THEORIE DES NOMBRES

Denis Benois

Bibliographie

[K] N. Koblitz, *p-adic numbers, p-adic analysis and zeta-functions*, (second edition) Springer, 1984.
[L] S. Lang, *Algèbre*, (3-ième édition révisée) Dunod, Paris, 2004.
[S] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967.

CHAPITRE 0. PRELIMINAIRES

§1. Anneaux et modules

1.1. Anneaux.

DÉFINITION. *Soit A un anneau. On dit que A est*
• *commutatif, si pour tout $a, b \in A$ on a*

$$ab = ba;$$

• *unitaire, s'il existe un élément $1 \in A$ tel que $a \cdot 1 = 1 \cdot a = a$ pour tout $a \in A$;*
• *intègre, si le produit de deux éléments non nuls quelconques de A est non nul, i.e. si*

$$ab = 0 \Rightarrow a = 0 \text{ ou } b = 0\,.$$

Dans ce cours "anneau" veut dire anneau commutatif unitaire.
On dit qu'un élément $u \in A$ est une unité s'il est inversible i.e. s'il existe $u^{-1} \in A$ tel que $uu^{-1} = 1$. Les unités de A forment un groupe pour la multiplication qu'on note $U(A)$ ou A^*.

Exemples. 1) Soit K un corps. Alors, tout élément non-nul $a \in K$ est inversible et on a $K^* = K - \{0\}$. Le groupe K^* est appelé le groupe multiplicatif de K.
2) Soit $\mathbb{Z}$ l'anneau des entiers. Alors $U(\mathbb{Z}) = \{1, -1\}$.
3) Soient K un corps et $K[X]$ l'anneau des polynômes à coéfficients dans K. Il est facile de voir que $U(K[X]) = K^*$.

DÉFINITION. *Soit A un anneau. On dit que $\mathfrak{a}A \subseteq A$ est un idéal de A, si $\mathfrak{a}$ vérifie les propriétés suivantes:*
i) Pour tous $x, y \in \mathfrak{a}$ on a $x \pm y \in \mathfrak{a}$;
ii) Si $a \in A$ et $x \in \mathfrak{a}$, alors $ax \in \mathfrak{a}$.

Donc, un idéal de A est un sous-groupe additif $\mathfrak{a} \subseteq A$ tel que $a \in A$ et $x \in \mathfrak{a}$ implique $ax \in \mathfrak{a}$.

Exemples. 1) Soit $a \in A$. Posons

$$(a) = aA = \{ax \,|\, x \in A\}.$$

Alors, (a) est un idéal de A appelé l'idéal principal engendré par a.
2) Plus généralement, si $a_1, \ldots, a_n \in A$, alors l'ensemble

$$(a_1, \ldots, a_n) \,=\, \{x_1a_1 + \ldots + x_na_n \,|\, x_i \in A\}$$

est un idéal de A appelé l'idéal engendré par $a_1, \ldots, a_n$.
3) Soit K un corps. Les seuls idéaux de K sont $\{0\}$ et K.

Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de A. Alors, l'ensemble $\mathfrak{a} + \mathfrak{b}$ défini par

$$\mathfrak{a} + \mathfrak{b} = \{a + b \,|\, a \in \mathfrak{a},\, b \in \mathfrak{b}\}$$

est un idéal de A appelé somme des idéaux $\mathfrak{a}$ et $\mathfrak{b}$. On définit la produit $\mathfrak{ab}$ comme l'idéal engendré par tous les produits ab avec $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, i.e.

$$\mathfrak{ab} = \{\sum_i a_i b_i \,|\, a_i \in \mathfrak{a},\, b_i \in \mathfrak{b}\}.$$

On montre 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 de A, alors $\mathfrak{a} \cap \mathfrak{b}$ l'est aussi et

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

Définition. *Deux idéaux $\mathfrak{a}, \mathfrak{b} \subseteq A$ sont dits premiers entre eux (ou étrangérs) si*

$$\mathfrak{a} + \mathfrak{b} = (1)\,(= A)\,.$$

En particulier, deux idéaux principaux (a) et (b) sont premiers entre eux si et seulement s'il existe des éléments $x, y \in A$ tels que

$$ax + by = 1,$$

i.e. si 1 est un de leurs p.g.c.d..

iii) Si $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux, alors

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

Preuve. Supposons que $\mathfrak{a} + \mathfrak{b} = A$. Alors il existe $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $1 = a + b$. Si $x \in \mathfrak{a} \cap \mathfrak{b}$, alors

$$x = x \cdot 1 = xa + xb \in \mathfrak{ab} + \mathfrak{ab} = \mathfrak{ab},$$

d'où $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$. Comme l'inclusion $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$ est toujours vraie, on obtient $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

Définition. *Soit $\mathfrak{a}$ un idéal de A. On dit que deux éléments $a, b \in A$ sont congrus modulo $\mathfrak{a}$ si $a - b \in \mathfrak{a}$; notation*

$$a \equiv b \pmod{\mathfrak{a}}\,.$$

Pour tout $a \in A$ on pose $\bar{a} = \{x \in A | x \equiv a \pmod{\mathfrak{a}}\}$. Il est facile de voir que $\bar{a} = a + \mathfrak{a} = \{a + y | y \in \mathfrak{a}\}$ et que deux éléments a et b engendrent la même classe si et seulement si $a \equiv b \pmod{\mathfrak{a}}$. Les classes d'équivalences forment un anneau, appelé anneau quotient de A par $\mathfrak{a}$; notation:

$$A/\mathfrak{a} = \{\bar{a} = a + \mathfrak{a}, \,|\, a \in A\}.$$

Le lemme suivant est très utile pour étuduer les anneaux quotients.

LEMME 0.1.1 (DIT CHINOIS).*Soient* $\mathfrak{a}$ *et* $\mathfrak{b}$ *des idéaux de* A *qui sont premiers entre eux. Alors l'application*

$$f \ : \ A/\mathfrak{ab} \to (A/\mathfrak{a}) \times (A/\mathfrak{b}),$$
$$f(x+\mathfrak{ab}) = (x+\mathfrak{a}, x+\mathfrak{b})$$

est un isomorphisme.

PREUVE. (voir, par exemple, [L], p.101). Comme $\mathfrak{ab} \subseteq \mathfrak{a}, \mathfrak{b}$, l'application f est bien définie et il est facile de voir qu'elle 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, $x \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, d'où $x+\mathfrak{ab} = \mathfrak{ab} = \bar{0}_{A/\mathfrak{ab}}$.

Montrons maintenant que f est surjective. Comme $\mathfrak{a}+\mathfrak{b} = (1)$, 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

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

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 antécedant dans $A/\mathfrak{ab}$ et f est surjective.

Par récurrence, on obtient:

PROPOSITION 0.1.2. *Soit* $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ *une famille d'idéaux de* A *tels que* $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ *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

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

Si on applique cette proposition à l'anneau $\mathbb{Z}$, on obtient le corpollaire suivant:

COROLLAIRE 0.1.3. *Soit* $n_1, \ldots, n_k$ *une famille d'entiers tels que* $(n_i, n_j) = 1$ *si* $i \neq j$ *et soit* $n = n_1 n_2 \ldots n_k$. *Alors*

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_k\mathbb{Z}.$$

En particulier, si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est la factorisation de n en facteurs premiers, alors on a

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

DÉFINITION. *Soit* A *un anneaux.*

i) On dit qu'un idéal $\mathfrak{p}$ *est premier, si et seulement si l'anneau* $A/\mathfrak{p}$ *est intègre, i.e. si*

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

ii) On dit qu'un idéal $\mathfrak{m}$ *est maximal, si et seulement si* $\mathfrak{m} \neq A$ *et il n'y a pas d'idéaux* $\mathfrak{a}$ *vérifiant*

$$\mathfrak{m} \subset \mathfrak{a} \subset A$$

(rappelons que les inclusions sont strictes).

PROPOSITION 0.1.4. *Soit A un anneau commutatif unitaire. Alors*
i) Un idéal $\mathfrak{m} \subset A$ est maximal si et seulement si $A/\mathfrak{m}$ est un corps;
ii) Tout idéal maximal est premier;
iii) Pour tout idéal $\mathfrak{a} \neq A$ il existe un idéal maximal $\mathfrak{m}$ contenant $\mathfrak{a}$.

PREUVE. Voir [L], p.100.

COROLLAIRE 0.1.5. *Soit $a \in A$ un élemént tel que $a \notin \mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$ de A. Alors, $a \in U(A)$.*

PREUVE. Supposons que $a \notin U(A)$. Alors, $(a) \neq A$ et il existe un idéal maximal $\mathfrak{m}$ tel que $(a) \subseteq \mathfrak{m}$.

Soit $f : A \to B$ un homomorphisme d'anneaux. Si $\mathfrak{a}$ est un idéal de A, alors on note $f(\mathfrak{a})B$ ou tout simplement $\mathfrak{a}B$ l'idéal de B engendré par $f(\mathfrak{a})$. Si $\mathfrak{b}$ est un idéal de B, alors son image réciproque $f^{-1}(\mathfrak{b})$ est un idéal de A.

PROPOSITION 0.1.6. *Si $\mathfrak{q}$ est un idéal premier de B, alors $\mathfrak{p} = f^{-1}(\mathfrak{q})$ est un idéal premier de A.*

PREUVE. Si $ab \in \mathfrak{p}$, alors $f(a)f(b) = f(ab) \in \mathfrak{q}$. Comme $\mathfrak{q}$ est premier, on a $f(a) \in \mathfrak{q}$ ou $f(b) \in \mathfrak{q}$, d'où $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

En particulier, si $A \subset B$ et $\mathfrak{q} \subset B$ est premier, alors $\mathfrak{p} = \mathfrak{b} \cap A$ est premier dans A.

1.2. Modules.

DÉFINITION. *Soit A un anneau. On appelle module sur A (ou A-module) un groupe abélien M muni d'une action de A*

$$A \times M \to M$$
$$(a, m) \mapsto am$$

vérifiant les propriétés suivantes:
i) $\forall m_1, m_2 \in M$ et $\forall a \in A$ on a

$$a(m_1 + m_2) = am_1 + am_2;$$

ii) $\forall a, b \in A$ et $\forall m \in M$ on a

$$(a + b)m = am + bm;$$

iii) $\forall a, b \in A$ et $\forall m \in M$ on a

$$(ab)m = a(bm);$$

iv) Pour tout $m \in M$ on a

$$1 \cdot m = m.$$

Exemples. 1) Si $A = K$ est un corps, alors la définition d'un K-modules coïncide avec la définition d'un espace vectoriel sur K. Donc,

$$\{K - modules\} \ = \ \{K - espaces\ vectoriels\}.$$

2) Soit $A = \mathbb{Z}$. Tout groupe abélien M peut être vu comme un $\mathbb{Z}$-module si pour tous $a \in \mathbb{Z}$ et $m \in M$ on pose

$$a \cdot m = \begin{cases} \underbrace{m + \cdots + m}_{a\ fois}, & \text{si } a > 0 \\ 0, & \text{si } a = 0 \\ -(\underbrace{m + \cdots + m}_{-a\ fois}), & \text{si } a < 0. \end{cases}$$

Donc,

$$\{\mathbb{Z} - modules\} \ = \ \{groupes\ abéliens\}.$$

3) Un idéal $\mathfrak{a}$ de A est un A-module;
4) Soit $n \geqslant 1$ et soit

$$A^{(n)} = \underbrace{A \times \cdots \times A}_{n\ fois}.$$

On munit $A^{(n)}$ d'une action de A en posant

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n).$$

Alors $A^{(n)}$ est un A-module.

Définition. *On dit qu'un A-module L est libre de rang n s'il est isomorphe à $A^{(n)}$.*

Définition. *Soit M un A-module. On dit que M est de type fini si et seulement si il admet un système générateur fini i.e. s'il existent $m_1, \ldots, m_n \in M$ tels que*

$$M \ = \ A\,m_1 \ + \ \ldots + \ A\,m_n\,.$$

Proposition 0.1.7. *Soit M un A-module de type fini. Alors, il existe un A-module libre L de rang fini et un sous-module $N \subseteq L$ tels que M soit isomorphe à L/N.*

Preuve. Voir [L], §3.4, p.145.

1.3. Anneaux noethériens.

Définition. *On dit q'un anneau A est noethérien, si tout suite croissante d'idéaux de A*

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

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

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

PROPOSITION 0.1.8. *Les assertions suivantes sont équivalentes:*
i) A est noethérien;
ii) Tout idéal $\mathfrak{a}$ de A est de type fini (i.e. engendé par une famille finie d'éléments).

PREUVE. *i)* $\Rightarrow$ *ii)*. 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 strictement croissante:

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

Comme A est noethérien, cette suite est finie, ce qui signifie qu'il existe n tel que $\mathfrak{a}_n = \mathfrak{a}$.
ii) $\Rightarrow$ *i)*. Soit

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

une suite d'idéaux de A. Alors $\mathfrak{a} = \cup_{i=1}^{\infty} \mathfrak{a}_i$ est un idéal (exercice). Si tout idéal de A est de type fini, alors il existe $a_1, \dots a_k \in A$ tels que $\mathfrak{a} = (a_1, \dots, a_k)$. Donc, 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,

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

La proposition est démontrée.

THÉORÈME 0.1.9. *Soit M un A-module de type fini. Si A est noethérien, alors tout sous-module de M est de type fini.*

PREUVE. Voir [S], §§1.4 et 3.1.

Un exemple important est donné par le théorème suivant:

THÉORÈME 0.1.10 (HILBERT).*Si A est un anneau noethérien, alors pour tout $n \geqslant 1$ l'anneau des polynômes $A[X_1, \dots X_n]$ l'est aussi.*

PREUVE. Voir [L], §4.4, p.194.

§2. Extensions algébriques

2.1. Extensions algébriques.

Le but de ce paragraphe est de rappeler quelques résultats sur les extensions algébriques des corps. Soient K et L deux corps. On dit que L est une extension de K si $K \subseteq L$; notation L/K. Dans ce cas, L peut être vu comme un espace vectoriel sur K. Sa dimension $[L : K]$ s'appelle le degré de L/K. On dit que l'extension L/K est finie si $[L : K] \leq \infty$ i.e. si L est de dimension finie sur K.

THÉORÈME 0.2.1. *Si L/K et M/L sont deux extensions finies, alors M/K l'est aussi et on a*

$$[M : K] = [M : L]\,[L : K]\,.$$

PREUVE. Voir [L],§5.1 , p.234 ou[S], chapitre I, §2.3.

Soit L/K une extension de corps. On dit que $\alpha \in L$ est algébrique sur K s'il existe un polynôme non-nul $F(X) \in K[X]$ tel que $F(\alpha) = 0$. Si α n'est pas algébrique, on dit qu'il est transcendant sur K.

PROPOSITION 0.2.2. *Si $\alpha \in L$ est algébrique sur K, alors il existe un unique polynôme unitaire irréductible $f(X) \in K[X]$ vérifiant les propriétés suivantes:*
i) $f(\alpha) = 0$;
ii) Si $F(X) \in K[X]$ est un polynôme vérifiant $F(\alpha) = 0$, alors $f(X)$ divise $F(X)$.

PREUVE. Voir [L], §5.1, p.234.

DÉFINITION. *Le polynôme $f(X)$ vérifiant les conditions i) et ii) de la proposition 2.1 est appelé le polynôme minimal de α (sur K).*

Si $\alpha_1, \dots, \alpha_n \in L$, on appelle extension engendrée par $\alpha_1, \dots, \alpha_n$ et on note $K(\alpha_1, \dots, \alpha_n)$ la plus petite extension de K contenant $\alpha_1, \dots, \alpha_n$. Il est facile de voir que $K(\alpha_1, \dots, \alpha_n)$ est formée par toutes les fractions

$$\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)},$$

où $f(X_1, \dots, X_n)$ et $g(X_1, \dots, X_n)$ sont des polynômes à coéfficients dans K et tels que $g(\alpha_1, \dots, \alpha_n) \neq 0$. Le théorème suivant donne la structure d'extensions $K(\alpha)/K$.

THÉORÈME 0.2.3. *i) Soit α un élément algébrique sur K. Soient $f(X)$ son polynôme minimal et $(f(X))$ l'idéal principal de $K[X]$ engendré par $f(X)$. Alors l'application*

$$K[X] \to K(\alpha);$$
$$f(X) \mapsto f(\alpha)$$

induit un isomorphisme

$$K[X]/(f(X)) \simeq K(\alpha)\,.$$

En particulier, $K(\alpha)/K$ est finie de degré $n = deg(f(X))$ et les éléments $1, \alpha, \dots, \alpha^{n-1}$ forment une base de $K(\alpha)$ sur K.
ii) Si α est transcendant sur K, alors $K(\alpha)$ est isomorphe au corps $K(X)$ des fonctions rationnelles $g(X)/h(X)$, avec $g(X), h(X) \in K[X]$.

PREUVE. Voir [L],§5.1.

DÉFINITION. *On dit qu'une extension L/K est algébrique, si tout $\alpha \in L$ est algébrique sur K.*

Le lien entre les extensions algébriques et finies est donné par le théorème suivant:

THÉORÈME 0.2.4. *Toute extension finie est algébrique.*

PREUVE. Soit L/K une extension finie de degré n. Si $\alpha \in L$, alors $(n+1)$ éléments $1, \alpha, \alpha^2, \dots, \alpha^n$ sont liés sur K i.e.

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

avec $a_0, a_1, \dots, a_{n-1} \in K$. Donc, α est algébrique.

On déduit de ce théorème deux propriétés importantes d'extensions algébriques:
1) Si L/K et M/L sont algébriques, alors M/K l'est aussi.
2) Si L/K est finie, alors il existe une famille $\alpha_1, \dots, \alpha_m$ d'éléments algébriques tels que

$$L = K(\alpha_1, \dots, \alpha_m).$$

DÉFINITION. *On dit qu'un corps F est algébriquement clos, s'il n'a pas d'extensions algébriques non-triviales, i.e. si*

$$M/F \text{ algébrique } \Rightarrow M = F.$$

Exemple. Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos (théorème de Gauss).

On vérifie facilement que les assertions suivantes sont équivalentes:
i) F est algébriquement clos;
ii) Tout polynôme $f(X) \in F[X]$ de degré $\geqslant 1$ a une racine dans F.
iii) Tout polynôme $f(X) \in F[X]$ de degré $\geqslant 1$ se décompose en produit de polynômes de degré 1:

$$f(X) = a(X - \alpha_1) \cdots (X - \alpha_n).$$

iv) Tout polynôme irréductible sur F est de degré 1.

