Christian Maire

THÉORIE DES NOMBRES

Christian Maire
E-mail : christian.maire@univ-fcomte.fr
Url : http://members.femto-st.fr/christian-maire/fr
Institut FEMTO-ST, Université Bourgogne Franche-Comté et CNRS - 15B Avenue des Montboucons - 25030 Besançon.

THÉORIE DES NOMBRES

Christian Maire

TABLE DES MATIÈRES

Quelques conventions

Les anneaux considérés sont commutatifs et unitaires.

Si A désigne un anneau, on notera par $A^\times$ les éléments inversibles de cet anneau.

Si A désigne un anneau principal et M un A module libre de type fini, on notera par $\mathrm{Rang}_A(\mathrm{M})$ le rang de M sur A.

Les extensions de corps sont supposées séparables.

Si K est un corps, on notera par $\overline{\mathrm{K}}$ une clôture algébrique de K.

Si K désigne un corps et $x \in \overline{\mathrm{K}}$, on notera par $\mathrm{Irr}(x, \mathrm{K})$ le polynôme irréductible (unitaire) de x sur K.

CHAPITRE 1

ANNEAUX D'ENTIERS

1.1. Eléments entiers

Définition 1.1.1. — Soient $A \subset B$ deux anneaux. Un élément $b \in B$ est dit entier sur A s'il est racine d'un polynôme unitaire à coefficients dans A : il existe $a_0, \cdots, a_{n-1} \in A$ tels que

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

L'anneau B est entier sur A si tout élément de B est entier sur A.

Exemple 1.1.2. — L'élément $\sqrt{2}$ est entier sur $\mathbb{Z}$, mais $1/2$ ne l'est pas.

Exemple 1.1.3. — Tout élément de A est entier sur A. Ainsi A est entier sur lui-même.

Proposition 1.1.4. — *Les assertions suivantes sont équivalentes :*

(i) L'élément b est entier sur A.

(ii) L'anneau $A[b]$ est un A-module de type fini sur A.

(iii) Il existe un sous-anneau M de B contenant A et b, de type fini sur A (vu comme A-module).

Démonstration. — (i)⇒ (ii). Soit b entier sur A : il existe $a_0, a_1, \ldots, a_{n-1} \in A$ tels que

$$b^n = -a_0 - a_1 b - \cdots - a_{n-1}b^{n-1}.$$

Soit $M = A + Ab + \ldots + Ab^{n-1}$ le A-module engendré par $1, b, \ldots, b^{n-1}$ (qui est évidemment de type fini). L'élément b^n appartient à M. En utilisant la formule

$$b^{n+i} = -a_0 b^i - a_1 b^{i+1} - \cdots - a_{n-1}b^{n+i-1}$$

on montre, par récurrence, que $b^k \in M$ pour tout k. Comme $A[b]$ est engendré par b^k, $k \geqslant 0$, on en déduit que $A[b] = M$ ce qui donne (ii).

(ii) $\Rightarrow$ (iii). Il suffit de prendre $M = A[b]$.

(iii) $\Rightarrow$ (i). Soit M un module (non-nul) vérifiant (iii) : il possède un système fini de générateurs $m_1, \ldots, m_n \in M$. Comme $bM \subseteq M$, il existe $a_{ij} \in A$ tels que

$$\begin{array}{rcl} bm_1 & = & a_{11}m_1 + a_{12}m_2 + \cdots + a_{1n}m_n \\ bm_2 & = & a_{21}m_1 + a_{22}m_2 + \cdots + a_{2n}m_n \\ \ldots & & \ldots \\ bm_n & = & a_{n1}m_1 + a_{n2}m_2 + \cdots + a_{nn}m_n \end{array}$$

Donc $(m_1, \ldots, m_n)$ peut être vu comme une solution non-triviale du système linéaire

$$\left\{ \begin{array}{rcl} (a_{11} - b)X_1 + a_{12}X_2 + \ldots a_{1n}X_n & = & 0 \\ a_{21}X_1 + (a_{22} - b)X_2 + \ldots a_{2n}X_n & = & 0 \\ & \ldots & \\ a_{n1}X_1 + a_{n2}X_2 + \ldots (a_{nn} - b)X_n & = & 0 \end{array} \right.$$

Soit δ le déterminant de la matrice

$$\begin{pmatrix} a_{11} - b & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} - b \end{pmatrix}.$$

Les formules de Cramer indiquent alors que pour $i = 1, \cdots, n$, on a $\delta \cdot m_i = 0$. Ainsi, comme $1 \in A \subset M$, on écrit $1 = \sum_i a_i m_i \in M$, $a_i \in A$ pour en déduire :

$$\delta = \sum_i a_i \delta m_i = 0.$$

En développant δ, on obtient une équation de la forme $f(b) = 0$, où f est un polynôme unitaire de degré n à coefficients dans A. Ainsi b est entier sur A. □

Proposition 1.1.5. — *Soient deux anneaux $A \subset B$.*

(i) Les éléments $b_1, \ldots, b_n \in B$ sont entiers sur A si et seulement si l'anneau $A[b_1, \ldots, b_n]$ est un A-module de type fini.

(ii) L'ensemble des éléments b de B entiers sur A est un sous-anneau de B contenant A.
(iii) Soient trois anneaux $A \subset B \subset C$. Alors C est entier sur A si, et seulement si, C est entier sur B et B est entier sur A.

Démonstration. — (i) Si $A[b_1, \ldots, b_n]$ est un A-module de type fini, alors en notant que $A[b_i] \subset A[b_1, \ldots, b_n]$, on a immédiatement que b_i est entier sur A (grâce à la proposition 1.1.4).
Réciproquement. Si $n = 1$, c'est le point (ii) de la proposition 1.1.4. Supposons $n > 1$. Par récurrence, $A' = A[b_1, \ldots, b_{n-1}]$ est un A-module de type fini. L'élément b_n est entier sur A donc sur $A' = A[b_1, \cdots, b_{n-1}]$. Ainsi, $A'[b_n] = A[b_1, \ldots, b_n]$ est un A'-module de type fini et ainsi $A'[b_n]$ est un A-module de type fini.

(ii) Si x et $y \in B$ sont entiers sur A alors d'après le point (i) le A-module $A[x, y]$ est de type fini. Ainsi d'après la proposition 1.1.4 les éléments xy et $x \pm y$ sont entiers sur A.

(iii) Un sens est évident. Montrons l'autre sens. Soit $x \in C$. Comme x est entier sur B, on a

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0,$$

avec $b_i \in B$. Posons $B_1 = A[b_0, b_1, \ldots, b_{n-1}]$ et $M = B_1[x]$. Alors M est de type fini sur B_1 et B_1 est de type fini sur A car $b_0, \ldots, b_{n-1}$ sont entiers sur A (c'est le point (i)). Ainsi le module M qui contient x et A, est de type fini sur A : d'après le théorème 1.1.4, l'élément x est entier sur A. □

Corollaire 1.1.6. — *Soit* K *un corps et soit B un anneau intègre et entier sur* K. *Alors B est un corps.*

Démonstration. — Il suffit de montrer que tout élément non nul $b \in B$ est inversible. Comme b est entier sur K, il existe un polynôme non-nul $f(X) \in \mathrm{K}[X]$ tel que $f(b) = 0$: l'élément b est algébrique sur K et l'anneau $\mathrm{K}[b]$ est alors isomorphe à $\mathrm{K}[X]/(\mathrm{Irr}(b, \mathrm{K}))$ qui est un corps, où ici $\mathrm{Irr}(b, \mathrm{K})$ est le polynôme irréductible de b sur K. Ainsi $b^{-1} \in \mathrm{K}[b] \subset B$. □

Définition 1.1.7. — Soient deux anneaux $A \subset B$. On note

$$\overline{A} = \{b \in B,\ b \text{ entier sur } A\}$$

la fermeture de A dans B. On dit que A est intégralement clos dans B si $\overline{A} = A$.

Exemple 1.1.8. — Soit A un anneau factoriel et soit $\mathrm{K} = \mathrm{Frac}(A)$ son corps des fractions. Alors A est intégralement clos dans K.

Démonstration. — En effet, soit un élément $x \in \mathrm{K}$ entier sur A. L'élément x s'écrit $x = s/t \in \mathrm{K}$, avec s et $t \neq 0$ dans A premiers entre eux. Il existe $a_0, \ldots, a_{n-1} \in A$ tels que

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

Ainsi, on obtient $s^n = t\alpha$, avec $\alpha = -(a_0 t^{n-1} + \cdots + a_{n-1})$. On en déduit ainsi que $t \in A^\times$ et donc que $x \in A$. □

Définition 1.1.9. — Soit A un anneau intègre et $\mathrm{K} = \mathrm{Frac}(A)$ son corps des fractions. L'anneau A est dit intégralement clos si A est intégralement clos dans K.

Exemple 1.1.10. — Un anneau factoriel est intégralement clos.

Définition 1.1.11. — Soit A un anneau intègre et $\mathrm{K} = \mathrm{Frac}(A)$ son corps des fractions. La fermeture intégrale de A dans K est appelée clôture intégrale de A.

Exemple 1.1.12. — Soit A un anneau intègre et B sa clôture intégrale. Alors B est intégralement clos.

Démonstration. — On commence par remarquer que K est le corps des fractions de B. Soit donc $x \in \mathrm{K}$, avec x entier sur B. Alors comme B est entier sur A, par transitivité (cf. proposition 1.1.5), x est entier sur A. Ainsi, $x \in B$. □

Proposition 1.1.13. — *Soit A un anneau intègre et soit $\mathrm{K} = \mathrm{Frac}(A)$ le corps des fractions de A. On suppose A intégralement clos. Soit L/K une extension finie de corps. Soit B la fermeture intégrale de A dans L. Soit $x \in \mathrm{L}$. Alors $x \in B$ si et seulement si le polynôme irréductible $\mathrm{Irr}(x, \mathrm{K})$ de x sur K est à coefficients dans A.*

Démonstration. — On rappelle que

$$\mathrm{Irr}(x, \mathrm{K}) = \prod_i (X - x_i) \in \mathrm{K}[X],$$

où les éléments x_i sont les conjugués de x (dans une clôture algébrique de K fixée).
Si $\mathrm{Irr}(x, \mathrm{K})$ est à coefficients dans A, alors x qui est racine de $\mathrm{Irr}(x, \mathrm{K})$, est entier sur A.
Réciproquement. Supposons $x \in \mathrm{L}$ entier sur A. Alors x est racine d'un polynôme unitaire $P \in A[X]$. Le polynôme P est divisible par $\mathrm{Irr}(x, \mathrm{K})$. Ainsi les conjugués x_i de x sont racines de P et sont donc entiers sur A. Les coefficients de $\mathrm{Irr}(x, \mathrm{K})$ s'exprimant en fonction des x_i, le polynôme $\mathrm{Irr}(x, \mathrm{K})$ voit ses coefficients dans K et entiers sur A. Comme A est supposé intégralement clos, on en déduit que les coefficients de $\mathrm{Irr}(x, \mathrm{K})$ sont donc dans A. □

Remarque 1.1.14. — Soit A intègre et soit $\mathrm{K} = \mathrm{Frac}(A)$ le corps des fractions de A. Soit L/K une extension algébrique de corps et soit B la fermeture de A dans L.
Soit $x \in \mathrm{L}$. Il existe $a_n, \cdots, a_0 \in A$ tels que

$$a_n x^n + \cdots + a_0 = 0.$$

Ainsi

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_n^{n-1} a_0 = 0,$$

et par conséquent $a_n x \in B$. L'élément x s'écrit ainsi $x = b/a$, avec $b \in B$ et $a \in A$. Ainsi, L est le corps des fractions de B.

1.2. Discriminant

1.2.1. Traces et normes. — On rappelle que les extensions de corps sont supposées séparables (ce qui est toujours le cas par exemple si la caractéristique est nulle).
Soit L/K une extension finie de corps et soit $x \in \mathrm{L}$. Soit l'endomorphisme du K-espace vectoriel L :

$$\begin{array}{rccc} \mathrm{m}_x : & \mathrm{L} & \to & \mathrm{L} \\ & y & \mapsto & xy \end{array}$$

Définition 1.2.1. — Soit $x \in \mathrm{L}$.
On définit la trace $\mathrm{Tr}_{\mathrm{L/K}}(x)$ de x dans L/K comme étant la trace de l'endomorphisme m_x.
On définit la norme $\mathrm{N}_{\mathrm{L/K}}(x)$ de x dans L/K comme étant le déterminant de l'endomorphsime m_x.

Ainsi $x \mapsto \mathrm{Tr}_{\mathrm{L/K}}(x)$ est K-linéaire et $x \mapsto \mathrm{N}_{\mathrm{L/K}}(x)$ est multiplicatif :

$$\mathrm{N}_{\mathrm{L/K}}(xx') = \mathrm{N}_{\mathrm{L/K}}(x)\mathrm{N}_{\mathrm{L/K}}(x')$$

et si $\lambda \in \mathrm{K}$,

$$\mathrm{N}_{\mathrm{L/K}}(\lambda x) = \lambda^n \mathrm{N}_{\mathrm{L/K}}(x),$$

où ici $n = [\mathrm{L} : \mathrm{K}]$.
Les éléments $\mathrm{Tr}_{\mathrm{L/K}}(x)$ et $\mathrm{N}_{\mathrm{L/K}}(x)$ sont des invariants de L/K qui se trouvent K.

Proposition 1.2.2. — *Soit* L/K *une extension de degré* n. *Notons par* σ_i, $i = 1, \cdots, n$, *les* K*-plongements de* L *dans une clôture algébrique* $\overline{\mathrm{L}}$ *de* L. *Soit* $x \in \mathrm{L}$. *On pose* $d = [\mathrm{K}(x) : \mathrm{K}]$. *Soient* $x_1, \cdots, x_d$ *les conjugués de* x *dans* $\overline{\mathrm{L}}$. *Alors*

(i) $\mathrm{Tr}_{\mathrm{K}(x)/\mathrm{K}}(x) = x_1 + \cdots + x_d$, $\mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}(x) = x_1 \cdots x_d$;

(ii) $\mathrm{Tr}_{\mathrm{L/K}}(x) = \dfrac{n}{d}\mathrm{Tr}_{\mathrm{K}(x)/\mathrm{K}}(x) = \displaystyle\sum_{i=1}^{n} \sigma_i(x)$ *et*

$$\mathrm{N}_{\mathrm{L/K}}(x) = \left(\mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}\right)^{n/d} = \prod_{i=1}^{n} \sigma_i(x).$$

Démonstration. — C'est immédiat. Dans la situation (i), on trouve que le polynôme caractéristique de m_x est exactement $\mathrm{Irr}(x, \mathrm{K})$.
Dans la situation (ii), le polynôme caractéristique de m_x est $\mathrm{Irr}(x, \mathrm{K})^{n/d}$. □

Corollaire 1.2.3. — *Soit* A *un anneau intégralement clos ;* $\mathrm{K} = \mathrm{Frac}(A)$. *Soit* L/K *une extension de degré fini et soit* B *la fermeture intégrale de* A *dans* L. *Soit* $x \in B$. *Alors* $\mathrm{Tr}_{\mathrm{L/K}}(x) \in A$ *et de même,* $\mathrm{N}_{\mathrm{L/K}}(x) \in A$.

Démonstration. — Cela peut être vu comme une conséquence de la proposition 1.1.13. Mais montrons le directement. D'après la proposition

1.2.2, $\mathrm{Tr}_{\mathrm{L/K}}(x) \in \mathrm{K}$. D'autre part, comme $x \in B$, les conjugués de x sont également entiers sur A. Ainsi, $\mathrm{Tr}_{\mathrm{L/K}}(x)$ est un élément de K, entier sur A. Comme A est intégralement clos, $\mathrm{Tr}_{\mathrm{L/K}}(x) \in A$.
Le raisonnement est identique pour $\mathrm{N}_{\mathrm{L/K}}(x)$.

□

Terminons par une propriété bien utile.

***Proposition 1.2.4* (Transitivité).** — *Soit la tour d'extensions* $\mathrm{K} \subset l \subset \mathrm{M}$. *Soit* $x \in \mathrm{M}$. *Alors*

$$\mathrm{Tr}_{\mathrm{M/K}}(\mathrm{Tr}_{\mathrm{M/L}}(x)) = \mathrm{Tr}_{\mathrm{L/K}}(x),$$

et

$$\mathrm{N}_{\mathrm{M/K}}(\mathrm{N}_{\mathrm{M/L}}(x)) = \mathrm{N}_{\mathrm{L/K}}(x).$$

Démonstration. — La preuve est immédiate. C'est une conséquence du théorème de prolongement des isomorphismes. □

1.2.2. Discriminant et forme trace. —

Définition 1.2.5. — Soit L/K une extension de corps de degré n. Soit $\{x_1, \ldots, x_n\}$ une famille de n éléments de L. Le discriminant $\mathrm{d}(x_1, \cdots, x_n)$ de la famille $\{x_1, \ldots, x_n\}$ est défini comme suit :

$$\mathrm{d}(x_1, \ldots, x_n) = \det(\left(\mathrm{Tr}_{\mathrm{L/K}}(x_i x_j)\right)_{i,j}).$$

Proposition 1.2.6. — *Soit* $\sigma_1, \ldots, \sigma_n$ *les* K*-plongements de* L *dans* $\overline{\mathrm{K}}$. *Alors* $\mathrm{d}(x_1, \ldots, x_n) = (\det((\sigma_i(x_j))_{i,j}))^2$. *De plus si* $\{x_1, \ldots, x_n\}$ *est une* K*-base de* L, *alors* $\mathrm{d}(x_1, \ldots, x_n) \neq 0$.

Démonstration. — (i) C'est immédiat.

$$\begin{aligned}
\mathrm{d}(x_1, \cdots, x_n) &= \det\left((\mathrm{Tr}_{\mathrm{L/K}}(x_i x_j))_{i,j}\right) \\
&= \det\left((\textstyle\sum_k \sigma_k(x_i x_j))_{i,j}\right) \\
&= \det\left((\textstyle\sum_k \sigma_k(x_i)\sigma_k(x_j))_{i,j}\right) \\
&= \det\left((\sigma_k(x_i))_{k,i}(\sigma_k(x_j))_{k,j}\right) \\
&= \left(\det(\sigma_i(x_j))_{i,j}\right)^2
\end{aligned}$$

(ii) Comme l'extension L/K est séparable, d'après le théorème de l'élément primitif, il existe $\theta \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\theta)$.

Si l'on note par $\theta_1, \ldots, \theta_n$ les K-conjugués de θ, il vient

$$\mathrm{d}(1, \cdots, \theta^{n-1}) = \begin{vmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ & \vdots & & \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{vmatrix}^2 = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0,$$

car $\theta_i \neq \theta_j$, l'extension L/K étant séparable.
Soit maintenant $\{x_1, \ldots, x_n\}$ une K-base quelconque de L. Alors,

$$\mathrm{d}(x_1, \ldots, x_n) = \mathrm{d}(1, \ldots, \theta^{n-1}) \det(M)^2,$$

où M est la matrice de passage entre les bases $\{x_1, \ldots, x_n\}$ et $\{1, \ldots, \theta^{n-1}\}$. D'où le résultat. □

Corollaire 1.2.7. — *Soit* L/K *une extension finie (séparable) de degré n. Alors* $\{x_1, \ldots, x_n\}$ *est une* K*-base de* L *si, et seulement si,* $\mathrm{d}(x_1, \ldots, x_n) \neq 0$.

Démonstration. — C'est immédiat. □

Il vient immédiatement le corollaire suivant :

Corollaire 1.2.8. — *La forme bilinéaire (ou encore la forme trace)*

$$\begin{array}{rcl} \mathrm{Tr} : \mathrm{L} \times \mathrm{L} & \to & \mathrm{K} \\ (x, y) & \mapsto & \mathrm{Tr}_{\mathrm{L/K}}(xy) \end{array}$$

est non-dégénérée.

Démonstration. — Dans la base $\{x_1, \ldots, x_n\}$, la matrice de Gram de la forme bilinéaire symétrique $\mathrm{Tr}_{\mathrm{L/K}}$ a pour déterminant $\mathrm{d}(x_1, \ldots, x_n)$ qui est non nul. □

Corollaire 1.2.9. — *Soit A un anneau principal,* $\mathrm{K} = \mathrm{Frac}(A)$. *Soit* L/K *une extension finie de degré n et soit B la fermeture intégrale de A dans* L. *Alors B est un A-module libre de rang n ou encore* $B \simeq A^n$.
Plus précisémment, tout sous-B-module non nul de type fini et contenu dans L *est un A-module libre de rang n.*

Remarque 1.2.10. — Ainsi, tout idéal $\mathfrak{a}$ non nul de B, de type fini (ce qui est immédiat - à venir), est isomorphe, en tant que A-module, à A^n.

Démonstration. — Commençons par le lemme suivant :

Lemme 1.2.11. — *Soit A un anneau intègre et soit $\mathrm{K} = \mathrm{Frac}(A)$. Soit L/K une extension de degré n et soit B la fermeture intégrale de A dans L. Soit $\{x_1, \ldots, x_n\}$ une K-base de L. D'après la remarque 1.1.14, on peut supposer que les éléments x_i sont dans B. Posons $\mathrm{d} = \mathrm{d}(x_1, \ldots, x_n)$. Alors*

$$\mathrm{d}B \subset Ax_1 + \cdots + Ax_n.$$

Démonstration. — Soit $x = \alpha_1 x_1 + \cdots + \alpha_n x_n \in B$, avec $\alpha_i \in \mathrm{K}$. Alors pour $i = 1, \ldots, n$,

$$\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(xx_i) = \sum_{j=1}^{n} \alpha_j \mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(x_j x_i).$$

On a alors le système

$$\begin{pmatrix} \vdots \\ \mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(xx_i) \\ \vdots \end{pmatrix} = \begin{pmatrix} & \cdots & \\ \ldots & \mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(x_j x_i) & \ldots \\ & \cdots & \end{pmatrix} \begin{pmatrix} \vdots \\ \alpha_j \\ \vdots \end{pmatrix}$$

Par les formules de Cramer et grâce au corollaire 1.2.3,

$$\mathrm{d}\alpha_j \in A,$$

et ainsi $\mathrm{d}x \in Ax_1 + \cdots + Ax_n$. □

Fin de la preuve du corollaire 1.2.9. D'après le lemme 1.2.11, B est un A-sous-module de $1/d(Ax_1 + \cdots + Ax_n) \simeq A^n$. L'anneau A étant principal, B est donc libre sur A de rang plus petit que n. Comme B contient une K-base de L, on en déduit que le A-rang de B est exactement n.

Soit $M \neq (0)$ un B-module de type fini contenu dans L. Comme L est un corps, M est sans torsion.

Soit $y_1, \ldots, y_r$ un système de générateurs du B-module M. D'après la remarque 1.1.14, il existe $a \in A$ tel que pour $i = 1, \ldots, r$, les éléments ay_i sont dans B. Ainsi $aM \subset B$. Par conséquent

$$adM \subset dB \subset Ax_1 + \cdots + Ax_n,$$

et ainsi le A-module M est de type fini et de rang au plus n.
Maintenant comme M est non nul, on peut supposer par exemple que y_1 est non nul. Alors $y_1 B \subset M$ et ainsi

$$n = \mathrm{Rang}_A(B) = \mathrm{Rang}_A(y_1 B) \leq \mathrm{Rang}_A(M) \leq n,$$

d'où au final $\mathrm{Rang}_A(M) = n$.

□

1.3. L'anneau des entiers d'un corps de nombres

1.3.1. Le discriminant absolu d'un corps de nombres. —

Définition 1.3.1. — Un corps de nombres K est un corps qui est de degré fini sur $\mathbb{Q}$.
L'anneau des entiers $\mathcal{O}_\mathrm{K}$ de K est la fermeture intégrale de $\mathbb{Z}$ dans K :

$$\mathcal{O}_\mathrm{K} = \{x \in \mathrm{K},\ \mathrm{Irr}(x, \mathbb{Q}) \in \mathbb{Z}[X]\}.$$

Grâce au corollaire 1.2.9, nous avons immédiatement :

Proposition 1.3.2. — *L'anneau des entiers $\mathcal{O}_\mathrm{K}$ de* K *est un $\mathbb{Z}$-module libre de rang $n = [\mathrm{K} : \mathbb{Q}]$.*

Soit donc $\{x_1, \ldots, x_n\}$ une $\mathbb{Z}$-base de l'anneau des entiers $\mathcal{O}_\mathrm{K}$ du corps de nombres K. Posons $\mathrm{d} = \mathrm{d}(x_1, \ldots, x_n)$. La quantité d est un entier car les éléments x_i sont entiers sur $\mathbb{Z}$. Si $\{x'_1, \ldots, x'_n\}$ forme une autre $\mathbb{Z}$-base de $\mathcal{O}_\mathrm{K}$, alors

$$\mathrm{d} = (\det M)^2 \mathrm{d}(x'_1, \ldots, x'_n),$$

où M est la matrice de passage entre ces deux bases (formule du changement de base pour une forme bilinéaire). Or comme $M \in \mathrm{Gl}_n(\mathbb{Z})$, son déterminant vaut ± 1. Ainsi la quantité d *est un invariant de* K.

Définition 1.3.3. — Le discriminant absolu d'un corps de nombres K est l'entier naturel $\mathrm{d} = \mathrm{d}(x_1, \ldots, x_n)$, où $\{x_1, \ldots, x_n\}$ est une $\mathbb{Z}$-base de $\mathcal{O}_\mathrm{K}$. On le note $\mathrm{d}(\mathcal{O}_\mathrm{K})$ ou encore d_K.

Remarque 1.3.4. — Plus généralement. Si $\mathrm{M} \subset \mathrm{K}$ est un $\mathbb{Z}$-module libre de rang n engendré par les éléments $x_1, \ldots, x_n$, on note par $\mathrm{d}(\mathrm{M})$ le discriminant de la famille $\mathrm{d}(x_1, \ldots, x_n)$.

1.3.2. A la recherche d'une $\mathbb{Z}$-base. — Soit $\mathrm{K}/\mathbb{Q}$ une extension de degré n et soit $\{y_1, \ldots, y_n\}$ une famille libre d'éléments de $\mathcal{O}_\mathrm{K}$.
Soit $\mathrm{M} = \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_n$. Alors M est sous-$\mathbb{Z}$-module de $\mathcal{O}_\mathrm{K}$ de même rang donc d'indice fini.
Commençons par la proposition suivante.

Proposition 1.3.5. — *Soit* K *un corps de nombres de degré n sur $\mathbb{Q}$. Soit $\{y_1, \ldots, y_n\}$ une famille libre d'éléments de $\mathcal{O}_\mathrm{K}$. Si $\mathrm{d}(y_1, \ldots, y_n)$ est sans facteur carré, alors $\mathcal{O}_\mathrm{K} = \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_n$.*

Démonstration. — Soit $\{x_1, \ldots, x_n\}$ une $\mathbb{Z}$-base de $\mathcal{O}_\mathrm{K}$. Alors le déterminant de la matrice de passage M, à coefficients dans $\mathbb{Z}$, qui exprime la famille $\{y_1, \ldots, y_n\}$ dans la base $\{x_1, \ldots, x_n\}$, vérifie $\mathrm{d}(\mathrm{M}) = \mathrm{d}(y_1, \ldots, y_n) = (\det M)^2 \mathrm{d}(x_1, \ldots, x_n) = (\det M)^2 \mathrm{d}(\mathcal{O}_\mathrm{K})$. Comme $\mathrm{d}(y_1, \ldots, y_n)$ est sans facteur carré, on a $\det M = \pm 1$. Ainsi $M \in \mathrm{Gl}_n(\mathbb{Z})$ et par conséquent $\{y_1, \ldots, y_n\}$ forme aussi une $\mathbb{Z}$-base de $\mathcal{O}_\mathrm{K}$. □

Exemple 1.3.6. — Soit le corps de nombres $\mathrm{K} = \mathbb{Q}(\theta)$ de degré n sur $\mathbb{Q}$. Posons $P = \mathrm{Irr}(\theta, \mathbb{Q})$. Alors

$$\begin{aligned} \mathrm{d}(1, \theta, \ldots, \theta^{n-1}) &= \textstyle\prod_{i<j}(\theta_i - \theta_j)^2 \\ &= (-1)^{n(n-1)/2} \textstyle\prod_{i \neq j}(\theta_i - \theta_j) \\ &= (-1)^{n(n-1)/2} \textstyle\prod_{i=1}^{n} \prod_{j=1, j\neq i}^{n}(\theta_i - \theta_j) \\ &= (-1)^{n(n-1)/2} \mathrm{N}_{\mathrm{K}/\mathbb{Q}} P'(\theta) \end{aligned}$$

où P' est le polynôme dérivé de P.
Prenons par exemple $P = X^3 + aX + b$. Alors $\mathrm{d}(1, \theta, \theta^2) = -(27b^2 + 4a^3)$. Choisissons $a = -b = -1$. Il vient $\mathrm{d}_\mathrm{K} = -23$ et ainsi pour $\mathrm{K} = \mathbb{Q}(\theta)$, où θ vérifie $\theta^3 - \theta + 1 = 0$, on obtient que $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\theta]$. L'anneau $\mathcal{O}_\mathrm{K}$ est dit monogène.

Que faire lorsque $\mathrm{d}(y_1, \ldots, y_n)$ contient un facteur carré ?
On cherche à comparer $\mathrm{M} = \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_n$ à $\mathcal{O}_\mathrm{K}$. Soit $\{x_1, \ldots, x_n\}$ une $\mathbb{Z}$-base de $\mathcal{O}_\mathrm{K}$. Comme M est un sous-$\mathbb{Z}$-module de $\mathcal{O}_\mathrm{K}$ de rang n, d'après la théorie des modules sur $\mathbb{Z}$, il existe des entiers naturels $d_1, \ldots, d_n$, avec $d_1 | \cdots | d_n$, tels que que $\{d_1x_1, \ldots, d_nx_n\}$ forme une $\mathbb{Z}$-base de M. Les entiers d_i sont les facteurs invariants de M. Alors

$$\mathrm{d}(\mathrm{M}) = \mathrm{d}(y_1, \ldots, y_n) = \mathrm{d}(d_1x_1 \ldots, d_nx_n) = (d_1 \cdots d_n)^2 \mathrm{d}(\mathcal{O}_\mathrm{K}).$$

Ainsi les facteurs invariants apparaîssent dans les facteurs carrés de $\mathrm{d}(y_1, \ldots, y_n)$ et $\mathcal{O}_\mathrm{K} = \mathrm{M}$ si et seulement si $d_1 = \cdots = d_n = 1$, si et seulement si $\det(N) = \pm 1$, où N est la matrice qui exprime la famille $\{y_1, \ldots, y_n\}$ dans la base $\{x_1, \ldots, x_n\}$. A noter que $\det N = \pm d_1 \cdots d_n$.

Soit donc un nombre premier p tel que p^2 divise $\mathrm{d}(y_1, \ldots, y_n)$.

Si $p | d_n$. Alors il existe $y \in \mathcal{O}_\mathrm{K}$, $y \neq 0$, tel que $py \in \mathrm{M}$ et ainsi, il existe $a_i \in \mathbb{Z}$ tels que

$$\frac{a_1x_1 + \cdots + a_ny_n}{p} \in \mathcal{O}_\mathrm{K}.$$

On peut s'assurer que $a_i \in 0, \ldots, p-1$ et, par la relation de Bezout, on peut également s'assurer que le premier entier non nul a_{i_0} de la famille $\{a_0, \ldots, a_n\}$ est égal à 1. Un nombre fini de calculs permet de voir si c'est possible (i.e. si $y \neq 0$).
Si c'est impossible, alors $p \nmid d_n$. Puis on teste le nombre premier suivant dont le carré divise $\mathrm{d}(y_1, \ldots, y_n)$. Etc.
Supposons maintenant que l'on trouve effectivement un élément

$$y = \frac{y_{i_0} + \cdots + a_ny_n}{p} \in \mathcal{O}_\mathrm{K}.$$

Soit alors le sous-$\mathbb{Z}$-module de $\mathcal{O}_\mathrm{K}$

$$\mathrm{M}' = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_{i_0-1} + \mathbb{Z}y + \mathbb{Z}y_{i_0+1} + \cdots + \mathbb{Z}y_n.$$

Alors $\mathrm{M} \subset \mathrm{M}'$ et un calcul de déterminant montre que cet indice est exactement p. Ainsi

$$\mathrm{d}(\mathrm{M}') = \frac{\mathrm{d}(\mathrm{M})}{p^2}.$$

En passant de M à M′, le facteur carré de d(M) a été divisé par p^2. Plus précisément

$$(\mathcal{O}_{\mathrm{K}} : \mathrm{M}') = \frac{(\mathcal{O}_{\mathrm{K}} : \mathrm{M})}{p}.$$

On recommence le raisonnement à partir du nouveau $\mathbb{Z}$-module M′.
Etc.

Exemple 1.3.7. — Soit $\theta \in \mathbb{C}$ vérifiant $\theta^3 = 2$.
Alors $\mathrm{d}(1, \theta, \theta^2) = 2^2 \cdot 3^3$. Seuls les premiers $p = 2$ et $p = 3$ peuvent diviser les facteurs invariants de $\mathbb{Z}[\theta]$.

Traitons le cas $p = 2$. Existe-t-il un entier non nul $y \in \mathcal{O}_{\mathrm{K}}$ de la forme

$$y = \frac{a + b\theta + c\theta^2}{2},$$

avec $a, b, c \in \{0, 1\}$?
Testons par exemple $y = (1 + \theta)/2$. Alors $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(y) = 3/2 \notin \mathbb{Z}$, donc $y \notin \mathcal{O}_{\mathrm{K}}$. En regardant la trace, on élimine aussi $(1+\theta+\theta^2)/2$ et $(1+\theta^2)/2$.
Testons ensuite, $y = (\theta + \theta^2)/2$. Alors

$$\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(y) = \frac{\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\theta)\ \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(1 + \theta)}{8} = 3/4 \notin \mathbb{Z}.$$

En regardant la norme, on élimite également $\theta/2$ et $\theta^2/2$.
On obtient ainsi que 2 ne divise pas les facteurs invariants de $\mathbb{Z}[\theta]$.
On traite de même le cas $p = 3$, pour obtenir finalement que $\mathcal{O}_{\mathrm{K}} = \mathbb{Z}[\sqrt[3]{2}]$.

1.3.3. Le cas des corps quadratiques. — Un corps quadratique K est une extension de degré 2 de $\mathbb{Q}$. Ainsi $\mathrm{K} = \mathbb{Q}(\alpha)$, où α est racine d'un polynôme irréductible $P = X^2 + aX + b \in \mathbb{Q}[X]$.
Alors $\mathrm{K} = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}(\sqrt{d})$, pour un certain entier $d \in \mathbb{Z}$ sans facteur carré ($d \neq 1$).
Clairement $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathrm{K}}$ et $\mathrm{d}(\mathbb{Z}[\sqrt{d}]) = 4d$. L'indice de $\mathbb{Z}[\sqrt{d}]$ dans $\mathcal{O}_{\mathrm{K}}$ est 1 ou 2.
Il nous faut alors tester si les éléments $\dfrac{a + b\sqrt{d}}{2}$, $a, b \in \{0, 1\}$, sont dans $\mathcal{O}_{\mathrm{K}}$.
L'élément $1/2$ est immédiatement exclu. De même, comme $\mathrm{Irr}(\sqrt{d}/2, \mathbb{Q}) = X^2 - d/4 \notin \mathbb{Z}[X]$, l'élément $\sqrt{d}/2 \notin \mathcal{O}_{\mathrm{K}}$.

Il reste donc l'élément $\dfrac{1+\sqrt{d}}{2}$ qui a pour polynôme irréductible sur $\mathbb{Q}$: $\mathrm{Irr}(\theta,\mathbb{Q}) = X^2 - X + (1-d)/4$. Ce polynôme est à coefficients dans $\mathbb{Z}$ si et seulement si, $d \equiv 1 (\mathrm{mod}\ 4)$.

Théorème 1.3.8. — *Soit le corps quadratique* $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ *sans facteur carré* ($d \neq 1$). *Alors*

$$\mathcal{O}_{\mathrm{K}} = \begin{cases} \mathbb{Z}[\sqrt{d}] \ \text{ si } \ d \equiv 2,3 (\mathrm{mod}\ 4) \ \text{ et } \ \mathrm{d_K} = 4d \\ \mathbb{Z}[\dfrac{1+\sqrt{d}}{2}] \ \text{ si } \ d \equiv 1 (\mathrm{mod}\ 4) \ \text{ et } \ \mathrm{d_K} = d \end{cases}$$

Démonstration. — • Supposons $d \equiv 2,3 (\mathrm{mod}\ 4)$. Alors nous venons de voir que l'indice de $\mathbb{Z}[\sqrt{d}]$ dans $\mathcal{O}_{\mathrm{K}}$ n'est pas divisible par 2 d'où l'égalité $\mathcal{O}_{\mathrm{K}} = \mathbb{Z}[\sqrt{d}]$.
• Supposons $d \equiv 1 (\mathrm{mod}\ 4)$. Alors

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \ \subset \ \mathbb{Z}\frac{1+\sqrt{d}}{2} \oplus \mathbb{Z}\sqrt{d}$$

et l'indice entre ces deux modules est exactement 2. Comme ces anneaux sont contenus dans $\mathcal{O}_{\mathrm{K}}$ et que l'indice de $\mathbb{Z}[\sqrt{d}]$ dans $\mathcal{O}_{\mathrm{K}}$ est au plus 2, on conclut que

$$\mathcal{O}_{\mathrm{K}} = \mathbb{Z}\frac{1+\sqrt{d}}{2} \oplus \mathbb{Z}\sqrt{d} = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}].$$

□

1.3.4. Le cas des corps cyclotomiques. — Soit un nombre premier $p > 2$. Posons $\zeta_p = \exp(2i\pi/p)$.
On rappelle que le polynôme $P = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ est irréductible et ses racines dans $\mathbb{C}$ sont les racines primitives p-èmes de l'unité ζ_p^i, $i = 1, \ldots, p-1$.

Théorème 1.3.9. — *Soit* $\mathrm{K} = \mathbb{Q}(\zeta_p)$. *Alors* $\mathcal{O}_{\mathrm{K}} = \mathbb{Z}[\zeta_p]$ *et* $d_{\mathrm{K}} = (-1)^{(p-1)/2} p^{p-2}$. *En particulier,* $\sqrt{(-1)^{(p-1)/2} p} \in \mathrm{K}$.

Démonstration. — Clairement, $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_{\mathrm{K}}$. Il nous faut donc montrer l'inclusion inverse. Posons $z = \zeta_p$.
En s'appuyant sur P, on en déduit que pour $i = 1, \ldots, p-2$,

$$\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(z^i) = -1, \quad \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(1 - z^i) = p$$

puis que

$$\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(1-z) = p.$$

(Noter que $P(X+1)$ est le polynôme irréductible des $1-z^i$.)

Notons que $(1-z)\mathcal{O}_\mathrm{K} \cap \mathbb{Z} = p\mathbb{Z}$. En effet, on a immédiatement, $p\mathbb{Z} \subset (1-z)\mathcal{O}_\mathrm{K} \cap \mathbb{Z}$. Mais comme $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$, alors ou bien $(1-z)\mathcal{O}_\mathrm{K} \cap \mathbb{Z} = \mathbb{Z}$, ou bien $(1-z)\mathcal{O}_\mathrm{K} \cap \mathbb{Z} = p\mathbb{Z}$. Le premier cas est à exclure, sinon il existerait $x \in \mathcal{O}_\mathrm{K}$ tel que $x(1-z) = 1$. En passant à la norme cela impliquerait que $(\mathrm{N}_{\mathrm{K}/\mathbb{Q}}x)p = 1$ ce qui est impossible car $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}x \in \mathbb{Z}$.

Ainsi, pour $x \in \mathcal{O}_\mathrm{K}$, on obtient

$$\begin{array}{rcl} \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}x(1-z) & \in & \left(\sum_i^{p-1} \mathcal{O}_\mathrm{K}(1-z^i)\right) \cap \mathbb{Z} \\ & \in & \mathcal{O}_\mathrm{K}(1-z) \cap \mathbb{Z} = p\mathbb{Z} \end{array}$$

car $(1-z^i) = (1-z)(1+z+\cdots, z^{i-1}) \in (1-z)\mathcal{O}_\mathrm{K}$.

Soit donc $x \in \mathcal{O}_\mathrm{K}$. Il existe $a_0, \ldots, a_{p-2} \in \mathbb{Q}$ tels que $x = a_0 + \cdots, a_{p-2}z^{p-2}$. Alors

$$\begin{array}{rcl} \mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}x(1-z) & = & a_0\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(1-z) + \cdots + a_{p-2}\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}(z^{p-2} - z^{p-1}) \\ & = & a_0 p. \end{array}$$

Comme $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}x(1-z) \in p\mathbb{Z}$, on en déduit que $a_0 \in \mathbb{Z}$.

Posons ensuite $x' = (x-a_0)z^{-1} = a_1 + \cdots + a_{p-2}z^{p-3}$. Alors, comme pour x, en considérant $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}x'(1-z)$, on en déduit que $a_1 \in \mathbb{Z}$. Etc. En conclusion les éléments a_i sont dans $\mathbb{Z}$, c'est à dire que $x \in \mathbb{Z}[\zeta_p]$.

Calculons d_K. Soit $P = \dfrac{X^p-1}{X-1}$. Alors $P'(z) = p(z-1)^{-1}z^{p-1}$ et

$$\mathrm{N}_{\mathrm{K}/\mathbb{Q}}P'(\zeta) = p^{p-2},$$

d'où $\mathrm{d}_\mathrm{K} = (-1)^{(p-1)/2}p^{p-2}$.

Enfin, la proposition 1.2.6 montre que $\mathrm{d}_\mathrm{K} \in \mathrm{K}^2$ et donc $\sqrt{(-1)^{(p-1)/2}p} \in \mathrm{K}$. □

Pour terminer, donnons une base d'entiers pour le sous-corps réel maximal $\mathbb{Q}(\zeta_p)^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ de $\mathbb{Q}(\zeta_p)$.

Lemme 1.3.10. — *Le corps $\mathbb{Q}(\zeta_p)^+$ est la sous-extension de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ fixée par la conjugaison complexe σ.*

Démonstration. — Tout d'abord on a bien que $\mathbb{Q}(\zeta_p)^+ \subset \mathbb{Q}(\zeta_p)^{\langle\sigma\rangle}$.
D'autre part, les conjugués de $\zeta_p + \zeta_p^{-1}$ sont les éléments de la forme $\zeta_p^i + \zeta_p^{-i} = 2\cos(2i\pi/p)$, et on voit qu'ils sont au nombre de $(p-1)/2$, montrant ainsi que $[\mathbb{Q}(\zeta_p)^+ : \mathbb{Q}] = [\mathbb{Q}(\zeta_p)^{\langle\sigma\rangle} : \mathbb{Q}] = (p-1)/2$. Le lemme s'en déduit. □

Au passage, on remarque que la famille $\{1, \zeta_p + \zeta_p^{-1}, \cdots, \zeta_p^n + \zeta_p^{-n}\}$ où $n = (p-3)/2$, forme une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta_p)^+$. Nous avons alors

Corollaire 1.3.11. — *Le corps $\mathbb{Q}(\zeta_p)^+$ a pour anneau des entiers $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.*

Démonstration. — Soit $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\zeta_p)^+$. Clairement, $\mathbb{Z}[\zeta_p + \zeta_p^{-1}] \subset \mathcal{O}$.
Partons alors d'un élément $z \in \mathcal{O}$. Alors z est un entier de $\mathbb{Q}(\zeta_p)$, et ainsi il existe $a_1, \cdots, a_{p-1} \in \mathbb{Z}$ tel que $z = a_1\zeta_p + a_1\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1}$: ici, par commodité, on prend la famille $\{\zeta_p \cdots, \zeta_p^{p-1}\}$ comme $\mathbb{Z}$-base de l'anneau des entiers de $\mathbb{Q}(\zeta_p)$. On fait ensuite agir la conjugaison complexe sur cette relation pour obtenir la relation

$$a_1\zeta_p + a_1\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} = a_1\zeta_p^{-1} + a_1\zeta_p^{-2} + \cdots + a_{p-1}\zeta_p^{-p+1}$$

ce qui implique $a_i = a_{p-i}$, pour $i = 1, \cdots, (p-1)/2$. Et ainsi, en regroupant les termes de façon adéquate, on obtient que $z = \sum_{i=0}^{(p-1)/2} a_i(\zeta_p^i + \zeta_p^{-i})$.
Il reste alors à observer que $\zeta_p^i + \zeta_p^{-i} \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Cela peut se faire par récurrence, à partir du calcul de $(\zeta_p + \zeta_p^{-1})^i$. □

CHAPITRE 2

ANNEAUX DE DEDEKIND

2.1. Rappels sur les anneaux noetheriens

Soit A un anneau commutatif unitaire.

Définition 2.1.1. — Un A-module M est dit noetherien si tout sous-A-module de M est de type fini.
L'anneau A est dit noethérien si tout idéal $\mathfrak{a}$ de A est de type fini.

Exemple 2.1.2. — Un anneau principal est noetherien.

Proposition 2.1.3. — *Les assertions suivantes sont équivalentes :*
(i) A est noethérien ;
(ii) toute suite croissante d'idéaux de A

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

est stationnaire, i.e. il existe n tel que

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots .$$

Démonstration. — *ii)* $\Rightarrow$ *i)*. Soit a_1 un élément non nul de $\mathfrak{a}$ et soit $\mathfrak{a}_1 = (a_1)$ l'idéal principal engendré par a_1. Si $\mathfrak{a}_1 = \mathfrak{a}$, l'idéal $\mathfrak{a}$ est de type fini. Sinon, il existe $a_2 \in \mathfrak{a} \setminus \mathfrak{a}_1$ et on pose $\mathfrak{a}_2 = (a_1, a_2)$. Si $\mathfrak{a}_2 = \mathfrak{a}$, l'idéal $\mathfrak{a}$ est de type fini. Sinon, on choisit $a_3 \in \mathfrak{a} \setminus \mathfrak{a}_2$ etc. On obtient, ainsi, une suite d'idéaux de type fini strictement croissante :

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subseteq \cdots .$$

Par hypothèse cette suite est stationnaire, ce qui signifie qu'il existe n tel que $\mathfrak{a}_n = \mathfrak{a}$, et $\mathfrak{a}$ est de type fini.

$i) \Rightarrow ii)$. Soit

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \cdots$$

une suite d'idéaux de A. Alors $\mathfrak{a} = \bigcup_{i=1}^{\infty} \mathfrak{a}_i$ est un idéal. Comme tout idéal de A est de type fini, il existe $a_1, \ldots, a_k \in A$ tels que $\mathfrak{a} = (a_1, \ldots, a_k)$. Il existe $n \geqslant 1$ tel que $\mathfrak{a}_n$ contient tous les éléments a_i $(1 \leqslant i \leqslant k)$, d'où $\mathfrak{a} = \mathfrak{a}_n$. Alors,

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots .$$

La proposition est démontrée. □

Proposition 2.1.4. — *Soient M_1 et M_2 deux A-modules noetheriens. Alors $M_1 \times M_2$ est noetherien.*

Démonstration. — Soit la projection $\mathrm{pr} : M_1 \times M_2 \to M_2$ et soit M un sous-A-module de $M_1 \times M_2$. Alors, la restriction de pr à M a pour noyau le sous-A-module $M \cap M_1$ de M_1, qui est donc de type fini. Idem pour l'image. On en déduit que M est de type fini. □

Corollaire 2.1.5. — *Soit A un anneau noetherien et M un A-module de type fini. Alors M est noetherien.*

Démonstration. — Comme M est de type fini, il existe un entier n et un morphisme de A-modules $\varphi : A^n \twoheadrightarrow M$. Soit N un sous-A-module de M. Alors $\varphi^{-1}(N)$ est un sous-A-module de A^n donc de type fini. On en déduit que N est un A-module de type fini. □

2.2. Anneaux d'entiers

Commençons par une définition.

Définition 2.2.1. — Un anneau intègre (commutatif, unitaire) est dit de Dedekind s'il vérifie les propriétés suivantes :

(i) l'anneau A est noetherien ;
(ii) l'anneau A est intégralement clos ;
(iii) tout idéal premier non nul de A est maximal.

Exemple 2.2.2. — Un anneau principal est un anneau de Dedekind.

Théorème 2.2.3. — *Soit A un anneau de Dedekind,* $\mathrm{K} = \mathrm{Frac}(A)$. *Soit* L/K *une extension de degré fini n et soit B la fermeture intégrale de A dans* L. *Alors B est un anneau de Dedekind.*

Démonstration. — • Soit $\mathfrak{a}$ un idéal de B. On a vu (corollaire 1.2.9) que B est isomorphe à A^n (en tant que A-module). Il vient ainsi que tout sous-A-module M de B est de type fini car A^n est noetherien (corollaire 2.1.5). Donc $\mathfrak{a}$ est de type fini en tant que A-module et donc de type fini en tant que B-module. Donc B est noetherien.

• On a déjà vu (remarque 1.1.14) que L est le corps des fractions de B. Soit $x \in \mathrm{L}$, x entier sur B. Alors par transitivité x est entier sur A et donc $x \in B$: l'anneau B est intégralement clos.

• Il nous reste à montrer que tout idéal non nul et premier de B est maximal. Soit donc $\mathfrak{p}$ un tel idéal. Comme $\mathfrak{p}$ est non nul, il existe $0 \neq x \in \mathfrak{p}$. Comme $x \in B$, l'élément x est entier sur A : il existe $a_0, \cdots, a_{k-1} \in A$ tels que

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

L'anneau B étant intégre, on peut s'assurer que a_0 est non nul (il suffit de partir de $\mathrm{Irr}(x, \mathrm{K})$). Alors l'ideal $A \cap \mathfrak{p} \subset A$ est un idéal premier non nul de A (il contient a_0). Ainsi $A \cap \mathfrak{p}$ est un idéal maximal de A et $A/\mathfrak{p} \cap A$ est un corps.

Partons ensuite de l'injection $A/\mathfrak{p} \cap A \overset{\varphi}{\hookrightarrow} B/\mathfrak{p}$ et soit $y \in B - \mathfrak{p}$. L'élément y est entier sur A donc sur $A/\mathfrak{p} \cap A$: il existe $b_i \in A$ tels que

$$y^r + b_{r-1}y^{r-1} + \cdots + b_0 \equiv 0 \pmod{\mathfrak{p}}.$$

L'anneau $B/\mathfrak{p}$ étant intégre on peut s'assurer que $b_0 \notin \mathfrak{p}$. Comme $A/\mathfrak{p} \cap A$ est un corps, il existe $\alpha \in A$ tel que $b_0\alpha \equiv -1 (\mathrm{mod}\ \mathfrak{p})$. Il vient ainsi : $y\alpha(y^{r-1} + \cdots + b_1) \equiv 1 (\mathrm{mod}\ \mathfrak{p})$. Ainsi l'élément y est inversible dans $B/\mathfrak{p}$. En conclusion, l'anneau $B/\mathfrak{p}$ est un corps et l'idéal $\mathfrak{p}$ est maximal. □

Remarque 2.2.4. — Soit $\mathfrak{p}$ un idéal premier non nul de B. Montrons que l'on obtient rapidement que $\mathfrak{p}$ est maximal quand $\mathfrak{A}/\mathfrak{p} \cap A$ est fini. En effet, dans ce cas $B/\mathfrak{p}$ est aussi fini (car B est de type fini sur A) et est intègre : par conséquent $B/\mathfrak{p}$ est un corps et donc $\mathfrak{p}$ est maximal.

Corollaire 2.2.5. — *L'anneau des entiers $\mathcal{O}_{\mathrm{K}}$ d'un corps de nombres* K *est un anneau de Dedekind.*

Remarque 2.2.6. — Sous les conditions du théorème 2.2.3 et lorsque l'on part de $A = \mathbb{Z}$, il est assez immédiat de voir que tout idéal premier non nul $\mathfrak{p}$ de B est maximal. En effet, comme B est de type fini sur $\mathbb{Z}$, alors l'anneau $B/\mathfrak{p}$ est intégre et fini (de type fini sur $\mathbb{Z}/p\mathbb{Z}$, où $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$), c'est donc un corps. En effet pour $0 \neq x \in B/\mathfrak{p}$, l'application (non nécessairement linéaire) φ_x définie sur $B/\mathfrak{p}$ par $\varphi_x(z) = xz$ est injective et donc bijective (en calculant le cardinal de l'image), ce qui montre que $x \in (B/\mathfrak{p})^{\times}$.

Remarque 2.2.7. — Un anneau de Dedekind n'est pas forcément factoriel. En effet, l'anneau des entiers $\mathbb{Z}[\sqrt{-5}]$ du corps $\mathbb{Q}(\sqrt{-5})$ est de Dedekind. Mais dans cet anneau, on a

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

où les éléments $3, 7, 1 + 2\sqrt{-5}$ et $1 - 2\sqrt{-5}$ sont irréductibles et non conjugués entre eux. Il n'y a pas unicité de la factorisation, $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

2.3. Factorisation des idéaux - Groupe des classes

Dans cette section fixons un anneau de Dedekind A de corps des fractions $\mathrm{K} = \mathrm{Frac}(A)$.

2.3.1. Idéaux fractionnaires. —

Définition 2.3.1. — Un idéal fractionnaire $\mathfrak{a}$ de K par rapport à A, est un sous-A-module *non nul* de type fini contenu dans K.
Un idéal fractionnaire $\mathfrak{a}$ est dit entier (ou plus simplement idéal de A) si $\mathfrak{a} \subset A$, *i.e.* si c'est un idéal de A.

Soient deux idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{b}$. On définit une somme et un produit, en posant

$$\mathfrak{a} + \mathfrak{b} = \{a + b, a \in \mathfrak{a},\ b \in \mathfrak{b}\},$$
$$\mathfrak{a}\mathfrak{b} = \{\sum_{i \in I} a_i b_i, a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}, I \text{ fini}\},$$

et on vérifie que $\mathfrak{a}+\mathfrak{b}$ et $\mathfrak{ab}$ sont des idéaux fractionnaires de A.
On peut vérifier facilement les propriétés suivantes :

(i) $\mathfrak{a}(\mathfrak{b}_1+\mathfrak{b}_2)=\mathfrak{ab}_1+\mathfrak{ab}_2$;

(ii) Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux fractionnaires de A, alors $\mathfrak{a}\cap\mathfrak{b}$ l'est aussi et si de plus $\mathfrak{a}$ et $\mathfrak{b}$ sont entiers, il vient $\mathfrak{ab}\subseteq\mathfrak{a}\cap\mathfrak{b}$.

On définit l'inverse d'un idéal fractionnaire $\mathfrak{a}$ par

$$\mathfrak{a}^{-1} = \{x\in \mathrm{K}, x\mathfrak{a}\subseteq A\}.$$

Lemme 2.3.2. — *Soit $\mathfrak{a}$ un idéal fractionnaire de A. Alors $\mathfrak{a}^{-1}$ est également un idéal fractionnaire de A.*

Démonstration. — Soit $x\in\mathfrak{a}$, $x\neq 0$. Alors $x\mathfrak{a}^{-1}:=\{xb, b\in\mathfrak{a}^{-1}\}\subset A$ et on vérifie que c'est un idéal de A donc de type fini. On conclut en notant que $x\mathfrak{a}^{-1}\simeq\mathfrak{a}^{-1}$, isomorphisme de A-modules. □

Remarque 2.3.3. — Si $\mathfrak{a}$ est un idéal entier de A, alors $A\subset\mathfrak{a}^{-1}$.

Définition 2.3.4. — Soit $0\neq x\in\mathrm{K}$. Alors $xA:=\{xa, a\in A\}$ est un idéal fractionnaire principal de A. On écrit également $xA=(x)$.

Remarque 2.3.5. — Soit $\mathfrak{a}$ un idéal fractionnaire de A et soit $x\in\mathrm{K}^\times$. Alors $(x)\mathfrak{a}=x\mathfrak{a}=\{xa, a\in\mathfrak{a}\}$.

Remarque 2.3.6. — Pour $x\in\mathrm{K}^\times$, il vient $(x)^{-1}=(x^{-1})$.

Proposition 2.3.7. — *Un idéal fractionnaire $\mathfrak{b}$ s'écrit sous la forme*

$$\mathfrak{b}=a^{-1}\mathfrak{a}=\{a^{-1}x \mid x\in\mathfrak{a}\},$$

où $\mathfrak{a}$ est un idéal de A et $a\in A$ est un élément non nul.

Démonstration. — Soit $\mathfrak{b}$ un idéal fractionnaire. Comme $\mathfrak{b}$ est de type fini, il existe $a\in A$ tel que $\mathfrak{a}=a\mathfrak{b}\subseteq A$. On voit que $\mathfrak{a}$ est un idéal entier de A et que

$$\mathfrak{b}=a^{-1}\mathfrak{a}.$$

□

Définition 2.3.8. — Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de A. On dit que $\mathfrak{a}$ divise $\mathfrak{b}$ si $\mathfrak{b}\subseteq\mathfrak{a}$. On note $\mathfrak{a}\mid\mathfrak{b}$.

Lemme 2.3.9. — *L'idéal* $\mathfrak{p}$ *est un idéal premier de* A *si et seulement si*

$$\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \text{ ou } \mathfrak{p} \mid \mathfrak{b}\,.$$

Démonstration. — C'est immédiat. Si $\mathfrak{p} \nmid \mathfrak{a}$ et $\mathfrak{p} \nmid \mathfrak{b}$, il existe $x \in \mathfrak{a} - \mathfrak{p}$ et $y \in \mathfrak{b} - \mathfrak{p}$. Ainsi $xy \in \mathfrak{p}$ ce qui contredit le caractère premier de $\mathfrak{p}$. □

2.3.2. Résultat principal. — On souhaite montrer le résultat central suivant :

Théorème 2.3.10. — *Soit* A *un anneau de Dedekind. Tout idéal non nul* $\mathfrak{a}$ *de* A *admet une factorisation de la forme*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

où les $\mathfrak{p}_i$ *sont des idéaux premiers de* A*. Cette factorisation est unique à l'ordre près.*

Commençons par montrer deux lemmes techniques.

Lemme 2.3.11. — *Soit* A *un anneau de Dedekind et soit* $\mathfrak{a} \subseteq A$ *un idéal non nul. Alors il existe une famille finie d'idéaux premiers non nuls* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \subseteq A$ *telle que*

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_s \subseteq \mathfrak{a}\,.$$

Démonstration. — On fait un raisonnement par l'absurde. On considère l'ensemble S formé par les idéaux $\mathfrak{a}$ de A qui ne vérifient pas la conclusion du lemme. Supposons S non vide. L'ensemble S possède un plus grand élément $\mathfrak{a}$ pour l'inclusion (car l'anneau A est noetherien). Il est clair que $\mathfrak{a}$ n'est pas premier (sinon on pose $\mathfrak{p}_1 = \mathfrak{a}$ et on obtient $\mathfrak{p}_1 \subseteq \mathfrak{a}$). Donc, il existe $b_1, b_2 \notin \mathfrak{a}$ tels que $b_1b_2 \in \mathfrak{a}$. Posons $\mathfrak{a}_1 = b_1A + \mathfrak{a}$ et $\mathfrak{a}_2 = b_2A + \mathfrak{a}$. Comme $b_1, b_2 \notin \mathfrak{a}$, on a des inclusions strictes $\mathfrak{a} \subsetneq \mathfrak{a}_1$ et $\mathfrak{a} \subsetneq \mathfrak{a}_2$. D'autre part, $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ car $b_1b_2 \in \mathfrak{a}$. Par définition de $\mathfrak{a}$, les idéaux $\mathfrak{a}_1$ et $\mathfrak{a}_2$ vérifient la conclusion du lemme, donc il existe des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, $\mathfrak{p}_{k+1}, \ldots, \mathfrak{p}_s$ tels que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \mathfrak{a}_1,$$
$$\mathfrak{p}_{k+1} \cdots \mathfrak{p}_s \subseteq \mathfrak{a}_2,$$

d'où

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k\mathfrak{p}_{k+1} \cdots \mathfrak{p}_s \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}.$$

Contradiction et $S = \emptyset$. □

Lemme 2.3.12. — *Soit $\mathfrak{p}$ un idéal premier non nul de A. Alors quelque soit l'idéal non nul $\mathfrak{a}$ de A, il vient $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$. En particulier, $\mathfrak{p}^{-1}\mathfrak{p} = A$.*

Démonstration. — On montre d'abord que $\mathfrak{p}^{-1} \neq A$. On fixe un élément non nul a de $\mathfrak{p}$. On utilise le lemme 2.3.11 et on choisit une plus courte chaîne d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ telle que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}\mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}.$$

Alors $\mathfrak{p} \mid \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}\mathfrak{p}_r$ d'où $\mathfrak{p} \mid \mathfrak{p}_i$ pour un certain i. Pour simplifier la notation on peut supposer $i = 1$. Comme tout idéal premier non nul est maximal (A est de Dedekind !), on en déduit que $\mathfrak{p} = \mathfrak{p}_1$.
D'autre part, par le choix des idéaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ on a :

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq (a).$$

Donc, il existe $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tel que $b \notin (a)$, mais

$$(b)\mathfrak{p} = (b)\mathfrak{p}_1 \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}\mathfrak{p}_r \subseteq (a).$$

On en déduit que l'élément $x = a^{-1}b$ appartient à $\mathfrak{p}^{-1}$. D'autre part, $x \notin A$ car $b \notin (a)$. On a démontré que $\mathfrak{p}^{-1} \neq A$.

Soit $\mathfrak{a}$ un idéal non nul de A tel que $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$. Alors pour tout $x \in \mathfrak{p}^{-1}$ on a $(x)\mathfrak{a} \subset \mathfrak{a}$. Comme A est noethérien, l'idéal $\mathfrak{a}$ est de type fini et un raisonnement analogue à celui de la preuve de la proposition 1.1.4 implique que x est entier sur A. Comme A est intégralement clos, ceci signifie que $x \in A$ et donc $\mathfrak{p}^{-1} \subseteq A$ puis que $\mathfrak{p}^{-1} = A$ car $\mathfrak{p}$ est entier (donc $A \subseteq \mathfrak{p}^{-1}$). Ce qui contredit le fait que $\mathfrak{p}^{-1} \neq A$.

Terminons la preuve du lemme. Comme $A \subseteq \mathfrak{p}^{-1}$, on a

$$\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq A.$$

Comme $\mathfrak{p}$ est maximal, il suffit de se rappeler que $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$ pour conclure que $\mathfrak{p}\mathfrak{p}^{-1} = A$. □

Démonstration. — du théorème 2.3.10.
Existence. Donnons une démonstration par l'absurde. Soit $\mathfrak{a}$ un idéal non nul de A. Supposons que $\mathfrak{a}$ ne s'écrive pas comme produit d'idéaux premiers. Comme A est noetherien, on peut supposer $\mathfrak{a}$ maximal pour cette propriété. L'idéal $\mathfrak{a}$ n'est pas premier.

