conséquent, $(\mathrm{Tr}(y_p y_q))_{p,q} = A(\mathrm{Tr}(x_i x_j))_{i,j}\,{}^tA$, d'où le résultat. □

Définition 1.4.6

Le discriminant de B sur A est $\mathscr{D}_{B/A} = (D(x_1,\dots,x_n))$ pour toute base $(x_1,\dots,x_n)$ de B sur A.

La cohérence de la définition découle de la proposition précédente, étant donné qu'une matrice de passage a un déterminant inversible.

L'intérêt de la notion réside dans la caractérisation suivante :

Proposition 1.4.7

Si A est un anneau intègre, et si $(x_1,\dots,x_n) \in B^n$, alors $(x_1,\dots,x_n)$ est une base de B si et seulement si son discriminant engendre $\mathscr{D}_{B/A}$.

Démonstration. Le sens indirect a déjà été prouvé.

Supposons que $d = D(x_1,\dots,x_n)$ engendre $\mathscr{D}_{B/A}$. Soit $(e_1,\dots,e_n)$ une base de B sur A. Alors $d' = D(e_1,\dots,e_n)$ engendre $\mathscr{D}_{B/A}$ donc on peut fixer $b \in A$ tel que $d' = bd$. De plus, $d = \det(A)^2 d'$ où A est la matrice de $(x_1,\dots,x_n)$ dans $(e_1,\dots,e_n)$.

Donc comme $d \neq 0$, on a $b\det(A)^2 = 1$ donc $\det(A)$ est inversible ce qui assure l'inversibilité de A, donc $(x_1,\dots,x_n)$ est une base de B. □

Proposition 1.4.8

Soient K un corps parfait, L/K une extension de degré n, et $\sigma_1,\dots,\sigma_n$ les n K-isomorphismes de L dans C clôture algébrique de K. Si $(x_1,\dots,x_n)$ est une base de L sur K, on a

$$D(x_1,\dots,x_n) = \det((\sigma_i(x_j))_{i,j})^2$$

Démonstration. On a $\forall x \in L, \mathrm{Tr}(x) = \sum_{k=1}^{n} \sigma_k(x)$ donc :

$$\begin{aligned} D(x_1,\dots,x_n) &= \det((\mathrm{Tr}(x_i x_j))_{i,j}) = \det\left[\left(\sum_{k=1}^{n}\sigma_k(x_i)\sigma_k(x_j)\right)_{i,j}\right] \\ &= \det((\sigma_j(x_i))_{i,j} \times (\sigma_i(x_j))_{i,j}) = \det((\sigma_i(x_j)_{i,j})^2. \end{aligned}$$

On admet que ce discriminant est non nul, ce qui est conséquence d'un lemme de Dedekind de peu d'intérêt. □

A l'aide de ce résultat et de quelques manipulations élémentaires, on obtient :

Théorème 1.4.9

Soient A un anneau intégralement clos de corps des fractions K, L une extension de degré n de K, A' la fermeture intégrale de A dans L. Alors si K est un corps parfait, A' est un sous A-module d'un A-module libre de rang n.

Corollaire 1.4.10

Sous les hypothèses du théorème précédent, si A est de plus principal, A' est un A-module libre de rang n.

Pour finir, calculons un discriminant qui nous sera utile pour la suite :

Exemple. Soit K un corps parfait, L une extension finie n de K,x un élément primitif de L et P son polynôme minimal.

$$D(1,x,\dots,x^{n-1}) = N_{L/K}(P'(x))$$

En effet, soient $x_1,\dots,x_n$ les n racines distinctes de P dans une clôture algébrique C de K, et $\sigma_1,\dots,\sigma_n$ les n K-isomorphismes de L dans C. Alors quitte à renuméroter les σ_i, on a $\forall i, \sigma_i(x) = x_i$.

Par suite,

$$D(1,x,\dots,x^{n-1}) = \det((\sigma_i(x^j))_{i,j})^2 = \det((x_i^j)_{i,j})^2 = \prod_{i<j}(x_i-x_j)^2 = \prod_{i\neq j}(x_i-x_j)$$

En effet, cet dernier déterminant est un déterminant de Vandermonde. De plus, comme $P(X) = \prod_{i=1}^{n}(X-x_i)$, on a $P'(X) = \sum_{i=1}^{n}\left(\prod_{j\neq i}(X-x_j)\right)$ donc pour $1 \leqslant i \leqslant n$, $P'(x_i) = \prod_{j\neq i}(x_i-x_j)$.

De plus, $\forall i, \sigma_i(P'(x)) = P'(\sigma_i(x)) = P'(x_i)$.

Par conséquent,

$$D(1,x,\dots,x^{n-1}) = \prod_{i=1}^{n} P'(x_i) = N_{L/K}(P'(x))$$

Chapitre 2

Anneaux de Dedekind

L'objectif de ce chapitre est de généraliser la décomposition en facteurs premiers bien connue dans un anneau factoriel en l'obtenant pour les idéaux d'un anneau de Dedekind, c'est à dire un anneau noethérien, intégralement clos et dans lequel tout idéal premier est maximal.

2.1 Anneaux noethériens

Théorème 2.1.1

Soient A un anneau et M un A-module. Les propriétés suivantes sont équivalentes :

1. *Toute famille non vide de sous-A-modules de M admet un élément maximal.*
2. *Toute suite croissante de sous-A-modules de M est stationnaire.*
3. *Tout sous-A-module de M est de type fini.*

Si l'une de ces conditions équivalentes est vérifiée, on dit que M est un module noethérien.

Si A est un anneau, il peut-être considéré comme un A-module, ses sous-modules sont alors ses idéaux. On dit que A est un anneau noethérien s'il est un A-module noethérien.

Exemple. Un anneau principal est noethérien, puisque tous ses idéaux sont principaux donc de type fini.

Proposition 2.1.2

Si A est un anneau, E un A-module, E' un sous-module de E. Alors E est un module noethérien si et seulement si E' et E/E' le sont.

Démonstration.

- Si E est noethérien. Les sous-modules de E' sont clairement les sous-modules de E contenus dans E' donc E' est noethérien.

  De plus, selon le théorème de correspondance des sous-modules, $\alpha : J/E' \longleftrightarrow J$ est une bijection de l'ensemble des sous-modules de E/E' dans l'ensemble des sous-modules de E contenant E', et cette bijection respecte les inclusions. Par conséquent, si $(J_n/E')_{n\in\mathbb{N}}$ est une suite croissante de sous-modules de E/E', (J_n) est aussi une suite croissante donc stationnaire car E est noethérien, ce qui conclut.

- Supposons que E/E' et E' sont noethériens.

  Soit (F_n) une suite croissante de sous-modules de E. E' est un module noethérien donc à partir d'un certain rang n_0, $F_n \cap E' = F_{n+1} \cap E'$. (a)

Or E/E' est noethérien donc il existe $n_1 \in \mathbb{N}$ tel que $\forall n \geqslant n_1, F_n/E' = F_{n+1}/E'$, et on peut prendre $n_1 = n_0$ sans perte de généralité.

Il s'ensuit que si $n \geqslant n_0$ et $(x,y) \in F_n \times F_{n+1}, x - y \in E'$. Donc $F_n + E' = F_{n+1} + E'$.

Montrons maintenant que $F_n = F_{n+1}$. Si $x \in F_{n+1}$, on peut trouver $y \in F_n, z \in E'$ tels que $x = y + z$ donc $x - y \in E'$. De plus, comme $F_n \subset F_{n+1}, x - y \in F_{n+1}$, donc $x - y \in F_n \cap E'$ selon (a). Donc $x \in F_n$ car $y \in F_n$.

Donc $F_{n+1} \subset F_n$, d'où par croissance de (F_n), $F_n = F_{n+1}$ à partir d'un certain rang.

□

On en déduit facilement les deux résultats suivants :

Corollaire 2.1.3

Si A est un anneau, $E_1, \ldots, E_n$ sont des A-modules, alors si tous les E_i sont noethériens, leur produit $F = \prod_{i=1}^{n} E_i$ est noethérien.

Démonstration. On effectue une récurrence sur n, triviale une fois que le cas $n = 2$ est prouvé.

Dans ce cas, classiquement, $E_1 \simeq E_1 \times \{0\} = F_1$ sous-module de F et $\varphi : \begin{array}{ccc} F & \longrightarrow & E_2 \\ (x,y) & \longmapsto & y \end{array}$ est un morphisme surjectif de noyau F_1 donc $F/F_1 \simeq E_2$ par théorème d'isomorphisme. Donc, puisque F/F_1 et F_1 sont noethériens, F est noethérien selon la proposition précédente. □

Proposition 2.1.4

Si A est un anneau noethérien et E un A-module de type fini, alors E est un module noethérien.

Démonstration. Si $(e_1, \ldots, e_n)$ est un système générateur de E, alors $\varphi : \begin{array}{ccc} A^n & \longrightarrow & E \\ (x_1, \ldots, x_n) & \longmapsto & \sum x_i e_i \end{array}$ est une application A-linéaire surjective donc $E \simeq A^n/\ker(\varphi)$ et selon la proposition et le corollaire précédent, E est noethérien. □

En particulier, on dispose du théorème suivant :

Théorème 2.1.5

Si A est un anneau noethérien intégralement clos, $K = \mathrm{Frac}(A)$, L une extension de degré n sur K, et si A' est la fermeture intégrale de A dans L, alors, en supposant que K est un corps parfait, A' est un A-module de type fini et un anneau noethérien.

Démonstration. On a montré dans le chapitre précédent que sous ces hypothèses, A' est un sous-module d'un A-module libre de rang n, donc d'un A-module noethérien selon la proposition précédente, donc par définition, A' est un A-module de type fini.

De plus, si I est un idéal de A', c'est aussi un sous A-module de A' donc les idéaux satisfont la condition "toute famille non vide d'idéaux admet un élément maximal", ce qui prouve que A' est un anneau noethérien. □

2.2 Définition des anneaux de Dedekind

Définition 2.2.1

Soit A un anneau. A est un anneau de Dedekind si c'est un anneau noethérien, intégralement clos et si tout idéal premier de A est maximal.

Exemple. $\mathbb{Z}$ est un anneau de Dedekind. En effet il est principal donc noethérien et intégralement clos. De plus, si $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps donc $p\mathbb{Z}$ est un idéal maximal.

Théorème 2.2.2

Si A est un anneau de Dedekind et $K = \mathrm{Frac}(A)$, si L est une extension finie de K et A' est la fermeture intégrale de A dans L, et si K est un corps parfait, alors A' est un anneau de Dedekind et un A-module de type fini.

Démonstration.

- A' est intégralement clos par définition.
- A' est un A-module de type fini selon la proposition 1.4.9. Par conséquent, selon la proposition 2.1.4, c'est un A-module noethérien donc en particulier un anneau noethérien puisque les idéaux de A' sont des sous A-modules de A'.
- Soit β idéal premier non nul de A'. Soit $x \neq 0 \in \beta$. On a une équation de dépendance intégrale, qu'on suppose de degré minimal.

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

Il est donc immédiat que $a_0 \in A'x \cap A \subset \beta \cap A$, et $a_0 \neq 0$ sinon on obtiendrait une équation de degré $n-1$ en simplifiant par x.

Donc $a_0 \in \beta \cap A$ et donc $\beta \cap A \neq \{0\}$.

Mais on montre sans difficulté que $\beta \cap A$ est un idéal premier de A, c'est donc un idéal maximal car A est de Dedekind, donc $A/(\beta \cap A)$ est un corps.

Or $\varphi : \begin{array}{ccc} A & \longrightarrow & A'/\beta \\ a & \longmapsto & a \bmod \beta \end{array}$ est un morphisme de noyau $\beta \cap A$ qui passe donc au quotient en $\tilde{\varphi} : \begin{array}{ccc} A & \longrightarrow & A'/\beta \\ a \bmod \beta \cap A & \longmapsto & a \bmod \beta \end{array}$ morphisme injectif. Donc A'/β contient un sous-corps (*i.e.* un sous-anneau qui est un corps) B isomorphe à $A/(\beta \cap A)$.

De plus, A'/β est entier sur B. En effet, $B = \{a \mod \beta, a \in A\}$ et il suffit de réduire pour chaque $x \in A'$ son équation de dépendance intégrale modulo β. Donc A'/β est un corps car B en est un, et β est maximal, ce qui conclut.

□

2.3 Décomposition des idéaux fractionnaires dans un anneau de Dedekind

Dans toute cette section, on se place dans le cadre suivant : A est un anneau de Dedekind, K est son corps des fractions.

Définition 2.3.1

Un idéal fractionnaire de A est un sous A-module I de K tel qu'il existe $d \in A \setminus \{0\}$ tel que $I \subset d^{-1}A$.

Cela revient à dire que tous les éléments de I ont un dénominateur commun d.
Quelques propriétés :

- Un idéal de A est un idéal fractionnaire, on l'appelle alors *idéal entier*.
- Un sous A-module de type fini I de K est un idéal fractionnaire. En effet, si $(x_1, \dots, x_n)$ est un système générateur de I, on peut trouver un dénominateur commun d aux $x_i \in K$. Alors $\forall i, x_i = d^{-1}\alpha_i$ où $\alpha_i \in A$, donc par linéarité, $I \subset d^{-1}A$.
- Réciproquement, comme A est noethérien, tout idéal fractionnaire I est un sous A-module de K de type fini. En effet, $I \subset d^{-1}A$ et A est un A-module de type fini donc I est de type fini puisque $d^{-1}A \simeq A$ en tant que modules.
- L'ensemble des idéaux fractionnaires non nuls de A forme un monoïde commutatif pour la multiplication définie comme suit : si I, I' idéaux fractionnaires,

$$II' = \left\{ \sum_{i=1}^{n} x_i y_i, n \in \mathbb{N}, x_i \in I, y_i \in I' \right\}$$

  Son élément neutre est A.

On va maintenant obtenir la décomposition d'un idéal fractionnaire en produits d'idéaux premiers.

Proposition 2.3.2

Soit A anneau de Dedekind qui n'est pas un corps. Alors tout idéal maximal de A est inversible dans le monoïde des idéaux fractionnaires de A.

On aura besoin de deux petits lemmes pour mener à bien la preuve :

Lemme 2.3.3

Soit A un anneau noethérien, soit $\mathfrak{p}$ un idéal premier de A, $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ r des idéaux de A tels que $\mathfrak{a}_1 \dots \mathfrak{a}_r \subset \mathfrak{p}$. Alors $\exists 1 \leqslant i \leqslant r : \mathfrak{a}_i \subset \mathfrak{p}$.

Démonstration. Supposons que $\forall i, \mathfrak{a}_i \not\subset \mathfrak{p}$, on peut fixer $a_i \in \mathfrak{a}_i$ tel que $a_i \notin \mathfrak{p}$. Donc $a_1 \dots a_r \notin \mathfrak{p}$ puisque $\mathfrak{p}$ est un idéal premier : contradiction. □

Lemme 2.3.4

Soit A un anneau noethérien intègre. Tout idéal non nul de A contient un produit d'idéaux premiers non nuls.

Démonstration. Soit ϕ l'ensemble des idéaux I non nuls de A tels que I ne contient aucun produit d'idéaux premiers non nuls, et supposons $\phi \neq \emptyset$. Comme A est noethérien, ϕ possède un élément maximal $\mathfrak{b}$.

Si $\mathfrak{b}$ était premier, on aurait $\mathfrak{b} \notin \phi$ donc $\mathfrak{b}$ n'est pas premier. Par suite, on peut trouver $(x, y) \in (A \setminus \mathfrak{b})^2$ tels que $xy \in \mathfrak{b}$.

$\mathfrak{b}+Ax$ et $\mathfrak{b}+Ay$ sont des idéaux contenant strictement $\mathfrak{b}$ donc ils ne peuvent appartenir à ϕ par maximalité de $\mathfrak{b}$. Donc il existe $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ tels que $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \mathfrak{b}+Ax$, $\mathfrak{q}_1 \dots \mathfrak{q}_s \subset \mathfrak{b}+Ay$.

Or, $xy \in \mathfrak{b}$ donc $(\mathfrak{b}+Ax)(\mathfrak{b}+Ay) = \mathfrak{b}$ donc

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \subset \mathfrak{b}$$

Cela contredit le fait que $\mathfrak{b} \in \phi$ donc $\phi = \emptyset$. □

Démonstration (de la proposition)**.** Soit $\mathfrak{m}$ un idéal maximal de A ; $\mathfrak{m} \neq \{0\}$ car A n'est pas un corps.

On pose $\mathfrak{m}' = \{x \in K, x\mathfrak{m} \subset A\}$.

$\mathfrak{m}'$ est évidemment un sous A-module de K et si $a \in \mathfrak{m} \setminus \{0\}$ et $x \in \mathfrak{m}'$, alors $xa \in A$ donc $x \in a^{-1}A$, d'où $\mathfrak{m}' \subset a^{-1}A$ et $\mathfrak{m}'$ est donc un idéal fractionnaire de A.

Montrons que $\mathfrak{m}\mathfrak{m}' = A$.

On a, par définition de $\mathfrak{m}'$, $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}' \subset A$. Or, $\mathfrak{m}$ est un idéal maximal donc $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ ou $\mathfrak{m}\mathfrak{m}' = A$.

Supposons que $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$.

Soit $x \in \mathfrak{m}'$. $x\mathfrak{m} \subset A$ donc par une récurrence immédiate, $\forall n \in \mathbb{N}, x^n\mathfrak{m} \subset A$. Par conséquent, si $d \neq 0$ et $d \in \mathfrak{m}$, d est un dénominateur commun des $(x^n)_{n\in\mathbb{N}}$ de sorte que $A[x]$ est un idéal fractionnaire. Mais A est noethérien donc $A[x]$ est un A-module de type fini selon une des propriétés ci-dessus. Donc x est entier sur A et comme A est intégralement clos, $x \in A$. On a ainsi $\mathfrak{m}\mathfrak{m}' = \mathfrak{m} \Rightarrow \mathfrak{m}' = A$.

Il s'agit donc en dernier lieu de prouver qu'on ne peut avoir $\mathfrak{m}' = A$.

Soit $a \in \mathfrak{m} \setminus \{0\}$. Alors Aa contient un produit d'idéaux premiers non nuls $\mathfrak{p}_1 \dots \mathfrak{p}_r$ selon le lemme 2.3.4, et on peut prendre r minimal. On a donc $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \mathfrak{m}$, donc comme $\mathfrak{m}$ est premier, selon le lemme 1, il contient un $\mathfrak{p}_i$, prenons $i = 1$ par exemple. Par maximalité de $\mathfrak{p}_1$, on a $\mathfrak{m} = \mathfrak{p}_1$.

Si $\mathfrak{b} := \mathfrak{p}_2 \dots \mathfrak{p}_r$, on a $\mathfrak{m}\mathfrak{b} \subset Aa$ mais $\mathfrak{b} \not\subset Aa$ car on a pris r minimal. Donc $\exists b \in \mathfrak{b} : b \notin Aa$. Or, $\mathfrak{m}b \subset \mathfrak{m}\mathfrak{b} \subset Aa$ donc $\mathfrak{m}ba^{-1} \subset A$, d'où par définition de $\mathfrak{m}'$, $ba^{-1} \in \mathfrak{m}'$. Or, si $\mathfrak{m}' = A$, on aurait $b \in Aa$ ce qui est absurde. Donc $\mathfrak{m}' \neq A$, et finalement $\mathfrak{m}\mathfrak{m}' = A$. □

Théorème 2.3.5 (*de décomposition en idéaux premiers*)

Soit A un anneau de Dedekind, $\mathscr{P}$ l'ensemble des idéaux premiers non nuls de A. Alors tout idéal fractionnaire non nul $\mathfrak{b}$ de A se décompose de manière unique sous la forme

$$\mathfrak{b} = \prod_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})}$$

où les $n_\mathfrak{p}(\mathfrak{b})$ sont des entiers relatifs presque tous nuls.

Démonstration. • **Existence** : On peut se ramener au cas où $\mathfrak{b}$ est un idéal de A. En effet, $\exists d \in A : d\mathfrak{b} \subset A$ donc $d\mathfrak{b}$ est un idéal de A et en supposant le résultat obtenu pour Ad, on a $\mathfrak{b} = (d\mathfrak{b})(Ad)^{-1}$. On suppose donc $\mathfrak{b}$ idéal de A.

Soit ϕ l'ensemble des idéaux non nuls de A qui ne sont pas produit d'idéaux premiers, et on suppose $\phi \neq \emptyset$. Il admet donc un élément maximal $\mathfrak{a}$.

Soit $\mathfrak{p}$ l'élément maximal de la famille des idéaux contenant $\mathfrak{a}$, qui existe car A est noethérien. C'est clairement un idéal maximal. On note $\mathfrak{p}'$ son inverse dans le monoïde des idéaux fractionnaires de A, selon la proposition précédente.

On a $\mathfrak{a}\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$ et $A = \mathfrak{p}\mathfrak{p}' \subset A\mathfrak{p}' \subset \mathfrak{p}'$, donc $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}'$.

Si $\mathfrak{a} = \mathfrak{a}\mathfrak{p}'$, alors si $x \in \mathfrak{p}'$, on a $\forall n \in \mathbb{N}, x\mathfrak{a} \subset \mathfrak{a}, \dots, x^n\mathfrak{a} \subset \mathfrak{a}$, donc en réutilisant le raisonnement de la démonstration de la proposition précédente, x est entier sur A intégralement clos donc $x \in A$, ce qui est absurde puisque $\mathfrak{p}' \neq A$. Donc $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}'$. Donc par maximalité de $\mathfrak{a}$, $\mathfrak{a}\mathfrak{p}' \notin \phi$ donc on peut fixer $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ idéaux premiers tels que $\mathfrak{a}\mathfrak{p}' = \mathfrak{p}_1 \dots \mathfrak{p}_n$. Par suite, $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_n$ et $\mathfrak{a} \notin \phi$ ce qui est contradictoire.

Donc $\phi = \emptyset$, ce qui conclut.

- **Unicité** : Si $\prod_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p}^{n(\mathfrak{p})} = \prod_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p}^{m(\mathfrak{p})}$ où les $n(\mathfrak{p}), m(\mathfrak{p})$ sont des entiers relatifs presque tous nuls, on a $\prod_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p}^{n(\mathfrak{p})-m(\mathfrak{p})} = A$. Si les $n(\mathfrak{p})-m(\mathfrak{p})$ ne sont pas tous nuls, il existe des idéaux p_i et q_j deux à deux distincts et $\alpha_i > 0, \beta_j > 0$ tels que $p_1 \supset \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{j=1}^{s} q_j^{\beta_j}$.

  En particulier, selon le premier lemme de la proposition ci-dessus, il existe $1 \leqslant j \leqslant s$: $p_1 \supset q_j$ donc par maximalité de q_j, $p_1 = q_j$ ce qui est absurde.

□

Corollaire 2.3.6

Si A est un anneau de Dedekind, l'ensemble des idéaux fractionnaires de A a une structure de groupe commutatif.