DÉFINITION. *Soit K un corps. On dit que $\bar{K}/K$ est une clôture algébrique de K si*
i) $\bar{K}/K$ est une extension algébrique;
ii) $K\bar{K}$ est algébriquement clos.

Exemple. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Le théorème suivant est fondamental:

THÉORÈME 0.2.5. *Soit K un corps. Alors, il existe une clôture algébrique $\bar{K}$ de K; cette clôture est unique à un isomorphisme près. Plus précisement, si $\tilde{K}$ est une autre clôture algébrique de K, alors il existe un isomorphisme*

$$\phi \ : \ \tilde{K} \to \bar{K},$$

tel que $\phi|_K = id_K$.

PREUVE. Voir [L], §5.2.

2.2. Extensions séparables.

On fixe une clôture algébrique $\bar{K}/K$. Soit L/K une extension finie de degré n. On note

$$\sigma_i \ : \ L/K \hookrightarrow \bar{K}/K, \qquad i = 1, \ldots, m$$

les K-homomorphismes de L dans $\bar{K}$ (i.e. $\sigma_i|_K = id_K$). On peut montrer que $m \leqslant n = [L : K]$.

DÉFINITION. *On dit qu'une extension L/K est séparable, si $m = n$ i.e. s'il existe $n = [L : K]$ homomorphismes de L dans $\bar{K}$ sur K.*

On montre d'abord un critère pour qu'une extension $K(\alpha)/K$ soit séparable.

PROPOSITION 0.2.6. *Une extension algébrique $K(\alpha)/K$ est séparable si et seulement si le polynôme minimal $f(X)$ de α est séparable i.e. si $(f(X), f'(X)) = 1$.*

PREUVE. Voir [L], §5.4.

Comme le polynome minimal $f(X)$ est irréductible et comme $deg(f'(X)) < deg(f(X))$, le polynôme $f(X)$ n'est pas séparable seulement si $f'(X)$ est nul. En particulier, si K est de caractéristique 0 (voir §4), alors $f'(X)$ est non-nul, donc dans ce cas toute extension $K(\alpha)/K$ est séparable. En caractéristique p un exemple typique d'un polynôme non-séparable est donné par $f(X) = X^p - a$.

Les propriétés principales d'extensions séparables découlent de la proposition suivante:

PROPOSITION 0.2.7. *Soient L/K une extension finie et*

$$\sigma \ : \ L/K \hookrightarrow \bar{K}/K$$

un K- homomorphisme de L dans $\bar{K}$. Si M/L est une extension séparable de degré n, alors il σ admet n prolongements sur M i.e. il existe n homomorphismes

$$\tau_i \ : \ M/K \hookrightarrow \bar{K}/K, \qquad i = 1, \dots, n$$

tels que $\tau_i|_L = \sigma$.

PREUVE. Voir [L], §5.4.

En utilisant cette proposition on montre les propriétés suivantes d'extensions séparables:

1) Soient L/K et M/L deux extensions algébriques. Alors M/K est séparable si et seulement si L/K et M/L sont séparables.

2) Si L/K est séparable, alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.

En composant 2) avec les remarques après la proposition 0.2.6 on obtient que en caractéristique 0 le problème de séparabilité ne se pose pas:

3) **Si K est de caractéristique 0, alors tout extension finie de K est séparable.**

2.3. Extensions galoisiennes.

DÉFINITION. *On dit qu'une extension finie L/K est normale, si tout homomorphisme*

$$\sigma \ : \ L/K \to \bar{K}/K$$

laisse L stable, i.e. si $\sigma(L) = L$ (ceci ne signifie pas que $\sigma|_L = id_L$!).

Donc, si L/K est normale, alors tout homomorphisme $\sigma \ : \ L/K \to \bar{K}/K$ est un automorphisme de L qui fixe K.

PROPOSITION 0.2.8. *Soit L/K une extension finie. Alors, les assertions suivantes sont équivalentes:*

i) L/K est normale;

ii) L est le corps de décomposition d'un polynôme à coéfficients dans K i.e. il existe $f(X) \in K[X]$ tel que $L = K(\alpha_1, \dots, \alpha_n)$, où $\alpha_1, \dots, \alpha_n$ sont les racines de $f(X)$.

PREUVE. Voir [L], §5.3, p.245-247.

DÉFINITION. *On dit qu'une extension L/K est galoisienne, si elle est normale et séparable.*

Soit L/K une extension galoisienne de degré n. Alors il existe n automorphismes de L qui fixent K. Ces automorphismes forment un groupe d'ordre n appelé le groupe de Galois de L/K et noté $Gal(L/K)$.

Rappelons les résultats principaux de la théorie de Galois.

THÉORÈME 0.2.9. *Soit L/K une extension galoisienne de groupe de Galois $G = Gal(L/K)$.*

i) Il existe une bijection entre l'ensemble des sous-corps E de L contenant K et l'ensemble des sous-groupes H de G donnée par $E = \{x \in L \,|\, \forall h \in H \text{ on a } h(x) = x\}$. L'extension L/E est galoisienne et le groupe de Galois $Gal(L/E)$ s'identifie à H.

ii) L'extension E/K est galoisienne si et seulement si H est un sous-groupe distingué dans G. Dans ce cas, l'application $\sigma \mapsto \sigma|_E$ induit un isomorphisme

$$Gal(E/K) \simeq G/H\,.$$

PREUVE. Voir [L], §6.1.

§3. Normes et traces

Soit L/K une extension finie de degré $n = [L : K]$. On fixe une base $\omega_1, \ldots, \omega_n\}$ de L sur K. Pour tout $\alpha \in L$ l'application "multiplication par α":

$$\begin{aligned} f_\alpha \;&:\; L \to L \\ f_\alpha(x) &= \alpha x \end{aligned}$$

est K-linéaire. Pour tout i le produit $\alpha\omega_i$ s'écrit:

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ji}\omega_i$$

avec $a_{ji} \in K$. Alors la matrice

$$M(\alpha) = (a_{ij})_{1 \leqslant i,j \leqslant n}$$

est la matrice de f_α dans la base $\omega_1, \ldots, \omega_n$. Soit

$$\chi_\alpha(X) = \det(XI_n - M(\alpha))$$

le polynôme caractéristique de f_α. Il est bien connu qu'il ne dépend pas du choix de la base. Posons

$$\chi_\alpha(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0.$$

DÉFINITION. *On définit la trace $Tr_{L/K}(\alpha)$ et la norme $N_{L/K}(\alpha)$ de α par les formules:*

$$Tr_{L/K}(\alpha) = -b_{n-1}$$
$$N_{L/K}(\alpha) = (-1)^n b_0 \,.$$

Voici quelques propriétés qui découlent directement de la définition:
i) $Tr_{L/K}(\alpha+\beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$;
ii) Si $\alpha \in K$ et $\beta \in L$, alors $Tr_{L/K}(\alpha+\beta) = \alpha Tr_{L/K}(\beta)$; En particulier, $Tr_{L/K}(\alpha) = n\alpha$.
iii) $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)\, N_{L/K}(\beta)$;
iv) Si $\alpha \in K$ et $\beta \in L$, alors $N_{L/K}(\alpha\beta) = \alpha^n N_{L/K}(\beta)$; En particulier, $N_{L/K}(\alpha) = \alpha^n$.

PROPOSITION 0.3.1. *Soit $L = K(\alpha)$ et soit*

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

le polynôme minimal de α. Alors

$$Tr_{L/K}(\alpha) = -a_{n-1},$$
$$N_{L/K}(\alpha) = (-1)^n a_0.$$

PREUVE. Les éléments $1, \alpha, \ldots, \alpha^{n-1}$ forment une base de L/K. Il est facile de voir que la matrice de f_α dans cette base est

$$M(\alpha) = \begin{pmatrix} 0 & 0 & \ldots & -a_0 \\ 1 & 0 & \ldots & -a_1 \\ 0 & 1 & \ldots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ \ldots & \ldots & \ldots & -a_{n-1} \end{pmatrix}.$$

On en déduit le résultat.

THÉORÈME 0.3.2. *Soit L/K une extension séparable de degré n. Alors pour tout $\alpha \in L$ on a*

$$Tr_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$
$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

où $\sigma_i : L/K \hookrightarrow \bar{K}/K$ sont les plongement de L dans $\bar{K}$ sur K.

PREUVE. Considérons d'abord le cas $L = K(\alpha)$. Soit $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ le polynome minimal de α. Comme L/K est séparable, on a

$$f(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha)),$$

d'où $a_{n-1} = -\sum_{i=1}^{n} \sigma_i(\alpha)$ et $a_0 = (-1)^n \prod_{i=1}^{n} \sigma_i(\alpha)$ et le théorème découle de la proposition précédente.

Dans le cas général, on considère la tour d'extensions $K \subset K(\alpha) \subset L$. Posons $m = [L : K(\alpha)$. N'utilisant que la définition il est facile de montrer (exercice) que

$$Tr_{L/K}(\alpha) = mTr_{K(\alpha)/K}(\alpha),$$
$$N_{L/K}(\alpha) = (N_{K(\alpha)/K}(\alpha))^m.$$

Tout plongement τ_i de $K(\alpha)/K$ dans $\bar{K}/K$ admet m prolongements différents σ_{ij} sur L. Donc,

$$Tr_{L/K}(\alpha) = -\sum_{i=1}^{n} m\tau_i(\alpha) = -\sum_{i=1}^{n} \sigma_{ij}(\alpha),$$
$$N_{L/K}(\alpha) = ((-1)^n \prod_{i=1}^{n} \tau_i(\alpha))^m = (-1)^{nm} \prod_{i=1}^{n} \sigma_{ij}(\alpha),$$

où σ_{ij} parcourt tous les plongements de L/K dans $\bar{K}/K$. Le théorème est démontré.

En utilisant les mêmes arguments on montre le théorème suivant:

THÉORÈME 0.3.3. *Soit $K \subset L \subset M$ une tour d'extensions finies. Alors, pour tout $\alpha \in M$ on a*

$$Tr_{M/K}(\alpha) = Tr_{L/K} \circ Tr_{M/L}(\alpha),$$
$$N_{M/K}(\alpha) = N_{L/K} \circ N_{M/L}(\alpha).$$

DÉFINITION. *Soit L/K une extension finie et soit $\{\omega_1, \dots, \omega_n\}$ une base de L/K. On appelle discriminant de $\{\omega_1, \dots, \omega_n\}$ et on note $D_{L/K}(\omega_1, \dots, \omega_n)$ le détérminant:*

$$\begin{vmatrix} Tr_{L/K}(\omega_1\omega_1) & Tr_{L/K}(\omega_1\omega_2) & \dots & Tr_{L/K}(\omega_1\omega_n) \\ Tr_{L/K}(\omega_2\omega_1) & Tr_{L/K}(\omega_2\omega_2) & \dots & Tr_{L/K}(\omega_2\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{L/K}(\omega_n\omega_1) & Tr_{L/K}(\omega_n\omega_2) & \dots & Tr_{L/K}(\omega_n\omega_n) \end{vmatrix}.$$

Il est clair, que si $\{\omega'_1, \dots, \omega'_n\}$ est une autre base de L/K avec la matrice de passage A, i.e. si

$$(\omega'_1, \dots, \omega'_n) = (\omega_1, \dots, \omega_n)A,$$

alors

$$D_{L/K}(\omega'_1, \dots, \omega'_n) = det(A)^2 D_{L/K}(\omega_1, \dots, \omega_n).$$

THÉORÈME 0.3.4. *Si L/K est séparable, alors*

$$D_{L/K}(\omega_1, \dots, \omega_n) \neq 0.$$

PREUVE. Soit

$$\Delta_{L/K}(\omega_1, \dots, \omega_n) = \begin{vmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \dots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \dots & \sigma_n(\omega_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \dots & \sigma_n(\omega_n) \end{vmatrix}.$$

En utilisant le théorème 0.3.2 et la formule $\det(AB) = \det(A)\det(B)$ on obtient que $D_{L/K}(\omega_1, \dots, \omega_n)$ est égal à

$$\begin{vmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \dots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \dots & \sigma_n(\omega_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \dots & \sigma_n(\omega_n) \end{vmatrix} \begin{vmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \dots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \dots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \dots & \sigma_n(\omega_n) \end{vmatrix}$$

i.e. à $\Delta_{L/K}(\omega_1, \dots, \omega_n)^2$. Comme L/K est séparable, il existe $\alpha \in L$ tel que $L = K(\alpha)$ et il suffit de considerer le cas des $\omega_i = \alpha^i$. Das ce cas, $\Delta_{L/K}(1, \alpha, \dots, \alpha^{n-1})$ est le déterminant de Vandermonde et on a

$$\Delta_{L/K}(1, \alpha, \dots, \alpha^{n-1}) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \dots & \sigma_n(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha^{n-1}) & \sigma_2(\alpha^{n-1}) & \dots & \sigma_n(\alpha^{n-1}) \end{vmatrix} =$$

$$= \prod_{j<i} (\sigma_i(\alpha) - \sigma_j(\alpha)) \neq 0,$$

car $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ si $i \neq j$.

Nous pouvons extraire de cette preuve la formule explicite suivante:

PROPOSITION 0.3.5. *Soit $L = K(\alpha)$ une extension séparable de degré n et soit $f(X)$ le polynôme minimal de α. Alors*

$$D_{L/K}(1, \alpha, \dots, \alpha^{n-1}) = N_{L/K}(f'(\alpha)).$$

PREUVE. On a

$$D_{L/K}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{j<i} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha)) =$$

$$(-1)^{n(n-1)/2} \prod_{i=1}^{n} \sigma_i(f'(\alpha)) = (-1)^{n(n-1)/2} N_{L/K}(f'(\alpha)).$$

§4. Corps finis

Soit K un corps. Dans ce paragraphe on note 1_K l'élément unité de K. Pour tout $n \in \mathbb{Z}$ on pose

$$n \cdot 1_K = \begin{cases} \underbrace{1_K + \dots + 1_K}_{n \ fois}, & \text{si } n > 0 \\ 0_K, & \text{si } n = 0 \\ -(\underbrace{1_K + \dots + 1_K}_{-n \ fois}), & \text{si } n < 0. \end{cases}$$

DÉFINITION. *On appelle caractéristique de K et on note* $\mathrm{car}(K)$ *le plus petit* $p > 0$ *tel que* $p \cdot 1_K = 0_K$. *Si* $n \cdot 1_K \neq 0_K$ *pour tout* $n > 0$, *on pose* $\mathrm{car}(K) = 0$.

THÉORÈME 0.4.1. *Si* $\mathrm{car}(K) = 0$, *alors K contient un sous-corps isomorphe à* $\mathbb{Q}$. *Sinon, la caractéristique de K est un nombre premier p et K contient un sous-corps qui est isomorphe à* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

PREUVE. Soit $\psi : \mathbb{Z} \to K$ l'application définie par $\psi(n) = n \cdot 1_K$. On vérifie facilement que

$$\begin{aligned}&\psi(n+m) = \psi(n) + \psi(m),\\ &\psi(nm) = \psi(n)\,\psi(m),\\ &\psi(1) = 1_K\end{aligned}$$

i.e. que ψ est un homomorphisme d'anneaux. Le noyau de ψ est un idéal de $\mathbb{Z}$ et, comme $\mathbb{Z}$ est principal, il existe $p \geqslant 0$ tel que

$$\ker(\psi) = p\mathbb{Z}\,.$$

Par définition, on a $p = \mathrm{car}(K)$.

Si $p = 0$, alors ψ est injectif et identifie $\mathbb{Z}$ à un sous -anneau de K. On prolonge ψ sur $\mathbb{Q}$ en posant $\psi(m/n) = \psi(m)/\psi(n)$. Comme $\psi(n) \neq 0$ si $n \neq 0$, cette application est bien définie et identifie $\mathbb{Q}$ à un sous-corps de K.

Supposons maintenant que $p \neq 0$. Alors, le théorème de factorisation donne une injection

$$\bar{\psi} : \mathbb{Z}/p\mathbb{Z} \to K\,.$$

Comme K est intègre, $\mathbb{Z}/p\mathbb{Z}$ l'est aussi, d'où on déduit que p est un nombre premier. Donc, $\bar{\psi}$ identifie $\mathbb{F}_p$ à un sous-corps de K.

PROPOSITION 0.4.2. *Soit K un corps de caractéristique $p > 0$. Alors l'application*

$$\begin{aligned}&F : K \to K,\\ &F(x) = x^p\end{aligned}$$

est un endomorphisme de K.

PREUVE. Il est clair que

$$F(xy) = F(x)F(y)\,.$$

D'autre part, pour tout $1 \leqslant k \leqslant p-1$ le nombre premier p divise le coéfficient binomial $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, d'où

$$F(x+y) = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \;=\; x^p + y^p = F(x) + F(y).$$

Donc, F est un endomorphisme de K.

DÉFINITION. *L'endomorphisme F est appelé l'endomorphisme de Frobenius de K.*

Maintenant nous allons étudier les sous-groupes finis du groupe multiplicatif d'un corps.

THÉORÈME 0.4.3 *(voir* [S], *§1.6, th.1). Soit K un corps. Tout sous-groupe fini G de K^* est formé de racines de l'unité, et est cyclique.*

PREUVE. Comme G est abélien et fini, il est isomorphe à un groupe A du type

$$A = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z},$$

où $m_1|m_2|\ldots|m_k$. Donc, $x^{m_k} = 1$ pour tout $x \in G$ i.e. G est formé de racines de l'unité d'ordre m_k. Comme le polynôme $X^{m_k} - 1$ a $\leqslant m_k$ racines, on en déduit que $|G| \leqslant m_k$. D'autre part, $|G| = |A| = m_1 \cdot m_2 \cdots m_k$, d'où $m_1 = m_2 = \cdots = m_{k-1} = 1$. Donc, G est isomorphe à $\mathbb{Z}/m_k\mathbb{Z}$ et est cyclique.

Soit $K^{sép}$ une clôture séparable de K et soit

$$\mu_n = \{x \in K^{sép} \,|\, x^n = 1\}$$

le groupe des racines n-ièmes de l'unité. Nous allons déterminer la structure de ce groupe. Soit $p = car(K)$.

Si $p \nmid n$, alors le polynôme $X^n - 1$ est séparable et a n racines dans $K^{sép}$ et μ_n est cyclique d'ordre n.

Si $n = p^m$, alors tout élément $x \in \mu_n$ vérifie

$$F^m(x - 1_K) = F^m(x) - F^m(1_K) = x^{p^m} - 1_K = 0_K$$

d'où $x = 1_K$. Donc,

$$\mu_{p^m} = \{1_K\}, \qquad \text{si } p = car(K).$$

Dans le cas général, si $n = p^m k$ avec $p \nmid k$, on a

$$\mu_n = \mu_k \times \mu_{p^m} = \mu_k$$

i.e. μ_n est cyclique d'ordre k.