Soit $\mathfrak{p}$ un idéal premier contenant $\mathfrak{a}$ et soit $\mathfrak{b} = \mathfrak{a}\mathfrak{p}^{-1}$; l'idéal $\mathfrak{b}$ est un idéal de A et $\mathfrak{a} \subseteq \mathfrak{b}$. D'après le lemme 2.3.12, l'inclusion est stricte. Alors $\mathfrak{a} \subsetneq \mathfrak{b}$ et par le choix de $\mathfrak{a}$, l'idéal $\mathfrak{b}$ s'écrit

$$\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k.$$

Donc,

$$\mathfrak{a} = (\mathfrak{p}\mathfrak{p}^{-1})\mathfrak{a} = \mathfrak{p}(\mathfrak{p}^{-1}\mathfrak{a}) = \mathfrak{p}\mathfrak{b} = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k.$$

Contradiction.

Unicité de la factorisation. Soit

$$\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

une autre factorisation de $\mathfrak{a}$. Alors

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s \tag{1}$$

On a $\mathfrak{q}_1 \mid \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$. Comme $\mathfrak{q}_1$ est premier, il existe i tel que $\mathfrak{q}_1 \mid \mathfrak{p}_i$ et comme $\mathfrak{p}_i$ est maximal on en déduit que $\mathfrak{q}_1 = \mathfrak{p}_i$. Pour simplifier la notation supposons $i = 1$, d'où $\mathfrak{q}_1 = \mathfrak{p}_1$. En multipliant (1) par $\mathfrak{p}_1^{-1}$, on obtient

$$\mathfrak{p}_2 \cdots \mathfrak{p}_k = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

En appliquant les mêmes arguments à cette égalité on trouve que $\mathfrak{q}_2 = \mathfrak{p}_2$ etc. Le théorème est démontré. □

Corollaire 2.3.13. — *Soit A un anneau de Dedekind de corps de fractions* K. *Tout idéal fractionnaire $\mathfrak{a}$ de* K *par rapport à* K *s'écrit d'une façon et d'une seule sous la forme :*

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{a})},$$

où $n_\mathfrak{p}(\mathfrak{a})$ sont des entiers presque tous nuls et où $\mathbb{P}$ est l'ensemble des idéaux premiers $\mathfrak{p}$ de A.
L'entier $n_\mathfrak{p}(\mathfrak{a})$ est la valuation $\mathfrak{p}$-adique de $\mathfrak{a}$. Il est également noté $\mathrm{v}_\mathfrak{p}(\mathfrak{a})$.

Démonstration. — Il existe $a \in A$ tel que $\mathfrak{b} = a\mathfrak{a}$ est un idéal de A. Soient

$$\mathfrak{b} = \prod_{\mathfrak{p}\in\mathbb{P}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})},$$
$$(a) = \prod_{\mathfrak{p}\in\mathbb{P}} \mathfrak{p}^{n_\mathfrak{p}((a))}$$

les factorisations des idéaux entiers $\mathfrak{b}$ et (a). Alors,

$$\mathfrak{a} = (a)^{-1}\mathfrak{b} = \prod_{\mathfrak{p}\in\mathbb{P}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})-n_\mathfrak{p}((a))}$$

et on pose $n_\mathfrak{p}(\mathfrak{a}) = n_\mathfrak{p}(\mathfrak{b}) - n_\mathfrak{p}((a))$. L'unicité se déduit du théorème 2.3.10. □

Remarque 2.3.14. — On note que $\mathrm{v}_\mathfrak{p}(\mathfrak{ab}) = \mathrm{v}_\mathfrak{p}(\mathfrak{a}) + \mathrm{v}_p(\mathfrak{b})$.

Théorème 2.3.15. — *Soit A un anneau de Dedekind de corps des fractions* K. *Alors l'ensemble des d'idéaux fractionnaires $\mathcal{I}_\mathrm{K}$ (ou encore $\mathcal{I}_A$) de A est un groupe abélien pour la multiplication. Le neutre est l'idéal A et l'idéal $\mathfrak{a}^{-1}$ est l'inverse de l'idéal $\mathfrak{a}$.*

Démonstration. — Il est clair que le produit d'idéaux fractionnaires vérifie les propriétés suivantes :

$$\mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c},$$
$$\mathfrak{ab} = \mathfrak{ba},$$
$$\mathfrak{a}A = \mathfrak{a}.$$

Donc, le seul point difficile est de montrer la formule

$$\mathfrak{a}\mathfrak{a}^{-1} = A.$$

On montre d'abord que tout idéal $\mathfrak{a}$ non nul entier est inversible.
D'après le corollaire 2.3.13, $\mathfrak{a}$ s'écrit $\mathfrak{a} = \mathfrak{p}_1^{n_{\mathfrak{p}_1}(\mathfrak{a})} \cdots \mathfrak{p}_k^{n_{\mathfrak{p}_k}(\mathfrak{a})}$. Soit l'idéal fractionnaire $\mathfrak{b} = \mathfrak{p}_k^{-n_{\mathfrak{p}_k}(\mathfrak{a})} \cdots \mathfrak{p}_1^{-n_{\mathfrak{p}_1}(\mathfrak{a})}$. Alors, d'après le lemme 2.3.12, il vient $\mathfrak{ab} = A$.

Il reste donc à montrer la formule $\mathfrak{a}\mathfrak{a}^{-1} = A$, ou encore que $\mathfrak{a}^{-1}$ est bien l'inverse de $\mathfrak{a}$. On sait qu'il existe un idéal fractionnaire $\mathfrak{b}$ tel que $\mathfrak{ab} = A$.

Par définition, $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Réciproquement, soit $x \in \mathfrak{a}^{-1}$. Alors $(x)\mathfrak{a} \subseteq A$, d'où

$$x \in (x)\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}.$$

Donc, $\mathfrak{a}^{-1} \subseteq \mathfrak{b}$ ce qui montre que $\mathfrak{a}^{-1} = \mathfrak{b}$. Le théorème est démontré. □

Remarque 2.3.16. — Pour tout idéal fractionnaire $\mathfrak{a}$ et tout premier $\mathfrak{p}$ non nul, il vient : $\mathrm{v}_{\mathfrak{p}}(\mathfrak{a}^{-1}) = -\mathrm{v}_{\mathfrak{p}}(\mathfrak{a})$.

Corollaire 2.3.17. — *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux entiers de A. Alors $\mathfrak{a} \mid \mathfrak{b}$ si et seulement si, il existe un idéal $\mathfrak{c}$ de A tel que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.*

Démonstration. — On a $\mathfrak{a} \mid \mathfrak{b}$ si et seulement si $\mathfrak{b} \subset \mathfrak{a}$. Si tel est le cas, $\mathfrak{c} := \mathfrak{b}\mathfrak{a}^{-1}$ est un idéal entier de A et on a alors bien $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$. La réciproque est immédiate. □

Remarque 2.3.18. — L'ensemble $\mathcal{P}_{\mathrm{K}}$ constitués des idéaux fractionnaires principaux forme un sous-groupe de $\mathcal{I}_{\mathrm{K}}$.

Définition 2.3.19. — Soit A un anneau de Dedekind de corps des fractions $\mathrm{K} = \mathrm{Frac}(A)$. Soit $\mathcal{I}_{\mathrm{K}}$ le groupe des idéaux fractionnaires de A et $\mathcal{P}_{\mathrm{K}}$ le sous-groupe des idéaux fractionnaires principaux. Alors le groupe des classes Cl_{K} de K (ou de A) est le groupe quotient

$$\mathrm{Cl}_{\mathrm{K}} = \mathcal{I}_{\mathrm{K}}/\mathcal{P}_{\mathrm{K}}.$$

C'est un groupe abélien.

Il résulte de cette définition la propriété suivante :

Remarque 2.3.20. — A est principal si et seulement si $\mathrm{Cl}_{\mathrm{K}} = \{1\}$ (i.e. si Cl_{K} est réduit à l'élément neutre).

2.4. Propriétés des idéaux fractionnaires

Fixons un anneau de Dedekind A. Les idéaux étudiés sont non nuls.

Définition 2.4.1. — Deux idéaux non nuls $\mathfrak{a}$ et $\mathfrak{b}$ de A sont dits premiers entre eux si $\mathfrak{a} + \mathfrak{b} = A$. On notera alors $(\mathfrak{a}, \mathfrak{b}) = 1$.

Remarque 2.4.2. — Si $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux premiers non nuls de A, alors $(\mathfrak{p}, \mathfrak{p}') = 1$ si et seulement si $\mathfrak{p} \neq \mathfrak{p}'$.

Lemme 2.4.3. — *Soient les factorisations* $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ *et* $\mathfrak{b} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$ *de* $\mathfrak{a}$ *et de* $\mathfrak{b}$ *en produit d'idéaux premiers. Alors* $(\mathfrak{a}, \mathfrak{b}) = 1$ *si et seulement si, pour tout* i *et* j, $(\mathfrak{p}_i, \mathfrak{p}'_j) = 1$.

Démonstration. — Un sens est évident. Contentons nous de montrer que si pour tout i et j, $(\mathfrak{p}_i, \mathfrak{p}'_j) = 1$, alors $(\mathfrak{a}, \mathfrak{b}) = 1$. Supposons qu'il existe un premier $\mathfrak{q}$ tel que $\mathfrak{q} \mid \mathfrak{a}+\mathfrak{b}$. Alors comme $\mathfrak{a} \subset \mathfrak{a}+\mathfrak{b} \subset \mathfrak{q}$, il vient $\mathfrak{q} \mid \mathfrak{p}_1 \cdots \mathfrak{p}_r$ et par unicité, $\mathfrak{q} = \mathfrak{p}_i$ pour un certain entier i. De même $\mathfrak{q} \mid \mathfrak{b}$ et donc $\mathfrak{q} = \mathfrak{p}'_j$, pour un certain entier j. Contradiction. Donc $\mathfrak{a} + \mathfrak{b} = A$. □

Proposition 2.4.4. — *Soient* $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{a})}$ *et* $\mathfrak{b} = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})}$ *deux idéaux de* A.

(i) Alors $\mathfrak{a} \mid \mathfrak{b}$ *si et seulement si*

$$n_\mathfrak{p}(\mathfrak{a}) \leqslant n_\mathfrak{p}(\mathfrak{b}) \text{ pour tout } \mathfrak{p}.$$

(ii) On a

$$\mathfrak{a} + \mathfrak{b} = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{\min\{n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b})\}},$$

$$\mathfrak{a} \cap \mathfrak{b} = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{\max\{n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b})\}}.$$

(iii) Soit a *et* b *deux éléments de* A. *Alors, pour tout idéal premier* $\mathfrak{p}$, *il vient* $\mathrm{v}_\mathfrak{p}((a+b)) \geq \min(\mathrm{v}_\mathfrak{p}((a)), \mathrm{v}_p((b)))$, *avec égalité si les quantités* $\mathrm{v}_\mathfrak{p}((a))$ *et* $\mathrm{v}_\mathfrak{p}((b))$ *sont différentes.*

Démonstration. — (i) C'est une conséquence du corollaire 2.3.17. En effet, $\mathfrak{a} \mid \mathfrak{b}$ si et seulement si il existe un idéal de A

$$\mathfrak{c} = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{c})}$$

tel que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Donc, on obtient que $n_\mathfrak{p}(\mathfrak{b}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{c})$, d'où la propriété.

(ii) Posons $\mathfrak{c} = \mathfrak{a}+\mathfrak{b}$. Alors $\mathfrak{c}$ est le plus petit idéal tel que $\mathfrak{c} \mid \mathfrak{a}$ et $\mathfrak{c} \mid \mathfrak{b}$. En utilisant (i) on obtient que $n_\mathfrak{p}(\mathfrak{c})$ est le plus grand entier vérifiant $n_\mathfrak{p}(\mathfrak{c}) \leqslant n_\mathfrak{p}(\mathfrak{a})$ et $n_\mathfrak{p}(\mathfrak{c}) \leqslant n_\mathfrak{p}(\mathfrak{b})$, d'où $n_\mathfrak{p}(\mathfrak{c}) \leq \min\{n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b})\}$. L'inégalité dans l'autre sens provient du fait que $(a) + (b) \subset \mathfrak{p}^{\min\{n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b})\}}$. La preuve de

la deuxième formule est analogue et utilise le fait que $\mathfrak{a} \cap \mathfrak{b}$ est le plus grand idéal tel que $\mathfrak{a}, \mathfrak{b} \mid \mathfrak{a} \cap \mathfrak{b}$.

(iii) On note tout d'abord que $(a+b) \subset (a) + (b)$. Ainsi

$$\mathrm{v}_{\mathfrak{p}}((a) + (b)) = \min(\mathrm{v}_{\mathfrak{p}}((a)), \mathrm{v}_{\mathfrak{p}}((b))) \leq \mathrm{v}_{\mathfrak{p}}((a+b)).$$

Supposons que $\mathrm{v}_{\mathfrak{p}}((a)) < \mathrm{v}_{\mathfrak{p}}((b))$. Alors de l'égalité $a = -b + (b+a)$, on en déduit $(a) \subset (b) + (b+a)$ et ainsi

$$\mathrm{v}_{\mathfrak{p}}((a)) \geq \min(\mathrm{v}_{\mathfrak{p}}((b)), \mathrm{v}_{\mathfrak{p}}((b+a))) = \mathrm{v}_{\mathfrak{p}}((a+b)).$$

□

On obtient ainsi donc :

Corollaire 2.4.5. — *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux, alors*

$$\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}\,.$$

***Théorème 2.4.6* (des restes chinois)**. — *Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux de A qui sont premiers entre eux. Alors l'application*

$$\begin{array}{rcl} f : A/\mathfrak{ab} & \to & (A/\mathfrak{a}) \times (A/\mathfrak{b}) \\ (x + \mathfrak{ab}) & \mapsto & (x + \mathfrak{a}, x + \mathfrak{b}) \end{array}$$

est un isomorphisme.

Démonstration. — Comme $\mathfrak{ab} \subseteq \mathfrak{a}, \mathfrak{b}$, l'application f est bien définie et il est facile de voir que f est un homomorphisme d'anneaux. Pour montrer que f est injective, on calcule $\ker(f)$. Soit $f(x+\mathfrak{ab}) = (\bar{0}_{A/\mathfrak{a}}, \bar{0}_{A/\mathfrak{b}})$. Alors, $x + \mathfrak{a} = \mathfrak{a}$ et $x + \mathfrak{b} = \mathfrak{b}$ ce qui signifie que $x \in \mathfrak{a}$ et $x \in \mathfrak{b}$. Donc, $x \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.
Montrons maintenant que f est surjective. Comme $\mathfrak{a} + \mathfrak{b} = A$, il existe $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$. Soit $(y + \mathfrak{a}, z + \mathfrak{b})$ un élément de $(A/\mathfrak{a}) \times (A/\mathfrak{b})$. Posons $x = az + by$. Alors

$$\begin{aligned} x = az + (1-a)y \equiv y \pmod{\mathfrak{a}}, \\ x = (1-b)z + by \equiv z \pmod{\mathfrak{b}} \end{aligned}$$

d'ou $f(x + \mathfrak{ab}) = (y + \mathfrak{a}, z + \mathfrak{b})$. Donc, tout élément de $(A/\mathfrak{a}) \times (A/\mathfrak{b})$ possède un antécedent dans $A/\mathfrak{ab}$ et f est surjective. □

Par récurrence, on obtient :

Théorème 2.4.7. — *Soit $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ une famille d'idéaux de A tels que $\mathfrak{a}_i + \mathfrak{a}_j = A$ si $i \neq j$. Posons*

$$\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdot \ldots \cdot \mathfrak{a}_k.$$

Alors on a un isomorphisme canonique

$$A/\mathfrak{a} \simeq (A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_k).$$

Corollaire 2.4.8. — *Si l'ensemble $\mathbb{P}$ des idéaux premiers de A est fini, alors A est principal.*

Démonstration. — Soit $\mathbb{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Montrons que l'idéal $\mathfrak{p}_1$ est principal (le même argument marche pour tout $\mathfrak{p}_i$). D'après l'unicité de la factorisation, $\mathfrak{p}_1^2 \neq \mathfrak{p}_1$. Donc on a l'inclusion stricte $\mathfrak{p}_1^2 \subsetneq \mathfrak{p}_1$. Choisissons $a \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$ et considérons le système :

$$\begin{array}{ll} x \equiv a & (\mathrm{mod}\ \mathfrak{p}_1^2) \\ x \equiv 1 & (\mathrm{mod}\ \mathfrak{p}_2) \\ \cdots\cdots\cdots\cdots & \\ x \equiv 1 & (\mathrm{mod}\ \mathfrak{p}_n) \end{array}$$

Comme $\mathfrak{p}_i + \mathfrak{p}_j = A$ si $i \neq j$, le théorème des restes chinois implique que ce système est résoluble. Soit x une solution. Alors $\mathfrak{p}_1 \mid (x)$, $\mathfrak{p}_1^2 \nmid (x)$ et $\mathfrak{p}_i \nmid (x)$ pour $i = 2, \ldots, n$. Comme $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ sont les idéaux premiers de A ceci signifie que la factorisation de (x) s'écrit

$$(x) = \mathfrak{p}_1,$$

d'où le résultat voulu. □

Donnons le lemme d'approximation qui peut être vu comme une extension du théorème des restes chinois.

Lemme 2.4.9 **(lemme d'approximation)**. —
Pour $i = 1, \ldots, k$, soient $\mathfrak{p}_i$ des idéaux premiers non nuls de A distincts deux à deux, des éléments $x_i \in \mathrm{K}$ et $n_i \geqslant 0$. Alors il existe $x \in \mathrm{K}$ tel que pour $i = 1, \ldots, k$

$$\mathrm{v}_{\mathfrak{p}_i}(x - x_i) \geqslant n_i$$

et tel que pour $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k$,

$$\mathrm{v}_{\mathfrak{q}}(x) \geqslant 0.$$

Démonstration. — Si les éléments x_i sont dans A, c'est le théorème 2.4.7.

Considérons maintenant le cas général. Soit $x_i = a_i/s_i$ avec $a_i, s_i \in A$. Posons $s = s_1 \cdot \ldots \cdot s_k$. Alors $x_i = b_i/s$, où $b_i = a_i s_1 \cdots s_{i-1} s_{i+1} \cdots s_k$. Considérons le système suivant : pour $i = 1, \ldots, k$

$$\mathrm{v}_{\mathfrak{p}_i}(y - b_i) \geqslant n_i + v_{\mathfrak{p}_i}(s)$$

et pour $\mathfrak{q} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k$

$$\mathrm{v}_{\mathfrak{q}}(y) \geqslant \mathrm{v}_{\mathfrak{q}}(s).$$

Comme $\mathrm{v}_{\mathfrak{q}}(s) = 0$ pour presque tout $\mathfrak{q}$, c'est un système fini correspondant au cadre du théorème des restes chinois (il faut ajouter à la famille $\{\mathfrak{p}_i\}$ les idéaux $\mathfrak{q}$ tels que $\mathrm{v}_{\mathfrak{q}}(s) > 0$). Il est résoluble. Soit y une solution. Posons $x = y/s$. Alors

$$\mathrm{v}_{\mathfrak{p}_i}(x - x_i) = \mathrm{v}_{\mathfrak{p}_i}\left(\frac{y - b_i}{s}\right) = \mathrm{v}_{\mathfrak{p}_i}(y - b_i) - \mathrm{v}_{\mathfrak{p}_i}(s) \geqslant n_i$$

et

$$\mathrm{v}_{\mathfrak{q}}(x) = \mathrm{v}_{\mathfrak{q}}(y) - \mathrm{v}_{\mathfrak{q}}(s) \geqslant 0.$$

Le lemme est démontré. □

Nous avons vu qu'un anneau de Dedekind peut ne pas être principal. Nous avons en fait :

Proposition 2.4.10. — *Tout idéal fractionnaire $\mathfrak{a}$ de A est engendré par au plus deux éléments (en tant que A-module).*

Démonstration. — Il suffit de montrer la proposition pour les idéaux entiers non nuls de A.
Soit donc $\mathfrak{a}$ un idéal non nul de A. Soit $0 \neq a \in \mathfrak{a}$. Alors $(a) \subset \mathfrak{a}$ et ainsi $\mathfrak{a} \mid (a)$:

$$(a) = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{\alpha_\mathfrak{p}}, \quad \mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}} \mathfrak{p}^{\beta_\mathfrak{p}},$$

avec $\beta_\mathfrak{p} \leq \alpha_\mathfrak{p}$.
Choisissons, pour $\mathfrak{p} | \mathfrak{a}$, $b_\mathfrak{p}$ tel que $b_\mathfrak{p} \in \mathfrak{p}^{\beta_\mathfrak{p}} - \mathfrak{p}^{\beta_\mathfrak{p}+1}$: c'est possible car ces idéaux sont bien différents (par unicité de la factorisation). Soit alors $b \in A$ vérifiant :

(i) $b \equiv b_\mathfrak{p} (\mathrm{mod}\ \mathfrak{p}^{\beta_\mathfrak{p}+1})$ pour tout premier $\mathfrak{p}$ divisant $\mathfrak{a}$;

(ii) $b \equiv 1 (\mathrm{mod}\ \mathfrak{q})$ pour tout premier $\mathfrak{q}$ divisant (a) mais ne divisant pas $\mathfrak{a}$.

Par le théorème des restes chinois, un tel élément b existe.
Alors pour tout premier $\mathfrak{p}$ divisant $\mathfrak{a}$ (et en utilisant le point (iii) de la proposition 2.4.4), on a

$$\mathrm{v}_{\mathfrak{p}}((b)) = \mathrm{v}_{\mathfrak{p}}((b_{\mathfrak{p}})) = \beta_{\mathfrak{p}} = \mathrm{v}_{\mathfrak{p}}(\mathfrak{a}).$$

Ainsi $\mathfrak{a} \mid (b)$ i.e. $(b) \subset \mathfrak{a}$, ou encore que $b \in \mathfrak{a}$. Notons ensuite que si $\mathfrak{q}$ est un premier de A étranger à $\mathfrak{a}$ mais divisant (a), alors $\mathrm{v}_{\mathfrak{q}}((b)) = \mathrm{v}_{\mathfrak{q}}(\mathfrak{a}) = 0$. Ainsi pour tout premier $\mathfrak{p}$ de A, nous venons de montrer que

$$\mathrm{v}_{\mathfrak{p}}((a) + (b)) = \min(\mathrm{v}_{\mathfrak{p}}((a)), \mathrm{v}_{\mathfrak{p}}((b))) = \mathrm{v}_{\mathfrak{p}}(\mathfrak{a}),$$

i.e.

$$\mathfrak{a} = (a) + (b) = (a, b).$$

□

2.5. Décomposition des idéaux premiers dans une extension

2.5.1. La norme d'un idéal. — Soit $\mathrm{K}/\mathbb{Q}$ une extension de degré n. Notons par $\mathcal{O}_{\mathrm{K}} = \mathcal{O}$ l'anneau des entiers de K : c'est la fermeture intégrale de $\mathbb{Z}$ dans K.

Lemme 2.5.1. — *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$. Alors $\mathcal{O}/\mathfrak{p}$ est un corps fini.*

Démonstration. — On sait déja que $\mathcal{O}/\mathfrak{p}$ est un corps. Plus précisément c'est une extension du corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, où $p = \mathfrak{p} \cap \mathbb{Z}$ pour un certain nombre premier p. Comme l'anneau $\mathcal{O}_{\mathrm{K}}$ est de type fini sur $\mathbb{Z}$, on en déduit que $\mathcal{O}/\mathfrak{p}$ est aussi de type fini sur $\mathbb{F}_p$, ou encore que $\mathcal{O}_{\mathfrak{p}} \simeq \mathbb{F}_{p^f}$. □

Corollaire 2.5.2. — *Soit $\mathfrak{a}$ un idéal entier non nul de $\mathcal{O}$. Alors l'anneau $\mathcal{O}/\mathfrak{a}$ est fini.*

Démonstration. — D'après le théorème 2.4.7, il suffit de montrer le corollaire quand $\mathfrak{a} = \mathfrak{p}^r$, ici $\mathfrak{p}$ est un idéal premier. Notons la suite d'inclusion

$$\mathfrak{p}^r \subset \mathfrak{p}^{r-1} \subset \cdots \subset \mathfrak{p} \subset \mathcal{O}.$$

Pour $i \geq 1$, soit alors le morphisme naturel

$$\mathcal{O}/\mathfrak{p}^i \to \mathcal{O}/\mathfrak{p}^{i-1}.$$

Ce morphisme est surjectif de noyau $\mathfrak{p}^{i-1}/\mathfrak{p}^i$.
Soit $x \in \mathfrak{p}^{i-1} - \mathfrak{p}^i$ et soit

$$\begin{array}{rccc} \varphi_x : \mathcal{O} & \to & \mathfrak{p}^{i-1}/\mathfrak{p}^i \\ y & \mapsto & xy \end{array}$$

Alors $\ker(\varphi_x) = \mathfrak{p}$. Ensuite on note que $\mathrm{v}_\mathfrak{p}((x) + \mathfrak{p}^i) = i - 1$ et que pour $\mathfrak{q} \neq \mathfrak{p}$, $\mathrm{v}_\mathfrak{q}((x) + \mathfrak{p}^i) = 0$. Ainsi $((x) + \mathfrak{p}^i) = \mathfrak{p}^{i-1}$ et donc φ_x est surjectif.
Au final, après dévissage donc, on obtient que

$$\#\mathcal{O}/\mathfrak{p}^r = (\#\mathcal{O}/\mathfrak{p})^r.$$

□

Définition 2.5.3. — Soit $\mathfrak{a} \subset \mathcal{O}$ un idéal entier de A. On définit la norme $\mathrm{N}(\mathfrak{a})$ de A par

$$\mathrm{N}(\mathfrak{a}) = \#(\mathcal{O}/\mathfrak{a}).$$

La norme est multiplicative :

Proposition 2.5.4. — *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $\mathcal{O}$. Alors*

$$\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}).$$

Démonstration. — C'est immédiat. □

Cette propriété de multiplicativé nous permet de définir la norme d'un idéal fractionnaire.

Définition 2.5.5. — Soit $\mathfrak{a}$ un idéal fractionnaire de $\mathcal{O}$. Il existe un élément $x \in \mathcal{O}$ tel que $x\mathfrak{a} = \mathfrak{b} \subset \mathcal{O}$. On pose alors

$$\mathrm{N}(\mathfrak{a}) = \frac{\mathrm{N}(\mathfrak{b})}{\mathrm{N}((x))}.$$

(On peut s'assurer que cette définition ne dépend pas du choix de x.)

Pour être complet :

Proposition 2.5.6. — *Soit $0 \neq x \in \mathcal{O}$. Alors*

$$\mathrm{N}((x)) = |\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)|.$$

Remarque 2.5.7. — Là-aussi, on peut étendre cette propriété aux idéaux fractionnaires principaux.

Démonstration. — On rappelle que $(x) = x\mathcal{O}$ est un $\mathbb{Z}$-module de rang $n = [\mathrm{K} : \mathbb{Q}]$. D'après la théorie des modules sur $\mathbb{Z}$, il existe une $\mathbb{Z}$-base $\{x_1, \cdots, x_n\}$ de $\mathcal{O}$ et des entiers $d_1 \mid \cdots \mid d_n$ tels que $\{d_1 x_1, \cdots, d_n x_n\}$ forme une $\mathbb{Z}$-base de $(x) = x\mathcal{O}$. Alors

$$\mathcal{O}/(x) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z},$$

et ainsi $\mathrm{N}((x)) = d_1 \cdots d_n$.
D'autre part $\{xx_1, \cdots, xx_n\}$ est aussi une $\mathbb{Z}$-base de (x).
Posons $u : x_i \mapsto d_i x_i$ et $v : d_i x_i \mapsto x x_i$ (pour $i = 1, \cdots, n$). Alors $v \circ u$ est la multiplication par x et donc, par définition, $\det(v \circ u) = \mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)$. Or v est un isomorphisme sur le $\mathbb{Z}$-module $(x) = x\mathcal{O}$ et ainsi $\det(v) = \pm 1$. D'autre part, clairement, $\det(u) = d_1, \cdots, d_n$. D'où le résultat. □

2.5.2. Le résultat principal. — Soit $\mathrm{K}/\mathbb{Q}$ une extension de degré fini n. Soit $\mathcal{O}$ l'anneau des entiers de K. Soit un nombre premier $p \in \mathbb{Z}$. Alors, par la théorème 2.3.10,

$$p\mathcal{O} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}$ (nous verrons que $i \geq 1$). On peut noter que $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$. On dit alors que l'idéal premier $\mathfrak{p}_i$ est au-dessus de p.
Soit maintenant $\mathfrak{p}$ un idéal maximal de $\mathcal{O}$. Alors $\mathfrak{p} \cap \mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$ donc de la forme $p\mathbb{Z}$, pour un certain nombre premier p. Ainsi, $\mathfrak{p}$ divise $p\mathcal{O}$ et l'idéal $\mathfrak{p}$ apparaît dans la factorisation de $p\mathcal{O}$.
Grâce au lemme 2.5.1, on sait que $\mathcal{O}/\mathfrak{p}_i$ est une extension de degré fini de $\mathbb{F}_p$. Notons $f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$.

Proposition 2.5.8. — *On a la formule*

$$n = [\mathrm{K} : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i.$$

Démonstration. — C'est assez immédiat. On prend la norme de l'égalité $p\mathcal{O} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ pour obtenir $p^n = \prod_i p^{e_i f_i}$, d'où le résultat. □

Plus généralement, nous avons :

Théorème 2.5.9. — *Soit A un anneau de Dedekind de corps des fractions* K. *Soit* L/K *une extension de degré n et soit B la fermeture intégrale de A dans* L. *Enfin soit $\mathfrak{p}$ un idéal premier non nul de A. Alors*

$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

où pour $i = 1, \cdots, g$, $\mathfrak{P}_i$ est un idéal premier de B au-dessus de $\mathfrak{p}$; de plus

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

où $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ est le degré résiduel de $\mathfrak{P}_i$ dans L/K *(et e_i l'indice de ramification).*

Avant de passer à la preuve donnons une extension du lemme 2.5.1 et du corollaire 2.5.2 :

Lemme 2.5.10. — *Sous les conditions du théorème 2.5.9, l'extension $B/\mathfrak{P}_i$ est de degré fini et pour tout entier $m \geq 1$, le $A/\mathfrak{p}$-espace vectoriel $B/\mathfrak{P}_i^m$ est de dimension mf_i, où $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ est le degré résiduel de $\mathfrak{P}_i$ dans* L/K.

Démonstration. — Partons d'une K-base $\{x_1, \ldots, x_m\} \subset B$ de L. Soit d le discriminant de celle-ci. D'apès le lemme 1.2.11, on a $\mathrm{d}B \subset Ax_1 + \cdots + x_n \simeq A^n$. Comme A est noetherien, il vient que B est de type fini comme A-module, il en est de même de $B/\mathfrak{P}$ comme $A/\mathfrak{p}$-module.
Comme pour le corollaire 2.5.2 i.e., par dévissage, et comme $B/\mathfrak{P}$ est de dimension finie sur $A/\mathfrak{p}$, on obtient que $B/\mathfrak{p}$ est de dimension finie sur le corps $A/\mathfrak{p}$. □

Démonstration. — Par le théorème 2.3.10, on sait que $\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, où $\mathfrak{P}_i$ sont des idéaux premiers de B. On peut noter que $\mathfrak{P}_i \cap A = \mathfrak{p}$.

Réciproquement, si $\mathfrak{P}$ est un idéal maximal de B au-dessus de $\mathfrak{p}$, alors $\mathfrak{P} \mid \mathfrak{p}B$ et ainsi $\mathfrak{P}$ apparaît dans la factorisation de $\mathfrak{p}B$.

Posons $k = A/\mathfrak{p}$.
Par le théorème des restes chinois,

$$B/\mathfrak{p}B \simeq \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}.$$

Cet isomorphisme est un isomorphisme de k-espace vectoriel. Ainsi

$$\dim_k B/\mathfrak{p}B = \sum_i \dim_{\mathrm{k}} B/\mathfrak{P}_i^{e_i}.$$

Il nous faut donc montrer que

$$n = \dim_{\mathrm{k}} B/\mathfrak{p}B$$

et que

$$\dim_{\mathrm{k}} B/\mathfrak{P}_i^{e_i} = e_i f_i.$$

Pour un idéal maximal $\mathfrak{P}$ de B, on a vu (lemme 2.5.10) que

$$\dim_k B/\mathfrak{P}_i^{e_i} = e_i \dim_k B/\mathfrak{P}_i = e_i f_i.$$

Il nous reste à montrer que $n = \dim_k B/\mathfrak{p}B$.

Soit $\{x_1, \ldots, x_m\} \subset B$ tels que $\{\overline{x_1}, \ldots, \overline{x_m}\}$ forme une k-base de $B/\mathfrak{p}$. Montrons que $\{x_1, \ldots, x_m\}$ forme aussi une K-base de L. Dans ce cas, nous aurons bien $m = n$.
• Supposons la famille $\{x_1, \ldots, x_m\}$ linéairement dépendante sur K. Alors, il existe $\alpha_i \in A$, $i = 1, \ldots, m$, non tous nuls, tels que

$$\alpha_1 x_1 + \cdots, \alpha_m x_m = 0.$$

Soit alors l'idéal $0 \neq \mathfrak{a} = (\alpha_1, \ldots, \alpha_m) \subset A$. Comme $\mathfrak{a}^{-1}\mathfrak{p} \neq \mathfrak{a}^{-1}$, on peut trouver $a \in \mathfrak{a}^{-1}$ tel que a $\notin \mathfrak{a}^{-1}\mathfrak{p}$ i.e. $\mathfrak{p} \nmid (a)\mathfrak{a} \subset A$. Ainsi les éléments $(a\alpha_i)_i$ ne sont pas tous dans $\mathfrak{p}$: la relation

$$a\alpha_1 x_1 + \cdots a\alpha_m x_m = 0 (\mathrm{mod}\ \mathfrak{p}),$$

n'est pas triviale dans k. Contradiction.

• Il reste maintenant à s'assurer que $\{x_1, \ldots, x_m\}$ engendre bien L en tant que K-espace vectoriel. Soit le A-module $M = x_1 B + \cdots + x_m B$ et soit $N = B/M$. Comme $B = M + \mathfrak{p}B$, on a

$$N = \mathfrak{p}N.$$

Le A-module N est de type fini. Soit $\{y_1, \ldots, y_r\}$ un système de générateurs de N. Alors il existe $\alpha_{i,j} \in \mathfrak{p}$ tels que

$$y_i = \sum_j^s \alpha_{i,j} y_j,$$

ou encore

$$\sum_i^s (\delta_{i,j} - \alpha_{i,j}) y_j = 0,$$

où $\delta_{i,j}$ est le symbole de Kronecker. Les formules de Cramer indiquent que pour tout j :

$$\det((\delta_{i,j} - \alpha_{i,j})_{i,j}) y_j = 0.$$

Or mod $\mathfrak{p}$, la quantité $d = \det((\delta_{i,j} - \alpha_{i,j})_{i,j})$ est non nulle. Ainsi $d \neq 0$ et $dN = 0$. Par conséquent, $dB \subset M$ et $\mathrm{L} \subset \mathrm{K}x_1 + \cdots + \mathrm{K}x_m$. □

Définition 2.5.11. — L'entier e_i est appelé indice de ramification de $\mathfrak{P}_i$ dans L/K et f_i est appelé degré résiduel de $\mathfrak{P}_i$ dans L/K.

2.5.3. Une recette. — Soit A un anneau de Dedekind (par exemple l'anneau des entiers d'un corps de nombres), $\mathrm{K} = \mathrm{Frac}(A)$. Soit L/K une extension de degré n que l'on suppose séparable (ce qui est toutjours vrai en caractéristique nulle), et soit B la fermeture de A dans L. D'après le théorème de l'elément primitif et la remarque 1.1.14, il existe $\theta \in B$ tel que $\mathrm{L} = \mathrm{K}(\theta)$. Alors l'anneau $A[\theta]$ est un sous-anneau de B.

Définition 2.5.12. — Le conducteur $\mathcal{F}$ de l'anneau $A[\theta]$ est l'idéal de B défini comme suit :

$$\mathcal{F} = \{x \in B \mid xB \subset A[\theta]\}.$$

L'idéal $\mathcal{F}$ est non nul car, par le lemme 1.2.11, $0 \neq \mathrm{d}(1, \ldots, \theta^{n-1}) \in \mathcal{F}$.

Remarque 2.5.13. — Il vient immédiatement : $B = A[\theta]$ si et seulement si $\mathcal{F} = B$.

Théorème 2.5.14. — *Soit* $\mathfrak{p}$ *un idéal premier non nul de* A *tel que* $(\mathcal{F}, \mathfrak{p}B) = 1$. *Soit* $P = \mathrm{Irr}(\theta, \mathrm{K})$ *et soit*

$$\overline{P} = \overline{P_1}^{e_1} \cdots \overline{P_g}^{e_g} \pmod{\mathfrak{p}}$$

la factorisation de P *dans* $A/\mathfrak{p}[X]$ *(les polynômes* $\overline{P_i}$ *sont irréductibles dans* $A/\mathfrak{p}[X]$*).*
Pour $i = 1, \ldots, g$, *fixons un relèvement* $P_i \in A[X]$ *de* $\overline{P_i}$.
Alors les idéaux

$$\mathfrak{P}_i = \mathfrak{p}B + P_i(\theta)B$$

sont les idéaux maximaux de B *au-dessus de* $\mathfrak{p}$. *De plus, le degré résiduel* f_i *de* $\mathfrak{P}_i$ *dans* L/K *est exactement le degré de* $\overline{P_i}$ *et on a*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Démonstration. — Posons $B' = A[\theta]$. Soit donc un idéal maximal $\mathfrak{p}$ de A avec $\mathfrak{p}B$ premier à $\mathcal{F}$.
Soit le morphisme naturel $\varphi : B' \to B/\mathfrak{p}B$.
Détaillons la surjectivité de φ. Comme $(\mathfrak{p}B, \mathcal{F}) = 1$, écrivons $1 = a + b$ avec $a \in \mathcal{F}$ et $b \in \mathfrak{p}B$. Soit $y \in B$. Alors $y = y(a + b) \equiv ay \pmod{\mathfrak{p}B}$ et par définition du conducteur, $ay \in B'$, d'où la surjectivité de φ. De la même façon, on a $\ker(\varphi) = \mathfrak{p}B'$.
Ainsi,

$$B'/\mathfrak{p}B' \simeq B/\mathfrak{p}B.$$

Soit le morphisme naturel

$$\psi : A[X] \to \mathrm{k}[X]/(\overline{P}),$$

où $\mathrm{k} = A/\mathfrak{p}$ et où $P = \mathrm{Irr}(\theta, \mathrm{K})$.
Alors le morphisme ψ est clairement surjectif et $\ker(\psi) = (\mathfrak{p}, P)$. Ainsi

$$B/\mathfrak{p}B \simeq B'/\mathfrak{p}B' = A[\theta]/\mathfrak{p}A[\theta] \simeq A[X]/(P, \mathfrak{p}) \simeq \mathrm{k}[X]/(\overline{P}),$$

et donc

$$\prod_{i=1}^{g'} B/(\mathfrak{P}_i)^{e'_i} \simeq \prod_{i=1}^{g} \mathrm{k}[X]/(\overline{P}^{e_i}) \tag{2}$$

si $\mathfrak{p}B = \prod_{i=1}^{g'} \mathfrak{P}_i^{e'_i}$ est la décomposition de l'idéal $\mathfrak{p}B$ et si $\overline{P} \equiv \prod_{i=1}^{g} \overline{P_i}^{e_i} \pmod{\mathfrak{p}}$ est la factorisation de P dans $\mathrm{k}[X]$. Détaillons ce dernier isomorphisme. Soit

$$\begin{array}{rcl} \varphi_i : B' = A[\theta] & \to & \mathrm{k}[X]/(\overline{P_i}) \\ f(\theta) & \mapsto & \overline{f} \pmod{\overline{P_i}}. \end{array}$$

Le morphisme φ_i est bien défini et est surjectif. Comme $\overline{P_i}$ est irréductible dans $\mathrm{k}[X]$, alors $\ker(\varphi_i) = P_i(\theta)B' + \mathfrak{p}B'$ est un idéal maximal de B' qui contient $\mathfrak{p}B'$. Soit maintenant le morphisme naturel

$$\varphi'_i : B'/(\mathfrak{p}B' + P_i(\theta)B') \to B/(\mathfrak{p}B + P_i(\theta)B).$$

Comme $(\mathfrak{p}, \mathcal{F}) = 1$, le morphisme φ'_i est un isomorphisme et ainsi l'idéal $\mathfrak{p}B + P_i(\theta)B$ est un idéal maximal de B contenant $\mathfrak{p}B$: c'est donc un idéal premier $\mathfrak{P}_i$ de B au-dessus de $\mathfrak{p}$. Notons ensuite que pour $i \neq j$, $\mathrm{k}[X]/(\overline{P_i}) \ncong \mathrm{k}[X]/(\overline{P_j})$ et ainsi $\mathfrak{P}_i \neq \mathfrak{P}_j$.

Posons donc $\mathfrak{P}_i = \mathfrak{p}B + P_i(\theta)B$.
Alors

$$\prod_{i=1}^{g} \mathfrak{P}_i^{e_i} \subset \mathfrak{p}B + \prod_{i=1}^{g} P_i(\theta)^{e_i} B = \mathfrak{p}B = \prod_{i=1}^{g'} \mathfrak{P}_i^{e'_i}.$$

Ainsi

$$\prod_{i=1}^{g'} \mathfrak{P}_i^{e'_i} \mid \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}.$$

Pour les degrés résiduels des idéaux premiers $\mathfrak{P}_i$, $i = \ldots, g$, il vient

$$f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}] = [\mathrm{k}[X]/(\overline{P_i}) : \mathrm{k}] = \deg(\overline{P_i}),$$

car $B/\mathfrak{P}_i \simeq A[X]/(\overline{P_i}, \mathfrak{p}) \simeq \mathrm{k}[X]/(\overline{P_i})$.
Après arrangement, il vient $g' \leq g$, $e'_i \leq e_i$ et pour $i \leq g$, $f_i = f'_i$. Or d'après (2),

$$\sum_{i=1}^{g} e_i f_i = \sum_{i=1}^{g'} e'_i f'_i,$$

d'où $g = g'$ et $e'_i = e_i$. □

Définition 2.5.15. — Conservons les notations du précédent théorème. Soit $\mathfrak{p}$ un premier de A et soit

$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

la factorisation de $\mathfrak{p}B$ dans B.

(i) Le premier $\mathfrak{p}$ de A est dit ramifié dans L/K s'il existe un indice de ramification e_i strictement plus grand que 1.
(ii) Le premier $\mathfrak{p}$ est dit totalement ramifié si $g = f_1 = 1$ et $e_1 = n$.
(iii) Le premier $\mathfrak{p}$ est dit inerte si $\mathfrak{p} = \mathfrak{P}$, i.e. $g = e_1 = 1$.
(iv) Le premier $\mathfrak{p}$ est dit totalement décomposé si $g = n$.

On en arrive à un résultat important.

Théorème 2.5.16. — *Soit A un anneau de Dedekind de corps des fractions* K. *Soit* L/K *une extension (séparable) de degré n et soit B la fermeture intégrale de A dans* L. *Alors il n'existe qu'un nombre fini d'idéaux premiers de A ramifiés dans* L/K.

Démonstration. — Prenons $\theta \in B$ tel que $\mathrm{L} = \mathrm{K}(\theta)$. Soit $P = \mathrm{Irr}(\theta, \mathrm{K})$. Soit $\mathfrak{p} \nmid \mathcal{F}$. Posons $\mathrm{k} = A/\mathfrak{p}$.
Soit $\mathfrak{p} \nmid \mathcal{F}$. La décomposition de $\mathfrak{p}B$ se lit dans la réduction de $P(\mathrm{mod}\ \mathfrak{p})$. Ainsi $\mathfrak{p}$ ne se ramifie pas dès que $\overline{P} \in A/\mathfrak{p}[X]$ n'a que des racines simples dans une clôture algébrique de $A/\mathfrak{p}$.
Or pour $\mathfrak{p} \nmid \mathrm{d}A$, le discriminant d mod $\mathfrak{p}$ n'est pas nul, ce qui siginifie que le polynôme $\overline{P}(\mathrm{mod}\ \mathfrak{p})$ n'a pas de racine double . Au final donc, seuls les premiers $\mathfrak{p}$ qui divisent l'idéal (non nul) $\mathrm{d}A$ peuvent éventuellement être ramifiés. □

Remarque 2.5.17. — Comme $\mathrm{d}(1, \ldots, \theta^{n-1}) \in \mathcal{F}$, on a ainsi que si $\mathfrak{p}$ est ramifié, alors $\mathfrak{p} \mid (\mathrm{d}(1, \ldots, \theta^{n-1}))$.

Définition 2.5.18. — Posons $k_i = B/\mathfrak{P}_i$ et $k = A/\mathfrak{p}$.
Le premier $\mathfrak{p}$ est dit non ramifiée dans L/K si pour $i = 1, \ldots, g$, on a que $e_i = 1$ et que l'extension des corps résiduels k_i/k est séparable.

Remarque 2.5.19. — Supposons que $B = A[\theta]$ et également que l'extension des corps résiduels k_i/k est séparable. Alors $\mathfrak{p}$ est non ramifié dans L/K si, et seulement si, $\mathfrak{p}|(\mathrm{d}(1, \ldots, \theta^{n-1}))$.

Dans le cas des corps de nombres, on a le théorème suivant :

Théorème 2.5.20. — *L'extension* $\mathrm{K}/\mathbb{Q}$ *est ramifiée en* $\mathfrak{p}$ *si et seulement si* $\mathfrak{p} \mid \mathrm{d}_{\mathrm{K}}$.

Démonstration. — Un sens a déja été vu (remarque 2.5.17). La réciproque est admise. □

2.5.4. Le cas galoisien. — Conservons le contexte de la section 2.5.3 et supposons que L/K est galoisienne. Soit $G = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$.

Soit $\mathfrak{a}$ un idéal fractionnaire de L et soit $g \in G$. On sait que $\mathfrak{a}$ un $\mathcal{O}_{\mathrm{L}}$-module de type fini engendré par deux éléments x et y.
On pose alors

$$g(\mathfrak{a}) = \mathfrak{a}^g = (g(x), g(y)),$$

l'idéal fractionnaire de L engendré par les éléments $g(x)$ et $g(y)$.

Pour tout idéal premier $\mathfrak{p}$ de A on note

$$S_{\mathfrak{p}} = \{\mathfrak{P},\ \mathfrak{P} \cap A = \mathfrak{p}\}$$

l'ensemble des idéaux premiers $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. On note très facilement que pour tout $g \in G$ l'idéal $g(\mathfrak{P})$ est un idéal premier de B. Comme

$$g(\mathfrak{P}) \cap A = g(\mathfrak{P} \cap A) = g(\mathfrak{p}) = \mathfrak{p},$$

on voit que $g(\mathfrak{P}) \in S_{\mathfrak{p}}$ i.e., le groupe de Galois opère sur $S_{\mathfrak{p}}$.

Définition 2.5.21. — Soit $\mathfrak{P}$ un idéal premier non nul de B. Alors $D_{\mathfrak{P}} = \{g \in G,\ g(\mathfrak{P}) = \mathfrak{P}\}$ est le groupe de décomposition de $\mathfrak{P}$ dans L/K.

Théorème 2.5.22. — *Soit* L/K *une extension galoisienne et soit* $\mathfrak{p}$ *un idéal premier non nul de* A. *Alors :*

(i) Le groupe de Galois $G = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ *opère transitivement sur* $S_{\mathfrak{p}}$.

(ii) Les indices de ramification $e(\mathfrak{P})$ *et degré résiduel* $f(\mathfrak{P})$ *ne dépendent pas de* $\mathfrak{P} \mid \mathfrak{p}$. *Si on les note* $e_{\mathfrak{p}}$ *et* $f_{\mathfrak{p}}$ *et si* $g_{\mathfrak{p}}$ *est le nombre des idéaux premiers* $\mathfrak{P} \mid \mathfrak{p}$, *alors on a*

$$e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} = [\mathrm{L} : \mathrm{K}]$$

et la factorisation de $\mathfrak{p}$ *dans* B *s'écrit*

$$\mathfrak{p}B = (\mathfrak{P}_1 \mathfrak{P}_2 \cdot \ldots \cdot \mathfrak{P}_{g_{\mathfrak{p}}})^{e_{\mathfrak{p}}}.$$

(iii) Si $\mathfrak{Q} = g(\mathfrak{P})$, alors $D_{\mathfrak{Q}} = g^{-1}D_{\mathfrak{P}}g$, et le groupe de décomposition $D_{\mathfrak{P}}$ est d'ordre $e_{\mathfrak{p}}f_{\mathfrak{p}}$.

Démonstration. — i) Soit $\mathfrak{P}$ un premier de B au-dessus de $\mathfrak{p}$. Supposons qu'il existe un premier $\mathfrak{Q}$ également au-dessus de $\mathfrak{p}$ tel que

$$\forall g \in G,\ g(\mathfrak{P}) \neq \mathfrak{Q}.$$

Choisissons, grâce au théorème des restes chinois, $x \in B$ tel que $x \in \mathfrak{Q}$ et tel que pour tout $g \in G$, $x \notin g(\mathfrak{P})$.
Alors $\mathrm{N}_{\mathrm{L/K}}(x) \in A \cap \mathfrak{Q} = \mathfrak{p} = A \cap \mathfrak{P}$ ce qui implique $g(x) \in \mathfrak{P}$ pour un certain élément g de G, d'où la contradiction.
ii) Soit $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$ la factorisation de $\mathfrak{p}$ dans B. Comme G opère transitivement sur $S_{\mathfrak{p}}$, pour tout i il existe $g_i \in G$ tel que $g_i(\mathfrak{P}_1) = \mathfrak{P}_i$. Donc g_i induit un isomorphisme entre $\mathrm{k}_{\mathfrak{P}_1} = B/\mathfrak{P}_1$ et $\mathrm{k}_{\mathfrak{P}_i} = B/\mathfrak{P}_i$, d'où $f(\mathfrak{P}_1/\mathfrak{p}) = f(\mathfrak{P}_i/\mathfrak{p})$. D'autre part, comme G agit trivialement sur $\mathfrak{p}$, on a

$$\mathfrak{p}B = g_i(\mathfrak{p}B) = (g_i(\mathfrak{P}_1))^{e_1} \cdot \ldots \cdot (g_i(\mathfrak{P}_g))^{e_g},$$

d'où $e_1 = e_i$. La formule $e_{\mathfrak{p}}f_{\mathfrak{p}}g_{\mathfrak{p}} = [\mathrm{L} : \mathrm{K}]$ résulte maintenant du théorème 2.5.9.
iii) La première partie est immédiate. Pour la seconde, cela repose sur le fait que le groupe G opère transitivement sur les idéaux premiers $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. En effet, fixons un premier $\mathfrak{P}|\mathfrak{p}$. Le fixateur de l'action de G sur $\mathfrak{P}$ est exactement le sous-groupe $D_{\mathfrak{P}}$ et il vient l'égalité $g = |G|/|D_{\mathfrak{P}}|$. □

2.5.5. L'automorphisme de Frobenius. — Revenons aux entiers des corps de nombres. Soit L/K une extension galoisienne de corps de nombres de degré n. Notons $G = \mathrm{Gal}(\mathrm{L/K})$. Fixons une premier $\mathfrak{P}$ de $\mathcal{O}_{\mathrm{L}}$ et soit $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_{\mathrm{K}}$. Soient les corps résiduels $\mathrm{k}_{\mathfrak{P}} := \mathcal{O}_{\mathrm{L}}/\mathfrak{P}$ et $\mathrm{k}_{\mathfrak{p}} := \mathcal{O}_{\mathrm{K}}/\mathfrak{p}$. On rappelle que $\mathrm{k}_{\mathfrak{P}}/\mathrm{k}_{\mathfrak{p}}$ est une extension de corps finis de degré $f_{\mathfrak{P}}$, donc galoisienne (et en fait cyclique).

Notons par $\mathrm{K}' := \mathrm{L}^{D_{\mathfrak{P}}}$ (c'est le corps de décomposition de $\mathfrak{P}$ dans L/K) et posons $\mathfrak{P}' = \mathcal{O}_{\mathrm{K}'} \cap \mathfrak{P}$. L'extension L/K′ est galoisienne de groupe de Galois $D_{\mathfrak{P}}$. Clairement $\mathfrak{P}'$ est un premier au-dessus de $\mathfrak{p}$. D'autre part, comme $D_{\mathfrak{P}}$ agit transivement sur les premiers de L au-dessus de $\mathfrak{P}'$, il vient que $\mathfrak{P}$ est l'unique premier de L au-dessus de $\mathfrak{P}'$.

En considérant le premier $\mathfrak{P}$ dans les extensions L/K et L/K′ (associé aux injections : $\mathcal{O}_{\mathrm{K}}/\mathfrak{p} \hookrightarrow \mathcal{O}_{\mathrm{K}'}/\mathfrak{P}' \hookrightarrow \mathcal{O}_{\mathrm{L}}/\mathfrak{P}$), on a $f_{\mathfrak{P}} \geq f'_{\mathfrak{P}}$ et $e_{\mathfrak{P}} \geq e'_{\mathfrak{P}}$, où $f'_{\mathfrak{P}}$ (respectivement $e_{\mathfrak{P}}$) est le degré résiduel (respectivement l'indice de ramification) de $\mathfrak{P}$ dans L/K′. Comme $e_{\mathfrak{P}} f_{\mathfrak{P}} = |D_{\mathfrak{P}}| = e'_{\mathfrak{P}} f'_{\mathfrak{P}}$, il vient alors $e_{\mathfrak{P}} = e'_{\mathfrak{P}}$ et $f_{\mathfrak{P}} = f'_{\mathfrak{P}}$. En particulier, on vient de montrer

Lemme 2.5.23. — *On a :* $\mathcal{O}_{\mathrm{K}}/\mathfrak{P} \simeq \mathcal{O}_{\mathrm{K}'}/\mathfrak{P}'$.

Soit $I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}},\ \sigma(x) \equiv x \pmod{\mathfrak{P}}, \forall x \in B\}$. C'est le sous-groupe d'inertie de $\mathfrak{P}$ dans L/K.

Proposition 2.5.24. — *On a un l'isomorphisme naturel* $D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(\mathrm{k}_{\mathfrak{P}}/\mathrm{k}_{\mathfrak{p}})$.

Démonstration. — Soit $\sigma \in D_{\mathfrak{P}}$. Alors, par restriction σ induit un élément de $\mathrm{Gal}(\mathrm{k}_{\mathfrak{P}}/\mathrm{k}_{\mathfrak{p}})$. Soit alors le morphisme $\psi : D_{\mathfrak{P}} \to \mathrm{Gal}(\mathrm{k}_{\mathfrak{P}}/\mathrm{k}_{\mathfrak{p}})$. Clairement, $\ker(\psi) = I_{\mathfrak{P}}$. Cherchons l'image de ψ. Notons, par le lemme 2.5.23, que $\mathrm{k}_{\mathfrak{p}} = \mathrm{k}_{\mathfrak{P}'}$. Soit $\theta \in \mathcal{O}_{\mathrm{L}}$ un relèvement de $\overline{\theta} \in \mathrm{k}_{\mathfrak{P}}$, où $\mathrm{k}_{\mathfrak{p}}(\overline{\theta}) = \mathrm{k}_{\mathfrak{P}}$ est un élément primitif de $\mathrm{k}_{\mathfrak{P}}/\mathrm{k}_{\mathfrak{p}}$. Soit $P = \mathrm{Irr}(\theta, \mathrm{K}')$ et soit $\overline{P} = \mathrm{Irr}(\overline{\theta}, \mathrm{k}_{\mathfrak{p}})$. Alors clairement $\overline{P}$ divise $P \pmod{\mathfrak{p}} \in \mathrm{k}_{\mathfrak{p}}[X]$. Ainsi, si $\overline{\beta}$ est un $\mathrm{k}_{\mathfrak{p}}$-conjugué de $\overline{\theta}$ *i.e.*, une racine de $\overline{P}$ dans $\mathrm{k}_{\mathfrak{P}}$, il existe une racine β de P, avec $\beta \in \mathcal{O}_{\mathrm{L}}$, car L/K′ est galoisienne, telle que $\beta \pmod{\mathfrak{P}} = \overline{\beta}$, ce qui signifie exactement que ψ est surjectif. D'où le résultat. □

Corollaire 2.5.25. — *On a* $\#I_{\mathfrak{P}} = e_{\mathfrak{P}}$. *Par conséquent si* $\mathfrak{P}$ *est non ramifié dans* L/K, *le groupe de décomposition* $D_{\mathfrak{P}}$ *est isomorphe à* $\mathrm{Gal}(\mathrm{k}_{\mathfrak{P}}/\mathrm{k}_{\mathfrak{p}})$.

Démonstration. — Ce qui précède indique que $e_{\mathfrak{P}} f_{\mathfrak{P}} = \#D_{\mathfrak{P}} = \#I_{\mathfrak{P}} f_{\mathfrak{P}}$, d'où $\#I_{\mathfrak{P}} = e_{\mathfrak{P}}$. Lorsque $\mathfrak{P}$ est non ramifié, il vient alors que $D_{\mathfrak{P}} \simeq \mathrm{Gal}(\mathrm{k}_{\mathfrak{P}}/\mathrm{k}_{\mathfrak{p}})$. □

Corollaire 2.5.26. — *Le premier* $\mathfrak{P}$ *est non ramifié dans* L/K *si et seulement si,* $I_{\mathfrak{P}} = \{e\}$.

Démonstration. — Immédiat. □

Définition 2.5.27. — L'unique élément $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ engendrant $D_{\mathfrak{P}}$ et vérifiant $\sigma_{\mathfrak{P}}(x) \equiv x^{|\mathrm{k}_{\mathfrak{p}}|} \pmod{\mathfrak{P}}$ est appelé automorphisme de Frobenius de $\mathfrak{P}$ dans L/K.

Remarque 2.5.28. — Si $\mathfrak{P}$ et $\mathfrak{P}'$ sont deux premiers au-dessus de $\mathfrak{p}$, alors $\sigma_{\mathfrak{P}}$ et $\sigma_{\mathfrak{P}'}$ sont conjugués dans Gal(L/K). En particulier, ils sont égaux si Gal(L/K) est un groupe abélien.

Proposition 2.5.29. — *Soit l'inclusion de corps de nombres* $\mathrm{K} \subset \mathrm{F} \subset \mathrm{L}$. *On suppose les extensions* L/K *et* F/K *galoisiennes. Soit* $\mathfrak{P}$ *un idéal premier de* L *et soit* $\mathfrak{P}' = \mathcal{O}_{\mathrm{F}} \cap \mathfrak{P}$. *Alors* $(\sigma_{\mathfrak{P}})_{|F} = \sigma_{\mathfrak{P}'} \in \mathrm{Gal}(\mathrm{F/K})$.

Démonstration. — Immédiat. □

2.5.6. Exemples. —

2.5.6.1. Décomposition dans les extensions quadratiques. — Soit $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, où d est un entier sans facteur carré. Si p est un nombre premier, alors

$$\mathfrak{p}\mathcal{O}_{\mathrm{K}} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

avec $2 = \sum_{i=1}^{g} e_i f_i$.

• Supposons $d \equiv 2, 3 (\mathrm{mod}\ 4)$. Alors $\mathcal{O}_{\mathrm{K}} = \mathbb{Z}[\sqrt{d}]$ et $\mathrm{Irr}(\sqrt{d}, \mathbb{Q}) = X^2 - d$. Alors pour $p \mid d$, le premier p est ramifié. Dans ce cas, $\mathfrak{p} = \mathfrak{P}^2$ avec $\mathfrak{P} = (p, \sqrt{d})$.
Si $p = 2$ et $d \equiv 3 (\mathrm{mod}\ 4)$, alors 2 est ramifié et $2\mathcal{O}_{\mathrm{K}} = (2, \sqrt{d} - 1)^2$. De même pour $d \equiv 2 (\mathrm{mod}\ 4)$, on obtient $2\mathcal{O}_{\mathrm{K}} = (\sqrt{d}, 2)^2$.
Si p est tel que $d \notin \mathbb{F}_p^2$, alors p est inerte, i.e. $p\mathcal{O}_{\mathrm{K}}$ est un idéal maximal. Enfin si $d \equiv a^2 (\mathrm{mod}\ p)$, (avec $p \nmid d$), alors p est totalement décomposé :

$$p\mathcal{O}_{\mathrm{K}} = \mathfrak{P}\mathfrak{P}',$$

avec $\mathfrak{P} = (\sqrt{d} - a, p)$ et $\mathfrak{P}' = (\sqrt{d} + a, p)$.
• Supposons maintenant $d \equiv 1 (\mathrm{mod}\ 4)$.
Alors $\mathcal{O}_{\mathrm{K}} = \mathbb{Z}[\theta]$, avec $\theta = \dfrac{1 + \sqrt{d}}{2}$; ainsi, $\mathrm{Irr}(\theta, \mathbb{Q}) = X^2 - X + \dfrac{1 - d}{4}$.
Soit $B = \mathbb{Z}[\sqrt{d}]$. Alors conducteur $\mathcal{F}$ de B est l'idéal $2\mathcal{O}_{\mathrm{K}}$.
Ainsi pour $p \neq 2$, la factorisation de $p\mathcal{O}_{\mathrm{K}}$ se lit dans la réduction de $X^2 - d \ (\mathrm{mod}\ p)$.
On se retrouve dans la situation précédente. Soit $p > 2$. Si $p \mid d$, le premier p est ramifié et $p\mathcal{O}_{\mathrm{K}} = (\sqrt{d}, p)^2$. Si d n'est pas un carré dans

$\mathbb{F}_p$, alors p est inerte. Enfin, si d est un carré dans $\mathbb{F}_p$, le premier p est totalement décomposé.
Il reste donc à traiter le cas $p = 2$. La factorisation de $2\mathcal{O}_\mathrm{K}$ se lit dans la factorisation de $P = \mathrm{Irr}(\theta, \mathbb{Q})$ dans $\mathbb{F}_2$. Ecrivons $d = 1 + 4\lambda$, avec $\lambda \in \mathbb{Z}$.
Si $\lambda \equiv 0 (\mathrm{mod}\ 2)$, i.e. $d \equiv 1 (\mathrm{mod}\ 8)$, alors $P = X(X-1) \in \mathbb{F}_2[X]$. Ainsi $2\mathcal{O}_\mathrm{K} = (\theta, 2)(\theta - 1, 2)$.
Si $\lambda \equiv 1 (\mathrm{mod}\ 2)$, i.e. $d \equiv 5 (\mathrm{mod}\ 8)$, alors $X^2 + X + 1$ est irréductible et $2\mathcal{O}_\mathrm{K}$ est inerte.