On a quelques propriétés aisément vérifiables sur cette décomposition :

1. $\forall \mathfrak{p} \in \mathscr{P}, n_{\mathfrak{p}}(\mathfrak{ab}) = n_{\mathfrak{p}}(\mathfrak{a}) + n_{\mathfrak{p}}(\mathfrak{b})$
2. $\mathfrak{a} \subset \mathfrak{b} \iff \forall \mathfrak{p} \in \mathscr{P}, n_{\mathfrak{p}}(\mathfrak{b}) \leqslant n_{\mathfrak{p}}(\mathfrak{a})$
3. $\forall \mathfrak{p} \in \mathscr{P}, n_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) = \inf(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b}))$ ($\mathfrak{a}+\mathfrak{b}$ est la borne supérieure pour l'inclusion de l'ensemble des idéaux contenant $\mathfrak{a}$ et $\mathfrak{b}$)

Chapitre 3

Corps de nombres

3.1 Définition et traduction des résultats précédents

Définition 3.1.1

Un corps de nombres est une extension finie de $\mathbb{Q}$.

Définition 3.1.2

Si K *est un corps de nombres, la fermeture intégrale de* $\mathbb{Z}$ *dans* K *est appelée anneau des entiers de* K *et est notée* $\mathcal{O}_K$.

$\mathcal{O}_K$ est à K ce que $\mathbb{Z}$ est à $\mathbb{Q}$, comme le montre le lemme suivant :

Lemme 3.1.3

$K = \mathrm{Frac}(\mathcal{O}_K)$.

Démonstration. On a $\mathcal{O}_K \subset K$ qui est un corps donc $\mathrm{Frac}(\mathcal{O}_K) \subset K$.

Soit $x \in K$. x est algébrique sur $\mathbb{Q}$ donc on a une équation de dépendance intégrale

$$x^n + \frac{p_{n-1}}{q_{n-1}}x^{n-1} + \cdots + \frac{p_0}{q_0} = 0$$

En multipliant par $(q_0 \dots q_{n-1})^n$, on a

$$x^n + p_{n-1}q_0 \dots q_{n-2}(q_0 \dots q_{n-1}x)^{n-1} + \cdots + p_0 q_1 \dots q_{n-1}(q_0 \dots q_{n-1})^{n-1} = 0$$

ce qui prouve que $q_0 \dots q_{n-1}x$ appartient à $\mathcal{O}_K$. Donc $K \subset \mathrm{Frac}(\mathcal{O}_K)$ □

Si L est une extension finie de K, on note $\mathcal{O}_L$ la fermeture intégrale de $\mathcal{O}_K$ dans L, qui est aussi l'anneau des entiers de L selon la transitivité du caractère entier (proposition 1.2.5).

Proposition 3.1.4

Soient K *un corps de nombres et* $x \in \mathcal{O}_K$. *Alors* $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Z}, N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$

Démonstration. C'est la traduction de la proposition 1.4.3. □

Proposition 3.1.5

Si K *est un corps de nombres,* $\mathcal{O}_K$ *est un anneau de Dedekind et un* $\mathbb{Z}$*-module libre de rang* $[K : \mathbb{Q}]$.

Démonstration. K est une extension finie de $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ où $\mathbb{Z}$ est principal. Selon le théorème 2.2.2, $\mathcal{O}_K$ est un anneau de Dedekind ; et le corollaire 1.4.10 nous donne que $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.

□

Le concept d'anneau de Dedekind est donc un cadre idéal pour l'étude d'un corps de nombres K pour deux raisons : d'une part, il permet d'obtenir sous des hypothèses minimales la décomposition d'un idéal fractionnaire en produit d'idéaux premiers. Mais surtout, le théorème 2.2.2 nous donne que pour toute extension finie L d'un corps de nombres K, $\mathcal{O}_L$ et $\mathcal{O}_K$ sont des anneaux de Dedekind.

Notation : Dans toute la suite, $\mathrm{Spec}(\mathcal{O}_K)$ désignera l'ensemble des idéaux premiers d'un corps de nombres K. On dira d'ailleurs « idéal premier de K » pour « idéal premier de $\mathcal{O}_K$ ».

Si K est un corps de nombres, l'ensemble P des idéaux fractionnaires principaux, c'est-à-dire de la forme (a) où $a \in K^\times$ est un sous-groupe du groupe des idéaux fractionnaires I.

Définition 3.1.6

Le groupe des classes d'idéaux est $C := I/P$.

On admet le théorème suivant :

Théorème 3.1.7

Si K est un corps de nombres, C est fini.

Démonstration. Voir [4], page 75. □

3.2 Décomposition dans une extension, idéaux ramifiés

On considère désormais un corps de nombres K, et une extension finie L de K. On

Le problème, qui sera central dans toute la fin de ce mémoire, est de savoir comment se décompose un idéal $\mathfrak{p}$ premier de K (c'est à dire de $\mathcal{O}_K$) dans L.

En effet, $\mathfrak{p}\mathcal{O}_L$ est un idéal de $\mathcal{O}_L$ donc selon le théorème de décomposition en idéaux premiers, on peut trouver $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ idéaux premiers et $e_1, \ldots, e_r \geqslant 1$ tels que

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

Définition 3.2.1

Soit $\mathfrak{p}$ un idéal premier de K. On dit que $\mathfrak{P}$ idéal premier de L est au-dessus de $\mathfrak{p}$ si $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

Remarque. On a vu que $\mathfrak{P} \cap \mathcal{O}_K$ est un idéal premier de K donc tout idéal premier $\mathfrak{P}$ de L est nécessairement au-dessus d'un idéal premier de K.

Proposition 3.2.2

Soit $\mathfrak{p}$ un idéal premier de K tel que $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$. Alors les idéaux au-dessus de $\mathfrak{p}$ sont les $\mathfrak{P}_i$.

Démonstration.

- Si $\mathfrak{P}$ est un idéal premier de $\mathcal{O}_L$ et $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, alors $\prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \subset \mathfrak{p}\mathcal{O}_L = (\mathfrak{P} \cap \mathcal{O}_K)\mathcal{O}_L \subset \mathfrak{P}$ donc comme $\mathfrak{P}$ est premier, il contient un des $\mathfrak{P}_i$, donc est égal à l'un d'entre eux par maximalité.

- Soit $j \in [\![1; r]\!]$, on a $\mathfrak{p} = (\mathfrak{p}\mathcal{O}_L) \cap \mathcal{O}_K = \left(\prod_{i=1}^{r} \mathfrak{P}_i^{e_i}\right) \cap \mathcal{O}_K \subset \mathfrak{P}_j \cap \mathcal{O}_K$ donc par maximalité, $\mathfrak{p} = \mathfrak{P}_j \cap \mathcal{O}_K$.

□

On va maintenant expliquer la notion de *degré résiduel*.

On reprend les notations de la proposition précédente. Soit $j : \mathcal{O}_K \to \mathcal{O}_L$ le morphisme d'inclusion, et $\pi_i : \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}_i$ la projection. $\varphi = j \circ \pi_i$ est un morphisme de noyau $\mathfrak{p}$. En effet, $\varphi(x) = 0 \Leftrightarrow (x \mod \mathfrak{P}_i = 0 \text{ et } x \in \mathcal{O}_K) \Leftrightarrow x \in \mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$.

Donc φ passe au quotient en un morphisme injectif $\overline{\varphi} : \begin{array}{ccc} \mathcal{O}_K/\mathfrak{p} & \longrightarrow & \mathcal{O}_L/\mathfrak{P}_i \\ a \mod \mathfrak{p} & \longmapsto & a \mod \mathfrak{P}_i \end{array}$,
de sorte que $\mathcal{O}_K/\mathfrak{p}$ s'identifie à un sous-corps de $\mathcal{O}_L/\mathfrak{P}_i$ (qui est un corps car $\mathfrak{P}_i$ est maximal car premier dans $\mathcal{O}_L$ de Dedekind).

Or, on a vu dans le théorème 2.1.5 que $\mathcal{O}_L$ est un $\mathcal{O}_K$-module de type fini, donc $\mathcal{O}_L/\mathfrak{P}_i$ est un espace vectoriel de dimension finie sur $\mathcal{O}_K/\mathfrak{p}$. En effet, si $(\alpha_1, \ldots, \alpha_r)$ est une famille génératrice de $\mathcal{O}_L$ en tant que $\mathcal{O}_K$-module, on a $\forall b \in \mathcal{O}_L, \exists (a_1, \ldots, a_r) \in \mathcal{O}_K^r : b = \sum_{i=1}^{r} a_i \alpha_i$
donc $b \mod \mathfrak{P}_i = \sum_{i=1}^{r} (a_i \mod \mathfrak{P}_i)(\alpha_i \mod \mathfrak{P}_i) = \sum_{i=1}^{r} \overline{\varphi}(a_i \mod \mathfrak{p})(\alpha_i \mod \mathfrak{P}_i)$.

Définition 3.2.3

On reprend les notations de la proposition précédente.
Le degré $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ est appelé degré résiduel de $\mathfrak{P}_i$ sur $\mathcal{O}_K$.
Le coefficient e_i est appelé indice de ramification de $\mathfrak{P}_i$ sur $\mathcal{O}_K$.

Remarque. On a également $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{p}$ ($\supset$ est évident, $\subset$ se déduit alors de la première propriété suivant le théorème de décomposition).

Donc $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ est également un espace vectoriel de dimension finie sur $\mathcal{O}_K/\mathfrak{p}$, ce qui justifie la cohérence de l'énoncé suivant.

Théorème 3.2.4

En gardant les notations précédentes, on a :

$$\sum_{i=1}^{r} e_i f_i = [\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L : \mathcal{O}_K/\mathfrak{p}] = [L : K]$$

Démonstration. On ne montrera que la première égalité, pour ne pas avoir à développer trop d'algèbre commutative.

Écrivons $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$.

Les $\mathfrak{P}_i^{e_i}$ sont étrangers deux à deux. En effet, supposons qu'un idéal autre que $\mathcal{O}_L$ contienne $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j}$ pour $i \neq j$ fixés. Si $\mathfrak{m}$ est un idéal maximal contenant $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j}$ ($\mathcal{O}_L$ est noethérien), on a $\mathfrak{P}_i^{e_i} \subset \mathfrak{m}$ et $\mathfrak{P}_j^{e_j} \subset \mathfrak{m}$ donc comme $\mathfrak{m}$ est premier, $\mathfrak{P}_i \subset \mathfrak{m}$ et $\mathfrak{P}_j \subset \mathfrak{m}$, ce qui, par maximalité de $\mathfrak{P}_i$ et $\mathfrak{P}_j$ donne $\mathfrak{m} = \mathfrak{P}_i = \mathfrak{P}_j$: absurde. Donc $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = \mathcal{O}_L$.

Ainsi, en appliquant le théorème chinois, on a un isomorphisme d'anneaux

$$\begin{array}{rccc} \overline{\varphi} : & \mathscr{O}_L/\mathfrak{p}\mathscr{O}_L & \longrightarrow & \prod_{i=1}^{r} \mathscr{O}_L/\mathfrak{P}_i^{e_i} \\ & x \mod \mathfrak{p}\mathscr{O}_L & \longmapsto & (x \mod \mathfrak{P}_1^{e_1}, \ldots, x \mod \mathfrak{P}_r^{e_r}) \end{array}$$

qui est également un isomorphisme de $\mathscr{O}_K/\mathfrak{p}$-espaces vectoriels.

En effet, $\mathscr{O}_K/\mathfrak{p}$ s'identifie à un sous-corps de $\mathscr{O}_L/\mathfrak{p}\mathscr{O}_L$ via $a \mod \mathfrak{p} \longmapsto a \mod \mathfrak{p}\mathscr{O}_L$, et à un sous corps de $\prod_{i=1}^{r} \mathscr{O}_L/\mathfrak{P}_i^{e_i}$ via $a \mod \mathfrak{p} \longmapsto (a \mod \mathfrak{P}_1^{e_1}, \ldots, a \mod \mathfrak{P}_r^{e_r})$.

On peut donc se restreindre au cas où $\mathfrak{p}\mathscr{O}_L = \mathfrak{P}^e$, $\mathfrak{P}$ idéal premier de $\mathscr{O}_L$, $e \geqslant 1$.

$$\mathscr{O}_L \supset \mathfrak{P} \supset \mathfrak{P}^2 \supset \cdots \subset \mathfrak{P}^e = \mathfrak{p}\mathscr{O}_L$$

$\mathfrak{P}$ et $\mathfrak{P}^2$ sont des idéaux de $\mathscr{O}_L$ donc des $\mathscr{O}_L$-modules. Donc $\mathfrak{P}/\mathfrak{P}^2$ est un $\mathscr{O}_L$-module avec la loi $b.[x]_{\mathfrak{P}^2} = [bx]_{\mathfrak{P}^2}$, et si $b \in \mathfrak{P}, [bx]_{\mathfrak{P}^2} = 0$ donc $\mathfrak{P}/\mathfrak{P}^2$ est un $\mathscr{O}_L/\mathfrak{P}$-espace vectoriel.

Selon le théorème de correspondance des sous-modules, les sous $\mathscr{O}_L/\mathfrak{P}$-espaces vectoriels de $\mathfrak{P}/\mathfrak{P}^2$, qui sont évidemment ses sous $\mathscr{O}_L$-modules, sont les $J/\mathfrak{P}^2$ quand $\mathfrak{P}$ est un sous-module de $\mathfrak{P}$ contenant $\mathfrak{P}^2$, soit $\mathfrak{P}^2 \subset J \subset \mathfrak{P}$, soit $J = \mathfrak{P}$ ou $J = \mathfrak{P}^2$ en considérant la $\mathfrak{P}$-valuation de J, car $\mathfrak{P}$ est un idéal premier.

Donc $\mathfrak{P}/\mathfrak{P}^2$ n'a que deux sous-espaces vectoriels : $\{0\}$ et lui-même, ce qui prouve qu'il est de dimension 1 sur $\mathscr{O}_L/\mathfrak{P}$. Donc comme $\mathscr{O}_L/\mathfrak{P}$ est un espace vectoriel de dimension f sur $\mathscr{O}_K/\mathfrak{p}$, selon la formule des degrés, $\mathfrak{P}/\mathfrak{P}^2$ est de dimension f sur $\mathscr{O}_K/\mathfrak{p}$.

En faisant le même raisonnement pour tous les $\mathfrak{P}^j/\mathfrak{P}^{j+1}$, où $1 \leqslant j \leqslant e-1$, on obtient que ce sont des $\mathscr{O}_K/\mathfrak{p}$-espaces vectoriels de dimension f.

Enfin, $\mathscr{O}_L/\mathfrak{p}\mathscr{O}_L = \mathscr{O}_L/\mathfrak{P}^e$ est un $\mathscr{O}_K/\mathfrak{p}$-espace vectoriel et on a une suite de sous-espaces vectoriels :

$$\{0\} \subset \mathfrak{P}^{e-1}/\mathfrak{P} \subset \cdots \subset \mathfrak{P}^2/\mathfrak{P}^e \subset \mathfrak{P}/\mathfrak{P}^e \subset \mathscr{O}_L/\mathfrak{P}^e$$

De plus, il est clair qu'en tant qu'$\mathscr{O}_K/\mathfrak{p}$-espaces vectoriels, $\forall j, (\mathfrak{P}^j/\mathfrak{P}^e)/(\mathfrak{P}^{j+1}/\mathfrak{P}^e) \simeq (\mathfrak{P}^j/\mathfrak{P}^{j+1})$ (on pose $\mathfrak{P}^0 = \mathscr{O}_L$, le raisonnement est le même) donc selon ce qui précède, $\dim(\mathfrak{P}^j/\mathfrak{P}^e) - \dim(\mathfrak{P}^{j+1}/\mathfrak{P}^e) = f$, d'où en sommant de $j = 0$ à $r-1$, on a $fr = [\mathscr{O}_L/\mathfrak{P}^e : \mathscr{O}_K/\mathfrak{p}]$. □

Remarque. Étant donné un idéal premier de K, cette formule nous assure qu'il y a au plus $[L : K]$ idéaux premiers au-dessus de lui.

Définition 3.2.5

Soit $\mathfrak{p}$ idéal premier de K, L une extension finie de K. On note $\mathfrak{p}\mathscr{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ sa décomposition en facteurs premiers dans L.

- *On dit que $\mathfrak{p}$ est ramifié dans L si $\exists i : e_i \geqslant 2$.*
- *Sinon, on dit que $\mathfrak{p}$ est non ramifié ou décomposé.*
- *Si $\mathfrak{p}$ est non ramifié et $r = [L : K]$, on dit qu'il est totalement décomposé.*

Remarque. Un idéal premier est donc totalement décomposé si tous les degrés résiduels f_i valent 1.

En fait, les idéaux premiers de K qui se ramifient dans L sont en nombre fini. Ce fait sera crucial pour démontrer le théorème de Chebotarev, qui étudie la répartition des idéaux totalement décomposés, puisqu'il nous permettra de les « ignorer » au sein de l'infinité des idéaux décomposés.

Théorème 3.2.6

Soit K un corps de nombres, L une extension finie de K, on note $\mathfrak{D}_{L/K}$ l'idéal de $\mathcal{O}_K$ engendré par les discriminants des bases de L sur K contenues dans $\mathcal{O}_L$. Alors si $\mathfrak{p}$ est un idéal premier de K, $\mathfrak{p}$ est ramifié dans L si et seulement si il contient $\mathfrak{D}_{L/K}$. Par conséquent, les idéaux premiers de K ramifiés dans L sont en nombre fini.

Démonstration. Admis (la démonstration est assez technique). □

3.3 Norme d'un idéal

On prend K un corps de nombres, et on note $N(x) = N_{K/\mathbb{Q}}(x)$.

Proposition 3.3.1

Pour $x \in \mathcal{O}_K$, $|N(x)| = \mathrm{Card}(\mathcal{O}_K/(x))$.

Démonstration. Comme $\mathbb{Z}$ est principal, selon le corollaire 1.4.10, $\mathcal{O}_K$ est un $\mathbb{Z}$-module de rang $n = [K : \mathbb{Q}]$. On en fixe une base $(e_1, \dots, e_n)$.

Alors $(x) = \mathcal{O}_K x$ est un sous-$\mathbb{Z}$-module de $\mathcal{O}_K$, de rang n car $(xe_1, \dots, xe_n)$ en est une base, donc on sait qu'il existe $(c_1, \dots, c_n) \in \mathbb{Z}^n$ tel que $c_i | c_{i+1}$ et $(c_1 e_1, \dots, c_n e_n)$ est une base de $\mathcal{O}_K x$. On peut prendre $c_i > 0$ sans perte de généralités.

On a donc $\mathcal{O}_K/(x) \simeq \prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$ via le morphisme de $\mathbb{Z}$-modules

$$\begin{array}{rccl} \varphi : & \mathbb{Z}^n & \longrightarrow & \mathcal{O}_K/(x) \\ & (x_1, \dots, x_n) & \longmapsto & \left(\sum_{i=1}^{n} x_i e_i\right) \mod A \end{array}$$

de noyau $\prod_{i=1}^{n} c_i\mathbb{Z}$ donc $\mathcal{O}_K/(x)$ a $c_1 \dots c_n$ éléments.

Par ailleurs, comme $(xe_1, \dots, xe_n)$ est une autre base de $\mathcal{O}_K x$, donc on définit un automorphisme u de $\mathcal{O}_K x$ en posant $u(c_i e_i) = xe_i$. On a par suite $\det(u) = \pm 1$.

De plus, si $v : \begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_K \\ e_i & \longmapsto & c_i e_i \end{array}$, alors v est représentée par $\mathrm{Diag}(c_1, \dots, c_n)$ dans $(e_1, \dots, e_n)$, d'où $\det(v) = c_1 \dots c_n$.

Finalement, l'application de multiplication par x restreinte à $\mathcal{O}_K$ n'est autre que $u \circ v$, donc $N(x) = \det(m_x) = \pm c_1 \dots c_n$ selon ce qui précède.

En effet, $K = \mathrm{Frac}(\mathcal{O}_K)$ et $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ donc m_x et sa restriction à $\mathcal{O}_K$ ont le même déterminant. □

Par extension, on peut donc définir, pour m idéal entier non nul de K, $N(\mathfrak{m}) = \mathrm{Card}(\mathcal{O}_K/\mathfrak{m})$.

Théorème 3.3.2

Si $\mathfrak{a}, \mathfrak{b}$ sont deux idéaux entiers non nuls de K, $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Démonstration. • Premier cas : $\mathfrak{b} = \mathfrak{m}$ est un idéal maximal.

Alors la projection $\pi : \mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{a}$ passe au quotient en $\nu : \mathcal{O}_K/(\mathfrak{am}) \to \mathcal{O}_K/\mathfrak{a}$ car $\mathfrak{am} \subset \mathfrak{a} = \ker \pi$. ν est un morphisme surjectif de noyau $\mathfrak{a}/\mathfrak{am}$.

Finalement, $\mathcal{O}_K/\mathfrak{a} \simeq (\mathcal{O}_K/\mathfrak{am})/(\mathfrak{a}/\mathfrak{am})$ et $\mathrm{Card}(\mathcal{O}_K/\mathfrak{am}) = \mathrm{Card}(\mathcal{O}_K/\mathfrak{a})\mathrm{Card}(\mathfrak{a}/\mathfrak{am})$.

De plus $\mathfrak{a}/\mathfrak{am}$ est un $\mathcal{O}_K$-module en tant que quotient de $\mathcal{O}_K$-modules. De plus si $x \in \mathfrak{m}$, alors $\forall \alpha \in \mathfrak{a}/\mathfrak{am}, x \cdot \alpha = 0$, donc $\mathfrak{a}/\mathfrak{am}$ est en réalité un $\mathcal{O}_K/\mathfrak{m}$-espace vectoriel, et ses sous-espaces vectoriels sont ses sous $\mathcal{O}_K$-modules.

Selon le théorème de correspondance des sous-modules, ils sont de la forme $\mathfrak{q}/\mathfrak{am}$ où $\mathfrak{q}$ est un idéal de $\mathfrak{a}$ tel que $\mathfrak{am} \subset \mathfrak{q} \subset \mathfrak{a}$.

Un tel idéal q vérifie donc $\forall \mathfrak{p} \in \mathscr{P}, n_\mathfrak{p}(\mathfrak{am}) \geqslant n_\mathfrak{p}(\mathfrak{q}) \geqslant n_\mathfrak{p}(\mathfrak{a})$.

Or, $n_\mathfrak{p}(\mathfrak{am}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{m}) = \begin{cases} n_\mathfrak{p}(\mathfrak{a}) & \text{si} \quad \mathfrak{p} \neq \mathfrak{m} \\ n_\mathfrak{p}(\mathfrak{a}) + 1 & \text{sinon} \end{cases}$.