On va appliquer ces resultats à l'étude des corps finis.

THÉORÈME 0.4.4. *Soit K un corps fini à q éléments. Alors*

i) La caractéristique de K est un nombre premier p et il existe $n \geqslant 1$ tel que $q = p^n$.

ii) Le groupe multiplicatif K^* est cyclique d'ordre $q - 1$.

PREUVE. Comme K est fini, il ne peut pas contenir $\mathbb{Q}$, d'où $car(K) = p > 0$. Donc, K est une extension de $\mathbb{F}_p$ de degré fini n (sinon K serait infini). Alors, en tant qu'espace vectoriel sur $\mathbb{F}_p$, K est isomorphe à $\mathbb{F}_p \times \ldots \times \mathbb{F}_p$, d'où $q = |K| = p^n$. L'assertion ii) resulte maintenant du théorème 0.4.3.

THÉORÈME 0.4.5. *Pour tout $n \geqslant 1$ il existe, à isomorphisme près un seul corps à $q = p^n$ éléments.*

La théorie de Galois pour les corps fini est donnée par le théorème suivant:

THÉORÈME 0.4.6. *Soient K un corps fini à q éléments et L/K une extension finie de degré n. Alors*

i) L/K est galoisienne;

ii) $Gal(L/K)$ est un groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius

$$F_{L/K}(x) = x^q \, .$$

PREUVE. Comme $F_{L/K} = F^n$, c'est un endomorphisme injectif de L. Comme L est fini, l'injectivité entraîne la surjectivité, donc $F_{L/K}$ est un automorphisme de L. Tout $x \in K$ vérifie $F_{L/K}(x) = x^q = x$, ce qui signifie que $F_{L/K} \in Gal(L/K)$. Il est facile de voir que l'ordre de $F_{L/K}$ dans $Gal(L/K)$ est egal a n car $F^k_{L/K}(x) = x^{q^k}$ et L^* est cyclique d'ordre $q^n - 1$. Comme $|Gal(L/K)| = [L : K] = n$ on en déduit que $Gal(L/K)$ est engendré par $F_{L/K}$.

CHAPITRE I. ANNEAUX DE DEDEKIND

§1. Divisibilité dans les anneaux

Soit A un anneau (unitaire, commutatif, intègre).

DÉFINITION. *Soient a et b deux éléments de A. On dit que a divise b s'il existe $x \in A$ tel que $b = ax$.*

La relation "*a divise b*" se note $a \mid b$, et sa négation $a \nmid b$.

Rappelons les propriétés élémentaires de divisibilité qui se démontrent facilement:

i) $a \mid b$ si et seulement si $(b) \subseteq (a)$;
ii) $a \mid a$ pour tout $a \in A$;
iii) si $u \in U(A)$, alors $u \mid a$ pour tout $a \in A$;
iv) $1 \mid a$ pour tout $a \in A$;
v) si $a \mid b$ et $b \mid c$, alors $a \mid c$;
vi) si $a \mid b$ et $a \mid c$, alors $a \mid bx + cy$ pour tous $x, y \in A$;
vii) si $a \mid b$ et $c \mid d$, alors $ac \mid bd$

DÉFINITION. *On dit que deux éléments $a, a' \in A$ sont associés et on le note $a \sim a'$ s'il existe $u \in U(A)$ tel que $a = a'u$.*

On vérifie facilement les propriétés suivantes:

1) $\sim$ est une relation d'équivalence;
2) si $a \mid b$ et $a' \sim a$, alors $a' \mid b$;
3) $a \sim b$ si et seulement si $a \mid b$ et $b \mid a$;
4) $a \sim b$ si et seulement si $(a) = (b)$.

DÉFINITION. *On dit qu'un élément $\pi \in A$ est irréductible si $\pi \notin U(A)$ et s'il vérifie la propriété suivante:*

$$a \mid \pi \Rightarrow a \in U(A) \text{ ou } a \sim \pi .$$

On vérifie que si π est irréductible et $\pi' \sim \pi$, alors π' est irréductible.

PROPOSITION 1.1.1. *Soit A un anneau noethérien. Alors*
i) Pour tout $a \notin U(A)$ il existe un élément irréductible qui divise a.
ii) Tout élément $a \notin U(A)$ s'écrit comme produit d'éléments irréductibles:

$$a = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_n .$$

DÉMONSTRATION. i) Si a est irréductible, il n'y a rien à montrer. Sinon il existe $a_1 \mid a$ tel que $a_1 \notin U(A)$ et $a_1 \not\sim a$. Donc $(a) \subset (a_1) \subset A$. Si a_1 est irréductible, la proposition est démontrée. Sinon le même argument montre qu'il existe $a_2 \in A$ tel que $(a) \subset (a_1) \subset (a_2) \subset A$ etc. On obtient ainsi une chaine d'idéaux

$$(a) \subset (a_1) \subset (a_2) \subset \ldots$$

qui est finie car A est noethérien i.e. on a

$$(a) \subset (a_1) \subset (a_2) \subset \ldots \subset (a_n) .$$

Posons $\pi = a_n$. Alors π est un élément irréductible qui divise a et la première assertion est démontrée.

ii) Soit $a \notin U(A)$. Si a est irréductible, on pose $\pi_1 = a$ et il n'y a rien à montrer. Sinon il existe un élément irréductible π_1 et un élément $b_1 \notin U(A)$ tels que $a = \pi_1 b_1$. Si b_1 est irréductible, on pose $\pi_2 = b_1$ et on obtient la factorisation $a = \pi_1\pi_2$. Sinon, il existe un élément irréductible π_2 et un élément $b_2 \notin U(A)$ tels que $b_1 = \pi_2 b_2$ i.e. $a = \pi_1\pi_2 b_2$. On obtient, ainsi, une suite de factorisations:

$$\begin{aligned} a &= \pi_1 b_1, \\ a &= \pi_1\pi_2 b_2, \\ a &= \pi_1\pi_2\pi_3 b_3 \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

avec π_i irréductibles et $b_{i+1} \mid b_i$. Donc, on a une chaîne d'idéaux strictement croissante:

$$(b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \dots$$

qui est finie car A est noethérien. Donc, il existe n tel que $b_{n-1} = \pi_n$ est irréductible, d'où

$$a = \pi_1\pi_2 \cdots \pi_n \, .$$

La proposition est démontrée.

Définition. *1) Soit A un anneau. On dit qu'un élément $a \in A$ admet une factorisation unique en éléments irréductibles si*

i) il existe une unité u et des éléments irréductibles π_i tels que

$$a = u\pi_1\pi_2 \cdots \pi_n \, ;$$

ii) si $a = u'\pi'_1\pi'_2 \cdots \pi'_m$ est une autre factorisation de a, alors $m = n$ et on peut rénuméroter les facteurs π'_i de telle façon que $\pi'_i \sim \pi_i$.

2) Un anneau est appelé factoriel (ou à factorisation unique) s'il est intègre et si tout élément non-nul a une factorisation unique.

Soit A un anneau factoriel. On appelle système représentatif d'éléments irréductibles de A une famille P d'éléments irréductibles telle que tout élément irréductible soit associé à un élément de P et à un seul. Alors, tout élément non-nul de A s'écrit, et d'une seule manière, sous la forme

$$a = u\pi_1^{\alpha_1}\pi_2^{\alpha_2} \cdots \pi_k^{\alpha_k},$$

avec $u \in U(A)$, $\pi_i \in P$ et $\alpha_i \geqslant 1$.

Définition. *Soit A un anneau intègre. On dit que $p \in A$ est un élément premier, si $p \notin U(A)$ et vérifie la propriété suivante:*

$$p \mid ab \text{ entraîne } p \mid a \text{ ou } p \mid b.$$

On montre d'abord, que tout élément premier est irréductible.

Preuve. Soit p un élément premier. Si $p = ab$, alors $p \mid ab$, d'où $p \mid a$ ou $p \mid b$. Si, par exemple, $p \mid a$, alors $a = pc$, d'où $bc = 1$ ce qui signifie que $b \in U(A)$. Donc, p est irréductible.

PROPOSITION 1.1.2. *Un anneau noethérien est factoriel si et seulement si tout élément irréductible est premier.*

PREUVE. Supposons que tout élément irréductible de A est premier. On sait déjà que tout élément $a \in A$ se décompose en produit de facteurs irréductibles

$$a = u\pi_1\pi_2 \cdots \pi_k.$$

Soit

$$a = u'\pi_1'\pi_2' \cdots \pi_k',$$

une autre factorisation de a. Alors

$$\pi_1' \mid \pi_1\pi_2 \cdots \pi_k.$$

Comme π_1' est premier, il existe i tel que $\pi_1' \mid \pi_i$, d'o'u $\pi_1' \sim \pi_i$. On peut supposer que $i = 1$ (rénumérotation!) i.e. que $\pi_1' = u_1\pi_1$, avec $u_1 \in U(A)$. En divisant par π_1, on obtient

$$u\pi_2\pi_3 \cdots \pi_k = u'u_1\pi_2'\pi_3' \cdots \pi_k'.$$

Donc, $\pi_2' \mid \pi_2\pi_3 \cdots \pi_k$ et en appliquant le même raisonnement on obtient que $\pi_2 \sim \pi_2'$ etc.

Supposons maintenant que A est factoriel. Soit π un élément irréductible qui divise ab. Alors, il existe $c \in A$ tel que

$$ab = \pi c.$$

Soient

$$\begin{aligned} a &= u\pi_1 \cdots \pi_n, \\ b &= v\pi_1' \cdots \pi_m', \\ c &= w\pi_1'' \cdots \pi_k'' \end{aligned}$$

les factorisations des a, b et c. Alors

$$uv\pi_1 \cdots \pi_n\pi_1' \cdots \pi_m' = w\pi\pi_1'' \cdots \pi_k''\,.$$

Comme A est factoriel, π est associé à un des éléments π_i, π_j' ce qui montre que $\pi \mid a$ ou $\pi \mid b$. Le théorème est démontré.

DÉFINITION. *Soit A un anneau intègre et soient $\mathfrak{a}, \mathfrak{b} \subseteq A$ deux idéaux. On dit que $\mathfrak{a}$ divise $\mathfrak{b}$ et on écrit $\mathfrak{a} \mid \mathfrak{b}$ si $\mathfrak{b} \subseteq \mathfrak{a}$.*

Cette définition est justifiée par la propriété suivante:
i) Soient $a, b \in A$. Alors $a \mid b$ si et seulement si $(a) \mid (b)$.
ii) Si $\mathfrak{a} \mid \mathfrak{b}$ et $\mathfrak{b} \mid \mathfrak{c}$, alors $\mathfrak{a} \mid \mathfrak{c}$.
iii) $\mathfrak{a} \mid \mathfrak{b}$ et $\mathfrak{b} \mid \mathfrak{a}$ si et seulement si $\mathfrak{a} = \mathfrak{b}$.
iv) Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux. Alors $\mathfrak{a} + \mathfrak{b}$ est le plus petit idéal divisant $\mathfrak{a}$ et $\mathfrak{b}$.

PREUVE. Soit I un idéal divisant $\mathfrak{a}$ et $\mathfrak{b}$. Alors $\mathfrak{a}, \mathfrak{b} \subseteq I$, d'où $\mathfrak{a} + \mathfrak{b} \subseteq I$.

v) $I = \mathfrak{a} \cap \mathfrak{b}$ est le plus grand idéal tel que $\mathfrak{a} \mid I$ et $\mathfrak{b} \mid I$.

PREUVE. Si $\mathfrak{a} \mid I$ et $\mathfrak{b} \mid I$, alors $I \subseteq \mathfrak{a}, \mathfrak{b}$, d'òu $I \subseteq \mathfrak{a} \cap \mathfrak{b}$.

Donnons maintenant **le plan de ce chapitre.** On veut développer la théorie de divisibilité pour certaine classe d'anneaux commutatifs pour l'appliquer, ensuite, à l'étude des corps de nombres. L'anneau $\mathbb{Z}$ fournit un modèle pour une telle théorie: il est factoriel et tout entier non-nul sécrit de façon unique comme produit des nombres premiers. Dans le §2 on rappelle la théorie de divisibilité dans les anneaux principaux qui est essentiellement la même que dans $\mathbb{Z}$. Certains anneaux qui apparaissent en théorie des nombres sont principaux, mais en général ils ne sont même pas factoriels. Voici un exemple typique. Soit

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\}.$$

Comme

$$(a + b\sqrt{-5}) \pm (x + y\sqrt{-5}) = (a \pm x) + (b \pm y)\sqrt{-5},$$
$$(a + b\sqrt{-5})(x + y\sqrt{-5}) = (ax - 5by) + (ay + bx)\sqrt{-5},$$

$\mathbb{Z}[\sqrt{-5}]$ est un anneau qui contient $\mathbb{Z}$. Posons $\pi_1 = 3$, $\pi_2 = 7$, $\pi_3 = (1 + 2\sqrt{-5}$ et $\pi_4 = 1 - 2\sqrt{-5}$. On peut vérifier que ces nombres sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$. Alors

$$21 = \pi_1\pi_2 = \pi_3\pi_4$$

fournit 2 factorisantions différentes de 21. Donc $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.
Néanmoins, on peut montrer qu'il existent des idéaux premiers $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ et $\mathfrak{p}_4$ de $\mathbb{Z}[\sqrt{-5}]$ tels que

$$(3) = \mathfrak{p}_1\mathfrak{p}_2,$$
$$(7) = \mathfrak{p}_3\mathfrak{p}_4,$$
$$(1 + 2\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3,$$
$$(1 - 2\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4,$$

et que *l'ideal* (21) se factorise de façon unique en produit d'idéaux premiers:

$$(21) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4.$$

Donc, pour avoir une bonne théorie de divisibilité, il faut passer à l'étude de la factorisation d'idéaux en produit d'idéaux premiers. Cette théorie a été développée par Kummer (1810-1893) et Dedekind (1831-1916) et fait l'objet principal de ce chapitre. Les résultats principaux sont démontrés dans les §§5-8. Les §§3-4 sont préliminaires mais leur contenu est crucial pour la suite.

§2. Anneaux principaux

Définition. *On dit qu'un anneau intègre A est principal, si tout idéal de A est principal.*

Proposition 1.2.1. *Si A est principal, alors il est noethérien.*

Preuve. Soit $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ une chaine croissante d'idéaux. Alors $\mathfrak{a} = \bigcup_{i=1}^{\infty} \mathfrak{a}_i$ est un idéal de A. Par l'hypothèse il est principal, i.e. il existe $a \in \mathfrak{a}$ tel que $\mathfrak{a} = (a)$. Alors il existe n tel que $a \in \mathfrak{a}_n$. Donc, pour tout $m \geqslant n$ on a $\mathfrak{a} \subseteq \mathfrak{a}_m$. Comme l'inclusion réciproque $\mathfrak{a}_m \subseteq \mathfrak{a}$ est automatique, on en déduit que $\mathfrak{a} = \mathfrak{a}_m$ pour tout $m \geqslant n$ i.e. que $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$.

A partir de maintenant on suppose que A est un anneau principal.

DÉFINITION. *Soient a et b deux éléments de A. On appelle plus grand commun diviseur de a et b un élément $d \in A$ vérifiant les conditions suivantes*

i) d divise a et b;

ii) Si δ est un autre élément qui divise a et b, alors δ divise d.

Si d est un pgcd de a et b, alors tout élément d' associé à d et aussi un pgcd de a et b. En particulier, le pgcd, quand il existe, n'est pas unique.

PROPOSITION 1.2.2. *Soit A un anneau principal. Pour deux éléments non-nuls $a, b \in A$ on note $(a, b) = (d)$ l'idéal qu'ils engendrent. Alors d est un pgcd de a et b.*

DÉMONSTRATION. Soit $I = (a, b)$ l'idéal engendré par a et b. Il est principal, donc il existe $d \in A$ tel que $I = (d)$. Comme $a, b \in I$ on en déduit que d divise a et b.

D'autre part, comme $d \in I$, il existe $x, y \in A$ tels que $d = ax + by$. On en déduit que, si δ divise a et b, alors δ divise d, d'où la proposition.

COROLLAIRE 1.2.3. *Soit A un anneau principal et soit $d = pgcd(a, b)$. Alors il existe $x, y \in A$ tels que $d = ax + by$.*

PROPOSITION 1.2.4. *Soit A un anneau principal et soit π un élément différent de 0. Alors les conditions suivantes sont équivalentes:*

i) π est premier;

ii) π est irréductible;

iii) l'idéal (π) est maximal;

iv) l'idéal (π) est premier;

PREUVE. *i)* $\Rightarrow$ *ii)*. On sait déjà que dans un anneau noethérien tout élément premier est irréductible (voir §1).

ii) $\Rightarrow$ *iii)*. Soit π un élément irréductible et soit I un idéal contenant (π). Comme A est principal, on a $I = (x)$, d'où $x \mid \pi$. Donc, $x \sim \pi$ ou $x \sim 1$. Dans le premier cas on obtient $I = (x) = (\pi)$ et dans le deuxième cas on a $I = (x) = A$. Donc, (π) est maximal.

iii) $\Rightarrow$ *iv)*. Tout idéal maximal est premier (prop. 0.1.4).

iv) $\Rightarrow$ *i)*. Soit (π) un idéal premier. Si $\pi \mid ab$, alors $ab \in (\pi)$ ce qui implique que $a \in (\pi)$ ou $b \in (\pi)$.

En appliquant la prop. 1.1.2, on obtient le théorème suivant:

THÉORÈME 1.2.5. *Soit A un anneau principal. Alors A est factoriel.*

PREUVE. On a montré que tout élément irréductible est premier.

Donnons maintenant quelques exemples d'anneaux principaux.

DÉFINITION. *Soit A un anneau intègre et soit $A^* = A \setminus \{0\}$. On dit que A est euclidien, s'il est muni d'une application*

$$\psi \ : \ A^* \to \mathbb{N}$$

telle que pour tous $a, b \in A^*$ il existe $q, r \in A$ tels que $b = aq + r$ et $r = 0$ ou $\psi(r) < \psi(a)$.

r est appelé le reste de la division de b par a.

THÉORÈME 1.2.6. *Tout anneau euclidien est principal.*

PREUVE. Soit A un anneau euclidien et soit I un idéal de A. Si $I = (0)$, alors il est principal. Sinon dans I il existe un élément a tel que $\psi(a) \leqslant \psi(b)$ pour tout $b \in I \setminus \{0\}$. Il est clair, que $(a) \subseteq I$. Réciproquement, soit $b \in I$. Alors $b = aq + r$, d'où $r = b - aq \in I$. Comme r vérifie $\psi(r) < \psi(a)$, par définition de a la seule possibilité est $r = 0$. Donc, $a \mid b$ et $b \in (a)$, ce qui montre que $I = (a)$.