Exemple 2.5.30. — Soit $\mathrm{K} = \mathbb{Q}(\sqrt{-5})$. Alors $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\sqrt{-5}]$.
On a :

$$7\mathcal{O}_\mathrm{K} = \mathfrak{P}_7\mathfrak{P}_7'$$

avec $\mathfrak{P}_7 = (7, \sqrt{-5} + 3)$ et $\mathfrak{P}_7' = (7, \sqrt{-5} - 3)$ et

$$3\mathcal{O}_\mathrm{K} = \mathfrak{P}_3\mathfrak{P}_3'$$

avec $\mathfrak{P}_3 = (3, \sqrt{-5} - 1)$ et $\mathfrak{P}_3 = (3, \sqrt{-5} + 1)$.
Soit maintenant l'idéal $\mathfrak{a} = (1 + 2\sqrt{-5})\mathcal{O}_\mathrm{K}$. Comme $\mathrm{N}(\mathfrak{a}) = 21$, on en déduit que $\mathfrak{a} = \mathfrak{P}\mathfrak{Q}$ avec $\mathrm{N}(\mathfrak{P}) = 3$ et $\mathrm{N}(\mathfrak{Q}) = 7$. Alors $\mathfrak{P}$ est un idéal au-dessus de 3 et $\mathfrak{Q}$ un idéal au-dessus de 7.
Posons $x = 1 + 2\sqrt{-5}$. Comme $\sqrt{-3} \equiv 1 (\mathrm{mod}\ \mathfrak{P}_3)$, alors $x \equiv 0 (\mathrm{mod}\ \mathfrak{P}_3)$, ce qui signifie que $\mathfrak{P}_3 \mid (x)$.
Maintenant $\sqrt{-5} \equiv -3 (\mathrm{mod}\ \mathfrak{P}_7)$ alors $x \equiv -5 (\mathrm{mod}\ 7) \neq 0$. Ainsi $\mathfrak{P}_7 \nmid (x)$ et $\mathfrak{P}_7' \mid (x)$. Par conséquent

$$(x) = \mathfrak{P}_3\mathfrak{P}_7'.$$

2.5.6.2. Décomposition dans les extensions cyclotomiques. — Soit un nombre premier $\ell > 2$. Soit $\zeta = \zeta_\ell = \exp(2i\pi/\ell)$ une racine primitive ℓ-ème de l'unité.
On rappelle que $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\zeta]$ et que $\mathrm{Irr}(\zeta, \mathbb{Q}) = P = X^{\ell-1} + \cdots + X + 1$.
On a : $X^\ell - 1 = (X-1)P$.
Alors dans $\mathbb{F}_\ell[X]$, il vient immédiatement la factorisation suivante

$$\overline{P} = (X-1)^{\ell-1}.$$

Ainsi $\ell\mathcal{O}_\mathrm{K} = (\ell, \zeta - 1)^{\ell-1}$. Or pour $i = 1, \ldots, \ell - 1$, il vient $1 - \zeta^i \in (1-\zeta)\mathcal{O}_\mathrm{K}$ et ainsi $\ell \in (1-\zeta)\mathcal{O}_\mathrm{K}$ (voir la preuve du théoreme 1.3.9). Soit alors l'idéal maximal $\mathfrak{L} = (1-\zeta)$; il est principal et $\ell\mathcal{O}_\mathrm{K} = \mathfrak{L}^{\ell-1}$.

Soit maintenant un nombre premier $p \neq \ell$. Alors la factorisation de $p\mathcal{O}_{\mathrm{K}}$ se lit sur la factorisation de P dans $\mathbb{F}_p[X]$.
Remarquons pour commencer que P admet une racine dans $\mathbb{F}_p$ si et seulement si, toutes les racines de P sont dans $\mathbb{F}_p$ i.e., si et seulement si $\ell | p-1$. Dans ce cas, p est totalement décomposé :

$$p\mathcal{O}_{\mathrm{K}} = \mathfrak{P}_1 \cdots \mathfrak{P}_{\ell-1},$$

avec $\mathfrak{P}_i = (p, \zeta - i)$, $i = 1, \ldots, \ell - 1$.

Plus généralement, soit t le plus petit entier tel que $p^t \equiv 1 (\mathrm{mod}\ \ell)$. Notons encore par ζ une racine primitive ℓ-ème de l'unité dans $\overline{\mathbb{F}_p}$. Alors $\zeta \in \mathbb{F}_{p^t} - \mathbb{F}_{p^{t-1}}$. L'élément ζ est donc de degré t sur $\mathbb{F}_p$ i.e. $\deg(\mathrm{Irr}(\zeta, \mathbb{F}_p)) = t$. Et ainsi

$$P = \prod_{i=1}^{g} P_i \in \mathbb{F}_p[X],$$

où les polynômes P_i sont irréductibles sur $\mathbb{F}_p$ avec $\deg(P_i) = t$ (à noter que $(P_i, P_j) = 1$ pour $i \neq j$). En particulier $g = (\ell - 1)/t$.

Exemple 2.5.31. — Prenons $\mathrm{K} = \mathbb{Q}(\zeta_5)$. Soit alors $p = 11$. Alors comme $11 \equiv 1 (\mathrm{mod}\ 5)$, le premier 11 est totalement décomposé dans $\mathrm{K}/\mathbb{Q}$.
Par contre pour $p = 19$, $t = 2$. L'anneau $\mathbb{Z}[\zeta_5]$ contient deux idéaux premiers au-dessus de 19 chacun de degré résiduel 2.

CHAPITRE 3

GÉOMÉTRIE DES NOMBRES

3.1. Réseaux de $\mathbb{R}^n$

Soit $\{v_1, \cdots, v_m\}$ m -vecteurs indépendants de $\mathbb{R}^n$ et soit

$$\mathrm{H} = \{\sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z}\} \subset \mathbb{R}^n.$$

Alors H est un sous-groupe discret de $\mathbb{R}^n$ (muni de sa topologie naturelle).

Définition 3.1.1. — L'ensemble $\mathrm{P} = \{\sum_{i=1}^{m} \lambda_i v_i, 0 \leq \lambda_i \leq 1\}$ est appelé parallélotope de H associé à la base $\{v_1, \cdots, v_m\}$.

Théorème 3.1.2. — *Soit* $\mathrm{H} \subset \mathbb{R}^n$ *un sous-groupe discret de* $\mathbb{R}^n$*. Alors il existe une famille de vecteurs indépendants* $\{v_1, \cdots, v_m\} \subset \mathbb{R}^n$ *telle que* $\mathrm{H} = \{\sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z}\}$*. De plus,* m *est la dimension de l'espace vectoriel engendré par* H.

Démonstration. — Soit m la dimension du sous-espace de $\mathbb{R}^n$ engendré par les vecteurs de H. Soit $\{v_1, \cdots, v_m\}$ m vecteurs de H linéairement indépendants.
Posons $\mathrm{H}' = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ et soit P le parallélotope associé à $\{v_1, \cdots, v_m\}$. Alors P est compact ainsi $\mathrm{P} \cap \mathrm{H}$ est fini.

Soit $x = \sum_{i=1}^{n} \lambda_i v_i \in \mathrm{H}$. Pour $j \in \mathbb{Z}$, posons

$$x_j = j \cdot x - \sum_{i=1}^{m} [j\lambda_i] v_i,$$

où $[\cdot]$ désigne la partie entière. Alors $x_j \in \mathrm{H} \cap \mathrm{P}$.
Comme $\mathrm{P} \cap H$ est fini, il existe $j \neq k$, tels que $x_j = x_k$, i.e. pour $i = 1, \cdots, m$,

$$(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i].$$

Ainsi $\lambda_i \in \mathbb{Q}$.
D'autre part,

$$x = x_1 + \sum_{i} [\lambda_i] v_i,$$

i.e. $\mathrm{H} \subset \mathrm{P} \cap \mathrm{H} + \mathrm{H}'$. Ainsi H est un $\mathbb{Z}$-module de type fini.
En résumé

$$\mathrm{H} = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_r,$$

avec $r \geq m$ et

$$w_j = \sum_{i} \lambda_{i,j} v_i,$$

avec $\lambda_{i,j} \in \mathbb{Q}$. D'où une première partie du théorème. Il reste à préciser le rang de H.
Soit d un dénominateur commun aux éléments $\lambda_{i,j}$. Alors, pour $j = 1, \cdots, r$, il vient $dw_j \in \mathrm{H}'$, i.e. $d\mathrm{H} \subset \mathrm{H}'$. De cette inclusion on en déduit $r = m$. □

Définition 3.1.3. — Un sous-groupe discret de $\mathbb{R}^n$ de rang maximal n est appelé réseau de $\mathbb{R}^n$.

Remarque 3.1.4. — Si H est un réseau de $\mathbb{R}^n$, alors $\mathrm{H} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ et $\mathbb{R}^n = \mathbb{R}v_1 \oplus \cdots \oplus \mathbb{R}v_n$.

Définition 3.1.5. — Soit H un réseau de $\mathbb{R}^n$: $\mathrm{H} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$. Le sous-ensemble $\mathcal{P} = \{\sum_{i=1}^{n} \lambda_i v_i,\ 0 \leq \lambda_i < 1\}$ de $\mathbb{R}^n$ est appelé parallélotope fondamental (ou encore domaine fondamental) du réseau (associé à la base $\{v_1, \cdots, v_n\}$).

Soit $x = \sum_{i=1}^{n} \lambda_i v_i \in \mathbb{R}^n$, $\lambda_i \in \mathbb{R}$. Alors

$$x = \sum_i (\lambda_i - [\lambda_i]) v_i + \sum_i [\lambda_i] v_i.$$

Ainsi $x \in \mathcal{P} + \mathrm{H}$: tout point de $\mathbb{R}^n$ est congru modulo H à un point (et à un seul) de $\mathcal{P}$.

Notons par μ la mesure de Lebesgue sur $\mathbb{R}^n$.

Lemme 3.1.6. — *On a* $\mu(\mathcal{P}) = |\det(v_1, \cdots, v_n)|$. *En particulier, la quantité* $\mu(\mathcal{P})$ *est un invariant du réseau* H.

Démonstration. — C'est immédiat. □

Définition 3.1.7. — La quantité $\mu(\mathcal{P})$ est appelée volume du réseau H et est notée Vol(H).

***Théorème 3.1.8* (de Minkowski)**. — *Soit* H *un réseau de* $\mathbb{R}^n$ *et* S *un sous-ensemble mesurable de* $\mathbb{R}^n$ *tels que* $\mu(S) > \mathrm{Vol}(H)$. *Alors il existe deux éléments distincts* $x, y \in S$ *tels que* $x - y \in \mathrm{H}$.

Démonstration. — Soit $\{v_1, \cdots, v_n\}$ une base de H et $\mathcal{P}$ le parallélotope fondamental construit sur cette base.
Alors, nous avons vu que

$$S = S \bigcap \left(\bigcup_{h \in \mathrm{H}} \{h + \mathcal{P}\} \right),$$

la réunion étant disjointe. Ainsi

$$\mu(S) = \sum_{h \in \mathrm{H}} \mu(S \cap (h + \mathcal{P})).$$

Or $\mu(S \cap (h + \mathcal{P})) = \mu((S - h) \cap \mathcal{P}))$. Notons ensuite que les ensembles $(S - h) \cap \mathcal{P}$, $h \in \mathrm{H}$ ne peuvent pas être deux à disjoints : sinon,

$$\mu(\mathcal{P}) \geq \sum_{h \in \mathrm{H}} \mu((S - h) \cap \mathcal{P}) = \mu(S),$$

ce qui est à exclure par hypothèse.
Ainsi, il existe $h_1 \neq h_2$ tous deux dans H tels que

$$(S - h_1) \cap (S - h_2) \cap \mathcal{P} \neq \emptyset,$$

i.e., l'existence de $s_1, s_2 \in S$ tel que $s_1 - h_1 = s_2 - h_2$ ou encore $s_1 - s_2 \in \mathrm{H}$ et $s_1 \neq s_2$. □

Corollaire 3.1.9. — *Soit* H *un réseau de* $\mathbb{R}^n$ *et* S *une partie mesurable de* $\mathbb{R}^n$ *symétrique par rapport à l'origine* O *et convexe. Supposons satisfaite l'une des deux conditions suivantes :*

(i) $\mu(S) > 2^n \mathrm{Vol}(\mathrm{H})$ *;*

(ii) $\mu(S) \geq 2^n \mathrm{Vol}(\mathrm{H})$ *et* S *compacte.*

Alors $S \cap \mathrm{H}$ *contient un autre point que* O*.*

Démonstration. — (i) On applique le théorème de Minkowski à $S' = 1/2S$. Alors $\mu(S') = 1/2^n \mu(S) > \mathrm{Vol}(\mathrm{H})$. Il existe $x, y \in S'$, avec $x - y \neq O$ et $x - y \in \mathrm{H}$. Alors $z = x - y$ convient. En effet

$$z = \frac{2x + (-2y)}{2} \in S \cap \mathrm{H}$$

et ce par symétrie et convexité de H.

(ii) On applique le point (i) à $S_\varepsilon = (1 + \varepsilon)S$, pour $\varepsilon > 0$. Pour $r > 0$, soit $B(0, r)$ la boule ouverte de centre O et de rayon r. Soit r petit tel que $\mathrm{H} \cap B(O, r) = \{0\}$ et soit $\mathrm{H}' = \mathrm{H} - B(O, r)$. Alors pour tout $\varepsilon > 0$, il vient que $\mathrm{H}' \cap S_\varepsilon$ est non vide (et est fini). Ainsi

$$\bigcap_{\varepsilon > 0} (\mathrm{H}' \cap S_\varepsilon)$$

est non vide d'intersection $S \cap \mathrm{H}'$ car $S \cap \mathrm{H}'$ est compacte. □

3.2. Le plongement canonique d'un corps de nombres

Fixons un corps de nombres K, i.e. une extension de degré n de $\mathbb{Q}$.
Le corps K a n plongements σ_i dans $\mathbb{C}$.
Un plongement $\sigma_i : \mathrm{K} \to \mathbb{C}$ est dit réel si $\sigma(\mathrm{K}) \subset \mathbb{R}$. Sinon, σ_i est dit complexe.
Soit r_1 le nombre de plongements réels de K. Si σ est un plongement complexe de K alors $\mathrm{c} \circ \sigma$ est également un plongement complexe de K, différent de σ (ici c est la conjugaison complexe). Ainsi, les plongements complexes sont en nombre pair $2r_2$.

Au total, $r_1 + 2r_2 = n$ et le couple (r_1, r_2) est appelé signature du corps K.

Exemple 3.2.1. — Le corps $\mathbb{Q}(\sqrt[3]{2})$ a pour signature $(1, 1)$.

Par la suite, on numérotera les plongements σ_i comme suit :
pour $i = 1, \cdots, r_1$, σ_i est un plongement réel ;
pour $j = 1, \cdots, r_2$, $\sigma_{r_1+j} = \mathrm{c} \circ \sigma_{r_1+r_2+j}$.

Définition 3.2.2. — Le plongement canonique d'un corps de nombres K est l'application

$$\begin{array}{rcccc} \sigma : \mathrm{K} & \to & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} & \to & \mathbb{R}^n \\ x & \mapsto & X = \big(\sigma_1(x), \cdots, \sigma_{r_1+r_2}(x)\big) & \mapsto & f(X) \end{array}$$

où $f(..., x_i, ..., x_j) = (\cdots, x_i, \cdots, \Re(x_{r_1+i}), \mathrm{Im}(x_{r_1+i}(x)), \cdots)$ est l'isomorphisme naturel entre $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ et $\mathbb{R}^n$.

L'application σ est un homomorphisme d'anneaux qui est injectif.

Un simple calcul de déterminant permet de montrer la proposition :

Proposition 3.2.3. — *Si* M *est un sous-*$\mathbb{Z}$*-module libre de rang* n *de* K *et si* $\{v_1, \cdots, v_n\}$ *est une* $\mathbb{Z}$*-base de* M *alors* $\sigma(\mathrm{M})$ *est un réseau de* $\mathbb{R}^n$. *Le volume* $\mathrm{Vol}(\mathrm{M})$ *de* M *est donné par*

$$\mathrm{Vol}(\mathrm{M}) = 2^{-r_2} |\det\left((\sigma_i(v_j))_{i,j}\right)|,$$

où ici $i, j = 1, \cdots, n$.

Remarque 3.2.4. — La famille $\{v_1, \cdots, v_n\}$ forme une $\mathbb{Q}$-base de K.

Démonstration. — Il suffit de noter que si σ_j est complexe alors la partie réelle $\Re(\sigma_j(v_i))$ de $\sigma_j(v_i)$ vérifie

$$\Re(\sigma_j(v_i)) = \frac{\sigma_j(v_i) + \sigma_{r_2+j}(v_i)}{2}.$$

Idem pour la partie imaginaire.
Comme le déterminant est non-nul (corollaire 1.2.7), $\sigma(\mathrm{M})$ est bien un réseau de $\mathbb{R}^n$ de volume $2^{-r_2} |\det\left((\sigma_i(v_j))_{i,j}\right)|$. □

Théorème 3.2.5. — *Soit* K *un corps de nombres d'anneau des entiers* $\mathcal{O}_\mathrm{K}$. *Soit* $\mathfrak{a} \subset \mathcal{O}_\mathrm{K}$ *un idéal entier non nul. Alors le plongement canonique* $\sigma(\mathfrak{a})$ *de* $\mathfrak{a}$ *est un réseau de volume*

$$\mathrm{Vol}(\sigma(\mathfrak{a})) = 2^{-r_2}|\mathrm{d_K}|^{1/2}\mathrm{N}(\mathfrak{a}),$$

où $\mathrm{d_K}$ *est le discriminant absolu de* K.

Exemple 3.2.6. — Pour $\mathrm{K} = \mathbb{Q}(i)$, le plongement de $\mathcal{O}_\mathrm{K}$ donne le réseau cubique $\mathbb{Z}^2$. Pour $\mathrm{K} = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_\mathrm{K}$ donne le réseau hexagonal $\mathbb{Z}[j]$.

Démonstration. — On a vu que $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de rang n (corollaire 1.2.9). Ainsi d'après la proposition 3.2.3, $\sigma(\mathfrak{a})$ est bien un réseau de $\mathbb{R}^n$.
Si $\mathfrak{a} = \mathcal{O}_\mathrm{K}$, on sait que $\mathrm{d_K} = \det((\sigma_i(e_j))_{i,j})^2$, d'où le résultat.
Soit donc $\mathfrak{a} \subset \mathcal{O}_\mathrm{K}$ un idéal non nul de $\mathcal{O}_\mathrm{K}$. On sait qu'il existe une base $\{v_1, \cdots, v_n\}$ de $\mathcal{O}_\mathrm{K}$ et des entiers $\lambda_1, \cdots, \lambda_n$ tels que $\{\lambda_1 v_1, \cdots, \lambda_n v_n\}$ forme une $\mathbb{Z}$-base de $\mathfrak{a}$. Alors (voir la section 1.3.2)

$$\mathrm{N}(\mathfrak{a}) = \#\mathcal{O}_\mathrm{K}/\mathfrak{a} = |\lambda_1 \cdots \lambda_n|$$

et

$$\det((\sigma_i(\lambda_j v_j))_{i,j})^2 = \mathrm{d}(\lambda_1 v_1, \cdots, \lambda_n v_n) = (\lambda_1 \cdots \lambda_n)^2 \mathrm{d_K}.$$

Ainsi,

$$\begin{aligned} \mathrm{Vol}(\mathfrak{a}) &= 2^{-r_2}|\lambda_1 \cdots \lambda_n| \det((\sigma_i(\lambda_j v_j))_{i,j}) \\ &= 2^{-r_2}\mathrm{N}(\mathfrak{a})|\mathrm{d_K}|^{1/2} \end{aligned}$$

□

Exemple 3.2.7. — Partons de $\mathrm{K} = \mathbb{Q}(i)$ avec $\mathcal{O}_\mathrm{K} = \mathbb{Z} \oplus \mathbb{Z}i$. Alors $\sigma(\mathcal{O}_\mathrm{k}) = \mathbb{Z}(1,0) \oplus \mathbb{Z}(0,1)$, de volume 1 : c'est le réseau cubique.
Si l'on part de $\mathrm{K} = \mathbb{Q}(\sqrt{-3})$ avec $\mathcal{O}_\mathrm{K} = \mathbb{Z} \oplus \mathbb{Z}\dfrac{1+\sqrt{-3}}{2}$, alors $\sigma(\mathcal{O}_\mathrm{k}) = \mathbb{Z}(1,0) \oplus \mathbb{Z}(\dfrac{1}{2}, \dfrac{\sqrt{3}}{2})$, de volume $\sqrt{3}/2$: c'est le réseau hexagonal.
Si l'on part de $\mathrm{K} = \mathbb{Q}(\sqrt{3})$ avec $\mathcal{O}_\mathrm{K} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{3}$, il vient $\sigma(\mathcal{O}_\mathrm{K}) = \mathbb{Z}(1,1) \oplus \mathbb{Z}(\sqrt{3}, -\sqrt{3})$, de volume $2\sqrt{3}$.

3.3. Application à la détermination du groupe des classes

Commençons par donner un calcul de volume.

Lemme 3.3.1. — *Soit $t > 0$. Notons*

$$B_t = \{(y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},\ \sum_{i=1}^{r_1} |y_i| + 2\sum_{i=1}^{r_2} |z_i| \leq t\}.$$

Alors $B_t \subset \mathbb{R}^n$ est un sous-ensemble de $\mathbb{R}^n$, compact, symétrique par rapport à O, convexe et de volume

$$\mathrm{Vol}(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

Démonstration. — Le calcul du volume se fait à partir d'une double récurrence (sur r_1 et sur r_2). □

Proposition 3.3.2. — *Soit $\mathrm{K}/\mathbb{Q}$ un corps de nombres de signature (r_1, r_2). Soit $\mathfrak{a}$ un idéal entier (non nul) de $\mathcal{O}_\mathrm{K}$. Alors $\mathfrak{a}$ contient un élément non nul x tel que*

$$|\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\mathrm{d}_\mathrm{K}|^{1/2}\ \mathrm{N}(\mathfrak{a}).$$

Démonstration. — Soit σ le plongement canonique de K. Pour $t > 0$, notons B_t défini comme dans le lemme 3.3.1 puis prenons t tel que $\mu(B_t) = 2^n \mathrm{Vol}(\sigma(\mathfrak{a}))$ *i.e.*

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} = 2^{n-r_2} |\mathrm{d}_\mathrm{K}|^{1/2} \mathrm{N}(\mathfrak{a}).$$

D'après le théorème de Minkowski (en fait le corollaire 3.1.9), il existe $x \in \mathfrak{a}$, $x \neq 0$, tel que $\sigma(x) \in B_t$.
Or

$$\begin{aligned} |\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)| &= \prod_{i=1}^{r_1} |\sigma_i(x)| \cdots \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|^2 \\ &\leq \left(\frac{1}{n}\left(\sum_{i=1}^{r_1} |\sigma_i(x)| + 2\sum_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|\right)\right)^n \\ &\leq \frac{t^n}{n^n}, \end{aligned}$$

car $x \in B_t$. □

On en arrive à un résultat très utile en pratique (pour déterminer le groupe des classes d'un corps de nombres K).

Corollaire 3.3.3. — *Toute classe d'idéaux du groupe des classes* $\mathrm{Cl_K}$ *de* K *contient un idéal entier* $\mathfrak{a}$ *tel que*

$$\mathrm{N}(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\mathrm{d_K}|^{1/2}.$$

En particulier le groupe $\mathrm{Cl_K}$ *est fini.*

Démonstration. — Soit C une classe de $\mathrm{Cl_K}$ et soit $\mathfrak{b}$ un idéal fractionnaire de K représentant C. De $\mathfrak{b}^{-1}\mathfrak{b} = \mathcal{O}_K$, on a que $\mathfrak{b}^{-1}$ est l'un des représentants de la classe C^{-1}. On peut trouver un entier y de $\mathcal{O}_\mathrm{K}$, tel $(y)\mathfrak{b}^{-1} \subset \mathcal{O}_\mathrm{K}$ *i.e.*, $(y)\mathfrak{b}^{-1}$ est un idéal entier. Or $(y)\mathfrak{b}^{-1}$ et $\mathfrak{b}^{-1}$ sont dans la même classe C^{-1}. Ainsi, on peut supposer que $\mathfrak{b}^{-1}$ est entier.
D'après la proposition 3.3.2, il existe $x \in \mathfrak{b}^{-1}$, x non nul, tel que

$$|\mathrm{N_{K/\mathbb{Q}}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\mathrm{d_K}|^{1/2}\, \mathrm{N}(\mathfrak{b}^{-1}).$$

Comme $x \in \mathfrak{b}^{-1}$, l'idéal $\mathfrak{a} = (x)\mathfrak{b}$ est un idéal entier de norme

$$\mathrm{N}(\mathfrak{a}) = \mathrm{N}((x)\mathfrak{b}) = \mathrm{N}((x))\mathrm{N}(\mathfrak{b}) = |\mathrm{N_{K/\mathbb{Q}}}(x)|\mathrm{N}(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\mathrm{d_k}|^{1/2},$$

car de $(x)\mathfrak{b}\mathfrak{b}^{-1} = (x)$, il vient $\mathrm{N}(((x)\mathfrak{b}) = \mathrm{N}((x))\mathrm{N}(\mathfrak{b})$. On conclut en notant que les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont dans la même classe C de $\mathrm{Cl_K}$.

La finitude de $\mathrm{Cl_K}$ est alors immédiate : elle repose sur le fait qu'il n'y a qu'un nombre d'idéaux premiers de norme bornée par une constance D. □

Pour terminer ce paragraphe, donnons deux résultats importants pour les corps de nombres.

Proposition 3.3.4. — *Soit* K *un corps de nombres et* $n = [\mathrm{K} : \mathbb{Q}]$. *Alors*

$$|\mathrm{d_K}| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

Démonstration. — Cela se déduit du corollaire 3.3.3 et du fait que pour tout idéal entier $\mathfrak{a}$, $\mathrm{N}(\mathfrak{a}) \geq 1$. □

***Corollaire 3.3.5* (Hermite-Minkowski).** — *Pour tout corps de nombres* $\mathrm{K} \neq \mathbb{Q}$*, il vient* $|\mathrm{d_K}| > 1$*. Ainsi, toute extension non triviale de corps de nombres* $\mathrm{K}/\mathbb{Q}$ *est ramifiée.*

Démonstration. — La première partie de l'assertion provient de la proposition 3.3.4 et la seconde du théorème 2.5.20. □

3.4. Exemples

3.4.1. Le cas des corps quadratiques. —

3.4.1.1. — Soit un corps quadratique $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, où d est entier sans facteur carré. Alors $\mathrm{Cl_K}$ est trivial dès lors que

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{1}{2}|\mathrm{d_K}|^{1/2} < 2.$$

En se rappelant que $\mathrm{d_K} = d$ si $d \equiv 1 (\mathrm{mod}\ 4)$, et $\mathrm{d_K} = 4d$ sinon, on obtient que l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est principal pour $d = -1, -2, -3, -7, -11, 2, 3, 5, 13$.

Remarque 3.4.1. — Il y a exactement neuf corps quadratiques imaginaires dont le groupe des classes est trivial :

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

On a même (d'après Brauer-Siegel) que $\log|\mathrm{Cl_K}| \sim_{|d|\to\infty} \log\sqrt{|\mathrm{d_K}|}$, lorsque $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ varie dans la famille des corps quadratiques imaginaires.
Mais on pense (conjecture de Gauss) qu'il existe une infinité de corps quadratiques réels dont le groupe des classes est trivial.

3.4.1.2. — Détaillons un exemple non trivial. Soit $\mathrm{K} = \mathbb{Q}(\sqrt{-17})$. Alors $\mathcal{O}_\mathrm{K} = \mathcal{O} = \mathbb{Z}[\sqrt{-17}]$ et $|\mathrm{d_K}| = 68$. D'après la proposition 3.3.2, toute classe de $\mathrm{Cl_K}$ contient un idéal entier $\mathfrak{a}$ de norme

$$\mathrm{N}(\mathfrak{a}) \leq \frac{4 \cdot \sqrt{68}}{2\pi} \approx 5,24.$$

Ainsi, il est nécessaire de connaître la décomposition des premiers p, pour $p = 2, 3, 5$.
L'idéal $2\mathcal{O} = \mathfrak{p}_2^2$ est ramifié.

Comme $-17 \equiv 1 (\text{mod } 3)$, il vient que $3\mathcal{O} = \mathfrak{p}_3\mathfrak{q}_3$.
Enfin, $-15 \equiv -2 (\text{mod } 5)$ qui n'est pas un carré dans $\mathbb{F}_5$, alors $5\mathcal{O}$ est maximal. Au final, les seuls idéaux entiers de norme plus petite que 5 sont :

$$\mathcal{O}_\mathrm{K}, \mathfrak{p}_2, \mathfrak{p}_2^2, \mathfrak{p}_3, \mathfrak{q}_3.$$

(A noter que $\mathrm{N}(\mathfrak{p}_2\mathfrak{p}_3) = 6$ et que $\mathrm{N}((5)) = 25$.)

Au total, Cl_K est un groupe abélien qui contient au plus 5 éléments... la liste est donc courte !

Cherchons l'ordre de $\mathfrak{p}_2$ dans Cl_K. Comme $\mathfrak{p}_2^2 = (2)$, l'ordre de $\mathfrak{p}_2$ divise 2. Supposons $\mathfrak{p}_2$ principal. Alors il existe un entier $x \in \mathcal{O}$ tel que $(x) = \mathfrak{p}_2$, ce qui équivaut à $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x) = 2$.
Ecrivons $x = a + b\sqrt{-17}$, avec $a, b \in \mathbb{Z}$. Alors $\mathrm{N}_{\mathrm{K}/\mathbb{Q}} = a^2 + 17b^2$, et on voit que l'équation $a^2 + 17b^2 = 2$ n'a pas de solution. Ainsi, $\mathfrak{p}_2$ n'est pas principal et (la classe de) $\mathfrak{p}_2$ est d'ordre 2.

Cherchons l'ordre de $\mathfrak{p}_3$ dans Cl_K. A-t'on $\mathfrak{p}_3$ principal ? Ceci équivaut à ce que l'équation $a^2 + 17b^2 = 3$ ait une solution dans $\mathbb{Z}$. Donc $\mathfrak{p}_3$ et $\mathfrak{q}_3$ ne sont pas principaux.
Regardons $\mathfrak{p}_3^2$. A-t'on $\mathfrak{p}_3^2 = (x)$? Ceci équivaut à résoudre dans $\mathbb{Z}$ l'équation : $a^2 + 17b^2 = 9$. Les solutions sont ± 3. Or $(3) = \mathfrak{p}_3\mathfrak{q}_3 \neq \mathfrak{p}_3^2$. Donc $\mathfrak{p}_3^2$ n'est pas principal.
L'idéal $\mathfrak{p}_3$ ne peut pas être d'ordre 3 car sinon Cl_K contiendrait un sous-groupe d'ordre 6... or $|\mathrm{Cl}_\mathrm{K}| \leq 5$.
Donc $\mathfrak{p}_3$ est nécessairement d'ordre 4. Soyons plus explicite. On cherche à résoudre $\mathfrak{p}_3^4 = (x)$, ceci équivaut à résoudre dans $\mathbb{Z}$: $a^2 + 17b^2 = 81$. Alors $a = \pm 8$ et $b = \pm 1$ sont des solutions non triviales. Fixons $\mathfrak{p}_3 = (3, \sqrt{-17} - 1)$ et $\mathfrak{q}_3 = (3, \sqrt{-17} + 1)$. Alors

$$\mathfrak{p}_3^4 = (8 + \sqrt{-17}), \quad \mathfrak{q}_3^4 = (8 - \sqrt{-17}).$$

(Pour ce faire, on utilise le fait que $\sqrt{-17} \equiv 1 (\text{mod } \mathfrak{p}_3)$ et $\sqrt{-17} \equiv -1 (\text{mod } \mathfrak{q}_3)$.)

Ainsi, Cl_K est un groupe d'ordre au plus 5 qui contient un élément d'ordre 4, alors $\mathrm{Cl}_\mathrm{K} =< \mathrm{Cl}(\mathfrak{p}_3) > \simeq \mathbb{Z}/4\mathbb{Z}$.

A noter que comme $\mathfrak{p}_3\mathfrak{q}_3 = (3)$, alors la classes de $\mathfrak{q}_3$ est l'inverse de celle de $\mathfrak{p}_3$. Puis que $\mathrm{Cl}(\mathfrak{p}_3^2) = \mathrm{Cl}(\mathfrak{p}_2)$. Donnons une relation explicite. Pour

ce faire, il faut de trouver un élément entier x de norme 18. Soit alors $x = 1 - \sqrt{-17}$. Cet élément est bien de norme 18. Notons que $\mathfrak{q}_3 \nmid (x)$: en effet, comme $\sqrt{-17} \equiv -1 (\mathrm{mod}\ \mathfrak{q}_3)$, il vient

$$1 - \sqrt{-17} \equiv 2 (\mathrm{mod}\ \mathfrak{q}_3) \neq 0 (\mathrm{mod}\ \mathfrak{q}_3).$$

Ainsi, l'idéal principal (x) s'écrit

$$(x) = \mathfrak{p}_2 \mathfrak{p}_3^2,$$

ce qui confirme bien que $\mathrm{Cl}(\mathfrak{p}_3^2) = \mathrm{Cl}(\mathfrak{p}_2)^{-1} = \mathrm{Cl}(\mathfrak{p}_2)$ car $\mathfrak{p}_2$ est d'ordre 2.

3.4.1.3. — Soit le corps $\mathrm{K} = \mathbb{Q}(\sqrt{10})$. On rappelle que $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\sqrt{10}]$. Alors par la proposition 3.3.2, on sait que toute classe de Cl_K contient un idéal entier $\mathfrak{a}$ de norme plus petite que 3.
Ici 2 est ramifié : $2\mathcal{O}_\mathrm{K} = \mathfrak{p}_2^2$. Est ce que $\mathfrak{p}_2$ est principal ? Ceci équivaut à résoudre l'équation diophantienne

$$a^2 - 10b^2 = \pm 2,\ a, b \in \mathbb{Z}. \tag{3}$$

Or modulo 5, l'équation (3) n'a pas de solution et ainsi $\mathfrak{p}_2$ n'est pas principal : $\mathrm{Cl}(\mathfrak{p}_2)$ est d'ordre 2 dans Cl_K.
Idem pour les premiers de $\mathbb{Z}[\sqrt{10}]$ au-dessus de 3, i.e. $\mathfrak{p}_3 = (3, \sqrt{10} - 1)$ et $\mathfrak{q}_3 = (3, \sqrt{10} + 1)$.
On note ensuite que $(2 + \sqrt{10}) = \mathfrak{p}_3 \mathfrak{p}_2$ et $(2 - \sqrt{10}) = \mathfrak{q}_3 \mathfrak{p}_2$. Ainsi, $\mathrm{Cl}_\mathrm{K} = \langle \mathrm{Cl}(\mathfrak{p}_2) \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

3.4.2. Le cas des corps cyclotomiques. — Soit un nombre premier $\ell > 3$ et soit $\mathrm{K} = \mathbb{Q}(\zeta_\ell)$. Alors $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\zeta_\ell]$, $r_2 = (\ell - 1)/2$ et $|\mathrm{d}_\mathrm{K}| = \ell^{\ell-2}$. Posons

$$r_\ell = \left(\frac{4}{\pi}\right)^{r_2} \frac{(\ell-1)!}{(\ell-1)^{\ell-1}} \ell^{(\ell-1)/2}.$$

On rappelle que toute classe de Cl_K contient un idéal entier $\mathfrak{a}$ de norme plus petite que r_ℓ.
Il vient

ℓ	3	5	7	11
$r_\ell <$	2	4	11	196

Ainsi, immédiatement, $\mathbb{Z}[\zeta_3]$ est principal.

Prenons $\ell = 5$. Alors $P = X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{F}_2$ et dans $\mathbb{F}_3$. Ainsi, le seul idéal entier $\mathfrak{a}$ de $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\zeta_5]$ de norme plus

petite que 4 est $\mathfrak{a} = \mathcal{O}_K$. Le groupe des classes Cl_K de K est trivial : l'anneau $\mathbb{Z}[\zeta_5]$ est principal.

Prenons $\ell = 7$. Soit $P = X^6 + X^5 + \cdots + X + 1 = \mathrm{Irr}(\zeta_7, \mathbb{Q})$.
Alors $P = (X^3+X+1)(X^3+X^2+1) \in \mathbb{F}_2[X]$. Il existe donc deux idéaux premiers $\mathfrak{p}_2$ et $\mathfrak{q}_2$ de $\mathbb{Z}[\zeta_7]$ au dessus de 2. Or $\mathrm{N}_{K/\mathbb{Q}}(1 + \zeta_7 + \zeta_7^3) = 8$ et $\mathrm{N}_{K/\mathbb{Q}}(1+\zeta_7^2+\zeta_7^3) = 8$, par conséquent les idéaux $\mathfrak{p}_2$ et $\mathfrak{q}_2$ sont principaux.
On note ensuite que P est irréductible dans $\mathbb{F}_3$ et $\mathbb{F}_5$. Enfin, 7 est totalement ramifié et $\mathfrak{p}_7 = (1 - \zeta_7)$.
En conclusion, les seuls idéaux de normes plus petite que 10 sont : $\mathfrak{a} = \mathcal{O}_K$, $\mathfrak{p}_2$, $\mathfrak{q}_2$ et $\mathfrak{p}_7$.
Le groupe des classes de $\mathbb{Z}[\zeta_7]$ est trivial et l'anneau $\mathbb{Z}[\zeta_7]$ est principal.

Remarque 3.4.2. — A savoir : il n'y a qu'un nombre fini de corps cyclotomiques $\mathbb{Q}(\zeta_n)$ dont l'anneau des entiers est principal.

3.5. Le théorème d'Hermite

***Théorème 3.5.1* (Hermite).** — *Il n'y a qu'un nombre fini d'extensions* $K/\mathbb{Q}$ *de discriminant* d *donné (dans une clôture algébrique* $\overline{\mathbb{Q}}$ *fixée).*

Démonstration. — D'après la proposition 3.3.4, le degré n de $K/\mathbb{Q}$ est borné. On peut ainsi se donner n et la signature (r_1, r_2). Soit K un corps de nombres de signature (r_1, r_2) et de discriminant donné d.
Dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, considérons l'ensemble B suivant :
(i) Si $r_1 > 0$,

$$B = \{(y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2}), |y_1| \leq c/2, |y_i| \leq 1/2, i > 1, |z_j| \leq 1/2\},$$

où $c = 2^n \left(\frac{\pi}{2}\right)^{-r_2} |\mathrm{d}|^{1/2}$.
(ii) Si $r_1 = 0$,

$$B = \{(z_1, \cdots, z_{r_2}), |z_1 - \overline{z_1}| \leq b/2, |z_1 + \overline{z_1}| \leq 1/2, |z_j| \leq 1/2, j > 1\},$$

où $b = 2^n \left(\frac{2}{\pi}\right)^{-r_2} \frac{\pi}{4} |\mathrm{d}|^{1/2}$.
Alors les ensembles B sont compacts, symétriques par rapport à O, convexes et de volume

$$\mathrm{Vol}(B) = 2^n 2^{-r_2} |\mathrm{d}|^{1/2}.$$

Comme $\mathrm{Vol}(\mathcal{O}_\mathrm{K}) = 2^{-r_2}|\mathrm{d}|^{1/2}$, d'après le théorème de Minkowski, il existe un entier $x \neq 0$ tel que $\sigma(x) \in B$.
Supposons $r_1 > 0$. Alors, comme $|\mathrm{N}_{\mathrm{K}/\mathbb{Q}}x| \geq 1$, on en déduit que $|\sigma_1(x)| \geq 2^{n-1}$ et ainsi que $\sigma_1(x) \neq \sigma_i(x)$, pour $i \geq 2$. Ceci implique que $\mathrm{K} = \mathbb{Q}(x)$. De même quand $r_1 = 0$, on obtient, pour $i \geq 2$, $\sigma_1(x) \neq \sigma_i(x)$ et ainsi $\mathrm{K} = \mathbb{Q}(x)$.

D'autre part, pour tout i, $|\sigma_i(x)| \leq c(\mathrm{d}, n)$ et ainsi les fonctions symétriques élémentaires en les $\sigma_i(x)$ de degré n sont bornées. Ces fonctions correspondent aux coefficients de $\mathrm{Irr}(x, \mathbb{Q})$ et sont à valeurs dans $\mathbb{Z}$. Il n'y a donc qu'un nombre fini de tels polynômes donc de corps K à n et $\mathrm{d}_\mathrm{K} = d$ donnés. Comme n est borné, le théorème s'en déduit. □

3.6. Le groupe des unités d'un anneau d'entiers

Soit K un corps de nombres de degré n (et de signature (r_1, r_2)). Dans cette section nous allons étudier le groupe des unites $\mathcal{O}_\mathrm{K}^\times$ de $\mathcal{O}_\mathrm{K}$.

Lemme 3.6.1. — *Soit $x \in \mathcal{O}_\mathrm{K}$. L'élément x est une unité de $\mathcal{O}_\mathrm{K}$ si et seulement si $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}x = \pm 1$.*

Démonstration. — Soit $x \in \mathcal{O}_\mathrm{K}^\times$. Alors il existe $y \in \mathcal{O}_\mathrm{K}$ tel que $xy = 1$. En prenant la norme, on obtient $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}x\mathrm{N}_{\mathrm{K}/\mathbb{Q}}y = 1$. On conclut en notant que $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}x$ et $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}y$ sont dans $\mathbb{Z}$.

Réciproquement. Comme $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}x = \pm 1$, alors

$$\mathrm{Irr}(x, \mathbb{Q}) = X^m + a_{m-1}X^{m-1} \cdots \pm 1 \in \mathbb{Z}[X].$$

Ainsi $xy = \pm 1$, avec $y = x^{m-1} + a_{m-1}x^{m-2} + \cdots + a_1 \in \mathcal{O}_\mathrm{K}$. □

3.6.1. Le plongement logarithmique d'un corps de nombres. — Considérons l'application

$$\mathcal{L} : \ \mathrm{K}^\times \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \mathbb{R}^{r_1+r_2}$$

$$x \longmapsto \sigma(x) = (x_1, \cdots, x_{r_1+r_2}) \longmapsto (\log|x_1|, \cdots, \log(|x_{r_1+r_2}|)$$

C'est un morphisme de groupes : c'est le plongement logarithmique de $\mathrm{K}^\times$.

Grâce à $\mathcal{L}$, nous allons pouvoir montrer le :

***Théorème 3.6.2* (de Dirichlet).** — *Soit* K *un corps de nombres de degré* n *et de signature* (r_1, r_2). *Notons par* $\mathcal{O}_\mathrm{K}$ *l'anneau des entiers de* K. *Alors*

$$\mathcal{O}_\mathrm{K}^\times \simeq \mu_\mathrm{K} \times \mathbb{Z}^{r_1+r_2-1},$$

où $\mu_\mathrm{k} = \{x \in \mathrm{K}^\times, \exists k \in \mathbb{N}, x^k = 1\}$ *est le groupe des racines de l'unité de* K. *Le groupe* μ_K *est un groupe cyclique fini.*

Démonstration. — Nous allons regarder la restriction de $\mathcal{L}$ à $\mathcal{O}_\mathrm{K}^\times$.

Commençons par noter que μ_K est fini : cela provient du fait (associé à $[\mathrm{K} : \mathbb{Q}] < \infty$) que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \to \infty$ avec n.
Pour la cyclicité, on utilise le résultat bien connu suivant : tout sous-groupe fini du groupe multiplicatif d'un corps K est cyclique.

Ensuite, clairement $\mathcal{L}(\mu_\mathrm{K}) = 0$.
Réciproquement. Supposons que pour tout $x \in \mathcal{O}_\mathrm{K}^\times$, $\mathcal{L}(x) = 0$. Alors pour tout i, $|\sigma_i(x)| = 1$. Ainsi, les coefficients des polynômes irréductibles $\mathrm{Irr}(x, \mathbb{Q})$ des éléments $x \in \ker(\mathcal{L})$ sont bornés par une constante ne dépendant que de n.
Ainsi, $\ker(\mathcal{L})$ ne contient qu'un nombre fini d'éléments. Par conséquent, pour tout $x \in \ker(\mathcal{L})$, il existe deux entiers distincts k et m tels que $x^m = x^n$ (car $x^k \in \ker(\mathcal{L})$), i.e. $x \in \mu_\mathrm{K}$.
Ainsi

$$\ker(\mathcal{L}_{|\mathcal{O}_\mathrm{K}^\times}) = \mu_\mathrm{K}.$$

Pour les mêmes raisons que le point précédent, quelque soit le compact D de $\mathbb{R}^{r_1+r_2}$, il n'existe qu'un nombre fini d'éléments $x \in \mathcal{O}_\mathrm{K}^\times$ tels que $\mathcal{L}(x) \in D$. Ainsi $\mathcal{L}(\mathcal{O}_\mathrm{K}^\times)$ est un sous-groupe discret.

En conséquence, $\mathcal{L}(\mathcal{O}_\mathrm{K}^\times)$ est isomorphe à $\mathbb{Z}^r$, avec $r \leq r_1 + r_2$ et ainsi

$$\mathcal{O}_\mathrm{K}^\times \simeq \mu_\mathrm{K} \times \mathbb{Z}^r.$$

Il nous reste à montrer que $r = r_1 + r_2 - 1$.

Soit $x \in \mathcal{O}_\mathrm{K}^\times$. Nous avons vu que $\mathrm{N}_{\mathrm{K}/\mathbb{Q}} x = \pm 1$ et ainsi,

$$\mathcal{L}(\mathcal{O}_\mathrm{K}^\times) \subset \{(x_1, \cdots, x_{r_1+r_2}) \mid \sum_{i=1}^{r_1} x_i + 2 \sum_{i=r_1+1}^{r_1+r_2} x_i = 0\},$$

i.e. que $\mathcal{L}(\mathcal{O}_{\mathrm{K}}^{\times})$ est dans un hyperplan de $\mathbb{R}^{r_1+r_2}$. Par conséquent $r \leq r_1 + r_2 - 1$ et il nous reste à montrer que $\mathcal{L}(\mathcal{O}_{\mathrm{K}}^{\times})$ contient $r_1 + r_2 - 1$ vecteurs linéairement indépendants.

Lemme 3.6.3. — *Soit $1 \leq k \leq r_1 + r_2$. Alors pour tout $x \in \mathcal{O}_{\mathrm{K}}$, $x \neq 0$, il existe $\beta \in \mathcal{O}_{\mathrm{K}}$, $\beta \neq 0$, tel que*

$$|\mathrm{N}_{\mathrm{K}/\mathbb{Q}}\beta| \leq \left(\frac{2}{\pi}\right)^{r_2} |\mathrm{d}_{\mathrm{K}}|^{1/2},$$

et tel que si $\mathcal{L}(x) = (x_1, \cdots, x_{r_1+r_2})$ et $\mathcal{L}(\beta) = (\beta_1, \cdots, \beta_{r_1+r_2})$ alors, pour $i \neq k$, on a : $\beta_i \leq x_i$.

Démonstration. — Soit

$$B = \{(x_1, \cdots, x_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_i| \leq c_i, i = 1, \cdots, r_1, |x_j|^2 \leq c_j, \\ j = r_1 + 1, \cdots, r_1 + r_2\}$$

pour certains réels c_i. Alors $\mathrm{Vol}(B) = 2^{r_1}\pi^{r_2}c_1 \cdots c_{r_1+r_2}$.
Choisissons maintenant les éléments c_i tels que

$$2^{r_1}\pi^{r_2}c_1 \cdots c_{r_1+r_2} = 2^n \mathrm{Vol}(\mathcal{O}_{\mathrm{K}}).$$

Par le théorème de Minkowski, il existe un élément $\beta \neq 0$, tel que $\sigma(\beta) \in \sigma(\mathcal{O}_{\mathrm{K}}) \cap B$.
Il suffit alors d'imposer que pour $i \neq k$, $0 < c_i < e^{x_i}$. □

Lemme 3.6.4. — *Soit $1 \leq k \leq r_1 + r_2$. Il existe $x \in \mathcal{O}_{\mathrm{K}}^{\times}$ tel que pour $i \neq k$, on ait $x_i < 0$, où $\mathcal{L}(x) = (x_1, \cdots, x_{r_1+r_2})$.*

Démonstration. — Posons $s = r_1 + r_2$.
Soit $\alpha = \alpha^{(1)} \in \mathcal{O}_{\mathrm{K}}$, $\alpha \neq 0$.
Posons $\mathcal{L}(\alpha) = (\alpha_1, \cdots, \alpha_s)$. D'après le lemme 3.6.3, il existe $\alpha^{(2)} \in \mathcal{O}_{\mathrm{K}}$ tel que

$$\alpha_i^{(2)} < \alpha_i^{(1)},$$

pour $i \neq k$, où $\mathcal{L}(\alpha^{(2)}) = (\alpha_1^{(2)}, \cdots, \alpha_s^{(2)})$. En continuant, on construit une famille d'éléments $(\alpha^{(i)})_i \in \mathcal{O}_{\mathrm{K}}$ aussi grande que possible et vérifiant pour $j \neq k$

$$\alpha_j^{(i)} < \alpha_j^{(i-1)},$$

où $\mathcal{L}(\alpha^{(i)}) = (\alpha_1^{(i)}, \cdots, \alpha_s^{(i)})$. De plus, ces éléments $\alpha^{(i)}$ vérifient

$$|\mathrm{N}_{\mathrm{K}/\mathbb{Q}}\alpha^{(i)}| \leq \left(\frac{2}{\pi}\right)^{r_2} |\mathrm{d}_{\mathrm{K}}|^{1/2} := C.$$

Comme le nombre d'idéaux entiers de $\mathcal{O}_{\mathrm{K}}$ de norme plus petite que C est en nombre fini, il existe $i < j$ tel que $\alpha^{(i)}\mathcal{O}_{\mathrm{K}} = \alpha^{(j)}\mathcal{O}_{\mathrm{K}}$, i.e.

$$\alpha^{(i)} = x\alpha^{(j)},$$

avec $x \in \mathcal{O}_{\mathrm{K}}^{\times}$. Alors $\mathcal{L}(x) = \mathcal{L}(\alpha^{(i)}) - \mathcal{L}(\alpha^{(j)}) < 0$ et $x_i < 0$ pour $i \neq k$. □

Pour terminer considérons des unités $x^{(1)}, \cdots, x^{(s)}$ vérifiant les conditions du lemme 3.6.4 (pour $k = 1, \cdots, s$). Considérons ensuite la matrice carrée $\mathcal{M} = (x_i^{(j)})_{i,j}$ dont les colonnes sont les plongements logarithmiques $\mathcal{L}(x^{(j)}) = (\cdots, x_i^{(j)}, \cdots)$ des éléments $x^{(j)}$. Il nous suffit de montrer que le rang de $\mathcal{M}$ est exactement $r_1 + r_2 - 1 (= s - 1)$.

La matrice $\mathcal{M}$ a la même rang que la matrice $\mathcal{M}' = (\delta_i x_i^{(j)})_{i,j}$, où $\delta_i = 1$ si le plongement associé est réel et $\delta_i = 2$ sinon. Rappelons ensuite que pour tout $j = 1, \cdots, s$, on a :

$$\sum_{i=1}^{s} \delta_i x_i^{(j)} = 0,$$

ce qui signifie que $< (1, \cdots, 1) > \subset \mathrm{Ker}(\mathcal{M}')$.
Soit alors $0 \neq (\cdots, \lambda_i, \cdots) \in \mathrm{Ker}(\mathcal{M}')$. La fin de la preuve va reposer sur la lecture du produit « d'une ligne » de la matrice avec le vecteur $(\cdots, \lambda_i, \cdots)$. Quitte à faire un changement de variables, on peut supposer $\lambda_1 = 1$ et pour $i = 2, \cdots, s$, $\lambda_1 \geq \lambda_i$. Alors

$$0 = \sum_{i=1}^{s} \delta_i(\lambda_i - 1)x_i^{(1)} = \sum_{i=2}^{s} \delta_i(\lambda_i - 1)x_i^{(1)}.$$

Comme pour $i = 2, \cdots, s$, $(\lambda_i - 1)x_i^{(1)} \leq 0$, on a nécessairement pour $i = 1, \cdots, s$, $\lambda_i = 1$ et ainsi $\mathrm{Ker}(\mathcal{M}') =< (1, \cdots, 1) >$. □

3.6.2. Unités dans les corps quadratiques. —

3.6.2.1. Les corps quadratiques imaginaires. — Soit $\mathrm{K} = \mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire, $d > 0$ sans facteur carré. Alors $r_1 = 0$ et $r_2 = 1$. Dans ce cas, $\mathcal{O}_\mathrm{K}^\times = \mu_\mathrm{K}$ est fini.

Supposons $d \equiv 1, 2 (\mathrm{mod}\ 4)$. Alors $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\sqrt{-d}]$ et $x = a + b\sqrt{-d} \in \mathcal{O}_\mathrm{K}^\times$ si et seulement si

$$a^2 + db^2 = 1.$$

On voit alors que si $d > 1$, les seules unités de $\mathcal{O}_\mathrm{K}^\times$ sont ± 1.
Pour $d = 1$, i.e. $\mathrm{K} = \mathbb{Q}(i)$, on trouve $\mu_\mathrm{K} =< i >$.

Supposons $d \equiv 3 (\mathrm{mod}\ 4)$. Posons $\theta = (1+\sqrt{-d})/2$. Alors $x = a+b\theta \in \mathcal{O}_\mathrm{K}^\times$ si et seulement si

$$(a + b\theta)(a + b\overline{\theta}) = 1,$$

i.e.

$$a^2 + ab + b^2(1 + d)/4 = 1,$$

ou encore

$$(2a + b)^2 + db^2 = 4.$$

Ainsi on a immédiatement pour $d > 3$, $\mu_\mathrm{K} = \{\pm 1\}$, et pour $d = 3$ (i.e. $\mathrm{K} = \mathbb{Q}(\zeta_3)$) : $\mu_\mathrm{K} =< \pm\zeta_3 >$.

3.6.2.2. Les corps quadratiques réels. — Soit $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, $d > 1$ sans facteur carré, un corps quadratique réel. Comme K est réel, $\mu_\mathrm{K} = \{\pm 1\}$. Ainsi, par le théorème de Dirichlet,

$$\mathcal{O}_\mathrm{K}^\times =< -1 > \times < \varepsilon > .$$

En notant que si ε est un générateur de $\mathcal{O}_\mathrm{K}^\times/\mu_\mathrm{K}$, alors $-\varepsilon$ et $\pm\varepsilon^{-1}$ sont également des générateurs de ce quotient. Parmi ces générateurs, une unité (et une seule) est plus grande que 1. Une telle unité est appelée *unité fondamentale* du corps K. Observons que si $\varepsilon = a + b\sqrt{d}$ avec $a, b \in \mathbb{Z}$, est l'unité fondamentale de K alors $a, b > 0$.

Supposons $d \equiv 2, 3 \ (\mathrm{mod}\ 4)$. Alors $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\sqrt{d}]$. Soit $x = a + b\sqrt{d} \in \mathcal{O}_\mathrm{K}$, avec $a, b \in \mathbb{Z}$, $a, b > 0$. Pour $n > 0$, considérons les deux d'entiers a_n et b_n tels que

$$(a + b\sqrt{d})^n = a_n + b_n\sqrt{d}.$$

Alors on peut noter que la suite $(b_n)_n$ est croissante. Cette remarque permet de trouver l'unité fondamentale. Détaillons un exemple

Exemple 3.6.5. — Soit $\mathrm{K} = \mathbb{Q}(\sqrt{7})$. Les unités $x = a + b\sqrt{7}$ de $\mathcal{O}_K$ sont solutions de l'équation de Pell-Fermat suivante :

$$a^2 - 7b^2 = \pm 1.$$

Il faut donc tester si cette équation a des solutions quand $b = 1$. S'il n'y pas pas de solution, on passe à $b = 2$, etc. On arrête quand on a trouvé une solution ! Dans ce cas, la première solution trouvée donne l'unité fondamentale.
Revenons à l'exemple. On note que $a^2 = \pm 1 + 7$ (ici $b = 1$) et $a^2 = \pm 1 + 28$ (ici $b = 2$) n'ont pas de solution avec $a \in \mathbb{Z}$. Par contre, $a^2 = \pm 1 + 63$ a une solution. Ainsi on trouve que $\varepsilon = 8 + 3\sqrt{7}$ est l'unité fondamentale de $\mathcal{O}_{\mathrm{K}}$.

On peut procéder de même quand $d \equiv 1 (\mathrm{mod}\ 4)$.

Remarque 3.6.6. — Soit $d > 1$ sans facteur carré et soit l'équation de Pell-Fermat

$$X^2 - dY^2 = \pm 1,\ X, Y \in \mathbb{Z}.$$

Notons que s'il existe un nombre premier $p|d$ avec $p \equiv 3 (\mathrm{mod}\ 4)$, l'équation $X^2 - dY^2 = -1$ n'a pas de solution (voir également l'exercice 1 du sujet 2008/09 de la dernière section).
Sinon, lorsqu'une solution de l'équation de Pell-Fermat existe (autre que ± 1), toutes les solutions sont paramétrées par les puissances de l'unité fondamentale.

3.6.3. Unités dans les corps cyclotomiques. — Soit un entier $n \geq 3$. Posons $\zeta_n = \exp(2i\pi/n)$ puis $z = \zeta_n + \zeta_n^{-1}$. On rappelle que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne de degré $\varphi(n)$, que le corps $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ est le sous-corps réel maximal de $\mathbb{Q}(\zeta_n)$, correspondant par la théorie de Galois au corps fixé par la conjugaison complexe σ.
Soit $\mathcal{O}_n$ l'anneau des entiers de $\mathbb{Q}(\zeta_n)$ et soit $\mathcal{O}_n^+$ celui de $\mathbb{Q}(\zeta_n)^+$. On va montrer le théorème suivant

Théorème 3.6.7. — *L'indice* $[\mathcal{O}_n^\times : \langle \pm\mu_n \rangle \mathcal{O}_n^+ \rangle]$ *divise* 2.
De plus, cet indice est égal à 1 *quand* n *est un nombre premier* p. *Ainsi dans ce cas toute unité* $\varepsilon \in \mathcal{O}_p^\times$ *sécrit sous la forme* $\varepsilon = \zeta_p^k \eta$, *pour un certain entier* k *et avec* $\eta \in \mathcal{O}_n^+$.

Ce théorème indique donc que quand $n = p$, aux racines de l'unité près, les unités de $\mathcal{O}_p$ proviennent de $\mathbb{Q}(\zeta_p)^+$.

Démonstration. — Soit φ le morphisme de groupe suivant :

$$\begin{array}{rccc} \varphi : & \mathcal{O}_n^\times & \longrightarrow & \mathcal{O}_n^\times \\ & \varepsilon & \mapsto & \varepsilon/\sigma(\varepsilon) \end{array}$$

Le noyau de φ correspond exactement aux unités de $\mathbb{Q}(\zeta_n)^+$.
On note ensuite que $|\varphi(\varepsilon)| = 1$, et même mieux, comme l'extension $\mathbb{Q}(\zeta_n/\mathbb{Q})$ est abélienne, σ commute avec tous les éléments de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Ainsi, si l'on pose $z = \varphi(\varepsilon) \in \mathcal{O}_n^\times$, il vient pour tout $g \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$,

$$|g(z)| = |g(\varepsilon)/g(\sigma(\varepsilon))| = |g(\varepsilon)/\sigma(g(\varepsilon))| = 1.$$

Ainsi tous les conjugués de z sont de module 1. Ceci implique que z est une racine de l'unité (voir l'exercice 14, ou la preuve du théorème de Dirichlet 3.6.2). Or les seules racines de l'unité dans $\mathbb{Q}(\zeta_n)$ sont de la forme $\pm\zeta_n^k$.
Posons $W = \langle \pm\mu_n \mathcal{O}_n^+ \rangle$. On a donc $\mathrm{Im}(\varphi) \subset W$. Considérons alors le morphisme θ regardant la classe de $\varphi(\varepsilon)$ modulo W^2.
On note que si $\varepsilon = \pm\zeta_n^k \eta$ avec $\eta \in \mathcal{O}_n^+$, alors $\theta(\varepsilon) \in W^2$. Ainsi, $\langle \pm\zeta_n^k \eta \rangle \subset \ker(\theta)$. Réciproquement. Soit $\varepsilon \in \mathcal{O}_n$ telle que $\varphi(\varepsilon) = \zeta_n^{2k} \in W^2$. Alors, on voit très facilement que σ laisse stable $\varepsilon\zeta_n^{-k}$, ce qui signifie que $\varepsilon\zeta_n^{-k} \in \mathcal{O}_n^+$.
On conclut la première partie en remarquant que $[W : W^2] = 2$.

Pour déterminer l'indice la question est donc de savoir si $\varphi(\mathcal{O}_n) = W$ ou W^2.

Prenons $n = p$ (avec $p > 2$). On remarque alors que pour $k \in \{1, \cdots, p-1\}$ on a $\zeta_p^k = \zeta_p^{2a} \in W^2$ pour un certain entier a. Ainsi dans ce cas la question est de savoir si $\varphi(\varepsilon) = +\zeta_p^k$ ou $-\zeta_p^k$.
On écrit tout d'abord $\varepsilon = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ avec $a_i \in \mathbb{Z}$. Il vient alors $\varepsilon \equiv a_0 + \cdots + a_{p-2} \pmod{\mathfrak{p}}$, où $\mathfrak{p} = (1 - \zeta_p)$. Ceci implique que $\sigma(\varepsilon) \equiv \varepsilon \pmod{\mathfrak{p}}$. Supposons alors que $\varepsilon/\sigma(\varepsilon) = -\zeta_n^k$, il vient alors $0 \equiv \varepsilon(1 + \zeta_n^k) \equiv 2\varepsilon \pmod{\mathfrak{p}}$, d'où la contradiction. On vient donc de montrer que pour $n = p$, $\varphi(\mathcal{O}_p) = W$. □

CHAPITRE 4

VALEURS ABSOLUES

4.1. Préliminaires topologiques

4.1.1. Valeurs absolues sur un corps. —

Définition 4.1.1. — Soit K un corps. On appelle valeur absolue sur K une fonction

$$\|\cdot\| : \mathrm{K} \to \mathbb{R}$$

satisfaisant les trois propriétés suivantes :

(i) $\|x\| \geqslant 0$ pour tout $x \in \mathrm{K}$ et $\|x\| = 0$ si, et seulement si, $x = 0$;

(ii) Pour $x, y \in \mathrm{K}$ on a

$$\|xy\| = \|x\| \, \|y\| \ ;$$

(iii) Pour $x, y \in \mathrm{K}$ on a

$$\|x + y\| \leqslant \|x\| + \|y\|.$$

Exemple 4.1.2. — La valeur absolue définie par $\|x\| = 1$ si $x \neq 0$ est dite triviale.