Donc nécessairement $\mathfrak{q} = \mathfrak{a}$ ou $\mathfrak{q} = \mathfrak{am}$. Ainsi, $\mathfrak{a}/\mathfrak{am}$ n'ayant que deux sous-espaces vectoriels, il est de dimension 1 sur $\mathcal{O}_K/\mathfrak{m}$ et $N(\mathfrak{am}) = \mathrm{Card}(\mathcal{O}_K/\mathfrak{am}) = \mathrm{Card}(\mathcal{O}_K/\mathfrak{a})\mathrm{Card}(\mathfrak{a}/\mathfrak{am}) = \mathrm{Card}(\mathcal{O}_K/\mathfrak{a})\mathrm{Card}(\mathcal{O}_K/\mathfrak{m}) = N(\mathfrak{a})N(\mathfrak{m})$.

- Deuxième cas : $\mathfrak{b}$ quelconque. On décompose $\mathfrak{b}$ en produit d'idéaux maximaux $\mathfrak{m}_1 \dots \mathfrak{m}_n$ et on a

$$N(\mathfrak{a}m_1 \dots \mathfrak{m}_n) = N(\mathfrak{am}_1 \dots \mathfrak{m}_{n-1})N(\mathfrak{m}_n) = \dots = N(\mathfrak{a})N(\mathfrak{m}_1)\dots N(\mathfrak{m}_n) = N(\mathfrak{a})N(\mathfrak{b})$$

□

Remarque. On peut montrer que si $n \in \mathbb{N}^*$, il y a un nombre fini d'idéaux premiers $\mathfrak{p}$ du corps de nombres K tel que $N(\mathfrak{p}) \leqslant n$. (voir [4], chapitre IV, pour la démonstration).

Ce fait sera très utile par la suite, notamment dans le chapitre 6.

Chapitre 4

Théorie de Galois

4.1 Extensions galoisiennes

On a vu précédemment (cf théorème 1.3.8) que si K est un corps parfait, et L une extension de degré n de K, alors il y a exactement n K-isomorphismes de L dans un corps algébriquement clos C contenant L. Comme, selon le théorème de l'élément primitif, on a $L = K[x]$ où $x \in L$ est dit primitif, ces K-isomorphismes sont entièrement déterminés par x et envoient x sur les n racines de son polynôme minimal dans C. Ils forment de plus un groupe.

Le principe de la théorie de Galois est de regarder dans quel cas tous les K-isomorphismes de L dans C sont des K-automorphismes de L, ce qui signifie que le polynôme minimal de x a toutes ses racines dans L.

Définition 4.1.1

Si L est un corps et G un ensemble d'automorphismes de L, $I = \{x \in L : \forall \sigma \in G, \sigma(x) = x\}$ est un sous-corps de L appelé corps des invariants de L.

Théorème 4.1.2

Soit K un corps parfait et L une extension finie de K. Il y a équivalence entre

1. *K est le corps des invariants du groupe G des K-automorphismes de L.*
2. *$\forall x \in L$, le polynôme minimal Π_x de x sur K a toutes ses racines dans L.*
3. *L est engendré par les racines d'un polynôme sur K.*

Dans ces conditions, G a n éléments. On dit alors que L est une extension galoisienne de K, et G est appelé groupe de Galois de L sur K et est noté $\mathrm{Gal}(L/K)$*. Si de plus, G est abélien (resp. cyclique), on dit que L est extension abélienne (resp. cyclique) de K.*

Démonstration. $1 \Rightarrow 2$: si $x \in L$, $P_x := \prod_{g \in G}(X - \sigma(x))$ est un polynôme invariant par G dans le sens où chacun de ses coefficients est fixé par tout élément de G.

En effet, si $\tau \in G$, $\tau(P_x) := \prod_{g \in G}(X - \tau(\sigma(x))) = \prod_{g \in G}(X - (\tau \circ \sigma)(x)) = \prod_{g \in G}(X - \sigma(x))) = P_x$ puisque $\sigma \longmapsto \tau \circ \sigma$ est une permutation du groupe fini G. Cela donne ce que l'on veut, étant donné que chaque coefficient de P_x s'exprime en fonction de produits et de sommes des $\sigma(x)$. Donc, comme K est le corps des invariants de G, $P_x \in K[X]$.

Qui plus est, P_x admet x pour racine car $\mathrm{id} \in G$ donc $\Pi_x | P_x$ et toutes les racines de Π_x sont des racines de P_x donc des $\sigma(x)$ quand $\sigma \in G$. Par conséquent, Π_x a toutes ses racines dans L.

$2 \Rightarrow 3$: Si x est un élément primitif de L sur K, Π_x a toutes ses racines dans L, en particulier x et $L = K[x]$ est engendré par les racines de Π_x sur K.

$3 \Rightarrow 1$: Notons $\sigma_1, \ldots, \sigma_n$ les K-isomorphismes de L dans C algébriquement clos contenant L. Si L est engendré sur K par les racines d'un polynôme P, étant donné que si x de L est racine de P, tous ses conjugués $\sigma_j(x)$, $j = 1, \ldots, n$ sont également racines de P, L est engendré par $(x^{(1)}, \ldots, x^{(l)})$ et leurs conjugués $(x_j^{(i)}) = (\sigma_j(x^{(i)}))$ qui sont dans L par hypothèse.

Soit $\sigma \in \{\sigma_1, \ldots, \sigma_n\}$. Alors $\sigma(L) \subset L$ puisque σ permute les $(x_j^{(i)})$ et $\sigma(L)$ est engendré par les $\sigma(x_j^{(i)})$. Donc comme σ est K-linéaire injective, on a $\sigma(L) = L$.

Donc on a $G = \{\sigma_1, \ldots, \sigma_n\}$ et G a n éléments.

Soit $x \in L$ invariant par G. Alors $K[x]$ est invariant par G donc G est un groupe de $K[x]$-automorphismes de L, dont G a au plus $[L : K[x]]$ éléments, d'où $n \leqslant [L : K[x]] \leqslant n$, ce qui assure que $K[x] = K$ et $x \in K$. □

Corollaire 4.1.3

Soit K un corps parfait. Si L est une extension de degré n de K, H un groupe d'automorphismes de L admettant K pour corps d'invariants, alors L est extension galoisienne de K et H est son groupe de Galois.

Démonstration. $\forall x \in L$, $P_x = \prod_{\sigma \in H} (X - \sigma(x))$ est invariant par H (de même que dans la démonstration précédente) donc a tous ses coefficients dans K, d'où, comme de plus x est racine de P_x, Π_x divise P_x. Par conséquent, comme $\forall \sigma \in H, \sigma(x) \in L$, Π_x a toutes ses racines dans L également et la condition 2 du théorème précédent est vérifiée. Donc L est extension galoisienne de K.

Qui plus est, $H \subset G$, groupe de Galois de L/K puisque H est un groupe de K-automorphismes. D'autre part, soit $x \in L$ élément primitif de L sur K, soit $P(X) = \prod_{\sigma \in H} (X - \sigma(x))$. Selon ce qui précède, P est à coefficients dans K et $\Pi_x | P$ donc comme Π_x est de degré n (x primitif), on a $|G| = n \leqslant \deg P = |H|$ donc $|G| = |H|$ et $G = H$. □

4.2 Correspondance de Galois

Le théorème suivant est la pierre d'angle de la théorie de Galois. Notamment il résume les résultats de la section précédente.

Théorème 4.2.1 (*correpondance de Galois*)

Soient K un corps parfait et L une extension galoisienne de K. On note G le groupe de Galois de L/K.

Pour tout sous-groupe G' de G, on note $k(G') = \{x \in L : \forall \sigma \in G', \sigma(x) = x\}$ le corps des invariants de G'.

Pour tout sous-corps K' de L, L est une extension galoisienne de K' et on note $g(K') = \mathrm{Gal}(L/K')$. Alors :

1. *g et k sont des applications réciproques l'une de l'autre.*
2. *Si $K \subset K' \subset L$, K' est extension galoisienne de K si et seulement si $\mathrm{Gal}(L/K')$ est un sous-groupe normal de G, et dans ces conditions, $\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/K')$.*

Démonstration. Prouvons le premier point. Soit $x \in L$, $\Pi_{K'}$ (resp. Π_K) son polynôme minimal sur K' (resp K). Alors Π_K est un polynôme à coefficients dans K' admettant x pour racine donc $\Pi_{K'} | \Pi_K$. Ainsi, toute racine de $\Pi_{K'}$ est racine de Π_K donc est dans L, ce qui montre que L est extension galoisienne de K'.

$g(K')$ est un sous-groupe de G admettant, par définition, K' pour corps des invariants donc $k(g(K')) = K'$.

De plus, si G' est un sous-groupe de G, selon le corollaire ci-dessus, $G' = \mathrm{Gal}(L/k(G'))$, soit $g(k(G')) = G'$.

Montrons maintenant le second point. Pour $x \in K'$, on note Π_x son polynôme minimal sur K. Pour que K' soit extension galoisienne de K, il faut et suffit, puisque Π_x admet les $\sigma(x), \sigma \in G$ pour racines que $\forall \sigma \in G, \forall x \in K', \sigma(x) \in K'$, soit $\forall \sigma \in G, \sigma(K') \subset K'$.

Si K' est une extension galoisienne de K, $\forall \sigma \in G, \sigma(K') \subset K'$. Soit $\sigma \in G$ et $\tau \in \mathrm{Gal}(L/K')$. $\forall x \in K', (\sigma^{-1}\tau\sigma)(x) = (\sigma^{-1}\sigma)(x) = x$ car τ est un K'-automorphisme.

Donc $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/K')$ qui est par suite un groupe distingué dans G.

Supposons que $\mathrm{Gal}(L/K')$ est distingué dans G.

Soit $\sigma \in G$, et $\tau \in \mathrm{Gal}(L/K')$. On a $\sigma^{-1}\tau\sigma = \nu \in \mathrm{Gal}(L/K')$ donc $\tau\sigma = \sigma\nu$.

D'où $\forall \tau \in \mathrm{Gal}(L/K'), \forall x \in K', \tau(\sigma(x)) = \sigma(x)$ donc $\sigma(x)$ est dans le corps des invariants de $\mathrm{Gal}(L/K')$ qui est K', ce qui donne $\sigma(K') \subset K'$.

Déterminons pour finir $\mathrm{Gal}(K'/K)$ sous l'hypothèse que K'/K est galoisien. Soit

$$\begin{array}{rccc} \varphi : & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(L/K') \\ & \sigma & \longmapsto & \sigma_{|K'} \end{array}$$

Ce "morphisme de restriction" est bien défini puisque $\forall \sigma \in G, \sigma(K') \subset K'$. De plus, son noyau est le groupe de Galois de K'/K de manière évidente donc φ passe au quotient en $\overline{\varphi} : \mathrm{Gal}(L/K)/\mathrm{Gal}(K'/K) \longrightarrow \mathrm{Im}(\varphi)$ morphisme injectif.

Mais $\mathrm{Gal}(L/K)/\mathrm{Gal}(K'/K)$ a pour cardinal $\dfrac{[L:K]}{[K':K]} = [L:K']$ selon la formule des degrés, donc $\overline{\varphi}$ est surjectif et on a l'isomorphisme voulu. □

4.3 Ramification dans les extensions galoisiennes de corps de nombres

4.3.1 Décomposition d'un idéal premier dans une extension galoisienne

Soit K un corps de nombres et L une extension galoisienne de K de degré n. Dans ce cadre, on va pouvoir obtenir des résultats plus forts que ceux du chapitre 2 concernant la décomposition d'un idéal dans une extension. On montrera que dans la décomposition d'un idéal premier de K dans L, tous les idéaux au-dessus de $\mathfrak{p}$ ont le même indice de ramification et le même degré résiduel.

Notons $G = \mathrm{Gal}(L/K)$. Si $\sigma \in G$ et $x \in \mathcal{O}_L$, en appliquant σ à une équation de dépendance intégrale de x, on obtient $\sigma(x) \in \mathcal{O}_L$ donc $\sigma(\mathcal{O}_L) \subset \mathcal{O}_L$. En utilisant ce résultat pour σ^{-1}, on a donc $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.

De plus, si $\mathfrak{p}$ est un idéal premier de K et $\mathfrak{P}$ un idéal premier de L au-dessus de $\mathfrak{p}$, on a $\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \mathfrak{p}$. En effet, comme σ est bijectif, $\sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{P}) \cap \sigma(\mathcal{O}_K) = \sigma(\mathfrak{P}) \cap \mathcal{O}_K = \sigma(\mathfrak{p}) = \mathfrak{p}$ car σ est un K-automorphisme.

Par conséquent, comme $\sigma(\mathfrak{P})$ est un idéal premier de L, $\sigma(\mathfrak{P})$ est au-dessus de $\mathfrak{p}$.

Par ailleurs, si I, J sont des idéaux de $\mathcal{O}_L$, $\sigma(IJ) = \sigma(I)\sigma(J)$ ce qu'on généralise sans peine à un produit fini d'idéaux. Donc, en écrivant $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, on a $\sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{g} \sigma(\mathfrak{P}_i)^{e_i}$ donc $\sigma(\mathfrak{P}_i)$ apparaît dans la décomposition en idéaux premiers de $\mathfrak{p}\mathcal{O}_L$ avec le même indice de ramification que $\mathfrak{P}$.

Définition 4.3.1

Si $\sigma \in \mathrm{Gal}(L/K)$ et $\mathfrak{P}$ est un idéal premier de L, $\mathfrak{P}$ et $\sigma(\mathfrak{P})$ sont dits idéaux premiers conjugués dans $\mathcal{O}_L$.

Proposition 4.3.2

Soit $\mathfrak{p}$ idéal premier de $\mathcal{O}_K$. Alors les idéaux premiers $\mathfrak{P}_i$ au-dessus de $\mathfrak{p}$ sont deux à deux conjugués, ont même degré résiduel f et même indice de ramification e. Ainsi :

$$\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$$

Et $n = efg$.

Pour cette démonstration, on aura besoin du lemme technique suivant :

Lemme 4.3.3

Soit A un anneau de Dedekind et $\mathfrak{p}_1, \ldots, \mathfrak{p}_q$ des idéaux premiers de A. Soit $\mathfrak{b}$ un idéal de A tel que $\forall i, \mathfrak{b} \not\subset \mathfrak{p}_i$. Alors $\exists b \in \mathfrak{b} : \forall i, b \notin \mathfrak{p}_i$.

Démonstration. Tous les $\mathfrak{p}_i$ étant maximaux distincts, on a $\forall i \neq j, \mathfrak{p}_i \not\subset \mathfrak{p}_j$. On fixe donc $u_{ij} \in \mathfrak{p}_j \setminus \mathfrak{p}_i$.

Mais $\forall i, \mathfrak{b} \not\subset \mathfrak{p}_i$ donc il existe $a_i \in b$ tel que $a_i \notin \mathfrak{p}_i$. On pose $b_i = a_i \prod_{j \neq i} u_{ij}$. Comme b et $\mathfrak{p}_j$ sont des idéaux, $b_i \in \mathfrak{b}$ et $\forall j \neq i, b_i \in \mathfrak{p}_j$. Mais $b_i \notin \mathfrak{p}_i$ puisque $\mathfrak{p}_i$ est un idéal premier.

Finalement, en posant $b = \sum_{i=1}^{q} b_i$, on a $b \in \mathfrak{b}$, et $\forall i, \sum_{j \neq i} b_j \in \mathfrak{p}_i, b_i \notin \mathfrak{p}_i$, ce qui donne $b \notin \mathfrak{p}_i$. □

Démonstration (de la proposition)**.** Soit $\mathfrak{P}$ l'un des $\mathfrak{P}_i$, supposons qu'il existe $\mathfrak{P}_j = \mathfrak{Q}$ non conjugué de $\mathfrak{P}$. Alors $\forall \sigma \in G$, $\mathfrak{Q}$ et $\sigma(\mathfrak{P})$ sont maximaux et distincts donc $\sigma(\mathfrak{P}) \not\subset \mathfrak{Q}$ et $Q \not\subset \sigma(\mathfrak{P})$. Donc selon le lemme, il existe $x \in \mathfrak{Q} : \forall \sigma, x \notin \sigma(\mathfrak{P})$.

Mais la norme de x est $N(x) = \prod_{\tau \in G} \tau(x)$ (voir la remarque suivant le théorème 1.4.2) et on sait que $N(x) \in \mathcal{O}_K$ (cf proposition 1.4.3). De plus, comme $\forall \tau \in G, \tau(x) \in \mathcal{O}_L$ et $\mathrm{id} \in G$, $N(x) \in \mathfrak{Q}$, donc $N(x) \in \mathfrak{Q} \cap \mathcal{O}_K = \mathfrak{p}$.

D'autre part, $\forall \tau \in G, x \notin \tau^{-1}(\mathfrak{P})$ donc $\tau(x) \notin \mathfrak{P}$ donc, comme $\mathfrak{P}$ est premier, $N(x) \notin \mathfrak{P}$ ce qui est absurde étant donné que $N(x) \in \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

A partir de là, les autres affirmations sont simples : selon la remarque préliminaires, deux idéaux conjugués ont même indice de ramification ; ils ont également même degré résiduel. En effet, soit $\sigma \in G$, $\mathfrak{P}$ idéal premier de L et $\mathfrak{Q} = \sigma(\mathfrak{P})$. On a $\mathcal{O}_L/\mathfrak{P} \simeq \mathcal{O}_L/\mathfrak{Q}$ en tant que $(\mathcal{O}_K/p)$-espaces vectoriels via $\phi : \begin{array}{ccc} \mathcal{O}_L & \longrightarrow & \mathcal{O}_L/\mathfrak{P} \\ x & \longmapsto & \sigma^{-1}(x) \mod \mathfrak{P} \end{array}$ de noyau $\sigma(\mathfrak{P}) = \mathfrak{Q}$

qui passe au quotient en $\overline{\phi} : \begin{array}{ccc} \mathcal{O}_L & \longrightarrow & \mathcal{O}_L/\mathfrak{P} \\ x \mod \sigma(\mathfrak{P}) & \longmapsto & \sigma^{-1}(x) \mod \mathfrak{P} \end{array}$.

Cette application est bien $\mathcal{O}_K/\mathfrak{p}$ linéaire car si $a \in \mathcal{O}_K$, $\overline{\phi}((a \mod \sigma(\mathfrak{P}))(x \mod \sigma(\mathfrak{P})) = (\sigma^{-1}(a)\sigma^{-1}(x)) \mod \mathfrak{P})(a \mod \mathfrak{P})(\sigma^{-1}(x) \mod \mathfrak{P})$. □

4.3.2 Le relèvement de Frobenius

On se donne L/K une extension galoisienne de corps de nombres.

Définition 4.3.4

Soit $\mathfrak{p}$ idéal premier de K, soit $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. On appelle groupe de décomposition de $\mathfrak{P}$ le groupe

$$D(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

Soit $\sigma \in D(\mathfrak{P})$. On a $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ et $\sigma(\mathfrak{P}) = \mathfrak{P}$ donc on peut définir

$$\begin{array}{rccc} \overline{\sigma} : & \mathcal{O}_L/\mathfrak{P} & \longrightarrow & \mathcal{O}_L/\mathfrak{P} \\ & x \mod \mathfrak{P} & \longmapsto & \sigma(x) \mod \mathfrak{P} \end{array}$$

automorphisme de $l_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ dont on montrera que c'est une extension galoisienne de $k_p = \mathcal{O}_K/p$.

On note $\begin{array}{rccc} \varphi_{\mathfrak{P}} : & D(\mathfrak{P}) & \longrightarrow & \mathrm{Gal}(l_{\mathfrak{P}}/k_p) \\ & \sigma & \longmapsto & \overline{\sigma} \end{array}$.

$\varphi_{\mathfrak{P}}$ est un morphisme de groupes de noyau $I = \{\sigma \in D(\mathfrak{P}) : \forall x \in \mathcal{O}_L, \sigma(x) - x \in \mathfrak{P}\}$, sous-groupe normal de $D(\mathfrak{P})$ appelé *groupe d'inertie* de $\mathfrak{P}$.

Remarque. Soit E l'ensemble des conjugués de $\mathfrak{P}$. On note $\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$ où les $\mathfrak{P}_i$ ont pour degré résiduel f.

En posant $\forall \sigma \in G, \forall \mathfrak{Q} \in E, \sigma \cdot \mathfrak{Q} = \sigma(\mathfrak{Q})$, on a évidemment une action de groupe, qui est de plus transitive.

Donc selon la formule des classes, $|D(\mathfrak{P})| = \dfrac{|G|}{|E|} = \dfrac{n}{g} = ef$.

Cette incursion du vocabulaire des actions de groupe dans l'étude de la théorie de Galois est révélatrice d'un point de vue général sur cette théorie que l'on retrouvera dans les généralisations du chapitre 7.

Proposition 4.3.5

On garde les notations de la remarque Si $\mathcal{O}_K/\mathfrak{p}$ est un corps parfait, $\mathcal{O}_L/\mathfrak{P}$ est une extension galoisienne de degré f de $\mathcal{O}_K/\mathfrak{p}$ et $\varphi_{\mathfrak{P}}$ est un morphisme surjectif de $D(\mathfrak{P})$ sur $\mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$.

On a de plus $|I(\mathfrak{P})| = e$.

Démonstration. Notons K_D le corps des invariants de $D(\mathfrak{P})$. La fermeture intégrale de $\mathcal{O}_K$ dans K_D est trivialement $\mathcal{O}_D = \mathcal{O}_L \cap K_D$, et $\mathfrak{p}_D = \mathfrak{P} \cap \mathcal{O}_D$ est un idéal premier de $\mathcal{O}_D$.

Selon la proposition 4.3.2, et par définition de $D(\mathfrak{P})$, $\mathfrak{P}$ est le seul facteur premier apparaissant dans la décomposition de $\mathfrak{p}_D\mathcal{O}_L$. En effet, $\forall \sigma \in \mathrm{Gal}(L/K_D) = D(\mathfrak{P}), \sigma(\mathfrak{P}) = \mathfrak{P}$

On peut donc noter $\mathfrak{p}_D\mathcal{O}_L = \mathfrak{P}^{e'}$. On note $f' = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_D/\mathfrak{p}_D]$. Alors selon la remarque précédente, $e'f'$ est le cardinal du groupe de décomposition de $\mathfrak{P}$ relativement à l'extension L/K_D, qui n'est autre que $D(\mathfrak{P})$. Mais par ailleurs, $e'f' = [L : K_D]$, d'où $[L : K_D] = |D(\mathfrak{P})|$, et $e'f' = ef$.

Or, on a une suite d'extensions résiduelles $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_D/\mathfrak{p}_D \subset \mathcal{O}_L/\mathfrak{P}$ donc $f \geqslant f'$. De plus, $\mathfrak{p}\mathcal{O}_D \subset \mathfrak{p}_D$ puisque $\mathfrak{p} \subset \mathfrak{p}_D$, donc $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{p}_D\mathcal{O}_L$ et $e' \leqslant e$.

Tout cela nous donne donc $e = e'$ et $f = f'$, d'où $\mathcal{O}_D/\mathfrak{p}_D \simeq \mathcal{O}_K/\mathfrak{p}$.