Exemples. i) L'anneau $\mathbb{Z}$ est euclidien ($\psi(x) =\mid x \mid$).

ii) L'anneau $K[X]$ des polynômes sur un corps K est euclidien ($\psi(f(X)) = deg(f(X))$.)

iii) On peut montrer que pour $n \geqslant 2$ l'anneau $K[X_1, \ldots, X_n]$ est factoriel. Neanmoins, il n'est pas principal (par exemple, l'idéal (X_1, X_2) n'est pas principal).

§3. Fermeture intégrale

Dans ce paragraphe A est un anneau intègre. On note $K = \mathrm{Fr}(A)$ son corps des fractions. Soit L/K une extension de K. Rappelons qu'un élément $x \in L$ est algébrique sur K s'il existe un polynôme non-nul $f(X) \in K[X]$ tel que $f(x) = 0$. Donnons maintenant une version "entière" de cette définition.

DÉFINITION. *On dit qu'un élément $x \in L$ est entier sur A s'il existe $n \geqslant 1$ et des éléments $a_0, a_1, \ldots, a_{n-1} \in A$ tels que*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0\,,$$

i.e. s'il existe un polynôme unitaire $f(X) \in A[X]$ tel que $f(x) = 0$.

Il est clair que tout élément entier sur A est algébrique sur K.

Exemples. 1) Soient $A = \mathbb{Z}$ et $L = K = \mathbb{Q}$. Alors $1/2$ est algébrique sur $\mathbb{Q}$, mais il n'est pas entier sur $\mathbb{Z}$.

2) $\sqrt{2}$ est entier sur $\mathbb{Z}$ (le polynôme $X^2 - 2$ est unitaire et annule $\sqrt{2}$.

3) Tout élément $x \in A$ est algébrique sur A (on peut prendre $f(X) = X - x$).

On a vu qu'en général unélément algébrique sur K n'est pas entier sur A. Neanmoins, on a la propriété suivante:

PROPOSITION 1.3.1. *Soit $x \in L$ un élément algébrique sur K. Alors il existe $c \in A$ tel que cx est entier sur A.*

PREUVE. Si x est algébrique sur K, alors il existe $b_0, \ldots, b_{n-1} \in K$ tels que

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0\,. \tag{*}$$

Comme K est l'anneau des fractions de A, on a $b_i = s_i/t_i$, où $s_i, t_i \in A$. En multipliant (*) par le produit $t = t_1 \cdot \ldots \cdot t_{n-1}$ on obtient:

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

où $a_i = b_i t \in A$. Soit $c = a_n$. Alors, en multipliant la dernière égalité par c^n, on obtient

$$(cx)^n + ca_{n-1}(cx)^{n-1} + \ldots + c^n a_0 = 0,$$

ce qui montre que cx est entier sur A.

Maintenant nous allons démontrer un théorème important qui relie la notion d'un élément entier à la théorie des modules.

THÉORÈME 1.3.2 *(voir* [S], *§2.1, th.1). Les propriétés suivantes sont équivalentes:*
1) $x \in L$ *est entier sur* A;
2) Le A*-module* $A[x]$ *est de type fini;*
3) Il existe un A*-module non-nul* M *de type fini contenu dans* L *et tel que* $xM \subseteq M$.

DÉMONSTRATION. 1) $\Rightarrow$ 2) : Soit $M = A + Ax + \ldots + Ax^{n-1}$ le A-module engendré par $1, x, \ldots, x^{n-1}$ (qui est évidemment de type fini). Si x est entier sur A, alors il existe $a_0, a_1, \ldots, a_{n-1} \in A$ tels que

$$x^n = -a_0 - a_1 x - \ldots - a_{n-1}x^{n-1},$$

d'où on déduit que $x^n \in M$. En utilisant la formule

$$x^{n+i} = -a_0 x^i - a_1 x^{i+1} - \ldots - a_{n-1}x^{n+i-1}$$

on montre , par récurrence, que $x^k \in M$ pour tout k. Comme $A[x]$ est engendré par x^k, $k \geqslant 0$ on en déduit que $A[x] = M$ ce qui donne 2).

2) $\Rightarrow$ 3) : Il suffit de prendre $M = A[x]$.

3) $\Rightarrow$ 1) : Soit M un module vérifiant 3). Alors, il possède un système fini de gńérateurs $m_1, \ldots, m_n \in M$. Comme $xM \subseteq M$, il existe $a_{ij} \in A$ tels que

$$\begin{aligned}
xm_1 &= a_{11}m_1 + a_{12}m_2 + \ldots a_{1n}m_n \\
xm_2 &= a_{21}m_1 + a_{22}m_2 + \ldots a_{2n}m_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
xm_n &= a_{n1}m_1 + a_{n2}m_2 + \ldots a_{nn}m_n.
\end{aligned}$$

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

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

On en déduit que le déterminant du système

$$\Delta = \begin{vmatrix} a_{11} - x & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} - x \end{vmatrix}$$

est égal à 0. En développant Δ, on obtient une équation de la forme $f(x) = 0$, où f est une polynôme unitaire de degré n à coéfficients dans A. Donc, x est entier sur A.

On utilise le théorème 1.3.2 pour démontrer la proposition suivante:

PROPOSITION 1.3.3 *(voir* [S], *§2.1, prop.1 et corollaire 1).*
Soient $x, y \in L$ deux éléments entiers sur A. Alors $x+y$, $x-y$ et xy sont entiers sur A.

PREUVE. Si x et y sont entiers sur A, alors il existe des modules de type fini:

$$M = Am_1 + \ldots + Am_k \subseteq L,$$
$$N = An_1 + \ldots + An_l \subseteq L,$$

tels que $xM \subseteq M$ et $yN \subseteq N$. Soit S le A-module engendré par les produits $m_i n_j$, $1 \leqslant i \leqslant k$, $1_l eqslantj \leqslant l$, i.e.

$$S = Am_1n_1 + \ldots + Am_in_j + \ldots + Am_kn_l.$$

Comme $xM \subseteq M$, il existe $a_{ij} \in A$ tels que

$$xm_i = a_{i1}m_1 + \ldots + a_{ik}m_k,$$

d'où on déduit que $xS \subseteq S$. Le même argument montre que $yS \subseteq S$. Donc, on a

$$(x \pm y)S \subseteq xS + yS \subseteq S + S = S,$$
$$(xy)S = x(yS) \subseteq xS \subseteq S.$$

Comme S est de type fini sur A, le théorème 1 implique que $x \pm y$ et xy sonts entiers sur A.

DÉFINITION. *Soient A et B deux anneaux commutatifs, intègres, $A \subseteq B$. On dit que B est entier sur A si tout élément de B est entier sur A.*

DÉFINITION. *Soient A un anneau intègre, K son corps des fractions et L une extension de K. La proposition 1.3.3 montre que l'ensemble B de tous les éléments $x \in L$ qui sont entiers sur A, est un anneau contenant A. Cet anneau est appelé la fermeture intégrale de A dans L. On appelle clôture intégrale de A la fermeture intégrale de A dans son corps des fractions K.*

Il est clair que, par définition, la fermeture intégrale de A dans L est entière sur A.

PROPOSITION 1.3.4. *Soient $A \subseteq B \subseteq C$ trois anneaux intègres. Si B est entier sur A et C est entier sur B, alors C est entier sur A.*

PREUVE. Soit $x \in C$. Comme x est entier sur B, on a

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0 = 0,$$

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. Alors, la proposition 1.? entraîne que M est de type fini sur A. D'autre part, on a $xM \subset M$ (voir la démonstration du théorème 1), ce qui fait que x est entier sur A.

PROPOSITION 1.3.5. *Soit k un corps et soit B un anneau entier sur k. Alors B est un corps.*

PREUVE. Il suffit de montrer que tout élément non-nul $b \in B$ est invérsible. Comme b est entier sur k, il existe un polynôme non-nul $f(X) \in k[X]$ tel que $f(b) = 0$. Alors l'anneaux $k[b]$ engendré par b est isomorphe à $k[X]/(f(X))$ qui est un corps (théorème 0.2.3) ce qui signifie que $k[b]$ est un corps et que b est inversible dans $k[b]$. Comme $k[b] \subseteq B$, on en déduit que b est invérsible dans B.

§4 Anneaux intégralement clos

Dans ce paragraphe on garde les notations du paragraphe précédent. On note A un anneau intègre et K son corps des fractions.

DÉFINITION. *On dit que A est intégralement clos, si sa clôture intégrale (i.e. la fermeture intégrale de A dans K) est égale à A.*

Un exemple important d'anneaux intégralement clos est donné par la proposition suivante:

PROPOSITION 1.4.1. *Tout anneau factoriel est intégralement clos. En particulier, tout anneaux principal est intégralement clos.*

PREUVE. On veut montrer que si $x \in K$ est entier sur A, alors $x \in A$. Il existe $a_0, a_1, \ldots, a_{n-1} \in A$ tels que

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

D'autre part, le théorème de décomposition en facteurs premiers permet d'écrire x sous la forme $x = \alpha/\beta$, où α et β sont des éléments de A qui sont premiers entre eux. Donc, on a

$$(\alpha/\beta)^n + a_{n-1}(\alpha/\beta)^{n-1} + \ldots + a_0 = 0,$$

d'où

$$\alpha^n + a_{n-1}\alpha^{n-1}\beta + \ldots + a_0\beta^n = 0.$$

On en déduit que β divise α^n et comme α et β sont premiers entre eux, ceci signifie que β est une unité de A. Donc, on a $x = \alpha\beta^{-1} \in A$, d'où la proposition.

Maintenant nous démontrons le résultat principal de ce paragraphe.

THÉORÈME 1.4.2 *(voir* [S]*, §2.7, th. 1). Soit L/K une extension finie séparable. Si A est noethérien et intégralement clos, alors la fermeture intégrale de A dans L est un A-module de type fini.*

DÉMONSTRATION. Comme L/K est séparable, la forme trace:

$$\begin{aligned} &(\ , \ ) \ : \ L \times L \to K, \\ &(x, y) = Tr_{L/K}(xy) \end{aligned}$$

est non-dégénérée et elle définit, ainsi, un isomorphisme

$$\begin{aligned} &L \simeq Hom_K(L, K), \\ &x \mapsto f_x, \qquad f_x(y) = Tr_{L/K}(xy)\,. \end{aligned}$$

Soit $\omega_1, \ldots, \omega_n$ une base de L sur K et soit $\omega_1', \ldots, \omega_n'$ la base duale, i.e.

$$f_{\omega_j'}(\omega_i) = Tr_{L/K}(\omega_i\omega_j') = \begin{cases} 1, & \text{si } i = j \\ 0, & \text{sinon.} \end{cases}$$

Par la proposition 2.1, il existe $c \in A$ tel que $c\omega_1', \ldots, c\omega_n'$ sont entiers sur A.

Soit B la fermeture intégrale de A dans L. Nous allons montrer que

$$(*) \qquad B \subseteq A(c^{-1}\omega_1) + \ldots + A(c^{-1}\omega_n)\,.$$

Si $b \in B$, alors pour tout i le produit $b(c\omega_i')$ est entier sur A. Alors, par le théorème 0.3.2, on a $Tr_{L/K}(bc\omega_i') \in A$, car $Tr_{L/K}(bc\omega_i') \in K$ est entier sur A et A est intégralement clos. Si on écrit b sous la forme

$$b = a_1\omega_1 + \ldots + a_n\omega_n,$$

avec $a_i \in K$, alors un petit calcul montre que

$$Tr_{L/K}(bc\omega_i') = \sum_{j=1}^{n} Tr_{L/K}(a_j\omega_j c\omega_i') = a_i c$$

et on obtient que $a_i c \in A$. Donc, on a $a_i \in c^{-1}A$ et la formule (*) est établie.

Comme A est noethérien et comme $A(c^{-1}\omega_1) + \ldots + A(c^{-1}\omega_n)$ est evidemment de type fini, on en déduit, en utilisant la proposition 0.1.9, que B est de type fini sur A, d'où le théorème.

COROLLAIRE 1.4.3. *Avec les hypothèses du théorème 1.4.2, supposons de plus A principal. Alors, la fermeture intégrale de A dans L est un A-module libre de rang $[L : K]$.*

PREUVE. On a démontré que B est contenu dans

$$A(c^{-1}\omega_1) + \ldots + A(c^{-1}\omega_n)$$

qui est A-libre de rang $n = [L : K]$ (rappelons que $\omega_1, \ldots, \omega_n$ est une base de L sur K). Comme A est principal, on en déduit que B est A-libre de rang $\leqslant n$. D'autre part, B contient la famille libre $c\omega_1', \ldots, c\omega_n'$, donc il est de rang n.

§5 Anneaux de Dedekind

Dans ce paragraphe A est un anneau commutatif, unitaire, intègre. Soit $K = \mathrm{Fr}(A)$ l'anneau des fractions de A.

DÉFINITION. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de A. On dit que $\mathfrak{a}$ divise $\mathfrak{b}$ si $\mathfrak{b} \subseteq \mathfrak{a}$.*

Soit $\mathfrak{p}$ un idéal premier. Alors

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

DÉFINITION. *On appelle idéal fractionnaire une partie $\mathfrak{a}$ de A vérifiant les propriétés suivantes:*

i) $\mathfrak{a}$ est un A-module, c'est à dire

- *$a \pm b \in \mathfrak{a}$ pour tous $a, b \in \mathfrak{a}$;*
- *$\lambda\mathfrak{a} \subseteq \mathfrak{a}$ pour tout $\lambda \in A$;*

ii) il existe $a \in A$ tel que $a\mathfrak{a} \subseteq A$.

Remarquons que tout idéal $\mathfrak{a}$ de A est un idéal fractionnaire.

PROPOSITION. *Tout 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.

PREUVE. Soit $\mathfrak{b}$ un idéal fractionnaire. Alors il existe $a \in A$ tel que $\mathfrak{a} = a\mathfrak{b} \subseteq A$. On voit que $\mathfrak{a}$ est un idéal de A et que

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

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

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\},$$
$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\},$$

et on vérifie que $\mathfrak{a} + \mathfrak{b}$ et $\mathfrak{a} \cdot \mathfrak{b}$ sont des idéaux fractionnaires.

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

((*)) $$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq A\}.$$

DÉFINITION. *Soit A un anneau commutatif, intègre. On dit que A est un anneau de Dedekind si il vérifie les propriétés suivantes*

i) A est noethérien;

ii) A est intégralement clos;

iii) tout idéal premier non-nul de A est maximal.

Démontrons d'abord la proposition suivante.

PROPOSITION 1.5.1. *Tout anneau principal est un anneau de Dedekind.*

PREUVE. On sait déjà qu'un anneau principal est noethérien (prop. 1.2.1) et intégralement clos (prop.1.4.1). En plus, tout idéal premier est maximal (prop. 1.2.4). Donc, il est un anneau de Dedekind.

Le premier résultat important sur les anneaux de Dedekind est le théorème:

THÉORÈME 1.5.2. *Soit A un anneau de Dedekind. Alors l'ensemble $\mathcal{F}(A)$ d'idéaux fractionnaires de A est un groupe abélien pour la multiplication. L'inverse d'un idéal $\mathfrak{a} \in \mathcal{F}(A)$ est donné par la formule (*).*

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

$$\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c},$$
$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a},$$
$$\mathfrak{a}(1) = \mathfrak{a}.$$

Donc, le seul point difficile est de montrer la formule

$$\mathfrak{a}\mathfrak{a}^{-1} = (1).$$

Commençons par quelques résultats préliminaires. Le lemme suivant, bien que technique, est le coeur de la démonstrarion.

LEMME 1.5.3. *Soit A un anneau de Dedekind et soit $\mathfrak{a} \subseteq A$ un idéal. Alors il existe une famille finie d'idéaux premiers*

$$\mathfrak{p}_1, \dots, \mathfrak{p}_s \subseteq A$$

telle que $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_s \subseteq a$.

DÉMONSTRATION DU LEMME. On fait raisonnement par l'absurde. On considère l'ensemble X formé par les idéaux I qui ne vérifient pas la conclusion du lemme. Si le lemme est faux, X n'est pas vide et possède, donc, un plus grand élément $\mathfrak{a}$ pour l'ordre $\subseteq$. 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 $b_1 b_2 \in \mathfrak{a}$. Posons $\mathfrak{a}_1 = (b_1, \mathfrak{a})$ et $\mathfrak{a}_2 = (b_2, \mathfrak{a})$. Comme $b_1, b_2 \notin \mathfrak{a}$, on a des inclusions strictes $\mathfrak{a} \subset \mathfrak{a}_1$ et $\mathfrak{a} \subset \mathfrak{a}_2$. D'autre part, $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ car $b_1 b_2 \in \mathfrak{a}$. 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 $\mathfrak{p}_1, \dots, \mathfrak{p}_k$, $\mathfrak{p}_{k+1}, \dots, \mathfrak{p}_s$ 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.

LEMME 1.5.4. *Soit $\mathfrak{p}$ un idéal premier. Alors $\mathfrak{p}^{-1}\mathfrak{p} = (1)$.*

DÉMONSTRATION DU LEMME. i) On montre d'abord que $\mathfrak{p}^{-1} \neq A$. On fixe un élément non-nul a de $\mathfrak{p}$. On utilise le lemme 1.5.3 et on choisit une plus courte chaîne d'idéaux premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 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 certain i. Pour simplifier la notation on peut supposer $i = 1$. Comme tout idéal premier est maximal (A est de Dedekind!) on en déduit que $\mathfrak{p} = \mathfrak{p}_1$.

D'autre part, par le choix des idéaux $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 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 $\mathfrak{p}^{-1} \neq A$.

ii) Maintenant on peut montrer le 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 montrer que $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1}$ pour conclure que $\mathfrak{p}\mathfrak{p}^{-1} = A$. On fait raisonnement par l'absurde. Supposons que $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$. Alors pour tout $x \in \mathfrak{p}^{-1}$ on a $x\mathfrak{p} \subset \mathfrak{p}$. Comme A est noethérien, l'idéal $\mathfrak{p}$ est de type fini et le

théorème 1.2.3 implique que x est entier sur A. Comme A est intégralement clos, ceci signifie que $\mathfrak{p}^{-1} = A$. Mais dans la partie i) on a montré que $\mathfrak{p}^{-1} \neq A$. Contradiction.