Exemple 4.1.3. — Soit $\mathrm{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Alors la fonction "module" $x \mapsto |x|$ est une valeur absolue sur K.

Donnons quelques propriétés élémentaires.

Proposition 4.1.4. — *(i) On a* $\|1_{\mathrm{K}}\| = \| - 1_{\mathrm{K}}\| = 1$.

(ii) Pour tout $n \in \mathbb{N}$ *on a* $\|n1_{\mathrm{K}}\| \leq n$.

(iii) Pour tout $x \in \mathrm{K}$, $\| - x\| = \|x\|$.

(iv) Pour $x \neq 0$, $\|x^{-1}\| = \|x\|^{-1}$.

(v) Pour $x, y \in \mathrm{K}$ on a $\;|\,\|x\| - \|y\|\,| \leqslant \|x - y\|$.

Démonstration. — C'est immédiat. □

Proposition 4.1.5. — *Soit $\|\cdot\| : \mathrm{K} \to \mathbb{R}$ une application vérifiant les propriétés suivantes :*

(i) $\|x\| \geqslant 0$ pour tout $x \in \mathrm{K}$ et $\|x\| = 0$ si, et seulement si, $x = 0$;

(ii) Pour $x, y \in \mathrm{K}$ on a

$$\|xy\| = \|x\|\,\|y\|.$$

Alors $\|\cdot\|$ est une valeur absolue sur K *si et seulement si*

(4) $\qquad \|1 + x\| \leqslant 2 \qquad$ *pour tout $x \in \mathrm{K}$ tel que* $\quad \|x\| \leqslant 1$.

Démonstration. — Si $\|\cdot\|$ est une valeur absolue, alors pour tout x vérifiant $\|x\| \leqslant 1$ on a

$$\|1 + x\| \leqslant \|1\| + \|x\| \leqslant 2.$$

Réciproquement, supposons que $\|\cdot\|$ vérifie (4). Alors pour $x, y \in \mathrm{K}$ on a

$$\|x + y\| \leqslant 2\max\{\|x\|, \|y\|\}$$

(si, par exemple, $\|x\| \leqslant \|y\|$, on pose $\alpha = x/y$ et on applique (4) à α.) Par récurrence on obtient :

$$\|\sum_{i=1}^{2^m} x_i\| \leqslant 2^m \max\{\|x_i\|,\ 1 \leq i \leq 2^m\}$$

pour $x_i \in \mathrm{K}$. Si n est un nombre naturel quelconque il existe m tel que $2^{m-1} \leq n < 2^m$. Pour $x_1, \ldots, x_n \in \mathrm{K}$ on obtient (en ajoutant $2^m - n$ termes nuls) :

$$\|\sum_{i=1}^{n} x_i\| \leq 2^m \max\{\|x_i\| \,|\, 1 \leq i \leq n\} \leq (2n)\max\{\|x_i\| \,|\, 1 \leq i \leq n\}.$$

En particulier, on a

$$\|\sum_{i=1}^{n} x_i\| \leq 2n \sum_{i=1}^{n} \|x_i\|$$

et, pour tout $n \in \mathbb{N}$,

$$\|n\| \leq 2n.$$

Maintenant nous pouvons montrer que (4) implique l'inégalité triangulaire. Pour $x, y \in \mathrm{K}$ et $n \in \mathbb{N}$, on a :

$$\begin{aligned} \|x+y\|^n = \|(x+y)^n\| &= \|\sum_{i=0}^{n} C_n^i x^i y^{n-i}\| \\ &\leq (2n+1)\sum_{i=0}^{n} \|C_n^i 1_{\mathrm{K}}\|\,\|x\|^i\,\|y\|^{n-i} \\ &\leq 2(2n+1)\sum_{i=0}^{n} C_n^i \|x\|^i\,\|y\|^{n-i} = 2(2n+1)(\|x\|+\|y\|)^n. \end{aligned}$$

Ainsi

$$\|x+y\| \leq (2(2n+1))^{1/n}(\|x\|+\|y\|)$$

pour tout $n \in \mathbb{N}$. En passant à la limite quand $n \to \infty$ on obtient $\|x+y\| \leq \|x\| + \|y\|$. □

Soit $\|\cdot\|$ une valeur absolue sur K. Posons

$$d(x,y) = \|x-y\|\,.$$

Alors d est une distance sur K :

(i) $d(x,y) \geqslant 0$ et $d(x,y) = 0$ si, et seulement si, $x = y$;

(ii) $d(x,y) = d(y,x)$ pour $x, y \in \mathrm{K}$;

(iii) Pour $x, y, z \in \mathrm{K}$ on a l'inégalité triangulaire

$$d(x,z) \leqslant d(x,y) + d(y,z).$$

On définit la boule ouverte de centre $a \in \mathrm{K}$ et de rayon $r > 0$ l'ensemble

$$B(a,r) = \{x \in \mathrm{K},\ \|x-a\| < r\},$$

et on appelle boule fermée de centre a et de rayon $r > 0$ l'ensemble

$$B_f(a,r) = \{x \in \mathrm{K},\ \|x-a\|_{\mathrm{K}} \leq r\}.$$

Comme l'application $\|\cdot\|_{\mathrm{K}} : \mathrm{K} \to \mathbb{R}$ est continue, la boule $B_f(a,r)$ est une partie fermée de K.

Soit $\bar{B}(a,r)$ l'adhérence de la boule ouverte $B(a,r)$ dans K. Par continuité on obtient que $\bar{B}(a,r) \subseteq B_f(a,r)$.

Définition 4.1.6. — Deux valeurs absolues $\|\cdot\|_1$ et $\|\cdot\|_2$ sur K sont topologiquement équivalentes si elles définissent la même topologie.

Remarque 4.1.7. — On rappelle que $\|\cdot\|_1$ et $\|\cdot\|_2$ définissent la même topologie si et seulement si, pour pour tout $C_1 > 0$ (resp. $C_2 > 0$) il existe C_2' (resp. C_1') telle que pour tout $x \in \mathrm{K}$,

$$\|x\|_2 \leq C_2' \Longrightarrow \|x\|_1 \leq C_1$$

(resp. $\|x\|_1 \leq C_1' \Longrightarrow \|x\|_2 \leq C_2$).

Proposition 4.1.8. — *Soient $\|\cdot\|_1$ et $\|\cdot\|_2$ deux valeurs absolues sur* K *topologiquement équivalentes. Alors il existe $c \in \mathbb{R}^{*,+}$ tel que $\|\cdot\|_2 = \|\cdot\|_1^c$.*

Remarque 4.1.9. — La réciproque est immédiate.

Démonstration. — Soit $\|\cdot\|_1$ et $\|\cdot\|_2$ deux valeurs absolues sur K topologiquement équivalentes. Alors les ensembles $\{x \in \mathrm{K}, \|x\|_1 < 1\}$ et $\{x \in \mathrm{K}, \|x\|_2 < 1\}$ sont identiques : en effet, cela provient tout simplement du fait que la suite $\|x^n\|_i = \|x\|_i^n$ tend vers 0 si et seulement si, $\|x\|_i < 1$, $i = 1, 2$.
Ces ensembles sont réduits à $\{0\}$ si et seulement si, les normes considérées sont triviales.
Supposons que cela ne soit pas le cas et soit $x \in \mathrm{K}^\times$ tel que $\|x\|_1 < 1$.
Soit $y \in \mathrm{K}^\times$ et soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}$. Alors $\|x^{-a}y^b\|_1 < 1$ si et seulement si, $\|x^{-a}y^b\|_2 < 1$ et ainsi $\dfrac{a}{b} < \dfrac{\ln \|y\|_1}{\ln \|x\|_1}$ si et seulement si, $\dfrac{a}{b} < \dfrac{\ln \|y\|_2}{\ln \|x\|_2}$. Ceci montre que pour tout $y \in \mathrm{K}^\times$, $\dfrac{\ln \|y\|_1}{\ln \|x\|_1} = \dfrac{\ln \|y\|_2}{\ln \|x\|_2}$. On conclut en posant $c := \dfrac{\ln \|x\|_1}{\ln \|x\|_2}$. □

Définition 4.1.10. — Deux valeurs absolues $\|\cdot\|_1$ et $\|\cdot\|_2$ sur K sont équivalentes si, et seulement si, il existe $A, B > 0$ tels que pour tout $x \in \mathrm{K}$,

$$A\|x\|_1 \leq \|x\|_2 \leq B\|x\|_1.$$

Proposition 4.1.11. — *Deux valeurs absolues équivalentes sont topologiquement équivalentes.*

Démonstration. — Immédiat. □

Proposition 4.1.12. — *Soient $\|\cdot\|_1$ et $\|\cdot\|_2$ deux valeurs absolues de* K*, équivalentes. Alors $\|\cdot\|_2 = \|\cdot\|_1$.*

Démonstration. — Supposons qu'il existe x tel que $\|x\|_1 > \|x\|_2$. Alors, comme

$$\frac{\|x^n\|_2}{\|x^n\|_1} = \frac{\|x\|_2^n}{\|x\|_1^n},$$

la suite $\left(\frac{\|x^n\|_2}{\|x^n\|_1}\right)_n$ tend vers 0 ce qui contredit l'inégalité de la définition 4.1.10. □

Terminons ce paragraphe par quelques évidences.

Proposition 4.1.13. — *Soit* K *un corps muni d'une valeur absolue. Les applications suivantes sont continues :*

(i) $\|\cdot\| \ : \ \mathrm{K} \to \mathbb{R}, \ x \mapsto \|x\|$;
(ii) $f_a \ : \ \mathrm{K} \times \mathrm{K} \to \mathrm{K}, \ f_a(x,y) = x + y$;
(iii) $f_m \ : \ \mathrm{K} \times \mathrm{K} \to \mathrm{K}, \ f_m(x,y) = xy$;
(iv) $inv \ : \ \mathrm{K}^* \to \mathrm{K}^*, \ inv(x) = x^{-1}$.

Démonstration. — C'est immédiat. □

4.1.2. Complétion. — Soit K un corps muni d'une valeur absolue non-triviale. On dit que $\{x_n\}$ est une suite de Cauchy, si pour tout $\epsilon > 0$ il existe N tel que pour tous $n, m \geqslant N$

$$d(x_n, x_m) = \|x_n - x_m\| < \epsilon.$$

Définition 4.1.14. — On dit que K est complet pour la valeur absolue $\|\cdot\|$ si toute suite de Cauchy est convergente.

Le théorème suivant est crucial.

Théorème 4.1.15. — *Soit* K *un corps muni d'une valeur absolue* $\|\cdot\|$. *Il existe un corps* $\hat{\mathrm{K}}$ *muni d'une valeur absolue* $\|\cdot\|_{\hat{\mathrm{K}}}$ *et un plongement*

$$i \ : \ \mathrm{K} \hookrightarrow \hat{\mathrm{K}}$$

vérifiant les propriétés suivantes :

(i) la valeur absolue $\|\cdot\|_{\hat{\mathrm{K}}}$ *prolonge* $\|\cdot\|$ *i.e. pour tout* $x \in \mathrm{K}$ *on a*

$$\|i(x)\|_{\hat{\mathrm{K}}} = \|x\|;$$

(ii) $\hat{\mathrm{K}}$ *est complet pour la valeur absolue* $\|\cdot\|_{\hat{\mathrm{K}}}$;
(iii) $i(\mathrm{K})$ *est dense dans* $\hat{\mathrm{K}}$.

Si $(\tilde{\mathrm{K}}, \|\cdot\|_{\tilde{\mathrm{K}}}, \tilde{i})$ *est un autre corps muni d'une valeur absolue et d'un plongement* $\tilde{i} : \mathrm{K} \hookrightarrow \tilde{\mathrm{K}}$ *avec les mêmes propriétés, alors il existe un unique isomorphisme*

$$j : \hat{\mathrm{K}} \to \tilde{\mathrm{K}}$$

tel que

(i) j *est compatible avec les valeurs absolues, i.e.* $\|j(x)\|_{\tilde{\mathrm{K}}} = \|x\|_{\hat{\mathrm{K}}}$ *pour tout* $x \in \hat{\mathrm{K}}$;

(ii) les plongements i *et* $\tilde{i}$ *sont compatibles avec* j*, i.e.*

$$\tilde{i}(x) = j(i(x)) \quad \textit{pour tout } x \in \mathrm{K}.$$

Démonstration. — Démontrons tout d'abord l'unicité. Dans la démonstration nous utiliserons plusieurs fois l'observation suivante : comme $\|\cdot\|_{\hat{\mathrm{K}}}$ prolonge $\|\cdot\|$, $\{x_n\} \subset \mathrm{K}$ est une suite de Cauchy si, et seulement si, $\{i(x_n)\}$ l'est dans $\hat{\mathrm{K}}$.
Soit $(\tilde{\mathrm{K}}, \|\cdot\|_{\tilde{\mathrm{K}}}, \tilde{i})$ un autre corps vérifiant (i)-(iii). Nous allons construire l'application $j : \hat{\mathrm{K}} \to \tilde{\mathrm{K}}$ de la façon suivante. Comme $i(\mathrm{K})$ est dense dans $\hat{\mathrm{K}}$, pour tout $x \in \hat{\mathrm{K}}$ il existe une suite $x_n \in \mathrm{K}$ telle que $x = \lim_{n\to\infty} i(x_n)$. Comme x_n est une suite de Cauchy, la suite $\{\tilde{i}(x_n)\} \subset \tilde{\mathrm{K}}$ l'est aussi et comme $\tilde{\mathrm{K}}$ est complet on peut poser

$$j(x) = \lim_{n\to\infty} \tilde{i}(x_n).$$

On va montrer que $j(x)$ est bien défini *i.e.*, qu'elle ne dépend pas du choix de la suite $\{x_n\}$. Soit $\{x'_n\}$ une autre suite telle que $\lim_{n\to\infty} x'_n = x$. On construit une nouvelle suite $\{\alpha_n\}$ en posant

$$\begin{aligned}
\alpha_1 &= x_1,\\
\alpha_2 &= x'_1,\\
\alpha_3 &= x_2,\\
\alpha_4 &= x'_2,\\
&\cdots\cdots\cdots
\end{aligned}$$

i.e.

$$\alpha_n = \begin{cases} x_{(n+1)/2} & \textit{si } n \textit{ est impair},\\ x'_{n/2} & \textit{si } n \textit{ est pair}. \end{cases}$$

Alors $\lim_{n\to\infty} i(\alpha_n) = x$ et en appliquant le même argument on voit que la suite $\tilde{i}(\alpha_n)$ converge dans $\tilde{\mathrm{K}}$. Donc, les sous-suites $\{\tilde{i}(x'_n)\}$ et $\{\tilde{i}(x_n)\}$

de $\{\tilde{i}(\alpha_n)\}$ converge vers le même élément *i.e.*,

$$\lim_{n\to\infty} \tilde{i}(x'_n) = \lim_{n\to\infty} \tilde{i}(\alpha_n) = \lim_{n\to\infty} \tilde{i}(x_n) = j(x),$$

ce qui montre que $j(x)$ ne dépend pas du choix de $\{x_n\}$.

Si $x = \lim_{n\to\infty} i(x_n)$ et $y = \lim_{n\to\infty} i(y_n)$, alors

$$x + y = \lim_{n\to\infty} (i(x_n) + i(y_n)) = \lim_{n\to\infty} i(x_n + y_n),$$
$$xy = \lim_{n\to\infty} (i(x_n)\, i(y_n)) = \lim_{n\to\infty} i(x_n y_n),$$

d'où

$$j(x + y) = j(x) + j(y),$$
$$j(xy) = j(x)\, j(y).$$

On en déduit que j est un homomorphisme de corps. Par construction, on a $j(i(x)) = \tilde{i}(x)$, si $x \in \mathrm{K}$ (si $x \in \mathrm{K}$ on peut poser $x_n = x$). En particulier, l'homomorphisme j est non-nul, donc injectif. Pour montrer qu'il est surjectif on remarque que comme $\tilde{i}(\mathrm{K})$ est dense dans $\tilde{\mathrm{K}}$, pour tout $z \in \tilde{\mathrm{K}}$ il existe une suite $\{z_n\}$ dans K telle que $z = \lim_{n\to\infty} \tilde{i}(z_n)$. Comme $\{z_n\}$ est une suite de Cauchy, on peut poser $x = \lim_{n\to\infty} i(z_n)$. Alors, par définition, on a $z = j(x)$, d'où la surjectivité de j.

Donnons maintenant la preuve de l'existence du corps $\hat{\mathrm{K}}$ vérifiant (i)-(iii). Soit $C(\mathrm{K})$ l'ensemble des suites de Cauchy $\{x_n\}$ de K. On définit la somme et le produit des deux suites de Cauchy en posant

$$\{x_n\} + \{y_n\} = \{x_n + y_n\},$$
$$\{x_n\}\, \{y_n\} = \{x_n y_n\}.$$

On vérifie facilement que $\{x_n + y_n\}$ et $\{x_n y_n\}$ sont des suites de Cauchy. Ainsi $C(\mathrm{K})$ est un anneau commutatif pour l'addition et la multiplication terme à terme.
Soit

$$I_{\mathrm{K}} = \{\{x_n\} \subset \mathrm{K},\ \lim_{n\to\infty} x_n = 0\}.$$

On va montrer que I_{K} est un idéal *maximal* de $C(\mathrm{K})$. Il est clair que si $\{x_n\}, \{y_n\} \in I_{\mathrm{K}}$, alors $\{x_n\} \pm \{y_n\} \in I_{\mathrm{K}}$. Soient maintenant $\{x_n\} \in I_{\mathrm{K}}$ et $\{y_n\} \in C(\mathrm{K})$ une suite de Cauchy quelconque. Alors $\{y_n\}$ est bornée i.e. il existe c tel que $\|y_n\| \leqslant c$ pour tout n. Alors,

$$\|x_n y_n\| = \|x_n\|\, \|y_n\| \leqslant c\|x_n\| \underset{n\to\infty}{\to} 0,$$

ce qui montre que $\{x_n\}\,\{y_n\} \in I_{\mathrm{K}}$. Donc, I_{K} est un idéal. Montrons qu'il est maximal. Soit $\{x_n\} \notin I_{\mathrm{K}}$: il existe $M > 0$ et $N \in \mathbb{N}$ tels que

$$\|x_n\| \geqslant M, \quad si\ n \geqslant N.$$

Soit la suite $\{x'_n\}$ définie par $x'_n = x_n$ pour $n \geq N$ et par $x'_n = 1$ pour $n < N$. Soit enfin la suite $\{y_n\}$ définie par $y_n = (x'_n)^{-1}$. On a pour $n \geq N$,

$$\|y_n - y_m\| = \left\| \frac{1}{x_n} - \frac{1}{x_m} \right\| = \frac{\|x_n - x_m\|}{x_n x_m} \leqslant \frac{\|x_n - x_m\|}{M^2},$$

ce qui montre que $\{y_n\}$ est une suite de Cauchy. Comme $\{x'_n\}\,\{y_n\} = 1$, on en déduit

$$1 = \{x'_n\}\{y_n\} = \{x_n\}\{y_n\} + \{x'_n - x_n\}\{y_n\}.$$

Comme $\{x'_n - x_n\} \in I_{\mathrm{K}}$, on en déduit que $\mathcal{I}_{\mathrm{K}}$ est maximal.
On définit le corps $\hat{\mathrm{K}}$ comme le quotient

$$\hat{\mathrm{K}} = C(\mathrm{K})/I(\mathrm{K}).$$

Le corps K est plongé diagonalement dans $\hat{\mathrm{K}}$: l'image $i(x)$ de $x \in \mathrm{K}$ est la classe de la suite constante $x_n = x$. La valeur absolue de K se prolonge sur $\hat{\mathrm{K}}$ de la façon suivante : si $\{x_n\} \in C(\mathrm{K})$ représente une classe $\alpha \in \hat{\mathrm{K}}$, on pose

$$\|\alpha\|_{\hat{\mathrm{K}}} = \lim_{n\to\infty} \|x_n\|.$$

(Remarquons que l'inégalité $\big|\|x_n\| - \|x_m\|\big| \leqslant \|x_n - x_m\|$ implique que $\|x_n\|$ est une suite de Cauchy dans $\mathbb{R}$, d'où la convergence. Remarquons également que la limite ne dépend pas du choix de la suite $\{x_n\}$.) On note que $\|\cdot\|_{\hat{\mathrm{K}}}$ est bien une norme sur K. Enfin, par construction, le corps K est dense dans $\hat{\mathrm{K}}$.
Il reste à montrer que $\hat{\mathrm{K}}$ est complet. Soit $\{\alpha_n\}$ une suite de Cauchy dans $\hat{\mathrm{K}}$. Comme $i(\mathrm{K})$ est dense dans $\hat{\mathrm{K}}$, pour tout α_n il existe $x_n \in \mathrm{K}$ tel que $\|i(x_n) - \alpha_n\|_{\hat{\mathrm{K}}} < 1/n$. Soit $\epsilon > 0$. Alors il existe N tel que pour tout $n, m \geqslant N$ on a

$$\|i(x_n) - \alpha_n\|_{\hat{\mathrm{K}}} < \epsilon/3,$$
$$\|\alpha_m - \alpha_n\|_{\hat{\mathrm{K}}} < \epsilon/3.$$

Donc, pour tout $n, m \geqslant N$ on a

$$\|x_n - x_m\| = \|i(x_n) - i(x_m)\|_{\hat{\mathrm{K}}} \leqslant \|i(x_n) - \alpha_n\|_{\hat{\mathrm{K}}} + \|\alpha_n - \alpha_m\|_{\hat{\mathrm{K}}} + \|\alpha_m - i(x_n)\|_{\hat{\mathrm{K}}} < \epsilon$$

ce qui montre que $\{x_n\}$ est une suite de Cauchy de $C(\mathrm{K})$. Posons $\alpha = (x_n) \in \hat{\mathrm{K}}$. En utilisant l'inégalité

$$\|\alpha_n - \alpha\|_{\hat{\mathrm{K}}} \leqslant \|\alpha_n - i(x_n)\|_{\hat{\mathrm{K}}} + \|i(x_n) - \alpha\|_{\hat{\mathrm{K}}}$$

on montre facilement que α_n converge vers α. Donc $\hat{\mathrm{K}}$ est complet. □

Pour simplifier la notation nous identifierons K à son image $i(\mathrm{K})$ dans $\hat{\mathrm{K}}$. En particulier, nous écrirons x au lieu de $i(x)$.

4.1.3. Espace vectoriel sur un corps complet. — Pour étudier les prolongements des valeurs absolues aux extensions finies nous avons besoin de la notion de norme sur un espace vectoriel.

Définition 4.1.16. — Soit K un corps muni d'une valeur absolue $\|\cdot\|_{\mathrm{K}}$ et soit V un K-espace vectoriel de dimension finie. On appelle norme sur V une fonction

$$\|\cdot\|_V \ : \ V \to \mathbb{R}$$

vérifiant

(i) pour tout $v \in V$ on a $\|v\|_V \geqslant 0$ et $\|v\|_V = 0$ si et seulement si $v = 0$;

(ii) pour tous $\alpha \in \mathrm{K}$ et $v \in V$ on a

$$\|\alpha v\|_V = \|\alpha\|_{\mathrm{K}} \|v\|_V;$$

(iii) pour tous $v, w \in V$ on a

$$\|v + w\|_V \leqslant \|v\|_V + \|w\|_V.$$

Exemple 4.1.17. — Soit $v_1, \ldots, v_n$ une base de V. Tout élément$v \in V$ s'écrit : $v = x_1 v_1 + \cdots + x_n v_n$, avec $x_i \in \mathrm{K}$. Posons

$$\|v\|_1 = \sum_{i=1}^{n} \|x_i\|_{\mathrm{K}},$$

$$\|v\|_2 = \left(\sum_{i=1}^{n} \|x_i\|_{\mathrm{K}}^2 \right)^{1/2},$$

$$\|v\|_\infty = \max_{1 \leqslant i \leqslant n} \|x_i\|_{\mathrm{K}}.$$

Alors $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$ sont des normes sur V (qui dépendent, bien sûr, du choix de la base $v_1, \ldots, v_n$).

Exemple 4.1.18. — Soit $M_n(\mathrm{K})$ l'espace vectoriel des matrices carrées de taille n à coefficients dans K. Alors la norme $\| \cdot \|_\infty$ par rapport à la base canonique de $M_n(\mathrm{K})$ s'écrit :

$$\|M\|_\infty = \max_{1\leq i,j\leq n} \|a_{ij}\|_{\mathrm{K}}, \qquad M = (a_{ij})_{1\leq i,j\leq n}.$$

Soient $v_0 \in V$ et $r > 0$. L'ensemble

$$B(v_0, r) = \{v \in V, \|v - v_0\|_V < r\}$$

est la boule ouverte de centre v_0 et de rayon r. On dit que $X \subseteq V$ est un ouvert si et seulement si pour tout $v \in X$ il existe $r > 0$ tel que

$$B(v, r) \subseteq X.$$

Donc, une norme $\| \cdot \|_V$ définie une topologie sur V.

Définition 4.1.19. — Deux normes $\| \cdot \|_V$ et $\| \cdot \|'_V$ sur V sont dites équivalentes s'il existe des réels $C_1, C_2 > 0$ tels que pour tout $v \in V$

$$C_1\|v\|_V \leqslant \|v\|'_V \leqslant C_2\|v\|_V.$$

Proposition 4.1.20. — *Si deux normes $\| \cdot \|_V$ et $\| \cdot \|'_V$ sont équivalentes, elles définissent la même topologie sur V.*

Démonstration. — Immédiat. □

Comme K est complet, le raisonnement "coordonnée par coordonnée" montre que V est complet pour la topologie infinie $\| \cdot \|_\infty$. Nous avons en fait :

Théorème 4.1.21. — *Soit V un espace vectoriel de dimension finie sur un corps complet pour une valeur absolue. Alors toutes les normes sur V sont équivalentes.*

Démonstration. — C'est un résultat classique. On montre que toutes les normes sont équivalentes à la norme $\| \cdot \|_\infty$, relativement à une K-base $\{e_1, \cdots, e_n\}$ de V.

Soit $\| \cdot \|$ une norme sur V. On note immédiatement que

$$\| \cdot \| \leq \max\{\|e_i\|_\infty, i = 1, \cdots, n\} \| \cdot \|_\infty.$$

Montrons qu'il existe $C > 0$ tel que $\| \cdot \|_\infty \leq C\| \cdot \|$.

Si $n = 1$, c'est immédiat.
Supposons donc $n > 1$. Raisonnons par l'absurde. Il existe une suite (x_k) de V telle que $\|x_k\|_\infty \geq k\|x_k\|$. Ecrivons

$$x_k = \lambda_{1,k}e_1 + \cdots \lambda_{n,k}e_n,$$

avec $\lambda_{i,k} \in \mathrm{K}$. Quitte à normaliser, on peut supposer que $\lambda_{1,k} = 1$ et $\|x_k\|_\infty = 1$. Il vient : $\|x_k\| \leq 1/k$.
Soit $y_k = x_k - e_1$. Alors $y_k \in \mathrm{K}e_2 + \cdots + \mathrm{K}e_n$, i.e. la suite $(y_k)_k$ se trouve dans un sous-espace vectoriel de dimension $n-1$ et

$$\|y_k - y_l\| = \|x_k - x_l\| \leq 1/l + 1/k.$$

La suite $(y_k)_k$ est de Cauchy dans $\mathrm{K}e_2 + \cdots + \mathrm{K}e_n$. Par hypothèse de récurrence sur la dimension, les suites $(\lambda_{i,k})_k$, pour $i = 2, \cdots, n$ sont de Cauchy dans K. Comme K est complet, pour $i = 2, \cdots, n$, il existe $\lambda_i \in \mathrm{K}$ tel que

$$\lim_{k\to\infty} \lambda_{i,k} = \lambda_i.$$

Posons $x = e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n$. Alors

$$\|x\| \leq \|x - x_k\| + \|x_k\| \leq C'\|x - x_k\|_\infty + 1/k \to 0.$$

Ainsi $x = 0$, ce qui contredit la liberté des éléments $e_1, \cdots, e_n$. □

Corollaire 4.1.22. — *Si* K *est complet, alors* V *est complet pour toute norme* $\|\cdot\|_V$ *sur* V.

4.1.4. Corps localement compact. — Rappelons la définition d'un espace topologique localement compact.

Définition 4.1.23. — Un espace topologique X est localement compact si pour tout $x \in X$ il existe un voisinage ouvert U_x de x tel que l'adhérence $\bar{U}_x$ soit compacte.

Exemple 4.1.24. — $\mathbb{R}$ et $\mathbb{C}$ sont localement compacts.

Proposition 4.1.25. —
Soit K *un corps muni d'une valeur absolue* $\|\cdot\|_\mathrm{K}$. *Les assertions suivantes sont équivalentes.*

(i) K *est localement compact.*

(ii) Pour tout $a \in \mathrm{K}$ *il existe* $r > 0$ *tel que* $B_f(a, r)$ *est compact.*

(iii) Pour tout $a \in \mathrm{K}$ et $r > 0$ la boule fermée $B_f(a, r)$ est compacte.

Démonstration. — i) $\Rightarrow$ ii). Comme K est localement compact, il existe un voisinage U_a de a tel que $\bar{U}_a$ soit compact. Soit $r' > 0$ un réel vérifiant $B(0, r') \subseteq U_a$. Si $r < r'$, alors $B_f(a, r) \subseteq B(a, r') \subseteq \bar{U}_a$. Comme une partie fermée d'un compact est compacte, on obtient que $B_f(0, r)$ est compact.
ii) $\Rightarrow$ iii). Comme la valeur absolue sur K est non-triviale, il existe $\lambda \neq 0$ tel que $\|\lambda\|_{\mathrm{K}} < 1$. En remplacant λ par λ^n pour n assez grand on voit que pour tout $\epsilon > 0$ il existe $\lambda \neq 0$ tel que $\|\lambda\|_{\mathrm{K}} < \epsilon$.
Soit $r > 0$. Par ii) il existe $r' > 0$ tel que $B_f(0, r')$ est compact. Choisissons λ vérifiant $\|\lambda\|_{\mathrm{K}} < r'/r$ (c'est toujours possible que la valeur absolue est non-triviale). Soit $h_\lambda : \mathrm{K} \to \mathrm{K}$ l'application "multiplication par λ" :

$$h_\lambda(x) = \lambda x.$$

L'application h_λ est continue et $h_{\lambda^{-1}}$ est l'application réciproque de h_λ. Donc, h_λ est un homéomorphisme de K sur K.
En particulier, $F = h_\lambda(B_f(0, r))$ est une partie fermée et par le choix de λ on a $F \subset B_f(0, r')$. Donc F est compact. Comme $B_f(0, r)$ et F sont homéomorphes on en déduit la compacité de $B_f(0, r)$.
Il reste à remarquer que la translation

$$\mathrm{K} \to \mathrm{K},$$
$$x \mapsto a + x$$

est un homéomorphisme qui envoie $B_f(0, r)$ sur $B_f(a, r)$ d'où on obtient que toute boule fermée $\bar{B}(a, r)$ est compacte.
iii) $\Rightarrow$ i). Comme $\bar{B}(a, r) \subseteq B_f(a, r)$, l'hypothèse iii) implique la compacité de $\bar{B}(a, r)$. □

Proposition 4.1.26. — *Soit V un espace vectoriel normé de dimension finie sur un corps complet* K. *Alors* K *est localement compact si et seulement si V est localement compact.*

Démonstration. — Supposons K localement compact. Comme toutes les normes sur V sont équivalentes, on fixe une base $e_1, \ldots, e_n$ de V et on

considère la norme $\|\cdot\|_\infty$ par rapport à cette base. Comme K est localement compact, il existe un voisinage ouvert U de 0 tel que $\bar{U}$ est compact. Alors

$$W = Ue_1 + Ue_2 \cdots + Ue_n = \{\sum_{i=1}^{n} a_i e_i \,|\, a_i \in U\}$$

est un voisinage de 0. L'adhérence

$$\bar{W} = \bar{U}e_1 + \bar{U}e_2 + \cdots + \bar{U}e_n$$

est compacte car la somme directe des compacts est compact.
Réciproquement, supposons que V est localement compact. Alors $B_f(0,r)$ est un compact. Soit pr_1 la projection

$$\begin{aligned} pr_1 \ &: \ V \to \mathrm{K}, \\ &pr_1(a_1e_1 + \cdots + a_ne_n) = a_1. \end{aligned}$$

Par la définition de la norme $\|\cdot\|_\infty$ on a $pr_1(B_f(0,r)) = B_f(0,r)$. Comme l'image continue d'un compact est compact on en déduit la compacité de $B_f(0,r)$. □

4.2. Prolongement des valeurs absolues

4.2.1. Le cas des corps complets. — Dans ce paragraphe K désigne un corps complet pour une valeur absolue non-triviale $\|\cdot\|_\mathrm{K}$.
On rappelle que nous ne considérons que des extensions séparables L/K.

Définition 4.2.1. — Soit K un corps muni d'une valeur absolue $\|\cdot\|_\mathrm{K}$ et soit L/K une extension finie de K. On dit qu'une valeur absolue $\|\cdot\|_\mathrm{L}$ sur L prolonge $\|\cdot\|_\mathrm{K}$ si pour tout $x \in \mathrm{K}$, on a $\|x\|_\mathrm{L} = \|x\|_\mathrm{K}$.

Théorème 4.2.2. — *Soit* K *un corps complet pour une valeur absolue* $\|\cdot\|_\mathrm{K}$ *et soit* L/K *une extension (séparable) de degré* n*. Alors il existe un unique prolongement* $\|\cdot\|_\mathrm{L}$ *de* $\|\cdot\|_\mathrm{K}$ *à* L*. Pour* $x \in \mathrm{L}$*, ce prolongement est donné par la formule :*

$$\|x\|_\mathrm{L} = \|\mathrm{N}_{\mathrm{L/K}}(x)\|_\mathrm{K}^{1/n}.$$

Le corps L *est complet pour la topologie définie par* $\|\cdot\|_\mathrm{L}$.

Démonstration. — Pour l'unicité, L doit être vu comme un espace vectoriel de dimension finie sur K. Soit alors $\|\cdot\|_{\mathrm{L}}$ et $\|\cdot\|'_{\mathrm{L}}$ deux normes sur L prolongeant $\|\cdot\|_{\mathrm{K}}$. Par le théorème 4.1.21, elles sont équivalentes et par la proposition 4.1.12, elles sont alors identiques sur L.

Passons maintenant à la preuve de l'existence. Posons, pour $x \in \mathrm{L}$

$$\|x\|_{\mathrm{L}} = \|\mathrm{N}_{\mathrm{L/K}}(x)\|_{\mathrm{K}}^{1/n}$$

où $n = [\mathrm{L} : \mathrm{K}]$. Nous allons montrer que $\|\cdot\|_{\mathrm{L}}$ fournit un prolongement de $\|\cdot\|_{\mathrm{K}}$ à L. On a :

- $\|x\|_{\mathrm{L}} = 0 \Leftrightarrow \mathrm{N}_{\mathrm{L/K}}(x) = 0 \Leftrightarrow x = 0$,
- $\|xy\|_{\mathrm{L}} = \|\mathrm{N}_{\mathrm{L/K}}(xy)\|_{\mathrm{L}} = \|\mathrm{N}_{\mathrm{L/K}}(x)\,\mathrm{N}_{\mathrm{L/K}}(y)\|_{\mathrm{K}} = \|x\|_{\mathrm{L}}\|y\|_{\mathrm{L}}$,
- Si $x \in \mathrm{K}$, alors $\mathrm{N}_{\mathrm{L/K}}(x) = x^n$ d'où $\|x\|_{\mathrm{L}} = \|x\|_{\mathrm{K}}$.

Donc il reste à montrer que $\|\cdot\|_{\mathrm{L}}$ vérifie

$$\|x + y\|_{\mathrm{L}} \leqslant \|x\|_{\mathrm{L}} + \|y\|_{\mathrm{L}}.$$

Nous allons montrer que si $\|x\|_{\mathrm{L}} \leq 1$. alors

$$\|1 + x\|_{\mathrm{L}} \leqslant 2$$

Par la proposition 4.1.5, on aura l'inégalité triangulaire.

Soit $x \in \mathrm{L}$ et soit $\mathrm{K}(x)$ l'extension de K engendrée par x. Alors

$$\mathrm{N}_{\mathrm{L/K}}(x) = (\mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}(x))^{[\mathrm{L}:\mathrm{K}(x)]},$$

d'où

$$\|x\|_{\mathrm{L}} = \|\mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}(x)\|_{\mathrm{K}}^{1/[\mathrm{K}(x):\mathrm{K}]} = \|x\|_{\mathrm{K}(x)}$$

et

$$\|1 + x\|_{\mathrm{L}} = \|1 + x\|_{\mathrm{K}(x)}.$$

On peut ainsi supposer que $\mathrm{L} = \mathrm{K}(x)$.

Soit $f_x : \mathrm{L} \to \mathrm{L}$ la multiplication par x et soit M la matrice de f_x dans la base $1, x, \ldots, x^{n-1}$ de L/K. Alors :

$$\mathrm{N}_{\mathrm{L/K}}(x) = \det(M), \qquad \mathrm{N}_{\mathrm{L/K}}(1 + x) = \det(I_n + M).$$

Soit $\|M\|_\infty$ la norme du maximum des coefficients. Le lemme suivant joue un rôle clé dans la démonstration.

Lemme 4.2.3. — *La suite $\|M^k\|_\infty$, $k \in \mathbb{N}$, est bornée.*

Démonstration. — Soit $M^k = (a_{ij}^{(k)})_{1\leq i,j\leq n}$. Pour tout k on note $b_k = a_{i_k,j_k}^{(k)}$ un élément de M^k vérifiant

$$\|b_k\|_K = \|M^k\|_\infty.$$

Posons

$$B_k = \frac{1}{b_k} M^k.$$

Alors $\|B_k\|_\infty = 1$ i.e. les matrices B_k appartiennent au compact

$$S = \{X \in M_n(K),\ \|X\|_\infty = 1\}.$$

Demontrons le lemme par l'absurde. Supposons la suite $\|M^k\|_\infty$ non bornée. Alors il existe une sous-suite $\{b_{k_s}\}$ de $\{b_k\}$ telle que $\|b_{k_s}\|_K \to +\infty$. Comme S est compact il existe une sous-suite convergente de la suite B_{k_s}. Pour simplifier la notation on note cette sous-suite encore B_{k_s}. Soit $B = \lim_{s\to\infty} B_{k_s}$ et soit $\psi : \mathrm{L} \to \mathrm{L}$ l'application linéaire dont la matrice dans la base $1, x, \ldots, x^{n-1}$ est B. Comme B_k commutent avec M le passage à la limite donne $BM = MB$, d'où $\psi \circ f_x = f_x \circ \psi$.
Comme $\|x\|_\mathrm{L} \leq 1$, on a

$$\|\det(B)\|_K = \lim_{s\to\infty} \frac{\|\det(M^{k_s})\|_\mathrm{K}}{\|b_{k_s}\|_\mathrm{K}^n} = \lim_{s\to\infty} \frac{\|\mathrm{N}_{\mathrm{L}/\mathrm{K}}(x)\|_K^{k_s}}{\|b_{k_s}\|_\mathrm{K}^n} = \lim_{s\to\infty} \frac{\|x\|_\mathrm{L}^{k_s}}{\|b_{k_s}\|_\mathrm{K}^n} = 0.$$

Donc $\det(B) = 0$ ce qui signifie qu'il existe un élément non-nul $\alpha \in \mathrm{L}$ tel que $\psi(\alpha) = 0$. Comme ψ et f_x commutent on en déduit que

$$\psi(\alpha x^i) = \psi(f_x^i(\alpha)) = f_x^i(\psi(\alpha)) = 0$$

pour tout $i = 1, \ldots, n-1$. Les éléments $\alpha, \alpha x, \ldots, \alpha x^{n-1}$ formant une base de L/K on obtient que $\psi = 0$, d'où $B = 0$. Mais $\|B\|_\infty = \lim_{s\to\infty} \|B_{k_s}\|_\infty = 1$, ce qui donne une contradiction. □

Nous pouvons maintenant terminer la preuve du théorème 4.2.2. Il existe une constante C_1 telle que $\|M^k\|_\infty \leq C_1$ pour tout k. Soit S_n le groupe symétrique. Comme

$$\det(M) = \sum_{\sigma\in S_n} \pm a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

et comme $\#S_n = n!$, on a

$$\|\det(M)\|_{\mathrm{K}} \leqslant n!\|M\|_\infty^n.$$

Soit $C_2 = (n!)^{1/n}$. Alors pour tout $m \geq 1$ on a

$$\|\mathrm{N}_{\mathrm{L/K}}(1+x)\|_{\mathrm{K}}^m = \|\det(I_n+M)^m\|_{\mathrm{K}}^{1/n} \leq C_2\|(I_n+M)^m\|_\infty$$
$$\leq C_2\sum_{k=0}^m \|C_m^k M^k\|_\infty = C_2\sum_{k=0}^m \|C_m^k 1_{\mathrm{K}}\|_{\mathrm{K}}\|M^k\|_\infty \leq C_2C_1\sum_{k=0}^m \|C_m^k 1_{\mathrm{K}}\|_{\mathrm{K}}.$$

Comme $\|C_m^k 1_{\mathrm{K}}\|_{\mathrm{K}} \leq C_n^k$, on obtient

$$\|\mathrm{N}_{\mathrm{L/K}}(1+x)\|_{\mathrm{K}}^m \leq C_1C_2\sum_{k=0}^m C_m^k = C_1C_2 2^m,$$

donc au final

$$\|\mathrm{N}_{\mathrm{L/K}}(1+x)\|_{\mathrm{K}} \leq 2(C_1C_2)^{1/m}$$

pour tout $m \geq 1$. En passant à la limite quand $m \to \infty$ on obtient l'inégalité souhaitée. □

Corollaire 4.2.4. — *Soit* L/K *une extension galoisienne et soit* $G = \mathrm{Gal(L/K)}$. *Alors pour* $x \in \mathrm{L}$ *et* $g \in G$ *on a*

$$\|g(x)\|_{\mathrm{L}} = \|x\|_{\mathrm{L}}.$$

Démonstration. — Il est facile de voir que la formule $\|x\|'_{\mathrm{L}} = \|g(x)\|_{\mathrm{L}}$ définit une valeur absolue sur L qui prolonge $\|\cdot\|_{\mathrm{K}}$. Par unicité du prolongement on a $\|\cdot\|'_{\mathrm{L}} = \|\cdot\|_{\mathrm{L}}$, d'où le corollaire. □

Corollaire 4.2.5. — *Soit* L/K *un extension galoisienne. Alors l'action de* $G = \mathrm{Gal(L/K)}$ *sur* L *est continue.*

Démonstration. — Par le corollaire 4.2.4, on a

$$\|g(x) - g(y)\|_{\mathrm{L}} = \|x-y\|_{\mathrm{L}},$$

d'où le résultat. □

Corollaire 4.2.6. — *Soit* L/K *une extension séparable. Alors les applications* $\mathrm{N_{L/K}}$ *et* $\mathrm{Tr_{L/K}}$ *sont continues.*

Démonstration. — On a

$$\mathrm{N}_{\mathrm{L/K}}(x) = \prod_{\sigma \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\bar{\mathrm{K}})} \sigma(x).$$

Soit M une extension galoisienne finie qui contient L. Alors tout $\sigma \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\bar{\mathrm{K}})$ admet un prolongement $\hat{\sigma}$ à M. Par le corollaire 4.2.6 $\hat{\sigma}$ est continu sur M, donc la fonction

$$x \mapsto \prod_{\hat{\sigma}} \hat{\sigma}(x)$$

est continue sur M ; elle est continue sur $\mathrm{L} \subseteq \mathrm{M}$, d'où le corollaire. Pour $\mathrm{Tr}_{\mathrm{L/K}}$ la preuve est identique. □

4.2.2. Le cas général. —

4.2.2.1. Prolongement. — Dans ce paragraphe on ne suppose pas K complet. On s'intéresse à toutes les valeurs absolues de K qu'on note $\|\cdot\|_v$, où v parcourt une certaine famille d'indices. Pour simplifier la notation on écrira souvent v au lieu de $\|\cdot\|_v$. Soit L/K une extension finie. Une valeur absolue $\|\cdot\|_w$ sur L prolonge $\|\cdot\|_v$ (ou que w est au-dessus de v et on écrit $w \mid v$), si $\|x\|_w = \|x\|_v$ pour tout $x \in \mathrm{K}$. Nous verrons qu'il existe toujours un prolongement de $\|\cdot\|_v$ à L mais qui, en général, n'est pas unique.

Pour simplifier nous supposons toujours que L/K est séparable (c'est le seul cas qui nous intéresse). Alors il existe $\alpha \in \mathrm{L}$ tel que $\mathrm{L} = \mathrm{K}(\alpha)$. On note $f(X) \in \mathrm{K}[X]$ le polynôme minimal de α sur K.

Soit K_v le complété de K pour v.

Le polynôme $f(X)$ peut être réductible sur K_v et on note

$$f(X) = f_1(X)f_2(X)\cdots f_k(X),$$

la factorisation de $f(X)$ en produit de facteurs irréductibles $f_i(X) \in \mathrm{K}_v[X]$.

Comme $i_v : \mathrm{K} \hookrightarrow \mathrm{K}_v$, on a $\bar{\mathrm{K}} \hookrightarrow \bar{\mathrm{K}}_v$ ce qui permet d'identifier les racines de $f(X)$ aux racines des polynômes $f_i(X)$. Comme $f(X)$ est séparable, on a $f_i(X) \neq f_j(X)$ pour $i \neq j$.

Pour tout i, notons $\alpha_{i,1}, \dots \alpha_{i,m_i}$ les racines de $f_i(X)$ puis posons $\mathrm{L}_{ij} = \mathrm{K}_v(\alpha_{ij})$. Comme $f_i(X)$ est irréductible, les corps $\mathrm{L}_{i,1}, \mathrm{L}_{i,2}, \dots, \mathrm{L}_{i,m_i}$ sont conjugués sur K_v. Plus précisement, il existe des isomorphismes

$$\tau_{ij} \ : \ \mathrm{L}_{i1}/\mathrm{K}_v \xrightarrow{\sim} \mathrm{L}_{ij}/\mathrm{K}_v, \qquad j = 1, \dots, m_i$$

vérifiant $\tau_{ij}(\alpha_{i1}) = \alpha_{ij}$.
Soit $\| \cdot \|_{ij}$ la valeur absolue sur L_{ij}. Par unicité du prolongement de la valeur absolue (théorème 4.1.15), il vient pour $x \in \mathrm{L}_{i1}$:

$$\|\tau_{ij}(x)\|_{ij} = \|x\|_{i1}.$$

Pour tout $1 \leqslant i \leqslant k$ et $1 \leqslant j \leqslant m_i$ on note

$$\sigma_{ij} \ : \ \mathrm{L}/\mathrm{K} \to \bar{\mathrm{K}}/\mathrm{K}$$

l'homomorphisme défini par $\sigma_{ij}(\alpha) = \alpha_{ij}$. En composant σ_{ij} avec le plongement $\mathrm{K}(\alpha_{ij}) \hookrightarrow \mathrm{L}_{ij}$ on obtient des homomorphismes

$$\mathrm{L} \xrightarrow{\sigma_{ij}} \mathrm{K}(\alpha_{ij}) \hookrightarrow \mathrm{L}_{ij}$$

qu'on notera encore σ_{ij} pour simplifier. Alors

$$\sigma_{ij} = \tau_{ij} \circ \sigma_{i1}, \qquad j = 1, \dots, m_i.$$

Pour tout $i = 1, \dots, k$ on définit une valeur absolue w_i de L en posant pour $\forall x \in \mathrm{L}$:

$$\|x\|_{w_i} = \|\sigma_{ij}(x)\|_{ij}.$$

Proposition 4.2.7. — *(i) La valeur absolue w_i ne depend pas du choix de $j = 1, \dots, m_i$.*
(ii) Le complété de L *pour w_i est isomorphe à L_{ij}.*
(iii) Les valeurs absolues $w_1, \dots, w_k$ sont deux à deux distincts.

Démonstration. — (i) On a $\|\sigma_{ij}(x)\|_{ij} = \|\tau_{ij}(\sigma_{i1}(x))\|_{ij} = \|\sigma_{i1}(x)\|_{i1}$ ce qui montre que l'on peut poser $j = 1$ dans la définition de w_i.
(ii) Il suffit de se rappeler que $\sigma_{ij}(\mathrm{L})$ est dense dans L_{ij}.
(iii) Comme les polynômes $f_i(X)$ sont deux à deux distincts, les extensions $\mathrm{L}_{1,1}/\mathrm{K}_v, \dots, \mathrm{L}_{k,1}/\mathrm{K}_v$ sont deux à deux non-isomorphes ce qui entraîne que les valeurs absolues $w_1, \dots, w_k$ sont deux à deux non-équivalentes : en effet, si pour tout $x \in \mathrm{L}$, $\|x\|_{w_1} = \|x\|_{w_k}$, alors, par densité de L, il viendrait alors $\mathrm{L}_{1,1} \simeq \mathrm{L}_{k,1}$. □

Théorème 4.2.8. — *Sous les hypothèses de cette section, les valeurs absolues $w_1, \ldots, w_k$ sont précisement celles qui prolongent v. De plus, on a*

$$\sum_{w|v} [\mathrm{L}_w : \mathrm{K}_v] = [\mathrm{L} : \mathrm{K}].$$

Démonstration. — Il est clair que $w_1, \ldots, w_k$ prolongent v. Réciproquement, soit w une valeur absolue sur L qui prolonge v. Alors L_w est une extension de K_v. Soit un homomorphisme $\sigma \ : \ \mathrm{L}_w/\mathrm{K}_v \to \bar{\mathrm{K}}_v/\mathrm{K}_v$. L'élément $\sigma(\alpha)$ est une racine de $f(X)$ dans $\bar{\mathrm{K}}_v$ i.e. il existe i et j tels que $\sigma(\alpha) = \alpha_{ij}$. Donc σ fournit un isomorphisme

$$\sigma \ : \ \mathrm{L}_w/\mathrm{K}_v \to \mathrm{L}_{ij}/\mathrm{K}_v.$$

Par l'unicité du prolongement, la valeur absolue sur L_w est donnée par

$$\|x\|_{\mathrm{L}_w} = \|\sigma(x)\|_{ij}.$$

En particulier, si $x \in \mathrm{L}$ on a

$$\|x\|_{\mathrm{L}_w} = \|\sigma_{ij}(x)\|_{ij} = \|x\|_{w_i},$$

d'où $w = w_i$.
Comme $[\mathrm{L}_{w_i} : \mathrm{K}_v] = [\mathrm{L}_{ij} : \mathrm{K}_v] = m_i$ on a

$$\sum_{i=1}^{k} [\mathrm{L}_{w_i} : \mathrm{K}_v] = \sum_{i=1}^{k} m_i = \deg(f) = [\mathrm{L} : \mathrm{K}].$$

Le théorème est démontré. □

Corollaire 4.2.9. — *Pour tout $\sigma \in \mathrm{Hom}_{\mathrm{K}_v}(\mathrm{L}_w, \bar{\mathrm{K}}_v)$ la restriction $\sigma|_{\mathrm{L}}$ de σ à* L *est un homomorphisme* $\mathrm{L}/\mathrm{K} \to \bar{\mathrm{K}}/\mathrm{K}$ *et l'application*

$$\begin{array}{rcl} \bigcup_{w|v} \mathrm{Hom}_{\mathrm{K}_v}(\mathrm{L}_w, \bar{\mathrm{K}}_v) & \to & \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \bar{\mathrm{K}}), \\ \sigma & \mapsto & \sigma|_{\mathrm{L}} \end{array}$$

ainsi définie, est une bijection.

Démonstration. — Comme

$$\#(\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \bar{\mathrm{K}})) = [\mathrm{L} : \mathrm{K}]$$

et

$$\#(\mathrm{Hom}_{\mathrm{K}_v}(\mathrm{L}_w, \bar{\mathrm{K}}_v)) = [\mathrm{L}_w : \mathrm{K}_v]$$

les ensembles $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\bar{\mathrm{K}})$ et $\bigcup_{w|v}\mathrm{Hom}_{\mathrm{K}_v}(\mathrm{L}_w,\bar{\mathrm{K}}_v)$ ont même cardinal, il suffit de montrer la surjectivité. Tout élément de $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\bar{\mathrm{K}})$ est de la forme $\sigma_{ij}\ :\ \mathrm{L}/\mathrm{K}\to\mathrm{K}(\alpha_{ij})$, $1\leqslant i\leqslant k$, $1\leqslant j\leqslant m_i$. Par continuité, σ_{ij} se prolonge à un isomorphisme $\phi_{ij}\ :\ \mathrm{L}_{w_i}\simeq\mathrm{L}_{ij}\subset\bar{\mathrm{K}}_v$ qui vérifie, donc, la condition $\phi_{ij}|_{\mathrm{L}}=\sigma_{ij}$. □

Corollaire 4.2.10. — *Soit v une valeur absolue sur* K. *Alors pour tout $x\in\mathrm{L}$ on a*

$$i_w(\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(x))=\sum_{w|v}\mathrm{Tr}_{\mathrm{L}_w/\mathrm{K}_v}(i_w(x)),$$

$$i_w(\mathrm{N}_{\mathrm{L}/\mathrm{K}}(x))=\prod_{w|v}\mathrm{N}_{\mathrm{L}_w/\mathrm{K}_v}(i_w(x)),$$

où i_w est le plongement de L *dans* L_w.

Démonstration. — Comme

$$\mathrm{Tr}_{\mathrm{L}/\mathrm{K}}(x)=\sum_{\sigma\in\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\bar{\mathrm{K}})}\sigma(x),$$

$$\mathrm{N}_{\mathrm{L}/\mathrm{K}}(x)=\prod_{\sigma\in\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\bar{\mathrm{K}})}\sigma(x),$$

le corollaire découle du corollaire 4.2.9. □

4.2.2.2. Extensions galoisiennes. — Nous supposons maintenant que L/K est une extension galoisienne finie. On note $G=\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ le groupe de Galois de L/K. Soit v une valeur absolue sur K et soit

$$S_v=\{w,\ \ w\mid v\}$$

l'ensemble des valeurs absolues sur L qui prolongent v. Soit $w\in S_v$. Pour tout $g\in G$ on pose :

$$\|x\|_{gw}=\|g^{-1}(x)\|_w.$$

Il est facile de voir que gw est une valeur absolue qui prolonge v. Pour tous $g_1,g_2\in G$ on a :

$$\|x\|_{(g_1g_2)w}=\|(g_1g_2)^{-1}(x)\|_w=\|g_2^{-1}(g_1^{-1}x)\|_w=\|g_1^{-1}(x)\|_{g_2w}=\|x\|_{g_1(g_2w)}.$$

Ainsi

$$(g_1 g_2)w = g_1(g_2 w),$$

ce qui signifie que le groupe G opère sur S_v.

Définition 4.2.11. — Le stabilisateur de w dans G est appelé groupe de décomposition de w et on le note G_w :

$$G_w = \{g \in G \,|\, gw = w\}.$$

Remarque 4.2.12. — Avant de continuer, remarquons que comme L/K est galoisienne, il vient $\mathrm{L}_{11} = \mathrm{K}_v(\alpha_{11}) = \mathrm{K}_v(\alpha_{i1}) = \mathrm{L}_{i1}$.

On déduit de cette définition les propriétés suivantes :

Proposition 4.2.13. — *(i) Pour tout $g \in G$ on a $G_{gw} = g\, G_w g^{-1}$;*
(ii) Soit $\{x_n\} \subset \mathrm{L}$ une suite de Cauchy pour w. Si $g \in G_w$, alors $\{g(x_n)\}$ est une suite de Cauchy pour w.
(iii) On a une injection naturelle

$$G_w \hookrightarrow \mathrm{Gal}(\mathrm{L}_w/\mathrm{K}_v) = \mathrm{Gal}(\mathrm{L}_{ij}/\mathrm{K}_v),$$

pour un certain couple (i, j).

Démonstration. — (i) C'est immédiat.

Ensuite

$$\|g(x_n) - g(x_m)\|_w = \|g(x_n - x_m)\|_w = \|x_n - x_m\|_{g^{-1}w} = \|x_n - x_m\|_w,$$

d'où la propriété (ii).
(iii) Par (ii), tout automorphisme $g \in G_w$ se prolonge par continuité à L_w. □

La proposition précédente peut être précisée.

Théorème 4.2.14. — *(i) Le groupe de Galois G opère sur S_v transitivement i.e. pour tout $w, w' \in S_v$ il existe $g \in G$ tel que $w' = gw$.*
(ii) L'injection $G_w \hookrightarrow \mathrm{Gal}(\mathrm{L}_w/\mathrm{K}_v)$ est un isomorphisme.

Démonstration. — Soit $G = \bigcup_{i=1}^{r} g_i G_w$ la décomposition de G selon G_w et soit $w_i = g_i w$. Comme l'ordre de $\mathrm{Gal}(\mathrm{L}_w/\mathrm{K}_v)$ est égal à $[\mathrm{L}_w : \mathrm{K}_v]$, on a :

$$|G| = r|G_w| = \sum_{i=1}^{r} |G_{w_i}| \leq \sum_{i=1}^{r} [\mathrm{L}_{w_i} : \mathrm{K}_v = \sum_{w|v} [\mathrm{L}_w : \mathrm{K}_v] = [\mathrm{L} : \mathrm{K}] = |G|.$$

On a des égalités partout. En particulier :
a) $|G_{w_i}| = [\mathrm{L}_{w_i} : \mathrm{K}_v]$ ce qui montre que les injections $G_{w_i} \hookrightarrow \mathrm{Gal}(\mathrm{L}_{w_i}/\mathrm{K}_v)$ sont des isomorphismes ;
b) $w_1 = g_1(w), \ldots, w_r = g_r(w)$ sont exactement les valeurs absolues au-dessus de v, d'où l'on en déduit que G opère transitivement sur S_v. □

4.3. Valeurs absolues non-archimédiennes

4.3.1. Anneau de valuation. —

Définition 4.3.1. — Soient K un corps et $\| \cdot \|$ une valeur absolue sur K. On dit que $\| \cdot \|$ est non-archimédienne (ou ultramétrique) si

$$\|x + y\| \leqslant \max\{\|x\|, \|y\|\}.$$

Voici quatre propriétés élémentaires des valeurs absolues non-archimédiennes qui découlent directement de cette définition.

Proposition 4.3.2. — *(i) Soit $\| \cdot \|$ une valeur absolue non-archimédienne. Si $\|x\| > \|y\|$, alors*

$$\|x + y\| = \|x\|.$$

(ii) $\| \cdot \|$ est non-archimédienne si, et seulement si, $\|x\| \leq 1$ implique $\|1 + x\| \leq 1$.

(iii) Une valeur absolue $\| \cdot \|$ est non-archimédienne si et seulement si

$$\|n1_{\mathrm{K}}\| \leq 1, \qquad \text{pour tout } n \in \mathbb{N}.$$

(iv) Soit L/K *une extension de corps. Soit $\| \cdot \|'$ une valeur absolue sur* L *qui prolonge $\| \cdot \|$. Si $\| \cdot \|$ est non-archimédienne, alors $\| \cdot \|'$ l'est aussi.*

Démonstration. — i) Si $\| \cdot \|$ est non-archimédienne, alors

$$\|x+y\| \leqslant \max\{\|x\|, \|y\|\} = \|x\|.$$

D'autre part,

$$\|x\| = \|(x+y)-y\| \leqslant \max\{\|x+y\|, \|y\|\} = \|x+y\|,$$

car $\|x\| > \|y\|$.
ii) C'est clair.
iii) Soit $\|x\| \leq 1$. Alors

$$\begin{aligned}\|1+x\|^n = \|(1+x)^n\| = \ & \|\sum_{k=0}^{n} C_n^k x^k\| \leq \sum_{k=0}^{n} \|C_n^k 1_{\mathrm{K}}\| \|x\|^k \\ & \leq \sum_{k=0}^{n} \|x\|^k \leq n+1.\end{aligned}$$

Donc $\|1+x\| \leq (n+1)^{1/n}$. En passant à la limite quand $n \to \infty$ on obtient $\|1+x\| \leq 1$ ce qui montre que $\| \cdot \|$ est non-archimédienne.
iv) Découle directement de iii). □

Proposition 4.3.3. — *Soit* K *un corps muni d'une valeur absolue non-archimédienne* $\| \cdot \|$. *Alors l'ensemble*

$$\mathcal{O} = \{x \in \mathrm{K},\ \|x\| \leq 1\}$$

est l'anneau de valuation de K. *Le groupe des unité* $\mathcal{O}^\times$ *de* $\mathcal{O}$ *coïncide avec*

$$U = \{x \in \mathrm{K},\ \|x\| = 1\}.$$

L'ensemble

$$\mathfrak{m} = \{x \in \mathrm{K},\ \|x\| < 1\}$$

est l'unique idéal maximal de $\mathcal{O}$. *Le corps des fractions de* $\mathcal{O}$ *coïncide avec* K *dans lequel* $\mathcal{O}$ *est intégralement clos.*

Démonstration. — Soient $x, y \in \mathcal{O}$. Alors

$$\begin{aligned}&\|x \pm y\| \leq \max\{\|x\|, \|y\|\} \leq 1, \\ &\|xy\| = \|x\|\,\|y\|,\end{aligned}$$

d'où l'on en déduit que $\mathcal{O}$ est un anneau.
Soit $x \in \mathcal{O}$. Alors $x^{-1} \in \mathcal{O}$ si et seulement si $\|x\|^{-1} = \|x^{-1}\| \leq 1$. On en déduit que x est une unité si et seulement si $\|x\| = 1$.