Par ailleurs, soit $\overline{x}$ un élément primitif de $\mathcal{O}_L/\mathfrak{P}$ sur $\mathcal{O}_K/\mathfrak{p}$ représenté par $x \in \mathcal{O}_L$, et $\Pi_x = X^r + a_{r-1}X^{r-1} + \cdots + a_0$ le polynôme minimal de x sur K_D. Comme L/K_D est une extension galoisienne de groupe de Galois $|D(\mathfrak{P})|$ de K_D, ses racines dans L sont les $\sigma(x), \sigma \in D(\mathfrak{P})$.

De plus, comme x est entier sur $\mathcal{O}_D$, les coefficients de Π_x sont dans $\mathcal{O}_D$ (cf proposition 1.4.3).

Soit le polynôme réduit modulo $\mathfrak{P}$: $\overline{\Pi_x} = X^r + \overline{a_{r-1}}X^{r-1} + \cdots + \overline{a_0}$.

Puisque $\Pi_x = \prod_{u\in\{\sigma(x),\sigma\in D\}} (X-u)$ et que la projection modulo $\mathfrak{P}$ est un morphisme d'anneaux, on a $\overline{\Pi_x} = \prod_{u\in\{\sigma(x),\sigma\in D\}} (X-\overline{u})$.

Ses racines sont donc les $\overline{\sigma(x)} = \overline{\sigma}(\overline{x}), \sigma \in D$, cette dernière égalité provenant directement de la définition de $\overline{\sigma}$.

Or, L/K_D étant galoisien, et $\mathcal{O}_L$ étant stable par K_D-automorphisme, les $\sigma(x)$ appartiennent à $\mathcal{O}_L$. Par suite, les $\overline{\sigma}(\overline{x})$ sont dans $\mathcal{O}_L/\mathfrak{P}$. (a)

Par ailleurs, $\overline{a_i} := a_i \mod \mathfrak{P} = a_i \mod \mathfrak{p}_D$ à isomorphisme près, d'où comme $\mathcal{O}_D/\mathfrak{p}_D \simeq \mathcal{O}_K/\mathfrak{p}$, $\overline{a_i} = a_i \mod \mathfrak{p}$ à isomorphisme près. Ainsi, $\overline{\Pi_x}$ est à coefficients dans $\mathcal{O}_K/\mathfrak{p}$. (b)

Comme l'élément primitif, $\overline{x}$ vaut $\overline{\mathrm{id}}(\overline{x})$, la conjonction des résultats (a) et (b) permet d'affirmer que $\mathcal{O}_L/\mathfrak{P}$ est engendré par les racines d'un polynôme à coefficients dans $\mathcal{O}_K/\mathfrak{p}$ et donc, selon le théorème 4.1.2, que $\mathcal{O}_L/\mathfrak{P}$ est une extension galoisienne de $\mathcal{O}_K/\mathfrak{p}$.

Qui plus est, si Q est le polynôme minimal de $\overline{x}$ sur $\mathcal{O}_K/\mathfrak{p}$, on a $Q \mid \overline{\Pi_x}$ donc les racines de Q sont de la forme $\overline{\sigma}(\overline{x})$, donc, comme $\overline{x}$ est primitif, les $\mathcal{O}_K/\mathfrak{p}$-automorphismes de $\mathcal{O}_L/\mathfrak{P}$ sont des $\overline{\sigma}$, ce qui démontre la surjectivité de $\varphi_{\mathfrak{P}}$.

Par suite, $\varphi_{\mathfrak{P}}$ est un isomorphisme de $D(\mathfrak{P})/I(\mathfrak{P})$ sur $\mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$.

Enfin, on sait que $\mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$ a pour ordre $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = f$ donc $\dfrac{|D(\mathfrak{P})|}{|I(\mathfrak{P})|} = f$ donc comme D a pour ordre ef, $|I(\mathfrak{P})| = e$.

□

On obtient le corollaire fondamental suivant, qui est immédiat :

Corollaire 4.3.6

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. $\mathfrak{p}$ est non ramifié dans $\mathcal{O}_L$ si et seulement si il existe un idéal premier $\mathfrak{P}$ de L au-dessus de $\mathfrak{p}$ tel que le groupe d'inertie $I(\mathfrak{P})$ soit $\{\mathrm{id}\}$.

Et de manière générale, si $\mathfrak{p}$ est non ramifié, le morphisme $\varphi_{\mathfrak{P}}$ est un isomorphisme de $D(\mathfrak{P})$ dans $\mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$.

Plaçons-nous maintenant dans le cas où K est un corps de nombres, L est une extension galoisienne de K. Pour comprendre l'intérêt de l'isomorphisme $\varphi_{\mathfrak{P}}$ dans cas, il faut voir que, pour $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, $l_{\mathfrak{P}}/k_{\mathfrak{p}}$ est une extension de corps finis.

En effet, $\mathfrak{p}$ est au-dessus d'un premier $p \in \mathbb{Z}$ car K est un corps de nombres, et de plus, comme K est une extension finie de $\mathbb{Q}$, on a vu que le degré résiduel $s = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ est fini, donc en notant $q = p^s$, $k_{\mathfrak{p}}$ est le corps $\mathbb{F}_q$.

Donc en notant $f = [l_{\mathfrak{P}} : k_{\mathfrak{p}}]$ le degré résiduel de $l_{\mathfrak{P}}$ sur $k_{\mathfrak{p}}$, on a $l_p/k_{\mathfrak{p}} = \mathbb{F}_{q^f}/\mathbb{F}_q$

Or, le groupe de Galois d'une extension de corps finis est cyclique comme le montre la proposition suivante :

Proposition 4.3.7

Soient $K = \mathbb{F}_q$ un corps fini, où $q = p^s$, p premier, et $L = \mathbb{F}_{q^n}$ une extension finie de degré n de K.

L/K est alors une extension galoisienne et son groupe de Galois $\mathrm{Gal}(L/K)$ *est cyclique engendré par le morphisme de Frobenius* $\mathrm{Frob}_q : x \longmapsto x^q$.

Démonstration. On sait, selon la proposition 1.3.5 que $\sigma = \text{Frob}_q : x \longmapsto x^q$ est un automorphisme de L de corps des invariants $\mathbb{F}_q = K$. En effet, les q éléments de $\mathbb{F}_q$ sont évidemment fixés par ce morphisme, et ses invariants sont les racines du polynôme $X^q - X$ qui en a au plus q.

De plus, $\forall x \in L, \forall j \in [\![1; n]\!], \sigma^j(x) = x^{q^j}$, donc en particulier, $\sigma^n = \text{id}$.

Or, soit y un générateur de $(\mathbb{F}_{q^n})^\times$. On a $\forall 1 \leqslant j \leqslant n-1, \sigma^j(y) = y^{q^j} \neq 1$ car y est d'ordre $q^n - 1$. Donc σ est d'ordre n et son groupe engendré est donc le groupe des K-automorphismes de L qui est à n éléments, donc l'extension est bien galoisienne.

□

Voyons comment utiliser ce résultat. Si $\mathfrak{p} \in \text{Spec}(\mathcal{O}_K)$ est non ramifié et $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$, alors $\varphi_{\mathfrak{P}}$ est un isomorphisme de $D(\mathfrak{P})$ dans $\text{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$ qui est engendré par

$$\begin{array}{rccc} \text{Frob}_q : & l_{\mathfrak{P}} & \longrightarrow & l_{\mathfrak{P}} \\ & \overline{x} & \longmapsto & \overline{x}^q \end{array}$$

Donc $D(\mathfrak{P})$ est également cyclique de générateur privilégié $\sigma = \varphi_{\mathfrak{P}}^{-1}(\text{Frob}_q)$. σ est l'unique élément de $\text{Gal}(L/K)$ vérifiant :

- $\sigma(\mathfrak{P}) = \mathfrak{P}$.
- $\forall x \in \mathcal{O}_L, \sigma(x) \equiv x^q \mod \mathfrak{P}$.

On appelle σ *relèvement de Frobenius* ou *substitution de Frobenius* et on le note $(\mathfrak{P}, L/K)$.

Remarque. Soit un autre idéal $\sigma(\mathfrak{P}), \sigma \in G = \text{Gal}(L/K)$ au-dessus de p (les idéaux au-dessus de p sont deux à deux conjugués).

Alors

$$\begin{aligned} D(\sigma(\mathfrak{P})) &= \{\tau \in G : \tau(\sigma(\mathfrak{P})) = \sigma(\mathfrak{P})\} = \left\{\tau \in G : (\sigma^{-1}\tau\sigma)(\mathfrak{P}) = \mathfrak{P}\right\} \\ &= \left\{\tau \in G : \sigma^{-1}\tau\sigma \in D(\mathfrak{P})\right\} = \sigma D(\mathfrak{P})\sigma^{-1} \end{aligned}$$

De plus, $(\sigma(\mathfrak{P}), L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}$.

En effet, si $\tau = (\mathfrak{P}, L/K)$, on a $\sigma\tau\sigma^{-1} \in (\sigma(\mathfrak{P}), L/K)$ et $\forall x \in \mathcal{O}_L, (\sigma\tau\sigma^{-1})(x) - x^q = \sigma((\tau\sigma^{-1})(x) - (\sigma^{-1}(x))^q) \in \sigma(\mathfrak{P})$ puisque $(\tau\sigma^{-1})(x) - (\sigma^{-1}(x))^q \in \mathfrak{P}$ par définition de τ.

On peut donc définir la *classe de conjugaison* $(\mathfrak{p}, L/K) = \{(\mathfrak{P}, L/K), \mathfrak{P} \cap \mathcal{O}_K = p\}$.

Dans le cas où L est une extension abélienne de K, $(\mathfrak{p}, L/K)$ est donc un élément du groupe de Galois, qu'on appelle encore *relèvement de Frobenius* de $\mathfrak{p}$.

Terminons par quelques propriétés du relèvement de Frobenius

Proposition 4.3.8

Soit K un corps de nombres, L une extension galoisienne de K et F un corps tel que $K \subset F \subset L$.

Soit p idéal premier non ramifié de K, $\mathfrak{P}$ idéal de L au-dessus de $\mathfrak{p}$ et f le degré résiduel de $\mathfrak{P} \cap \mathcal{O}_F$ sur K.

- $(\mathfrak{P}, L/F) = (\mathfrak{P}, L/K)^f$.
- *Si F est une extension galoisienne de K, alors* $(\mathfrak{P}, L/K)_{|\mathcal{O}_F} = (\mathfrak{P} \cap \mathcal{O}_F, F/K)$.

Démonstration.

- Notons $\sigma = (\mathfrak{P}, L/F) \in D(\mathfrak{P})$. Par définition, $\sigma(\mathfrak{P}) = \mathfrak{P}$ et $\forall x \in \mathscr{O}_L, \sigma(x) \equiv x^q \mod \mathfrak{P}$, où $q = \mathrm{Card}(\mathscr{O}_K/\mathfrak{p})$.

  Donc immédiatement, $\forall x \in \mathscr{O}_L, \sigma^f(x) \equiv x^{q^f}$ et $\sigma^f(\mathfrak{P}) = \mathfrak{P}$.

  Or, $q^f = \mathrm{Card}((\mathscr{O}_L \cap F)/(\mathfrak{P} \cap F))$ corps résiduel sur $\mathscr{O}_K/\mathfrak{p}$.

  Par ailleurs, le groupe de décomposition $D_F(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(L/F) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$ est un sous-groupe de $D_K(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$, et son ordre est $[\mathscr{O}_L/\mathfrak{P} : (\mathscr{O}_L \cap F)/(\mathfrak{P} \cap F)] = \dfrac{|D_K(\mathfrak{P})|}{f}$ (formule des degrés) car $\mathfrak{P} \cap F$ est non ramifié dans $\mathscr{O}_L$.

  En effet, $\mathfrak{p}\mathscr{O}_L \subset (\mathfrak{P} \cap \mathscr{O}_K)\mathscr{O}_L \subset (\mathfrak{P} \cap F)\mathscr{O}_L$ et $\mathfrak{p}$ est non ramifié dans L.

  Or, $D_K(\mathfrak{P})$ est cyclique engendré par σ, son seul sous-groupe d'ordre $\dfrac{|D_K(\mathfrak{P})|}{f}$ est le sous-groupe engendré par σ^f, ce qui montre le premier point.

- Si F est galoisien sur K, en gardant les mêmes notations, soit $\sigma' = \sigma_{|F}$.

  Si $x \in F$ de polynôme minimal Π_x, on a par le raisonnement habituel $\Pi_x \mid \prod_{\alpha \in \mathrm{Gal}(L/K}} (X - \alpha(x))$ donc les $\alpha(x)$ sont racines de Π_x donc comme F/K est galoisienne, appartiennent à F. En particulier, $\sigma(F) = F$.

  Par suite, comme de plus $\sigma(\mathfrak{P}) = \mathfrak{P}$, on a $\sigma'(\mathfrak{P} \cap F) = \mathfrak{P} \cap F$, d'où $\sigma' \in D_K(\mathfrak{P} \cap F)$. Évidemment, $\forall x \in \mathscr{O}_L \cap F, \sigma'(x) \equiv x^q \mod \mathfrak{P}$ où $q = \mathrm{Card}(\mathscr{O}_K/\mathfrak{p})$, ce qui prouve que $\sigma' = (\mathfrak{P} \cap F, F/K)$.

□

4.4 Exemples

4.4.1 Extension quadratique

Soit $K = \mathbb{Q}[\sqrt{d}]$ où d est un entier relatif sans facteurs carrés. Le polynôme minimal de $\sqrt{d}$ est $P = X^2 - d$ de racines $\pm\sqrt{d} \in K$ donc $K/\mathbb{Q}$ est engendré par les racines d'un polynôme sur K donc est une extension galoisienne et les $\mathbb{Q}$-automorphismes de K sont id et $\sigma : a + b\sqrt{d} \longmapsto a - b\sqrt{d}$. Le groupe de Galois de K sur $\mathbb{Q}$ a donc deux éléments.

4.4.2 Extension cyclotomique

Soit ζ une racine primitive n-ième de l'unité, et $K = \mathbb{Q}[\zeta]$. ζ est racine de $X^n - 1$ donc son polynôme minimal a pour racines des racines n-ièmes de l'unité qui sont des puissances de ζ, puisque ζ est un générateur de $\mathbb{U}_n$. Ainsi, K est engendré par les racines d'un polynôme sur $\mathbb{Q}$ donc $K/\mathbb{Q}$ est galoisienne.

De plus, on a un morphisme injectif $j : \mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$.

En effet, soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. σ est entièrement déterminé par la donnée de $\sigma(\zeta)$. ζ est un générateur de $\mathbb{U}_n$ et σ envoie ζ sur une racine de son polynôme minimal, donc on peut trouver $j(\sigma) \in \mathbb{Z}/n\mathbb{Z}$ tel que $\sigma(\zeta) = \zeta^{j(\sigma)}$, dans le sens où $j(\sigma)$ est déterminé modulo n.

De plus, si $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$, $j(\sigma)j(\tau) = j(\sigma\tau)$, puisque si $l \in j(\sigma), m \in j(\tau)$, $(\sigma\tau)(\zeta) = \sigma(\zeta^m) = (\sigma(\zeta))^m = \zeta^{lm}$ donc $lm \in j(\sigma\tau)$.

Donc, comme j est trivialement injectif, j est un morphisme injectif de $\mathrm{Gal}(K/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$, groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, ce qu'on voulait montrer.

Par conséquent, $\mathrm{Gal}(K/\mathbb{Q})$ est un groupe abélien.

Nous montrerons dans le chapitre suivant que j est en fait un isomorphisme.

Chapitre 5

Théorie du corps de classe pour les corps de nombres

Pour cette section, on a utilisé le cours de James Milne (voir [3]).

Le but de ce chapitre est de décrire les extensions abéliennes d'un corps de nombres K, à travers leur groupe de Galois, qui sont des objets extérieurs à K, en termes de données intrinsèquement liées à K, à savoir des sous-groupes de son groupe des idéaux fractionnaires I_K. La loi d'Artin décrite en 5.2 est ce qui met en relation ces deux objets.

Il est tout à fait remarquable qu'une telle description soit possible, c'est-à-dire, comme l'a dit Chevalley, qu'on puisse montrer « comment un corps possède en soi les éléments de son propre dépassement ».

5.1 Le groupe des classes de rayon modulo m

5.1.1 Premiers d'un corps de nombres

Soit K un corps de nombres. Alors $\mathbb{C}$ est une clôture algébrique de K puisque tout élément de K est racine d'un polynôme à coefficients dans $\mathbb{Q}$.

On peut donc considérer les $n = [K : \mathbb{Q}]$ $\mathbb{Q}$-isomorphismes $\sigma_1, \dots, \sigma_n$ de K dans $\mathbb{C}$. Le morphisme de conjugaison $u : z \longmapsto \overline{z}$ est un $\mathbb{Q}$-isomorphisme de K dans $\mathbb{C}$. Donc $\forall i \in [\![1; n]\!], \exists j \in [\![1; n]\!] : u \circ \sigma_i = \sigma_j$.

Si $i = j$, alors $\sigma_i(K) \subset \mathbb{R}$. On note r_1 le nombre de tels plongements, appelés plongements réels.

Sinon, comme u est involutif, on peut apparier deux par deux les autres plongements, ce qui nous donne $2r_2$ plongements appelés plongements complexes.

On peut donc définir les premiers de K :

Définition 5.1.1

Les premiers de K sont d'une part les idéaux premiers de K, appelés premiers finis et d'autre part les premiers infinis divisés en deux catégories : les premiers infinis réels qui sont les plongements réels de K dans $\mathbb{C}$ et les premiers infinis complexes qui sont les paires de plongements complexes (σ_i, σ_j) tels que $u \circ \sigma_i = \sigma_j$.

Remarque. En réalité, cette définition quelque peu incongrue provient de réflexions sur les valuations d'un corps de nombres, qui sont des applications jouant le rôle de la valeur absolue dans $\mathbb{R}$ pour K. En cherchant à classifier ces valuations, on obtient des classes d'équivalence de valuations, chacune pouvant être associée à un premier comme défini ci-dessus.

5.1.2 Groupe des classes de rayon

Définition 5.1.2

Soit K un corps de nombres. Un module pour K est une fonction $\mathfrak{m}$ de l'ensemble des premiers de K dans $\mathbb{Z}$ telle que :

1. *Si $\mathfrak{p}$ premier fini, $m(\mathfrak{p}) \geqslant 0$ et les $m(\mathfrak{p})$ sont presque tous nuls.*
2. *Si $\mathfrak{p}$ est réel, $m(\mathfrak{p}) \in \{0, 1\}$.*
3. *Si $\mathfrak{p}$ est complexe, $m(\mathfrak{p}) = 0$.*

Si $m(\mathfrak{p}) > 0$, on dit que $\mathfrak{p}$ divise $\mathfrak{m}$ ($\mathfrak{p} \mid \mathfrak{m}$). On note alors $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ où $\mathfrak{m}_0 = \prod_{\mathfrak{p}|\mathfrak{m}} \mathfrak{p}^{m(\mathfrak{p})}$, et $\mathfrak{m}_\infty$ est le produit des premiers réels divisant $\mathfrak{m}$.

En particulier, on peut identifier un premier fini ou réel à un module.

Définition 5.1.3

Soient $\mathfrak{m}, \mathfrak{n}$ deux modules pour K. On dit que $\mathfrak{m}$ divise $\mathfrak{n}$ si $\forall \mathfrak{p}, \mathfrak{m}(\mathfrak{p}) \leqslant \mathfrak{n}(\mathfrak{p})$.

Définition 5.1.4

Soit $\mathfrak{m}$ un module.

- *Son support $S(\mathfrak{m})$ est l'ensemble des premiers divisant $\mathfrak{m}$.*
- *$K_{\mathfrak{m},1}$ est l'ensemble des $a \in K^\times$ tels que $\forall \mathfrak{p}$ premier fini divisant $\mathfrak{m}$, $v_\mathfrak{p}(a-1) \geqslant m(\mathfrak{p})$ où $v_\mathfrak{p}$ est la valuation $\mathfrak{p}$-adique, et $\forall \mathfrak{p}$ premier réel divisant m, $a_\mathfrak{p} > 0$ où $a_\mathfrak{p}$ est l'évaluation en a du plongement $\mathfrak{p}$.*

Proposition 5.1.5

$K_{\mathfrak{m},1}$ est un groupe, et $i(K_{\mathfrak{m},1}) \subset I_K^{S(\mathfrak{m})}$ où $i : \begin{array}{ccc} K^\times & \longrightarrow & I_K \\ a & \longmapsto & (a) = a\mathcal{O}_K \end{array}$

Lemme 5.1.6

Soient $a, b \in K^\times$. Alors pour $\mathfrak{p} \in \mathrm{Spec}(K)$, $v_\mathfrak{p}(a+b) \geqslant \min(v_\mathfrak{p}(a), v_\mathfrak{p}(b))$ avec égalité si $v_\mathfrak{p}(a) \neq v_\mathfrak{p}(b)$.

Démonstration.

- On a $(a+b) \subset (a)+(b)$ donc selon les propriétés suivant le théorème 2.3.6, $v_\mathfrak{p}(a+b) \geqslant \min(v_\mathfrak{p}(a), v_\mathfrak{p}(b))$, valuation en $\mathfrak{p}$ de l'idéal $(a)+(b)$.
- Supposons que $v_\mathfrak{p}(a) \neq v_\mathfrak{p}(b)$, par exemple $v_\mathfrak{p}(a) > v_\mathfrak{p}(b)$. On a $b = a+b-a$ donc $(b) \subset (a+b)+(a)$ donc $v_\mathfrak{p}(b) \geqslant \min(v_\mathfrak{p}(a+b), v_\mathfrak{p}(a))$. Or, $v_\mathfrak{p}(a) > v_\mathfrak{p}(b)$, donc $\min(v_\mathfrak{p}(a+b), v_\mathfrak{p}(a)) = v_\mathfrak{p}(a+b)$.

  Ainsi, en utilisant le premier point, $v_\mathfrak{p}(b) \geqslant v_\mathfrak{p}(a+b) \geqslant v_\mathfrak{p}(b)$ ce qui donne le résultat.

□

Démonstration (de la proposition). Soient $a \in K_{\mathfrak{m},1}$ et $\mathfrak{p} \in S(\mathfrak{m})$. On a $v_\mathfrak{p}(1) = 0$ et $v_\mathfrak{p}(a-1) > 0$.

Donc selon le lemme, $v_\mathfrak{p}(a) = v_\mathfrak{p}(a-1+1) = 0$ et $(a) \in I_K^{S(\mathfrak{m})}$, ce qui justifie que $i(K_{\mathfrak{m},1}) \subset I_K^{S(\mathfrak{m})}$.

$K_{\mathfrak{m},1}$ est un groupe car si $v_\mathfrak{p}(a-1) \geqslant m(\mathfrak{p}), v_\mathfrak{p}(b-1) \geqslant m(\mathfrak{p})$, $v_\mathfrak{p}(ab^{-1}-1) = v_\mathfrak{p}(b^{-1}(a-b)) = v_\mathfrak{p}(b^{-1}) + v_\mathfrak{p}(a-b)$.