Nous pouvons maintenant terminer la PREUVE DU THÉORÈME 1.5.2.

i) On montre d'abord, que tout idéal est inversible. On fait une preuve par l'absurde. Si$\mathfrak{a} = \mathfrak{p}$, est premier, on a déjà $\mathfrak{p}^{-1}\mathfrak{p} = (1)$ (lemme 1.5.4) ce qui montre que $\mathfrak{p}$ est inversible. Soit X l'ensemble des idéaux I non-inversibles de A i.e. tels que $IJ \neq (1)$ pour tout idéal fractionnaire $J \in \mathcal{F}(A)$. Si le lemme est faux, alors X est non-vide et possède un plus grand élément $\mathfrak{a}$. On a

$$\mathfrak{a}\mathfrak{b} \neq (1)\,, \qquad \forall \mathfrak{b} \in \mathcal{F}(A).$$

Comme $\mathfrak{a}$ n'est pas premier, il existe un idéal premier (=maximal) $\mathfrak{p}$ tel que $\mathfrak{a} \subset \mathfrak{p}$. Comme $A \subset \mathfrak{p}^{-1}$, on a

$$\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{p} = (1).$$

Montrons que $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$ (inclusion stricte). En effet, comme dans la partie ii) de la preuve du lemme 1.5.4, l'égalité $\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$ impliquerait que $\mathfrak{p}^{-1} \subseteq A$ ce qui est faux (lemme 1.5.4). Donc, on a $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$ et par le choix de $\mathfrak{a}$ l'idéal $\mathfrak{p}^{-1}\mathfrak{a}$ est inversible. Il existe, donc, un idéal fractionnaire $\mathfrak{c}$ tel que

$$\mathfrak{c}(\mathfrak{p}^{-1}\mathfrak{a}) = (1).$$

En posant $\mathfrak{b} = \mathfrak{p}^{-1}\mathfrak{c}$, on obtient $\mathfrak{b}\mathfrak{a} = (1)$, ce qui montre que $\mathfrak{a}$ est inversible. Contradiction.

ii) On montre maintenant la formule $\mathfrak{a}\mathfrak{a}^{-1} = (1)$. Par i), il existe $\mathfrak{b} \in \mathcal{F}(A)$ tel que $\mathfrak{a}\mathfrak{b} = (1)$. Il est clair que $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$ (voir la définition de $\mathfrak{a}^{-1}$). Réciproquement, soit $x \in \mathfrak{a}^{-1}$. Alors $x\mathfrak{a} \subseteq A$, d'où

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

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

THÉORÈME 1.5.5. *Soit A un anneau de Dedekind. Alors tout idéal non-nul $\mathfrak{a}$ de A admet une décomposition et une seule de la forme*

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k,$$

où $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ sont des idéaux premiers.

PREUVE. i) Démonstration par l'absurde. Supposons que le théorème est faux. Il existe, donc, un plus grand idéal $\mathfrak{a}$ qui ne s'écrit pas comme produit d'idéaux premiers. Soit $\mathfrak{p}$ un idéal premier (=maximal) contenant $\mathfrak{a}$ et soit $\mathfrak{b} = \mathfrak{a}\mathfrak{p}^{-1}$. Alors $\mathfrak{a} \subseteq \mathfrak{b}$ et comme dans la preuve du théorème 1.5.2 on montre que l'inclusion est stricte. Alors $\mathfrak{a} \subset \mathfrak{b}$ 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,

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

Contradiction.

ii) Montrons maintenant l'unicité de la factorisation. Soit

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

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

$$(*) \qquad \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s.$$

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 (*) 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.

§6. Propriétés des anneaux de Dedekind

Dans ce paragraphe on déduit quelques corollaires des théorèmes 1.5.2 et 1.5.5. Soit A un anneau de Dedekind et soit $\mathcal{P}$ l'ensemble des idéaux premiers de A.

i) Tout idéal $\mathfrak{a}$ de A s'écrit d'une façon et d'une seule sous la forme:

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

où $n_\mathfrak{p}(\mathfrak{a})$ sont des nombres naturels prèsque tous nuls.

Preuve. la formule découle directement du théorème 1.5.5.

ii) Tout idéal fractionnaire $\mathfrak{a} \in \mathcal{F}(A)$ s'écrit d'une façon et d'une seule sous la forme

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

où $n_\mathfrak{p}(\mathfrak{a})$ sont des nombres entiers prèsque tous nuls.

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

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

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

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

et on pose $n_\mathfrak{p}(\mathfrak{a}) = n_\mathfrak{p}(\mathfrak{b}) - n_\mathfrak{p}(a)$.

iii) Soient

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

deux idéaux de A. Alors $\mathfrak{a} \mid \mathfrak{b}$ si et seulement si

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

PREUVE. $\mathfrak{a} \mid \mathfrak{b}$ si et seulement si il existe un idéal

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

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.

iv) On a

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

PREUVE. Posons $\mathfrak{c} = \mathfrak{a} + \mathfrak{b}$. Alors $\mathfrak{c}$ est le plus petit idéal tel que $\mathfrak{c} \mid a$ et $\mathfrak{c} \mid b$. Un utilisant iii) 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 $n_\mathfrak{p}(\mathfrak{c}) = \min\{n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b})\}$. 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 $\mathfrak{a}, \mathfrak{b} \mid \mathfrak{a} \cap \mathfrak{b}$.

Soit K le corps des fractions de A. Pour tout $x = a/b \in K^*$ l'ensemble $(x) = xA$ est un idéal fractionnaire de A ($b(x) = (a) \subseteq A$) appelé idéal fractionnaire principal engendré par x. Comme $(x)(y) = (xy)$ et $(x)^{-1} = (x^{-1})$, les idéaux fractionnaires principaux forment un sous-groupe $\mathcal{FP}(A)$ de $\mathcal{F}(A)$.

DÉFINITION. *Le groupe quotient*

$$Cl(A) = \mathcal{F}(A)/\mathcal{FP}(A)$$

s'appelle le groupe des classes d'idéaux de A.

Il résulte de cette définition la propriété suivante:

v) A est principal si et seulement si $Cl(A) = \{1\}$ (i.e. si $Cl(A)$ se réduit à son élément neutre).

vi) Si l'ensemble $\mathcal{P}$ des idéaux premiers de A est fini, alors A est principal.

PREUVE. Soit $\mathcal{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Montrons que l'idéal $\mathfrak{p}_1$ est principal (le même argument marche pour tout $\mathfrak{p}_i$). D'après le théorème 1.5.5 $\mathfrak{p}_1^2 \neq \mathfrak{p}_1$ (unicité de factorisation), donc on a une inclusion stricte $\mathfrak{p}_1^2 \subset \mathfrak{p}_1$. Choisissons $a \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$ et considérons le système:

$$\begin{cases} x \equiv a \pmod{\mathfrak{p}_1^2} \\ x \equiv 1 \pmod{\mathfrak{p}_2} \\ \cdots\cdots\cdots\cdots \\ x \equiv 1 \pmod{\mathfrak{p}_n} \end{cases}$$

Comme $\mathfrak{p}_i + \mathfrak{p}_j = (1)$ si $i \neq j$, le lemme chinois (proposition 0.1.2) 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 premièrs de A ceci signifie que la factorisation de (x) s'écrit

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

d'où le résultat voulu.

§7. Localisation

7.1. Anneaux de valuation discrète.

DÉFINITION. *Soit A un anneau intègre. On dit que A est un anneau de valuation discrète s'il est principal et possède un idéal premier non-nul $\mathfrak{m}$ et un seul.*

Donnons d'abord quelques propriétés élémentaires de ces anneaux.

i) Comme tout idéal maximal est premier, $\mathfrak{m}$ est un idéal maximal de A et un seul.

ii) Le groupe des unités $U(A)$ de A est

$$U(A) = A \setminus \mathfrak{m},$$

i.e.

$$u \in U(A) \Leftrightarrow u \notin \mathfrak{m}.$$

PREUVE. Si $u \in U(A)$, alors $u \notin \mathfrak{m}$ (sinon $1 = u^{-1}u \in \mathfrak{m}$??). Réciproquement, soit $u \notin \mathfrak{m}$. Alors $(u) \not\subseteq \mathfrak{m}$ et comme tout idéal $\neq (1)$ est contenu dans un idéal maximal on en déduit que $(u) = (1)$. Donc, u est inversible.

iii) L'idéal $\mathfrak{m}$ est principal. On appelle uniformisante de A un générateur π de $\mathfrak{m}$. Si π' est une autre uniformisante, alors $\pi' = u\pi$ avec $u \in U(A)$.

iv) Tout élément non-nul $a \in A$ s'écrit

$$a = u\pi^k\,,$$

avec $u \in U(A)$ et $k \in \mathbb{N}$.

PREUVE. On peut appliquer à A le théorème de factorisation dans un anneau principal (théorème 1.2.5). Comme un élément non-nul $x \in A$ est irréductible si et seulement si (x) est premier (prop. 1.2.4), on obtient que

$$\pi \text{ est irréductible} \Leftrightarrow \pi \text{ est une uniformisante}\,.$$

Le résultat s'en déduit.

v) Tout idéal non-nul de A est engendré par une puissance de π.

PREUVE. Soit I un idéal. Comme A est principal, il existe $a = u\pi^k$ tel que $I = (a) = (\pi^k)$.

vi) Le quotient $k = A/\mathfrak{m}$ est un corps appelé le corps résiduel de A.

7.2. Localisation.

Soit K un anneau intègre et soit K son corps des fractions.

DÉFINITION. *On appelle partie multiplicative une partie S de A vérifiant les propriétés suivantes:*
i) $0 \notin S$ *et* $1 \in S$;
ii) Si $a, b \in S$, *alors* $ab \in S$.

Soit S une partie multiplicative et soit $S^{-1}A$ l'ensemble des éléments de $\frac{a}{s} \in K$ avec $a \in A$ et $s \in S$. Comme

$$\frac{a}{s} \pm \frac{a'}{s'} = \frac{as' \pm a's}{ss'} \in S^{-1}A,$$
$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'} \in S^{-1}A,$$

$S^{-1}A$ est un anneau commutatif contenu dans K.

DÉFINITION. *$S^{-1}A$ est appelé la localisation de A par rapport à S.*

Exemples. 1) Si $S = \{1\}$, alors $S^{-1}A = A$.
2) Si $S = A \setminus \{0\}$, alors $S^{-1}A = K$.
3) **L'exemple suivant est très important.** Soit $\mathfrak{p}$ un idéal premier de A. Alors $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ est une partie multiplicative (ii) découle de la définition d'un idéal premier). On note $A_{\mathfrak{p}}$ et on appelle anneau local de A en $\mathfrak{p}$ la localisation $S_{\mathfrak{p}}^{-1}A$.

PROPOSITION 1.7.1. *Soient A un anneau intègre et S une partie multiplicative de A.*
i) Soit I' un idéal de $S^{-1}A$. Alors $I = I' \cap A$ est un idéal de A vérifiant $I' = I(S^{-1}A)$.
ii) L'application

$$\mathfrak{p}' \mapsto \mathfrak{p} = \mathfrak{p}' \cap A$$

est une bijection entre les idéaux premiers de $S^{-1}A$ et les idéaux premiers $\mathfrak{p}$ de A tels que $\mathfrak{p} \cap S = \varnothing$. L'application réciproque est

$$\mathfrak{p} \mapsto \mathfrak{p}' = \mathfrak{p}(S^{-1}A).$$

PREUVE. Voir, par exemple, [S], §5.1.

COROLLAIRE 1.7.2. *Soit $\mathfrak{p}$ un idéal premier. Alors $\mathfrak{p}A_{\mathfrak{p}}$ est un idéal maximal de $A_{\mathfrak{p}}$ et un seul.*

PREUVE. Soit $\mathfrak{m}'$ un idéal maximal de $A_{\mathfrak{p}}$. Alors il existe un idéal $\mathfrak{m} \subset A$ tel que $\mathfrak{m} \cap S_{\mathfrak{p}} = \varnothing$ tel que $\mathfrak{m}' = \mathfrak{m}A_{\mathfrak{p}}$. La condition $\mathfrak{m} \cap S_{\mathfrak{p}} = \varnothing$ implique $\mathfrak{m} \subseteq \mathfrak{p}$, d'où $\mathfrak{m}' \subseteq \mathfrak{p}A_{\mathfrak{p}}$. Le corollaire est démontré.

7.3. Localisation des anneaux de Dedekind.

PROPOSITION 1.7.3. *Soient A un anneau de Dedekind et S une partie multiplicative. Alors $S^{-1}A$ est un anneau de Dedekind.*

PREUVE (VOIR AUSSI [S], §5.1). i) On montre d'abord que $S^{-1}A$ est noethérien. Soit

$$I_1' \subseteq I_2' \subseteq \dots$$

une chaîne croissante d'idéaux de $S^{-1}A$. Posons $I_i = I_i' \cap A$. Alors on a une chaîne croissante d'idéaux de A :

$$I_1 \subseteq I_2 \subseteq \dots .$$

Comme A est noethérien, il existe n tel que $I_n = I_{n+1} = \dots$. Mais $I_i' = I_i(S^{-1}A)$, d'où $I_n' = I_{n+1}' = \dots$. Donc $S^{-1}A$ est noethérien.

ii) On montre que $S^{-1}A$ est intégralement clos. Soit $x \in S^{-1}A$ un élément entier sur $S^{-1}A$ i.e.

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \dots + \frac{a_1}{s_1}x + \frac{a_0}{s_0} = 0.$$

Soit $s = s_{n-1} \cdot s_1 s_0$. Alors $y = sx$ vérifie l'équation

$$y^n + (a_{n-1}s_{n-2}\dots s_0)y^{n-1} + \dots + \frac{s^n a_0}{s_0} = 0,$$

i.e. il est entier sur A. Comme A est intégralement clos, on a $y \in A$, d'où $x \in S^{-1}A$.

iii) On montre que tout idéal premier $\mathfrak{p}'$ de $S^{-1}A$ est maximal. Soit $\mathfrak{m}'$ un idéal contenant $\mathfrak{p}$ et soient $\mathfrak{p} = \mathfrak{p}' \cap A$ et $\mathfrak{m} = \mathfrak{m}' \cap A$. Comme $\mathfrak{p}$ est maximal dans A, on a $\mathfrak{m} = \mathfrak{p}$, d'où $\mathfrak{m}' = \mathfrak{m}(S^{-1}A) = \mathfrak{p}'$. Donc, $\mathfrak{p}'$ est maximal.

THÉORÈME 1.7.4. *Soit A un anneau de Dedekind.*
i) Pour tout idéal premier $\mathfrak{p} \subset A$ l'anneau $A_\mathfrak{p}$ est un anneau de valuation discrète.
ii) Son corps résiduel $A_\mathfrak{p}/\mathfrak{m}_{A_\mathfrak{p}}$ est isomorphe à $k_\mathfrak{p} = A/\mathfrak{p}$.

PREUVE. $A_\mathfrak{p}$ est un anneau de Dedekind (prop. 1.7.3). Par le corollaire 1.7.2, $\mathfrak{p}A_\mathfrak{p}$ est l'unique idéal premier de $A_\mathfrak{p}$ et en utilisant la propriété vi), du §6 on en déduit que $A_\mathfrak{p}$ est principal.

Comme $\mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{p}$ (voir prop. 1.7.1), l'inclusion $A \subseteq A_\mathfrak{p}$ induit une inclusion

$$i_\mathfrak{p} \ : \ k_\mathfrak{p} = A/\mathfrak{p} \subseteq A_\mathfrak{p}/\mathfrak{m}_{A_\mathfrak{p}}.$$

Il reste à montrer qu'elle est surjective. Soit $y = a/s \in A_\mathfrak{p}$, $s \notin \mathfrak{p}$. Comme $\mathfrak{p}$ est un idéal maximal, on a $(s) + \mathfrak{p} = (1)$, i.e. il existe $b \in A$ et $c \in \mathfrak{p}$ tels que $sb + c = 1$. Posons $x = ab \in A$. Alors $ac/s \in \mathfrak{m}_{A_\mathfrak{p}}$, d'où

$$y = \frac{a}{s} = ab + \frac{ac}{s} \equiv x \pmod{\mathfrak{m}_{A_\mathfrak{p}}}.$$

Donc $i_\mathfrak{p}(x) = x + \mathfrak{m}_{A_\mathfrak{p}} = y + \mathfrak{m}_{A_\mathfrak{p}}$ d'où la surjectivité.

Exemple. Soit p un nombre premier et soit (p) l'idéal principal engendré par p. Alors la localisation $\mathbb{Z}_{(p)}$ de $\mathbb{Z}$ en (p) coïncide avec l'ensemble des rationnels $x = \frac{a}{s}$ avec $a, s \in \mathbb{Z}$ tels que $p \nmid s$. Par le théorème 1.7.4, $\mathbb{Z}_{(p)}$ est un anneau de valuation discrète. L'idéal maximal de $\mathbb{Z}_{(p)}$ est

$$(p) = \left\{ \frac{a}{s} \ : \ p \mid a, p \nmid s \right\}.$$

§8. Extensions

8.1. Dans cette section on étudie le comportement des idéaux premiers dans les extensions $A \subset B$ où B est entier sur A. Dans la section 8.2 on applique ces résultats aux anneaux de Dedekind. Nous commençons par un lemme technique mais très utile en théorie des modules.

LEMME 1.8.1 (DE NAKAYAMA). *Soient A un anneau et $\mathfrak{a}$ un idéal de A qui est contenu dans tous les idéaux maximaux de A. Soit M un A-module de type fini. Si*

$$\mathfrak{a}M = M,$$

alors $M = \{0\}$.

PREUVE. Soit $m_1, \dots, m_n$ un système de générateurs de M. Alors $\mathfrak{a}M = M$ implique que tout m_i s'écrit:

$$m_i = a_{i1}m_1 + a_{i2}m_2 + \cdots a_{in}m_n,$$

avec $a_{ij} \in \mathfrak{a}$. On obtient, ainsi, un système

$$\begin{cases} (1 - a_{11})m_1 - a_{12}m_2 - \cdots - a_{1n}m_n = 0 \\ -a_{21}m_1 + (1 - a_{22})m_2 - \cdots - a_{2n}m_n = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ -a_{n1}m_1 - a_{n2})m_2 - \cdots + (1 - a_{nn})m_n = 0. \end{cases}$$

Si on pose $X = (a_{ij})_{1 \leqslant i,j \leqslant n}$, et $Y = I_n - X$, alors ce système s'écrit

$$(*) \qquad Y \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Comme $a_{ij} \in \mathfrak{a}$, on voit que $\det(Y) \in 1 + \mathfrak{a}$. Soit $\mathfrak{m}$ un idéal maximal de A. Comme $\mathfrak{a} \subseteq \mathfrak{m}$, on en déduit que $\det(Y) \notin \mathfrak{m}$, ce qui signifie que $\det(Y)$ n'appartient à aucun idéal maximal de A. Donc, $\det(Y)$ est une unité de A et la matrice Y est invérsible sur A. En multipliant (*) par Y^{-1} on en déduit que $m_i = 0$, d'où le lemme.