Pour tout $x, y \in \mathfrak{m}$ on a

$$\|x \pm y\| \leq \max\{\|x\|, \|y\|\} < 1.$$

Si $x \in \mathcal{O}$ et $y \in \mathfrak{m}$, alors

$$\|xy\| = \|x\| \, \|y\| < 1.$$

Donc, $\mathfrak{m}$ est un idéal de $\mathcal{O}$ et on a

$$U \cup \mathfrak{m} = \mathcal{O}.$$

Soit $\mathfrak{a}$ un idéal de $\mathcal{O}$. Si $\mathfrak{a} \nsubseteq \mathfrak{m}$, alors $\mathfrak{a} \cap U \neq \varnothing$ i.e. $\mathfrak{a}$ contient une unité de $\mathcal{O}$, d'où $\mathfrak{a} = \mathcal{O}$. Donc $\mathfrak{m}$ est l'idéal maximal de $\mathcal{O}$.
Soit $x \in \mathrm{K}$. Si $\|x\| \leq 1$, on a $x \in \mathcal{O}$ juste par définition. Sinon $\|x\| > 1$, d'où $\|1/x\| < 1$ et $x^{-1} \in \mathcal{O}$. Donc K est le corps des fractions de $\mathcal{O}$.
On montre que $\mathcal{O}$ est intégralement clos dans K. Soit $x \in \mathrm{K}$ un élément entier sur $\mathcal{O}$. Alors

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 = 0, \qquad a_i \in \mathcal{O}.$$

Supposons $x \notin \mathcal{O}$. Alors $\rho = \|x\| > 1$, d'où

$$\|x^n\| = \rho^n,$$
$$\|a_i x^i\| = \|a_i\|\|x\|^i \leq \|x\|^i = \rho^i \leq \rho^n, \qquad \textit{pour } 0 \leq i \leq n-1.$$

Par la proposition 4.3.2 i), on obtient

$$0 = \|0\| = \|x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0\| = \|x^n\| > 1,$$

d'où la contradiction. □

Définition 4.3.4. — Le corps $k = \mathcal{O}/\mathfrak{m}$ est appelé corps résiduel de l'anneau $\mathcal{O}$.

4.3.2. Convergence des séries. — Soit $(\mathrm{K}, \|\cdot\|_{\mathrm{K}})$ un corps complet et soit la série sur K

$$S = \sum_{k=0}^{\infty} a_k.$$

La série S est convergente dans K si et seulement si la suite

$$S_n = \sum_{k=0}^{n} a_k$$

est une suite de Cauchy. En particulier, si la série est convergente, alors

$$\|a_n\|_{\mathrm{K}} = \|S_n - S_{n-1}\|_{\mathrm{K}} \underset{n\to\infty}{\to} 0.$$

Dans le cas général la réciproque est fausse. Neanmoins, si la valeur absolue $\| \cdot \|_{\mathrm{K}}$ est non-archimédienne, la situation est très agréable :

Proposition 4.3.5. — *Soit* K *un corps complet pour une valeur absolue non-archimédienne. Alors une série*

$$\sum_{k=1}^{\infty} a_k, \qquad a_k \in \mathrm{K}$$

est convergente si et seulement si $a_k \underset{k\to\infty}{\to} 0$.

Démonstration. — Soit

$$S_n = \sum_{k=0}^{n} a_k.$$

Si $m \geqslant n$, alors

$$\|S_m - S_n\|_{\mathrm{K}} = \| \sum_{k=n+1}^{m} a_k\|_{\mathrm{K}} \leqslant \max_{n+1\leqslant k\leqslant m}\|a_k\|_{\mathrm{K}}.$$

Soit $\epsilon > 0$. Il existe N tel que $\|a_k\|_{\mathrm{K}} < \epsilon$ pour tout $k > N$. Alors, pour tous $m, n \geqslant N$ on a

$$\|S_m - S_n\|_{\mathrm{K}} < \epsilon.$$

Donc S_n est une suite de Cauchy ce qui entraîne la convergence car K est complet. □

4.3.3. Le lemme de Hensel. — Le résultat suivant est central.

Proposition 4.3.6 **(lemme de Hensel)**. — *Soit* K *un corps complet pour une valeur absolue non-archimédienne* $\|\cdot\|_{\mathrm{K}}$. *Soit* $f(X)$ *un polynôme à coefficients dans l'anneau de valuation* $\mathcal{O}$ *de* K. *Si* α_0 *est un élément de* $\mathcal{O}$ *vérifiant*

$$\|f(\alpha_0)\|_{\mathrm{K}} < \|f'(\alpha_0)^2\|_{\mathrm{K}}\,,$$

alors la suite

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

converge vers une racine α *de* $f(X)$. *De plus,* $\alpha \in \mathcal{O}$ *et* $\alpha \equiv \alpha_0 \pmod{\mathfrak{m}}$.

Démonstration. — Posons $\gamma = \left\| \dfrac{f(\alpha_0)}{f'(\alpha_0)^2} \right\|_{\mathrm{K}} < 1$. On va démontrer par récurrence que pour tout $i \geqslant 1$ on a

(i) $\|\alpha_i\|_{\mathrm{K}} \leq 1$;

(ii) $\|f'(\alpha_i)\|_{\mathrm{K}} = \|f'(\alpha_0)\|_{\mathrm{K}}$;

(iii) $\|\alpha_i - \alpha_0\|_{\mathrm{K}} \leq \gamma$;

(iv) $\|\dfrac{f(\alpha_i)}{f'(\alpha_i)^2}\|_{\mathrm{K}} \leq \gamma^{2^i}$.

Le développement en série de Taylor de f en α_i donne

$$f(\alpha_i + h) = f(\alpha_i) + hf'(\alpha_i) + h^2 g\,,$$

où $g \in \mathcal{O}$ est un élément qui dépend de h et de α_i. En prenant $h = -f(\alpha_i)/f'(\alpha_i)$, on obtient

$$f(\alpha_{i+1}) = -\frac{f(\alpha_i)^2}{f'(\alpha_i)^2} g\,.$$

Si les formules $i) - ii)$ sont vraies au rang i, alors

$$\|f(\alpha_{i+1})\|_{\mathrm{K}} \leqslant \|f'(\alpha_i)^2\|_{\mathrm{K}} \left\| \frac{f(\alpha_i)}{f'(\alpha_i)^2} \right\|_{\mathrm{K}}^2 \leqslant \|f'(\alpha_i)^2\|_{\mathrm{K}} \gamma^{2^{i+1}}\,.$$

D'autre part, de la même manière on a (en considérant le développement de Taylor de f' en α_i)

$$f'(\alpha_{i+1}) \;=\; f'(\alpha_i) - f''(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \cdots = f'(\alpha_i)\left(1 - f''(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)^2} + \cdots\right).$$

Comme

$$\left\| \frac{f(\alpha_i)}{f'(\alpha_i)^2} \right\|_{\mathrm{K}} < 1$$

alors

$$1 - f''(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)^2} + \cdots \in \mathcal{O}^\times.$$

Par conséquent

$$\|f'(\alpha_{i+1})\|_{\mathrm{K}} = \|f'(\alpha_i)\|_{\mathrm{K}} = \|f'(\alpha_0)\|_{\mathrm{K}}$$

et $(i), (ii)$ et (iv) sont établies (à l'ordre $i+1$).
Le point (iii) s'obtient par inégalité triangulaire.

Pour déduire la proposition de ces formules on remarque que comme

$$\left\| \frac{f(\alpha_i)}{f'(\alpha_i)} \right\|_{\mathrm{K}} = \left\| \frac{f(\alpha_i)}{f'(\alpha_i)^2} \right\|_{\mathrm{K}} \|f'(\alpha_0)\|_{\mathrm{K}} \leqslant \gamma^{2^i} \|f'(\alpha_0)\|_{\mathrm{K}} \underset{i\to\infty}{\to} 0$$

la suite $\dfrac{f(\alpha_i)}{f'(\alpha_i)}$ tend vers 0. En utilisant le fait que la norme est ultramétrique, on en déduit que la suite $\{\alpha_i\}$ est de Cauchy donc convergente. Soit $\alpha = \lim_{i\to\infty} \alpha_i$. A la limite on obtient

$$\alpha = \alpha - f(\alpha)/f'(\alpha)$$

i.e. $f(\alpha) = 0$. □

Voici un cas particulier très utile du lemme de Hensel.

Proposition 4.3.7. — *Soit* K *un corps complet pour une valeur absolue non-archimédienne* $\|\cdot\|_{\mathrm{K}}$. *Notons par* $\mathcal{O}$ *l'anneau de valuation de* K. *Soit* $f(X) \in \mathcal{O}[X]$ *un polynôme à coefficients dans* $\mathcal{O}$ *et soit* $\bar{f}(X) \in k[X]$ *la réduction de* $f(X)$ *modulo* $\mathfrak{m}$. *Si* $\bar{\alpha} \in k$ *est une racine simple de* $\bar{f}(X)$, *alors il existe une unique racine* $\alpha \in \mathcal{O}$ *de* $f(X)$ *telle que* $\bar{\alpha} = \alpha \pmod{\mathfrak{m}}$.

Démonstration. — Soit α_0 un relèvement de $\bar{\alpha}$. Comme $\bar{\alpha}$ est une racine simple de $\bar{f}(X)$, on a $\bar{f}'(\bar{\alpha}) \neq 0$ ce qui signifie que $f'(\alpha_0)$ est une unité de $\mathcal{O}$. D'autre part, comme $\bar{f}(\bar{\alpha}) = 0$, on a $\|f(\alpha_0)\|_{\mathrm{K}} < 1$ et on peut appliquer le lemme de Hensel. L'existence de α s'en déduit.
Pour démontrer l'unicité de la solution supposons que β est une autre racine de $f(X)$ vérifiant $\alpha = \beta \pmod{\mathfrak{m}}$. Alors $(X-\alpha)(X-\beta)$ divise f dans $\mathcal{O}[X]$. Après réduction modulo $\mathfrak{m}$, on obtient que $(X-\bar{\alpha})^2$ divise $\bar{f}$, ce qui donne une contradiction. □

4.3.4. Les anneaux à valuation discrète. —

Définition 4.3.8. — Soit K un corps. On appelle valuation discrète sur K une application surjective

$$v \ : \ \mathrm{K}^* \to \mathbb{Z},$$

satisfaisant aux propriétés suivantes :
i) v est un homomorphisme, i.e.

$$v(xy) = v(x) + v(y)$$

pour tout $x, y \in \mathrm{K}^*$.
ii) Pour tout $x, y \in \mathrm{K}^*$ on a

$$v(x+y) \geqslant \min\{v(x), v(y)\}.$$

On prolonge v sur K en posant $v(0) = +\infty$.

Remarque 4.3.9. — L'hypothèse de surjectivité n'est pas importante et sert à normaliser v. En effet, si $v : \mathrm{K}^* \to \mathbb{Z}$ est un homomorphisme non-nul, alors son image $v(\mathrm{K}^*)$ est un sous-groupe de $\mathbb{Z}$. Donc, il existe $n > 0$ tel que $v(\mathrm{K}^*) = n\mathbb{Z}$ et en posant $v'(x) = v(x)/n$ un obtient un homomorphisme surjectif $v' : \mathrm{K}^* \to \mathbb{Z}$.

Soit K un corps muni d'une valuation discrète v. On fixe un réel $\rho \in]0;1[$ et on pose

$$\|x\|_v = \rho^{v(x)}, \qquad x \in \mathrm{K}.$$

Alors on a

(i) $\|x\|_v = 0$ si et seulement si $v(x) = +\infty$ i.e. si et seulement si $x = 0$;
(ii) $\|xy\|_v = \rho^{v(x)+v(y)} = \|x\|_v \, \|y\|_v$;
(iii) $\|x+y\|_v \leqslant \rho^{\min\{v(x),v(y)\}} = \max\{\|x\|_v, \|y\|_v\}$.

Ainsi $\| \cdot \|_v$ est une valeur absolue non archimédienne sur K.

Soit ρ_1 un autre réel $\in]0;1[$. Alors il existe $c > 0$ tel que $\rho_1 = \rho^c$. Si $\|x\|_1 = \rho_1^{v(x)}$ est la valeur absolue associée à ρ_1, alors pour tout $x, y \in \mathrm{K}$,

$$\|x\|_1 = \|x\|_v^c$$

et ainsi $\| \cdot \|_1$ et $\| \cdot \|_v$ sont équivalentes *i.e.*, qu'elles induisent la même topologie sur K.

Définition 4.3.10. — Soit A un anneau intègre. On dit que A est un anneau de valuation discrète s'il est principal et s'il possède un unique idéal premier non-nul (cet idéal est aussi maximal).

Soit $\mathfrak{m}$ l'idéal maximal de A. Alors il est principal et son générateur π est appelé une uniformisante de A :

$$\mathfrak{m} = (\pi).$$

Si π' est une autre uniformisante de A, alors $\pi' = u\pi$, où $u \in A^\times$ est une unité de A. Tout élément non-nul $a \in A$ s'écrit

$$a = u\pi^k, \qquad u \in A^\times,\ k \in \mathbb{N}$$

et on a

$$A = \mathfrak{m} \cup A^\times, \qquad \mathfrak{m} \cap A^\times = \varnothing.$$

Etablissons le lien entre les anneaux de valuation discrète et les valuations discrètes.

Théorème 4.3.11. — *1) Soit* K *un corps muni d'une valuation discrète* v*. Alors*

$$A_v = \{x \in \mathrm{K} \,|\, v(x) \geqslant 0\}$$

est un anneau de valuation discrète. Plus précisement :

i) $U = \{x \in \mathrm{K} \,|\, v(x) = 0\}$ *coïncide avec le groupe des unités de* A_v*.*

ii) $\mathfrak{m}_{A_v} = \{x \in \mathrm{K} \,|\, v(x) > 0\}$ *est l'idéal maximal de* A_v *;*

iii) un élément $\pi \in A_v$ *est une uniformisante de* A_v *si et seulement si* $v(\pi) = 1$ *;*

v) Le corps des fractions de A_v *coïncide avec* K*.*

2) Réciproquement. Soit A *un anneau de valuation discrète et soit* K *son corps des fractions. Tout élément non-nul* $x \in \mathrm{K}$ *s'écrit de façon unique sous la forme*

$$x = \pi^n u, \qquad u \in A^\times,\ n \in \mathbb{Z}.$$

Posons

$$v(x) = n.$$

Alors v *est une valuation discrète sur* K *telle que* $A_v = A$ *et* $\mathfrak{m}_{A_v} = (\pi)$*.*

Démonstration. — Comme

$$A_v = \{x \in \mathrm{K},\ \|x\|_v \leq 1\},$$

la proposition 4.3.3 montre que A_v est l'anneau de valuation de v. La même proposition indique que $U = \{x \in A_v \,|\, v(x) = 0\}$ est le groupe des unités de A_v et que $\mathfrak{m}_{A_v}$ est l'unique idéal maximal de A_v.

Montrons que A_v est un anneau principal. Soit $\pi \in A_v$ un élément tel que $v(\pi) = 1$. Pour tout $x \in A_v$ posons

$$u = x/\pi^{v(x)}.$$

Alors $v(u) = v(x) - v(\pi^{v(x)}) = v(x) - v(x) = 0$, d'où

$$x = u\pi^{v(x)}, \qquad u \in U.$$

Soit $\mathfrak{a}$ un idéal non-nul de A_v. Posons

$$n = \min\{v(x) \,|\, x \in \mathfrak{a}\}.$$

Alors $\mathfrak{a}$ contient un élément $x_0 \in A_v$ tel que $v(x_0) = n$. Comme x_0 s'écrit $x_0 = u_0\pi^n$ avec $u_0 \in U$, on obtient que $\pi^n = u_0^{-1}x_0 \in \mathfrak{a}$, d'où

$$(\pi^n) \subseteq \mathfrak{a}.$$

Réciproquement, si $x \in \mathfrak{a}$, alors $v(x) \geqslant n$. Posons $y = x/\pi^n$. Comme $v(y) = v(x) - v(\pi^n) \geqslant 0$, on a $y \in A_v$. Alors $x = y\pi^n \in (\pi^n)$ ce qui montre que $I \subseteq (\pi^n)$. Donc $\mathfrak{a} = (\pi^n)$ ce qui montre que tout idéal de A_v est principal.
En particulier, on a :

$$\mathfrak{m}_{A_v} = (\pi)$$

ce qui montre que π est une uniformisante de A_v.

2) Soit A un anneau de valuation discrète. Alors tout élément non-nul $x \in A$ s'écrit de façon unique sous la forme

$$x = u\pi^n, \qquad n \in \mathbb{N},\ u \in A^\times.$$

Donc, tout élément x du corps des fractions K de A sécrit de façon unique sous la forme

$$x = u\pi^n, \qquad n \in \mathbb{Z},\ u \in A^\times.$$

On pose $v(x) = n$. Si $y = u'\pi^m$, alors

$$v(xy) = v(uu'\pi^{n+m}) = n + m = v(x) + v(y).$$

D'autre part, si $n \geqslant m$, alors

$$x + y = \pi^m(u' + u\pi^{n-m}),$$

où $u' + u\pi^{n-m} \in A$. Donc

$$v(x + y) \geqslant v(\pi^m) = m = \min\{v(x), v(y)\},$$

ce qui montre que v est une valuation discrète de K. Les formules $A_v = A$ et $\mathfrak{m}_{A_v} = (\pi)$ découlent directement de la définition de v. □

Soient K un corps muni d'une valuation discrète v, A_v l'anneau de valuation, et

$$\|x\|_v = \rho^{v(x)}$$

une valeur absolue associée à v. On note K_v le complété de K pour la topologie induite par $\| \cdot \|_v$.

Proposition 4.3.12. —
Soit K *un corps muni d'une valuation discrète v. Alors la valuation discrète v admet un unique prolongement sur* K_v. *Le corps* K_v *est muni, ainsi, d'une valuation discrète pour laquelle il est complet. L'anneau de valuation $\mathcal{O}_v$ de* K_v *coïncide avec l'adhérence de A_v dans* K_v *et son idéal maximal $\mathfrak{m}_v$ coïncide avec l'adhérence de $\mathfrak{m}_{A_v}$. Le corps résiduel $\mathcal{O}_v/\mathfrak{m}_v$ est canoniquement isomorphe à $k_v = A_v/\mathfrak{m}_{A_v}$.*

Démonstration. — Par le théorème 4.1.15, il existe un unique prolongement de $\| \cdot \|_v$ à K_v qu'on note encore $\| \cdot \|_v$ à K_v pour simplifier. Soit $x \in \mathrm{K}_v$ un élément non-nul. Il existe une suite $\{x_n\} \subset \mathrm{K}$ telle que $x = \lim_{n\to\infty} x_n$. On a

$$\|x\|_v = \lim_{n\to\infty} \|x_n\|_v = \lim_{n\to\infty} \rho^{v(x_n)}.$$

Comme la suite $\|x_n\|_v$ est convergente, la suite $v(x_n)$ l'est aussi et comme $v(x_n)$ sont des entiers ceci signifie qu'elle est stationnaire i.e. il existe $N > 0$ tel que $\forall n \geqslant N$:

$$v(x_n) = v(x_{n+1}).$$

Posons

$$v(x) = v(x_N) = \lim_{n\to\infty} v(x_n) \in \mathbb{Z}. \tag{5}$$

Alors

$$\|x\|_v = \rho^{v(x)}, \qquad x \in \mathrm{K}_v.$$

On en déduit que

$$v(x+y) \geqslant \min\{v(x), v(y)\},$$
$$v(xy) = v(x) + v(y),$$

ce qui montre que (5) fournit un prolongement de v à K_v. Il est unique.

Soit $\mathcal{O}_v$ l'anneau de valuation de K_v. Si $x = \lim_{n\to\infty} x_n \in \mathcal{O}_v$, alors $v(x) \geqslant 0$ d'où $v(x_n) \geqslant 0$ pour $n \geqslant N$. Donc $x_n \in A_v$ pour $n \geqslant N$ ce qui montre que x appartient à l'adhérence de A_v. Le même raisonnement montre que $\mathfrak{m}_v$ coïncide avec l'adhérence de $\mathfrak{m}_{A_v}$.
Comme $A_v \subseteq \mathcal{O}_v$ et $\mathfrak{m}_{A_v} = \mathfrak{m}_v \cap A_v$, on a une injection

$$A_v/\mathfrak{m}_{A_v} \hookrightarrow \mathcal{O}_v/\mathfrak{m}_v.$$

Pour montrer que c'est un isomorphisme on remarque que si $y \in \mathcal{O}_v$, il existe $x \in A_v$ tel que $v(x-y) \geqslant 1$ (A_v est dense dans $\mathcal{O}_v$). Donc, $x - y \in \mathfrak{m}_v$, d'où $x + \mathfrak{m}_v = y + \mathfrak{m}_v$, ce qui montre que l'image de $x + \mathfrak{m}_{A_v}$ dans $\mathcal{O}_v/\mathfrak{m}_v$ est $y + \mathfrak{m}_v$. La proposition est démontrée. □

Théorème 4.3.13. — *Soit* K *un corps muni d'une valuation discrète* v. *Notons par* $\|\cdot\|$ *le norme associée à cette valuation. Alors les assertions suivantes sont équivalentes :*

(i) L'anneau de valuation $\mathcal{O}$ *est compact.*
(ii) Le corps K *est localement compact.*
(iii) Le corps $(\mathrm{K}, \|\cdot\|)$ *est complet et le corps résiduel* $\mathcal{O}/\mathfrak{m}$ *est fini.*

Démonstration. — (i) $\Longrightarrow$ (ii) : On note que $\mathcal{O} = B_f(0,1)$ puis on utilise la proposition 4.1.25.
(ii) $\Longrightarrow$ (iii) : Si K est localement compact, alors K est complet. Supposons le corps résiduel k non fini. Alors, il existe une suite (x_n) d'élements de $\mathcal{O}$ d'images différentes dans k. Cela signifie $v(x_n - x_m) = 0$ pour $n \neq m$. Or, comme $\mathcal{O}$ est supposé compact, ceci est en contradiction avec le fait que l'on peut extraire de (x_n) une sous-suite convergente.
(iii) $\Longrightarrow$ (i) : Soit (x_n) une suite d'éléments de $\mathcal{O}$.
Comme $\mathcal{O}/\mathfrak{m}$ est fini, il existe une infinité d'indice i tels que $x_i \equiv a_0 (\mathrm{mod}\ \mathfrak{m}) \in k$, pour un certain $a_0 \in \mathrm{K}$. Notons $S_{a_0} = \{x_i \in \mathcal{O},\ x_i \equiv a_0 (\mathrm{mod}\ \mathfrak{m})\}$. Comme $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathcal{O}/\mathfrak{m}$, il existe une infinité d'indice i tel que $x_i \in S_{a_0}$ et tel que $x_i - a_0 \equiv a_1\pi (\mathrm{mod}\ \mathfrak{m}^2)$, pour un certain élément $a_1 \in \mathrm{K}$, ici π est une uniformisante de $\mathcal{O}$. Notons $S_{a_0,a_1} = \{x_i \in \mathcal{O},\ x_i \equiv a_0 + a_1\pi (\mathrm{mod}\ \mathfrak{m}^2)\}$. Remarquons alors que pour $x, y \in S_{a_0,a_1}$, on a $v(x-y) \geq 2$. En continuant ainsi, on obtient donc une sous-suite de $(x_i)_i$ qui est de Cauchy. Comme K est complet, cette sous-suite converge, d'où la compacité de $\mathcal{O}$. □

4.4. Valuations discrètes dans un anneau de Dedekind

4.4.1. Rappels. — Nous revenons à l'étude des anneaux de Dedekind. Soit A un anneau de Dedekind et soit K son corps des fractions. Soit $\mathfrak{p}$ un idéal premier non-nul de A. Rappelons alors (corollaire 2.3.13)

$$\mathrm{v}_{\mathfrak{p}} \ : \ \mathrm{K}^* \to \mathbb{Z}$$

la valuation discrète de K définie comme suit. Soit $x \in \mathrm{K}^*$. Alors l'idéal fractionnaire xA s'écrit de façon unique sous la forme

$$xA = \mathfrak{p}^{n_{\mathfrak{p}}} \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{n_{\mathfrak{q}}}.$$

On pose alors

$$\mathrm{v}_{\mathfrak{p}}(x) = n_{\mathfrak{p}}.$$

Voici une conséquence immédiate du lemme d'approximation (lemme 2.4.9).

Proposition 4.4.1. — *Si $\mathfrak{p} \neq \mathfrak{q}$, les valuations $\mathrm{v}_{\mathfrak{p}}$ et $\mathrm{v}_{\mathfrak{q}}$ ne sont pas équivalentes.*

Démonstration. — Soit $\pi_{\mathfrak{p}}$ une uniformisante de $A_{\mathfrak{p}}$. Par le lemme 2.4.9, il existe $x \in A$ tel que $\mathrm{v}_{\mathfrak{p}}(x - \pi_{\mathfrak{p}}) \geqslant 2$ et $\mathrm{v}_{\mathfrak{q}}(x - 1) \geqslant 1$. Donc

$$\mathrm{v}_{\mathfrak{p}}(x) = \mathrm{v}_{\mathfrak{p}}((x - \pi_{\mathfrak{p}}) + \pi_{\mathfrak{p}}) = \mathrm{v}_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$$

et

$$\mathrm{v}_{\mathfrak{q}}(x) = \mathrm{v}_{\mathfrak{q}}((x - 1) + 1) = \mathrm{v}_{\mathfrak{q}}(1) = 0.$$

Posons $x_n = x^n$. Alors $\mathrm{v}_{\mathfrak{p}}(x^n) = n$ ce qui montre que x^n tend vers 0 pour la topologie définie par $\mathrm{v}_{\mathfrak{p}}$. Par contre, $\mathrm{v}_{\mathfrak{q}}(x^n) = 0$ ce qui signifie que $x^n \not\to 0$ pour la topologie de $\mathrm{v}_{\mathfrak{q}}$. Ces deux topologies sont différentes. □

Soit $\mathfrak{p}$ un idéal premier de A et soit $\mathrm{v}_{\mathfrak{p}}$ la valuation discrète associée à $\mathfrak{p}$. En complétant K pour la topologie induite par cette valuation discrète on obtient un corps complet qu'on notera $\mathrm{K}_{\mathfrak{p}}$ au lieu de $\mathrm{K}_{\mathrm{v}_{\mathfrak{p}}}$ pour simplifier la notation.

La proposition suivante résume ses propriétés principales.

Proposition 4.4.2. — *(i) Le corps $\mathrm{K}_{\mathfrak{p}}$ est muni d'une valuation discrète $\mathrm{v}_{\mathfrak{p}}$.*

(ii) L'anneau de valuation $\mathcal{O}_\mathfrak{p}$ de $\mathrm{K}_\mathfrak{p}$ coïncide avec l'adhérence de A dans $\mathrm{K}_\mathfrak{p}$.
(iii) Le corps résiduel de $\mathcal{O}_\mathfrak{p}$ est isomorphe à $k = A/\mathfrak{p}$.

Démonstration. — i) est démontrée dans la proposition 4.3.12.
ii) Soit $x \in \mathcal{O}_\mathfrak{p}$. Par la proposition 4.3.12 $A_\mathfrak{p}$ est dense dans $\mathcal{O}_\mathfrak{p}$ i.e. pour tout $n \geqslant 0$ il existe $y_n \in A_\mathfrak{p}$ tel que $\mathrm{v}_\mathfrak{p}(x - y_n) \geqslant n$. D'autre part, par le lemme d'approximation 2.4.9, il existe $x_n \in A$ tel que $\mathrm{v}_\mathfrak{p}(y_n - x_n) \geqslant n$. Donc,

$$\mathrm{v}_\mathfrak{p}(x_n - x) = \mathrm{v}_\mathfrak{p}((x_n - y_n) + (y_n - x)) \geqslant n$$

ce qui montre que $\{x_n\}$ converge vers x. Donc, A est dense dans $\mathcal{O}_\mathfrak{p}$.
iii) Par la proposition 4.3.12, le corps résiduel de $\mathcal{O}_\mathfrak{p}$ est isomorphe à $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$. et d'autre part, par le lemme d'approximation, $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ est isomorphe à $k_\mathfrak{p} = A/\mathfrak{p}$. □

4.4.2. Extensions. — Soit A un anneau de Dedekind ; $\mathrm{K} = \mathrm{Frac}(A)$. Soit L/K une extension finie séparable et soit B la fermeture intégrale de A dans L.

Pour tout idéal premier non-nul $\mathfrak{P}$ de B on note $\mathrm{v}_\mathfrak{P}$ la valuation discrète de L qui correspond à $\mathfrak{P}$ et $\mathrm{L}_\mathfrak{P}$ le complété de L pour $\mathrm{v}_\mathfrak{P}$.
Rappelons la définition suivante :

Définition 4.4.3. — On dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$ ou que $\mathfrak{P}$ divise $\mathfrak{p}$ si $\mathfrak{P} \cap A = \mathfrak{p}$. On note : $\mathfrak{P} \mid \mathfrak{p}$.

Si $\mathfrak{p}$ est un idéal premier de A, on a

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}},$$

où $e_\mathfrak{P}$ est l'indice de ramification de $\mathfrak{P}$.

Soit $x \in \mathrm{K}^*$. Alors

$$xA = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{v}_\mathfrak{p}(x)}.$$

Ainsi, il vient

$$xB = (xA)B = \prod_{\mathfrak{p}} \prod_{\mathfrak{P}|\mathfrak{p}} (\mathfrak{P}^{e_\mathfrak{P}})^{\mathrm{v}_\mathfrak{p}(x)}.$$

En comparant cette formule à

$$xB = \prod_{\mathfrak{P}} \mathfrak{P}^{\mathrm{v}_{\mathfrak{P}}(x)}$$

on obtient

$$\mathrm{v}_{\mathfrak{p}}(x) = \frac{1}{e_{\mathfrak{P}}} \mathrm{v}_{\mathfrak{P}}(x).$$

Soit $\rho_{\mathfrak{p}} \in]0;1[$ et pour $x \in \mathrm{K}$, soit

$$\|x\|_{\mathfrak{p}} = \rho_{\mathfrak{p}}^{\mathrm{v}_{\mathfrak{p}}(x)}$$

la valeur absolue sur K associée à $\mathrm{v}_{\mathfrak{p}}$. En posant $\rho_{\mathfrak{P}} = \rho_{\mathfrak{p}}^{1/e_{\mathfrak{P}}}$ et, pour $x \in \mathrm{L}$,

$$\|x\|_{\mathfrak{P}} = \rho_{\mathfrak{P}}^{\mathrm{v}_{\mathfrak{P}}(x)},$$

on obtient une valeur absolue sur L qui prolonge $\| \cdot \|_{\mathfrak{p}}$. On dit par abus que $\mathrm{v}_{\mathfrak{P}}$ prolonge $\mathrm{v}_{\mathfrak{p}}$ avec l'indice $e_{\mathfrak{P}}$.

Théorème 4.4.4. — *Soit A un anneau de Dedekind ;* $\mathrm{K} = \mathrm{Frac}(A)$. *Soit* L/K *une extension finie séparable et soit $\mathfrak{p}$ un idéal premier non-nul de A. Alors les valeurs absolues $\| \cdot \|_{\mathfrak{P}}$, $\mathfrak{P} \mid \mathfrak{p}$, sont précisement celles qui prolongent $\| \cdot \|_{\mathfrak{p}}$.*

Démonstration. — Par la proposition 4.4.1 les valeurs absolues $\| \cdot \|_{\mathfrak{P}}$ sont deux à deux non-équivalentes.

Soit $\| \cdot \|_w$ une valeur absolue qui prolonge $\| \cdot \|_{\mathfrak{p}}$. Comme $\| \cdot \|_{\mathfrak{p}}$ est non-archimédienne, $\| \cdot \|_w$ l'est aussi (proposition 4.3.2). Soit B_w l'anneau de valuation de w et soit $\mathfrak{m}$ son idéal maximal. L'anneau B_w est intégralement clos de corps des fractions L. Comme $A \subset B_w$, l'anneau B_w contient la fermeture intégrale de A dans L, i.e. $B \subseteq B_w$. Soit $\mathfrak{P} = B \cap \mathfrak{m}$: c'est un idéal premier non nul de B donc maximal (car B est de Dedekind). Alors $\mathfrak{P} \cap A = \mathfrak{p}$, i.e. $\mathfrak{P}$ est un idéal premier de B qui divise $\mathfrak{p}$. Ainsi B_w contient l'anneau de valuation discrète $B_{\mathfrak{P}}$. Il est facile de voir que tout anneau de valuation discrète est un sous-anneau de son corps des fractions. Donc $B_w = B_{\mathfrak{P}}$.

Soit $\pi_{\mathfrak{P}}$ une uniformisante de $B_{\mathfrak{P}}$. Si $x = u\pi_{\mathfrak{P}}^m \in B_w$, $u \in U(B_w)$, alors

$$\|x\| = \|\pi_{\mathfrak{P}}\|^m,$$

où $m = \mathrm{v}_{\mathfrak{P}}(x)$.

Comme $\pi_{\mathfrak{P}} \in B_w$, on a $\|\pi_{\mathfrak{P}}\| < 1$. En posant $\rho = \|\pi_{\mathfrak{P}}\|$ on obtient

$$\|x\| = \rho^{w_{\mathfrak{P}}(x)},$$

ce qui montre que $\| \cdot \| = \| \cdot \|_{\mathfrak{P}}$. □

CHAPITRE 5

LES NOMBRES p-ADIQUES

5.1. Le corps $\mathbb{Q}_p$

5.1.1. Normes sur $\mathbb{Q}$. — Ce paragraphe est consacré à l'étude des valeurs absolues sur le corps des rationnels $\mathbb{Q}$. On dispose déjà de la valeur absolue usuelle qu'on note ici $\| \cdot \|_\infty$:

$$\|x\|_\infty = |x|.$$

Cette norme est archimédienne.

Comme $\mathbb{Z}$ est un anneau de Dedekind, à tout nombre premier p on peut associer une valuation discrète v_p sur $\mathbb{Q}$. Rappelons sa définition. Soit $x \in \mathbb{Q}$ un rationnel non-nul. En utilisant le théorème de factorisation on peut écrire x sous la forme

$$x = p^n \frac{a}{b},$$

où $n \in \mathbb{Z}$ et où a et b sont des entiers premiers à p. On définit

$$\mathrm{v}_p \ : \ \mathbb{Q}^* \to \mathbb{Z}$$

en posant

$$\mathrm{v}_p(x) = n$$

et

$$\mathrm{v}_p(0) = \infty.$$

Proposition 5.1.1. — *La fonction* v_p *est une valuation discrète sur* $\mathbb{Q}$.

Démonstration. — Cela découle du chapitre précédent. On peut aussi en donner une preuve directe.

Soit $y = p^m c/d$, où c et d sont premiers à p. Alors,

$$xy = p^{n+m}\frac{ac}{bd}, \qquad p \nmid ac, bd,$$

d'où

$$\mathrm{v}_p(xy) = n + m = \mathrm{v}_p(x) + \mathrm{v}_p(y).$$

D'autre part, si $m \geqslant n$, alors

$$x + y = p^n \, \frac{ad + bcp^{m-n}}{bd},$$

d'où

$$\mathrm{v}_p(x+y) = \mathrm{v}_p(p^n) + \mathrm{v}_p(ad + bcp^{m-n}) - \mathrm{v}_p(bd) \geqslant n = \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\},$$

car $\mathrm{v}_p(ad + bcp^{m-n}) \geqslant 0$ et $\mathrm{v}_p(bd) = 0$. Donc, v_p est une valuation discrète. □

Par définition, l'anneau de valuation de v_p est

$$\mathbb{Z}_{(p)} = \{x = p^n a/b \,|\, n \geqslant 0,\, p \nmid ab\}.$$

Le nombre premier p est une uniformisante de $\mathbb{Z}_{(p)}$ et

$$\mathfrak{m}_p = \{x = p^n a/b \,|\, n \geqslant 1,\, p \nmid ab\} = p\mathbb{Z}_{(p)}$$

est l'idéal maximal de $\mathbb{Z}_{(p)}$.

Proposition 5.1.2. — *Le corps résiduel $\mathbb{Z}_{(p)}/\mathfrak{m}_p$ de v_p est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Démonstration. — La preuve est élémentaire, elle repose sur le lemme suivant :

Lemme 5.1.3. — *Soit $x \in \mathbb{Z}_{(p)}$. Alors pour tout $n \in \mathbb{N}$ il existe $x_n \in \mathbb{Z}$ tel que*

$$v_p(x - x_n) \geqslant n.$$

Démonstration. — Soit $x = a/b$, avec a et b premiers entre eux. Comme $v_p(x) \geqslant 0$, p ne divise pas b. Donc p^n et b sont premiers entre eux et il existe $c, d \in \mathbb{Z}$ tels que

$$cp^n + bd = 1.$$

Posons $x_n = ad$. Alors

$$x = a\left(d + \frac{c}{b}\, p^n\right) \,=\, x_n + \frac{ac}{b}\, p^n,$$

d'où

$$v_p(x - x_n) = v_p\left(\frac{ac}{b}\, p^n\right) \geqslant n.$$

Le lemme est démontré. □

Nous pouvons terminer la preuve de la proposition 5.1.2. Comme $p\mathbb{Z}_{(p)} \cap \mathbb{Z} = p\mathbb{Z}$, l'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)}$ induit une injection

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}.$$

Par le lemme 5.1.3, pour tout $x \in \mathbb{Z}_{(p)}$ il existe $x' \in \mathbb{Z}$ tel que $x' \equiv x \pmod{p}$, d'où

$$x' + p\mathbb{Z}_{(p)} = x + p\mathbb{Z}_{(p)}.$$

Le résultat s'en déduit. □

On peut normaliser la valeur absolue associée à v_p en prenant $\rho = 1/p$ et en posant

$$\|x\|_p = \left(\frac{1}{p}\right)^{\mathrm{v}_p(x)}.$$

Définition 5.1.4. — La valeur absolue non-archimédienne $\|\cdot\|_p$ est appelé la valeur absolue p-adique sur $\mathbb{Q}$.

Nous avons le théorème suivant :

***Théorème 5.1.5* (Ostrowski)**. — *Toute valeur absolue non triviale $\|\cdot\|$ sur $\mathbb{Q}$ est équivalente soit à la valeur absolue usuelle $|\cdot|$ soit à la valeur absolue p-adique $\|\cdot\|_p$, pour un certain nombre premier p.*

Remarque 5.1.6. — Si p et ℓ sont deux nombres premiers distincts, les valeurs absolues $\|\cdot\|_p$ et $\|\cdot\|_\ell$ ne sont pas équivalentes.

Démonstration. — • Supposons qu'il existe $k \in \mathbb{N}$ tel que $\|k\| > 1$. Notons que pour tout entier n, $\|n\| \leq n$. Posons $\alpha := \dfrac{\ln \|k\|}{\ln k} > 0$, ou encore $\|k\| = k^\alpha$. Soit $m \in \mathbb{N}$. Ecrivons le développement de m en base k :

$$m = \sum_{i=0}^{r} a_i k^i,$$

avec $a_i \in \{0, \cdots, k-1\}$ et r tel que $m \geq k^r$. Comme $\|a_i\| \leq a_i \leq k-1$ et $\|k^i\| = \|k\|^i$, il vient

$$\|m\| \leq (k-1)\sum_{i=0}^{r} \|k\|^i \leq \frac{\|k\|(k-1)}{\|k\|-1}\|k\|^r.$$

Ainsi $\|m\| \leq Ck^{\alpha r} \leq Cm^{\alpha}$, où $C = \dfrac{\|k\|(k-1)}{\|k\|-1}$. De cette inégalité, on a pour tout entier $n \geq 1$: $\|m\|^n \leq Cm^{\alpha n}$; en prenant ensuite la racine n-ème et en faisant tendre n vers l'infini, on obtient $\|m\| \leq m^{\alpha}$ et ainsi

$$\frac{\ln \|m\|}{\ln m} \leq \frac{\ln \|k\|}{\ln k}.$$

Si m est tel que $\|m\| > 1$, par symétrie, on obtient l'égalité $\dfrac{\ln \|m\|}{\ln m} = \dfrac{\ln \|k\|}{\ln k}$.
Sinon, il existe $s \geq 2$ tel que $\|k^s m\| > 1$. Alors

$$\frac{\ln \|k^s m\|}{\ln k^s m} = \frac{\ln \|k\|}{\ln k}$$

et alors en utilisant la multiplicativité de la norme, il vient également l'égalité $\dfrac{\ln \|m\|}{\ln m} = \dfrac{\ln \|k\|}{\ln k}$.
Pour conclure, en utilisant la multiplicativité de la norme, on obtient que $\|\cdot\| = |\cdot|^{\alpha}$.

• Supposons maintenant que pour tout $n \in \mathbb{N}$, $\|n\| \leq 1$. Si $\|\cdot\|$ est non triviale, il existe $n \in \mathbb{N}$ tel que $\|n\| < 1$. Soit n_0 le plus petit entier vérifiant cette inégalité stricte. Alors n_0 est un nombre premier p.
Prenons ensuite un nombre premier ℓ différent de p. Soit $n \gg 0$ et soit la relation de Bezout $1 = ap^n + b\ell^n$. Alors

$$1 = \|1\| \leq \|p\|^n + \|\ell\|^n.$$

Ainsi nécessairement $\|\ell\| = 1$! Et ainsi, $\|\cdot\|$ est équivalente à $\|\cdot\|_p$. □

Corollaire 5.1.7. — *Soit* K *un corps de nombres. Alors toute valeur absolue non triviale* $\|\cdot\|$ *sur* K *est équivalente soit à l'une des valeurs absolues* $|\cdot|_\sigma$*, où* $\sigma : \mathrm{K} \hookrightarrow \mathbb{C}$*, soit à la valeur absolue* $\mathfrak{P}$*-adique* $\|\cdot\|_{\mathfrak{P}}$*, pour un certain idéal premier non nul* $\mathfrak{P}$ *de* $\mathcal{O}_{\mathrm{K}}$*.*

Démonstration. — C'est une conséquence du théorème d'Ostrowski associé aux théorèmes 4.4.4 et 4.2.8. □

Définition 5.1.8. — Le complété de $\mathbb{Q}$ pour la valeur absolue p-adique est appelé corps des nombres p-adiques et est noté $\mathbb{Q}_p$.

Le corps $\mathbb{Q}_p$ est muni d'une norme $\|\cdot\|_p$ non-archimédienne qui prolonge celle de $\mathbb{Q}$. On munit également $\mathbb{Q}_p$ d'une valuation discrète v_p prolongeant celle de $\mathbb{Q}$ en posant $\mathrm{v}_p(x) = -\dfrac{1}{\log(p)}\log\|x\|_p$. (Ou encore, si $x_n \in \mathbb{Q}$, avec $x_n \to x$, $\mathrm{v}_p(x) := \mathrm{v}_p(x_n)$ pour n assez grand.) On note par $\mathbb{Z}_p$ son anneau de valuation :

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p,\ \|x\|_p \leq 1\}.$$

Proposition 5.1.9. — *L'anneau $\mathbb{Z}_p$ est l'adhèrence de $\mathbb{Z}$ dans $\mathbb{Q}_p$.*

Démonstration. — Clairement, l'adhérence de $\mathbb{Z}$ est contenu dans $\mathbb{Z}_p$. La réciproque se déduit aussi aisément : comme $\mathbb{Z}_{(p)}$ est dense dans $\mathbb{Z}_p$, le résultat est alors conséquence du fait que $\mathbb{Z}$ est dense dans $\mathbb{Z}_{(p)}$ (par le lemme 5.1.3). □

L'idéal maximal de $\mathbb{Z}_p$ est engendré par p et le corps résiduel $\mathbb{Z}_p/p\mathbb{Z}_p$ est isomorphe à $\mathbb{F}_p$. L'anneau $\mathbb{Z}_p$ est compact et le corps $\mathbb{Q}_p$ est localement compact.

Donnons maintenant quelques propriétés élémentaires des nombres p-adiques qui découlent directement de la définition :

(i) Une suite $\{x_n\}$ converge vers $x \in \mathbb{Q}_p$ si et seulement si $\mathrm{v}_p(x - x_n) \underset{n\to\infty}{\to} +\infty$.

(ii) Tout élément de $x \in \mathbb{Q}_p$ peut être représenté par une suite de Cauchy $\{x_n\} \subset \mathbb{Q}$ telle que $x = \lim_{n\to\infty} x_n$. Deux suite de Cauchy représentent le même élément si $\lim_{n\to\infty}(x_n - x'_n) = 0$ i.e. si $\mathrm{v}_p(x_n - x'_n) \to +\infty$.

(iii) Une série $\displaystyle\sum_{k=1}^{\infty} a_k$, $a_k \in \mathbb{Q}_p$, est convergente si et seulement si $\mathrm{v}_p(a_k) \to \infty$.

5.1.2. Ecriture des éléments de $\mathbb{Q}_p$. —

Lemme 5.1.10. — *Pour tout $x \in \mathbb{Z}_p$ il existe une unique suite de Cauchy $\{x_n\}$ d'éléments de $\mathbb{N}$ qui satisfait aux conditions suivantes :*

(i) $\{x_n\}$ *représente* x, *i.e.* $\lim_{n\to\infty} x_n = x$;
(ii) $0 \leqslant x_n < p^n$ *pour tout* $n \geqslant 1$;
(iii) $x_n \equiv x_{n+1} \pmod{p^n}$ *pour tout* $n \geqslant 1$.

Démonstration. — Démontrons d'abord l'unicité. Soient $\{x_n\}$ et $\{y_n\}$ deux suites de Cauchy vérifiant les conditions (i)-(iii). Si $\{x_n\} \neq \{y_n\}$, on note n_0 le plus petit naturel tel que $x_{n_0} \neq y_{n_0}$. Alors pour tout $n \geqslant n_0$ on a

$$x_n \equiv x_{n_0} \neq y_{n_0} \equiv y_n \pmod{p^{n_0}},$$

d'où $v_p(x_n - y_n) < n_0$. Donc, $\lim_{n\to\infty} x_n \neq \lim_{n\to\infty} y_n$ ce qui donne une contradiction.

Démontrons maintenant l'existence d'une suite vérifiant (i)-(iii).
Soit $x \in \mathbb{Z}_p$. Comme $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$, pour tout $n \in \mathbb{N}$, il existe $y_n \in \mathbb{Z}$ tel que $v_p(x - y_n) \geqslant n$. Soit x_n le reste de la division euclidienne de y_n par p^n :

$$y_n = p^n q_n + x_n, \qquad 0 \leqslant x_n < p^n.$$

Comme $\mathrm{v}_p(x_n - y_n) \geqslant n$, on a

$$\mathrm{v}_p(x_n - x) = \mathrm{v}_p((x_n - y_n) + (y_n - x)) \geqslant \min\{\mathrm{v}_p(x_n - y_n), \mathrm{v}_p(y_n - x)\} \geqslant n,$$

d'où $\lim_{n\to\infty} x_n = x$. Le même argument montre que $\mathrm{v}_p(x_n - x_{n+1}) \geqslant n$ i.e. que $x_n \equiv x_{n+1} \pmod{p^n}$. Le lemme est démontré. □

Soit $\{x_n\}$ la suite vérifiant les conditions du lemme 5.1.10. Tout x_n s'écrit de manière unique sous la forme :

$$x_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}, \qquad 0 \leqslant a_i \leqslant p - 1.$$

et la condition $x_n \equiv x_{n+1} \pmod{p^n}$ implique que

$$x_{n+1} = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n$$

avec les mêmes $a_0, a_1, \ldots, a_{n-1}$. Donc, tout $x \in \mathbb{Z}_p$ s'écrit de façon unique sous la forme

$$x = \sum_{k=0}^{\infty} a_k p^k, \qquad 0 \leqslant a_k \leqslant p - 1.$$

Soit maintenant $x \in \mathbb{Q}_p$. Si $\mathrm{v}_p(x) = -n < 0$, alors $\mathrm{v}_p(xp^n) = 0$, d'où $xp^n \in \mathbb{Z}_p$. Donc xp^n s'écrit

$$xp^n = \sum_{k=0}^{\infty} b_k p^k, \qquad 0 \leqslant b_k \leqslant p-1$$

et en posant $a_k = b_{k+n}$ on obtient :

$$x = \sum_{k=-n}^{\infty} a_k p^k, \qquad 0 \leqslant a_k \leqslant p-1.$$

Exemple 5.1.11. — Soit un nombre premier p. Alors

$$\sum_{k=0}^{n} (p-1)p^k = -1 + p^{n+1},$$

et ainsi

$$-1 = (p-1) + (p-1)p + \cdots + (p-1)p^n + \cdots$$

Exemple 5.1.12. — Dans $\mathbb{Q}_p$:

$$\frac{1}{1-p} = 1 + p + p^2 + \cdots + p^n + \cdots$$

Exemple 5.1.13. — Dans $\mathbb{Q}_7$, on a

$$-3 \equiv -3 + 7^5 \equiv 16804 \pmod{7^5}.$$

Ainsi

$$-3 = 4 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + 6 \cdot 7^4 + \cdots .$$

5.1.3. Racine carrée. — Donnons une application du lemme de Hensel pour le corps $\mathbb{Q}_p$.
Rappelons tout d'abord ce lemme dans notre cadre.

***Lemme 5.1.14* (de Hensel)**. — *Soit $P \in \mathbb{Z}_p[X]$.*
Supposons avoir $x_0 \in \mathbb{Z}_p$ tel quel

$$\lambda = \mathrm{v}_p(P(x_0)) - 2\mathrm{v}_p(P'(x_0)) > 0,$$

alors il existe $\alpha \in \mathbb{Z}_p$ tel que $P(\alpha) = 0$ avec de plus $\alpha \equiv x_0 \pmod{p}$.

Remarque 5.1.15. — Si l'on considère le suite $(\alpha_n)_n$ du lemme de Hensel 4.3.6, on a $\mathrm{v}_p(x - \alpha_i) \geq 2^i$. Ainsi, le développement de α_i à l'ordre 2^i donne le développement de x à l'ordre 2^i.

Soit p un nombre premier et soit $a \in \mathbb{Z}_p$, $a \neq 0$. On cherche à résoudre dans $\mathbb{Q}_p$ l'équation

$$X^2 = a. \tag{6}$$

Si x est une solution alors nécessairement $\mathrm{v}_p(x) \geq 0$. De plus si a est un carré, alors nécessairement $\mathrm{v}_p(a)$ est paire et de ce fait, quitte à diviser par une puissance de p adéquate, on se ramène donc au cas où $a \in \mathbb{Z}_p^\times$.

Supposons $p \neq 2$. Si l'équation (6) a une solution dans $\mathbb{Z}_p$, on a alors que a est un carré modulo p.
Réciproquement, supposons que $a \in \mathbb{F}_p^2$. Il existe $x_0 \in \mathbb{Z}$, tel que $a = x_0^2 (\mathrm{mod}\ p)$. Posons $P(X) = X^2 - a$. Alors $\mathrm{v}_p(P(x_0)) \geq 1$ et

$$\mathrm{v}_p(P'(x_0)) = \mathrm{v}_p(2x_0) = 0.$$

Le lemme d'Hensel s'applique et a est bien un carré dans $\mathbb{Z}_p$.

Supposons maintenant que $p = 2$. Si $a \in \mathbb{Z}_2^2$, alors

$$a \equiv (1 + 2a_1 + 4a_2)^2 \ (\mathrm{mod}\ 8) \equiv 1 (\mathrm{mod}\ 8).$$

Montrons que cette condition nécessaire est suffisante.
Soit donc $a \in \mathbb{Z}_p$, avec $a \equiv 1 (\mathrm{mod}\ 8)$. Soit $P = X^2 - a$. Alors $\mathrm{v}_2(P(1)) \geq 3$ et $\mathrm{v}_2(P'(1)) = \mathrm{v}_2(2) = 1$. Le lemme de Hensel s'applique : il existe $\alpha \in \mathbb{Z}_2$ tel que $\alpha^2 = a$, avec de plus $\alpha \equiv 1 (\mathrm{mod}\ 8)$.

Exemple 5.1.16. — Prenons $p = 5$ et cherchons une racine carrée de -1 dans $\mathbb{Z}_5$. On sait qu'une telle racine existe. Comme $2^2 \equiv -1 \ (\mathrm{mod}\ 5)$, choisissons la racine carrée α vérifiant

$$\alpha = 2 + a_1 5 + \cdots$$

Regardons α^2 pour obtenir

$$4 + 20a_1 \equiv -1 \ (\mathrm{mod}\ 5^2),$$

et ainsi $a_1 = 1$. On regarde ensuite

$$(2 + 5 + a_2 5^2)^2 \equiv -1 (\mathrm{mod}\ 5^3)$$

pour trouver $a_2 = 2$.
Ainsi on obtient le début du développement d'une racine carrée de -1 :

$$\alpha = 2 + 5 + 2 \cdot 5^2 + a_3 5^3 + \cdots$$

Retrouvons ce développement à l'aide de la suite (α_i) du lemme de Hensel. Soit $\alpha_0 = 2$ puis $\alpha_{i+1} = \alpha_i - \dfrac{\alpha_i^2 + 1}{2\alpha_i}$. Alors $\alpha_1 = 3/4$, $\alpha_2 = -7/24$, $\alpha_3 = 527/336$. On a vu que α_3 permet de donner le développement à l'ordre 2^3 de la racine recherchée. On a la relation de Bézout $54641 \times 336 - 47 \times 5^8 = 1$. Ainsi,

$$\alpha_3 = 54641 \times 527 + 5^8(\cdots) = 2 + 5 + 2\cdot 5^2 + 5^3 + 3\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 3\cdot 5^7 + \cdots$$

5.1.4. Remarque : une définition alternative de $\mathbb{Q}_p$. — Remarquons qu'il est possible de définir $\mathbb{Q}_p$ plus directement, c'est à dire sans utiliser le formalisme de la section 4.1.

• On commence par définir $\mathbb{Q}_p$ comme l'ensemble des séries formelles de Laurent

$$x = \sum_{i \geq k} a_i p^i,$$

pour un certain entier $k := k_x \in \mathbb{Z}$, où $a_i \in \{0, \cdots, p-1\}$.
De façon évidente, on munit $\mathbb{Q}_p$ de deux lois $+$ et $\times$ qui en font un corps. Posons ensuite $\mathbb{Z}_p = \{x \in \mathbb{Q}_p, \mathrm{v}_p(x) \geq 0\}$: c'est clairement un anneau.
On munit également $\mathbb{Q}_p$ d'une valuation p-adique v_p définie par

$$\mathrm{v}_p(x) = \min_i \{a_i \neq 0\},$$

puis on pose $\|x\|_p = p^{-k}$: c'est une valeur absolue sur $\mathbb{Q}_p$. On vérifie alors assez facilement la proposition suivante

Proposition 5.1.17. — *Le corps $\mathbb{Q}_p$ muni de $\|\cdot\|_p$ est complet et $\mathbb{Z}_p$ est compact.*

• Le lemme 5.1.3 permet de plonger $\mathbb{Q}$ dans $\mathbb{Q}_p$. On remarque alors que $\|\cdot\|_p$ prolonge bien la norme p-adique sur $\mathbb{Q}$ puis que le plongement de $\mathbb{Q}$ dans $\mathbb{Q}_p$ est continu.
Enfin, on voit assez facilement que $\mathbb{Q}$ (resp. $\mathbb{Z}$) est dense dans $\mathbb{Q}_p$ (resp. dans $\mathbb{Z}_p$).

5.2. La structure de $\mathbb{Q}_p^\times$

5.2.1. Le groupe des unités principales. — Soit $p \neq 2$. Notons alors par $\mathcal{U}_0 = 1 + p\mathbb{Z}_p$. L'ensemble $\mathcal{U}_0$ est un sous-groupe de $\mathbb{Z}_p^\times$. En effet,

soit $x \in \mathcal{U}_0$, alors il existe $y \in \mathbb{Z}_p^\times$ tel que $xy = 1$. Alors $xy \equiv 1 (\mathrm{mod}\ p)$ ce qui implique que $y \equiv 1 (\mathrm{mod}\ p)$ i.e. $y \in \mathcal{U}_0$.

Proposition 5.2.1. — *Pour $p \neq 2$, le groupe $\mathcal{U}_0 = 1 + p\mathbb{Z}_p$ est sans $\mathbb{Z}$-torsion.*
Pour $p = 2$, le groupe $\mathcal{U}_0 = 1 + 4\mathbb{Z}_2$ est sans $\mathbb{Z}$-torsion.

Démonstration. — Nous nous contenterons de montrer le lemme pour $p \neq 2$.
Soit $x \in \mathcal{U}_0$ avec $x \neq 1$. Alors $x = 1 + p^r x_0 \in \mathcal{U}_0$, avec $r \geq 1$ et $x_0 \in \mathbb{Z}_p^\times$.
Soit $n = p^s m$, avec $s \geq 1$ et $(m, p) = 1$.
Alors,

$$x^m = 1 + mp^r x_0 + \cdots + p^{mr} x_0^,$$

et ainsi

$$\mathrm{v}_p(x^m - 1) = r,$$

puis

$$x^p = 1 + pp^r x_0 + \cdots + p^{pr} x_0^p.$$

Puisque $\mathrm{v}_p(p^{pr}) = pr > r + 1$ car $p > 2$ (c'est à ce niveau que pour $p = 2$, il faut considérer les unités $x \equiv 1 (\mathrm{mod}\ 4)$), il vient

$$\mathrm{v}_p(x^p - 1) = r + 1.$$

Au final, on obtient donc

$$\mathrm{v}_p(x^n - 1) = s + r$$

et par conséquent, $x^n \neq 1$. □

Remarque 5.2.2. — On notera que $-1 \in 1 + 2\mathbb{Z}_2$ et ainsi $1 + 2\mathbb{Z}_2$ est de torsion.

5.2.2. Racine $(p-1)$-ème de l'unité. — Notons par μ_{p-1} le groupe des racines $(p-1)$-ème de l'unité de $\overline{\mathbb{Q}_p}$.

On cherche à résoudre l'équation $X^{p-1} = 1$ dans $\mathbb{Z}_p$, c'est-à-dire à déterminer $\mu_{p-1} \cap \mathbb{Z}_p$.
Dans $\mathbb{F}_p^\times$, tout élément a vérifie $a^{p-1} = 1$. Ainsi $P(X) = X^{p-1} - 1$ admet $p - 1$ racines distinctes dans $\mathbb{F}_p$. D'autre part $P'(a) \neq 0$. Ainsi d'après le lemme de Hensel, l'équation $X^{p-1} = 1$ admet $p - 1$ solutions distinctes dans $\mathbb{Z}_p$, ou encore $\mathbb{Z}_p$ contient μ_{p-1}.

Soit $x \in \mathbb{Z}_p^\times$. Alors $x = a_0 + a_1 p + \cdots$. D'autre part, on sait qu'il existe une racine $(p-1)$-ème de l'unié ζ vérifiant

$$\zeta \equiv a_0 (\text{mod } p).$$

Ainsi $x\zeta^{-1} \in \mathcal{U}_0$ et par conséquent $\mathbb{Z}_p^\times = \langle \mu_{p-1}, \mathcal{U}_0 \rangle$.

Terminons en notant que $\mu_{p-1} \cap \mathcal{U}_0 = \{1\}$.
Ainsi

$$\mathbb{Z}_p^\times = \mu_{p-1} \times \mathcal{U}_0.$$

Considérons maintenant le cas où $p = 2$. Posons $\mathcal{U}_0 = 1 + 4\mathbb{Z}_2$. Alors

$$\mathbb{Z}_2^\times = \langle \pm 1 \rangle \times \mathcal{U}_0.$$

5.2.3. Quelques fonctions p-adiques. —

5.2.3.1. Fonction puissance. — Soit $x = a_0 + a_1 p + \cdots + a_n p^n + \cdots \in \mathbb{Z}_p$, où $a_i \in \{0, \cdots, p-1\}$. Posons $x_n = a_0 + a_1 p + \cdots + a_n p^n$.
Soit $u \in \mathcal{U}_0$.

Lemme 5.2.3. — *Soit $m > n$. On a*

$$\mathrm{v}_p(u^{x_m - x_n} - 1) \geq n + 1.$$

Démonstration. — On note que $\mathrm{v}_p(x_m - x_n)) \geq n + 1$ et on utilise alors un calcul similaire à celui de la preuve de la proposition 5.2.1. □

Ainsi

$$\|u^{x_m} - u^{x_n}\|_p = \|u^{x_n}\| \|1 - u^{x_m - x_n}\|_p \leq \|1 - u^{x_m - x_n}\|_p.$$

Par conséquent la suite $\{u^{x_n}\}_n$ est de Cauchy et converge donc dans $\mathbb{Z}_p$. On note u^x la limite et ainsi $\mathcal{U}_0$ devient un $\mathbb{Z}_p$-module sans torsion. A noter que la fonction $x \mapsto u^x$ est continue.

5.2.3.2. Logarithme p-adique. — Posons $q = p$ si $p > 2$ et $q = 4$ si $p = 2$.
On pose $q = p^\delta$.
Notons $\mu_{q-1} = \mu_{p-1}$ si $q = p$, sinon $\mu_{q-1} = \langle \pm 1 \rangle$ pour $p = 2$.

Soit $x_0 \in \mathbb{Z}_p$.
Commençons par un lemme

Lemme 5.2.4. — *La suite* $\left(\mathrm{v}_p(\frac{(qx_0)^n}{n}) \right)_n$ *tend vers l'infini avec n.*

Démonstration. — En effet, il suffit de noter que $\mathrm{v}_p(n) \leq \log(n)/\log(p)$ puis de remarquer que la fonction $\delta n - \log(n)/\log(p)$ est une suite strictement croissante. □

Définition 5.2.5. — Pour $x = 1 + qx_0 \in \mathcal{U}_0$, la série

$$\log_p(x) = \sum_{i \geq 1} (-1)^{i+1} \frac{(qx_0)^i}{i},$$

converge : c'est le logarithme p-adique de x.

Démonstration. — C'est une conséquence du lemme 5.2.4. □

Remarque 5.2.6. — On a $\log_p(1) = 0$.

Remarque 5.2.7. — La fonction $x \mapsto \log_p(x)$ est une fonction continue sur $\mathcal{U}_0$.

Proposition 5.2.8. — *Pour $x, y \in \mathcal{U}_0$, il vient*

$$\log_p(xy) = \log_p(x) + \log_p(y).$$

Démonstration. — C'est un calcul formel. En effet, soit la série formelle

$$\log(1+T) = \sum_{i \geq 1} (-1)^{i+1} \frac{T^i}{i}.$$

Alors formellement, il vient : $\log(1+X)(1+Y) = \log(1+X) + \log(1+Y)$. Il suffit ensuite de poser $X = x - 1$ et $Y = y - 1$. □

Ainsi, pour tout $n \in \mathbb{Z}$, et pour tout $x \in \mathcal{U}_0$, on a $\log_p(x^n) = n\log_p(x)$. Mieux. Par continuité de la fonction puissance et du logarithme p-adique, on a alors pour tout $a \in \mathbb{Z}_p$ et $x \in \mathcal{U}_0$,

$$\log_p(x^a) = a\log_p(x).$$

On étend le logarithme p-adique à tout $\mathbb{Q}_p^\times$ de la façon suivante.
Soit $x \in \mathbb{Q}_p^\times$. Alors

$$x = p^{\mathrm{v}_p(x)} \zeta y,$$

avec $\zeta \in \mu_{q-1}$ et $y \in \mathcal{U}_0$. Cette écriture est de plus unique.
On pose alors

$$\log_p(x) = \log_p(y).$$

On notera en particulier que $\log_p(p) = 0$.