Or, $v_\mathfrak{p}(b) = 0$ donc $0 = v_\mathfrak{p}(1) = v_\mathfrak{p}(bb^{-1}) = v_\mathfrak{p}(b) + v_\mathfrak{p}(b^{-1}) = v_\mathfrak{p}(b^{-1})$, d'où $v_\mathfrak{p}(ab^{-1}-1) = v_\mathfrak{p}((a-1)-(b-1)) \geqslant \min(v_\mathfrak{p}(a-1), v_\mathfrak{p}(b-1)) \geqslant \mathfrak{m}(\mathfrak{p})$.

□

Définition 5.1.7

On appelle groupe de classe de rayon modulo $\mathfrak{m}$ le groupe quotient $C_\mathfrak{m} = I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$.

Théorème 5.1.8

$C_\mathfrak{m}$ est un groupe fini.

Démonstration. Admis. Le cas clef est celui où $\mathfrak{m} = \mathfrak{m}_\infty$ (produit des premiers infinis de K), qui correspond au théorème 3.1.7. □

5.2 La loi de réciprocité d'Artin

5.2.1 Énoncé de la loi

Soit K un corps de nombres et L une extension abélienne de K.

Si S un ensemble de premiers de K contenant les premiers qui se ramifient dans L et les premiers infinis, on définit I_K^S comme le sous-groupe du groupe des idéaux fractionnaires de K engendré par les idéaux premiers qui ne sont pas dans S. C'est un groupe libre engendré par $\mathrm{Spec}(K)\backslash S$. On peut donc étendre l'application "relèvement de Frobenius" $\mathfrak{p} \longmapsto (\mathfrak{p}, L/K)$ en un morphisme de groupes

$$\begin{array}{rccc} \psi_{L/K}^S : & I_K^S & \longrightarrow & \mathrm{Gal}(L/K) \\ & \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r} & \longmapsto & (\mathfrak{p}_1, L/K)^{n_1} \dots (\mathfrak{p}_r, L/K)^{n_r} \end{array}$$

Cette application est appelée *fonction de réciprocité d'Artin* [1].

Théorème 5.2.1 (*Artin*)

Soit K un corps de nombres, L une extension abélienne de K. On note S l'ensemble des idéaux premiers de K qui se ramifient dans L et des premiers infinis de K. Alors il existe un module $\mathfrak{m}$ pour K tel que $S \subset S(\mathfrak{m})$ et tel que le diagramme suivant commute :

$$\begin{array}{ccc} \psi_{L/K}^S : I_K^{S(\mathfrak{m})} & \longrightarrow & \mathrm{Gal}(L/K) \\ \Big\downarrow \pi_\mathfrak{m} & \nearrow & \\ C_\mathfrak{m} & & \end{array}$$

On dit que ψ^S admet un module, et on appelle $\mathfrak{m}$ un module adapté.

Remarque. En réalité, ce résultat est la loi d'Artin *faible*. La loi forte affirme qu'il existe un module $\mathfrak{m}$, dont le support est exactement S, faisant commuter le diagramme ci-dessus.

On va pouvoir démontrer deux faits dans ce mémoire :

1. du nom d'Emil Artin (1887-1962), mathématicien autrichien qui a démontré la loi portant son nom entre 1924 et 1930.

- D'une part, que $\psi_{L/K}^{S(\mathfrak{m})}$ est surjective, ce qui sera en fait un cas particulier du théorème de Chebotarev.
- D'autre part, on va déterminer explicitement un *sous-groupe de congruence* H tel que $i(K_{\mathfrak{m},1}) \subset H \subset I_K^{S(\mathfrak{m})}$ tel que $\overline{H} = \pi_{\mathfrak{m}}(H)$ vérifie :

$$\begin{array}{ccc} C_{\mathfrak{m}} & \longrightarrow & \mathrm{Gal}(L/K) \\ \downarrow & \nearrow_{\simeq} & \\ C_{\mathfrak{m}}/\overline{H} & & \end{array}$$

  L'existence d'un tel H est déjà assurée par la loi d'Artin, puisque $i(K_{\mathfrak{m},1}) \subset \ker \psi^S$ pour un module adapté $\mathfrak{m}$.

Prouvons une partie de ce deuxième fait :

Définition 5.2.2

Soit L/K une extension finie de corps de nombres. I_L et I_K étant des groupes libres engendrés par les idéaux premiers, on définit un morphisme de groupes en posant, pour $\mathfrak{P}$ idéal premier de L, $\mathrm{Nm}(\mathfrak{P}) = \mathfrak{p}^f$ où $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ et f est le degré résiduel de $\mathfrak{P}$ sur $\mathfrak{p}$. Cette application est appelée application norme.

Dans le cas d'une extension $K/\mathbb{Q}$, on a, si $p = \mathfrak{p} \cap \mathcal{O}_K$, $N(\mathfrak{p}) = p^f$, où f degré résiduel et $(p) = \mathfrak{p} \cap \mathbb{Z}$. En effet, $\mathcal{O}_K/\mathfrak{p}$ est une extension de degré f de $\mathbb{Z}/p\mathbb{Z}$. Donc $\mathrm{Nm} = \mathrm{Card} \circ N_{K/\mathbb{Q}}$.

On peut donc définir $H = i(K_{\mathfrak{m},1})\mathrm{Nm}(I_L^{S'(\mathfrak{m})})$ pour $\mathfrak{m}$ un module adapté et $S(\mathfrak{m})_L$ l'ensemble des idéaux premiers de L qui sont au-dessus des éléments de $S(\mathfrak{m})$.

Proposition 5.2.3

Soient L/K une extension abélienne, K' un corps tel que $K \subset K' \subset L$, S un ensemble d'idéaux premiers de K contenant ceux qui se ramifient dans L, S' un ensemble d'idéaux premiers de K' contenant ceux qui sont au-dessus des éléments de S. Alors le diagramme suivant commute :

$$\begin{array}{ccc} I_{K'}^{S'} & \xrightarrow{\psi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow \mathrm{Nm} & & \downarrow \text{inclusion} \\ I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

Démonstration. C'est en fait la traduction du premier point de la proposition 4.3.8.

En effet, on veut montrer que $\forall \mathfrak{p}' \in \mathcal{O}_{K'} \backslash S', (p^{f(p'/p)}, L/K) = (p', L/K')$ où $p = p' \cap \mathcal{O}_K \notin S$, ce qui est exactement le résultat déjà prouvé. □

Corollaire 5.2.4

Si L/K est une extension abélienne, $\mathrm{Nm}(I_L^{S_L}) \subset \ker \psi_{L/K}$ où $\psi_{L/K} : I^S \to \mathrm{Gal}(L/K)$, où S_L est un ensemble d'idéaux premiers de L contenant ceux qui sont au-dessus des éléments de S.

Démonstration. En prenant $K' = L$ dans la proposition précédente, on a

$$\begin{array}{ccc} I_L^{S_L} & \longrightarrow & \{\mathrm{id}\} \\ \Big\downarrow \mathrm{Nm} & & \Big\downarrow \text{inclusion} \\ I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

□

Par conséquent, si m est un module adapté pour L/K, comme $i(K_{\mathfrak{m},1}) \subset \ker \psi_{L/K}^{S(\mathfrak{m})}$, on a $H = i(K_{\mathfrak{m},1})\mathrm{Nm}(I_L^{S(\mathfrak{m})_L}) \subset \ker \psi_{L/K}^{S(\mathfrak{m})}$, où $S(\mathfrak{m}_L)$ est l'ensemble des idéaux premiers de L au-dessus des idéaux de $S(\mathfrak{m})$, et des premiers infinis de L.

Ainsi, $\overline{\psi_{L/K}} : I_K^{S(\mathfrak{m})}/H \longrightarrow \mathrm{Gal}(L/K)$ est bien définie.

5.2.2 Démonstration dans le cas cyclotomique

On est en mesure de prouver la loi de réciprocité d'Artin dans le cas d'une extension cyclotomique $K/\mathbb{Q} = \mathbb{Q}[\zeta]/\mathbb{Q}$ où ζ est une racine primitive m-ième de l'unité.

On va d'abord montrer la proposition suivante :

Proposition 5.2.5

Les nombres premiers qui se ramifient dans $\mathbb{Q}[\zeta]$ sont ceux qui divisent m.

Démonstration. Montrons d'abord que si $p \nmid m$, p est non ramifié dans $\mathbb{Q}[\zeta]$.

Pour cela, calculons son polynôme minimal Π. On note $d = [K : \mathbb{Q}]$. On a $\Pi \mid X^m - 1$ donc on peut fixer $F \in \mathbb{Q}[X]$ tel que $X^n - 1 = F(X)\Pi(X)$. Donc $nX^{m-1} = F'(X)\Pi(X) + F(X)\Pi'(X)$, ce qui donne $n\zeta^{m-1} = F(\zeta)\Pi'(\zeta)$.

Or, $(1, \zeta, \ldots, \zeta^{d-1})$ est une base de K sur $\mathbb{Q}$ contenue dans $\mathcal{O}_K$, et le discriminant $D(1, \zeta, \ldots, \zeta^{d-1})$ vaut $N_{K/\mathbb{Q}}(\Pi'(\zeta))$ (voir l'exemple suivant le corollaire 1.4.10).

Et $N(F(\zeta))N(\Pi'(\zeta)) = m^d N(\zeta)^{n-1} = \pm m^d$ car ζ est une unité de $\mathbb{Q}[\zeta]$ puisque $\zeta^m = 1$. D'où $D(1, \zeta, \ldots, \zeta^{d-1}) \mid m^d$.

Mais si p est ramifié dans K, alors selon le théorème 3.2.6, $p \mid D(1, \zeta, \ldots, \zeta^{d-1})$ car $(1, \zeta, \ldots, \zeta^{d-1})$ est une base de K sur $\mathbb{Q}$ contenue dans $\mathcal{O}_K$. Donc $p \mid m^d$ donc selon le lemme de Gauss, $p \mid m$. Par contraposée, on obtient le résultat.

Maintenant, soit p premier tel que $p \mid m$. On peut donc écrire $m = p^r n$ où $p \nmid n$. On pose $\omega = \zeta^n$, ω est une racine primitive p^r-ième de l'unité.

Montrons que $\prod_{p \nmid k} (1 - \omega^k) = p$ $(1 \leqslant k \leqslant m)$. Définissons

$$P(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \sum_{k=0}^{p-1} \left(X^{p^{r-1}}\right)^k$$

$P(1) = p$ et si $k \in [\![1; m]\!]$ et $p \nmid k$, on a $\omega k p^{r-1} \neq 1$, car sinon, comme ω est une racine primitive, on aurait $p^r \mid kp^{r-1}$, soit $p \mid k$ ce qui est faux. Comme de plus, $\omega^{kp^r} = 1$, on a $P(\omega^k) = \dfrac{\omega^{kp^r} - 1}{\omega k p^{r-1} - 1} = 0$.

Donc P admet $\phi(p^r) = p^r - p^{r-1}$ racines distinctes (ϕ indicatrice d'Euler), donc comme P est de degré $p^r - p^{r-1}$, les ω^k sont ses seules racines et elles sont simples.

D'où $P(X) = \prod_{p \nmid k} (X - \omega^k)$ et on obtient ce qu'on voulait en évaluant en 1.

Soit $k \in [\![1;m]\!]$ tel que $p \nmid k$. Alors on peut trouver $(u,v) \in \mathbb{Z}^2 : uk + vp^r = 1$ donc $\dfrac{1-\omega}{1-\omega^k} = \dfrac{1-(\omega^k)^u}{1-\omega^k} = \sum_{j=0}^{u-1} (\omega^k)^j \in \mathcal{O}_K$ comme somme d'entiers.

Comme de plus, $\dfrac{1-\omega^k}{1-\omega} \in \mathcal{O}_K$, cet élément est un inversible de $\mathcal{O}_K$. Ainsi, on peut trouver (u_k) une famille d'unités tels que $p = \prod_{p\nmid k} u_k(1-\omega) = U(1-\omega)^{p^r - p^{r-1}}$ où $U \in (\mathcal{O}_K)^\times$.

Donc $p\mathcal{O}_K = [(1-\omega)\mathcal{O}_K]^{p^r-p^{r-1}}$, ce qui prouve que p est ramifié car $1-\omega$ n'est pas une unité.

□

On a également le fait suivant, en reprenant les notations de l'exemple traité au chapitre 4, section 2.2.

Proposition 5.2.6

j est un isomorphisme de $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ *dans* $(\mathbb{Z}/m\mathbb{Z})^\times$.

Démonstration. On sait déjà que $K = \mathbb{Q}[\zeta]$ est une extension abélienne de $\mathbb{Q}$ et que $j : \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \longmapsto (\mathbb{Z}/m\mathbb{Z})^\times$ est un morphisme injectif.

Soit p premier tel que $p \nmid m$, alors comme p est non ramifié dans $\mathbb{Q}[\zeta]$, $\sigma_p = (p, \mathbb{Q}[\zeta]/\mathbb{Q})$ est bien défini.

Notons $k = j(\sigma_p)$. Soit $\mathfrak{p}$ au-dessus de p. On a $\forall x \in \mathcal{O}_K, \sigma_p(x) \equiv x^p \mod \mathfrak{p}$, donc en particulier $\zeta^k \equiv \zeta^p \mod \mathfrak{p}$.

Or, soit $P(X) = X^n - 1 = \prod_{0\leqslant r\leqslant m-1} (X-\zeta^r)$. On a $P'(X) = \sum_{l=0}^{m-1} \prod_{\substack{0\leqslant r\leqslant m-1 \\ r\neq l}} (X-\zeta^r)$, d'où

$$P'(\zeta^p) = \prod_{\substack{0\leqslant r\leqslant m-1 \\ r\neq p[m]}} (\zeta^p - \zeta^r) = m\zeta^{p(m-1)}$$

Supposons que $\prod_{\substack{0\leqslant r\leqslant m-1 \\ r\neq p[m]}} (\zeta^p - \zeta^r) \in \mathfrak{p}$. Alors, $m\zeta^{p(m-1)} \in \mathfrak{p}$ donc en multipliant par $\zeta^{-p(m-1)} \in \mathcal{O}_K$ (ζ est inversible dans $\mathcal{O}_K$ car $1+\zeta+\cdots+\zeta^{m-1} = 0$), on obtient $m \in \mathfrak{p}$ si bien que $m\mathbb{Z} \subset \mathfrak{p}$. Comme $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, on a donc $m\mathbb{Z} \subset p\mathbb{Z}$ donc $p \mid m$ ce qui contredit l'hypothèse faite sur p.

Donc $\prod_{\substack{0\leqslant r\leqslant m-1 \\ r\neq p[m]}} (\zeta^p - \zeta^r) \notin \mathfrak{p}$.

D'où, par intégrité de $\mathcal{O}_K/\mathfrak{p}$, on a $\forall r \in [\![0;m-1]\!]$ tel que $r \not\equiv p[m]$, $\zeta^p \not\equiv \zeta^r \mod \mathfrak{p}$. Par conséquent, comme $\zeta^k \equiv \zeta^p \mod \mathfrak{p}$, on a $k \equiv p[m]$.

En fin de compte, pour tout premier p tel que $p \nmid m$, $[p]_m \in j(\mathrm{Gal}(\mathbb{Q}(\zeta]/\mathbb{Q}))$ donc, comme $(\mathbb{Z}/m\mathbb{Z})^\times$ est engendré par les $[p]_m$ quand $p \nmid m$, $j(\mathrm{Gal}(\mathbb{Q}(\zeta]/\mathbb{Q}))$ contient $(\mathbb{Z}/m\mathbb{Z})^\times$, d'où l'égalité. □

On va pouvoir traduire tous ces résultats dans le langage de la théorie du corps de classe :

Théorème 5.2.7

On considère S est l'ensemble des premiers divisant m auquel on ajoute $\mathfrak{m}_\infty$, le premier infini d'inclusion de $\mathbb{Q}$ dans $\mathbb{C}$, la fonction d'Artin $\psi^S_{\mathbb{Q}[\zeta]/\mathbb{Q}}$ est bien définie.

Cette fonction admet pour module adapté $\mathfrak{m} = \prod p_i^{n_i}\mathfrak{m}_\infty$ où $m = \prod p_i^{n_i}$, et le support de $\mathfrak{m}$ est de plus exactement S.

Démonstration. $\mathfrak{m}$ a évidemment pour support $S = \{p \in \mathrm{Spec}(\mathbb{Z}) : p \nmid m\}$ qui est exactement l'ensemble des idéaux premiers de $\mathbb{Q}$ non ramifiés dans $\mathbb{Q}[\zeta]$ selon la proposition 5.2.5.

On définit $\mathbb{Q}^S = i^{-1}(I^S) = \left\{x \in \mathbb{Q} : (x) \in I^S\right\} = \left\{\frac{r}{s} \in \mathbb{Q} : r \wedge m = s \wedge m = 1\right\}$ qui est l'ensemble des x premiers avec m (n'ayant aucun facteur premier commun avec m). On peut toujours prendre r premier avec s.

On a alors $\mathbb{Q}^S/\mathbb{Q}_{\mathfrak{m},1} \simeq I^S/i(\mathbb{Q}_{\mathfrak{m},1})$ via i. Soit

$$\begin{array}{rccc} \varphi : & I^{S(\mathfrak{m})} & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times \\ & \left(\frac{r}{s}\right) & \longmapsto & [r]_m[s]_m^{-1} \end{array}$$

où $\frac{r}{s}$, r et s premiers entre eux, est l'unique générateur positif de l'idéal fractionnaire $\left(\frac{r}{s}\right)$. φ est bien définie à valeurs dans $(\mathbb{Z}/m\mathbb{Z})^\times$ puisque tous les $a \in Q^S$ sont premiers avec m.

Le noyau de φ est l'ensemble des $\left(\frac{r}{s}\right)$ tels que $[r]_m[s]_m^{-1} = 1$ soit $r - s \in m\mathbb{Z}$, soit, pour p premier divisant m, $v_p(r-s) \geqslant v_p(m)$.

Mais si $p \mid m$, $v_p\left(\frac{r}{s} - 1\right) = v_p(r-s) + v_p\left(\frac{1}{s}\right) = v_p(r-s) - v_p(s)$.

Or, si $v_p(s) \neq 0$, comme r et s sont premiers entre eux, on a nécessairement $v_p(r) = 0 \neq v_p(s)$ d'où, selon le lemme 5.1.6, $v_p(r-s) = \min(v_p(r), v_p(s)) \geqslant v_p(m) > 0$ soit $0 > 0$ ce qui est absurde. Donc $v_p(s) = 0$.

Ainsi, pour $p \mid m, v_p\left(\frac{r}{s} - 1\right) \geqslant v_p(m)$ donc par définition $\left(\frac{r}{s}\right) \in i(\mathbb{Q}_{\mathfrak{m},1})$.

Réciproquement, si $\forall p \mid m, v_p\left(\frac{r}{s} - 1\right) \geqslant v_p(m)$, on a $v_p(r-s) \geqslant v_p(m) + v_p(s) \geqslant v_p(m)$ et si $p \nmid m, v_p(r-s) \geqslant 0 = v_p(m)$ donc m divise $r-s$, ce qui signifie puisque s est premier avec m que $\varphi\left(\frac{r}{s}\right) = 1$.

Donc φ induit un isomorphisme $\overline{\varphi} : I^S/i(\mathbb{Q}_{\mathfrak{m},1}) \to (\mathbb{Z}/m\mathbb{Z})^\times$.

De plus, on a établi précédemment que $\begin{array}{rccc} j : & (\mathbb{Z}/m\mathbb{Z})^\times & \longrightarrow & \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \\ & a & \longmapsto & \sigma_a : \zeta \mapsto \zeta^a \end{array}$ est un isomorphisme.

Le but est donc de prouver que le diagramme suivant commute :

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times & \xrightarrow{\ j\ } & \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \\ \uparrow{\scriptstyle \overline{\varphi}} & \nearrow_{\psi^S_{\mathbb{Q}[\zeta]/\mathbb{Q}}} & \\ I^S/i(\mathbb{Q}_{\mathfrak{m},1}) & & \end{array}$$

Soit p premier tel que $p \nmid m$. Montrons que $j(p) = \sigma_p = (p, \mathbb{Q}[\zeta]/\mathbb{Q})$. Soit $\mathfrak{p}$ au-dessus de p. Alors en notant f le degré résiduel $[\mathscr{O}_K/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$, on a $l_\mathfrak{p} = \mathscr{O}_K/\mathfrak{p} \simeq \mathbb{F}_{p^f}$ donc $l_\mathfrak{p}$ est de caractéristique p.

Par conséquent, le morphisme de Frobenius $x \longmapsto x^p$ est un automorphisme de $\mathscr{O}_K/\mathfrak{p}$.

On admet que $\mathscr{O}_K = \mathbb{Z}[\zeta]$, ce qui peut se prouver à l'aide des calculs effectués dans la proposition 5.2.5, ainsi que des calculs de discriminants, et une récurrence sur le nombre de facteurs premiers apparaissant dans la décomposition de m.

Si $x = P(\zeta) \in \mathfrak{p}$, où $P \in \mathbb{Z}[X]$, alors, en notant $\pi : \mathscr{O}_K \to \mathscr{O}_K/\mathfrak{p}$ la surjection canonique, on a $\sigma_p(x) \mod \mathfrak{p} = \pi(P(\zeta^p)) = \overline{P}(\overline{\zeta}^p) = \left(\overline{P}(\overline{\zeta})\right)^p$ puisque $x \longmapsto x^p$ est un automorphisme.

Par conséquent, $\pi(\sigma_p(x)) = (\overline{P(\zeta)}^p) = 0$ car $x \in \mathfrak{p}$ et $\sigma_p(x) \in \mathfrak{p}$, si bien que $\sigma_p(\mathfrak{p}) = \mathfrak{p}$.

En réutilisant le même calcul, on obtient alors que si $\overline{\sigma}$ est le morphisme réduit modulo $\mathfrak{p}$, on a $\forall x = P(\zeta) \in \mathcal{O}_K, \overline{\sigma}(\overline{P(\zeta)}) = (\overline{P(\zeta)})^p$.

σ_p remplit donc les deux conditions déterminant $(p, K/\mathbb{Q})$, ce qui montre que $j([p]_m) = \sigma_p = (p, K/\mathbb{Q})$. Ainsi, pour p premier ne divisant pas m, $(j \circ \varphi)(p) = \psi^S_{\mathbb{Q}[\zeta]/\mathbb{Q}}(p)$.

Comme I^S est un groupe libre engendré par les premiers ne divisant pas m, on en déduit immédiatement que $\psi^S_{\mathbb{Q}[\zeta]/\mathbb{Q}} = j \circ \overline{\varphi}$ donc $\ker \psi^S = i(\mathbb{Q}_{\mathfrak{m},1})$ ce qui prouve que $\mathfrak{m}$ est un module adapté pour ψ^S.

□

Chapitre 6

Le théorème de Chebotarev

Le but de cette section est d'enfin démontrer le théorème de Chebotarev, qui s'énonce ainsi :

Théorème 6.0.8

Soit L une extension abélienne de K un corps de nombres. Alors, pour tout $\sigma \in \mathrm{Gal}(L/K)$, l'ensemble

$$\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : \mathfrak{p} \text{ ne se ramifie pas dans } L, (\mathfrak{p}, L/K) = \sigma\}$$

a une densité de Dirichlet égale à $\frac{1}{|G|}$.