COROLLAIRE 1.8.2. *Soient Aun anneau intègre et $\mathfrak{p}$ un idéal premier de A. Soit M un $A_\mathfrak{p}$-module vérifiant*

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

Alors $M = \{0\}$.

PREUVE. Comme $\mathfrak{p}A_\mathfrak{p}$ est l'unique idéal premier de $A_\mathfrak{p}$, on peut appliquer le lemme de Nakayama en posant $\mathfrak{a} = \mathfrak{p}A_\mathfrak{p}$.

Soit $A \subset B$ une extension d'anneaux. Soient $\mathfrak{p} \subset A$ et $\mathfrak{P} \subset B$ des idéaux premiers. On dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$ (ou que $\mathfrak{P}$ divise $\mathfrak{p}$), si

$$\mathfrak{p} = \mathfrak{P} \cap A.$$

Si $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$, le passage aux quotients donne une injection

$$A/\mathfrak{p} = A/(A \cap \mathfrak{P}) \hookrightarrow B/\mathfrak{P}.$$

On utilise le lemme de Nakayama pour démontrer la proposition suivante:

PROPOSITION 1.8.3. *Soit $A \subseteq B$ et soit $\mathfrak{p}$ un idéal premier de A. Si B est entier sur A, alors*

i) $\mathfrak{p}B \neq B$;

ii) il existe un idéal premier $\mathfrak{P}$ de B au-dessus de $\mathfrak{p}$.

PREUVE. i) On sait que $\mathfrak{m}_{A_\mathfrak{p}} = \mathfrak{p}A_\mathfrak{p}$ est l'unique idéal maximal de $A_\mathfrak{p}$. Soit $B_\mathfrak{p}$ la localisation de B par rapport à la partie multiplicative $S_\mathfrak{p} = A \setminus \mathfrak{p}$. Alors $B_\mathfrak{p}$ est un $A_\mathfrak{p}$-module et on a

$$\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}B = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p} = \mathfrak{m}_{A_\mathfrak{p}}B_\mathfrak{p}.$$

Il suffit, donc, de montrer que $\mathfrak{m}_{A_\mathfrak{p}}B_\mathfrak{p} \neq B_\mathfrak{p}$. On montre cette assertion par l'absurde. Si $\mathfrak{m}_{A_\mathfrak{p}}B_\mathfrak{p} = B_\mathfrak{p}$, alors

$$(*) \qquad 1 = a_1b_1 + \cdots + a_nb_n,$$

avec $a_i \in \mathfrak{m}_{A_\mathfrak{p}}$ et $b_i \in B_\mathfrak{p}$.

Posons $B_0 = A_\mathfrak{p}[b_1, \ldots, b_n]$. Alors B_0 est de type fini sur $A_\mathfrak{p}$ (théorème 1.3.2) et

$$\mathfrak{m}_{A_\mathfrak{p}}B_0 = B_0$$

(grace à (*), on a $B_0 \subseteq \mathfrak{m}_{A_\mathfrak{p}}B_0$, l'inclusion $B_0 \subseteq \mathfrak{m}_{A_\mathfrak{p}}B_0$ est automatique). En appliquant le corollaire 1.8.2 à B_0 , on obtient $B_0 = 0$, d'òu $b_i = 0$ et $1 = 0$. Contradiction.

ii) Comme $\mathfrak{m}_{A_\mathfrak{p}}B_\mathfrak{p} \neq B_\mathfrak{p}$, il existe un idéal maximal $\mathfrak{M}$ de $B_\mathfrak{p}$ tel que

$$\mathfrak{m}_{A_\mathfrak{p}}B_\mathfrak{p} \subseteq \mathfrak{M}.$$

On a $\mathfrak{m}_{A_\mathfrak{p}} \subseteq \mathfrak{M} \cap A_\mathfrak{p}$ et comme $\mathfrak{m}_{A_\mathfrak{p}}$ est maximal, on a

$$\mathfrak{M} \cap A_\mathfrak{p} = \mathfrak{m}_{A_\mathfrak{p}}.$$

Posons $\mathfrak{P} = \mathfrak{M} \cap B$. Alors $\mathfrak{P}$ est un idéal premier de A et on a

$$\mathfrak{P} \cap A = \mathfrak{M} \cap A = (\mathfrak{M} \cap A_\mathfrak{p}) \cap A = \mathfrak{m}_{A_\mathfrak{p}} \cap A = \mathfrak{p}$$

(voir proposition 1.7.1). La proposition est démontrée.

PROPOSITION 1.8.4. *Soit B un anneau entier sur A. Un idéal $\mathfrak{P} \subset B$ est maximal si et seulement si $\mathfrak{p} = \mathfrak{P} \cap A$ est maximal.*

PREUVE. i) Si $\mathfrak{P}$ est maximal, alors $l = B/\mathfrak{P}$ est un corps et $A/\mathfrak{p} \subseteq l$. Comme B est entier sur A, le corps l est entier sur $A/\mathfrak{p}$. On applique la proposition 1.8.3 à l'anneau $A/\mathfrak{p}$. Si $\mathfrak{p}$ n'était pas maximal, $A/\mathfrak{p}$ ne serait pas un corps et il existerait un idéal maximal non nul $\mathfrak{m}$ de $A/\mathfrak{p}$. Par la proposition 1.8.3, il existerait un idéal maximal $\mathfrak{M}$ de l au-dessus de $\mathfrak{m}$ ce qui est absurde car l est un corps.

ii) Réciproquement, supposons que $\mathfrak{p}$ est maximal. Alors $B/\mathfrak{P}$ est entier sur $A/\mathfrak{p}$ et il suffit d'utiliser la proposition 1.3.5 pour conclure que $B/\mathfrak{P}$ est un corps.

8.2. Extensions des anneaux de Dedekind.

Soit A un anneau de Dedekind et soit K son corps des fractions. On fixe une extension finie et séparable L/K de K.

PROPOSITION 1.8.5. *Soit B la ferméture intégrale de A dans L. Alors B est un anneau de Dedekind.*

PREUVE. Il resulte du théorème 1.4.2 que B est un A-module de type fini. Comme A est noetherien on en déduit que B l'est aussi (cf. théorème 0.1.9).

Soit x est un élément du corps des fractions de B qui est entier sur B. Alors (voir prop. 1.3.4) il est entier sur A, d'où $x \in B$. On en déduit que B est intégralement clos.

Il reste de montrer que tout idéal premier de B est principal. Soit $\mathfrak{P} \subset B$ un idéal premier. Alors $\mathfrak{p} = \mathfrak{P} \cap A$ est un idéal premier de A qui est maximal car A est un anneau de Dedekind. On déduit de la prop. 1.8.4 que $\mathfrak{P}$ est maximal dans B,d'où la proposition.

Maintenant on veut étudier le comportement des idéaux de A dans l'extension L/K. Soit $\mathfrak{p}$ un idéal premier de A et soit $\mathfrak{p}B$ l'idéal qu'il engendre dans B. Soit

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

la décomposition de $\mathfrak{p}B$ en produit d'idéaux premiers de B. Chaque idéal $\mathfrak{P}_i$ divise $\mathfrak{p}B$, ce qui signifie que $\mathfrak{p} \subset \mathfrak{P}_i \cap A$ et comme $\mathfrak{P}_i \cap A$ est un idéal premier on obtient que

$$\mathfrak{p} = \mathfrak{P}_i \cap A \qquad i = 1, 2, \dots g,$$

i.e. que $\mathfrak{P}_i$ sont au-dessus de $\mathfrak{p}$. Réciproquement, si $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$, alors $\mathfrak{p}B \subseteq \mathfrak{P}$, i.e. $\mathfrak{P}$ est un diviseur premier de $\mathfrak{p}B$.

L'inclusion $A \subset B$ induit une inclusion

$$A/\mathfrak{p} = A/(\mathfrak{P}_i \cap A) \subset B/\mathfrak{P}_i$$

ce qui signifie que le corps résiduel $l_{\mathfrak{P}_i}$ de B en $\mathfrak{P}_i$ est une extension du corps résiduel $k_{\mathfrak{p}}$ de A en $\mathfrak{p}$.

DÉFINITION. *Le degré $f_i = f(\mathfrak{P}_i/\mathfrak{p})$ de $l_{\mathfrak{P}_i}/k_{\mathfrak{p}}$ est appelé l'indice d'inértie ou le degré résiduel de l'extension L/K en $\mathfrak{P}_i$.*

Le nombre $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$ est appelé l'indice de ramification.

Soit $K \subseteq L \subseteq M$ une tour des corps et soit $A \subseteq B \subseteq C$ la tour correspondante des fermétures intégrales. Soient $\mathfrak{p} \subset A$, $\mathfrak{q} \subset B$ et $\mathfrak{P} \subset C$ trois idéaux premiers tels que $\mathfrak{q}$ est au-dessus de $\mathfrak{p}$ et $\mathfrak{P}$ est au-dessus de $\mathfrak{q}$. On a les formules suivantes qui découlent des définitions:

$$f(\mathfrak{P}/\mathfrak{q})\, f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}),$$
$$e(\mathfrak{P}/\mathfrak{q})\, e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}).$$

THÉORÈME 1.8.6. *On a*

$$\sum_{i=1}^{g} e_i f_i = [L : K]\,.$$

PREUVE. (voir [S], §5.2, th.1). En utilisant par exemple la formule iv) du §6 on voit que

$$\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = (1), \qquad si\ i \neq j.$$

Soit $B_\mathfrak{p}$ la localisation de B par rapport à $S_\mathfrak{p} = A \setminus \mathfrak{p}$. Nous allons utiliser les propriétés suivantes de $B_\mathfrak{p}$:

a) Par la proposition 1.7.1 les idéaux premiers de $B_\mathfrak{p}$ sont de la forme $S_\mathfrak{p}^{-1}\mathfrak{P}$, où $\mathfrak{P}$ est un idéal premier de B tel que $\mathfrak{P} \cap S_\mathfrak{p} = \varnothing$. Soit $\mathfrak{q} = \mathfrak{P} \cap A$. Alors la condition $\mathfrak{P} \cap S_\mathfrak{p} = \varnothing$ signifie que $\mathfrak{q} = \mathfrak{p}$ i.e. que les idéaux premiers de $B_\mathfrak{p}$ sont exactement $\tilde{\mathfrak{P}}_i = S_\mathfrak{p}^{-1}\mathfrak{P}_i$, $i = 1, \dots, g$;

b) Par la propriété iv), §6, l'anneau $B_\mathfrak{p}$ est principal;

c) Par le théorème 1.7.4, $A_\mathfrak{p}$ est un anneau de valuation discrète. En particulier, il est principal et $B_\mathfrak{p}$ est un $A_\mathfrak{p}$-module libre de type fini sans torsion. Par la théorie des module sur un anneau principal, $B_\mathfrak{p}$ est libre sur $A_\mathfrak{p}$. Si $b_1, \dots, b_n$ est une base de $B_\mathfrak{p}$, alors , comme, K (résp. L) est un corps des fractions de $A_\mathfrak{p}$ (résp. de $B_\mathfrak{p}$) on voit que $b_1, \dots, b_n$ est une base de L sur K, i.e. que $n = [L : K]$.

Passons maintenant à la démonstration du théorème. Les idéaux $\tilde{\mathfrak{P}}_i$ sont deux à deux premiers entre eux et le lemme chinois (prop. 0.1.2) donne:

$$B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} \simeq (B_\mathfrak{p}/\tilde{\mathfrak{P}}_1^{e_1}) \times \cdots \times (B_\mathfrak{p}/\tilde{\mathfrak{P}}_g^{e_g}). \tag{1}$$

Comme $B_\mathfrak{p}$ est $A_\mathfrak{p}$-libre de rang $n = [L : K]$, il est isomorphe à $A_\mathfrak{p}^{(n)}$. Soit $k_\mathfrak{p} = A/\mathfrak{p}$ le corps résiduel de A en $\mathfrak{p}$. Alors,

$$B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} \simeq (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})^{(n)} = k_\mathfrak{p}^{(n)}.$$

On en déduit que $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ est un $k_\mathfrak{p}$-espace vectoriel de dimension

$$dim_{k_\mathfrak{p}}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = [L : K]. \tag{2}$$

Calculons maintenant les dimensions $dim_{k_\mathfrak{p}}(B_\mathfrak{p}/\tilde{\mathfrak{P}}_i^{e_i})$. Comme $B_\mathfrak{p}$ est principal, il existe un élément irréductible $\pi_i \in B_\mathfrak{p}$ tel que $\tilde{\mathfrak{P}}_i = (\pi_i)$. Donc,

$$B_\mathfrak{p}/\tilde{\mathfrak{P}}_i^{e_i} \simeq B_\mathfrak{p}/(\pi_i^{e_i}).$$

Considérons la chaîne d'idéaux

$$(\pi_i)^{e_i} \subset (\pi_i^{e_i - 1}) \subset \ldots \subset (\pi_i) \subset B_\mathfrak{p}.$$

On a

$$(\pi_i)^m/(\pi_i)^{m+1} = (\pi_i^m B_\mathfrak{p})/(\pi_i^{m+1} B_\mathfrak{p}) \simeq B_\mathfrak{p}/(\pi_i B_\mathfrak{p}) = B_\mathfrak{p}/\tilde{\mathfrak{P}}_i = l_{\mathfrak{P}_i}.$$

Donc, pour tout m, le quotient $(\pi_i)^m/(\pi_i)^{m+1}$ est un $k_\mathfrak{p}$-espace vectoriel de dimension $[l_{\mathfrak{P}_i} : k_\mathfrak{p}] = f_i$. Alors,

$$\begin{aligned} &dim_{k_\mathfrak{p}}(B_\mathfrak{p}/(\pi_i^{e_i}) = \\ &= dim_{k_\mathfrak{p}}(B_\mathfrak{p}/(\pi_i)) + dim_{k_\mathfrak{p}}((\pi_i)/(\pi_i^2)) + \cdots + dim_{k_\mathfrak{p}}((\pi^{e_i - 1})/(\pi_i^{e_i})) = \\ &= f_i + f_i + \cdots + f_i = e_i f_i. \end{aligned} \tag{3}$$

D'autre part, la décomposition (1) donne

$$dim_{k_\mathfrak{p}}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = \sum_{i=1}^{g} dim_{k_\mathfrak{p}}(B_\mathfrak{p}/\tilde{\mathfrak{P}}_i^{e_i})$$

et il suffit de mettre ensemble (2) et (3) pour conclure.

Si l'extension L/K est galoisienne, on peut démontrer un résultat plus précis. Voir le théorème 2.6.7.

§9. Les homomorphismes de norme et de l'injection pour les idéaux

Soient A un anneau de Dedekind, K son corps des fractions, L/K une extension finie séparable et B la fermeture intégrale de A dans L. On note $\mathcal{F}(A)$ (resp. $\mathcal{F}(B)$) le groupe des idéaux fractionnaires de A (resp. de B). On va définir deux homomorphismes:

$$i_{B/A} \ : \ \mathcal{F}(A) \to \mathcal{F}(B),$$
$$\mathcal{N}_{B/A} \ : \ (B) \to \mathcal{F}(A)$$

appelés l'injection et la norme. Comme $\mathcal{F}(A)$ (resp. $\mathcal{F}(B)$) est un groupe abélien libre engendré par les idéaux premiers non-nuls $\mathfrak{p}$ de A (resp. $\mathfrak{P}$ de B), il suffit de définir $i_{B/A}(\mathfrak{p})$ (resp. $\mathcal{N}_{B/A}(\mathfrak{P})$). On pose

$$i_{B/A}(\mathfrak{p}) = \mathfrak{p}B \ = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})},$$
$$\mathcal{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}, \qquad \textit{où } \mathfrak{p} = \mathfrak{P} \cap A.$$

Voici deux propriétés élémentaires qui découlent directement de cette définition:

i) Si $\mathfrak{a} \in \mathcal{F}(A)$, alors

$$\mathcal{N}_{B/A}(i_{B/A}(\mathfrak{a})) = \mathfrak{a}^n, \qquad \textit{où } n = [L:K].$$

ii) Soit $\mathfrak{p}$ un idéal premier non-nul de A. On pose $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$, $B_\mathfrak{p} = S_\mathfrak{p}^{-1}B$ et pour tout idéal $\mathfrak{b}$ de B on note $\mathfrak{b}_\mathfrak{p}$ l'idéal $\mathfrak{b}B_\mathfrak{p}$ de $B_\mathfrak{p}$. Alors

$$\mathcal{N}_{B_\mathfrak{p}/A_\mathfrak{p}}(\mathfrak{b}_\mathfrak{p}) = \mathcal{N}_{B/A}(\mathfrak{b})_\mathfrak{p}.$$

Preuve. Il suffit de vérifier ces formules pour les idéaux premiers.

i) Comme $\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = n$, (voir le théorème 1.8.6) , on a:

$$\mathcal{N}_{B/A}(i_{B/A}(\mathfrak{p})) = \mathcal{N}_{B/A}\left(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}\right) \ = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})} = \mathfrak{p}^n.$$

ii) Soit $\mathfrak{Q}$ un idéal premier de B et soit $\mathfrak{q} = \mathfrak{Q} \cap A$. Si $\mathfrak{q} = \mathfrak{p}$, alors $\mathfrak{Q}_\mathfrak{p}$ est un idéal de $B_\mathfrak{p}$ au-dessus de $\mathfrak{p}A_\mathfrak{p}$ et on a

$$\mathcal{N}_{B_\mathfrak{p}/A_\mathfrak{p}}(\mathfrak{Q}_\mathfrak{p}) = (\mathfrak{p}A_\mathfrak{p})^{f(\mathfrak{Q}/\mathfrak{p})} = \mathfrak{p}^{f(\mathfrak{Q}/\mathfrak{p})}A_\mathfrak{p} = \mathcal{N}_{B/A}(\mathfrak{Q})_\mathfrak{p}.$$

Si $\mathfrak{q} \neq \mathfrak{p}$, alors $S_\mathfrak{p} \cap \mathfrak{Q} \neq \varnothing$ et $\mathfrak{Q}_\mathfrak{p} = B_\mathfrak{p}$, d'où $\mathcal{N}_{B_\mathfrak{p}/A_\mathfrak{p}}(\mathfrak{Q}_\mathfrak{p}) = A_\mathfrak{p}$ et $\mathcal{N}_{B/A}(\mathfrak{Q})_\mathfrak{p} = S_\mathfrak{p}^{-1}\mathfrak{q}^{f(\mathfrak{Q}/\mathfrak{q})} = A_\mathfrak{p}$.