5.2.3.3. Exponentielle. — On s'intéresse maintenant à la série

$$\sum_{i\geq 0} \frac{x^i}{i!}.$$

Un simple calcul permet de montrer que cette série converge sur $q\mathbb{Z}_p$.

Définition 5.2.9. — Pour $x \in q\mathbb{Z}_p$, on note

$$\exp_p(x) = \sum_{i\geq 0} \frac{x^i}{i!}$$

l'exponentielle p-adique de x. C'est une fonction continue sur $q\mathbb{Z}_p$.

Proposition 5.2.10. —

(*i*) *Soit* $x \in q\mathbb{Z}_p$. *Alors* $\mathrm{v}_p(\exp_p(x) - 1) = \mathrm{v}_p(x)$.
(*ii*) *Soit* $x \in q\mathbb{Z}_p$ *et* $a \in \mathbb{Z}_p$. *Alors* $\exp_p(ax) = \big(\exp_p(x)\big)^a$.
(*iii*) *Pour tout* $x \in q\mathbb{Z}_p$ *et tout* $y \in \mathcal{U}_0$, *il vient*

$$\log_p(\exp_p(x)) = x$$

et

$$\exp_p(\log_p(y)) = y.$$

Démonstration. — Les points (*i*) et (*ii*) sont immédiats. Le point (*iii*) résulte d'un calcul formel. □

5.2.4. Le résultat principal. — Nous venons de voir que $\log_p$ induit un isomorphisme de groupes topologiques entre $(\mathcal{U}_0, \times)$ et $(q\mathbb{Z}_p, +)$ (*i.e* de $\mathbb{Z}_p$-modules), d'inverse $\exp_p$.
Or $q\mathbb{Z}_p$ est engendré topologiquement par q. Ainsi, $\mathcal{U}_0$ est topologiquement engendré par $\exp_p(q)$.

Lemme 5.2.11. — *Le groupe* $\mathcal{U}_0$ *est topologiquement engendré par* $1+q$.

Démonstration. — On a $\log_p(1+q) = q\varepsilon$, avec $\varepsilon \in \mathbb{Z}_p^\times$. Comme $1 + q = \exp_p(q\varepsilon) = \big(\exp_p(q)\big)^\varepsilon$ et que $\varepsilon \in \mathbb{Z}_p^\times$, le résultat est imméditat. □

On obtient la proposition suivante

Proposition 5.2.12. — *Pour $p > 2$, il vient*

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mu_{q-1} \times \langle 1+q \rangle_{\mathbb{Z}_p}$$

et ainsi

$$\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

Pour $p = 2$: $\mathbb{Q}_2^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \langle 1 + 4\mathbb{Z}_2 \rangle$.

Pour $p > 2$, il vient

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Plus précisémment,

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = \{1, a, p, pa\},$$

où $a \in \mathbb{Z}$ n'est pas un carré modulo p.
Ainsi, le corps $\mathbb{Q}_p$ a exactement trois extensions quadratiques : $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{ap})$.

Pour $p = 2$, il vient

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \langle -1, 2, 5 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Le corps $\mathbb{Q}_2$ a exactement 7 extensions quadratiques.

5.3. Une version polynômiale du lemme de Hensel

Théorème 5.3.1. — *Soit $f \in \mathbb{Z}_p[X]$, $f \neq 0 (\mathrm{mod}\ p)$, admettant la factorisation*

$$f = \overline{g} \cdot \overline{h} \in \mathbb{F}_p[X],$$

avec $(\overline{g}, \overline{h}) = 1$. Alors il existe $g, h \in \mathbb{Z}_p[X]$ tels que

(i) $f = gh$;
(ii) $g = \overline{g} \in \mathbb{F}_p[X]$; $h = \overline{h} \in \mathbb{F}_p[X]$
(iii) $\deg(\overline{g}) = \deg(g)$.

Démonstration. — Posons $d = \deg(f)$ et $m = \deg(\overline{g})$. Ainsi, $\deg(\overline{h}) \leq d - m$.
Soient $g_0, h_0 \in \mathbb{Z}_p[X]$ tels que

(i) $g_0 = \overline{g} \in \mathbb{F}_p[X]$;
(ii) $h_0 = \overline{h} \in \mathbb{F}_p[X]$;
(iii) $\deg(g_0) = m$, $\deg(h_0) \leq d - m$.

Comme $(\overline{h}, \overline{g}) = 1$, il existe $a, b \in \mathbb{Z}_p[X]$ tels que

$$ag_0 + bh_0 \equiv 1 (\text{mod } p\mathbb{Z}_p[X]).$$

Les coefficients des polynômes $f - h_0 g_0$ et $ag_0 + bh_0 - 1$ sont dans $p\mathbb{Z}_p$. Notons par j la valuation minimale de ceux-ci. Posons $\pi = p^j$.

Nous allons montrer qu'il existe deux suites de polynômes $(r_i)_i$ et $(s_i)_i$ vérifiant :

(i) $\deg(r_i) < m$; $\deg(s_i) \leq d - m$;
(ii) $g_n = g_0 + \pi r_1 + \cdots + \pi^n r_n \ (\text{mod } \pi^{n+1})$;
(iii) $h_n = h_0 + \pi s_1 + \cdots + \pi^n s_n \ (\text{mod } \pi^{n+1})$;
(iv) $f \equiv g_n \cdot h_n \ (\text{mod } \pi^{n+1})$.

Pour $n = 0$: c'est établi.
Supposons la propriété établie pour n. On veut donc trouver deux polynômes r_{n+1} et s_{n+1} tels que $g_{n+1} = g_n + \pi^{n+1} r_{n+1}$, $h_{n+1} = h_n + \pi^{n+1} s_{n+1}$ vérifient

$$f \equiv g_{n+1} \cdot h_{n+1} \ (\text{mod } \pi^{n+2}).$$

Une telle identité équivaut à

$$\frac{1}{\pi^{n+1}} (f - g_n h_n) \equiv g_n s_{n+1} + h_n r_{n+1} \equiv g_0 s_{n+1} + h_0 r_{n+1} \ (\text{mod } \pi).$$

Posons alors $f_{n+1} = \dfrac{1}{\pi^{n+1}} (f - g_n h_n)$. Par hypothèse, $f_{n+1} \in \mathbb{Z}_p[X]$ et $f = g_n f_n + \pi^{n+1} f_{n+1}$.

Partons alors de la congruence

$$f_{n+1} \equiv f_{n+1} a g_0 + f_{n+1} b h_0 \ (\text{mod } \pi).$$

Puis effectuons la division euclidienne de bf_{n+1} par g_0 et posons r_{n+1} le reste de celle-ci :

$$bf_{n+1} = qg_0 + r_{n+1},$$

avec $\deg(r_{n+1}) < \deg(g_0) = m$. Comme $\deg(g_0) = \deg(\overline{g})$, le coefficient dominant de g_0 est dans $\mathbb{Z}_p^\times$. La division euclidienne a bien lieu dans $\mathbb{Z}_p$. Ainsi, q et r_{n+1} sont dans $\mathbb{Z}_p[X]$.
Il vient ainsi

$$f_{n+1} \equiv f_{n+1} a g_0 + h_0 (q g_0 + r_{n+1}) \ (\text{mod } \pi).$$

Il suffit alors de poser $s_{n+1} = a f_{n+1} + q h_0$.

Le degré des polynômes r_{n+1} et s_{n+1} satisfont bien les conditions requises.

Les suites des polynômes (g_n) et (h_n) étant de degré borné, il existe alors deux polynômes $g, h \in \mathbb{Z}_p[X]$ et des suites extraites $g_{\varphi(n)}$ et $h_{\varphi(n)}$ tels que $g_{\varphi(n)} \to g$ et $h_{\varphi(n)} \to h$. A la limite, on obtient $f = gh$. □

Corollaire 5.3.2. — *Soit $f \in \mathbb{Z}_p[X] = a_0 + \cdots + a_n X^n$, $a_n \neq 0$, un polynôme irréductible sur $\mathbb{Q}_p$. Alors*

$$\max_i\{\|a_i\|_p\} = \max\{\|a_0\|_p, \|a_n\|_p\}.$$

Démonstration. — On peut supposer que $f \neq 0 \pmod p$. Soit a_r le premier élément de la suite $a_0, \cdots, a_n$ tel que $\|a_r\|_p = 1$.
Alors

$$f = x^r(a_r + \cdots + a_n x^{n-r}) \pmod p.$$

Si $r \neq 0$ et $r \neq n$, d'après la théorème 5.3.1, le polynôme f est réductible. Ainsi, soit $r = 0$ et alors $\max_i\{\|a_i\|_p\} = \|a_0\|_p$; soit $r = n$ et $\max_i\{\|a_i\|_p\} = \|a_n\|_p$. □

On en déduit immédiatement le corollaire suivant :

Corollaire 5.3.3. — *Soit $x \in \overline{\mathbb{Q}_p}$ et soit*

$$P = \mathrm{Irr}(x, \mathbb{Q}_p) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}_p[X]$$

le polynôme irréductible de x sur $\mathbb{Q}_p$. Alors $P \in \mathbb{Z}_p[X]$ si et seulement si $a_0 \in \mathbb{Z}_p$.

CHAPITRE 6

CORPS LOCAUX

6.1. Définition

Avant de rappeler quelques faits, donnons la définition centrale de ce chapitre.

Définition 6.1.1. — Un corps local est un corps complet pour une valuation discrète de corps résiduel fini.

6.1.1. Rappels. — Dans ce paragraphe K désigne un corps complet pour une valuation discrète

$$v_{\mathrm{K}} \ : \ \mathrm{K}^* \to \mathbb{Z}.$$

On note $\mathcal{O}_{\mathrm{K}}$ et on appelle anneau des entiers de K son anneau de valuation

$$\mathcal{O}_{\mathrm{K}} = \{x \,|\, v_{\mathrm{K}}(x) \geqslant 0\}.$$

On appelle groupe des unités de K et on note U_{K} le groupe des unités de $\mathcal{O}_{\mathrm{K}}$:

$$U_{\mathrm{K}} = \{x \,|\, v_{\mathrm{K}}(x) = 0\}.$$

On note π_{K} une uniformisante de $\mathcal{O}_{\mathrm{K}}$ et $\mathfrak{m}_{\mathrm{K}}$ son idéal maximal. On a ainsi

$$\mathfrak{m}_{\mathrm{K}} = \{x \in \mathrm{K},\ v_{\mathrm{K}}(x) > 0\},$$
$$\mathfrak{m}_{\mathrm{K}} = (\pi_{\mathrm{K}}).$$

Choisissons $\rho \in]0;1[$ et fixons une valeur absolue sur K en posant

$$\|x\|_{\mathrm{K}} = \rho^{v_{\mathrm{K}}(x)}.$$

Théorème 6.1.2. — *Soit* L/K *une extension finie séparable d'un corps complet* K *pour une valuation discrète. Alors,*

(i) La fermeture intégrale de $\mathcal{O}_\mathrm{K}$ *dans* L *est un anneau de valuation discrète qu'on note* B.

(ii) La valeur absolue $\|\cdot\|_\mathrm{K}$ *admet un unique prolongement* $\|\cdot\|_\mathrm{L}$ *à* L. *Ce prolongement est induit par la valuation discrète de* B.

(iii) Le corps L *est complet pour la topologie définie par* $\|\cdot\|_\mathrm{L}$. *Son anneau des entiers* $\mathcal{O}_\mathrm{L}$ *coïncide avec* B.

Démonstration. — Comme $\mathcal{O}_\mathrm{K}$ est principal (théorème 4.3.11), c'est un anneau de Dedekind, on peut appliquer le théorème 4.4.4. On obtient ainsi que les prolongements de $\|\cdot\|_\mathrm{K}$ à L sont induits par les valuations discrètes associées aux idéaux premiers non-nul de B. Comme par le théorème 4.2.2 il n'existe qu'un seul prolongement de $\|\cdot\|_\mathrm{K}$ à L on obtient que B possède un unique idéal premier $\mathfrak{m}_\mathrm{L}$. Comme B est un anneau de Dedekind, ceci implique que $\mathfrak{m}_\mathrm{L}$ est principal (voir le corollaire 2.4.8) ce qui montre que B est un anneau de valuation discrète. Les autres assertions sont évidentes. □

Corollaire 6.1.3. — *Une extension finie d'un corps local est encore un corps local.*

Nous allons utiliser les notations et les définitions suivantes. Soit π_L une uniformisante de L.
Les idéaux $\mathfrak{m}_\mathrm{K} = (\pi_\mathrm{K})$ et $\mathfrak{m}_\mathrm{L} = (\pi_\mathrm{L})$ sont les uniques idéaux premiers non-nuls des anneaux $\mathcal{O}_\mathrm{K}$ et $\mathcal{O}_\mathrm{L}$ et on note $k_\mathrm{K} = \mathcal{O}_\mathrm{K}/\mathfrak{m}_\mathrm{K}$ et $k_\mathrm{L} = \mathcal{O}_\mathrm{L}/\mathfrak{m}_\mathrm{L}$ les corps résiduels correspondants. En particulier k_L est une extension finie de k_K. Le degré $f = [k_\mathrm{L} : k_\mathrm{K}]$ est appelé le degré résiduel de L/K.

On note $e = e(\mathrm{L}/\mathrm{K})$ l'indice de ramification de l'idéal (π_L) :

$$\pi_\mathrm{K}\mathcal{O}_\mathrm{L} = \pi_\mathrm{L}^e\mathcal{O}_\mathrm{L}.$$

Cet entier e sera appelé l'indice de ramification de l'extension L/K.

L'uniformisante π_K s'écrit sous la forme :

$$\pi_\mathrm{K} = \pi_L^e u, \qquad u \in U_\mathrm{L}.$$

Si on note v_{L} la valuation discrète de L on obtient

$$e = v_{\mathrm{L}}(\pi_{\mathrm{K}}).$$

Plus généralement, si $x \in \mathrm{K}$, alors

$$v_{\mathrm{L}}(x) = e v_{\mathrm{K}}(x).$$

Corollaire 6.1.4. — *On a*

$$ef = [\mathrm{L} : \mathrm{K}].$$

Démonstration. — C'est un cas particulier du théorème 4.2.8. □

Proposition 6.1.5. — *Soient* $\mathrm{K} \subseteq \mathrm{L} \subseteq \mathrm{M}$ *une tour d'extensions finies. Alors*

$$e(M/L)\, e(L/\mathrm{K}) = e(M/\mathrm{K}),$$
$$f(M/L)\, f(M/\mathrm{K}) = f(M/\mathrm{K}).$$

Démonstration. — Ces formules découlent directement des définitions. □

Les propriétés suivantes ont déja été vues.

Proposition 6.1.6. — *(i) Soit* L/K *une extension galoisienne. Alors pour tout* $x \in \mathrm{L}$ *et* $g \in \mathrm{Gal}(L/\mathrm{K})$*, les éléments* x *et* $g(x)$ *ont même valuation. En particulier*

$$g(\mathcal{O}_L) = \mathcal{O}_L.$$

(ii) Soit L/K *une extension galoisienne. Alors l'action de* $G = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ *sur* L *est continue.*

(iii) Les applications $\mathrm{N}_{L/\mathrm{K}}$ *et* $\mathrm{Tr}_{L/\mathrm{K}}$ *sont continues.*

On rappelle que le prolongement de $\| \cdot \|_{\mathrm{K}}$ à L est donné par la formule explicite suivante :

$$\|x\|_{\mathrm{L}} = \|\mathrm{N}_{\mathrm{L}/\mathrm{K}}(x)\|_{\mathrm{K}}^{1/n},$$

où $n = [\mathrm{L} : \mathrm{K}]$.

Nous pouvons donner aussi une formule explicite pour v_{L} :

Proposition 6.1.7. — *Soit* L/K *une extension finie de degré* n*. Alors*

$$v_{\mathrm{L}}(x) = \frac{1}{f} v_{\mathrm{K}}(\mathrm{N}_{\mathrm{L}/\mathrm{K}}(x))\,.$$

Démonstration. — On a pour $x \in \mathrm{L}$

$$\|x\|_{\mathrm{K}} = \rho_{\mathrm{K}}^{v_{\mathrm{K}}(x)}$$

et

$$\|x\|_{\mathrm{L}} = \rho_{\mathrm{L}}^{v_{\mathrm{L}}(x)}.$$

Comme $0 < \rho_{\mathrm{K}}, \rho_{\mathrm{L}} < 1$, il existe $c > 0$ tel que $\rho_{\mathrm{K}} = \rho_{\mathrm{L}}^{c}$. Alors on obtient

$$v_{\mathrm{L}}(x) = \frac{c}{n}\, v_{\mathrm{K}}(N_{\mathrm{L/K}}(x)).$$

Pour déterminer la constante c posons $x = \pi_{\mathrm{K}}$.
Alors $e = v_{\mathrm{L}}(\pi_{\mathrm{K}}) = \dfrac{c}{n}\, v_{\mathrm{K}}(\pi_{\mathrm{K}}^{n}) = c$. Comme $e/n = f$, la formule s'en déduit. □

6.2. Exemples

6.2.1. Le corps des nombres p-adiques. — Le corps des nombres p-adiques $\mathbb{Q}_p$ est un corps local à corps résiduel $\mathbb{F}_p$.

Soit $\mathrm{L}/\mathbb{Q}_p$ une extension de degré fini n. On a vu l'existence d'une unique norme $\|\cdot\|_{\mathrm{L}}$ sur L prolongeant $\|\cdot\|_p$. Cette norme est associée à une valuation discrète, prolongeant donc la valuation p-adique v_p de $\mathbb{Q}_p$. Son anneau de valuation $\mathcal{O} = \{x \in \mathrm{K},\ \|x\|_{\mathrm{L}} \leq 1\}$ est compact : le corps L est localement compact. Le corps résiduel est un corps fini de degré f sur $\mathbb{F}_p$. Si π désigne une uniformisante de $\mathcal{O}$, alors $p\mathcal{O} = \pi^e$, où e est l'indice de ramification de $\mathrm{L}/\mathbb{Q}_p$ et donc $ef = n$. Enfin, l'anneau $\mathcal{O}$ est la fermeture intégrale de $\mathbb{Z}_p$ dans L et ainsi $\mathcal{O} \simeq \mathbb{Z}_p^n$.

Proposition 6.2.1. — *Soit $\mathrm{L}/\mathbb{Q}_p$ une extension de degré fini de $\mathbb{Q}_p$. Soit $\mathcal{O}$ l'anneau de valuation de* L. *Alors*

$$\mathcal{O} = \{x \in \mathrm{L},\ \mathrm{N}_{\mathrm{L}/\mathbb{Q}_p}(x) \in \mathbb{Z}_p\}.$$

Démonstration. — Clairement, $\mathcal{O} \subset \{x \in \mathrm{L},\ \mathrm{N}_{\mathrm{L}/\mathbb{Q}_p}(x) \in \mathbb{Z}_p\}$.
Réciproquement. Soit $x \in \mathrm{L}$ tel que $\mathrm{N}_{\mathrm{L}/\mathbb{Q}_p}(x) \in \mathbb{Z}_p$. Soit $P = \mathrm{Irr}(x, \mathrm{K}) \in \mathbb{Q}_p[X]$. Alors d'après le corollaire 5.3.3, $P \in \mathbb{Z}_p[X]$ et x est entier sur $\mathbb{Z}_p$. □

Remarque 6.2.2. — Grâce à la proposition 6.2.1, on obtient facilement que si $\|\mathrm{N}_{\mathrm{L}/\mathbb{Q}_p} x\|_p \leq 1$, alors $\|\mathrm{N}_{\mathrm{L}/\mathbb{Q}_p}(1+x)\|_p \leq 1$ (il suffit de se rappeler que $\mathcal{O}$ est un anneau !). On retrouve ainsi que $x \mapsto \|\mathrm{N}_{\mathrm{L}/\mathbb{Q}_p} x\|_p$ définit bien une norme sur L prolongeant $\|\cdot\|_p$.

Comme pour $\mathbb{Z}_p^\times$, le groupe des unités $\mathcal{O}^\times$ de $\mathcal{O}$ est un $\mathbb{Z}_p$-module et comme pour $\mathbb{Q}_p$, on peut considérer sur L la série logarithme p-adique $\log_p$ et la série exponentielle p-adique $\exp_p$.

Proposition 6.2.3. — *1) La série* $\displaystyle\sum_{i\geq 1} \frac{(-1)^i x^i}{i}$ *converge pour* $x \in \pi\mathcal{O}$.

2) Pour $j > e/(p-1)$, *la série* $\displaystyle\sum_{i\geq 0} \frac{x^i}{i!}$ *converge pour* $x \in \pi^j\mathcal{O}$.

Pour $j \geq 1$, posons $\mathcal{U}^j = 1 + \pi^j\mathcal{O} \subset 1 + \pi\mathcal{O}$.
Alors, on peut définir le logarithme p-adique d'une unité principale $x \in \mathcal{U}^1$ par

$$\log_p(x) = \sum_{i>0} \frac{(-1)^i (1-x)^i}{i}.$$

Soit $j > e/(p-1)$. Pour $x \in \pi^j$, on définit l'exponentielle p-adique de x

$$\exp_p(x) = \sum_{i\geq 0} \frac{x^i}{i!}.$$

Théorème 6.2.4. — *Soit* $j > e/(p-1)$. *Le logarithme p-adique induit un isomorphisme topologique de $\mathbb{Z}_p$-modules entre $\mathcal{U}^j$ et $\pi^j\mathcal{O}$, d'inverse* $\exp_p$.

Démonstration. — Identique à la situation où $\mathrm{L} = \mathbb{Q}_p$. □

Corollaire 6.2.5. — *Soit* $\mathrm{L}/\mathbb{Q}_p$ *une extension de degré n. Soit $\mathcal{O}$ l'anneau des entiers de* L. *Alors*

$$\mathcal{O}^\times \simeq \mu_{\mathrm{K}} \times \mathbb{Z}^n,$$

où μ_{K} *est le groupe des racines de l'unité de* K. *Le groupe* μ_{K} *est cyclique (fini).*

Démonstration. — Soit $j > e/(p-1)$.
On note que $\mathcal{O}^\times/\mathcal{U}^j$ est fini. Ainsi, le $\mathbb{Z}_p$-rang du module $\mathcal{O}^\times$ est identique à celui de $\mathcal{U}^j$ lui-même identique à celui de $\pi^j\mathcal{O} \simeq \mathcal{O}$ donc de rang n.
On a ainsi $\mathcal{O}^\times \simeq \mu_{\mathrm{K}} \times \mathbb{Z}_p^n$.
On conclut en notant que comme $\mathcal{O}^\times/\mathcal{U}^j$ est fini, μ_{K} est fini. □

Corollaire 6.2.6. — *Soit* $\mathrm{L}/\mathbb{Q}_p$ *une extension de degré* n. *Alors*

$$\mathrm{L}^\times \simeq \mathbb{Z} \times \mu_{\mathrm{K}} \times \mathbb{Z}_p^n.$$

6.2.2. Le corps des séries formelles sur un corps fini. — Soit k un corps fini et soit $k[[X]]$ l'anneau des séries formelles

$$f = \sum_{i=0}^{\infty} a_i X^i, \qquad a_i \in k.$$

On va montrer que $k[[X]]$ est un anneau de valuation discrète.

On montre tout d'abord que le groupe des unités $k[[X]]^*$ de $k[[X]]$ est

$$k[[X]]^* = \{\sum_{i=0}^{\infty} a_i X^i \mid a_0 \neq 0\}.$$

En effet, $\displaystyle\sum_{i=0}^{\infty} a_i X^i$ est inversible si et seulement s'il existe $\displaystyle\sum_{j=0}^{\infty} b_i X^i$ telle que

$$\left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{i=0}^{\infty} b_j X^j\right) = 1.$$

On en déduit que

$$\begin{aligned} &a_0 b_0 = 1, \\ &a_0 b_1 + a_1 b_0 = 0, \\ &a_0 b_2 + a_1 b_1 + a_2 b_2 = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots . \end{aligned}$$

En particulier, si $\displaystyle\sum_{i=0}^{\infty} a_i X^i$ est inversible, alors $a_0 \neq 0$. Inversement, supposons que $a_0 \neq 0$ et cherchons à déterminer les coefficients b_j par récurrence. Si on suppose avoir déterminé $b_0, \ldots, b_{n-1}$, alors l'équation

$$a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = 0$$

permet de calculer b_n. Donc, $\sum_{i=0}^{\infty} a_i X^i$ est inversible.

Notons ensuite que tout $f(X) \in k[[X]]$ s'écrit de façon unique sous la forme

$$f(X) = X^n u(X),$$

avec $u(X) \in k[[X]]^*$. On en déduit que $k[[X]]$ est un anneaux de valuation discrète. Son idéal maximal $Xk[[X]]$ est engendré par X. L'application

$$k[[X]] \to k,$$
$$f(X) \mapsto a_0$$

est un homomorphisme surjectif. Son noyau est l'idéal $Xk[[X]]$ ce qui fournit un isomorphisme

$$k[[X]]/Xk[[X]] \simeq k.$$

Ainsi, le corps résiduel de $k[[X]]$ est isomorphe à k.

On note $k((X))$ le corps des fractions de $k[[X]]$. Comme pour $k[[X]]$, tout $f \in k((X))$ sécrit de façon unique sous la forme :

$$f(X) = X^n u(X), \qquad n \in \mathbb{Z},\ u(X) \in k[[X]]^*.$$

On en déduit que que $k((X))$ s'identifie à l'ensemble des séries formélles

$$\sum_{i=i_0}^{\infty} a_i X^i, \qquad i_0 \in \mathbb{Z},\ a_i \in k.$$

La valuation discrète corréspondante est donnée par

$$v(f(X)) = n, \qquad si\ f(X) = X^n u(X),\ u(X) \in k[[X]]^*.$$

Autrement dit, si $f(X) = \sum_{i=i_0}^{\infty} a_i X^i$, alors

$$v(f(X)) = \min\{i \,|\, a_i \neq 0\}.$$

L'ecriture

$$v(f(X) - g(X)) \geqslant n$$

signifie que les séries $f(X)$ et $g(X)$ ont mêmes coefficients jusqu'au degré $n-1$. On en déduit facilement que toute suite de Cauchy est convergente i.e. que $k((X))$ est complet.

Ainsi $k((X))$ est un corps local de caractéristique p, la caracteristique de k.

6.3. Système de représentants

Soit K un corps local. Le corps résiduel $k_{\mathrm{K}} = \mathcal{O}_{\mathrm{K}}/\mathfrak{m}_{\mathrm{K}}$ est fini et on note p sa caractéristique. Alors k_{K} est une extension finie de $\mathbb{F}_p$ et on pose $f = [k_{\mathrm{K}} : \mathbb{F}_p]$, $q = p^f$.

On normalise la valeur absolue $\| \cdot \|_{\mathrm{K}}$ en posant $\rho = q^{-1}$, i.e.

$$\|x\|_{\mathrm{K}} = \left(\frac{1}{q}\right)^{v_{\mathrm{K}}(x)}.$$

Si $x \in \mathcal{O}_{\mathrm{K}}$, on note $\bar{x}$ la classe de x dans k_{K} :

$$\bar{x} = x + \mathfrak{m}_{\mathrm{K}} \equiv x \pmod{\pi_{\mathrm{K}}}.$$

Définition 6.3.1. — On appelle système de représentants de k_{K} dans $\mathcal{O}_{\mathrm{K}}$ une partie $S \subset \mathcal{O}_{\mathrm{K}}$ telle que pour tout $\xi \in k_{\mathrm{K}}$ il existe un unique élément $s \in S$ vérifiant $\bar{s} = \xi$.

Exemple 6.3.2. — Soit $\mathrm{K} = \mathbb{Q}_p$. Alors $S = \{0, 1, \ldots, p-1\}$ est un système de représentants de $\mathbb{F}_p$ dans $\mathbb{Z}_p$.

Exemple 6.3.3. — Soit $\mathrm{K} = k((X))$. Alors $S = k$ est un système de représentants de k dans $k[[X]]$.

Proposition 6.3.4. — *Soit S un système de représentants du corps local* K. *Alors tout $a \in \mathcal{O}_{\mathrm{K}}$ s'écrit de façon unique comme série convergente :*

$$a = \sum_{i=0}^{\infty} s_i \pi_{\mathrm{K}}^i, \qquad s_i \in S.$$

Tout $x \in \mathrm{K}$ s'écrit de même :

$$x = \sum_{i=i_0}^{\infty} s_i \pi_{\mathrm{K}}^i, \qquad i_0 \in \mathbb{Z},\ s_i \in S.$$

Démonstration. — Soit $a \in \mathcal{O}_{\mathrm{K}}$. Alors il existe un unique $s_0 \in S$ tel que $\bar{s}_0 = \bar{a}$, i.e.

$$a \equiv s_0 \pmod{\pi_{\mathrm{K}}}.$$

Alors a s'écrit :

$$a = s_0 + a_1 \pi_{\mathrm{K}}, \qquad a_1 \in \mathcal{O}_{\mathrm{K}}.$$

En appliquant ce qui précède à a_1 on obtient :

$$a_1 = s_1 + a_2\pi_{\mathrm{K}}, \qquad s_1 \in S, a_2 \in \mathcal{O}_{\mathrm{K}},$$

d'où

$$a = s_0 + s_1\pi_{\mathrm{K}} + a_2\pi_{\mathrm{K}}^2$$

et ainsi de suite. Comme pour tout n on a

$$a = s_0 + s_1\pi_{\mathrm{K}} + \cdots + s_n\pi_{\mathrm{K}}^n + a_{n+1}\pi_{\mathrm{K}}^{n+1}$$

avec $v_{\mathrm{K}}(a_{n+1}\pi_{\mathrm{K}}^{n+1}) \geqslant n+1$, la série

$$\sum_{i=0}^{\infty} s_i\pi_{\mathrm{K}}^i$$

converge vers a. Inversement, toute série de la forme $\sum_{i=0}^{\infty} s_i\pi_{\mathrm{K}}^i$ est convergente puisque son terme général tend vers 0 (voir la proposition 4.3.5).
Si $x \in \mathrm{K}$, alors $x = \pi_{\mathrm{K}}^{v_{\mathrm{K}}(x)}u$ avec $u \in U_{\mathrm{K}}$ et en développant u on obtient

$$x = \sum_{i=i_0}^{\infty} s_i\pi_{\mathrm{K}}^i,$$

où $i_0 = v_{\mathrm{K}}(x)$. La proposition est démontrée. □

Nous voulons montrer qu'un corps local possède un système de représentants particulier formé par des racines de l'unité.

Théorème 6.3.5. — *Soit* K *un corps local et soit* $q = \#k_{\mathrm{K}}$. *Alors*

(i) Tout $\xi \in k_{\mathrm{K}}$ *possède un unique relèvement* $[\xi] \in \mathcal{O}_{\mathrm{K}}$ *vérifiant*

$$[\xi]^q = [\xi] \ ;$$

(ii) Pour tout $\xi, \eta \in k_{\mathrm{K}}$ *on a*

$$[\xi]\,[\eta] = [\xi\eta];$$

(iii) La famille $S_m = \{[\xi],\ \xi \in k_{\mathrm{K}}\}$ *est un système de représentants de* k_{K} *dans* $\mathcal{O}_{\mathrm{K}}$.

Démonstration. — i) Soit $f(X) = X^q - X \in \mathcal{O}_{\mathrm{K}}[X]$ et soit $\bar{f}(X) \in k_{\mathrm{K}}[X]$ la réduction de $f(X)$ modulo $\mathfrak{m}_{\mathrm{K}}$. Comme $\bar{f}'(X) = \bar{q}X^{q-1} - \bar{1} = -\bar{1}$, le polynôme $\bar{f}(X)$ est séparable.

Soit $\xi \in k_{\mathrm{K}}$. Alors ξ est une racine de $\bar{f}(X)$ et par le lemme de Hensel, il existe une unique raçine $[\xi] \in \mathcal{O}_{\mathrm{K}}$ de $f(X)$ telle que $\xi = [\xi] \pmod{\pi_{\mathrm{K}}}$. On en déduit (i).

(ii) Comme $\xi = [\xi] \pmod{\pi_{\mathrm{K}}}$ et $\eta = [\eta] \pmod{\pi_{\mathrm{K}}}$, on a $\xi\eta = [\xi]\,[\eta] \pmod{\pi_{\mathrm{K}}}$, i.e. $[\xi]\,[\eta]$ est un représentant de $\xi\eta$ dans $\mathcal{O}_{\mathrm{K}}$. Comme

$$([\xi]\,[\eta])^q = ([\xi])^q\,([\eta])^q = [\xi]\,[\eta],$$

l'unicité du relèvement démontrée dans (i) implique que $[\xi]\,[\eta] = [\xi\eta]$.
(iii) est une conséquence immédiate de i). □

Corollaire 6.3.6. — *Soit* K *un corps local et soit* $q = \#k_{\mathrm{K}}$. *Alors* K *contient toutes les racines* $(q-1)$*-ièmes de l'unité.*

Démonstration. — Les éléments $[\xi]$, $\xi \neq 0$, sont les racines $(q-1)$-ièmes de l'unité. □

Définition 6.3.7. — Le système de représentants S_m est appelé système de représentants multiplicatif ou système de Teichmüller.

Proposition 6.3.8. — *Soit* L/K *une extension finie de corps locaux. Alors il existe* $a \in \mathcal{O}_L$ *tel que* $\mathcal{O}_{\mathrm{L}} = \mathcal{O}_{\mathrm{K}}[a]$.

Démonstration. — Soit l le corps résiduel de L et soit k celui de K. Comme l'extension l/k est séparable, il existe $\bar{\alpha} \in l$ tel que $l = k[\bar{\alpha}]$. On prend le relèvement $\alpha \in \mathcal{O}_L$ de $\bar{\alpha}$ vérifiant $\alpha^{|l|-1} = 1$.
Posons $a = \alpha + \pi_{\mathrm{L}}$, où π_{L} est une uniformisante de L. Soit $B = \mathcal{O}_{\mathrm{K}}[a]$. Alors B contient un système de représentants de l car $a^i \equiv \alpha^i (\mathrm{mod}\ \pi_{\mathrm{L}})$. D'autre part, B contient l'élément

$$x = a^{|l|-1} - 1 = (\alpha + \pi_{\mathrm{L}})^{|l|-1} - 1 = (q-1)\alpha^{|l|-2}\pi_{\mathrm{L}} + \cdots$$

qui est une uniformisante de L car $v_{\mathrm{L}}(x) = 1$. Comme B est compact et dense dans $\mathcal{O}_{\mathrm{L}}$, on en déduit que $B = \mathcal{O}_{\mathrm{L}}$. □

Exemple 6.3.9. — Soit $\mathrm{L}/\mathbb{Q}_p$ une extension de degré $n = ef$, d'anneau d'entiers $\mathcal{O}$. Soit π une uniformisante de L. Si $\mathbb{F}_{p^f}$ est le corps résiduel de L, le groupe $\mathcal{O}^\times$ contient les racines (p^f-1)-ème de l'unité et tout élément $x \in \mathrm{L}$ s'écrit de manière unique :

$$x = \pi^{\mathrm{v}(x)}(a_0 + a_1\pi + \cdots, a_k\pi^k + \cdots),$$

où les éléments a_i sont des racines primitives $(p^f - 1)$-ème de l'unité.

6.4. La classification des corps locaux

Nous pouvons maintenant classifier les corps locaux. Commençons par les corps de caractéristique 0.

Théorème 6.4.1. — *Soit* K *un corps local de caractéristique* 0 *à corps résiduel de caractéristique* $p > 0$. *Alors* K *est isomorphe à une extension finie de* $\mathbb{Q}_p$.

Démonstration. — Le corps K étant de caractérsitique nulle, il contient un sous-corps isomorphe à $\mathbb{Q}$. Donc, on peut supposer que $\mathbb{Q} \subset \mathrm{K}$. La réstriction de $\| \cdot \|_{\mathrm{K}}$ à $\mathbb{Q}$ est une valeur absolue non-archimédienne sur $\mathbb{Q}$. Par le théorème d'Ostrowski, il existe un nombre premier ℓ tel que la réstriction de $\| \cdot \|_{\mathrm{K}}$ à $\mathbb{Q}$ est équivalente à $\| \cdot \|_\ell$. Comme K est complet, il contient le complété $\mathbb{Q}_\ell$ de $\mathbb{Q}$. Donc, K est une extension de $\mathbb{Q}_\ell$. Le corps résiduel k_{K} est une extension de $\mathbb{F}_p = k_{\mathbb{Q}_\ell}$, d'où $\ell = p$.
Soient $f = [k_{\mathrm{K}} : \mathbb{F}_p]$ et $e = v_{\mathrm{K}}(p)$. Alors K est une extension finie de $\mathbb{Q}_p$ de degré fe. □

Résolvons maintenant le cas où le corps K est de caractéristique finie.

Théorème 6.4.2. — *Soit* K *un corps local de caractéristique* p *à corps résiduel* k. *Alors* K *est isomorphe à* $k((X))$.

Démonstration. — Soit $k = \mathbb{F}_q$.
Pour tout $\xi \in k$ soit $[\xi]$ le représentant de Teichmüller de ξ. Comme K est de caractéristique p, on a

$$([\xi] + [\eta])^q = [\xi]^q + [\eta]^q = [\xi] + [\eta].$$

Comme

$$\xi + \eta = [\xi] + [\eta] \pmod{\pi_{\mathrm{K}}}$$

l'unicité du relèvement implique que

$$[\xi + \eta] = [\xi] + [\eta].$$

Donc l'application

$$k \to \mathrm{K},$$
$$\xi \mapsto [\xi]$$

est un homomorphisme de corps qui identifie k à un sous-corps de K. Pour simplifier la notation on va écrire ξ au lieu de $[\xi]$. Par la proposition 6.3.4, tout élément de K s'écrit de manière unique

$$\sum_{i=i_0}^{\infty} a_i \pi_{\mathrm{K}}^i$$

avec $a_i \in k$. L'application

$$k((X)) \to \mathrm{K},$$
$$\sum_{i=i_0}^{\infty} a_i X^i \mapsto \sum_{i=i_0}^{\infty} a_i \pi_{\mathrm{K}}^i$$

est alors un isomorphisme. □

6.5. Extensions non-ramifiées

6.5.1. Quelques généralités. — Dans ce paragraphe K désigne un corps complet pour une valuation discrète.

Définition 6.5.1. — On dit qu'une extension finie L/K est non-ramifiée si $f(\mathrm{L}/\mathrm{K}) = [\mathrm{L} : \mathrm{K}]$ et si l'extension des corps résiduels $k_{\mathrm{L}}/k_{\mathrm{K}}$ est séparable.

Dans le cas général la condition de séparabilité de $k_{\mathrm{L}}/k_{\mathrm{K}}$ est *importante.* Neanmoins pour les *corps locaux* elle est automatiquement satisfaite car toute extension d'un corps fini est séparable.

Voici des propriétés des extensions non-ramifiées découlant directement de cette définition.

Proposition 6.5.2. — *(i)* L/K *est non-ramifiée si et seulement si* $e(\mathrm{L}/\mathrm{K}) = 1$ *et* $k_{\mathrm{L}}/k_{\mathrm{K}}$ *est séparable.*

(ii) L/K *est non-ramifiée si et seulement si* π_{K} *est une uniformisante de* L *et* $k_{\mathrm{L}}/k_{\mathrm{K}}$ *est séparable.*

(iii) Soit $\mathrm{K} \subseteq \mathrm{L} \subseteq \mathrm{M}$ *une tour d'extensions. Alors* M/K *est non-ramifiée si et seulement si* L/K *et* M/L *sont non-ramifiées.*

Soit L/K une extension non-ramifiée et soit $k_{\mathrm{L}}/k_{\mathrm{K}}$ l'extension résiduelle correspondante. Elle est séparable, il existe $\bar{\alpha} \in k_{\mathrm{L}}$ tel que $k_{\mathrm{L}} = k_{\mathrm{K}}(\bar{\alpha})$. Pour étudier la structure des extensions non-ramifiées nous avons besoin des propositions suivantes.

Proposition 6.5.3. — *Soit* K *un corps local et soit* $l = k_{\mathrm{K}}(\bar{\alpha})$ *une extension finie séparable de* k_{K}. *Soient* $\bar{f}(X) \in \mathcal{O}[X]$ *le polynôme minimal de* $\bar{\alpha}$ *et* $f(X)$ *un polynôme unitaire dont la réduction modulo* π_{K} *est égale à* $\bar{f}(X)$. *Soit* α *une racine de* f *dans* $\bar{\mathrm{K}}$. *Alors*

$$\mathrm{L} = \mathrm{K}(\alpha)$$

est une extension non-ramifiée de K *dont le corps résiduel* k_{L} *est isomorphe à* l.

Démonstration. — Comme $\bar{f}(X)$ est irréductible, $f(X)$ l'est aussi et L est une extension de K de degré

$$[\mathrm{L} : \mathrm{K}] = \deg(f) = \deg(\bar{f}) = [l : k_{\mathrm{K}}].$$

Soit α une racine du polynôme $f(X)$ et soit $\mathrm{L} = \mathrm{K}(\alpha)$. Alors α est entier sur $\mathcal{O}_{\mathrm{K}}$ et $\alpha(\mathrm{mod}\Pi_{\mathrm{L}}) \in k_{\mathrm{L}}$ est une racine de $\bar{f}(X)$ contenue dans $\mathrm{k_L}$. L'élément $\alpha(\mathrm{mod}\Pi_{\mathrm{L}})$ est de même degré sur $\mathrm{k_K}$ que $\bar{\alpha}$, *i.e.* de degré $\deg(\bar{f})$. Ainsi,

$$[\mathrm{L} : \mathrm{K}] \geqslant [k_{\mathrm{L}} : k_{\mathrm{K}}] \geqslant [k_{\mathrm{K}}(\bar{\alpha}) : k_{\mathrm{K}}] = \deg(\bar{f}) = \deg(f) = [\mathrm{L} : \mathrm{K}]$$

ce qui entraine que

$$[k_{\mathrm{L}} : k_{\mathrm{K}}] = [k_{\mathrm{K}}(\bar{\alpha}) : k_{\mathrm{K}}] = \deg(\bar{f}) = [\mathrm{L} : \mathrm{K}].$$

Donc, L/K est non-ramifiée et son corps résiduel est isomorphe à $l = k_{\mathrm{K}}(\bar{\alpha})$. □

Proposition 6.5.4. — *Soit* L/K *une extension non-ramifiée. Soient* $k_{\mathrm{L}} = k_{\mathrm{K}}(\bar{\alpha})$ *et* $\bar{f}(X) \in k_{\mathrm{K}}[X]$ *le polynôme minimal de* $\bar{\alpha}$. *Soit* $f(X) \in \mathcal{O}_{\mathrm{K}}[X]$ *un polynôme unitaire dont la réduction modulo* π_{K} *est exactement* $\bar{f}$. *Alors*

(i) $f(X)$ *a une unique racine* $\alpha \in \mathcal{O}_{\mathrm{L}}$ *telle que* $\bar{\alpha} = \alpha \pmod{\pi_{\mathrm{L}}}$.
(ii) $\mathrm{L} = \mathrm{K}(\alpha)$.
(iii) Si K *est de plus un corps local, alors* $\mathcal{O}_{\mathrm{L}} = \mathcal{O}_{\mathrm{K}}[\alpha]$.

Démonstration. — Comme $k_{\mathrm{L}}/k_{\mathrm{K}}$ est séparable, $\bar{\alpha}$ est une racine simple du polynôme $\bar{f}(X)$ et (i) découle du lemme de Hensel.
Point (ii). Posons $\mathrm{F} = \mathrm{K}(\alpha)$. Le corps F est contenu dans L. L'extension F/K est non-ramifiée, ainsi $[\mathrm{F} : \mathrm{K}] = [\mathrm{k_F} : \mathrm{k_K}]$. Ce qui donne

$$[\mathrm{L} : \mathrm{K}] = [\mathrm{k_L} : \mathrm{k_K}] = \deg(\bar{f}) = \deg(f) = [\mathrm{F} : \mathrm{K}],$$

et ainsi $\mathrm{F} = \mathrm{L}$.
(iii) C'est un cas particulier de la proposition 6.3.8. Il suffit de noter qu'ici l'anneau $\mathcal{O}_{\mathrm{K}}[\alpha]$ contient une uniformisante de $\mathcal{O}_{\mathrm{L}}$ ainsi qu'un système de représentants. □

Soient L/K et M/K deux extensions finies de K. On note $\mathrm{Hom_K}(\mathrm{L}, \mathrm{M})$ l'ensemble formé par les homomorphismes

$$\sigma \ : \ \mathrm{L/K} \to \mathrm{M/K}$$

qui fixent K. Soit $\sigma \in \mathrm{Hom_K}(\mathrm{L}, \mathrm{M})$. Comme $\sigma(\mathcal{O}_{\mathrm{L}}) \subseteq \mathcal{O}_{\mathrm{M}}$ en passant aux corps résiduels on obtient un homomorphisme

$$\bar{\sigma} \ : \ k_{\mathrm{L}}/k_{\mathrm{K}} \to k_{\mathrm{M}}/k_{\mathrm{K}} \, .$$

On a défini une application

$$\begin{array}{rccc} \varphi : \mathrm{Hom_K}(\mathrm{L}, \mathrm{M}) & \to & \mathrm{Hom}_{k_{\mathrm{K}}}(k_{\mathrm{L}}, k_{\mathrm{M}}) \\ \sigma & \mapsto & \bar{\sigma}. \end{array}$$

La proposition suivante joue un rôle clé.

Proposition 6.5.5. — *Si* L/K *est non-ramifiée, alors*

$$\varphi : \mathrm{Hom_K}(\mathrm{L}, \mathrm{M}) \to \mathrm{Hom}_{k_{\mathrm{K}}}(k_{\mathrm{L}}, k_{\mathrm{M}})$$

réalise une bijection. En particulier, si L/K *est une extension galoisienne non-ramifiée, alors on a un isomorphisme canonique*

$$\mathrm{Gal(L/K)} \simeq \mathrm{Gal}(k_{\mathrm{L}}/k_{\mathrm{K}}).$$

Démonstration. — Soit $k_{\mathrm{L}} = k_{\mathrm{K}}(\bar{\alpha})$ et soit $\bar{f}(X)$ le polynôme minimal de $\bar{\alpha}$. Soit $f(X) \in \mathcal{O}_{\mathrm{K}}[X]$ un polynôme unitaire dont la réduction est égale à $\bar{f}(X)$. Alors, d'après la proposition 6.5.3, on a $\mathrm{L} = \mathrm{K}(\alpha)$, où α est une racine de $f(X)$ vérifiant $\bar{\alpha} = \alpha \pmod{\pi_{\mathrm{L}}}$. L'extension L/K est séparable et la preuve de la proposition se base sur le fait suivant : l'application

$\sigma \mapsto \sigma(\alpha)$ établie une bijection entre $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{M})$ et les racines β du polynôme $f(X)$ dans M. Montrons d'abord que φ est surjective. Soit $\bar{\sigma} \in \mathrm{Hom}_{k_{\mathrm{K}}}(k_{\mathrm{L}}, k_{\mathrm{M}})$. Alors $\bar{\beta} = \bar{\sigma}(\bar{\alpha})$ est une racine de $\bar{f}(X)$ et par le lemme de Hensel, il existe une unique racine β de $f(X)$ telle que $\bar{\beta} = \beta \pmod{\pi_{\mathrm{L}}}$. En posant $\sigma(\alpha) = \beta$ on obtient un homomorphisme $\sigma \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{M})$ tel que $f(\sigma) = \bar{\sigma}$. Donc φ est surjectif.
Pour montrer l'injectivité on remarque que si σ_1 et σ_2 sont deux éléments de $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{M})$ tels que $\bar{\sigma}_1 = \bar{\sigma}_2$, alors $\sigma_1(\alpha)$ et $\sigma_2(\alpha)$ sont deux racines de $f(X)$ tels que $\sigma_1(\alpha) \equiv \sigma_2(\alpha) \pmod{\pi_{\mathrm{L}}}$. Mais dans ce cas $\sigma_1(\alpha) = \sigma_2(\alpha)$ toujours par le lemme de Hensel. □

Proposition 6.5.6. — *Soient* L_1 *et* L_2 *deux extensions non-ramifiées de* K. *Alors le compositum* $\mathrm{L}_1\mathrm{L}_2$ *est non-ramifié sur* K.

Démonstration. — Soient k_i et k_2 les corps résiduels des L_1 et L_2 et soit l le compositum k_1k_2. Soit L une extension non-ramifiée de K à corps résiduel l (une telle extension existe par la proposition 6.5.3). On a

$$\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}_i, \mathrm{L}) \equiv \mathrm{Hom}_{k_{\mathrm{K}}}(k_i, l)$$

et comme $k_i \subseteq l$ on obtient que $\mathrm{L}_i \subseteq \mathrm{L}$. Alors $\mathrm{L}_1\mathrm{L}_2 \subseteq \mathrm{L}$, et comme L/K est non-ramifiée, $\mathrm{L}_1\mathrm{L}_2$/K l'est aussi. □

6.5.2. Retour aux corps locaux. — Supposons maintenant que K est un corps local, i.e. que k_{K} est fini. Alors L/K est non-ramifiée si et seulement si $f(\mathrm{L}/\mathrm{K}) = 1$.

Théorème 6.5.7. — *Soit* K *un corps local. Alors pour tout* n *il existe une unique extension non-ramifiée de* K *de degré* n. *Cette extension est galoisienne et son groupe de Galois est cyclique d'ordre* n.

Démonstration. — Soit k_{K} le corps résiduel de K. Le corps k_{K} étant fini, il existe une unique extension l/k_{K} de degré n et par la proposition 6.5.3, on peut construire une extension non-ramifiée L/K à corps résiduel $k_{\mathrm{L}} = l$. L'existence de L est donc établie.

L'extension $k_{\mathrm{L}}/k_{\mathrm{K}}$ est galoisienne et $\mathrm{Gal}(k_{\mathrm{L}}/k_{\mathrm{K}})$ est cyclique d'ordre n. Par la proposition 6.5.5, on obtient

$$\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{L}) \simeq \mathrm{Hom}_{k_{\mathrm{K}}}(k_{\mathrm{L}}, k_{\mathrm{L}}) = \mathrm{Gal}(k_{\mathrm{L}}/k_{\mathrm{K}}).$$

Donc, il existe n automorphismes de L/K ce qui entraîne que L/K est galoisienne et ainsi

$$\mathrm{Gal}(\mathrm{L}/\mathrm{K}) = \mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{L}) \simeq \mathrm{Gal}(k_{\mathrm{L}}/k_{\mathrm{K}})$$

ce qui montre que L/K est cyclique d'ordre n.

On montre maintenant que L/K est l'unique extension non-ramifiée de degré n. Supposons que M/K est une autre extension non-ramifiée de corps résiduel $k_M = l$. Alors, en utilisant toujours la proposition 6.5.5, on a

$$\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M}) \simeq \mathrm{Hom}_{k_{\mathrm{K}}}(l,l).$$

Comme $\mathrm{Hom}_{k_{\mathrm{K}}}(l,l)$ est non-vide, il existe un homomorphisme $\sigma : \mathrm{L}/\mathrm{K} \to \mathrm{M}/\mathrm{K}$. On a déjà montré que L/K est galoisienne, d'où

$$\mathrm{L} = \sigma(\mathrm{L}) \subseteq \mathrm{M}.$$

Comme L/K et M/K ont même degré, on en déduit que $\mathrm{L} = \mathrm{M}$. □

Soit L/K une extension non-ramifiée finie. Dans la preuve du théorème 6.5.7, on a établi l'isomorphisme

$$\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \simeq \mathrm{Gal}(k_{\mathrm{L}}/k_{\mathrm{K}}).$$

Le groupe de Galois de $k_{\mathrm{L}}/k_{\mathrm{K}}$ est engendré par l'automorphisme $\mathrm{Frob}_{k_{\mathrm{L}}/k_{\mathrm{K}}}$ défini par

$$\mathrm{Frob}_{k_{\mathrm{L}}/k_{\mathrm{K}}}(x) = x^q,$$

où $q = \#k_{\mathrm{K}}$.

Définition 6.5.8. — On appelle automorphisme de Frobenius de L/K et on note $\mathrm{F}_{\mathrm{L}/\mathrm{K}}$ l'élément de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ qui correspond à $\mathrm{F}_{k_{\mathrm{L}}/k_{\mathrm{K}}}$. On a pour tout $x \in O_{\mathrm{L}}$,

$$\mathrm{F}_{\mathrm{L}/\mathrm{K}}(x) \equiv x^q \pmod{\pi_{\mathrm{L}}}.$$

Terminons en donnant une construction explicite des extensions non-ramifiées des corps locaux.

Théorème 6.5.9. — *Soit* K *un corps local et soit* $q = \#k_{\mathrm{K}}$. *Soit* ζ_{q^n-1} *une racine primitive* $q^n - 1$*-ième de l'unité. Alors* $\mathrm{K}(\zeta_{q^n-1})$ *est l'unique extension non-ramifiée de* K *de degré* n.

Démonstration. — Soit L/K une extension non-ramifiée de degré n. Alors $\#k_{\mathrm{L}} = q^n$ et par le corollaire 6.3.6, L contient ζ_{q^n-1}. Donc $\mathrm{K}(\zeta_{q^n-1}) \subseteq \mathrm{L}$. D'autre part le corps résiduel de $\mathrm{K}(\zeta_{q^n-1})$ contient toutes les racines $q^n - 1$-ièmes de l'unité i.e. coïncide avec k_{L}. Donc $\mathrm{L} = \mathrm{K}(\zeta_{q^n-1})$. □

Exemple 6.5.10. — Soit $p > 2$ et soit $a \in \mathbb{Z}$ avec $a \notin \mathbb{F}_p^2$. Alors $f = X^2 - a$ est irréductible sur $\mathbb{F}_p[X]$ et ainsi $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ est l'unique extension quadratique non ramifiée de $\mathbb{Q}_p$.

Soit $p = 2$. L'unique extension quadratique de $\mathbb{F}_2$ est donnée par $\bar{f} = X^2 + X + 1$. Soit le relèvement $f = X^2 + X + 1 \in \mathbb{Z}_2[X]$ de $\bar{f}$ et soit α une racine de f dans $\overline{\mathbb{Q}_2}$. Alors l'extension $\mathbb{Q}_2(\alpha)/\mathbb{Q}_2$ est l'unique extension quadratique non-ramifiée de $\mathbb{Q}_2$. Remarquons ensuite que $\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\sqrt{-3})$ puis que $-3 \cdot 5 \equiv 1 (\mathrm{mod}\ 8)$ et donc que $-3 \cdot 5 \in \mathbb{Q}_2^2$. Ainsi, $\mathbb{Q}_2(\alpha) = \mathbb{Q}_2(\sqrt{5})$.

6.6. Extensions totalement ramifiées

Dans ce paragraphe K est un corps complet pour une valuation discrète.

Définition 6.6.1. — On dit qu'une extension L/K est totalement ramifiée si $f(L/\mathrm{K}) = 1$.

Il résulte de cette définition que :

Proposition 6.6.2. — *(i)* L/K *est totalement ramifiée si et seulement si* $k_{\mathrm{L}} = k_{\mathrm{K}}$.
(ii) L/K *est totalement ramifiée si et seulement si* $e(\mathrm{L}/\mathrm{K}) = [\mathrm{L} : \mathrm{K}]$.
(iii) si $\mathrm{K} \subseteq \mathrm{L} \subseteq \mathrm{M}$, *alors* M/K *est totalement ramifiée si et seulement si* M/L *et* L/K *sont totalement ramifiées.*

Définition 6.6.3. — Le polynôme

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in O_{\mathrm{K}}[X]$$

est dit d'Eisenstein si
(i) $a_i \equiv 0 \pmod{\pi_{\mathrm{K}}}$;
(ii) $a_0 \neq 0 \pmod{\pi_{\mathrm{K}}^2}$.

Proposition 6.6.4. — *Si $f(X)$ est un polynôme d'Eisenstein, alors il est irréductible sur* K.

Démonstration. — C'est une application du critère d'Eisenstein. □

Théorème 6.6.5. — *1) Soit $f(X) \in \mathcal{O}_{\mathrm{K}}[X]$ un polynôme d'Eisenstein et soit α une racine de $f(X)$. Alors* $\mathrm{L} = \mathrm{K}(\alpha)$ *est une extension totalement ramifiée de* K *et α est une uniformisante de* L.
2) Réciproquement, soient L/K *une extension totalement ramifiée et π_{L} une uniformisante de* L. *Alors le polynôme minimal de π_{L} est un polynome d'Eisenstein et on a*

$$\mathcal{O}_{\mathrm{L}} = \mathcal{O}_{\mathrm{K}}[\pi_{\mathrm{L}}].$$

Démonstration. — 1) Soit α une racine d'un polynôme d'Eisenstein

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathcal{O}_{\mathrm{K}}[X].$$

Alors

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0.$$

Si v_{L} désigne la valuation discrète sur L, alors

$$nv_{\mathrm{L}}(\alpha) = v_{\mathrm{L}}(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \geqslant \min_i\{v_{\mathrm{L}}(a_i) + iv_{\mathrm{L}}(\alpha)\}.$$

Comme $v_{\mathrm{L}}(a_i) > 0$, on en déduit que $v_{\mathrm{L}}(\alpha) > 0$. Comme $v_{\mathrm{L}}(a_i) \geqslant v_{\mathrm{L}}(a_0)$, on obtient pour $i = 1, \ldots, n-1$

$$v_{\mathrm{L}}(a_i) + iv_L(\alpha) > v_{\mathrm{L}}(a_0),$$

d'où

$$nv_{\mathrm{L}}(\alpha) = v_{\mathrm{L}}(a_0).$$

On a $v_{\mathrm{L}}(a_0) = v_{\mathrm{L}}(\pi_{\mathrm{K}}) = e$ et $v_{\mathrm{L}}(\alpha) \geqslant v_{\mathrm{L}}(\pi_{\mathrm{L}}) = 1$. Donc,

$$n \leqslant nv_{\mathrm{L}}(\alpha) = e,$$

ce qui signifie que $n = e$ i.e. que L/K est totalement ramifiée.

2) Soit L/K une extension totalement ramifiée. Fixons une extension galoisienne M/K qui contient L. Alors M contient tous les conjugués $\sigma_i(\pi_{\mathrm{L}})$ et on a

$$v_{\mathrm{M}}(\sigma_i(\pi_{\mathrm{L}})) = v_{\mathrm{M}}(\pi_{\mathrm{L}}) > 0.$$

Soit $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ le polynôme minimal de π_L. Comme

$$f(X) = \prod_i (X - \sigma_i(\pi_{\mathrm{L}}))$$

on obtient que $v_{\mathrm{M}}(a_i) > 0$, d'où $v_{\mathrm{K}}(a_i) > 0$ i.e.

$$a_i \equiv 0 \pmod{\pi_{\mathrm{K}}}.$$

D'autre part, on a

$$v_{\mathrm{L}}(a_0) = v_{\mathrm{L}}(a_1\pi_{\mathrm{L}} + \cdots a_{n-1}\pi_{\mathrm{L}}^{n-1} + \pi_{\mathrm{L}}^n).$$

Comme

$$v_{\mathrm{L}}(a_i\pi_{\mathrm{L}}^i) = v_{\mathrm{L}}(a_i) + v_{\mathrm{L}}(\pi_{\mathrm{L}}^i) \geqslant ev_{\mathrm{K}}(a_i) + i \geqslant n + i$$

on a

$$v_L(\pi_{\mathrm{L}}^n) = n < v_{\mathrm{L}}(a_i\pi_{\mathrm{L}}^i)$$

d'où

$$v_{\mathrm{L}}(a_0) = v_{\mathrm{L}}(\pi_{\mathrm{L}}^n) = n.$$

Donc, $v_{\mathrm{K}}(a_0) = v_{\mathrm{L}}(a_0)/e = 1$ et on obtient donc que $f(X)$ est un polynôme d'Eisenstein.

Pour montrer que $\mathcal{O}_{\mathrm{L}} = \mathcal{O}_{\mathrm{K}}[\pi_{\mathrm{L}}]$, posons

$$B = \mathcal{O}_{\mathrm{K}}[[\pi_{\mathrm{L}}]] = \{\sum_{i=0}^{\infty} c_i\pi_{\mathrm{L}}^i \,|\, c_i \in \mathcal{O}_{\mathrm{K}}\}.$$

Comme $k_{\mathrm{L}} = k_{\mathrm{K}}$, l'anneau B contient un système de représentants de k_{L} et une uniformisante de L, d'où $B = \mathcal{O}_{\mathrm{L}}$. Pour montrer que $B = \mathcal{O}_{\mathrm{K}}[\pi_{\mathrm{L}}]$, on remarque que la formule

$$\pi_{\mathrm{L}}^n = -a_{n-1}\pi_{\mathrm{L}}^{n-1} - \cdots - a_1\pi_{\mathrm{L}} - a_0, \quad a_i \in \mathcal{O}_{\mathrm{K}},$$

permet d'écrire une série $\sum c_i\pi_{\mathrm{L}}^i$ comme un polynôme de π_{L} à coefficients dans $\mathcal{O}_{\mathrm{K}}$. □

Pour les corps locaux on peut montrer que toute extension finie peut être construite à partir des extensions non-ramifiées et totalement ramifiées de la façon suivante :

Théorème 6.6.6. — *Soit* L/K *une extension finie de corps locaux. Alors il existe une unique sous-extension* L_0/K *telle que*
i) L_0/K *est non-ramifiée ;*
ii) L/L_0 *est totalement ramifiée.*

Démonstration. — Soit k_L le corps résiduel de L et soit L_0 l'extension non-ramifiée de K à corps résiduel k_L. En utilisant la bijection

$$\mathrm{Hom}_K(L_0, L) \simeq \mathrm{Hom}_{k_K}(k_L, k_L),$$

on a l'existence d'un homomorphisme $\sigma : L_0/K \to L/K$ et comme L_0/K est galoisienne, on en déduit que $L_0 \subseteq L$. Comme

$$f(L/K) = f(L/L_0)f(L_0/K),$$

on voit que $f(L/L_0) = 1$, i.e. que L/L_0 est totalement ramifiée. □

Soit L/K une extension finie galoisienne. Suivant les notations du théorème 6.6.6, on pose

$$I_{L/K} = \mathrm{Gal}(L/L_0).$$

Alors $I_{L/K}$ est un sous-groupe distingué de Gal(L/K) et

$$\mathrm{Gal}(L/K)/I_{L/K} \simeq \mathrm{Gal}(L_0/L).$$

Définition 6.6.7. — La groupe $I_{L/K}$ est appelé le groupe d'inértie de l'extension L/K.