La notion de densité de Dirichlet est de nature analytique, ce qui justifie que l'on commence ce chapitre par des considérations d'analyse complexe. De plus, l'utilisation de séries comme les fonctions zêta permet en un certain sens de regrouper tous les premiers de K dans un seul objet.

En réalité, le théorème de Chebotarev est vrai pour la notion la plus simple de densité, celle de densité naturelle. Si $T \subset \mathrm{Spec}(\mathcal{O}_K)$, elle se définit par

$$\delta(T) = \lim_{n \to +\infty} \frac{\mathrm{Card}\,\{\mathfrak{p} \in T : N(\mathfrak{p}) \leqslant n\}}{\mathrm{Card}\,\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) : N(\mathfrak{p}) \leqslant n\}}$$

Malheureusement, même si le théorème de Chebotarev est vrai avec cette notion de densité, les résultats sont bien plus délicats à obtenir. C'est pourquoi on se restreint à la démonstration pour la densité de Dirichlet.

6.1 Fonctions L et prolongements méromorphes

Toutes les séries qu'on étudiera par la suite sont des *séries de Dirichlet*, c'est à dire des séries de la forme $\sum_{n \geqslant 1} \frac{a_n}{n^s}, s \in \mathbb{C}$.

Définition 6.1.1

Soit K un corps de nombres

- *Un caractère de Dirichlet associé à un module $\mathfrak{m}$ est un morphisme $\chi : C_{\mathfrak{m}} \longrightarrow \mathbb{C}^\times$. De manière équivalente, il peut être considéré comme un morphisme de $I_K^{S(\mathfrak{m})}$ dans $\mathbb{C}^\times$ dont le noyau contient $i(K_{\mathfrak{m},1})$.*

- *A tout caractère de Dirichlet χ, on associe une fonction $L(\cdot, \chi)$ telle que*

$$\forall s, L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

où la somme est sur les idéaux entiers $\mathfrak{a}$ de $\mathcal{O}_K$ premiers avec $\mathfrak{m}$.

Cette fonction est appelé fonction L associée à χ.

Remarque. Comme $C_{\mathfrak{m}}$ est un groupe fini, χ est à valeurs dans l'ensemble des racines de l'unité de $\mathbb{C}$ donc $\forall \mathfrak{p} \in I_K^{S(\mathfrak{m})}, |\chi(\mathfrak{p})| = 1$.

Définition 6.1.2

Soit K un corps de nombres.

$\zeta_K(s) = \sum_{\mathfrak{p}\in \mathrm{Spec}(K)} \frac{1}{N(\mathfrak{p})^s}$ *est appelée fonction zêta associée à K. On remarque que $\zeta_K = L(\cdot, \chi_0)$ où χ_0 est le caractère trivial.*

6.1.1 Prolongement des fonctions L

Le but de cette sous-section est de prolonger les fonctions L en des fonctions méromorphes sur un ouvert de $\mathbb{C}$ contenant 1, alors qu'elles sont à première vue définies uniquement pour les complexes de partie réelle strictement supérieure à 1. On pourra ainsi étudier leur comportement au voisinage de 1, ce qui est un point crucial pour démontrer le théorème de Chebotarev.

Dans toute la suite, on note Arg la fonction argument principal.

Théorème 6.1.3

Soit $f : s \longmapsto \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$, et $S : x \longmapsto \sum_{n\leqslant x} a_n$.

Si on suppose qu'il existe $a \geqslant 0, b \geqslant 0, C \geqslant 0$ tels que $\forall x \geqslant C, |S(x)| \leqslant a x^b$, alors pour tout $\delta, \varepsilon > 0$, $\sum_{n\geqslant 1} \frac{a_n}{n^s}$ converge uniformément sur $\in D(b,\delta,\varepsilon)$, où

$$D(b,\delta,\varepsilon) = \left\{ s \in \mathbb{C} : \mathrm{Re}(s) \geqslant b + \delta \text{ et } |\mathrm{Arg}(s-b)| \leqslant \frac{\pi}{2} - \varepsilon \right\}$$

Par conséquent, f est holomorphe dans le demi-plan $\{\mathrm{Re}(s) > b\}$.

Démonstration. On va s'appuyer sur le critère de Cauchy de convergence uniforme et utiliser une transformation d'Abel.

Prenons $n_1 > n_2 \geqslant C$. Soit $s = u + iv \in \mathbb{C}$.

$$\begin{aligned}
\left|\sum_{n=n_1}^{n_2} \frac{a_n}{n^s}\right| &= \left|\sum_{n=n_1}^{n_2} \frac{S(n)-S(n-1)}{n^s}\right| = \left|\sum_{n=n_1}^{n_2} \frac{S(n)}{n^s} - \sum_{n=n_1-1}^{n_2-1} \frac{S(n)}{(n+1)^s}\right| \\
&= \left|\frac{S(n_2)}{n_2^s} - \frac{S(n_1-1)}{n_1^s} + \sum_{n=n_1}^{n_2-1} S(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| \\
&\leqslant \frac{|S(n_2)|}{n_2^u} + \frac{|S(n_1-1)|}{n_1^u} + \sum_{n=n_1}^{n_2-1} |S(n)| \left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \\
&\leqslant \frac{|S(n_2)|}{n_2^u} + \frac{|S(n_1-1)|}{n_1^u} + \sum_{n=n_1}^{n_2-1} |S(n)| \left| s\int_n^{n+1} \frac{\mathrm{d}t}{t^{s+1}}\right|
\end{aligned}$$

En effet, $\displaystyle\int_n^{n+1} \frac{\mathrm{d}t}{t^{s+1}} = \left[\frac{-s}{t^s}\right]_n^{n+1}$. Donc, comme $|S(x)| \leqslant ax^b$, on a :

$$\begin{aligned}
\left|\sum_{n=n_1}^{n_2} \frac{a_n}{n^s}\right| &\leqslant \frac{a}{n_2^{u-b}} + \frac{a}{n_1^{u-b}} + \sum_{n=n_1}^{n_2-1} |s| a n^b \left|\int_n^{n+1} \frac{\mathrm{d}t}{t^{s+1}}\right| \\
&\leqslant \frac{2a}{n_1^{u-b}} + \sum_{n=n_1}^{n_2-1} |s| a \left|\int_n^{n+1} \frac{t^b \mathrm{d}t}{t^{s+1}}\right| \leqslant \frac{2a}{n_1^{u-b}} + |s| a \sum_{n=n_1}^{n_2-1} \int_n^{n+1} \frac{\mathrm{d}t}{t^{u+1-b}} \\
&\leqslant \frac{2a}{n_1^{u-b}} + |s| a \int_{n_1}^{+\infty} \frac{\mathrm{d}t}{t^{u+1-b}} \leqslant \frac{2a}{n_1^{u-b}} + |s| a \left[\frac{1}{-(u-b)t^{u-b}}\right]_{n_1}^{+\infty} \\
&\leqslant \frac{2a}{n_1^{u-b}} + \frac{|s| a}{u-b} \frac{1}{n_1^{u-b}}
\end{aligned}$$

Mais si $\delta, \varepsilon > 0$ et $s \in D(b, \delta, \varepsilon)$, on a, en écrivant $s - b = re^{i\theta}$,

$$\frac{|s|}{u-b} \leqslant \frac{|s-b|}{u-b} + \frac{b}{u-b} = \frac{1}{\cos(\theta)} + \frac{b}{u-b} \leqslant \frac{1}{\cos(\theta)} + \frac{b}{\delta} \leqslant M + \frac{b}{\delta}$$

où M est un minorant de cos sur $\left[-\frac{\pi}{2} + \varepsilon; \frac{\pi}{2} - \varepsilon\right]$ puisque $|\mathrm{Arg}(s-b)| \leqslant \frac{\pi}{2} - \varepsilon$.

Finalement, $\left|\sum_{n=n_1}^{n_2} \frac{a_n}{n^s}\right| \frac{2a}{n_1^{u-b}} + \frac{a}{n_1^{u-b}}\left[M + \frac{b}{\delta}\right] \longrightarrow_{n_1 \to +\infty} 0$, avec convergence uniforme par rapport à s sur $D(b, \delta, \varepsilon)$.

Par conséquent, f est holomorphe sur $D(b, \delta, \varepsilon)$ comme limite uniforme d'une suite de fonctions holomorphes [1].

En fin de compte, f est holomorphe sur $\{\mathrm{Re}(s) > b\} = \bigcup_{\delta, \varepsilon > 0} D(b, \delta, \varepsilon)$. □

Ce résultat est l'outil de base pour prolonger les fonctions L.

Remarque. Pour le cas (simple !) de la fonction zêta de Riemann, $S(x) = E(x) \leqslant x$, où E est la fonction partie entière, donc ζ est holomorphe sur $\{\mathrm{Re}(s) > 1\}$.

Proposition 6.1.4

La fonction ζ de Riemann admet un prolongement méromorphe sur le demi-plan $\{\mathrm{Re}(s) > 0\}$ avec un seul pôle possible en 1.

Démonstration. Soit $\zeta_2(s) = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n^s}$. Pour cette série de Dirichlet, $S_2(x) \in \{0, 1\}$ donc $\forall b > 0, \forall x \geqslant 1, |S(x)| \leqslant x^b$. Selon le théorème précédent, ζ_2 est holomorphe sur $\{\mathrm{Re}(s) > b\}$ pour tout $b > 0$, donc en fin de compte sur le demi-plan $\{\mathrm{Re}(s) > 0\}$.

De plus,

$$\forall s, \zeta(s) - \frac{2}{2^s}\zeta(s) = \left(1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots\right) - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s}\right) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots = \zeta_2(s)$$

Et $1 - \frac{2}{2^s} = 0 \Leftrightarrow \exp(\ln(2)(s-1)) = 1 \Leftrightarrow \exists k \in \mathbb{Z} : \ln(2)(s-1) = 2k\pi i \Leftrightarrow \exists k \in \mathbb{Z} : s = 1 + \frac{2k\pi i}{\ln 2} = s_k$.

En dehors de ces points, on a donc $\forall s \in \{\mathrm{Re}(s) > 1\}, \zeta(s) = \frac{\zeta_2(s)}{1 - 2^{1-s}}$.

1. pour la démonstration de ce fait, se référer à [2], page 16.

Donc ζ peut être prolongée en une fonction méromorphe sur $\{\mathrm{Re}(s) > 0\}$, avec des pôles éventuels en $s_k, k \in \mathbb{N}$.

Or, soit $\zeta_3(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \dots$. De même que pour ζ_2, ζ_3 est holomorphe sur $\{\mathrm{Re}(s) > 0\}$, et de plus :

$$\zeta(s) - \frac{3}{3^s}\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} - \sum_{n=1}^{+\infty} \frac{3}{(3n)^s} = \sum_{k=1}^{+\infty} \frac{1}{k^s} + \frac{1}{(2k)^s} - \frac{2}{(3k)^s} = \zeta_3(s)$$

Qui plus est, $3^{s-1} = 1 \iff \exists k \in \mathbb{Z} : s = 1 + \frac{2k\pi i}{\ln 3} = s'_k$. Donc, en dehors de ces s'_k, $\zeta(s) = \frac{\zeta_3(s)}{1 - 3^{1-s}}$.

En combinant ce qu'on a obtenu avec ζ_2 et ζ_3, un pôle de ζ doit nécessairement être de la forme $u = 1 + \frac{2k\pi i}{\ln 2} = 1 + \frac{2k'\pi i}{\ln 3}$ où $k, k' \in \mathbb{N}$.

Donc si $u \neq 1$, $\frac{k}{k'} = \frac{\ln 2}{\ln 3}$ donc $2^{k'} = 3^k$ ce qui n'est possible que si $k = k' = 0$. Donc ζ est méromorphe sur $\{\mathrm{Re}(s) > 0\}$ avec pour seul pôle possible 1.

□

Proposition 6.1.5

Si $s > 1$, on a $\frac{1}{s-1} \leqslant \zeta(s) \leqslant 1 + \frac{1}{s-1}$. ζ a donc un pôle simple en 1 de résidu 1.

$$\forall s \in \{\mathrm{Re}(s) > 0\}, \zeta(s) = \frac{1}{s-1} + g(s)$$

où g est holomorphe sur $\{\mathrm{Re}(s) > 0\}$.

Démonstration. Soit $s > 1$. Comme $x \longmapsto \frac{1}{x^s}$ est décroissante sur $\mathbb{R}_+^*$, on a :

$$\forall n \geqslant 2, \int_{n-1}^{n} \frac{\mathrm{d}x}{x^s} \geqslant \frac{1}{n^s} \geqslant \int_{n}^{n+1} \frac{\mathrm{d}x}{x^s}$$

Pour $n = 1$, on a $\int_1^2 \frac{\mathrm{d}x}{x^s} \leqslant 1$.

Donc en sommant de $n = 1$ à $+\infty$, on obtient :

$$1 + \int_1^{+\infty} \frac{\mathrm{d}x}{x^s} \geqslant \zeta(s) \geqslant \int_1^{+\infty} \frac{\mathrm{d}x}{x^s}$$

Mais $\int_1^{+\infty} \frac{\mathrm{d}x}{x^s} = \left[\frac{x^{1-s}}{1-s}\right]_1^{+\infty} = \frac{1}{s-1}$ donc $\frac{1}{s-1} \leqslant \zeta(s) \leqslant 1 + \frac{1}{s-1}$.

Donc $(s-1)\zeta(s) \to 1$ quand s tend vers 1 par valeurs réelles supérieures. Par conséquent, ζ ne peut avoir de singularité essentielle en 1, et on peut trouver $m \in N, c \in \mathbb{C}$ et g holomorphe autour de $s = 1$ tels que $\zeta(s) = \frac{c}{(s-1)^m} + \frac{g(s)}{(s-1)^{m-1}}$.

Or, $(s-1)\zeta(s) \to 1$ ce qui assure que $m = 1$, donc $\zeta(s) = \frac{c}{(s-1)} + g(s)$ et $\zeta(s) - \frac{c}{(s-1)}$ admet une limite finie en 1. En multipliant par $s-1$ et en prenant la limite en 1, on obtient $c = 1$. □

Ces résultats sur la fonction zêta nous serviront de base pour prolonger analytiquement les fonctions L à l'aide de ce principe :

Proposition 6.1.6

On reprend les notations du théorème 6.1.3.

Si $f : s \longmapsto \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$ *est une série de Dirichlet telle qu'il existe* $C \geqslant 0$ *et* $b \in [0;1[$ *tel que* $\forall n \in \mathbb{N}^*, |S(n) - a_0 n| \leqslant C n^b$ *, alors* f *s'étend en une fonction méromorphe sur* $\{\mathrm{Re}(s) > b\}$ *avec un pôle simple en 1 de résidu* a_0*.*

C'est-à-dire : au voisinage de 1, $f(s) = \frac{a_0}{s-1} + g(s)$ *où* g *est holomorphe.*

Démonstration. Soit $h : s \longmapsto f(s) - a_0\zeta(s)$. $h(s)$ est encore une série de Dirichlet et $\forall n \in \mathbb{N}, S_h(n) = \sum_{k=1}^{n}(a_k - a_0) = S(n) - a_0 n$.

Donc $\forall n \in \mathbb{N}, |S_h(n)| \leqslant C n^b$, d'où trivialement $\forall x \geqslant 0, |S_h(x)| \leqslant C x^b$.

Donc h est holomorphe sur $\{\mathrm{Re}(s) > b\}$, ce qui assure que f est méromorphe sur $\{\mathrm{Re}(s) > b\}$ avec un unique pôle en 1 de résidu a_0 au vu des propriétés de ζ. □

Définition 6.1.7

Soit K *un corps de nombres, et* $\mathfrak{m}$ *un module pour* K*. Pour* $l \in C_{\mathfrak{m}}$*, on définit la fonction zêta partielle :*

$$\zeta(s,l) = \sum_{\substack{\mathfrak{a} \text{ entier} \\ \mathfrak{a} \in l}} \frac{1}{N(\mathfrak{a})^s}$$

Si χ est un caractère de C_m, alors il est évident que $\forall s, L(s,\chi) = \sum_{l \in C_m} \chi(l)\zeta(s,l)$.

En particulier, pour $\chi = \chi_0$, on a $\zeta_K(s) = \sum_{l \in C_{\mathfrak{m}}} \zeta(s,l)$.

On admet le résultat suivant :

Théorème 6.1.8

Pour K *un corps de nombres et* $\mathfrak{m}$ *un module pour* K*, il existe une constante* $g_{\mathfrak{m}}$ *ne dépend que de* K *de* $\mathfrak{m}$ *telle que*

$$\forall x \geqslant 0, |S(x,l) - g_{\mathfrak{m}}| \leqslant C x^{1-\frac{1}{d}}$$

où $d = [K : \mathbb{Q}]$.

Ce théorème et la proposition 6.1.6 donnent les résultats suivants :

Corollaire 6.1.9

La fonction zêta partielle $\zeta(\cdot, l)$ *est méromorphe sur* $\left\{\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}\right\}$*, avec un unique pôle simple en* 1 *où son résidu est* $g_{\mathfrak{m}}$*.*

Corollaire 6.1.10

Soit K *un corps de nombres et* $\mathfrak{m}$ *un module pour* K *Si* χ *est un caractère non trivial de* $C_{\mathfrak{m}}$*, alors* $L(\cdot, \chi)$ *est holomorphe sur* $\left\{\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}\right\}$*.*

On va utiliser le lemme suivant :

Lemme 6.1.11

Soit G un groupe abélien fini et χ un caractère non trivial de G. Alors $\sum_{a\in G}\chi(a)=0$.

Démonstration. Soit $b\in G$ tel que $\chi(b)\neq 1$. Comme G est fini, $a\longmapsto ab$ est une permutation de G donc $\sum_{a\in G}\chi(a)=\sum_{a\in G}\chi(ab)=0=\chi(b)\sum_{a\in G}\chi(a)$ donc comme $\chi(b)-1\neq 0$, $\sum_{a\in G}\chi(a)=0$. □

Démonstration (du corollaire)**.** On écrit $\forall l\in C_{\mathfrak{m}},\zeta(s,l)=\frac{g_{\mathfrak{m}}}{s-1}+f_l(s)$, où f_l est holomorphe sur $\left\{\mathrm{Re}(s)>1-\frac{1}{[K:\mathbb{Q}]}\right\}$.

Alors $\forall s\in\left\{\mathrm{Re}(s)>1-\frac{1}{[K:\mathbb{Q}]}\right\}$,

$$\begin{aligned}L(s,\chi) &= \sum_{l\in C_m}\chi(l)\zeta(s,l)=\sum_{l\in C_m}\chi(l)\frac{g_{\mathfrak{m}}}{s-1}+\chi(l)f_l(s)\\ &= \frac{\sum_{l\in C_m}\chi(l)g_{\mathfrak{m}}}{s-1}+h(s)=h(s)\end{aligned}$$

où h est une fonction holomorphe, en utilisant le lemme.

□

Corollaire 6.1.12

Si K est un corps de nombres, ζ_K est méromorphe sur $\left\{\mathrm{Re}(s)>1-\frac{1}{[K:\mathbb{Q}]}\right\}$ avec un unique pôle simple en 1.

6.1.2 Développement en produit eulérien

Définition 6.1.13

Soit $(b_n)_{n\in\mathbb{N}}\in(\mathbb{C}\setminus\{-1\})^{\mathbb{N}}$

- *On dit que $\prod_{n\in\mathbb{N}}(1+b_n)$ converge si la suite des produits partiels $\pi_m=\prod_{n=0}^{m}(1+b_n)$ converge vers $l\neq 0$.*
- *On dit que $\prod_{n\in\mathbb{N}}(1+b_n)$ converge absolument si $\prod_{n\in\mathbb{N}}(1+|b_n|)$ converge.*

Cette proposition se montre aisément avec des manipulations élémentaires sur les produits et en utilisant la fonction exponentielle :

Proposition 6.1.14

Si $\forall n, b_n\geqslant 0$, alors $\prod(1+b_n)$ converge si et seulement si $\sum b_n$ converge.

Remarque. Donc toute permutation des termes d'un produit absolument convergent donne encore un produit absolument convergent.

Comme dans le cas des séries, la convergence absolue implique la convergence :

Proposition 6.1.15

Si $\prod_{n\in\mathbb{N}}(1+b_n)$ converge absolument, alors il converge.

Démonstration. On commence par montrer, par une récurrence facile, que pour tout $N\in\mathbb{N}$ et $(z_0,\dots,z_N)$, famille de complexes différents de -1, $\left|\prod_{n=0}^{N}(1+z_n)-1\right| \leqslant \prod_{n=0}^{N}(1+|z_n|)-1$.

Alors, si on note $P_n=\prod_{k=0}^{n}(1+b_n)$ et $Q_n=\prod_{k=0}^{n}(1+|b_n|)$, on a :

$$\begin{aligned}\forall n>m, |P_n-P_m| &= \left|\prod_{k=0}^{n}(1+b_n)-\prod_{k=0}^{m}(1+b_n)\right| = \left|\prod_{k=0}^{m}(1+b_n)\right|\left|\prod_{k=m+1}^{n}(1+b_n)-1\right| \\ &\leqslant \prod_{k=0}^{m}(1+|b_n|)\left(\prod_{k=m+1}^{n}(1+|b_n|)-1\right) = Q_n-Q_m\end{aligned}$$

en utilisant d'une part l'inégalité triangulaire et d'autre part l'inégalité qu'on vient de prouver.

Donc, puisque (Q_n) est de Cauchy car convergente, (P_n) est de Cauchy donc converge vers $l\in\mathbb{C}$.

Or, $\forall z, |z|<1, |\ln|1+z|| \leqslant -\ln(1-|z|)$ (conséquence de l'inégalité triangulaire). Donc comme (b_n) tend vers 0, $|b_n|<1$ à partir d'un certain rang et $|\ln(|1+b_n|)| \leqslant -\ln(1-|b_n|)$. Mais $-\ln(1-|b_n|)\sim_{n\to+\infty}|b_n|$ qui est le terme général positif d'une série convergente selon la proposition précédente puisque $\prod(1+b_n)$ converge absolument. Donc $\sum_{n\in\mathbb{N}}|\ln(|1+b_n|)|$ converge.

Si $l=0$, alors $|P_n|\longrightarrow 0$ et donc $\prod_{n\in\mathbb{N}}|u_n|$ tend vers 0, et en passant au logarithme, on voit que $\sum\ln|u_n|$ tend vers $-\infty$ ce qui est absurde. Donc $l\neq 0$ et le résultat est démontré.

□

On va maintenant développer les fonctions L en des produits infinis dits *eulériens*.

Il est bien connu que $\zeta(s)=\prod_{p\text{ premier}}\frac{1}{1-p^{-s}}$, cela a été démontré intuitivement par Euler en s'appuyant sur le crible d'Erathostène. En fait, toutes les fonctions L se développent en un produit similaire.