Proposition 1.9.1. *Si $\beta \in L^*$, alors $\mathcal{N}_{B/A}((\beta))$ coïncide avec l'idéal principal engendré par $N_{L/K}(\beta)$:*

$$\mathcal{N}_{B/A}((\beta)) = (N_{L/K}(\beta)).$$

Preuve. a) Supposons d'abord que A est un anneau de valuation discrète. Soit π une uniformisante de A. Alors $\mathfrak{p} = (\pi)$ est l'unique idéal premier non-nul de A.

Par la proriété iv), §6 B est principal et de type fini sur A. Comme de plus, B est sans torsion, il est libre sur A. Soit $e_1, \dots, e_n$ une base de B sur A. Comme les applications $\mathcal{N}_{B/A}$ et $N_{L/K}$ sont multiplicatives, il suffit de vérifier la formule pour les éléments irréductibles $\Pi \in B$. Soit $\mathfrak{P} = (\Pi)$. Alors $\mathfrak{P} \mid \mathfrak{p}$ et

$$f(\mathfrak{P}/\mathfrak{p}) = dim_{k_\mathfrak{p}} l_\mathfrak{P}; \qquad où\ k_\mathfrak{p} = A/\mathfrak{p},\ l_\mathfrak{P} = B/\mathfrak{P}.$$

Soit $f_\Pi : B \to B$ l'application "multiplication par Π":

$$f_\Pi(x) = \Pi x$$

et soit $M(\Pi)$ la matrice de f_Π dans la base $\{e_i\}$:

$$f_\Pi \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = M(\Pi) \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

Par le théorème des diviseurs élémentaires, il existe des matrices inversibles $U, V \in GL_n(A)$ telles que

$$UM(\Pi)V = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}, \qquad \lambda_i = \pi^{k_i},\ \lambda_i \mid \lambda_{i+1}.$$

Posons

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = U \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

et

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = V^{-1} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}.$$

Comme U et V sont inversibles sur A, les familles $\{u_i\}$ et $\{v_i\}$ sont des bases de B sur A et on a

$$f_\Pi \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = UM(\Pi) \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = UM(\Pi)V \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix},$$

i.e. $f_\Pi(u_i) = \lambda_i v_i$. Donc

$$\mathfrak{P} = \Pi B = f_\Pi(B) = \lambda_1 A v_1 + \ldots + \lambda_n A v_n,$$

ce qui montre qu'en tant que $k_\mathfrak{p}$-module, $l_\mathfrak{P} = B/\mathfrak{P}$ est isomorphe à

$$A/(\pi^{k_1}) \oplus A/(\pi^{k_2}) \oplus \cdots \oplus A/(\pi^{k_n}).$$

On en déduit que

$$dim_{k_\mathfrak{p}} l_\mathfrak{P} = k_1 + k_2 \cdots + k_n,$$

d'où

$$\mathcal{N}_{B/A}(\mathfrak{P}) = (\pi^{k_1+k_2+\ldots+k_n}) = (\lambda_1\lambda_2\cdots\lambda_n).$$

D'autre part, on a

$$N_{L/K}(\Pi) = \det(M(\Pi)) = (\det(U))^{-1}\det(V)\begin{vmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ 0 & 0 & \ldots & \lambda_n \end{vmatrix}.$$

Comme $\det(U)$ et $\det(V)$ sont des unités on obtient que

$$(N_{L/K}(\Pi)) = (\lambda_1\lambda_2\cdots\lambda_n),$$

d'où $\mathcal{N}_{B/A}((\Pi)) = (N_{L/K}(\Pi))$.

b) Considérons maintenant le cas général. Pour montrer que $\mathcal{N}_{B/A}((\beta)) = (N_{L/K}(\beta))$ il suffit de montrer que pour tout idéal premier $\mathfrak{p}$ de A on a

$$(*) \qquad \mathcal{N}_{B/A}((\Pi))_\mathfrak{p} = (N_{L/K}(\Pi))_\mathfrak{p}.$$

Par la propriété ii) on a $\mathcal{N}_{B/A}((\beta))_\mathfrak{p} = \mathcal{N}_{B_\mathfrak{p}/A_\mathfrak{p}}((\beta)_\mathfrak{p})$, et la formule (*) se reécrit:

$$\mathcal{N}_{B_\mathfrak{p}/A_\mathfrak{p}}(\beta A_\mathfrak{p}) = N_{L/K}(\beta)A_\mathfrak{p}.$$

Comme $A_\mathfrak{p}$ est principal, la dernière formule découle de a), d'où la proposition.

CHAPITRE II. VALUATIONS

§1. Valeurs absolues

1.1. Valeurs absolues.

DÉFINITION. *Soit K un corps. On appelle valeur absolue sur K une fonction*

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

satisfaisant aux trois propriétés suivantes:

i) On a $\|x\| \geqslant 0$ pour tout $x \in K$ et $\|x\| = 0$ si, et seulement si, $x = 0$;

ii) Pour tous $x, y \in K$ on a

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

iii) Pour tous $x, y \in K$ on a

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

Exemples. 1) La valeur absolue définie par $\|x\| = 1$ si $x \neq 0$ est dite triviale.

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

Donnons quelques propriétés élémentaires des valeurs absolues:

i) On a

$$\|1_K\| = \| - 1_K\| = 1.$$

PREUVE. On a

$$\|1_K\| = \|1_K \cdot 1_K\| = \|1_K\| \, \|1_K\|$$

d'où $\|1_K\| = 1$ et

$$\| - 1_K\|^2 = \|(-1_K)(-1_K)\| = \|1_K\| = 1,$$

d'où $\| - 1_K\| = 1$.

ii) Pour tout $n \in \mathbb{N}$ on a

$$\|n1_K\| \leq n.$$

PREUVE. On a

$$\|n1_K\| = \| \underbrace{1_K + \cdots + 1_K}_{n \ fois} \| \leq \underbrace{\|1_K\| + \cdots + \|1_K\|_K}_{n \ fois} = n.$$

iii) Pour tout $x \in K$ on a

$$\| - x\| = \|x\|.$$

iv) On a

$$\|x^{-1}\| = \|x\|^{-1}$$

si $x \neq 0$.

v) Pour tous $x, y \in K$ on a

$$| \, \|x\| - \|y\| \, | \leqslant \|x - y\|.$$

PREUVE. On a

$$\|x\| = \|x - y + y\| \leqslant \|x - y\| + \|y\|,$$

d'où $\|x\| - \|y\| \leqslant \|x - y\|$. En appliquant le même argument à $\|y\|$ on obtient que $\|y\| - \|x\| \leqslant \|x - y\|$, d'où l'inégalité voulue.

PROPOSITION 2.1.1. *Soit $\|\cdot\| : K \to \mathbb{R}$ une application vérifiant les propriétés suivantes:*

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

ii) Pour tous $x, y \in K$ on a

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

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

$$(*) \qquad \|x\| \leqslant 2 \qquad \text{pour tout } x \text{ tel que } \|x\| \leqslant 1.$$

PREUVE. 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 (*). Alors pour tous $x, y \in K$ on a

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

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

$$\|\sum_{i=0}^{2^m} x_i\| \leqslant 2^m max\{\|x_i\| \,|\, 1 \leq i \leq 2^m\}$$

pour tous $x_i \in K$. Si n est un nombre naturel quelconque il existe m tel que $2^{m-1} \leq n \leq 2^m$. Pour tous $x_1, \ldots, x_n \in K$ 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, pour tout $n \in \mathbb{N}$ on a

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

Maintenant nous pouvons montrer que (*) implique l'inégalité triangulaire. Soient $x, y \in K$. Alors pour tout n on a:

$$\|x + y\|^n = \|(x + y)^n\| = \|\sum_{i=0}^{n} C_n^i x^i y^{n-i}\| \leq \sum_{i=0}^{n} \|C_n^i 1_K\| \, \|x\|^i \, \|y\|^{n-i}\| \leq$$

$$\leq 2\sum_{i=0}^{n} C_n^i \|x\|^i \, \|y\|^{n-i} = 2(\|x\| + \|y\|)^n.$$

Donc

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

pour tout $n \in \mathbb{N}$. En passant a 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.e. elle vérifie les propriétés suivantes:
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 tous $x, y \in K$;
iii) Pour tous $x, y, z \in K$ on a

$$d(x,z) \leqslant d(x,y) + d(y,z) \quad (\textit{inégalité triangulaire}).$$

On appelle boule ouverte de centre $a \in K$ et de rayon $r > 0$ l'ensemble

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

La distance d définit une topologie sur K. Plus précisement, on dit que $U \subseteq K$ est un ouvert, si pour tout $x \in U$ il existe $r > 0$ tel que $B(x,r) \subseteq U$. On peut dire aussi que U est un ouvert s'il s'écrit comme union des boules ouvertes. Une suite $\{x_n\}$ converge vers $x \in K$ si, et seulement si, pour tout $\epsilon > 0$ il existe N tel que pour tout $n \geqslant N$

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

PROPOSITION 2.1.2. *Soit K un corps muni d'une valeur absolue. Les applications suivantes sont continues:*

$$i) \quad \begin{cases} \| \cdot \| \ : \ K \to \mathbb{R}, \\ x \mapsto \|x\|; \end{cases}$$

$$ii) \quad \begin{cases} f_a \ : \ K \times K \to K, \\ f_a(x,y) = x + y; \end{cases}$$

$$iii) \quad \begin{cases} f_m \ : \ K \times K \to K, \\ f_m(x,y) = xy; \end{cases}$$

$$iv) \quad \begin{cases} i \ : \ K^* \to K^*, \\ i(x) = x^{-1}. \end{cases}$$

PREUVE. i) Soit $\epsilon > 0$. Posons $\delta = \epsilon$. Par la propriété v) pour tous $x, x' \in K$ vérifiants $\|x - x'\| < \delta$ on a

$$| \, \|x\| - \|x'\| \, | < \|x - x'\| < \epsilon,$$

d'ou la continuité de la valeur absolue.
ii) Soit $\epsilon > 0$. Posons $\delta = \epsilon/2$. Si $\|x - x'\| < \delta$ et $\|y - y'\| < \delta$, on a

$$\|f_a(x,y) - f_a(x',y')\| < \|x - x'\| + \|y - y'\| < \epsilon.$$

iii) Soient $x, y \in K$. Pour tout $\epsilon > 0$ posons

$$\delta = \min\left\{ \frac{\epsilon}{3\|x\|}, \frac{\epsilon}{3\|y\|}, \sqrt{\epsilon/3} \right\}.$$

Alors, si $\|x - x'\| < \delta$ et $\|y - y'\| < \delta$, on a:

$$\|f_m(x,y) - f_m(x',y')\| = \|x(y-y') + (x-x')y + (x-x')(y'-y)\| \leq$$
$$\leq \|x\|\|y-y'\| + \|y\|\|y-y'\| + \|x-x'\|\|y-y'\| \leq \epsilon.$$

iv) La preuve est essentiellement la même (et facile).

DÉFINITION. *On dit que deux valeurs absolues $\| \cdot \|_1$ et $\| \cdot \|_2$ sur K sont équivalentes, si elles définissent la même topologie.*

Nous admettons la proposition suivante (voir [L], chapitre 12, prop. 12.1.1 pour démonstration):

PROPOSITION 2.1.3. *Soient $\| \cdot \|_1$ et $\| \cdot \|_2$ deux valeurs absolues non-triviales sur K. Elles sont équivalentes si et seulement si la relation $\|x\|_1 < 1$ implique $\|x\|_2 < 1$. Si elles sont équivalentes, il existe $c > 0$ tel que pour tout $x \in K$*

$$\|x\|_1 = \|x\|_2^c.$$

1.2. Complétions.

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

Le théorème suivant dit, en gros, qu'on peut toujour "compléter" K en le plongeant dans un corps complet.

THÉORÈME 2.1.4. *Soit K un corps muni d'une valeur absolue $\| \cdot \|$. Il existe un corps $\hat{K}$ muni d'une valeur absolue $\| \cdot \|_{\hat{K}}$ et un plongement $i : K \hookrightarrow \hat{K}$ vérifiant les propriétés suivantes:*

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

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

ii) $\hat{K}$ est complet pour la valeur absolue $\| \cdot \|_{\hat{K}}$;

iii) $i(K)$ est dense dans $\hat{K}$.

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

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

tel que

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

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

$$\tilde{i}(x) = j(i(x)) \quad \textit{pour tout } x \in K.$$

On peut résumer ce théorème en disant qu'il existe un corps complet $\hat{K}$ contenant K tel que K est dense dans $\hat{K}$ et un seul.

PREUVE. (voir [L], §12.2, proposition 12.2.1). Démontrons d'abord l'unicité. Dans la démonstration nous utilisons plusieurs fois l'observation suivante: comme

$\| \cdot \|_{\hat{K}}$ prolonge $\| \cdot \|$, $\{x_n\} \subset K$ est une suite de Cauchy si, et seulement si, $\{i(x_n)\}$ l'est dans $\hat{K}$.

Soit $(\tilde{K}, \| \cdot \|_{\tilde{K}}, \tilde{i})$ un autre corps vérifiant i)-iii). Nous allons construire l'application $j : \hat{K} \to \tilde{K}$ de façon suivante. Comme $i(K)$ est dense dans $\hat{K}$, pour tout $x \in \hat{K}$ il existe une suite $x_n \in K$ telle que $x = \lim_{n\to\infty} i(x_n)$. Comme x_n est une suite de Cauchy, la suite $\{\tilde{i}(x_n)\} \subset \tilde{K}$ l'est aussi et comme $\tilde{K}$ 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'il ne dépend pas de 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 $\tilde{K}$. Donc, les sous-suites $\{\tilde{i}(x'_n)\}$ et $\{\tilde{i}(x_n)\}$ de $\{\tilde{(}\alpha_n)\}$ 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

$$\begin{aligned} x + y &= \lim_{n\to\infty} (i(x_n) + i(y_n)) = \lim_{n\to\infty} i(x_n + y_n), \\ xy &= \lim_{n\to\infty} (i(x_n)\, i(y_n)) = \lim_{n\to\infty} i(x_n y_n), \end{aligned}$$

d'où

$$\begin{aligned} j(x + y) &= j(x) + j(y), \\ j(xy) &= j(x)\, j(y). \end{aligned}$$

On en déduit que j est un homomorphisme de corps. Par construction, on a $j(i(x)) = \tilde{i}(x)$, si $x \in K$ (si $x \in K$ 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 $\tilde{i}(K)$ est dense dans $\tilde{K}$, pour tout $z \in \tilde{K}$ 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 $\hat{K}$ vérifiant i)-iii). Soit $C(K)$ l'ensemble des suites de Cauchy $\{x_n\}$ dans K. On définit la somme et le produit des deux suites de Cauchy en posant

$$\begin{aligned} \{x_n\} + \{y_n\} &= \{x_n + y_n\}, \\ \{x_n\}\, \{y_n\} &= \{x_n y_n\}. \end{aligned}$$

On vérifie facilement que $\{x_n + y_n\}$ et $\{x_n y_n\}$ sont des suites de Cauchy. Donc, $C(K)$ est un anneau commutatif pour l'addition et la multiplication terme à terme.

Soit

$$I_K = \{\{x_n\} \subset K | \lim_{n\to\infty} x_n = 0\}.$$

On va montrer que I_K est un idéal maximal de $C(K)$. Il est clair que si $\{x_n\}, \{y_n\} \in I_K$, alors $\{x_n\} \pm \{y_n\} \in I_K$. Soient maintenant $\{x_n\} \in I_K$ et $\{y_n\} \in C(K)$ une suite de Cauchy quelconque. Alors $\{y_n\}$ est bornée (la preuve est exactement la même que dans le cas "classique") 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 $\{x_n\}\{y_n\} \in I_K$. Donc, I_K est un idéal. Pour montrer qu'il est maximal il suffit de remarquer que si $\{x_n\} \notin I_K$, il existe $M > 0$ et $N \in \mathbb{N}$ tels que

$$\|x_n\| \geqslant M, \quad si\ n \geqslant N.$$

On définit une suite $\{y_n\}$ en posant $y_n = x_n^{-1}$ si $n \geqslant N$. On a

$$\|y_n - y_m\| = \left\| \frac{1}{x_n} - \frac{1}{x_m} \right\| = \frac{\|x_n - x_m\|}{x_n x_m} \leqslant \frac{\|x_n - x_m\|}{M^2},$$

ce qui montre que $\{y_n\}$ est une suite de Cauchy. Comme $\{x_n\}\{y_n\} = 1$, on en déduit que $\{x_n\}$ est inversible dans $C(K)$. Donc, tout élément de $C(K)$ qui n'appartient pas à I_K est inversible ce qui entraîne que l'idéal I_K est maximal.

On définit le corps $\hat{K}$ comme le quotient

$$\hat{K} = C(K)/I(K).$$

Le corps K est plongé dans $\hat{K}$ "sur la diagonale": l'image $i(x)$ de $x \in K$ est la classe de la suite constante $x_n = x$. La valeur absolue de K se prolonge sur $\hat{K}$ par continuité: si $\{x_n\} \in C(K)$ représente une classe $\alpha \in \hat{K}$, on pose

$$\|\alpha\|_{\hat{K}} = \lim_{n\to\infty} \|x_n\|.$$

(Remarquons que l'inégalité $|\ \|x_n\| - \|x_m\|\ | \leqslant \|x_n - x_m\|$ implique que $\|x_n\|$ est une suite de Cauchy dans $\mathbb{R}$, d'où la convergence.) Par construction, le corps K est dense dans $\hat{K}$.

Il reste à montrer que $\hat{K}$ est complet. Soit $\{\alpha_n\}$ une suite de Cauchy dans $\hat{K}$. Comme $i(K)$ est dense dans $\hat{K}$, pour tout α_n il existe $x_n \in K$ tel que $\|x_n - \alpha_n\|_{\hat{K}} < 1/n$. Soit $\epsilon > 0$. Alors il existe N tel que pour tous $n, m \geqslant N$ on a

$$\|i(x_n) - \alpha_n\|_{\hat{K}} < \epsilon/3,$$
$$\|\alpha_m - \alpha_n\|_{\hat{K}} < \epsilon/3.$$

Donc, pour tous $n, m \geqslant N$ on a

$$\|x_n - x_m\| \leqslant \|i(x_n) - \alpha_n\|_{\hat{K}} + \|\alpha_n - \alpha_m\|_{\hat{K}} + \|\alpha_m - i(x_n)\|_{\hat{K}} < \epsilon$$

ce qui montre que $\{x_n\}$ est une suite de Cauchy. Posons $\alpha = \lim_{n\to\infty} i(x_n)$. En utilisant l'inégalité

$$\|\alpha_n - \alpha\|_{\hat{K}} \leqslant \|\alpha_n - i(x_n)\|_{\hat{K}} + \|i(x_n) - \alpha\|_{\hat{K}}$$

on montre facilement que α_n converge vers α. Donc $\hat{K}$ est complet.