6.7. Discriminant d'une extension de corps locaux

Soit K un coprs local et soit L/K une extension finie (séparable) de degré n. Notons par $\mathcal{O}_K$ et $\mathcal{O}_L$ les anneaux de valuation de K et de L.
On rappelle que $\mathcal{O}_L$ est un $\mathcal{O}_K$ module libre de rang n (voir le corollaire 1.2.9).
Soit $\{x_1, \cdots, x_n\}$ une $\mathcal{O}_K$-base de $\mathcal{O}_L$:

$$\mathcal{O}_L = \mathcal{O}_K x_1 \oplus \cdots \oplus \mathcal{O}_K x_n.$$

On rappelle que le discriminant de la famille $\{x_1, \cdots, x_n\}$ est égal à :

$$\mathrm{d}(x_1, \cdots, x_n) = \det\left((\mathrm{Tr}_{L/K}(x_i x_j))_{i,j}\right).$$

Définition 6.7.1. — Le discriminant de l'extension de corps locaux L/K est l'idéal de $\mathcal{O}_{\mathrm{K}}$ engendré par le discriminant $\mathrm{d}(x_1, \cdots, x_n)$ de la $\mathcal{O}_{\mathrm{K}}$-base $\{x_1, \cdots, x_n\}$ de $\mathcal{O}_{\mathrm{L}}$. On le note $\mathrm{d}_{\mathrm{L/K}}$:

$$\mathrm{d}_{\mathrm{L/K}} = (\mathrm{d}(x_1, \cdots, x_n)) = \mathrm{d}(x_1, \cdots, x_n)\mathcal{O}_{\mathrm{K}}.$$

Remarque 6.7.2. — La définition ne dépend pas du choix de la base $\{x_1, \cdots, x_n\}$ (voir la section 1.3.1).

Proposition 6.7.3. — *Soit* $\mathrm{K} \subset \mathrm{L} \subset \mathrm{M}$ *une tour d'extensions finies de corps locaux. Alors*

$$\mathrm{d}_{\mathrm{M/K}} = (\mathrm{N}_{\mathrm{L/K}}(\mathrm{d}_{\mathrm{M/L}}) \cdot (\mathrm{d}_{\mathrm{L/K}})^n),$$

où $n = [\mathrm{L} : \mathrm{M}]$.

Démonstration. — Soit $\{1, \cdots, b^{n-1}\}$ une $\mathcal{O}_{\mathrm{L}}$-base de $\mathcal{O}_{\mathrm{M}}$ et soit $\{1, \cdots, a^{m-1}\}$ une $\mathcal{O}_{\mathrm{K}}$-base de $\mathcal{O}_{\mathrm{L}}$. Alors la famille $\{a^i b^j, i = 0, \cdots, m-1; j = 0, \cdots, n-1\}$ forme une $\mathcal{O}_{\mathrm{K}}$-base de $\mathcal{O}_{\mathrm{M}}$. Une écriture matricielle adéquate donne alors le résultat. □

Théorème 6.7.4. — *Soit* L/K *une extension finie de corps locaux. Soit* $e = e(L/\mathrm{K})$ *l'indice de ramification et soit* f *le degré résiduel. Alors,*

(i) L/K *est non-ramifiée si, et seulement si,* $\mathrm{d}_{\mathrm{L/K}} = \mathcal{O}_{\mathrm{K}}$ *;*

(ii) Si L/K *est totalement ramifiée et si* $f(X)$ *est le polynôme minimal de* π_L*, alors*

$$\mathrm{d}_{\mathrm{L/K}} = (\mathrm{N}_{\mathrm{L/K}}(f'(\pi_L))) \ ;$$

(iii) L'idéal $(\pi_{\mathrm{K}}^{f(e-1)})$ *divise* $\mathrm{d}_{\mathrm{L/K}}$.

Démonstration. — (i) Soit L/K une extension non-ramifiée et soit $k_{\mathrm{L}} = k_{\mathrm{K}}(\bar{\alpha})$. Soit $\bar{f}(X)$ le polynôme minimal de $\bar{\alpha}$ et soit $f(X) \in \mathcal{O}_{\mathrm{K}}[X]$ un relèvement de $\bar{f}(X)$. Alors $\mathcal{O}_L = \mathcal{O}_{\mathrm{K}}[\alpha]$, où α est la racine de $f(X)$ au-dessus de $\bar{\alpha}$ (voir la proposition 6.5.4). Comme $\bar{f}'$ est séparable, on a $\bar{f}'(\bar{\alpha}) \neq 0$, d'où $v_{\mathrm{L}}(f'(\alpha)) = 0$. Donc, par l'exemple 1.3.6, on a :

$$\mathrm{d}_{\mathrm{L/K}} = (\mathrm{N}_{\mathrm{L/K}}(f'(\alpha)) = \mathcal{O}_{\mathrm{L}}.$$

Réciproquement, supposons que $\mathrm{d}_{\mathrm{L/K}} = \mathcal{O}_{\mathrm{L}}$. Soit $1, \theta, \ldots, \theta^{n-1}$ une base de $\mathcal{O}_{\mathrm{L}}$ sur $\mathcal{O}_{\mathrm{K}}$. Alors on a :

$$\mathrm{d}_{\mathrm{L/K}}(1, \cdots, \theta^{n-1}) \in \mathcal{O}_{\mathrm{K}}^{\times}.$$

Soit $\bar{\theta}^i = \theta^i \pmod{\pi_L}$. Alors $\bar{1}, \cdots, \bar{\theta}^{n-1}$ engendrent k_{L} sur k_{K} et on a

$$\mathrm{d}_{k_{\mathrm{L}}/k_{\mathrm{K}}}(\bar{1}, \cdots, \bar{\theta}^{n-1}) = \overline{\mathrm{d}_{\mathrm{L/K}}(1, \cdots, \theta^{n-1})} \neq 0.$$

On en déduit que $\bar{1}, \cdots, \bar{\theta}^{n-1}$ est une base de $k_{\mathrm{L}}/k_{\mathrm{K}}$ (voir le corollaire 1.2.7). Donc $k_{\mathrm{L}}/k_{\mathrm{K}}$ est une extension de degré n et L/K est non-ramifiée.
(ii) Si L/K est totalement ramifiée, par le théorème 6.6.5 on a $\mathcal{O}_L = \mathcal{O}_{\mathrm{K}}[\pi_L]$, d'où

$$\mathrm{d}_{\mathrm{L/K}} = (\mathrm{N}_{\mathrm{L/K}}(f'(\pi_L))).$$

(iii) Soit L_0 la sous-extension de L/K satisfaisant les conditions du théoreme 6.6.6. D'après la proposition 6.7.3, il vient :

$$\mathrm{d}_{\mathrm{M/K}} = (\mathrm{N}_{\mathrm{K}_0/\mathrm{K}}(\mathrm{d}_{\mathrm{L/L}_0})).$$

Soit $f = \mathrm{Irr}(\pi_{\mathrm{L}}, \mathrm{L}_0) = X^e + a_{e-1}X^{e-1} + \cdots + a_0$. C'est un polynôme d'Eisenstein. En particulier, $v_{\mathrm{L}}(a_i) \geq e$, par conséquent

$$v_{\mathrm{L}}(f'(\pi_{\mathrm{L}})) \geq \min_i\{v_{\mathrm{L}}(e\pi_{\mathrm{L}}^{e-1}), \mathrm{v}_{\mathrm{L}}(ia_i\pi_{\mathrm{L}}^{i-1})\} \geq e-1.$$

Par unicité du prolongement des valuations, on a pour tout $g \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \overline{\mathrm{K}})$ et tout $x \in \mathrm{L}$:

$$v_{\mathrm{L}}(g(x)) = v_{\mathrm{L}}(x).$$

Ainsi

$$v_{\mathrm{L}_0}(\mathrm{N}_{\mathrm{L/L}_0}(f'(\pi_{\mathrm{L}}))) \geq \frac{e(e-1)}{e} = e-1,$$

i.e.

$$v_{\mathrm{L}_0}(\mathrm{d}_{\mathrm{L/L}_0}) \geq e-1.$$

En prenant la norme dans $\mathrm{L/L}_0$, on obtient au final

$$v_{\mathrm{K}}(\mathrm{N}_{\mathrm{L}_0/\mathrm{K}}(\mathrm{d}_{\mathrm{L/L}_0})) \geq f(e-1).$$

□

Exemple 6.7.5. — • Soit $p > 2$. Sur $\mathbb{Q}_p$, on connaît les extenstions quadratiques totalement ramifiées : $\mathbb{Q}_p(\sqrt{p})$ et $\mathbb{Q}_p(\sqrt{pa})$ pour $a \in \mathbb{Z}$, $a \notin \mathbb{F}_p^2$.
Ensuite, $\mathrm{Irr}(\sqrt{p}, \mathbb{Q}_p) = X^2 - p$ qui est un polynôme d'Eisenstein. Ainsi, pour $\mathrm{K} = \mathbb{Q}_p(\sqrt{p})$, il vient $\mathcal{O}_{\mathrm{K}} = \mathbb{Z}_p[\sqrt{p}]$ et par conséquent

$$\mathrm{d}_{\mathrm{K}/\mathbb{Q}_p} = \big(\mathrm{N}_{\mathrm{K}/\mathbb{Q}_p}(2\sqrt{p})\big)\mathbb{Z}_p = p\mathbb{Z}_p.$$

Idem, pour $\mathrm{F} = \mathbb{Q}_p(\sqrt{ap})$, il vient $\mathrm{d}_{\mathrm{F}/\mathbb{Q}_p} = p\mathbb{Z}_p$.

• Sur $\mathbb{Q}_2$ on connaît les extensions quadratiques totalement ramifiées : ce sont celles différentes de $\mathbb{Q}_2(\sqrt{5})$.
Prenons le corps $\mathrm{K} = \mathbb{Q}_2(\sqrt{2})$. On a $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}_2) = X^2 - 2$ qui est un polynôme d'Eisenstein. Ainsi, $\mathcal{O}_\mathrm{K} = \mathbb{Z}_2[\sqrt{2}]$ et

$$\mathrm{d}_{\mathrm{K}/\mathbb{Q}_2} = \big(\mathrm{N}_{\mathrm{K}/\mathbb{Q}_2}(2\sqrt{2})\big)\mathbb{Z}_2 = 8\mathbb{Z}_2.$$

Prenons le corps $\mathrm{F} = \mathbb{Q}_2(\sqrt{-1})$. On note que $\mathrm{F} = \mathbb{Q}_2(\alpha)$, où α est une racine de X^2+2X+2 qui est un polynôme d'Eisenstein. Ainsi $\mathcal{O}_\mathrm{F} = \mathbb{Z}_2[\alpha]$ et

$$\mathrm{d}_{\mathrm{F}/\mathbb{Q}_2} = \Big(\mathrm{N}_{\mathrm{F}/\mathbb{Q}_2}\big(2(\alpha+1)\big)\Big)\mathbb{Z}_2 = 4\mathbb{Z}_2.$$

Exemple 6.7.6. — Soit K un corps local de corps résiduel ℓ. Soit $p \neq \ell$ un second nombre premier tel que $\mu_p \subset \mathrm{K}$. Soit $\varepsilon \in \mathcal{O}_\mathrm{K}^\times$. Alors l'extension $\mathrm{K}(\sqrt[p]{\varepsilon})/\mathrm{K}$ est non ramifiée (éventuellement triviale).
En effet, posons $x = \sqrt[p]{\varepsilon}$) ; c'est clairement une unité. Alors

$$\mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}(P'(x)) = \mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}(px^{p-1}) \in \mathcal{O}_\mathrm{K}^\times,$$

car px^{p-1} est une unité. On conclut avec le théorème 6.7.4.

Exemple 6.7.7. — Soit p un nombre premier (pair ou impair) et soit $\mathrm{K} = \mathbb{Q}_p(\zeta_p)$, où ζ_p est une racine primitive p-ème de l'unité. Posons $z = 1 - \zeta_p$. On rappelle que $\mathrm{K}/\mathbb{Q}_p$ est une extension de degré $p-1$ et que $\mathcal{O} := \mathcal{O}_\mathrm{K} = \mathbb{Z}_p[\zeta_p]$ (ce sont les mêmes arguments que pour $\mathbb{Q}$, voir section §1.3.4).
Soit $\alpha \in \mathcal{O}^\times$ tel que $\alpha = \beta^p + z^{kp}\gamma$, avec $k \geq 1$, et $\beta, \gamma \in \mathcal{O}^\times$. Alors l'extension galoisienne $\mathrm{K}(\sqrt[p]{\alpha})/\mathrm{K}$, éventuellement triviale, est non ramifiée.
En effet, posons $x = \dfrac{\sqrt[p]{\alpha} - \beta}{z}$. Clairement $\mathrm{K}(\sqrt[p]{\alpha}) = \mathrm{K}(x)$. De plus x est racine du polynôme

$$P(X) = \frac{(zX+\beta)^p - \alpha}{z^p}$$

Comme $p = z^{p-1}u$, avec $u \in \mathcal{O}^\times$, il vient immédiatement :

(i) $P \in \mathcal{O}[X]$ et est unitaire, et donc $x \in \mathcal{O}$,

(ii) P' a pour coefficient constant $\dfrac{p\beta^{p-1}}{z^{p-1}} \in \mathcal{O}_{\mathrm{K}(x)}^\times$, ce qui implique $\mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}(P'(x)) \in \mathcal{O}^\times$.

Comme $\mathrm{d}_{\mathrm{K}(x)/\mathrm{K}}$ divise $\mathrm{N}_{\mathrm{K}(x)/\mathrm{K}}(P'(x))\mathcal{O}$, on en déduit que $\mathrm{d}_{\mathrm{K}(x)/\mathrm{K}} = \mathcal{O}$ et on conclut avec le théorème 6.7.4.

CHAPITRE 7

L'ÉQUATION DE FERMAT

L'objectif de ce chapitre est l'étude de l'équation diophantienne de Fermat $X^n + Y^n = Z^n$, avec $X, Y, Z \in \mathbb{Z}$, et où $n \geq 2$ est fixé.
Mais avant de regarder ce cadre, nous allons regarder les solutions de cette équation lorsque les inconnues sont dans l'anneau $\mathbb{C}[x]$. Nous verrons alors les ingrédients utiles pour le cas entier.

7.1. Le théorème de Fermat pour les polynômes

Soit $A = \mathbb{C}[t]$ l'anneau des polynômes à coefficients dans $\mathbb{C}$. On rappelle que A est un anneau euclidien donc principal (et factoriel). Commençons par la proposition suivante.

Proposition 7.1.1. — *Les solutions de l'équation diophantienne $X^2 + Y^2 = Z^2$ d'inconnues $X, Y, Z \in A$ sont de la forme (au signe près)*

$$X = 2UVW,\ Y = W(U^2 - V^2),\ Z = W(U^2 + V^2),$$

où $U, V, W \in A$.

Remarque 7.1.2. — On peut observer qu'un triplet X, Y, Z comme dans la proposition 7.1.1 vérifie la relation $X^2 + Y^2 = Z^2$.

Démonstration. — Soit $X, Y \in A$, $XY \neq 0$ tels que $X^2 + Y^2$ est un carré Z^2. Soit W le pgcd de X et Y. On voit alors que W divise Z^2. En divisant alors l'équation $X^2 + Y^2 = Z^2$ par W, on peut supposer X et Y premiers entre eux. On écrit ensuite $Z^2 - Y^2 = (Z - Y)(Z + Y) = X^2$.

Soit D le pgcd de $Z-Y$ et de $Z+Y$. Alors D divise $Z-Y+Z+Y=2Z$ mais aussi, $Z-Y-(Z+Y)=-2Y$. Comme Z et Y sont premiers entre eux, cela implique que $D=1$.
Mais alors l'équation $(Z-Y)(Z+Y)=X^2$ indique que $Z-Y=a_0U_0^2$ et $Z+Y=b_0V_0^2$, avec $a_0,b_0\in A^\times$ et U_0 et $V_0\in A$; ici on utilise le fait que l'anneau A est factoriel. Or $A^\times=\mathbb{C}^\times$ et ainsi $a_0=a^2$ et $b_0=b^2$ dans $\mathbb{C}$. En posant $U_1=aV_0$ et $V_1=bV_0$, on obtient $Z-Y=U_1^2$ et $Z+Y=V_1^2$, ou encore $Z=U^2-V^2$, $Y=U^2+V^2$, avec $U=\frac{1}{\sqrt{2}}U_1$ et $V=\frac{1}{\sqrt{2}}V_1$. Enfin $X^2=(Z-Y)(Z+Y)=U_1^2V_1^2=4U^2V^2$, ou encore $Z=2UV$. □

Pour les puissances plus grandes que 2, nous avons le théorème suivant

Théorème 7.1.3. — *Soit $n\geq 3$. L'équation diophantienne $X^n+Y^n=Z^n$ n'a pas de solution dans $\mathbb{C}[x]$, avec $XYZ\notin\mathbb{C}$ et, X et Y premiers entre eux.*

Le théorème 7.1.3 est "le théorème de Fermat pour les polynômes".

Démonstration. — Soit X,Y,Z une solution non triviale de l'équation diophantienne étudiée, avec X et Y premiers entre eux.
On suppose que c'est une solution minimale dans le sens où $d=\max\{\deg(X),\deg(Y),\deg(Z)\}$ est minimal.
Notons par $\zeta=\exp(2i\pi/n)$ puis écrivons

$$(Z-Y)(Z-\zeta Y)(Z-\zeta^2Y)\prod_{i=3}^{n}(Z-\zeta^iY)=Z^n-Y^n=X^n.$$

Comme pour le cas $n=2$, on peut alors remarquer que les polynômes $Z-\zeta^iY$ et $Z-\zeta^jY$ sont premiers entre eux (pour $i\neq j(\mathrm{mod}\ n)$). Comme l'anneau A est factoriel, cela implique que chaque facteur $Z-\zeta^iY$ est une puissance n-ème (là aussi, comme pour le cas $n=2$, on peut utiliser le fait que $\mathbb{C}=\mathbb{C}^n$). En regardant les coefficients dominants des polynômes Y et Z, on remarque alors que les polynômes $Z-\zeta^iY$ sont tous de même degré m, à l'exception peut-être d'un des $Z-\zeta^jY$ qui sera de degré plus petit que $m-1$. Quoiqu'il en soit, en regardant les degrés il vient $(n-1)m\leq nd$, d'où $m\leq d+1/(n-1)$.
Ensuite on écrit $Z-Y=U^n$, $Z-\zeta Y=V^n$ et $Z-\zeta^2Y=W^n$. Les polynômes U,V,W sont deux à deux premiers entre eux et de degré plus petit que $d/n+1/(n^2-n)$ et donc plus petit que $d/2$.

En isolant Z, on obtient ensuite $XZ = Y + U^n$, $Y(1-\zeta) = V^n - U^n$ puis $Y(1-\zeta^2) = W^n - U^n$. On a alors $(1+\zeta)(V^n - U^n) = W^n - U^n$, ou encore $(1+\zeta)V^n + W^n = \zeta U^n$. Enfin, en rentrant $1+\zeta$ et ζ dans la puissance $n$ème, on obtient donc une nouvelle solution de l'équation diophantienne initiale, plus précisément $X_1, Y_1, Z_1 \in A$ vérifiant $X_1^n + Y_1^n = Z_1^n$. Comme $n \geq 3$, on a $1 + \zeta \neq 0$, la nouvelle solution n'est pas triviale (avec X_1, Y_1 premiers entre eux) : les polynômes X_1, Y_1, Z_1 sont respectivement de même degré que les polynômes U, V, W et donc de degré au plus $d/2$. Par minimalité de d, on aboutit alorsà une contradiction. □

Pour conclure cette partie, observons que si l'on s'autorise les dérivations, le théorème 7.1.3 se déduit immédiatement du théorème suivant

***Théorème 7.1.4* (Mason).** — *Soit trois polynômes non nuls A, B, C, avec A et B premiers entre eux tels que $A + B = C$. Notons par $n_0 = \#\{z \in \mathbb{C}, A(z)B(z)C(z) = 0\}$. Alors*

$$\max\{\deg A, \deg B, \deg C\} \leq n_0 - 1.$$

Remarque 7.1.5. — Le théorème de Mason est aussi appelé conjecture ABC pour les polynômes.

Montrons que le théorème 7.1.4 implique le théorème de Fermat dans $\mathbb{C}[t]$. Partons d'une solution $X^n + Y^n = Z^n$, avec $X, Y \in \mathbb{C}[t]$ premiers entre eux. Supposons par exemple que X est le polynôme de plus haut degré $d > 0$. On applique le théorème de Mason à $A = X^n$, $B = Y^n$ et $C = Z^n$ pour obtenir

$$nd < 3d - 1,$$

d'où une contradiction pour $n \geq 3$.
Montrons donc le théorème de Mason.

Démonstration. — Soit le polynôme $N_0 = \prod_{z \in S}(t - z)$, où $S = \{z \in \mathbb{C}, ABC(z) = 0\}$; ainsi $n_0 = \deg(N_0)$.
Posons $F = A/C$ et $G = B/C$. Alors $F' = -G'$, d'où la relation

$$A/B = F/G = -\frac{G'/G}{F'/F} = -\frac{(\log G)'}{(\log F)'} = -\frac{B'/B - C'/C}{A'/A - C'/C}.$$

Rappelons maintenant que pour un polynôme $Q = \prod_i (t-\alpha_i)^{n_i}$, il vient (en prenant sa dérivée logarithmique)

$$Q'/Q = n_i \sum_i \frac{1}{t-\alpha_i}.$$

On note alors que N_0A'/A, N_0B'/B et N_0C'/C sont des polynômes de degré strictement plus petit que celui de N_0, c'est à dire strictement plus petit que n_0. Ainsi de

$$A/B = -\frac{N_0(B'/B - C'/C)}{N_0(A'/A - C'/C)},$$

et du fait que A et B sont premiers entre eux, il vient que A divise le numérateur de la fraction de droite et que B divise son dénominateur (la fraction n'est peut être pas réduite) et ainsi, $\max\{\deg(A), \deg(B), \deg(C)\} \leq n_0 - 1$. □

7.2. L'équation de Fermat pour $n = 2$ et $n = 4$

Cette fois-ci, on se place dans l'anneau $A = \mathbb{Z}$.

7.2.1. Le cas $n = 2$. — En reproduisant la preuve pour le cas des poylynômes, nous allons déjà montrer la proposition suivante

Proposition 7.2.1. — *Les solutions de l'équation diophantienne $X^2 + Y^2 = Z^2$ d'inconnues $X, Y, Z \in Z$ sont toutes de la forme (à l'ordre près entre X et Y)*

$$X = \pm 2UW,\ Y = \pm W(U^2 - V^2),\ Z = \pm W(U^2 + V^2),$$

où $U, V, W \in \mathbb{Z}$, U impair et V pair.

Démonstration. — Tout d'abord, on remarque que les entiers de la forme de la proposition 7.2.1 vérifient bien la relation $X^2 + Y^2 = Z^2$.
Réciproquement, comme pour les polynômes on part d'une solution $X^2 + Y^2 = Z^2$ avec X et Y premiers entre eux. On suppose $X, Y, Z > 0$.
Observons que si X est impair (resp. pair) alors Y est pair (resp. impair) et Z est toujours impair (X et Y ne peuvent pas être simultanément pairs ou impairs, pour ce dernier point, la contradiction arrive modulo $4\mathbb{Z}$).

Supposons par exemple X pair. On écrit alors

$$(Z-Y)(Z+Y)=X^2$$

puis l'on étudie le pgcd d de $Z-Y$ et $Z+Y$. Alors d divise $2Z$ et $2Y$, et donc nécessairement $d=2$ (on observe que 2 divise bien $Z-Y$ et $Z+Y$). On écrit alors $Z-Y=2U_1$ et $Z+Y=2V_1$, avec U_1 et V_1 premiers entre eux. Comme $\mathbb{Z}$ est principal (donc factoriel), on en déduit que $U_1=U^2$ et $V_1=V^2$. Par conséquent, $Z=U^2+V^2$ et $Y=V^2-U^2$, puis $X=2UV$. □

7.2.2. Le cas $n=4$. — La proposition 7.2.1 nous permet d'obtenir le théorème suivant.

Théorème 7.2.2. — *L'équation $(E): X^4+Y^4=Z^4$ n'a pas de solution entière non triviale.*

Comme pour les polynômes, nous allons utiliser la méthode de *la descente infinie*. En fait nous allons montrer la proposition suivante qui entraîne le théorème.

Proposition 7.2.3. — *L'équation $X^4+Y^4=Z^2$ n'a pas de solution entière non triviale.*

Démonstration. — Soit $X,Y,Z\geq 0$ un triplet non trivial solution de (E) qui est telle que Z est minimal. Avec la proposition 7.2.1, on écrit $X^2=2UV, Y^2=U^2-V^2$ et $Z=U^2+V^2$, avec U et V premiers entre eux. Immédiatement on voit que U est impair et V est pair (en regardant Y^2 modulo $4\mathbb{Z}$). On pose alors $V=2V_0$, et il vient $X^2=2UV=4UV_0$. Ainsi, comme $\mathbb{Z}$ est factoriel, on obtient $U=a^2$ et $V_0=b^2$, pour certains entiers a,b. Ainsi $4b^4+Y^2=a^4$. On applique à nouveau la proposition 7.2.1, pour obtenir

$$Y=\alpha^2-\beta^2,\ 2b^2=2\alpha\beta,\ a^2=\alpha^2+\beta^2,$$

où $\alpha,\beta\in\mathbb{N}$. Il est immédiat de voir que α et β sont premiers entre eux. L'égalité $b^2=\alpha\beta$ indique que α et β sont deux carrés α_0^2 et β_0^2. D'où $a^2=\alpha_0^4+\beta_0^4$. Or $Z=U^2+V^2=a^4+4b^4>a^4\geq a$: on a donc trouver une solution de l'équation initiale avec le terme de droite au carré strictement plus petit que Z. Contradiction. □

7.3. Le théorème de Fermat

Rappelons l'énoncé de la question posée et déclarée comme résolue par Fermat.

Soit $n \geq 3$. Alors l'équation diophantienne $X^n + Y^n = Z^n$ n'a pas de solution entière non triviale.

On dit qu'un triplet X, Y, Z est une solution entière triviale si $XYZ = 0$.

Avec le théorème 7.2.2, l'étude du théorème de Fermat équivaut à montrer que pour tout nombre premier $p \geq 3$, *l'équation $X^p + Y^p = Z^p$ n'a pas de solution non triviale*. C'est la réduction classique que nous allons donc faire.
Nous allons montrer le résultat suivant

Théorème 7.3.1. — *Soit le nombre premier $p \geq 3$ tel que p ne divise pas l'ordre du groupe des classes de $\mathbb{Q}(\zeta_p)$. Alors l'équation $X^p + Y^p + Z^p$ n'a pas de solution entière non triviale.*

Nous discuterons ultérieurement de la condition de divisibilité. Si l'on veut suivre la preuve du théorème de Fermat pour les polynômes, l'étude des corps cyclotomiques montrent qu'il est nécessaire de dépasser le cadre où $\mathbb{Z}[\zeta_p]$ est principal. En effet, comme nous l'avons indiqué dans la section 3.4.2 du chapitre 3, l'ordre du groupe des classes de $\mathbb{Q}(\zeta_p)$ grandit avec p. En particulier $\mathbb{Z}[\zeta_p]$ est principal si et seulement si, $p \in \{3, 5, 7, 11, 13, 17, 19\}$.
Nous allons considérer, suivant que l'on parte d'une solution X, Y, Z telle que $p | XYZ$ ou non.
Si $p \nmid XYZ$, on parle du premier cas du théorème de Fermat ; du second cas sinon.

7.3.1. Le premier cas. — On va montrer le théorème 7.3.1 dans le premier cas. Soit $p \geq 3$. Partons d'une solution non triviale $X^p + Y^p = Z^p$ avec $p \nmid XYZ$ et $(X, Y) = 1$. On va montrer alors que l'on aboutit à une contradiction.

Remarquons tout d'abord que dans certains cas, cette contradiction se voit dès l'étude modulo p de la solution.

Par exemple prenons $p = 3$ et regardons l'équation $X^3+Y^3 = Z^3 (\text{mod } 3)$. Clairement, il est nécessaire d'avoir $X \equiv Y (\text{mod } 3)$. Alors si $X \equiv Y \equiv 1(\text{mod } 3)$, il vient $Z \equiv -1(\text{mod } 3)$. Mais dans ce cas, $X^3 \equiv Y^3 \equiv 1(\text{mod } 9)$, $Z^3 \equiv -1(\text{mod } 9)$ et donc $Z^3 \neq X^3+Y^3$. Le même raisonnement exclut aussi le cas où $X \equiv Y \equiv -1(\text{mod } 3)$.
Nous venons donc de montrer que l'équation $X^3 + Y^3 = Z^3$ n'a pas de solution (avec $3 \nmid XYZ$) dans $\mathbb{Z}/9\mathbb{Z}$.
Un raisonnement similaire marche pour $p = 5$. Cependant cette méthode est très limitée comme le montre la proposition suivante :

Proposition 7.3.2. — *Soit p un nombre premier congru à 1 modulo 3. Alors pour tout entier $k \geq 1$, l'équation $X^p + Y^p = Z^p$ a une solution dans $\mathbb{Z}/p^k\mathbb{Z}$, avec $p \nmid XYZ$.*

Démonstration. — Comme $3|p - 1$, l'anneau $\mathbb{Z}_p$ contient les racines d'ordre 3. Soit α une racine primitive d'ordre 3. Comme $\alpha \in \mathbb{Z}_p^\times$, on a donc $\alpha \neq 0(\text{mod } 3)$. On observe ensuite que $\alpha^p = \alpha$ et ainsi il vient la relation dans $\mathbb{Z}_p$:

$$1 + \alpha^p + (\alpha^2)^p = 0.$$

Il suffit alors de la regarder modulo p^n. □

Passons à la preuve du théorème 7.3.1. Revenons donc à une solution (X, Y, Z) non triviale de l'équation de Fermat, avec $(X, Y) = 1$, et vérfiant $X^p - Y^p = Z^p$.

Faisons alors une première réduction (qui apparaît déjà pour $p = 3$ plus haut) : on suppose que $X \not\equiv 1(\text{mod } p)$. En effet sinon, il vient $X^p + Y^p \equiv 0(\text{mod } p)$ impliquant que $p|Z$, ce qui est à exclure.

On factorise ensuite l'équation factorise dans $\mathbb{Z}[\zeta]$ de la façon suivante, où $\zeta = \zeta_p$:

$$(X - Y)(X - \zeta Y) \cdots (X - \zeta^{p-1}Y) = Z^p. \tag{7}$$

Le calcul a donc lieu dans l'anneau des entiers $\mathcal{O} := \mathbb{Z}[\zeta]$ de $\mathbb{Q}(\zeta)$.
On a alors un premier lemme

Lemme 7.3.3. — *Pour $i = 0, \cdots, p-1$, les idéaux principaux $(X - \zeta^i)$ de $\mathcal{O}$ sont deux à deux premiers entre eux.*

Démonstration. — Soit $\mathfrak{p} \subset \mathcal{O}$ un idéal maximal de $\mathcal{O}$ divisant $X - \zeta^i Y$ et $X - \zeta^j Y$ pour $i \neq j \in \{0, \cdots, p-1\}$. Alors $\mathfrak{p}$ divise $\zeta^i Y(1 - \zeta^{j-i})$ et $\mathfrak{p}$ divise aussi $\zeta^{-i} X(1 - \zeta^{i-j})$. Or comme $(X, Y) = 1$, et comme pour $a \neq 0 (\text{mod } p)$, on a $(1 - \zeta^a) = (1 - \zeta)$, il vient que nécessairement $\mathfrak{p} = (1-\zeta)$, l'unique idéal maximal de $\mathcal{O}$ au-dessus de p. Par conséquent, $\mathfrak{p}$ divise Z^p, impliquant que $p | Z^p$, ce qui contredit l'hypothèse $p \nmid XYZ$. □

Retournons alors à l'égalité (7). Tout d'abord, elle implique, grâce au lemme 7.3.3, que les idéaux principaux $(X - \zeta Y)$ sont des puissances p-èmes d'idéaux entiers : pour $i = 0, \cdots, p-1$, il existe un idéal $C_i \subset \mathcal{O}$ tel que $C_i^p = (X - \zeta Y)$. Cela signifie que dans le groupe des classes Cl de K, la classe de C_i est d'ordre p. Or par hypothèse, $p \nmid |\text{Cl}|$, on en déduit alors que C_i est principal. Il existe ainsi $\alpha_i \in \mathcal{O}$ tel que $C_i = (\alpha_i)$. Par conséquent $(\alpha_i^p) = (X - \zeta^i Y)$: il existe une unité $\varepsilon_i \in \mathcal{O}^\times$ telle que

$$X - \zeta^i Y = \varepsilon_i \alpha_i^p.$$

On se concentre sur le cas $i = 1$, et on écrit

$$X - \zeta Y = \varepsilon \alpha^p \tag{8}$$

pour une certaine unité ε de $\mathcal{O}$ et $a \in \mathcal{O}$.
Pour l'étape suivante, il est nécessaire d'avoir un peu plus d'informations sur $\mathcal{O}^\times$. Pour cela on utilise le théorème 3.6.7 du chapitre 3 (théorème de Kronecker). Rappelons-le. Soit $\text{K}^+ = \text{K}(\zeta + \zeta^{-1})$ le sous-corps réel maximal de K. On rappelle que K/K^+ est une extension galoisienne de groupe de Galois engendré par la conjugaison complexe σ. Alors, il existe $k \in \{0, \cdots, p-1\}$ et $\eta \in \mathcal{O}_{\text{K}^+}^\times$ tels que $\varepsilon = \zeta^k \eta$.
Enfin, avant de finir les calculs et la preuve, énonçons un résultat assez immédiat :

Lemme 7.3.4. — *Soit $\alpha \in \mathcal{O}$. Alors il existe $a \in \mathbb{Z}$ tel que $\alpha^p \equiv a (\text{mod } p)$, dans $\mathcal{O}$.*

Démonstration. — C'est immédiat. On écrit $\alpha = \sum_{i=0}^{p-1} a_i \zeta^i$, avec $a_i \in \mathbb{Z}$ et ensuite, en développant α^p modulo p, on obtient $\alpha^p \equiv a_0^p + \cdots + a_{p-1}^p (\text{mod } p)$. □

Ainsi, l'équation (8) devient

$$X - \zeta Y \equiv \zeta^k \eta a \ (\text{mod } p). \tag{9}$$

On fait ensuite agir la conjugaison complexe σ sur l'équation (9) pour obtenir

$$X - \zeta^{-1} Y \equiv \zeta^{-k} \eta a \ (\text{mod } p). \tag{10}$$

Ainsi, les égalités (9) et (10) impliquent

$$\zeta^{2k} X - \zeta^{2k-1} Y - X + \zeta Y \equiv 0 (\text{mod } p). \tag{11}$$

Nous allons maintenant distinguer trois cas.
(i) Supposons que les éléments de la famille $\{1, \zeta, \zeta^{2k}, \zeta^{2k-1}\}$ sont deux à deux distincts. Alors la famille $\{1, \zeta, \zeta^{2k}, \zeta^{2k-1}\}$ qui forme une partie de la $\mathbb{Z}$-base $\{1, \zeta, \cdots, \zeta^{p-2}\}$ de $\mathcal{O}$ est $\mathbb{Z}$-libre. Par unicité de l'écriture de (11), on doit avoir $p|X$ et $p|Y$. Contradiction.

(ii) Peut-on alors avoir $1 = \zeta^{2k}$? Dans ce cas (11) devient $\zeta^{-1} Y + \zeta Y \equiv 0 (\text{mod } p)$, ce qui implique que $p|Y$, et on conclut comme précédemment à une absurdité.

(iii) Peut-on avoir $1 = \zeta^{2k-1}$? Dans ce cas (11) devient $\zeta X - Y - X + \zeta Y \equiv 0 (\text{mod } p)$, ce qui implique que p divise $X + Y$, et donc que $X \equiv -Y (\text{mod } p)$, ce qui est à exclure.

(iv) Peut-on avoir $\zeta = \zeta^{2k}$? Dans ce cas (11) devient $-\zeta^{-1} Y - \zeta Y \equiv 0 (\text{mod } p)$ ce qui implique que $p|Y$, d'où une absurdité.

(v) Peut-on avoir $\zeta = \zeta^{2k-1}$? Dans ce cas (11) devient $-\zeta^{-1} X - X \equiv 0 (\text{mod } p)$ ce qui implique que $p|X$, d'où une absurdité.

(vi) Peut-on avoir $\zeta 2k = \zeta^{2k-1}$? Dans ce cas $\zeta = 1$, d'où une absurdité.

Ce qui termine la preuve du théorème 7.3.1 du premier cas.

7.3.2. Le second cas. — On va montrer le théorème 7.3.1 dans le second cas. Soit $p \geq 3$. Partons d'une solution non triviale $X^p + Y^p = Z^p$ avec $p \nmid Z$ par exemple, et $(X, Y) = 1$. On va montrer alors que l'on aboutit à une contradiction. Remarquons que $p \nmid XY$.
Ecrivons $Z = p^m Z_0$, avec $p \nmid Z_0$, alors X, Y, Z_0 sont premiers entre eux et vérifient $X^p + Y^p = p^m Z_0$, avec $m \geq 1$. Le second cas se déduit alors du théorème suivant valable dans le corps $\mathrm{K} := \mathbb{Q}(\zeta)$, où ici $\zeta = \zeta_p$, d'anneau

des entiers $\mathcal{O}$. Posons $z = 1 - \zeta$. On rappelle que $(z) := \mathfrak{p}$ est l'unique idéal premier de $\mathcal{O}$ au-dessus de p.

Théorème 7.3.5. — *Dans le corps $\mathbb{Q}(\zeta_p)$ l'équation diophantienne $X^p + Y^p = uz^{pm}Z^p$ n'a pas de solution $X, Y, Z \in \mathcal{O}$, avec $u \in \mathcal{O}^\times$, $z \nmid XYZ$ et $m \geq 1$.*

Comme pour le ce premier cas, nous partons de la factorisation

$$(X - Y)(X - \zeta Y) \cdots (X - \zeta^{p-1}Y) = uz^{pm}Z^p. \tag{12}$$

Commençons par la proposition suivante

Proposition 7.3.6. — *Sous les conditions du théorème 7.3.5, si une telle solution existe alors nécessairement $m > 1$.*

Démonstration. — D'une part, comme $p = (z^{p-1})$ il vient donc que $\mathrm{v}_{\mathfrak{p}}(X - Y) = (p-1)\mathrm{v}_p(X - Y)$. D'autre part, l'action galoisienne de $G = \mathrm{Gal}(\mathrm{K}/\mathbb{Q}_p)$ nous indique que la valuation $\mathrm{v}_{\mathfrak{p}}(X - \zeta^i Y)$ est contante pour tout $i = 1, \cdots, p-1$ (car ici G agit trivialement sur $\mathfrak{p}$) ; posons $m_0 = \mathrm{v}_{\mathfrak{p}}(X - \zeta Y)$. Ainsi $pm = (p-1)(m_0 + \mathrm{v}_p(X - Y))$, par conséquent $p - 1$ divise m, donc $m \geq 2$. □

Partons alors maintenant d'une solution respectant les conditions du théorème 7.3.5 avec m *minimal*. Ainsi $m \geq 2$.

Tout d'abord, comme pour la preuve du lemme 7.3.3, on a $m_0 \leq 1$. Egalement, la preuve de la proposition 7.3.6 indique que p divise la quantié $m_0 + a$, où $a = \mathrm{v}_p(X - Y)$). Et ainsi, $a \geq p - 1 \geq 2$. Si l'on écrit ensuite $X - \zeta Y = X - Y + Y(1 - \zeta)$, il apparaît que $X - \zeta Y \in \mathfrak{p}$, d'où $m_0 = 1$, et ainsi $(p-1)a = p(m-1) + 1$.
Pour $i = 1, \cdots, p-1$, écrivons maintenant

$$(X - \zeta^i Y) = \mathfrak{p}C_i, \quad (X - Y) = \mathfrak{p}^{(p-1)a}C_0 = \mathfrak{p}^{p(m-1)+1}C_0 \tag{13}$$

avec C_i des idéaux entiers de $\mathcal{O}$; en particulier $\mathfrak{p} \nmid C_0 \cdots C_{p-1}$. Le raisonnement de la preuve du lemme 7.3.3 indique que les C_i sont deux à deux premiers entre eux. Ensuite de l'égalité

$$C_0 \cdots C_{p-1} = (uZ^p) = (Z)^p$$

on en déduit que pour chaque i, on a $C_i = D_i^p$, pour un certain idéal entier D_i.
Regardons maintenant tout ceci dans le groupe des classes Cl de K. De (13), la classe $\mathrm{Cl}(C_i)$ est triviale (car $\mathfrak{p} = (z)$) et donc $\mathrm{Cl}(D_i)^p = \mathrm{Cl}(D_i^p)$ est aussi triviale. Mais, sous l'hypothèse que p ne divise pas l'ordre du groupe des classes de K, on en déduit que la classe $\mathrm{Cl}(D_i)$ est triviale dans Cl, c'est à dire que D_i est principal. Ecrivons $C_i = (\alpha_i)$, avec $\alpha_i \in \mathcal{O}$; ainsi $C_i = (\alpha_i^p)$. Observons que $\mathfrak{p}$ ne divise aucun idéal principal (α_i).
Comme pour le premier cas, regardons les conséquences pour les trois premiers éléments de la factorisation (12) : il existe $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \mathcal{O}^\times$ tel que

$$X - Y = \varepsilon_0 z^{p(m-1)+1} \alpha_0^p,\ X - \zeta Y = \varepsilon_1 z \alpha_1^p,\ X - \zeta^2 Y = \varepsilon_2 z \alpha_2^p.$$

En substituant, on obtient alors l'identié

$$e_1 \alpha_1^p + \alpha_2^p = e z^{p(m-1)} \alpha_0^p, \tag{14}$$

avec $e_1 = (1+\zeta)\varepsilon_2^{-1}\varepsilon_1 \in \mathcal{O}^\times$ (remarquer que $(1+\zeta) = (1-\zeta^2)/(1-\zeta)$ et est donc de valuation nulle en tous les idéaux premiers) et $e = \zeta\varepsilon_0\varepsilon_2^{-1} \in \mathcal{O}^\times$.

Proposition 7.3.7. — *Soit une unité e_1 comme dans l'équation (14). Alors l'extension $\mathrm{K}(\sqrt[p]{e_1})/\mathrm{K}$ est non-ramifiée en tous les idéaux premiers de $\mathcal{O}$.*

Remarque 7.3.8. — Observons que l'extension $\mathrm{K}(\sqrt[p]{e_1})/\mathrm{K}$ est galoisienne de groupe de Galois soit triviale soit cyclique de degré p.

Démonstration. — Il faut vérifier que pour tout idéal premier $\mathfrak{p} \subset \mathcal{O}_\mathrm{K}$, l'extension locale $\mathrm{K}_\mathfrak{q}(\sqrt[p]{e_1})/\mathrm{K}_\mathfrak{q}$ est non-ramifée (on la suppose non triviale) : l'exemple 6.7.7 traite du cas où $\mathfrak{q} = \mathfrak{p}$ et l'exemple 6.7.6 du cas où $\mathfrak{q} \neq \mathfrak{p}$. □

L'étape suivante est alors cruciale, elle est conséquence de la *théorie du corps de classes*. Les extensions *abéliennes et non ramifiées* (en tous les idéaux premiers de $\mathcal{O}_\mathrm{K}$) d'un corps de nombres K sont décrites par son groupe des classes. En particulier, quand p ne divise pas $|\mathrm{Cl}|$, il n'existe pas d'extension cyclique de degré p de K non ramifiée partout.

Revenons à notre problème, la condition sur le groupe des classes de $\mathbb{Q}(\zeta_p)$ implique alors $e_2 \in \mathrm{K}^p \cap \times\mathcal{O}^\times = \mathcal{O}^{\times p}$. Remarquons que l'on a utilisé à nouveau l'hypothèse sur le groupe des classes.
Par conséquent, dans la relation (14) on peut rentrer e_1 dans α_1^p, ce qui implique que l'équation diophantienne du théorème 7.3.5 a une solution si l'on remplace m par $m-1 \geq 1$, ce qui contredit la la minimalité de m. Ceci achève la preuve du théorème 7.3.1.

7.3.3. Commentaires. — On peut se poser la question sur l'hypothèse "p ne divise pas l'ordre du groupe des classes de $\mathbb{Q}(\zeta_p)$".

Définition 7.3.9. — Un nombre premier p est dit régulier si p ne divise pas l'ordre du groupe des classes de $\mathbb{Q}(\zeta_p)$. Il est dit irrégulier sinon.

Le calcul exact du groupe de $\mathbb{Q}(\zeta_p)$ est quelque chose d'inatteignable dès que p assez grand, mais par contre nous avons le critère suivant conséquence d'un résultat de Kummer (~ 1850) reliant la question de la régularité d'un nombre p au numérateur de certains nombres de Bernoulli. On rappelle que les nombres de Bernoulli B_n sont les coefficients qui apparaîssent dans le développement en série entière de $x/(\exp(x)-1)$ de la façon suivante :

$$\frac{x}{\exp(x)-1} = \sum_{n\geq 0} B_n \frac{x^n}{n!}.$$

On dit qu'un nombre premier ℓ divise B_n si ℓ divise le numérator de B_n (après réduction).

***Théorème 7.3.10* (Kummer)**. — *Le nombre premier p est régulier si et seulement si, p ne divise aucun des B_i, pour $i \in \{2, \cdots, p-3\}$ impair.*

Exemple 7.3.11. — Les nombres premiers $p = 37, 59, 67$ sont les seuls irréguliers plus petits que 100.

On sait qu'il y a une infinité de premiers irréguliers, mais le problème est ouvert pour les premiers réguliers. On suspecte une répartition environ $60-40$ en faveur des premiers réguliers. Précisons à ce niveau que le résultat de Kummer a été affiné par Herbrand (1932) et Ribet (1976).

On définit l'indice de régularité $i(p)$ du nombre premier p, comme

$$i(p) = \#\{i \in \{2, \cdots, p-3\},\ B_i \equiv 0 (\text{mod } p)\}.$$

Remarquons que dans la preuve du premier cas, nous avons isolé trois classes. En fait, un raisonnement de cette nature mais plus fin, marche dès lors que l'indice de régularité est petit compararativement à p.

***Théorème 7.3.12* (Eichler).** — *Soit un nombre premier $p > 2$ tel que $i(p) < \sqrt{p} - 2$. Alors le premier cas du théorème de Fermat est vrai pour p.*

Exemple 7.3.13. — Le plus petit nombre premier p avec $i(p) \geq 2$ est $p = 157$. On a dans ce cas $i(157) = 2$ avec $B_{62} \equiv B_{110} (\text{mod } 157)$.

En fait, nous ne connaissons pas de nombres premiers avec $i(p) \geq 6$. On pense que $i(p) = O(\log(p)/\log(\log p))$.
Enfin donnons un critère performant et convainquant.

***Théorème 7.3.14* (Wieferich (1909), Mirimanoff (1910))**
Supposons le premier cas du théorème de Fermat en défaut pour le premier p. Alors p vérifie simultanément les deux congruences suivantes : $2^{p-1} \equiv 1 (\text{mod } p^2)$ et $3^{p-1} \equiv 1 (\text{mod } p^2)$.

Un nombre premier p qui vérifie la première condition est appelé un nombre premier de Wieferich. Il s'avère que jusqu'à $p \leq 4 \times 10^{12}$, nous n'avons que deux nombres premiers de Wieferich : $p = 1093$ et $p = 3511$. La seconde congruence est aussi pauvre en solution, puisque pour $p \leq 4 \times 310^9$, il n'y a que $p = 11$ et $p = 1006003$ vérifiant celle-ci.
Ainsi, des méthodes relativement élémentaires permettent de montrer que le premier cas du théorème de Fermat est vrai pour $p \leq 4 \times 10^{12}$.
Pour le second cas, les critères utilisent la structure galoisienne du groupe des classes. Tout d'abord notons par h_p^+ l'ordre du groupe des classes de $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. La conjecture de Vandiver stipule que $p \nmid h_p^+$.

Théorème 7.3.15. — *Soit p un nombre premier tel que*

(i) $p^3 \nmid B_{pi}$ pour tout $i \in \{2, \cdots, p-3\}$, et

(ii) $p \nmid h_p^+$.

Alors le second cas du théorème de Fermat est vérifié pour p.

D'autres critères de cette forme se lisant sur $\mathbb{Q}$ ont permis de montrer que le second cas du théorème de Fermat est vrai pour $p < 4 \times 10^6$ (travaux de Buhler et ses coauteurs en 1993).

CHAPITRE 8

EXERCICES - ANNALES

Exercice 1. — *Soit le corps fini* $\mathrm{K} = \mathbb{F}_q$ *et soit* $\mathrm{L} = \mathbb{F}_{q^d}$.
1) Déterminer $\mathrm{Gal(L/K)}$.
2) Ecrire l'expression de $\mathrm{N_{L/K}}x$ *et* $\mathrm{Tr_{L/K}}x$ *pour* $x \in \mathrm{L}$.
3) Montrer que pour tout y *dans* L, $\mathrm{Tr_{L/K}}(y^q - y) = 0$.
4) Considérons

$$\begin{array}{rccc} \phi : & \mathrm{L} & \to & \mathrm{L} \\ & y & \mapsto & y^q - y \end{array}$$

a) Montrer que ϕ *est un homomorphisme de groupes.*
b) Déterminer $\mathrm{Ker}(\phi)$ *; en déduire* $|\mathrm{Im}(\phi)|$.
c) Montrer que $\mathrm{Tr_{L/K}}$ *n'est pas l'application nulle.*
d) En déduire que $\mathrm{Im}(\phi) = \mathrm{Ker}(\mathrm{Tr_{L/K}})$, *puis que* $\mathrm{Tr_{L/K}}x = 0$ *si et seulement si, il existe* $y \in \mathrm{L}$ *tel que* $x = y^q - y$.

Exercice 2. — *Soient* $q = p^n$ *une puissance d'un nombre premier* p, *et* $m > 1$ *un entier. On pose* $\mathrm{K} = \mathbb{F}_q$ *et* $\mathrm{L} = \mathbb{F}_{q^m}$.
Montrer que l'application norme $\mathrm{N_{L/K}} : \mathrm{L} \to \mathrm{K}$ *est surjective.*

Exercice 3. — *Soit* $\mathrm{K} = k(X)$, *où* k *est un corps de caractéristique différente de* 2. *Soit* P *un polynôme irréductible de* K *et* $\alpha \in \overline{\mathrm{K}}$ *une racine de* $Y^2 - P \in K[Y]$ *;* $\mathrm{F} = \mathrm{K}(\alpha)$.
1) Montrer que F/K *est galoisienne.*
2) Déterminer la fermeture intégrale de $A = k[X]$ *dans* F.

Exercice 4. — *A quelle condition* $\dfrac{\sqrt{m}+\sqrt{n}}{4}$ *est-il entier (sur* $\mathbb{Z}$*) ? (*$m,\ n \in \mathbb{Z}$*)*

Exercice 5. — *Soit* j *une racine cubique de l'unité ;* $\mathrm{K} = \mathbb{Q}(j)$*. On considère* $\mathrm{L} = \mathbb{Q}(\sqrt[3]{2-3j})$*. Déterminer* $[\mathrm{L} : \mathrm{K}]$*.*

Exercice 6. —

Résoudre $X^2 = \dfrac{4}{5} + \dfrac{3}{2}i$ dans $\mathbb{Q}(i)$.

Exercice 7. —

Soit α un nombre algébrique, racine d'un polynôme P à coefficients dans $\mathbb{Z}$:

$$P(X) = a_0X^n + \cdots + a_{n-1}X + a_n$$

avec $(a_0, \cdots, a_n) = 1$.
1) Montrer que $a_0\alpha$ est un entier algébrique.
2) Soi $d \geq 1$ le plus petit entier naturel tel que $d\alpha$ soit un entier algébrique. Montrer que d divise a_0.
3) On suppose P irréductible. Montrer que tout facteur premier de a_0 divise d.

Exercice 8. — *Soit* $P = X^3 - X - 1$*, et* θ *une racine* P *;* $\mathrm{K} = \mathbb{Q}(\theta)$*. Montrer que* $\{1, \theta, \theta^2\}$ *est une* $\mathbb{Z}$*-base de l'anneau des entiers de* K*.*

Exercice 9. — *Soit* $P = X^n + a_{n-1}X^{n-1} + \cdots + a_X + a_0$ *un polynôme d'Eisenstein et soit* $\theta \in \mathbb{C}$ *une racine de* P*. Soit le corps de nombres* $\mathrm{K} = \mathbb{Q}(\theta)$*. Considérons* $A = \mathbb{Z}[\theta] \subset \mathcal{O}_\mathrm{K}$*.*
1) Montrer que $[\mathcal{O}_\mathrm{K} : A]$ *est fini.*
2) Soit $x = b_0 + \cdots + b_k\theta^k \in A$ *avec* $k \leq n-1$*. En considérant la matrice de la multiplication* m_x *par* x*, montrer que* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(b_0) \equiv a_0 (\mathrm{mod}\ p)$*.*
3) En déduire que l'indice $[\mathcal{O}_\mathrm{K} : A]$ *est premier à* p*.*
4) Soit p *un nombre premier. Déterminer l'anneau des entiers de* $\mathbb{Q}(\sqrt[p]{p})$*.*

Exercice 10. — *Trouver une base d'entiers de* $\mathbb{Q}(\sqrt[3]{5})$*.*

Exercice 11. — *Soit* $P = X^3 + X^2 - 2X + 8$*, et* θ *une racine* P *;* $\mathrm{K} = \mathbb{Q}(\theta)$*.*
1) Calculer le discriminant $d(1, \theta, \theta^2)$*.*
2) On considère $\beta = 4/\alpha$*.*
a) Montrer que β *est un entier algébrique.*
b) Montrer que $\{1, \theta, \beta\}$ *forme une* $\mathbb{Q}$*-base de* K*.*
3) Montrer que $\{1, \theta, \beta\}$ *est une base d'entiers de* K *(i.e. une* $\mathbb{Z}$*-base de l'anneau des entiers de* K*).*

Exercice 12. — *On désire trouver une base d'entiers de* $\mathbb{Q}(\sqrt{2}, i)$*. Soit* $A = \{1, i, \sqrt{2}, i\sqrt{2}\}$*.*
1) Calculer $\mathrm{d}(1, i, \sqrt{2}, i\sqrt{2})$*. Conclusion ?*
2) Montrer que $\dfrac{\sqrt{2}}{2}(i+1)$ *est entier.*
3) En déduire une base d'entiers de $\mathbb{Q}(\sqrt{2}, i)$*.*

Exercice 13. — *Soit un nombe premier* $p \geq 3$*. Montrer que le discriminant du corps* $\mathbb{Q}(\zeta_p)^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ *a pour valeur* $p^{(p-1)/3}$*.*

Exercice 14. — *Soit* x *un entier algébrique tel que pour tout conjugué* x_i *de* x*,* $|x_i| \leq 1$*. Montrer alors que* x *est une racine de l'unité. (C'est un résultat connu sous le nom de théorème de Kronecker).*

Exercice 15. — *Donner un exemple de deux idéaux* $\mathfrak{a}$ *et* $\mathfrak{b}$ *d'un anneau* A *tels que* $\mathfrak{a} \cap \mathfrak{b} \neq \mathfrak{ab}$*. Montrer que l'on a toujours* $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$*.*

Exercice 16. — *Soit* A *un anneau noethérien. Montrons que pour tout ideal* $\mathfrak{a}$*, le quotient* $A/\mathfrak{a}$ *est encore noethérien.*

Exercice 17. — *Soit* K *un corps. L'anneau* $\mathrm{K}[X, Y]$ *est-il noetherien ? algébriquement clos ? de Dédékind ?*

Exercice 18. — *Montrer que l'anneau des entiers de* $\mathbb{Q}(\sqrt{-5})$ *n'est pas principal (idem pour* $\mathbb{Q}(\sqrt{-10})$*).*

Exercice 19. — *Soit* $\mathrm{K} = \mathbb{Q}(\sqrt{-5})$ *;* $A = \mathcal{O}_\mathrm{K}$ *l'anneau des entiers de* K*. Notons par* $\mathfrak{P}_\ell$ *un idéal premier de* A *au-dessus de* ℓ*.*
1) Donner la décomposition de $2A$*,* $3A$*,* $5A$*,* $11A$*; Calculer* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}\mathfrak{P}_2$*,* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}\mathfrak{P}_5$*,* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}\mathfrak{P}_{11}$*.*
2) Les idéaux premiers $\mathfrak{P}_3$ *et* $\mathfrak{P}_3'$ *au-dessus de* 3 *sont-ils principaux ?*
3) Donner la factorisation de $(1+\sqrt{-5})A$*.*

Exercice 20. — *Soit* $\mathrm{K} = \mathbb{Q}(\sqrt{-15})$ *;* $A = \mathcal{O}_k$*.*
Trouver la factorisation de $(1+\sqrt{-15})A$*, de* $(\dfrac{1+\sqrt{-15}}{3})A$*, de* $(5+2\sqrt{-15})A$*, et de* $(5-3\sqrt{-15})A$*.*

Exercice 21. — *Soit* $\mathrm{K} = \mathbb{Q}(\sqrt{17})$*. Factoriser* $(3+\sqrt{17})\mathcal{O}_\mathrm{K}$*.*

Exercice 22. — *Soit* $\mathrm{K} = \mathbb{Q}(\theta)$ *avec* $\theta \in \mathbb{C}$ *une racine de* $f(X) = X^3 - X - 1$*.*
1) Montrer que $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\theta]$*. L'extension* $\mathrm{K}/\mathbb{Q}$ *est-elle galoisienne ?*
2) Trouver la décomposition de $2\mathcal{O}_\mathrm{K}$*,* $5\mathcal{O}_\mathrm{K}$ *et* $23\mathcal{O}_\mathrm{K}$*.*

Exercice 23. — *Suite de l'exercice 11.*
Soit $P = X^3 + X^2 - 2X + 8$*, et* θ *une racine* P *;* $\mathrm{K} = \mathbb{Q}(\theta)$*. On a vu que* $\mathcal{O}_\mathrm{K} = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\beta$*, où* $\beta = 4/\theta$*.*
Pour $x = a + b\theta + c\beta \in \mathcal{O}_\mathrm{K}$*, on pose* $\phi_1(x) = a \pmod 2$*,* $\phi_2(x) = a + b \pmod 2$ *et* $\phi_3(x) = a + c \pmod 2$*.*
1) Montrer que les applications $\phi_i : \mathcal{O}_\mathrm{K} \to \mathbb{Z}/2\mathbb{Z}$ *sont des morphismes d'anneaux.*
2) Montrer que les noyaux des ϕ_i *sont des idéaux maximaux de* $\mathcal{O}_\mathrm{K}$*, deux à deux distincts. En déduire la décomposition de* $2\mathcal{O}_\mathrm{K}$*.*
2) Montrer qu'il n'existe pas d'élément $z \in \mathcal{O}_\mathrm{K}$ *tel que* $\mathcal{O}_\mathrm{K} = \mathbb{Z}[z]$*.*

Exercice 24. — *Soit* L/K *une extension galoisienne de corps de nombres. Posons* $G = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$.
Soit $\mathfrak{P}$ *un idéal premier de* $\mathcal{O}_L$ *divisant l'idéal maximal* $\mathfrak{p}$ *de* $\mathcal{O}_K$.
Définissons

$$G_{\mathfrak{P}} = \{\sigma \in G, \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

et

$$G_{0,\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}}, (\sigma(x) - x) \in \mathfrak{P}, \forall x \in \mathcal{O}_{\mathrm{L}}\}.$$

1) Montrer que $G_{0,\mathfrak{P}}$ *est un sous-groupe de* $G_{\mathfrak{P}}$. *Le groupe* $G_{0,\mathfrak{P}}$ *est le groupe d'inertie de* $\mathfrak{P}$ *; le groupe* $G_{\mathfrak{P}}$ *est le groupe de décomposition de* $\mathfrak{P}$.
2) Montrer que si $\mathfrak{P}$ *et* $\mathfrak{P}'$ *sont conjugués, alors il en est de même pour les groupes* $G_{0,\mathfrak{P}}$ *et* $G_{0,\mathfrak{P}'}$ *(idem pour les groupes* $G_{\mathfrak{P}}$ *et* $G_{\mathfrak{P}'}$*).*
3) Montrer que $G_{0,\mathfrak{P}}$ *agit trivialement sur* $\mathcal{O}_{\mathrm{L}}/\mathfrak{P}$.
4) En déduire que $G_{\mathfrak{P}}/G_{0,\mathfrak{P}}$ *agit sur* $\mathcal{O}_{\mathrm{L}}/\mathfrak{P}$ *puis que* $G_{\mathfrak{P}}/G_{0,\mathfrak{P}}$ *est naturellement isomorphe au groupe de Galois* $\mathrm{Gal}((\mathcal{O}_{\mathrm{L}}/\mathfrak{P})/(\mathcal{O}_{\mathrm{K}}/\mathfrak{p}))$.

Exercice 25. — *Soit* $\mathrm{L} = \mathbb{Q}(\zeta_5)$ *et* $\mathrm{K} = \mathbb{Q}(\sqrt{5})$. *On rappelle que* $\mathrm{K} \subset \mathrm{L}$, *et que* $\mathcal{O}_{\mathrm{L}} = \mathbb{Z}[\zeta_5]$.
1) Trouver la décomposition $2\mathcal{O}_{\mathrm{L}}$, $3\mathcal{O}_{\mathrm{L}}$ *et de* $5\mathcal{O}_{\mathrm{L}}$.
2) En déduire les degré résiduels et les indices de ramfication des premiers au-dessus de 2 3 *et* 5 *dans* L/K *; donner les groupes de décomposition (voir exercice 24), et d'inertie de ces premiers (dans* L/K*).*
3) Décrire parfaitement la décomposition de 11 *dans* $\mathrm{K}/\mathbb{Q}$ *puis dans* L/K.