Définition 6.1.16

Soit K un corps de nombres. Un produit eulérien est un produit infini de la forme

$$\prod_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_K)\setminus S}\frac{1}{(1-\theta_1(\mathfrak{p})N(\mathfrak{p})^{-s})\dots(1-\theta_d(\mathfrak{p})N(\mathfrak{p})^{-s})}$$

où S est un ensemble fini de premiers, $s\in\mathbb{C}$ et $\theta_i(\mathfrak{p})$ des complexes.

Théorème 6.1.17

Soit K un corps de nombres, χ un caractère de Dirichlet pour un module m. Alors pour tout s de partie réelle strictement plus grande que 1, le produit eulérien $\prod_{\mathfrak{p}\nmid\mathfrak{m}}\frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}}$ converge vers $L(s,\chi)$.

Démonstration. Si $\mathrm{Re}(s)>1$, on a, puisque $\forall\mathfrak{p}\in I_K^{S(\mathfrak{m})}, N(\mathfrak{p})=\mathrm{Card}(\mathcal{O}_K/\mathfrak{p})>1$ et $|\chi(\mathfrak{p})|=1$,

$$\frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}} = \sum_{n=0}^{+\infty} (\chi(\mathfrak{p})N(\mathfrak{p})^{-s})^n = \sum_{n=0}^{+\infty} \frac{\chi(\mathfrak{p}^n)}{(N(\mathfrak{p}^n))^s}$$

Donc (produit de Cauchy) : si $l \in \mathbb{N}^*$,

$$\prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ N(\mathfrak{p})\leqslant l}} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}} = \sum \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

la somme étant sur les idéaux $\mathfrak{a}$ entiers s'écrivant comme produits d'idéaux premiers de norme inférieure à l.

Le terme de droite converge absolument (l'ordre des termes n'important donc pas), donc celui de gauche également quand l tend vers l'infini, et leur limite commune est $L(s,\chi)$. □

6.2 Notions de densité

On va définir plusieurs densités, qui sont des notions décrivant la répartition d'un ensemble de premiers parmi tous les premiers d'un corps de nombres.

6.2.1 Densité polaire

On fixe K un corps de nombres.

Définition 6.2.1

Soit $T \subset \mathrm{Spec}(\mathcal{O}_K)$. On définit

$$\zeta_{K,T}(s) := \prod_{\mathfrak{p}\in T} \frac{1}{1-N(\mathfrak{p})^{-s}}$$

Si il existe n tel que $\zeta_{K,T}^n$ se prolonge en une fonction méromorphe au voisinage de 1 avec un pôle d'ordre m en 1, alors T a une densité polaire $\delta(T) = \frac{m}{n}$.

On adopte la convention qu'un zéro d'ordre m est un pôle d'ordre $-m$.

On a quelques propriétés correspondant à ce que l'on est en droit d'attendre d'une densité :

- L'ensemble de tous les idéaux premiers de K a une densité polaire de 1.
- Si T admet une densité polaire, $\delta(T) \geqslant 0$.
- Un ensemble fini a une densité nulle.
- Si T est l'union disjointe de T_1 et T_2, et si deux d'entre eux ont une densité polaire, le troisième en a une et $\delta(T) = \delta(T_1) + \delta(T_2)$.
- Si T_1 et T_2 ont des densités polaires et $T_1 \subset T_2$, alors $\delta(T_1) \leqslant \delta(T_2)$.

Le premier point n'est autre que le corollaire 6.1.12. Le deuxième est évident puisque si $\zeta_{K,T}$ n'a pas de pôle en 1, $\zeta_{K,T}(1) = \prod_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_K)} \frac{1}{1-N(\mathfrak{p})^{-1}} > 0$ donc 1 est pôle d'ordre 0.

Pour le troisième point, on remarque que $\zeta_{K,T}(s) = \zeta_{K,T_1}(s)\zeta_{K,T_2}(s)$ donc si $\zeta_{K,T_1}^{n_1}$ et $\zeta_{K,T_2}^{n_2}$ se prolongent en des fonctions méromorphes avec des pôles en 1 d'ordres respectifs m_1 et

m_2, $\zeta_{K,T}(s)^{n_1 n_2}(s)$ admet un pôle d'ordre $n_2 m_1 + n_1 m_2$ en 1 donc $\delta(T) = \dfrac{n_2 m_1 + n_1 m_2}{n_1 n_2} = \dfrac{n_1}{m_1} + \dfrac{n_2}{m_2} = \delta(T_1) + \delta(T_2)$.

Proposition 6.2.2

Si $T \subset \mathrm{Spec}(\mathcal{O}_K)$ ne contient pas d'idéaux premiers $\mathfrak{p}$ tels que $N(\mathfrak{p})$ soit un premier de $\mathbb{Z}$, alors $\delta(T) = 0$.

Démonstration. Soit $\mathfrak{p} \in T$. On a $N(\mathfrak{p}) = p^f$, où $p = \mathfrak{p} \cap \mathcal{O}_K$ premier de $\mathbb{Z}$ et $f \geqslant 2$ est le degré résiduel de $\mathfrak{p}$ sur p.

De plus, si p est un premier donné de $\mathbb{Z}$, il y a au plus $d = [K : \mathbb{Q}]$ premiers de K au-dessus de p. Donc $\zeta_{K,T}$ s'écrit comme un produit $\prod_{i=1}^{d} g_i$ où $g_i(s)$ est un produit infini sur les premiers de $\mathbb{Z}$ dont chaque facteur est soit 1 soit $\dfrac{1}{1-p^{-fs}}$ où $f \geqslant 2$.

Par conséquent, $\forall i \in [\![1; d]\!], g_i(1) \leqslant \prod_{p \text{ premier}} \dfrac{1}{1-p^{-f}} \leqslant \prod_{p \text{ premier}} \dfrac{1}{1-p^{-2}} = \zeta(2)$, car $p^f \geqslant p^2$

Donc g_i est holomorphe au voisinage de 1, donc $\zeta_{K,T}$ également. □

Remarque. Il est donc immédiat que si T_1 et T_2 sont deux ensembles d'idéaux premiers de K et si $T_1 \setminus T_2$ et $T_2 \setminus T_1$ ne contiennent que des premiers $\mathfrak{p}$ tels que $N(\mathfrak{p})$ n'est pas premier, alors, si l'un a une densité polaire, l'autre en a aussi une, et elles sont égales.

Cela nous permet donc de démontrer le cas $\sigma = \mathrm{id}$ du théorème de Chebotarev, du moins en utilisant le lien entre densité polaire et densité de Dirichlet qu'on verra dans la proposition 6.2.8.

Théorème 6.2.3

Si L/K est une extension galoisienne, l'ensemble des idéaux premiers de K totalement décomposés dans L a une densité polaire de $\dfrac{1}{[L : K]}$.

Démonstration. Soit S l'ensemble des idéaux premiers de K totalement décomposés dans L, et T l'ensemble des idéaux premiers de L au-dessus des éléments de S.

Si $\mathfrak{p} \in S$, par définition, il y a exactement $[L : K]$ idéaux premiers $\mathfrak{P}$ dans T au-dessus de $\mathfrak{p}$ avec un degré résiduel de 1, donc $N(\mathfrak{P}) = N(\mathfrak{p})$.

Donc $\zeta_{L,T} = \zeta_{K,S}^{[L:K]}$.

Or, T contient tous les $\mathfrak{P}$ quand $\mathfrak{P} \cap \mathcal{O}_K$ est un idéal non ramifié dans L et $N(\mathfrak{P}) = \mathfrak{p}$ premier. En effet, si $\mathfrak{P}$ est un tel idéal, et $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, alors $N(\mathfrak{P}) = N(\mathfrak{p})^f$, soit $p = N(\mathfrak{p})^f$ donc comme $N(\mathfrak{p}) \neq 1$, $N(\mathfrak{p}) = p = N(\mathfrak{P})$ et $f = 1$.

Donc T diffère de l'ensemble des idéaux premiers de K d'un ensemble de premiers de norme non première dans $\mathbb{Z}$ donc selon la proposition précédente, T a une densité et $\delta(T) = 1$.

Donc par définition, S a une densité de $\dfrac{1}{[L : K]}$. □

Corollaire 6.2.4

Si L/K est une extension abélienne, et S est un ensemble fini de premiers incluant les premiers infinis et ceux qui se ramifient dans L. Alors la fonction d'Artin $\psi_{L/K} : I_K^S \longrightarrow$

$\mathrm{Gal}(L/K)$ *est surjective.*

Démonstration. Soit H l'image de $\psi_{L/K}$, sous groupe de $G = \mathrm{Gal}(L/K)$. On peut donc considérer K' le corps des invariants de H. Comme G est abélien, H est distingué dans G donc K'/K est une extension abélienne et on sait alors que

$$\forall \mathfrak{p} \notin S, (\mathfrak{p}, K'/K) = (\mathfrak{p}, L/K)_{|K} = \mathrm{id}$$

puisque $(\mathfrak{p}, L/K) \in H$.

Donc $\mathfrak{p}$ est totalement décomposé dans K'. Ainsi, tous les idéaux premiers de K sauf un nombre fini se décomposent totalement dans K'.

Or, l'ensemble des $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ totalement décomposés dans K' a une densité polaire de $\dfrac{1}{[K' : K]}$ selon le théorème précédent. Mais comme un ensemble fini a une densité nulle, cet ensemble a également une densité de 1, donc $[K' : K] = 1$. Cela signifie que $K' = K$ et $H = G$, d'où la surjectivité de l'application d'Artin. □

6.2.2 Densité de Dirichlet

On se donne K un corps de nombres.

Définition 6.2.5

Soient f et g deux fonctions complexes définies au moins sur $]1; +\infty|$. On dit que $f(s) \sim_{s\downarrow 1} g(s)$ si $(f-g)(s)$ est bornée au voisinage de 1 pour s réel, $s > 1$.

Définition 6.2.6

Soit $T \subset \mathrm{Spec}(\mathcal{O}_K)$. T admet $\delta \geqslant 0$ pour densité de Dirichlet si

$$\sum_{\mathfrak{p}\in T} \frac{1}{N(\mathfrak{p})^s} \sim_{s\downarrow 1} \delta \ln\left(\frac{1}{s-1}\right)$$

Remarque. Dans ce cas, particulier, on a $f(s) = \sum_{\mathfrak{p}\in T} \dfrac{1}{N(\mathfrak{p})^s} \sim_{s\to 1} \delta \ln\left(\dfrac{1}{s-1}\right)$ au sens usuel - en se restreignant toutefois à $s > 1$. En effet, $g(s) = \delta \ln\left(\dfrac{1}{s-1}\right)$ tend vers 0 quand s tend vers 0 par valeurs supérieures et

$$\frac{f(s)}{g(s)} - 1 = \frac{f(s) - g(s)}{g(s)} \longrightarrow_{s\to 1} 0$$

puisque $f - g$ est bornée au voisinage de 1.

Commençons par un lemme :

Lemme 6.2.7

Si $(u_j)_{j\in\mathbb{N}} \in [2; +\infty[^{\mathbb{N}}$ est tel que $f(s) := \prod_{j=1}^{+\infty} \dfrac{1}{1-u_j^s}$ est un produit infini uniformément convergent sur chaque $D(1, \delta, \varepsilon) = \left\{ s \in \mathbb{C} \mid \mathrm{Re}(s) \geqslant 1+\delta, |\mathrm{Arg}(s-1)| \leqslant \dfrac{\pi}{2} - \varepsilon \right\}$. Alors

$$\ln f(s) \sim_{s\downarrow 1} \sum_{j=1}^{+\infty} \frac{1}{u_j^s}$$

Démonstration. Soit $s > 1$. Alors $f(s) > 0$ clairement et, en utilisant le développement $\ln\left(\frac{1}{1-z}\right) = \sum_{n=1}^{+\infty} \frac{z^n}{n}$,

$$\begin{aligned} \ln f(s) &= \sum_{j=1}^{+\infty} \ln\left(\frac{1}{1-u_j^{-s}}\right) = \sum_{j=1}^{+\infty}\sum_{m=1}^{+\infty} \frac{1}{mu_j^{sm}} \\ &= \sum_{j=1}^{+\infty} \frac{1}{u_j^s} + \sum_{j=1}^{+\infty}\sum_{m=2}^{+\infty} \frac{1}{mu_j^{sm}} = \sum_{j=1}^{+\infty} \frac{1}{u_j^s} + g(s) \end{aligned}$$

Donc, comme $\forall j, u_j > 0$ et $s \in \mathbb{R}$,

$$|g(s)| \leqslant \sum_{j=1}^{+\infty}\sum_{m=2}^{+\infty} \left|\frac{1}{mu_j^{sm}}\right| = \sum_{j=1}^{+\infty}\sum_{m=2}^{+\infty} \frac{1}{mu_j^{sm}}$$

Mais, si $u \geqslant 2, s > 1$,

$$\sum_{m=2}^{+\infty} \frac{1}{mu^{sm}} \leqslant \sum_{m=2}^{+\infty} \frac{1}{2}\left(\frac{1}{u^s}\right)^m = \frac{1}{2}\left(\frac{u^{-2s}}{1-u^{-s}}\right) < \frac{1}{u^{2s}}$$

Or, selon le même principe que le développement des fonctions L en produits eulériens, $f(2s) = \sum_{(j_1,\dots,j_r)\in(\mathbb{N}^*)^r, r\in\mathbb{N}} u_{j_1}^{-2s} \dots u_{j_r}^{-2s} \geqslant \sum_{j=1}^{+\infty} \frac{1}{u_j^2 s}$.

Donc $|g(s)| \leqslant h(2s)$ pour $s > 1$ où $h : s \longmapsto \sum_{j=1}^{+\infty} \frac{1}{u_j^s}$.

Or, f est holomorphe sur $\{\mathrm{Re}(s) > 1\}$ donc $s \longmapsto f(2s)$ est holomorphe sur $\left\{\mathrm{Re}(s) > \frac{1}{2}\right\}$. Par conséquent, g est bornée au voisinage de 1. Ceci joint à l'égalité $\ln f(s) = \sum \frac{1}{u_j^s} + g(s)$ montre le résultat voulu.

□

On peut en déduire ce résultat :

Proposition 6.2.8

Si la densité polaire de T existe, alors sa densité de Dirichlet aussi et les deux quantités sont égales.

La densité naturelle est également une notion plus forte que la densité de Dirichlet, mais c'est un fait plus délicat à prouver.

On dispose également les mêmes propriétés élémentaires que dans le cas de la densité polaire.

Lemme 6.2.9

Si G est un groupe abélien fini et $a \in G$ un élément différent de 1. Alors en notant $A^\vee$ l'ensemble des caractères sur G, on a

$$\sum_{\chi\in A^\vee} \chi(a) = 0$$

Démonstration. La démonstration est la même que celle du lemme 6.1.11, à condition de montrer qu'il existe $\chi_1 \in A^\vee$ tel que $\chi_1(a) \neq 1$.

Mais, selon le théorème de structure des groupes abéliens, on peut trouver $G_1, \dots, G_p$ des groupes cycliques tels que $G_1 \times \cdots \times G_p \simeq^\varphi G$. On montre alors aisément que $G_1^\vee \times \cdots \times G_p^\vee \simeq G^\vee$ via $(f_1, \dots, f_p) \longrightarrow (f : x = \varphi(x_1, \dots, x_p) \to f_1(x_1) \dots f_p(x_p))$.

Par ailleurs, si $H =< a >$ est cyclique d'ordre n, $\forall u \in \mathbb{U}_n$, il existe un caractère χ de H tel que $\chi(a) = u$.

Ainsi, si $a \in G$, $a \neq 1$, $\varphi^{-1}(a) \neq 1$ et donc on peut clairement trouver un caractère χ_1 tel que $\chi_1(a) \neq 1$. □

Théorème 6.2.10

Soit K un corps de nombres, $\mathfrak{m}$ un module pour K et H un sous-groupe de congruence pour $\mathfrak{m}$ (i.e. $i(K_{\mathfrak{m},1}) \subset H \subset I_K^{S(\mathfrak{m})}$).

Alors $\forall \overline{\mathfrak{a}} \in \overline{H}$, on a, au sens de la densité de Dirichlet,

$$\delta\left(T_{\mathfrak{a}} = \left\{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) \setminus S(\mathfrak{m}) : \overline{\mathfrak{p}} = \overline{\mathfrak{a}}\right\}\right) = \begin{cases} \dfrac{1}{[I_K^{S(\mathfrak{m}):H}]} = \dfrac{1}{[C_{\mathfrak{m}} : \overline{H}]} & \text{si} \quad \forall \chi \in \left(I_K^{S(\mathfrak{m})}/H\right)^\vee, L(1,\chi) \neq 0 \\ 0 \quad \text{sinon.} \end{cases}$$

Démonstration. Soit $\mathfrak{a} \in I_K^{S(\mathfrak{m})}$ et $\overline{\mathfrak{a}}$ sa classe dans $C_{\mathfrak{m}}/\overline{H}$. Soit χ un caractère de $I_K^{S(\mathfrak{m})}$ dont le noyau contient H, et

$$L_(\cdot, \chi) : s \longmapsto \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}}$$

On note $L_n(s, \chi) = \prod_{\substack{\mathfrak{p} \nmid \mathfrak{m} \\ N(\mathfrak{p}) \leqslant n}} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}}$.

On a $\forall s > 1, \log(L_n(s, \chi)) = \sum_{\substack{\mathfrak{p} \nmid \mathfrak{m} \\ N(\mathfrak{p}) \leqslant n}} \log\left(\frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}}\right)$.

En effet, en notant $S_n(s)$ le terme de droite, on a $\forall s > 1, \exp(S_n(s)) = L_n(s, \chi) = \exp(\log(L_n(s, \chi))$. Donc comme exp est un morphisme de $(\mathbb{C}, +)$ dans $(C^*, \times)$ de noyau $2i\pi\mathbb{Z}$, $\forall s > 1, T_n(s) := \log(L_n(s, \chi)) - S_n(s) \in 2i\pi\mathbb{Z}$. Or, T_n est continue sur $]1; +\infty[$ connexe donc T_n est constante sur cet intervalle.

Qui plus est, puisqu'on travaille sur des produits et sommes finies, on a $\lim_{s \to +\infty} \log(L_n(s, \chi)) = \lim_{s \to +\infty} S_n(s) = 0$ donc $T_n(s) = 0$, d'où $\forall n \in \mathbb{N}^*, \forall s > 1, \log(L_n(s, \chi)) = S_n(s)$.

En passant à la limite $n \longrightarrow +\infty$, on obtient

$$\forall s > 1, \log(L(s, \chi) = \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}}$$

Cette égalité était essentiellement tout ce qu'il fallait obtenir pour pouvoir adapter la preuve du lemme précédent au cas présent et affirmer que pour tout caractère χ, $\log(L(s, \chi)) \sim_{s \downarrow 1} \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$.

En utilisant le lemme 6.2.9, on obtient

$$\sum_{\chi\in}\chi(\mathfrak{a})^{-1}\log(L(s,\chi))\sim_{s\downarrow 1}\sum_{\chi\in}\chi(\mathfrak{a})^{-1}\sum_{\mathfrak{p}\nmid\mathfrak{m}}\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}=\sum_{\mathfrak{p}\nmid\mathfrak{m}}\frac{\sum_{\chi\in}\chi(\mathfrak{p})\chi(\mathfrak{a})^{-1}}{N(\mathfrak{p})^s}=\sum_{\mathfrak{p}\in\mathfrak{a}H}\frac{[I^{S(\mathfrak{m})}:H]}{N(\mathfrak{p})^s}$$

De plus, selon le corollaire 6.1.10, si $\chi\neq\chi_0$ (caractère trivial), $L(\cdot,\chi)$ est holomorphe au voisinage de 1, donc $L(s,\chi)=(s-1)^{m(\chi)}g(s)$ où $m(\chi)\in\mathbb{N}$ et $g(1)\neq 0$. Donc en passant au logarithme, $\log(L(s,\chi))\sim_{s\downarrow 1} m(\chi)\log(s-1)=-m(\chi)\log\left(\frac{1}{s-1}\right)$.

Et $L(s,\chi_0)=\dfrac{\zeta_K(s)}{\prod\limits_{\mathfrak{p}|\mathfrak{m}}\frac{1}{1-N(\mathfrak{p})^{-s}}}$, donc, comme selon le corollaire 6.1.12, ζ_K a un pôle simple en 1, on a $L(s,\chi_0)\sim_{s\downarrow 1}\log\left(\frac{1}{s-1}\right)$.

Donc

$$[I^{S(\mathfrak{m})}:H]\sum_{\mathfrak{p}\in\mathfrak{a}H}\frac{1}{N(\mathfrak{p})^s}\sim_{s\downarrow 1}\sum_{\chi\in}\chi(\mathfrak{a})^{-1}\log(L(s,\chi))\sim_{s\downarrow 1}\left(1-\sum_{\chi\neq\chi_0}m(\chi)\right)\log\left(\frac{1}{s-1}\right)$$

Ainsi, par définition de la densité de Dirichlet,

$$\delta(T_{\mathfrak{a}})=\delta(\{\mathfrak{p}\in\mathrm{Spec}(\mathscr{O}_K):\overline{\mathfrak{p}}=\overline{\mathfrak{a}}\})=\frac{\left(1-\sum_{\chi\neq\chi_0}m(\chi)\right)}{[I^{S(\mathfrak{m})}:H]}\geqslant 0$$

Donc si $\forall\chi\neq\chi_0, L(1,\chi)\neq 0$, $\left(1-\sum_{\chi\neq\chi_0}m(\chi)\right)=1$ et $\delta(T_{\mathfrak{a}})=\dfrac{1}{[I^{S(\mathfrak{m})}:H]}$, et sinon, $\delta(T_{\mathfrak{a}})=0$, ce qui prouve le résultat.

□

6.3 Conclusion de la démonstration

On dispose désormais de tous les résultats nécessaires pour montrer le théorème de Chebotarev, ainsi que les deux résultats promis après l'énoncé de la loi de réciprocité d'Artin.

- Le premier, c'est à dire la surjectivité de $\psi_{L/K}^{S(\mathfrak{m})}$ pour toute extension abélienne de corps de nombres L/K et tout module $\mathfrak{m}$ pour K, a été montré avec le corollaire 6.2.4.
- Le deuxième est le fait que pour un module adapté $\mathfrak{m}$, $H=i(K_{\mathfrak{m},1})\mathrm{Nm}(I_L^{S'(\mathfrak{m}})$ vérifie $I_K^{S(\mathfrak{m})}/H\simeq\mathrm{Gal}(L/K)$ via la fonction d'Artin. D'une part, la bonne définition et la surjectivité de $\overline{\psi_{L/K}}:I_K^{S(\mathfrak{m})}/H\longrightarrow\mathrm{Gal}(L/K)$ nous assurent que $[I_K^{S(\mathfrak{m})}:H]\geqslant[L:K]$. D'autre part, on a le théorème suivant :

Théorème 6.3.1

Si L/K est une extension abélienne de corps de nombres, et $\mathfrak{m}$ est un module pour K, alors

$$[I_K^{S(\mathfrak{m})}:H]\leqslant[L:K]$$

Démonstration. Selon le théorème précédent, $\delta(\{\mathfrak{p} \in \mathrm{Spec}(\mathscr{O}_K) : \mathfrak{p} \in H\}$ vaut $\frac{1}{[I^{S(\mathfrak{m})} : H]}$ ou 0 selon que $L(1,\chi) \neq 0 \forall \chi$ caractère non trivial de $I^{S(\mathfrak{m})}/H$ ou non.