Exercice 26. — *Soit* $\mathrm{L} = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$.
1) Montrer que $\mathcal{O}_{\mathrm{L}} = \mathbb{Z}[\sqrt{-1}, \dfrac{1+\sqrt{5}}{2}]$. *(utiliser le fait que* $\mathbb{Z}[i]$ *est principal).*
2) Calculer le discriminant absolu de L. *En déduire que les idéaux qui se ramifient dans* $\mathrm{L}/\mathbb{Q}$ *sont au-dessus de* 2 *et de* 5 *et que les indices de ramification valent* 2.
3) Donner les groupes de décomposition et d'inertie de 2 *et de* 5 *(voir exercice 24). (Pourquoi peut-on faire un abus de notation ?)*
4) Donner les groupes de décomposition et d'inertie de 7 *et* 11 *(dans* $\mathrm{L}/\mathbb{Q}$*).*

Exercice 27. — *Soit* $\mathrm{K} = \mathbb{Q}(\sqrt{-47})$.
1) Montrer que $2, 3, 7$ *sont décomposés dans* $\mathrm{K}/\mathbb{Q}$. *Montrer ensuite que* $\mathfrak{P}_2$, $\mathfrak{P}_3$, $\mathfrak{P}_7$ *ne sont pas principaux.*
2) Trouver le plus petit entier n *tel que* $\mathfrak{P}_2^n$ *est principal.*

Exercice 28. — *Soit* K *un corps de nombres.*
1) Soient $\mathfrak{a}$ *et* $\mathfrak{b}$ *deux idéaux non nuls de* $\mathcal{O}_K$. *Montrer que si pour certain entier* $m > 0$, $\mathfrak{a}^m = \mathfrak{b}^m$, *alors* $\mathfrak{a} = \mathfrak{b}$.
2) Soit $a \in \mathcal{O}_K$ *tel que* $\mathfrak{a}^n = a\mathcal{O}_K$. *Justifier l'existence de* a.
Posons $\mathrm{L} = \mathbb{Q}(\sqrt[n]{a})$. *Montrer que* $\mathfrak{a}\mathcal{O}_\mathrm{L}$ *est principal dans* $\mathcal{O}_\mathrm{L}$.
3) En déduire l'existence d'une extension finie F *de* K *telle que tout idéal* $\mathfrak{a}$ *de* $\mathcal{O}_\mathrm{K}$ *devient principal dans* F *(i.e.* $\mathfrak{a}\mathcal{O}_\mathrm{F}$ *est principal dans* $\mathcal{O}_\mathrm{F}$*).*

Exercice 29. — *Soit* $\mathrm{K} = \mathbb{Q}(j, \sqrt[3]{2})$.
Montrer qu'aucun idéal premier non nul de $\mathbb{Z}$ *ne reste premier dans* $\mathcal{O}_\mathrm{K}$.

Exercice 30 **(Symbole de Legendre)**. —
Résultats préliminaires
A) Soit L/K/F *une tour d'extensions galoisiennes de corps de nombres. Notons par* $\mathfrak{q}$ *un idéal premier de* L *au-dessus de* $\mathfrak{p}$ *idéal de* F. *On suppose que* $\mathfrak{q}$ *est non-ramifié. Notons par* $\sigma = \left(\dfrac{\mathrm{L/F}}{\mathfrak{p}}\right)$ *le Frobenius de* $\mathfrak{p}$ *dans* L/F.
Comment est caractérisé cet élément σ *? Montrer que* σ *restreint à* K *est égal à* $\left(\dfrac{\mathrm{K/F}}{\mathfrak{p} \cap \mathcal{O}_\mathrm{K}}\right)$.
B) Soit $\mathrm{K} = \mathbb{Q}(\zeta_n)$.

a) Montrer que pour p *ne divisant pas* n, p *n'est pas ramifié dans* $\mathrm{K}/\mathbb{Q}$. *Indic : on montrera que* $\mathrm{d}(\mathbb{Z}[\zeta_n])$ *divise une puissance de* n*).*

b) Soit $\mathfrak{p}|p$ *un premier ne divisant pas* n. *Notons* $\sigma_\mathfrak{p}$ *l'automorphisme de frobenius de* $\mathfrak{p}$ *dans* $\mathrm{K}/\mathbb{Q}$. *Soit* $j(\mathfrak{p})$ *défini par* $\sigma_\mathfrak{p}(\zeta_n) = \zeta_n^{j(\mathfrak{p})}$.
Montrer :

$$\prod_{0 \leq r \leq n-1,\ r \neq q(n)} (\zeta_n^q - \zeta_n^r) \notin \mathfrak{p}.$$

En déduire que $j(\mathfrak{p}) \equiv q\ (\ mod\ n)$.

Loi de réciprocité quadratique

Soit p un premier impair, et $d \in \mathbb{Z}^*$ étranger à p.
On pose

$\left(\frac{d}{p}\right) = 1$ *if* $d \in \mathbb{F}_p^2$;

$\left(\frac{d}{p}\right) = -1$ *if* $d \notin \mathbb{F}_p^2$.

1) Montrer que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

2) (Critère d'Euler). Montrer que $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$.

3) Soient p et q deux premiers impairs. Soit $\varepsilon_q = (-1)^{(q-1)/2}$. *On pose* $\mathrm{K} = \mathbb{Q}(\zeta_q)$ *et* $k = \mathfrak{q}(\sqrt{\varepsilon_q q}) \subset \mathrm{K}$.

Notons σ l'automorphisme de Frobenius $\left(\frac{K/\mathbb{Q}}{p}\right)$.

a) On rappelle que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{F}_q^\times$. *Montrer que* $\mathrm{Gal}(K/k) \simeq \mathbb{F}_q^{\times 2} := H$.

b) Montrer que la restriction de σ à k est ou bien l'identité si $\left(\frac{p}{q}\right) = 1$, *ou bien différent de l'identité si* $\left(\frac{p}{q}\right) = -1$.

c) En déduire $\left(\frac{k/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right)$.

d) En regardant la décomposition de p dans k, montrer que $\left(\frac{k/\mathbb{Q}}{p}\right) = \left(\frac{\varepsilon_q q}{p}\right)$.

e) En déduire : $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$.

4) (Formule complémentaire)

a) Montrer que

- $(-1)^{\frac{q^2-1}{8}} = 1$ *si* $\varepsilon_q q \equiv 1 \pmod 8$;
- $(-1)^{\frac{q^2-1}{8}} = -1$ *si* $\varepsilon_q q \equiv 5 \ (mod\ 8)$.

b) En déduire $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$.

5) Calculer $\left(\frac{69}{59}\right)$ *puis* $\left(\frac{110}{23}\right)$.

Exercice 31. — *Donner des exemples de corps quadratiques réels et imaginaires qui ont un groupe des classes trivial.*

Exercice 32. — *Montrer que le groupe des classes des corps* $\mathbb{Q}(\sqrt{d})$ *avec* $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$, *puis* $d = 3, 5, 7, 11, 13$ *est trivial.*

Exercice 33. — *Calculer le groupe des classes de :* $\mathbb{Q}(\sqrt{-47})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-2.3.5})$, $\mathbb{Q}(\sqrt{-26})$, $\mathbb{Q}(\sqrt{10})$.

Exercice 34. — *Montrer que le polynôme* $P(x) = x^3 - 3x + 1$ *est irréductible sur* $\mathbb{Q}$, *et que ses trois racines sont réelles. Soit* x *l'une d'entre elles. Posons* $\mathrm{K} = \mathbb{Q}(x)$.
1) Soit $B = \mathbb{Z}[x]$. *Calculer le discriminant de* B. *En utilisant l'inégalité de Minkowski, montrer que* $B = \mathcal{O}_k$.
2) Déterminer le groupe des classes de K.

Exercice 35. — *Soient* p *un nombre premier impair,* ζ_p *une racine primitive* p^{eme} *de l'unité,* $z = \zeta_p + \zeta_p^{-1}$, $\mathrm{L} = \mathbb{Q}(\zeta_p)$ *et* $\mathrm{K} = \mathbb{Q}(z)$.
1) Déterminer le groupe de Galois de $\mathrm{L}/\mathbb{Q}$ *puis de* $\mathrm{K}/\mathbb{Q}$.
2) Montrer que l'anneau des entiers de $\mathbb{Q}(z)$ *est* $\mathbb{Z}[z]$. *Indic : on utilisera le fait que l'anneau des entiers de* L *est* $\mathbb{Z}[\zeta_p]$.
3) On prend $p = 11$.
a) Déterminer le groupe des classes de $\mathbb{Q}(\zeta_{11})$.
b) Déterminer le groupe des classes de K.

Exercice 36. — *Soit* $\mathrm{K} = \mathbb{Q}(\theta)$, *où* θ *est la racine réelle de* $X^3 - 5 = 0$.
1) Calculer $\mathrm{d}(1, \theta, \theta^2)$. *En déduire que* 3 *est ramifié dans* $\mathrm{K}/\mathbb{Q}$. *Quelle est la décomposition possible de* $3\mathcal{O}_\mathrm{L}$ *? Calculer* $(\theta + 1)^3$ *et en déduire alors que* 3 *est totalement ramifié dans* $\mathrm{K}/\mathbb{Q}$.

2) En considérant l'idéal $\mathfrak{P} = \theta\mathcal{O}_{\mathrm{K}}$ *montrer que* 5 *est totalement ramifié dans* $\mathrm{K}/\mathbb{Q}$ *(on notera que* $\mathfrak{P}$ *est l'unique idéal de* K *au-dessus de* 5*).*
3) Donner une majoration de la constante de Minkowski. Calculer le groupe des classes de K*. Indic : On calculera* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\theta+1)$*,* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\theta-1)$*,* $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(\theta+3)$*.*
4) On veut montrer que $\mathcal{O}_{\mathrm{K}} = \mathbb{Z}[\theta]$*. On notera* $A = \mathbb{Z}[\theta]$*.*

a) Pour tout élément $x = a+b\theta+c\theta^2$ *de* K *(*$a, b, c \in \mathbb{Q}$*), déterminer* $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}x$*. En déduire* $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}\theta x$ *puis* $\mathrm{Tr}_{\mathrm{K}/\mathbb{Q}}\theta^2 x$*.*

b) Montrer que $A \subset \mathcal{O}_{\mathrm{K}} \subset 1/15A$*, puis que tout élément* x *de* $\mathcal{O}_{\mathrm{K}}$ *s'écrit* $x = 3^{\alpha}5^{\alpha'}a + 3^{\beta}5^{\beta'}b\theta + 3^{\gamma}5^{\gamma'}c\theta^2$*, avec* $a, b, c \in \mathbb{Z}$ *non multiples de* 3 *et* 5 *et* $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \geq -1$*.*

c) Remarquer que les $\mathfrak{P}$*-valuations des trois termes de la somme* $3^{\alpha}5^{\alpha'}a+3^{\beta}5^{\beta'}b\theta+3^{\gamma}5^{\gamma'}c\theta^2$ *sont disctinctes. En déduire alors que* $\mathrm{v}_{\mathfrak{P}}(x) = \min(3\alpha', 3\beta'+1, 3\gamma'+2) \geq 0$*, puis que* $\alpha', \beta', \gamma' \geq 0$*.*
On est donc ramener au cas $x = 3^{\alpha}a + 3^{\beta}b\theta + 3^{\gamma}c\theta^2$*,* $a, b, c \in \mathbb{Z}$ *non multiples de* 3*.*

d) Montrer l'égalité $x = 3^{\alpha}a - 3^{\beta}b + 3^{\gamma}c + (\theta+1)(3^{\beta}b - 3^{\gamma}2c) + (\theta+1)^2 3^{\gamma}c$*. En déduire* $\alpha, \beta, \gamma \geq 0$*.*
5) Quelle est la structure du groupe des unités de K *?*
6) Reprendre l'exercice avec $X^3 - 2$*,* $X^3 - 3$*, et* $X^4 - 2$*.*

Exercice 37. — *On se propose de résoudre dans* $\mathbb{Z}$ *l'équation* (E) *suivante :*

$$Y^2 = X^3 - 13.$$

1) Soit $\mathrm{K} = \mathbb{Q}(\sqrt{-13})$*. Calculer* Cl_{K}*.*
2) Soit (x, y) *une solution de* (E)*.*

a) Montrer que $13 \nmid x$*. Montrer de même que* $2 \nmid x$*. Indic : on pourra raisonner modulo* $4\mathbb{Z}$*.*

b) Soit l'idéal de $\mathcal{O}_{\mathrm{K}}$ *:* $\mathfrak{a} = (y + \sqrt{-13}, y - \sqrt{-13})$*. Montrer que* $\mathfrak{a} = \mathfrak{P}_2^i\mathfrak{P}_{13}^j$*.*

c) Montrer alors que les idéaux $(y + \sqrt{-13})$ *et* $(y - \sqrt{-13})$ *sont premiers entre eux.*

d) En déduire que $(y + \sqrt{-13})\mathcal{O}_{\mathrm{K}}$ *est le cube d'un idéal.*

e) Montrer ensuite l'existence de $a, b \in \mathbb{Z}$ vérifiant

$$y + \sqrt{-13} = (a + b\sqrt{-13})^3.$$

f) Résoudre (E).

Exercice 38. — *Soit $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, $d \geq 2$ sans facteurs carrés.*
1) Montrer que les unités de K supérieures à 1 sont les unités de la forme $a + b\sqrt{d}$, $a, b > 0$.
2) On suppose $d \equiv 2, 3 \ (mod\ 4)$.
Soit $\varepsilon = a_1 + b_1\sqrt{d}$ l'unité fondamentale de K. On pose $a_n + b_n\sqrt{d} = \varepsilon^n$.
a) Montrer que la suite $(b_n)_n$ est croissante.
b) En déduire les unités fondamentales de K pour $d = 2, 6, 7, 10$.
3) On suppose $d \equiv 1 \pmod 4$.
a) Montrer que les unités de K sont racines de

$$a^2 - db^2 = \pm 4,$$

avec a et b de même parité.
b) Trouver les unités fondamentales de K pour $d = 5, 13, 17$.

Exercice 39. — *Résoudre dans $\mathbb{Z}$ les équations*

- $X^2 - 11Y^2 - 5 = 0$,
- $X^2 - 11Y^2 + 5 = 0$.

Exercice 40. — *Soit $\mathrm{K} = \mathbb{Q}(\theta)$ où θ est la racine réelle de $x^3 - 2 = 0$. On admettra que $\mathcal{O}_\mathrm{K} = \mathbb{Z}[\theta]$.*
Le but de l'exercice est de trouver une unité fondamentale de K.
1) Soit u l'unité fondamentale supérieure à 1. Montrer que $\mathrm{N}_{\mathrm{K}/\mathbb{Q}} u = 1$.
2) Notons $u = r^2$. Montrer que les conjugués de u peuvent s'écrire $r^{-1}e^{ia}$, $r^{-1}e^{-ia}$.
En déduire le calcul du discriminant d de $\mathbb{Z}[u]$.
3) Soit $f(r, a) = (r^3 + r^{-3}) \sin a - \sin 2a$. Etudier le minimum de $f(r, a)$ pour r fixé. Par abus nous noterons a solution de $(r^3 + r^{-3}) \cos a - 2 \cos 2a = 0$.

Montrer que $|\mathrm{d}| \leq 4(r^6 + 6 + (r^{-6} - 4\cos^2 a - 4\cos^4 a))$.
4) Soit $g(x) = 2x^2 - 1/2(r^3 + r^{-3})x - 1 \in \mathbb{R}[x]$.
Montrer que $g(1) < 0$, *puis que* $g(-1/(2r^3)) < 0$. *En déduire que* g *a deux racines : l'une est supérieure à 1, l'autre est inférieure à* $-1/(2r^3)$. *En déduire alors que* $r^{-6} - 4\cos^2 a - 4\cos^4 a$ *est positif puis que* $|\mathrm{d}| \leq 4u^3 + 24$.
5) Soit $v > 1$ *unité de* k. *Montrer que si* $4v^{3/2} + 24 \leq |\mathrm{d_K}|$, *alors* v *est une unité fondamentale de* K.
6) Montrer que $\theta - 1$ *est une unité de* K. *En déduire l'unité fondamentale* $u > 1$ *(*$\theta \approx 1.84$*).*

Exercice 41. — *Sur le corps* K, *définissons l'application* $|.|$ *à valeurs dans* $\mathbb{R}$ *par :* $|x| = 1$ *pour* $x \neq 0$ *et* $|0| = 0$. *Montrer que* $|.|$ *est une valeur absolue sur* K *(c'est la valeur absolue triviale).*

Exercice 42. — *Soit* K *un corps fini. Montrer que la valeur absolue triviale est la seule valeur absolue sur* K.

Exercice 43. — *Soit* K *un corps. Soit* $A = \mathrm{K}[X]$ *l'anneau des polynômes sur* K, *puis* $\mathrm{L} = \mathrm{K}(X)$ *le corps des fractions de* A.
Pour $f/g \in \mathrm{L}^*$, *avec* $(f, g) = 1$, $f, g \in A$, *on pose* $v(f/g) = deg(g) - deg(f)$. *On prolonge* v *en* 0, *en posant :* $v(0) = +\infty$.
Soit $\rho \in]0, 1[$. *Posons alors pour* $x \in \mathrm{L}$, $||x|| = \rho^{v(x)}$.
1) Montrer que $||.||$ *définit une valeur absolue sur* K.
2) Montrer que $(K, ||.||)$ *n'est pas complet.*

Exercice 44. — *Soit* $||.||$ *une valeur absolue sur* K *et soit* $\sigma : \mathrm{K} \to \mathrm{K}$ *un automorphisme de* K.
Posons $||.||_\sigma = ||\sigma(.)||$. *Montrer que* $||.||_\sigma$ *est une valeur absolue sur* K.

Exercice 45. — *Soit* $|.|$ *la valeur absolue usuelle sur* $\mathbb{R}$. *Quels sont ses prolongements sur* $\mathbb{C}$ *?*

Exercice 46. — *Soit* $|.|$ *la valeur absolue usuelle sur* $\mathbb{Q}$. *Soit* α *une racine de* $X^3 - 2$ *(dans une clôture algébrique de* $\mathbb{Q}$*). Posons* $\mathrm{K} = \mathbb{Q}(\alpha)$. *Déterminer l'ensemble des prolongements de* $|.|$ *sur* K.

Exercice 47. — *Montrer que* $X^2 = 7$ *admet deux racines dans* $\mathbb{Q}_3$. *Calculer ces racines modulo* 27.

Exercice 48. — *Montrer que* $X^2 = 2$ *n'a pas de racine dans* $\mathbb{Q}_3$.

Exercice 49. — *Trouver toutes les racines de l'unité dans* $\mathbb{Q}_5$.

Exercice 50. — *Dans* $\overline{\mathbb{Q}_5}$, *soit* α *une racine de* $X^2 + X + 1$. *Montrer que* $\mathbb{Q}_5(\alpha)/\mathbb{Q}_5$ *est une extension non-ramifiée de degré* 2.

Exercice 51. — *Soit* L/K *une extension de corps locaux.*
1) Montrer que $\mathrm{Tr}_{\mathrm{L/K}}\mathcal{O}_L$ *est un idéal de* $\mathcal{O}_\mathrm{K}$.
2) Montrer que si L/K *est non-ramifiée, alors* $\mathrm{Tr}_{\mathrm{L/K}}\mathcal{O}_\mathrm{L} = \mathcal{O}_\mathrm{K}$.

Exercice 52. — *Soit* $\mathrm{K} = \mathbb{Q}_p(\pi)$, *où* π *est une racine de* $X^{p-1} = p$.
1) Montrer que $[\mathrm{K} : \mathbb{Q}_p] = p - 1$.
2) Montrer que l'extension $\mathrm{K}/\mathbb{Q}_p$ *est galoisienne.*
3) Montrer que l'extension $\mathrm{K}/\mathbb{Q}_p$ *est totalement ramifiée.*

Exercice 53. — *Soit* $\mathrm{K} = \mathbb{Q}_p(\zeta_p)$, *où* ζ_p *est une racine primitive* p*-ème de l'unité. Montrer que l'extension* $\mathrm{K}/\mathbb{Q}_p$ *est totalement ramifiée.*

Université de Franche-Comté - UFR Sciences et Techniques
Master 2 Mathématiques et Applications - Année 2008-2009

Examen final - CTU
Théorie Algébrique des Nombres
Cours autorisé

Exercice 1.

Soit p un nombre premier vérifiant $p \equiv 1 \pmod 4$.
Soit $\mathrm{K} = \mathbb{Q}(\sqrt{p})$. Notons par $\mathcal{O}_\mathrm{K}$ l'anneau des entiers de K et par $U = \mathcal{O}_\mathrm{K}^\times$ le groupe des unités de l'anneau $\mathcal{O}_\mathrm{K}$.
Soient $\sigma_0 : \sqrt{p} \mapsto \sqrt{p}$ et $\sigma_1 : \sqrt{p} \mapsto -\sqrt{p}$ les éléments du groupe de Galois de $\mathrm{K}/\mathbb{Q}$.
Si $x \in \mathrm{K}$, on note par $N(x) = \sigma_0(x)\sigma_1(x)$ la norme de x dans $\mathrm{K}/\mathbb{Q}$.

1) Montrer que $U =< \pm 1 > \times C$, où C est isomorphe à $\mathbb{Z}$. On notera par ε un générateur de C.

2) Montrer que $N(\varepsilon) \in \mathbb{Z}$. Quelles sont les valeurs possibles pour $N(\varepsilon)$?

3) Soit u une unité de $\mathcal{O}_\mathrm{K}$. Montrer qu'il existe $n \in \mathbb{Z}$ tel que $N(u) = N(\varepsilon)^n$.

4) Montrer que σ_0 et σ_1 sont libres sur K, c'est à dire si $a, b \in \mathrm{K}$ sont tels que pour tout $z \in \mathrm{K}$, il vient

$$a\sigma_0(z) + b\sigma_1(z) = 0,$$

alors $a = b = 0$.
En déduire que pour tout élément x de K, il existe $z \in \mathrm{K}$ tel que $y = x\sigma_0(z) + \sigma_1(z) \neq 0$.

5) Soit $x \in \mathrm{K}$ tel que $N(x) = +1$. Montrer qu'il existe $y \in \mathrm{K}$ tel que

$$x = y^{1-\sigma_1} = \frac{y}{y^{\sigma_1}}.$$

6) Supposons que $N(\varepsilon) = 1$. D'après 4), il existe $y \in \mathrm{K}$ tel que $\varepsilon = y^{1-\sigma_1}$.

a) Pourquoi peut-on s'assurer que $y \in \mathcal{O}_\mathrm{K}$?

b) Pourquoi peut-on s'assurer qu'aucun nombre premier de $\mathbb{Z}$ ne divise y ?

c) Soit l'idéal fractionnaire $\mathfrak{a} = y\mathcal{O}_\mathrm{K}$. Que peut-on dire de l'idéal fractionnaire $\mathfrak{a}^{1-\sigma_1}$?

d) À partir de la factorisation de $\mathfrak{a}$, montrer que ou bien $\mathfrak{a} = \sqrt{p}\ \mathcal{O}_\mathrm{K}$ ou bien $\mathfrak{a} = \mathcal{O}_\mathrm{K}$.

e) En déduire une contradiction et ainsi que $N(\varepsilon) = -1$.

7) Résoudre l'équation diophantienne $X^2 - 5Y^2 = 1,\ X, Y \in \mathbb{Z}$.

Indication : pour $\mathrm{K} = \mathbb{Q}(\sqrt{5})$, *prendre* $\varepsilon = \dfrac{1+\sqrt{5}}{2}$.

Exercice 2.

Soit $\mathrm{K}/\mathbb{Q}_p$ une extension de degré n. On suppose l'extension $\mathrm{K}/\mathbb{Q}_p$ galoisienne de groupe de Galois $G = \mathrm{Gal}(\mathrm{K}/\mathbb{Q}_p)$. Notons par

- $\mathcal{O}_\mathrm{K}$ l'anneau des entiers de K ;
- $U = \mathcal{O}_\mathrm{K}^\times$ le groupe des unités de $\mathcal{O}_\mathrm{K}$;
- π une uniformisante de K ;
- v la valuation normalisée de K : $v(\pi) = 1$;
- $k = \mathcal{O}_\mathrm{K}/(\pi)$ le corps résiduel : c'est une extension finie de $\mathbb{F}_p$ de degré f ;
- e l'indice de ramification de p dans $\mathrm{K}/\mathbb{Q}$: $p\mathcal{O}_K = \pi^e\mathcal{O}_\mathrm{K}$.

On rappelle que $ef = n$ et que $U = \{x \in \mathcal{O}_\mathrm{K},\ v(u) = 0\}$.

Partie I.

Pour $i \geq 0$, on définit $U^i = \{x \in U,\ v(x-1) \geq i\}$.

1) Montrer que U^i est sous-groupe de U.

2) Montrer que $U/U^1 \simeq (k^\times, .)$.

Soit $i \geq 1$. Pour $x = 1 + \pi^i u \in U^i$, on définit $\theta_i(x) \in k$ par

$$\theta_i(x) = u \pmod{\pi \mathcal{O}_{\mathrm{K}}}.$$

3) Montrer que θ_i induit un isomorphisme de groupes entre U^i/U^{i+1} et $(k, +)$.

Partie II.

4) Soit $\sigma \in G$ et $u \in U$. Montrer que $\sigma(u) = u^\sigma \in U$.

5) Montrer : $\forall \sigma \in G$, $v(\pi^\sigma) = 1$.

Pour $i \geq -1$, on pose $G_i = \{\sigma \in G,\ \forall x \in \mathcal{O}_{\mathrm{K}},\ v(x^\sigma - x) \geq i+1\}$. On a : $G_{-1} = G$.

6) Montrer que $G_{i+1} \lhd G_i$.

7) Soit $i \geq 0$. Montrer que si $u \in U$ et $\sigma \in G_i$ alors $v(\frac{u^\sigma}{u} - 1) \geq i+1$ et $v(\frac{\pi^\sigma}{\pi} - 1) \geq i$.

Soit $\{x_1, \cdots, x_n\}$ une $\mathbb{Z}_p$-base de $\mathcal{O}_{\mathrm{K}}$. Pour $\sigma \in G$, posons $f_j(\sigma) = v(x_j^\sigma - x_j)$.

8) Montrer que $\sigma \in G_i$ si et seulement si pour $j = 1, \cdots, n$, $f_j(\sigma) \geq i+1$. En déduire que pour i suffisament grand, $G_i = \{1\}$.

Partie III

Soit l'application $\varphi : G \to U$ définie par $\varphi(\sigma) = \dfrac{\pi^\sigma}{\pi}$.

9) Soit $i \geq 0$. Montrer que $\varphi(G_i) \subset U^i$.
Indication : utiliser la question 7).

10) Soit $i \geq 0$. Montrer que φ induit un homomorphisme de groupes de G_i vers U^i/U^{i+1}.
Indication : utiliser 5) et 7).

11) Montrer que $G/G_0 \simeq \mathrm{Gal}(k/\mathbb{F}_p)$ et que $\#G_0 = e$.

12) Montrer que $G_0/G_1 \hookrightarrow (k^\times, .)$ et que pour $i \geq 1$, $G_i/G_{i+1} \hookrightarrow (k, +)$.
On admettra le fait suivant : $\sigma \in G_i$ si et seulement si $v(\pi^\sigma/\pi - 1) \geq i$.

13) En déduire que G_1 est un p-groupe.

Partie IV

15) Soit $p > 2$ et $\mathrm{K} = \mathbb{Q}_p(\sqrt{p})$. Que vaut G_0 ? Que vaut G_1 ?

16) Soit $\mathrm{K} = \mathbb{Q}_2(\sqrt{2})$. Déterminer G_i, $i \geq 0$.

17) Soit $\mathrm{K} = \mathbb{Q}_2(\sqrt{3})$. Déterminer G_i, $i \geq 0$.

Université de Franche-Comté
Master 2 Mathématiques et Applications
CTU
Année 2011-2012
Théorie Algébrique des Nombres

Cours autorisé

Exercice 1.

Partie A
Soit le corps de nombres $K = \mathbb{Q}(\theta)$, où θ est une racine du polynôme $P = X^2 + 21 \in \mathbb{Q}[X]$.

On notera par $\mathcal{O}$ l'anneau des entiers de K.

On rappelle que $K/\mathbb{Q}$ est une extension quadratique de groupe de Galois engendré par l'automorphisme $\sigma : \theta \mapsto -\theta$.

1) Déterminer une $\mathbb{Z}$-base de l'anneau des entiers $\mathcal{O}$ de K. En déduire le discriminant d_K de K.

2) Déterminer le groupe des inversibles de $\mathcal{O}$.

3) a) Montrer que $\mathfrak{p}_2 = (2, \theta - 1)$ est un idéal premier de $\mathcal{O}$ puis que $2\mathcal{O} = \mathfrak{p}_2^2$.

b) Déterminer la décomposition de $3\mathcal{O}$ et de $7\mathcal{O}$. Donner la factorisation de l'idéal $\theta\mathcal{O}$ en produit d'idéaux premiers.

c) Montrer que $\mathfrak{p}_5 = (5, \theta + 2)$ et $\mathfrak{q}_5 = (5, \theta + 3)$ sont deux idéaux premiers distincts de $\mathcal{O}$ vérifiant $5\mathcal{O} = \mathfrak{p}_5\mathfrak{q}_5$.

Soit Cl le groupe des classes de $\mathcal{O}$. Si $\mathfrak{a}$ désigne un idéal de $\mathcal{O}$, on notera par $\mathrm{Cl}(\mathfrak{a})$ la classe de $\mathfrak{a}$ dans Cl.

4) Montrer que toute classe d'idéaux de Cl contient un idéal entier de norme plus petite que 5. En déduire que $|\mathrm{Cl}| \leq 5$.

5) Montrer que les idéaux $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ et $\mathfrak{q}_5$ ne sont pas principaux (ici $\mathfrak{p}_3$ est l'unique idéal premier de $\mathcal{O}$ divisant 3). Déterminer l'ordre de $\mathrm{Cl}(\mathfrak{p}_2)$ et l'ordre de $\mathrm{Cl}(\mathfrak{p}_3)$.

6) Montrer que $\mathfrak{p}_2\mathfrak{p}_3$ n'est pas principal puis déterminer la structure du sous-groupe engendré par $\mathrm{Cl}(\mathfrak{p}_2)$ et $\mathrm{Cl}(\mathfrak{p}_3)$. En déduire que $|\mathrm{Cl}| = 4$ puis la structure de Cl.

7) Déterminer le plus entier $n \geq 1$ tel que l'équation diophantienne $X^2 + 21Y^2 = 5^n$ ait une solution non triviale (c'est-à-dire avec $XY \neq 0$, ici X et Y sont des entiers). En déduire que la classe $\mathrm{Cl}(\mathfrak{p}_5)$ de $\mathfrak{p}_5$ dans Cl est d'ordre 2. Vérifier que $\mathrm{Cl}(\mathfrak{p}_2\mathfrak{p}_3) = \mathrm{Cl}(\mathfrak{p}_5)$.

Partie B

On souhaite résoudre l'équation diophantienne $X^2 - Y^3 = -21$.

Soient deux entiers x et y vérifiant $x^2 - y^3 = -21$.

8) Soit l'idéal $\mathfrak{a}$ de $\mathcal{O}$ défini par $\mathfrak{a} = (x + \theta, x - \theta)$. Montrer que $2\theta \in \mathfrak{a}$ et en déduire que $\mathfrak{a}$ divise l'idéal principal $\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_7$, où $\mathfrak{p}_7$ est l'unique idéal premier de $\mathcal{O}$ divisant 7.

9) Ecrivons $(x + \theta) = \mathfrak{p}_2^s\mathfrak{p}_3^t\mathfrak{p}_7^u\mathfrak{b}$ et $(x - \theta) = \mathfrak{p}_2^{s'}\mathfrak{p}_3^{t'}\mathfrak{p}_7^{u'}\mathfrak{b}'$, avec $\mathfrak{b}\mathfrak{b}'$ premier à $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$.
Montrer que $s = s'$, que $t = t'$ et que $u = u'$ (on pourra regarder l'action de σ sur les idéaux en jeu), puis en utilisant la question précédente que $\mathfrak{b}$ est premier à $\mathfrak{b}'$.

10) A partir de l'identité $\mathfrak{p}_2^{2s}\mathfrak{p}_3^{2t}\mathfrak{p}_7^{2u}\mathfrak{b}\mathfrak{b}' = (y^3)$, en déduire que s, t et u sont des multiples de 3 et que $\mathfrak{b}$ est le cube d'un idéal.

Ecrivons alors $\mathfrak{p}_2^s\mathfrak{p}_3^t\mathfrak{p}_7^u\mathfrak{b} = \mathfrak{c}^3$, pour un certain idéal entier $\mathfrak{c}$.

11) En utilisant la question 6), montrer qu'il existe $m, n \in \mathbb{Z}$ tels que $\mathfrak{c} = (m + n\theta)$.

12) En déduire que $x + \theta = \pm(m + n\theta)^3$.

13) En déduire la résolution de l'équation diophantienne $X^2 - Y^3 = -21$.

Exercice 2.
Soit p un nombre premier et soit le corps local $\mathrm{K} = \mathbb{F}_p((X))$: c'est le corps des séries formelles sur le corps fini $\mathbb{F}_p$.

On rappelle que l'indéterminée X est une uniformisante de K et que l'anneau des séries formelles $\mathcal{O} = \mathbb{F}_p[[X]]$ est son anneau de valuation. On notera par v la valuation de K et par $\mathrm{k} = \mathbb{F}_p$ le corps résiduel de $\mathcal{O}$.

On se fixe une clôture algébrique $\overline{\mathrm{K}}$ de K.

Soit $x \in \mathrm{K}$ et soit P le polynôme à coefficients dans K défini par $P = Y^p - Y + x \in \mathrm{K}[Y]$. On notera par L le corps des racines de P sur K.

1) Soit α une racine de P dans $\overline{\mathrm{K}}$. Exprimer toutes les racines de P à partir de α et des éléments de $\mathbb{F}_p$. En déduire que $\mathrm{L} = \mathrm{K}(\alpha)$ puis que L/K est une extension galoisienne.

2) Supposons que P a une racine α avec $\alpha \notin \mathrm{K}$.
Soit $R \in \mathrm{K}[X]$ un facteur irréductible de P de degré d. Montrer qu'il existe $a_1, \cdots, a_r \in \mathbb{F}_p$ tels que

$$R = (Y - \alpha - a_1) \cdots (Y - \alpha - a_r).$$

En regardant le terme de degré $r - 1$, en déduire que nécessairement $r = p$, puis que P est irréductible sur K.
Quels sont les groupes de Galois Gal(L/K) possibles ?

3) Montrer, en utilisant le lemme de Hensel, que si $\mathrm{v}(x) > 0$ alors le polynôme P est scindé sur K.

4) Dans cette question on suppose que $\mathrm{v}(x) = 0$.

a) Soit α une racine de P. Supposons que $\alpha \in \mathrm{K}$. Montrer que α est une unité de $\mathcal{O}$, ou encore qu'il existe $a \in \mathbb{F}_p - \{0\}$ et $y \in \mathcal{O}$, tels que $\alpha = a + Xy$. Conclure à une absurdité.

b) Soit le polynôme réduit $\overline{P} = Y^p - Y + \overline{x} \in \mathrm{k}[Y]$. Montrer que $\overline{P}$ est irréductible sur k.

c) En déduire que L/K est une extension non-ramifiée cyclique de degré p.

5) Dans cette question on suppose que $\mathrm{v}(x) < 0$ et que $p \nmid \mathrm{v}(x)$.

a) Montrer qu'aucune racine α de P ne se trouve dans K.

b) Montrer que L/K est une extension totalement ramifiée cyclique de degré p.

c) Soient deux entiers naturels u et v tels que $u\mathrm{v}(x)+pv=1$. Justifier l'existence de ces entiers. Montrer que $\pi_{\mathrm{L}} := T^v\alpha^u$ est une uniformisante de L, où α est une racine de P dans $\overline{\mathrm{K}}$. Donner le polynôme irréductible de π_{L} sur K. Vérifier que ce polynôme est bien un polynôme d'Eisenstein.

Université de Franche-Comté - UFR Sciences et Techniques
Master 2 Mathématiques et Applications - CTU
Année 2012-2013

Jeudi 29 août 2013

Le document "Théorie des Nombres" et les calculatrices sont autorisés.

Exercice.
Soit le corps quadratique $\mathrm{K} = \mathbb{Q}(\sqrt{-7 \cdot 11})$. Notons par $\mathcal{O}_\mathrm{K}$ l'anneau des entiers de K et par $\mathcal{C}_\mathrm{K}$ son groupe des classes.

1) Donner une $\mathbb{Z}$-base de $\mathcal{O}_\mathrm{K}$ et préciser $\mathcal{O}_\mathrm{K}^\times$.

2) Montrer qu'il existe un idéal premier $\mathfrak{p}_2$ de norme 2 et deux idéaux $\mathfrak{p}_3$ et $\mathfrak{p}_3'$ de norme 3.

3) En utilisant la borne de Minkowski, montrer que le groupe des classes de K est d'ordre au plus 8.

4) Déterminer la structure du sous-groupe de $\mathcal{C}_\mathrm{K}$ engendré par les classes de $\mathfrak{p}_2$ et de $\mathfrak{p}_3$.

5) En déduire la structure de $\mathcal{C}_\mathrm{K}$.

Problème. Sur le Symbole de Hilbert.

Dans tout le problème, le corps K désigne soit le corps des nombres réels $\mathbb{R}$ soit le corps des nombres p-adiques $\mathbb{Q}_p$. On se fixe $\bar{\mathrm{K}}$ une clôture algébrique de K.

Sur $\mathbb{Q}_p$, on note par v_p la valuation p-adique normalisée : $v_p(p) = 1$. Pour $x \in \mathbb{Q}_p^\times$, la partie p-primaire x_p de x est l'unité p-adique définie par

$$x_p := p^{-v_p(x)} x \ \in \mathbb{Z}_p^\times.$$

Pour $a, b \in \mathrm{K}$, on note par $f_{a,b}$ la forme quadratique sur K définie par

$$f_{a,b}(X, Y, Z) = Z^2 - aY^2 - bX^2.$$

On rappelle que l'on dit qu'une forme quadratique f sur K représente 0, s'il existe un vecteur v *non nul* (à coefficient dans K) tel que $f(v) = 0$.

Sur $\mathrm{K}^\times \times \mathrm{K}^\times$, on définit l'application suivante :

$$\begin{array}{rcl} \mathrm{K}^\times \times \mathrm{K}^\times & \to & \{-1, +1\} \\ (a, b) & \mapsto & S(a, b) = \left\{ \begin{array}{ll} +1 & \text{si } f_{a,b} \text{ représente 0} \\ -1 & \text{sinon} \end{array} \right. \end{array}$$

1) Montrer rapidement que S est définie sur $\mathrm{K}^\times/(\mathrm{K}^\times)^2 \times \mathrm{K}^\times/(\mathrm{K}^\times)^2$.

2) Notons par $\sqrt{b}$ une racine du polynôme $X^2 - b$ et soit le corps $\mathrm{K}_b = \mathrm{K}(\sqrt{b})$. Montrer que $S(a, b) = +1$ si et seulement si, a est norme dans l'extension K_b/K.

3) Soient $a, b, a' \in \mathrm{K}^\times$. Montrer que

i) S est symétrique, i.e. $S(a, b) = S(b, a)$;

ii) $S(a, -a) = 1$;

iii) $S(a, 1 - a) = 1$, pour a tel que $1 - a \neq 0$;

iv) Si $S(a, b) = 1$, alors $S(aa', b) = S(a', b)$
(*Indication : on pourra utiliser le résultat de la question 2.*) ;

v) $S(a, b) = S(a, -ab) = S(a, (1 - a)b)$, pour a tel que $1 - a \neq 0$.

4) Pour cette question, on suppose $\mathrm{K} = \mathbb{R}$.
Pour $a \in \mathbb{R}^\times$, on définit $v_\infty : \mathbb{R}^\times \to \mathbb{Z}/2\mathbb{Z}$, par $v_\infty(a) = \bar{0}$ si $a > 0$, $v_\infty(a) = \bar{1}$ sinon.

i) Vérifier que v_∞ est un homomorphisme de groupes.

ii) Montrer que $S(a, b) = (-1)^{v_\infty(a) v_\infty(b)}$.

iii) En déduire que sur $\mathbb{R}^\times/{\mathbb{R}^\times}^2$, S est une forme bilinéraire symétrique non-dégénérée.

5) Quand K $= \mathbb{Q}_p$, expliquer rapidement pourquoi lors du calcul de $S(a,b)$ on peut se ramener à a, b tels que $v_p(a), v_p(b) \in \{0,1\}$. Expliquer également pourquoi $S(a,b) = 1$ si et seulement si, il existe un triplet non-nul de solution (x,y,z) dans $\mathbb{Z}_p$ avec au moins une des coordonnées de valuation nulle.

Pour toute la suite, on se placera sous les conditions de la question 5).

6) Dans cette question, K $= \mathbb{Q}_p$, avec $p > 2$. On suppose de plus que p ne divise pas ab : $v_p(a) = v_p(b) = 0$.

i) On se place sur le corps $\mathbb{F}_p$. Soit $y \in \mathbb{F}_p^\times$. Minorer le cardinal de l'ensemble $E_{a,y} = \{z^2 - \bar{a}y^2,\ z \in \mathbb{F}_p\}$ et déterminer celui de $E_b = \{\bar{b}x^2,\ x \in \mathbb{F}_p\}$.

ii) En déduire que $E_{a,y} \cap E_b$ est non vide.

iii) En utilisant le lemme de Hensel, en déduire finalement que $S(a,b) = 1$.

7) On suppose toujours que K $= \mathbb{Q}_p$, $p > 2$, avec cette fois-ci, $v_p(a) = 1$ et $v_p(b) = 0$.

Notons par $\left(\frac{b}{p}\right)$ le symbole de Legendre (= 1 si $\bar{b}$ est un carré non nul dans $\mathbb{F}_p$, -1 si ce n'est pas un carré, et 0 si $\bar{b} = 0$). On rappelle que ce symbole est multiplicatif :

$$\left(\frac{b'b}{p}\right) = \left(\frac{b'}{p}\right)\left(\frac{b}{p}\right).$$

Montrer que $S(a,b) = \left(\frac{\bar{b}}{p}\right)$. (*Indication : On pourra utiliser le lemme de Hensel.*)

8) On suppose toujours K $= \mathbb{Q}_p$, avec $p > 2$. On suppose cette fois-ci que $v_p(a) = v_p(b) = 1$.

Montrer que $S(a,b) = \left(\frac{-\overline{a_p}\overline{b_p}}{p}\right)$.

(*Indication : On pourra considérer la forme quadratique* $af_{a,b}$.)

9) Sur $\mathbb{Q}_p$, $p > 2$, en déduire que l'on a la formule

$$S(a,b) = \left(\frac{-1}{p}\right)^{v_p(a)v_p(b)} \left(\frac{a_p}{p}\right)^{v_p(b)} \left(\frac{b_p}{p}\right)^{v_p(a)}.$$

En déduire que S est une forme bilinéaire symétrique non-dégénérée (sur $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$).

La fin du problème est hors barême ...

10) Cette fois-ci, on suppose $\mathrm{K} = \mathbb{Q}_2$.
Pour $x \in \mathbb{Z}_2^\times$, on pose

$$\varepsilon(x) \equiv \frac{x-1}{2} \pmod 2 = \begin{cases} \bar{0} & \text{si } x \equiv 1 \pmod 4 \\ \bar{1} & \text{si } x \equiv 3 \pmod 4 \end{cases}$$

et

$$\omega(x) \equiv \frac{x^2-1}{8} \pmod 2 = \begin{cases} \bar{0} & \text{si } x \equiv \pm 1 \pmod 8 \\ \bar{1} & \text{si } x \equiv \pm 5 \pmod 8 \end{cases}$$

On suppose ici : $v_2(a) = v_2(b) = 0$.

i) Montrer que si $a \equiv b \equiv 3 \pmod 4$, alors $S(a,b) = -1$.
(*Indication : On pourra regarder la réduction de la forme quadratique* $f_{a,b}$ *dans* $\mathbb{Z}/4\mathbb{Z}$.)

ii) Montrer que si $a \equiv 1 \pmod 4$, alors $S(a,b) = +1$.
(*Indication : étudier plusieurs cas en regardant* $f_{a,b}$ *dans* $\mathbb{Z}/8\mathbb{Z}$ *et utiliser le lemme de Hensel.*)

iii) En déduire : $S(a,b) = (-1)^{\varepsilon(a)\varepsilon(b)}$.

11) On suppose toujours $\mathrm{K} = \mathbb{Q}_2$ avec cette fois-ci $v_2(a) = 1$ et $v_2(b) = 0$.

i) Déterminer les carrés de $\mathbb{Z}/8\mathbb{Z}$.

ii) Montrer que $x \in (\mathbb{Z}_2^\times)^2$ si et seulement si $x \equiv 1 \pmod 8$.

iii) Montrer que s'il existe une solution non triviale $z^2 - 2y^2 - bx^2 = 0$, alors $b \equiv \pm 1 \pmod 8$.

iv) En déduire : $S(2,b) = (-1)^{\omega(b)}$.

v) Montrer que si $S(a_2, b) = S(2, b) = -1$, alors $S(a, b) = 1$, puis en déduire le formule :

$$S(a, b) = S(2, b)S(a_2, b).$$

(*Indication : On pourra utiliser le point (iv) de la question 3).*)

vi) En déduire : $S(a, b) = (-1)^{\varepsilon(a_2)\varepsilon(b)+\omega(b)}$.

12) Sur $\mathbb{Q}_2$, en déduire la formule générale :

$$S(a, b) = (-1)^{\varepsilon(a_2)\varepsilon(b_2)+v_2(a)\omega(b_2)+v_2(b)\omega(a_2)},$$

puis que S est une forme bilinéaire symétrique non-dégénérée (sur $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$).

13) Soient $a, b \in \mathbb{Q}^*$. Notons par S_∞ l'application sur $\mathbb{R}^\times \times \mathbb{R}^\times$ à valeurs dans ± 1 (définie au début du devoir) associée à la forme quadratique $f_{a,b}$. Pour p un nombre premier, nous notons par S_p l'application sur $\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times$ à valeurs dans ± 1 associée à la forme quadratique $f_{a,b}$.

i) Montrer qu'à l'exception d'un nombre fini de nombres premiers p, $S_p(a, b) = 1$.

ii) Montrer la "formule du produit"

$$S_\infty(a, b) \prod_p S_p(a, b) = 1.$$

(*Indication : On pourra se souvenir que* $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$.)

Université de Franche-Comté - UFR Sciences et Techniques
Master 2 Mathématiques et Applications - CTU
Année 2013-2014

Le document "Théorie des Nombres" et les calculatrices sont autorisés.

Problème 1.

Les éléments considérés sont vus dans le corps des complexes $\mathbb{C}$.

Soit le polynôme $P = X^3 - 7 \in \mathbb{Q}[X]$ et soit θ une *racine réelle* de P. Posons $\mathrm{K} = \mathbb{Q}(\theta)$.
Soit $\mathcal{O}$ l'anneau des entiers de K et soit Cl le groupe des classes de K.

Préliminaires

1) Déterminer le degré de l'extension $\mathrm{K}/\mathbb{Q}$.

2) Déterminer la signature du corps K.

3) Soit $y = a + b\theta + c\theta^2$ un élément de K, avec $a, b, c \in \mathbb{Q}$. Soit l'endomorphisme de K

$$\begin{array}{rccc} \varphi_y : & \mathrm{K} & \to & \mathrm{K} \\ & x & \mapsto & xy \end{array}$$

a) Exprimer la matrice de l'endomorphisme φ_x dans la $\mathbb{Q}$-base $(1, \theta, \theta^2)$.
b) Pour $y \in \mathrm{K}$, déterminer la trace $T(y)$ de y dans $\mathrm{K}/\mathbb{Q}$.
c) Pour $y \in \mathrm{K}$, déterminer la norme $N(y)$ de y dans $\mathrm{K}/\mathbb{Q}$.

Recherche d'une base d'entiers

4) Soit $A = \mathbb{Z}[\theta]$. Calculer le discriminant de A.

5) En déduire que tout élément x de $\mathcal{O}$ s'écrit

$$x = \frac{a}{3^{\alpha}7^{\beta}} + \frac{b}{3^{\alpha'}7^{\beta'}}\theta + \frac{c}{3^{\alpha''}7^{\beta''}}\theta^2,$$

avec $\alpha, \beta, \alpha', \beta', \alpha'', \beta'' \leq 1$, $a, b, c \in \mathbb{Z}$, $(abc, 21) = 1$.

6) En utilisant le fait que $N(x) \in \mathbb{Z}$, montrer que $\alpha, \beta, \alpha', \beta', \alpha'', \beta'' \leq 0$. En déduire que $\mathcal{O} = \mathbb{Z}[\theta]$.

Détermination du groupe des classes Cl *de* K

7) Soit l'idéal principal $(\theta) = \theta\mathcal{O}$. Montrer que (θ) est l'unique idéal premier $\mathfrak{p}_7$ de $\mathcal{O}$ au-dessus de 7 : (θ) est maximal et $(\theta) \cap \mathbb{Z} = 7\mathbb{Z}$.
Quel est le degré résiduel de $\mathfrak{p}_7$? Que vaut la norme de $\mathfrak{p}_7$?

8) Montrer que $3\mathcal{O} = \mathfrak{p}_3^3$, où $\mathfrak{p}_3$ est un idéal premier de $\mathcal{O}$. Quel est le degré résiduel de $\mathfrak{p}_3$? Que vaut la norme de $\mathfrak{p}_3$?

9) Montrer que $\mathfrak{p}_3$ est principal si et seulement si, il existe $a, b, c \in \mathbb{Z}$ tels que

$$3 = a^3 + 7b^3 + 49c^3 - 21abc.$$

Après avoir déterminé les cubes dans $\mathbb{Z}/7\mathbb{Z}$, montrer que l'équation précédente n'a pas de solution dans $\mathbb{Z}/7\mathbb{Z}$. Conclusion ?

10) Que vaut l'ordre de la classe de $\mathfrak{p}_3$ dans le groupe des classes Cl de K ?

11) Montrer qu'il existe deux idéaux premiers $\mathfrak{p}_2$ et $\mathfrak{p}_2'$ au-dessus de 2, de norme respective 2 et 4, tels que $2\mathcal{O} = \mathfrak{p}_2\mathfrak{p}_2'$.

12) Montrer que $\mathfrak{p}_2$ et $\mathfrak{p}_2'$ ne sont pas principaux.

13) Quel est l'ordre de la classe de $\mathfrak{p}_2$ dans Cl ?

14) Montrer qu'il existe deux idéaux premiers $\mathfrak{p}_5$ et $\mathfrak{p}_5'$ au-dessus de 5, de norme respective 5 et 25, tels que $5\mathcal{O} = \mathfrak{p}_5\mathfrak{p}_5'$.

15) Montrer que $\mathfrak{p}_5$ et $\mathfrak{p}_5'$ ne sont pas principaux.

16) Calculer $N(2+\theta)$ puis factoriser l'idéal $(2+\theta)\mathcal{O}$.

17) Factoriser l'idéal $(1-\theta)\mathcal{O}$.

18) En déduire que Cl est cyclique d'ordre 3 engendré par la classe de $\mathfrak{p}_2$.

Problème 2.

Soit p un nombre premier. Soit $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ en p muni de la valeur absolue p-adique normalisée $|.| : |p| = 1/p$.
Soit $\overline{\mathbb{Q}_p}$ une clôture algébrique de $\mathbb{Q}_p$.

On rappelle que la valeur absolue p-adique $|.|$ se prolonge en une unique valeur absolue à tout $\overline{\mathbb{Q}_p}$.

Partie A.

1) Soient α et β deux éléments de $\overline{\mathbb{Q}_p}$. Soient $\alpha_1, \cdots, \alpha_r$ les $\mathbb{Q}_p$-conjugués de α, avec $\alpha_1 = \alpha$.
Dans cette partie, on suppose que les conjugués de α vérifient pour $i \geq 2$:

$$|\beta - \alpha| < |\alpha_i - \alpha|.$$

Soit $\mathrm{K} = \mathbb{Q}_p(\beta)$ et supposons que $\alpha \notin \mathrm{K}$.

a) Montrer l'existence d'un conjugé α_{i_0} de α, $\alpha_{i_0} \neq \alpha$, et d'un isomorphisme $\sigma : \mathrm{K}(\alpha) \to \mathrm{K}(\alpha_{i_0})$ vérifiant $\sigma(\alpha) = \alpha_{i_0}$ et dont la restriction à K est l'identité.

b) Montrer que $|\beta - \alpha_{i_0}| = |\beta - \alpha|$.

c) Montrer que $|\alpha - \alpha_{i_0}| \leq |\beta - \alpha|$.

d) En déduire que $\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$.

Partie B.

Soient $P = \sum_{k=1}^{r} a_k X^k$ et $Q = \sum_{k=1}^{s} b_k X^k$ deux polynômes à coefficients dans $\mathbb{Q}_p$.
On définit la distance entre les polynômes P et Q par :

$$|P - Q| = \max_k |a_k - b_k|,$$

avec la convention que si $k > r$ (respectivement $k > s$), $a_k = 0$ (resp. $b_k = 0$).

Si $P = \sum_n a_n X^n \in \mathbb{Q}_p[X]$, alors $|P| = |P - 0| = \max_k |a_k|$.

2) Soit β une racine du polynôme $Q = X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0 \in \mathbb{Q}_p[X]$.

Donner une constante C (exprimée en fonction des coefficients de Q) telle que $|\beta| \leq C$. (Pour la suite, on s'assure que $C \geq 1$).

3) Soient $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Q}_p[X]$ et $Q = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in \mathbb{Q}_p[X]$.
On suppose le polynôme P séparable : les racines α_i de P son simples.
Soit β une racine de Q.

a) Montrer que $|P(\beta)| \leq |P - Q|C^n$.

b) Soit $m = \min_{i \neq j} |\alpha_i - \alpha_j|$. Montrer qu'il existe au plus un entier i tel que

$$|\beta - \alpha_i| < m.$$

c) En utilisant la question 3-a), montrer que si $|P - Q|$ est suffisament petit, alors pour $i = 1, \cdots, n$, il existe une unique racine β_i de Q telle $|\beta_i - \alpha_i| \leq m$.

d) En déduire le résultat suivant : Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}_p[X]$ séparable. Pour tout $\varepsilon > 0$, il existe $\delta > 0$ tel que pour tout polynôme $Q \in \mathbb{Q}_p[X]$ unitaire et de degré n, avec $|P - Q| < \delta$, et pour toute racine α_i de P, il existe une unique racine β_i de Q telle que $|\alpha_i - \beta_i| \leq \varepsilon$.

Partie C.

4) Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Q}_p[X]$ un polynôme irréductible. Soit α une racine de P. Soit $Q = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in \mathbb{Q}_p[X]$.
Si $|P - Q|$ est suffisament petit, montrer que Q est irréductible et qu'il existe une racine β de Q telle que $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$.

5) Soit $\mathrm{K}/\mathbb{Q}_p$ une extension de degré n. Montrer qu'il existe un polynôme $Q \in \mathbb{Z}[X]$ unitaire, irréductible, de degré n et une racine $\theta \in \overline{\mathbb{Q}_p}$ de Q tels que $\mathrm{K} = \mathbb{Q}_p(\theta)$.

Université de Franche-Comté
Master 2 Mathématiques et Applications
CTU
Année 2014-2015
Théorie Algébrique des Nombres

Cours et calculatrice autorisés

Exercice 1.

Soit le corps de nombres $\mathrm{K} = \mathbb{Q}(\theta)$, où θ est une racine du polynôme $P = X^2 + 210 \in \mathbb{Q}[X]$.

On notera par $\mathcal{O}$ l'anneau des entiers de K.

1) Déterminer une $\mathbb{Z}$-base de l'anneau des entiers $\mathcal{O}$ de K. En déduire le discriminant $\mathrm{d_K}$ de K.

2) Déterminer le groupe des inversibles de l'anneau $\mathcal{O}$.

3) a) Déterminer la décomposition de $2\mathcal{O}$, de $3\mathcal{O}$, de $5\mathcal{O}$ et de $7\mathcal{O}$. Pour $i = 2, 3, 5, 7$, montrer l'existence d'idéaux $\mathfrak{p}_i$ entiers de norme i. Donner la factorisation de l'idéal $\theta\mathcal{O}$ en produit d'idéaux premiers.
b) Déterminer la décomposition de $11\mathcal{O}$, $13\mathcal{O}$ et de $17\mathcal{O}$.

Soit Cl le groupe des classes de $\mathcal{O}$. Si $\mathfrak{a}$ désigne un idéal de $\mathcal{O}$, on notera par $\mathrm{Cl}(\mathfrak{a})$ la classe de $\mathfrak{a}$ dans Cl.

4) Pour $i = 2, 3, 5, 7$, déterminer l'ordre de $\mathrm{Cl}(\mathfrak{p}_i)$.

5) Montrer que toute classe d'idéaux de Cl contient un idéal entier de norme plus petite que 18.

6) Déterminer la structure de Cl.

Exercice 2.

Pour un corps K de caractéristique 0, nous noterons par i une racine de $X^2 = -1$ dans $\overline{\mathrm{K}}$ une clôture algébrique fixée de K et par $\sqrt{2}$ une racine de $X^2 - 2$ dans $\overline{\mathrm{K}}$.

1) Soit K un corps de caractéristique 0. Calculer $(1+i)^2$. En déduire que si K contient ou bien i, ou bien $\sqrt{2}$, ou bien $i\sqrt{2}$, alors $16 \in \mathrm{K}^8$ (ou encore que 16 est une puissance 8-ème dans K).

2) a) Pour $u \in \mathbb{Z}_2$ avec $u \equiv 1 (\mathrm{mod}\ 8)$, soit le polynôme $P(X) = X^2 - u \in \mathbb{Z}_2[X]$. Montrer que P est réductible sur $\mathbb{Q}_2$.

b) Soit $\sqrt{7}$ une racine de $X^2 - 7 = 0$ dans $\overline{\mathbb{Q}_2}$. Montrer que $\mathbb{Q}_2(i) = \mathbb{Q}_2(\sqrt{7})$. En déduire que 16 est une puissance 8-ème dans $\mathbb{Q}_2(\sqrt{7})$.

c) Soit p un nombre premier impair. Montrer que $\mathbb{Q}_p$ contient ou bien i, ou bien $\sqrt{2}$, ou bien $i\sqrt{2}$.
(Indication : utiliser le symbole de Kronecker et le lemme de Hensel.)

d) Conclure que pour tout nombre premier p, l'entier 16 est une puissance 8-ème dans $\mathbb{Q}_p(\sqrt{7})$.

3) Soit $\mathrm{K} = \mathbb{Q}(\sqrt{7})$. Montrer que $16 \notin \mathrm{K}^8$.

Exercice 3.

Partie A.
Soit le corps fini $\mathbb{F}_q$ à $q = p^t$ éléments et soit $n > 1$.
On rappelle que l'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est une extension cyclique de degré n engendrée par l'automorphisme de Frobenius σ défini par $\sigma(z) = z^q$.

Désignons par $T : \mathbb{F}_{q^n} \to \mathbb{F}_q$ la trace de l'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ et par $N : \mathbb{F}_{q^n} \to \mathbb{F}_q$ l'application norme de l'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. On rappelle que l'application norme restreinte aux groupes multiplicatifs $\mathbb{F}_{q^n}^\times$ et $\mathbb{F}_q^\times$ est un morphisme de groupes.

1) Montrer que l'application linéaire T est surjective.
(Indication. Utiliser le lemme d'indépendance de Dedekind.)

2) Soit $z \in \mathbb{F}_{q^n}$. Montrer que $N(z) = 1$ si et seulement si, il existe $y \in \mathbb{F}_q$ tel que $z = \sigma(y)/y$.
(Indication. Pour un sens de l'équivalence, on pourra montrer l'existence d'un élément $x \in \mathbb{F}_{q^n}$ tel que

$$y := x + z\sigma(x) + \cdots + \left[z\sigma(z)\cdots\sigma^{n-2}(z)\sigma^{n-1}(x)\right] \neq 0.)$$

3) On considère le morphisme de groupes $N : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ et soit le morphisme $\varphi : \mathbb{F}_{q^n}^\times \to \mathbb{F}_{q^n}^\times$ défini par $\varphi(y) = \sigma(y)/y$.

a) Déterminer $\ker(\varphi)$.

b) Déterminer $|\ker(N)|$.

c) En déduire que la norme N est surjective.

Partie B.

Soit $\mathrm{K}/\mathbb{Q}_p$ une extension finie. Soit $\mathcal{O}_\mathrm{K}$ l'anneau des entiers p-adiques de K : l'anneau $\mathcal{O}_\mathrm{K}$ est la fermeture intégrale de $\mathbb{Z}_p$ dans K ; c'est aussi l'ensemble des éléments de K qui sont entiers sur $\mathbb{Z}_p$.
Notons par π une uniformisante de $\mathcal{O}_\mathrm{K}$. Le corps résiduel F_K de K est le corps fini $\mathcal{O}_\mathrm{K}/(\pi) \simeq \mathbb{F}_q$.

Pour un entier $i \geq 1$, soit

$$\mathcal{U}_\mathrm{K}^{(i)} := \{\varepsilon \in \mathcal{O}_\mathrm{K}^\times,\ \varepsilon \equiv 1 (\mathrm{mod}\ \pi^i)\}.$$

4) Montrer que les ensembles $\mathcal{U}_\mathrm{K}^{(i)}$ sont des sous-groupes de $\mathcal{O}_\mathrm{K}^\times$.

5) Montrer que le quotient $\mathcal{O}_\mathrm{K}^\times/\mathcal{U}_\mathrm{K}^{(1)}$ est isomorphe au groupe multiplicatif $\mathrm{F}_\mathrm{K}^\times$.

6) Soit $i \geq 1$. Pour $x \in \mathcal{U}_\mathrm{K}^{(i)}$, $x = 1+\pi^i u$ avec $u \in \mathbb{Z}_p$, on définit $\theta(x) \in \mathrm{F}_\mathrm{K}$ par $\theta(x) := u \pmod{\pi}$.
Montrer que θ induit un isomorphisme entre $\mathcal{U}_\mathrm{K}^{(i)}/\mathcal{U}_\mathrm{K}^{(i+1)}$ et le groupe additif $(\mathrm{F}_\mathrm{K}, +)$.

Soit L/K une extension non ramifiée de degré n.
Notons par $N : \mathrm{L}^\times \to \mathrm{K}^\times$ la norme de l'extension galoisienne L/K.

7) Quel est le degré de l'extension $\mathrm{F_L/F_K}$? Donner une uniformisante de L.

8) Montrer que pour tout entier $i \geq 1$, il vient $N(\mathcal{U}_{\mathrm{L}}^{(i)}) \subset \mathcal{U}_{\mathrm{K}}^{(i)}$.

9) Montrer que pour tout $i \geq 1$, la norme N induit un isomorphisme entre $\mathcal{U}_{\mathrm{L}}^{(i)}/\mathcal{U}_{\mathrm{L}}^{(i+1)}$ et $\mathcal{U}_{\mathrm{K}}^{(i)}/\mathcal{U}_{\mathrm{K}}^{(i+1)}$.
(Indication. Utiliser la question 1) de la partie A.)

10) Montrer que la norme N induit un isomorphisme entre $\mathcal{O}_L^{\times}/\mathcal{U}_{\mathrm{L}}^{(1)}$ et $\mathcal{O}_{\mathrm{K}}^{\times}/\mathcal{U}_{\mathrm{K}}^{(1)}$.
(Indication. Utiliser la question 3) de la partie A.)

11) Montrer que toute unité x de $\mathcal{O}_{\mathrm{K}}$ est norme dans l'extension L/K : il existe $y \in \mathcal{O}_{\mathrm{L}}^{\times}$, telle que $N(y) = x$.