Si $\mathfrak{p}$ se décompose totalement dans L, c'est à dire que pour tout P au-dessus de $\mathfrak{p}$, le degré résiduel $f(P/\mathfrak{p})$ vaut 1, alors si P est au-dessus de $\mathfrak{p}$, $\mathrm{Nm}_{L/K}(P) = \mathfrak{p}^{f(P/\mathfrak{p})} = \mathfrak{p}$.

Donc $\{\mathfrak{p} \in H\}$ contient tous les idéaux de $\mathscr{O}_K$ totalement décomposés dans L, puisque $H = \mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})_L}) i(K_{\mathfrak{m},1})$.

Or, $\{\mathfrak{p} \in \mathrm{Spec}(\mathscr{O}_K) : \mathfrak{p}\,\text{totalement decompose}\}$ a une densité de Dirichlet de $\frac{1}{[L:K]} \neq 0$ selon le théorème 6.2.3 et la proposition 6.2.8.

Par conséquent, $\{\mathfrak{p} \in H\}$ ne peut avoir une densité de Dirichlet nulle, donc $\delta(\{\mathfrak{p} \in H\}) = \frac{1}{[I^{S(\mathfrak{m})} : H]} \geqslant \frac{1}{[L:K]}$ donc $[L:K] \leqslant [I^{S(\mathfrak{m})} : H]$. □

Enfin, on va démontrer le théorème de Chebotarev :

Démonstration (du théorème 6.0.8)**.** Selon le théorème précédent, pour $H = i(K_{\mathfrak{m},1})\mathrm{Nm}(I_L^{S'(\mathfrak{m}})$ et $a = 1 \in (I_K^{S(m)}/H)$, $\delta(T_a) = \frac{1}{[I_K^{S(\mathfrak{m})} : H]}$, donc selon le théorème 6.2.10, on a, pour tout caractère χ non trivial de $(I_K^{S(\mathfrak{m})}/H)$, $L(1,\chi) \neq 0$. Donc ce même théorème nous dit que $\forall a \in I_K^{S(\mathfrak{m})}, \delta(T_a) = \frac{1}{[I^{S(\mathfrak{m})} : H]} = \frac{1}{[L:K]}$.

Or, comme $\mathrm{Gal}(L/K)$ est en bijection avec $C_{\mathfrak{m}}/H$, la densité de Dirichlet de $T'_\sigma = \{\mathfrak{p} \in \mathrm{Spec}(\mathscr{O}_K) : \mathfrak{p}$ ne se ra
où σ est à un ensemble fini près celle de T_a où $\psi_{L/K}^{S(m)}(a) = \sigma$.

Comme le théorème de Chebotarev s'intéresse à des questions de densité, l'« oubli » d'un ensemble fini $S(\mathfrak{m})$ n'a aucune importance ici.

Cela démontre le théorème de Chebotarev pour une extension abélienne de corps de nombres. □

En conséquence importante de ce théorème, on obtient le fameux théorème de progression arithmétique de Dirichlet :

Théorème 6.3.2 (*Dirichlet*)

Soit $m \in \mathbb{N}$ et $a \in [\![0; m-1]\!]$. L'ensemble $T_a = \{p \in \mathrm{Spec}(\mathbb{Z}) : p \equiv a[m]\}$ a une densité de Dirichlet de $\frac{1}{\varphi(m)}$.

Démonstration. En effet, soit ζ une racine primitive m-ième de l'unité.

Selon la démonstration du théorème 5.2.7, si $p \nmid m$, p est non ramifié dans $\mathbb{Q}[\zeta]$ et $(p, \mathbb{Q}[\zeta]/\mathbb{Q}) = (\zeta \mapsto \zeta^a) \in \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \Leftrightarrow [p]_m = [a]_m \Leftrightarrow p \equiv a[m]$.

Cette même preuve nous donne de plus un isomorphisme entre $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ et $(\mathbb{Z}/m\mathbb{Z})^\times$ de cardinal $\varphi(m)$ donc le groupe de Galois de $\mathbb{Q}[\zeta]/\mathbb{Q}$ a pour ordre $\varphi(m)$.

Par suite, à l'ensemble fini des diviseurs premiers de m près, T_a est un ensemble de la forme de ceux considérés dans le théorème de Chebotarev, ce qui conclut la preuve. □

Remarque. On a donc démontré intégralement le théorème de progression arithmétique de Dirichlet, puisqu'on a prouvé la loi de réciprocité d'Artin dans le cas cyclotomique.

Chapitre 7

Un aperçu de géométrie algébrique

Dans cette section d'ouverture, on se contentera d'expliquer quelques concepts de géométrie algébrique permettant d'établir une analogie entre l'anneau des entiers d'un corps de nombres et la notion de *courbe*. Comme il s'agit d'un simple résumé d'une vaste théorie, on omettra de nombreux détails et objets de la géométrie algébriques.

Pour plus de détails, on peut se référer à [1] et [5].

7.1 Un aperçu de géométrie algébrique

7.1.1 Variété algébrique

Soit k un corps, qu'on prend dans un premier temps algébriquement clos. Le point de départ de la géométrie algébrique est d'étudier le lieu d'annulation d'un ensemble fini de polynômes à plusieurs variables donné. Naïvement, on peut définir un ensemble algébrique affine sur k comme $\{x \in k^n : P_1(x) = \cdots = P_r(x) = 0\}$ où $P_i \in k[X_1, \ldots, X_n]$. De manière équivalente, si I est un idéal de $k[X_1, \ldots, X_n]$, $Z(I) := \{x \in k^n : \forall P \in I, P(x) = 0\}$ est une variété algébrique affine, puisque, $k[X_1, \ldots, X_n]$ étant un anneau noethérien, $I = (P_1, \ldots, P_r)$ est de type fini, et $Z(I)$ est le lieu d'annulation de $P_1, \ldots, P_r$. On dira donc qu'un *ensemble algébrique affine* est un sous-ensemble de k^n en bijection avec un certain $Z(I)$.

Si I un idéal de $k[X_1, \ldots, X_n]$, $Z(I)$ peut être munie de la *topologie de Zariski* : ses fermés sont les $Z(J) \subset X$ quand J est un idéal de $k[X_1, \ldots, X_n]$. Un *espace topologique algébrique affine* est un espace topologique homéomorphe à un certain $Z(I)$ muni de sa topologie de Zariski.

Au-delà de la notion naïve d'espace topologique algébrique affine, on peut considérer des objets qui sont des réunions de tels espaces : ils possèdent des propriétés très similaires. Formellement, on dit qu'un espace topologique $(X, \mathcal{T})$ est un *espace topologique algébrique* sur k s'il s'écrit $X = \bigcup_{j=1}^{N} X_j$ où X_j est un fermé de X homéomorphe à un certain $Z(I_j) \subset k[X_1, \ldots, X_{n_j}]$, au sens de la topologie de Zariski.

Exemple. La droite projective $\mathbb{P}^1 = \left\{[x, y], (x, y) \in k^2 \setminus \{0\}\right\}$, définie comme $k^2 \setminus \{0\}$ quotienté par la relation de colinéarité, est un espace topologique algébrique.

En effet, si $(x, y) \in k^2 \setminus \{0\}$, soit $x \neq 0$ et $[x, y] = \left[1, \frac{y}{x}\right]$, soit $x = 0$ et $[x, y] = [0, 1]$. Donc $\mathbb{P}^1 = \{[1, \lambda], \lambda \in k \setminus \{0\}\} \cup \{[0, 1]\}$.

On peut alors définir la notion de dimension d'un espace topologique algébrique, qui est en fait très générale :

Si $(X, \mathcal{T})$ est un espace topologique, on dit qu'il est *irréductible* s'il ne peut s'écrire comme union de deux fermés stricts. La *dimension* de X est la longueur maximale n d'une chaîne

de fermés emboîtés irréductibles $X_0 \subset X_1 \subset \cdots \subset X_n = X$.

Dans le cas où l'on s'est placé d'abord, c'est à dire k algébriquement clos, on dispose d'un théorème fondamental, le *Nullstellensatz*, démontré par Hilbert. Il affirme que, si I est un idéal de $k[X_1,\ldots,X_n]$, l'ensemble des idéaux maximaux de $k[X_1,\ldots,X_n]/I$ est en bijection avec $Z(I)$.

L'étape suivante est donc de généraliser la notion d'espace topologique algébrique à un corps non algébriquement clos.

Dans ce cas, si I est un idéal de $k[X_1,\ldots,X_n]$, on peut définir :

$$\begin{array}{rccl} \phi : & Z(I) & \longrightarrow & \mathrm{Max}(k[X_1,\ldots,X_n]/I) \\ & x & \longmapsto & m_x = \ker\left(\begin{array}{rccl} \psi_x : & k[X_1,\ldots,X_n]/I & \longrightarrow & k \\ & & x & \longmapsto & P(x) \end{array} \right) \end{array}$$

où si A est un anneau, $\mathrm{Max}(A)$ désigne l'ensemble des idéaux maximaux de A. Là encore, on peut munir $\mathrm{Max}(A)$ de la topologie de Zariski dont les fermés sont les $V(J) = \{\mathfrak{m} \in \mathrm{Max}(A) : J \subset \mathfrak{m}\}$, quand J est un idéal de A.

On montre que ϕ est une injection continue de $Z(I)$ dans $\mathrm{Max}(k[X_1,\ldots,X_n]/I)$ pour cette topologie. Ainsi, on étend la notion d'espace topologique algébrique affine : c'est un espace topologique homéomorphe à $\mathrm{Max}(k[X_1,\ldots,X_n]/I)$, muni de la topologie de Zariski. Le passage aux espaces topologiques généraux se fait de la même manière que précédemment.

On peut alors introduire la notion d'extension résiduelle, par analogie avec la construction faite au chapitre 3, section 2.

On note $A = k[X_1,\ldots,X_n]/I$.

- Si $\mathfrak{m}$ est un idéal maximal de la forme $\mathfrak{m}_x$, $A/\mathfrak{m} \simeq k$.
- Si $\mathfrak{m}$ est un idéal maximal quelconque, on a une injection naturelle $j : k \hookrightarrow A$ et une surjection canonique $\pi_{\mathfrak{m}}$ de A dans $A/\mathfrak{m}$. $j \circ \pi_{\mathfrak{m}}$ est un morphisme injectif de k dans $A/\mathfrak{m}$. Donc $A/\mathfrak{m}$ est une extension finie de k. $k(\mathfrak{m}) = A/\mathfrak{m}$ est appelé *corps résiduel* de $\mathfrak{m}$ et on note $\deg(\mathfrak{m}) = [k(\mathfrak{m}) : k]$. Il est courant de noter les idéaux maximaux x.

Pour aboutir finalement à la notion de variété algébrique affine, il faut munir $Z(I)$ non seulement de sa topologie de Zariski, mais aussi de l'anneau $k[X_1,\ldots,X_n]/\sqrt{I}$ ($\sqrt{I} := \{P \in k[X_1,\ldots,X_n] : \exists n \in N^*, P^n \in I\}$ désignant la racine de l'idéal I).

7.1.2 Schéma

Pour définir un *schéma affine*, on remplace dans la définition d'une variété algébrique affine le couple $(Z(I), k[X_1,\ldots,X_n]/\sqrt{I})$ où $Z(I)$ est muni de sa topologie de Zariski par le couple $(\mathrm{Spec}(A), A)$ où A est un anneau et $\mathrm{Spec}(A)$ est muni de la topologie de Zariski dont les fermés dont les $V(I) = \{\mathfrak{p} \in \mathrm{Spec}(A) : I \subset \mathfrak{p}\}$ quand I est un idéal de A.

Un cas intéressant est celui où $A = \mathcal{O}_K$, K corps de nombres. Quel que soit le corps k considéré, $\mathcal{O}_K$ n'est pas une k-algèbre, ce qui empêche le schéma affine associé à A d'être une variété algébrique affine. C'est pourquoi la notion de schéma est nécessaire pour avoir un point de vue géométrique sur les corps de nombres.

Pour un schéma affine $X = \mathrm{Spec}(A)$, le *corps résiduel* de $x \in X$ est $k(x) = \mathrm{Frac}(A/\mathfrak{p})$ qui est une extension de $\mathrm{Frac}(A)$.

Le *point générique* d'un schéma affine est $\{0\}$: on l'appelle ainsi puisque son corps résiduel est le corps de base sur lequel on travaille, à savoir $K = \mathrm{Frac}(A)$.

7.2 Théorème de Chebotarev pour les schémas de type fini sur $\mathbb{Z}$

7.2.1 Présentation du théorème

On suit l'article de Serre (cf [5]).

On prend A un anneau intègre. On suppose que A est une $\mathbb{Z}$-algèbre de type fini. On introduit le schéma affine $X = \mathrm{Spec}(A)$. On note $E := \mathrm{Frac}(A)$ le corps générique.

On constate que $x \in X$ est un *point fermé* pour la topologie de Zariski si son corps résiduel $k(x)$ est fini. En effet, les points fermés sont les idéaux maximaux $\mathfrak{m}$ de A qui est une $\mathbb{Z}$-algèbre de type fini, donc $A/\mathfrak{m}$ est une extension finie d'un $\mathbb{Z}/p\mathbb{Z}$, p premier.

On note $\overline{X}$ l'ensemble des points fermés - ou atomisation - de X et on note $N(x) = \mathrm{Card}(k(x))$ la norme de x. De même que dans le cas des corps de nombres, cela a un sens de définir la fonction zêta :

$$\zeta(X,s) = \prod_{x\in\overline{X}} \frac{1}{1-N(x)^{-s}}$$

Ce produit eulérien converge absolument pour s tel que $\mathrm{Re}(s) > \dim X$.

Par exemple, si $A = \mathbb{Z}[X_1,\dots,X_n]$, les points fermés de A sont les idéaux maximaux de $\mathbb{Z}[X_1,\dots,X_n]$ qui est de dimension n. On peut alors montrer que $\zeta(X,s) = \prod_{p\in\mathrm{Spec}(\mathbb{Z})} \frac{1}{1-p^{n-s}} = \zeta(s-n)$ où ζ est la fonction zêta de Riemann. Un autre exemple est celui de $A = \mathcal{O}_K$ où K est un corps de nombres. On retrouve alors $\zeta(X,\cdot) = \zeta_K$.

Revenons au cas général. De même que dans le corollaire 6.1.12, on montre que $\zeta(X,\cdot)$ admet un prolongement méromorphe à $\left\{\mathrm{Re}(s) > \dim X - \frac{1}{2}\right\}$.

Si X est supposé irréductible, on peut préciser ses pôles en distinguant deux cas :

- si E est de caractéristique nulle, le seul pôle de $\zeta(X,\cdot)$ dans $\left\{\mathrm{Re}(s) > \dim X - \frac{1}{2}\right\}$ est $\dim X$ et c'est un pôle simple.
- sinon, E est de caractéristique $p > 0$, en posant $q := \max\left\{p^n \mid n \in \mathbb{N}, \mathbb{F}_{p^n} \subset E\right\}$, les seuls pôles de $\zeta(X,\cdot)$ dans $\left\{\mathrm{Re}(s) > \dim X - \frac{1}{2}\right\}$ sont les $\dim X + \frac{2\pi i n}{\log(q)}$ quand $n \in \mathbb{Z}$.

Par conséquent, $\zeta(X,\cdot)$ admet un pôle en $\dim X$.

Soit G un groupe fini. Une action de G sur le schéma affine $X = \mathrm{Spec}(A)$ doit respecter la structure de schéma de X. Pour cela, il faut avoir un morphisme de G dans $\mathfrak{S}_C(X)$ (ensemble des permutations continues de X), mais aussi un morphisme de G dans $\mathrm{Aut}(A)$. La donnée de ce second morphisme donne accès au premier. Il suffit donc d'agir par automorphismes sur A pour obtenir une action de groupe convenable sur X. Dans ce cas, le quotient $Y = X/G$ (dans la catégorie des schémas) est en fait $\mathrm{Spec}(A^G)$ où A^G est l'ensemble des invariants de A sous l'action de G.

Soit j^* le morphisme d'anneaux d'inclusion de A^G dans A. Il fournit un morphisme de schémas j de X dans Y (cf section précédente, paragraphe 3), qui n'est autre que $\mathfrak{p} \to \mathfrak{p}\cap A^G$. Si $x \in \overline{X}$, alors $y = j(x)$ est aussi un point fermé dans Y. En effet, le corps résiduel de y s'injecte dans $k(x)$. $k(x)/k(y)$ est donc une extension finie de corps finis donc elle est

galoisienne. De plus, on dispose d'une surjection naturelle du groupe de décomposition de x, défini par $D(x) := \{g \in G \mid g \cdot x = x\}$ sur $\mathrm{Gal}(k(x)/k(y))$. Le noyau de ce morphisme est noté $I(x)$ et est appelé *groupe d'inertie* de x. Le cas favorable est là encore celui où $I(x)$ est trivial, ce qui correspondait dans le cas des corps de nombres aux idéaux non ramifiés.

Une conséquence importante de ce raisonnement est qu'on a un générateur canonique Frob_x de $D(x)/I(x)$ qui est l'image réciproque du morphisme de Frobenius de $\mathrm{Gal}(k(x)/k(y))$.

Le théorème de Chebotarev s'énonce donc ainsi. On définit la densité de Dirichlet de la même manière que précédemment en remplaçant 1 par la dimension du schéma considéré.

Théorème 7.2.1

Soit X un schéma irréductible tel que G agit fidèlement sur le corps résiduel du point générique de X. Soit $Y = X/G$, et $R \subset G$ un ensemble stable par conjugaison. On suppose que $\forall x \in \overline{X}, I(x) = \{\mathrm{id}\}$, de sorte que $\mathrm{Frob}_x \in G$. L'ensemble des éléments y de $\overline{Y}$ tels que $\mathrm{Frob}_y := \{\mathrm{Frob}_x \mid j(x) = y\} \subset R$ a pour densité de Dirichlet $\dfrac{|R|}{|G|}$.

Quelques mots sur la démonstration :

Elle repose en partie sur l'étude des fonctions L. Si χ est un caractère de G, et si $y \in \overline{Y}$ tel que $y = j(x)$, $\chi(y^n)$ est défini comme étant la valeur moyenne de χ sur toutes les puissances n-ièmes (distinctes) de l'élément de Frobenius Frob_x.

On définit alors $L(X, \chi, \cdot)$ comme la fonction vérifiant :

$$\log L(X, \chi, s) = \sum_{y \in \overline{Y}} \sum_{n=1}^{+\infty} \frac{\chi(y^n) N(y)^{-ns}}{n}$$

Comme dans la démonstration du théorème de Chebotarev pour les corps de nombres, il est crucial d'étudier les prolongements méromorphes de ces fonctions L.

Il s'avère qu'elles peuvent être prolongées en des fonctions méromorphes sur $\left\{\mathrm{Re}(s) > \dim X - \frac{1}{2}\right\}$.

Pour le montrer, Serre utilise un procédé de réduction au cas $\dim X = 1$ qui correspond donc au cas des courbes, analogue à celui des corps de nombres comme on le verra dans la section 2.

Sous certaines conditions, on a en effet, $L(X, \chi, s) = H(s) \times L(X', \chi, s-1)$ où X et X' sont deux schémas, et H est holomorphe et non nulle sur $\left\{\mathrm{Re}(s) > \dim X - \frac{1}{2}\right\}$. Les hypothèses autorisent qu'on prenne X' de dimension $\dim X - 1$.

7.2.2 Dictionnaire courbes - corps de nombres

Une courbe sur un corps k est ici un schéma affine $X = \mathrm{Spec}(A)$ de dimension 1, où A est une k-algèbre de type fini.

Dans le paragraphe précédent, le cas $\dim X = 1$ contient celui des anneaux d'entiers de corps de nombres et celui des courbes sur un corps fini. Le point de vue unifié des schémas se particularise comme dans le tableau qui suit.

Corps de nombres	**Courbe intègre sur un corps fini**
$\mathrm{Spec}(\mathscr{O}_K)$	X
K	$\mathbb{F}_q(X) = \mathrm{Frac}(A)$ où $\mathrm{Spec}(A)$ est un ouvert non vide de X
$\mathrm{Spec}(\mathscr{O}_L) \to \mathrm{Spec}(\mathscr{O}_K)$	π revêtement de X' dans X génériquement étale
L/K	$\mathbb{F}_q(X')/\mathbb{F}_q(X)$
$\mathfrak{p} \in \mathrm{Spec}(\mathscr{O}_K) \setminus \{0\}$	$x \in \overline{X}$
$\mathrm{Gal}(L/K)$	$\mathrm{Aut}_X(X')$
$D(\mathfrak{P}) \simeq \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$	$D(x') \simeq \mathrm{Gal}(k(x')/k(x))$

Conclusion

Ce mémoire a été l'occasion d'explorer des outils classiques de la théorie des nombres pour démontrer un théorème important et de formulation relativement accessible. Chebotarev ne l'avait pas démontré comme nous l'avons fait ici, sa preuve était bien plus calculatoire et a inspiré de nombreuses versions « effectives » du théorème qui cherche à donner une majoration ou un équivalent explicite du nombre d'idéaux premiers de norme inférieure à n et de relèvement de Frobenius σ. Mais l'utilisation de la théorie du corps de classe permet une compréhension plus profonde des arguments. Nous avons cependant ici évité la difficulté majeure que constituait la preuve de la loi de réciprocité d'Artin, principe dont la formulation est aussi simple que sa justification est complexe et longue, étant l'un des objets principaux de toute la théorie du corps de classe.

La généralisation de la théorie du corps de classe à une extension non abélienne de corps de nombres reste une gageure : c'est l'un des objectifs principaux du programme de Langlands, sur lequel l'équipe qui m'a accueilli à Paris 13 travaille. Pour le théorème de Chebotarev cependant, il existe une version non abélienne qui se déduit du cas abélien.

Je tiens pour finir à remercier chaleureusement mon maître de stage, Cédric Pépin, qui a su répondre à mes questions par ses explications édifiantes et m'initier au monde fascinant de la théorie des nombres, ainsi que les membres du LAGA avec lesquels j'ai pu discuter.

Bibliographie

[1] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[2] Frédéric Hélein. Fonctions holomorphes. Consultable sur `http://webusers.imj-prg.fr/~frederic.helein/cours/holo.pdf`.

[3] J.S. Milne. Class field theory (v4.02), 2013. Consultable sur www.jmilne.org/math/.

[4] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, 1967.

[5] Jean Pierre Serre. Zeta and l functions. In O.F.G. Schilling, editor, *Arithmetical Algebraic Geometry*, pages 82–92. Purdue University, Harper and Row, 1965.