Pour simplifier la notation nous allons identifier K à son image $i(K)$ dans $\hat{K}$. En particulier, nous allons écrire x au lieu de $i(x)$.

§2. Prolongement des valeurs absolues: cas de corps complet

2.1. Préliminaires.

Dans ce paragraphe K désigne un corps complet pour une valeur absolue non-triviale $\| \cdot \|_K$. On appelle boule fermée de centre a et de rayon $r > 0$ l'ensemble:

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

Comme l'application $\| \cdot \|_K : K \to \mathbb{R}$ est continue (proposition 2.1.2) on voit que $B_f(a, r)$ 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 $\bar{B}(a, r) \subseteq B_f(a, r)$. Bien que dans les cas "classiques" (par exemple pour $K = \mathbb{R}$ ou $\mathbb{C}$) on a $\bar{B}(a, r) = B_f(a, r)$ en général on a uniquement l'inclusion.

Rappelons la définition d'un espace topologique localement compact.

Définition. *Soit X un espace topologique. On dit qu'il 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. $\mathbb{R}$ et $\mathbb{C}$ sont localement compacts.

Proposition 2.2.1. *Soit K un corps complet pour une valeur absolue $\| \cdot \|_K$. Les assertions suivantes sont équivalentes.*

i) K est localement compact;

ii) Pour tout $a \in K$ il existe $r > 0$ tel que $B_f(a, r)$ est compact.

iii) Pour tous $a \in K$ et $r > 0$ la boule fermée $B_f(a, r)$ est compacte.

Preuve. *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 $B(0, r') \subseteq U$. 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 $\|\lambda\|_K < 1$. En remplacant λ par λ^n pour n assez grand on voit que pour tout $\epsilon > 0$ il existe $\lambda \neq 0$ tel que $\|\lambda\|_K < \epsilon$.

Soit $r > 0$. Par ii) il existe $r' > 0$ tel que $B_f(0, r')$ est compact. Choisissons λ vérifiant $\|\lambda\|_K < r'/r$. Soit $h_\lambda : K \to K$ l'application "multiplication par λ":

$$h_\lambda(x) = \lambda x.$$

Par la proposition 2.1.2 ii) 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, $F = h_\lambda(B_f(O, r))$ 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 homéomorphent on en déduit la compacité de $B_f(0, r)$.

Il reste à remarquer que la translation

$$K \to K,$$
$$x \mapsto a + x$$

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 $\bar{B}(a,r)$.

Pour étudier les prolongements des valeurs absolues aux extensions finies nous avons besoin de la notion de norme sur un espace vectoriel.

DÉFINITION. *Soit K un corps muni d'une valeur absolue $\|\cdot\|_K$ et soit V un K-espace vectoriel de dimension finie. On appelle norme sur V une fonction*

$$\|\cdot\|_V \ : \ V \to \mathbb{R}$$

telle que:

i) pour tout $\overrightarrow{v} \in V$ on a $\|\overrightarrow{v}\|_V \geqslant 0$ et $\|\overrightarrow{v}\|_V = 0$ si et seulement si $\overrightarrow{v} = 0$;

ii) pour tous $\alpha \in K$ et $\overrightarrow{v} \in V$ on a

$$\|\alpha\overrightarrow{v}\|_V = \|\alpha\|_K \|\overrightarrow{v}\|_V;$$

iii) pour tous $\overrightarrow{u}, \overrightarrow{v} \in V$ on a

$$\|\overrightarrow{u} + \overrightarrow{v}\|_V \leqslant \|\overrightarrow{u}\|_V + \|\overrightarrow{v}\|_V.$$

*Exemples.*1) Soit $\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n$ une base de V. Tout $\overrightarrow{v} \in V$ s'écrit:

$$\overrightarrow{v} = x_1\overrightarrow{e}_1 + \cdots + x_n\overrightarrow{e}_n,$$

avec $x_i \in K$. Posons

$$\|\overrightarrow{v}\|_1 = \sum_{i=1}^{n} \|x_i\|_K,$$

$$\|\overrightarrow{v}\|_2 = \left(\sum_{i=1}^{n} \|x_i\|_K^2\right)^{1/2},$$

$$\|\overrightarrow{v}\|_\infty = \max_{1\leqslant i\leqslant n} \|x_i\|_K.$$

Alors $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$ sont des normes sur V (qui dépendent, bien sûr, du choix de la base $\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n$). La vérification des propriétés i)-iii) pour ces normes est bien connue si $K = \mathbb{R}$ et dans le cas général ça marche pareil.

2) Soit $M_n(K)$ 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 $M_n(K)$ s'écrit:

$$\|M\|_\infty = \max_{1\leq i,j\leq n} \|a_{ij}\|_K, \qquad M = (a_{ij})_{1\leq i,j\leq n}.$$

Cette norme joue un rôle important dans la preuve du théorème 2.2.7.

Soient $\overrightarrow{a} \in V$ et $r > 0$. L'ensemble

$$B(\overrightarrow{a}, r) = \{\overrightarrow{v} \in V \mid \|\overrightarrow{v} - \overrightarrow{a}\|_V < r\}$$

est appelé la boule ouverte de centre $\overrightarrow{a}$ et de rayon r. On dit que $X \subseteq V$ est un ouvert si et seulement si pour tout $\overrightarrow{v} \in X$ il existe $r > 0$ tel que

$$B(\overrightarrow{v}, r) \subseteq X.$$

Donc, une norme $\|\cdot\|_V$ définie une topologie sur V.

DÉFINITION. *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 $\overrightarrow{v} \in V$*

$$(*) \qquad C_1 \| \overrightarrow{v} \|_V \leqslant \| \overrightarrow{v} \|'_V \leqslant C_2 \| \overrightarrow{v} \|_V .$$

Nous admettons les résultats suivants:

PROPOSITION 2.2.2. *Deux normes $\| \cdot \|_V$ et $\| \cdot \|'_V$ sont équivalentes si et seulement si elles définissent la même topologie sur V.*

THÉORÈME 2.2.3. *Soit V un espace vectoriel de dimension finie sur un corps* **complet** *pour une valeur absolue non-triviale. Alors toutes les normes sur V sont équivalentes.*

PREUVE. Si $K = \mathbb{R}$, c'est un résultat "classique" bien connu. Dans le cas général la preuve est un peu plus compliquée. Voir [L], prop. 12.2.2.

Comme K est complet, le raisonnement "coordonnée par coordonnée" montre que V est complet pour la topologie $\| \cdot \|_\infty$. En appliquant le théorème on obtient:

COROLLAIRE 2.2.4. *Si K est complet, alors V est complet pour toute norme $\| \cdot \|_V$ sur V.*

PROPOSITION 2.2.5. *Soit K un corps complet pour une valeur absolue $\| \cdot \|_K$. Les assertions suivantes sont équivalentes.*
i) K est localement compact;
ii) Pour tous $\overrightarrow{a} \in V$ et $r > 0$ la boule fermée

$$B_f(\overrightarrow{a}, r) = \{ \overrightarrow{u} \in V \mid \| \overrightarrow{u} - \overrightarrow{a} \|_V \leq r \}$$

est compacte.

PREUVE. Reprendre la démonstration de la proposition 2.2.1 avec les modifications évidentes.

PROPOSITION 2.2.6. *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.*

PREUVE. Supposons que K est 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

$$W = Ue_1 + Ue_2 \cdots + Ue_n = \{ \sum_{i=1}^{n} a_i e_i \mid a_i \in U \}$$

est un voisinage de $\vec{0}_V$. 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 $B_f(\vec{O}_V, r)$ est un compact. Soit pr_1 la projection

$$\begin{aligned} pr_1 \ &: \ V \to K, \\ pr_1(a_1e_1 + \cdots + a_ne_n) &= a_1. \end{aligned}$$

Par la définition de la norme $\| \cdot \|_\infty$ on a $pr_1(B_f(0_V, r)) = B_f(0, r)$. Comme l'image continue d'un compact est compact on en déduit la compacité de $B_f(0, r)$.

2.2. Prolongement d'une valeur absolue.

Soit K un corps muni d'une valeur absolue $\| \cdot \|_K$ et soit L/K une extension finie de K. On dit qu'une valeur absolue $\| \cdot \|_L$ sur L prolonge $\| \cdot \|_K$ si $\|x\|_L = \|x\|_K$ pour tout $x \in K$.

THÉORÈME 2.2.7. *Soit K un corps complet pour une valeur absolue $\| \cdot \|_K$ et soit L/K une extension. Alors il existe un prolongement $\| \cdot \|_L$ de $\| \cdot \|_K$ à L est un seul. Ce prolongement est donné par la formule:*

$$\|x\|_L = \|N_{L/K}(x)\|_K^{1/n}, \qquad x \in L,$$

où $n = [L : K]$.

Le corps L est complet pour la topologie définie par $\| \cdot \|_L$.

PREUVE. Nous allons démontrer ce théorème pour les extensions séparables des corps localement compacts. C'est le seul cas qui nous intéresse. Dans le cas général la preuve est plus difficile (voir [L] ???).

a) Nous démontrons d'abord l'unicité du prolongement de $\| \cdot \|_K$ à L. Soient $\| \cdot \|_L$ et $\| \cdot \|'_L$ deux prolongements de $\| \cdot \|_K$. Considérons L comme un espace véctoriel de dimension finie sur K. Alors $\| \cdot \|_L$ et $\| \cdot \|'_L$ sont deux normes sur L. Par le théorème 2.2.3 elles sont équivalentes et définissent ainsi la même topologie sur L. Donc $\| \cdot \|_L$ et $\| \cdot \|'_L$ sont équivalentes en tant que valeurs absolues et par la proposition 2.1.3 il existe $c > 0$ tel que

$$\|x\|'_L = \|x\|_L^c$$

pour tout $x \in L$. Comme $\| \cdot \|_L$ et $\| \cdot \|'_L$ prolongent $\| \cdot \|_K$, pour tout $x \in K$ on doit avoir

$$\|x\|'_L = \|x\|_K = \|x\|_L,$$

d'où on obtient $c = 1$. Donc, $\| \cdot \|'_L = \| \cdot \|_L$.

b) Passons maintenant à la preuve de l'existence. Posons

$$\|x\|_L = \|N_{L/K}(x)\|_K^{1/n}, \qquad x \in L,$$

où $n = [L : K]$ et $N_{L/K}$ désigne l'application "norme". Nous allons montrer que $\| \cdot \|_L$ fournit un prolongement de $\| \cdot \|_K$ à L. On a:

- $\|x\|_L = 0 \Leftrightarrow N_{L/K}(x) = 0 \Leftrightarrow x = 0$,
- $\|xy\|_L = \|N_{L/K}(xy)\|_L = \|N_{L/K}(x)\, N_{L/K}(y)\|_K = \|x\|_L \|y\|_L$,
- *Si $x \in K$, alors $N_{L/K}(x) = x^n$, d'où $\|x\|_L = \|x\|_K$.*

Donc il reste à montrer que $\| \cdot \|_L$ vérifie

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

Nous allons montrer que

$$(*) \qquad \|1+x\|_L \leqslant 2, \qquad si\ \|x\|_L \leq 1.$$

Par la proposition 2.1.1 ça implique l'inégalité triangulaire.

c) Soit $x \in L$ et soit $K(x)$ l'extension de K qui est engendrée par x. Alors

$$N_{L/K}(x) = (N_{K(x)/K}(x))^{[L:K(x)]},$$

d'où

$$\|x\|_L = \|N_{K(x)/K}(x)\|_K^{1/[K(x):K]} = \|x\|_{K(x)}$$

et

$$\|1+x\|_L = \|1+x\|_{K(x)}.$$

La formule (*) s'écrit ainsi:

$$\|1+x\|_{K(x)} \leqslant 2, \qquad si\ \|x\|_{K(x)} \leq 1.$$

Donc, on peut supposer que $L = K(x)$.

d) Soit $f_x : L \to L$ l'application "multiplication par x" et soit M la matrice de f_x dans la base $1, x, \ldots, x^{n-1}$ de L/K. Alors:

$$N_{L/K}(x) = \det(M), \qquad N_{L/K}(1+x) = \det(I_n + M).$$

Soit $\|M\|_\infty$ la norme du maximum des coefficients. Le lemme suivant joue un rôle clé dans la démonstration.

LEMME 2.2.8. *La suite $\|M\|_\infty$, $k \in \mathbb{N}$ est bornée.*

PREUVE. 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

$$S = \{X \in M_n(K) \mid \|X\|_\infty = 1\}.$$

Demontrons le lemme par l'absurde. Supposons que la suite $\|M^k\|_\infty$ n'est pas 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 $\psi : L \to L$ 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 $\|x\|_L \leq 1$, on a

$$\|\det(B)\|_K = \lim_{s\to\infty} \frac{\|det(M^{k_s})\|_K}{\|b_{k_s}\|_K^n} = \lim_{s\to\infty} \frac{N_{L/K}(x)\|_K^{k_s}}{\|b_{k_s}\|_K^n} = \lim_{s\to\infty} \frac{\|x\|_L^{k_s}}{\|b_{k_s}\|_K^n} = 0.$$

Donc $\det(B) = 0$ ce qui signifie qu'il existe un élément non-nul $\alpha \in L$ 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 $i = 1, \dots, n-1$. Comme les éléments $\alpha, \alpha x, \dots, \alpha x^{n-1}$ forment 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 2.2.7. Par le lemme 2.2.8 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 $card(S_n) = n!$, on a

$$\|\det(M)\|_K \leqslant n!\|M\|_\infty^n.$$

Soit $C_2 = (n!)^{1/n}$. Alors pour tout $m \geq 1$ on a

$$\|N_{L/K}(1+x)\|_K^m = \|\det(I_n + M)^m\|_K^{1/n} \leq C_2\|(I_n + M)^m\|_\infty \leq$$
$$\leq C_2 \sum_{k=0}^m \|C_m^k M^k\|_\infty = C_2 \sum_{k=0}^m \|C_m^k 1_K\|_K \|M^k\|_\infty \leq C_2 C_1 \sum_{k=0}^m \|C_m^k 1_K\|_K.$$

Comme $\|C_m^k 1_K\|_K \leq C_n^k$, on obtient

$$\|N_{L/K}(1+x)\|_K^m \leq C_1 C_2 \sum_{k=0}^m C_m^k = C_1 C_2 2^m.$$

Donc

$$\|N_{L/K}(1+x)\|_K \leq 2(C_1 C_2)^{1/m}$$

pour tout $m \geq 1$. En passant à la limite quand $m \to \infty$ on obtient (*). Le théorème est démontré.

Corollaire 2.2.9. *Soit L/K une extension galoisienne et soit $G = Gal(L/K)$. Alors pour tous $x \in L$ et $g \in G$ on a*

$$\|g(x)\|_L = \|x\|_L.$$

Preuve. Il est facile à voir que la formule $\|x\|'_L = \|g(x)\|_L$ défini une valeur absolue sur L qui prolonge $\|\cdot\|_K$. Par l'unicite du prolongement on a $\|\cdot\|'_L = \|\cdot\|_L$, d'où le corollaire.

COROLLAIRE 2.2.10. *Soit L/K un extension galoisienne. Alors l'action de $G = Gal(L/K)$ sur L est continue.*

PREUVE. Par le corollaire 2.2.9 on a

$$\|g(x) - g(y)\|_L = \|x - y\|_L,$$

d'où le résultat.

COROLLAIRE 2.2.11. *Soit L/K une extension séparable. Alors les applications $N_{L/K}$ et $Tr_{L/K}$ sont continues.*

PREUVE. On a

$$N_{L/K}(x) = \prod_{\sigma \in Hom_K(L,\bar{K})} \sigma(x).$$

Soit M une extension galoisienne finie qui contient L. Alors tout $\sigma \in Hom_K(L, \bar{K})$ admet un prolongement $\hat{\sigma}$ à M. Par le corollaire 2.2.10 $\hat{\sigma}$ sont continues sur M, donc la fonction

$$x \mapsto \prod_{\hat{\sigma}} \hat{\sigma}(x)$$

est continue sur M. Alors elle est continue sur $L \subseteq M$, d'où le corollaire. Pour $Tr_{L/K}$ la preuve est la même.

§3. Prolongement des valeurs absolues: cas général

3.1. Prolongement des valeurs absolues.

Dans ce paragraphe on ne suppose K complet. On s'intéresse des toutes les valeurs absolues de K qu'on note $\| \cdot \|_v$, où v parcourt certaine famille d'indices. Pour simplifier la notation on écrira souvent v au lieu de $\| \cdot \|_v$. Soit L/K une extension finie. Comme dans le paragraphe précédent on dit qu'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 $x \in K$. 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 que L/K est séparable (c'est le seul cas qui nous intéresse). Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$. On note $f(X) \in K[X]$ le polynôme minimal de α sur K. Soit K_v le complété de K pour v. Alors le polynôme $f(X)$ peut être réductible sur K_v et on note

$$f(X) = f_1(X) \cdot f_2(X) \cdot \ldots \cdot f_k(X), \qquad f_i(X) \in K_v[X]$$

la factorisation de $f(X)$ en produit de facteurs irréductibles sur K_v. Comme $f(X)$ est séparable, on a $f_i(X) \neq f_j(X)$ si $i \neq j$.

Comme $K \subseteq K_v$, on a $\bar{K} \subseteq \bar{K}_v$ ce qui permet d'identifier les racines de $f(X)$ aux racines des polynômes $f_i(X)$. Pour tout i on note $\alpha_{i,1}, \ldots \alpha_{i,m_i}$ les racines de $f_i(X)$ et on pose $L_{ij} = K_{\mathfrak{p}}(\alpha_{ij})$. Comme $f_i(X)$ est irréductible, les corps $L_{i,1}, L_{i,2}, \ldots, L_{i,m_i}$ sont conjugués sur K_v. Plus précisement, il existe des isomorphismes

$$\tau_{ij} \ : \ L_{i1}/K_v \xrightarrow{\sim} L_{ij}/K_v, \qquad j = 1, \ldots, m_i$$

vérifiant $\tau_{ij}(\alpha_{i1}) = \alpha_{ij}$. Soit $\| \cdot \|_{ij}$ la valeur absolue sur L_{ij}. Par l'unicité du prolongement de valeur absolue (théorème 2.2.7) on a

$$\|\tau_{ij}(x)\|_{ij} = \|x\|_{i1}, \qquad x \in L_{i1}.$$

Pour tous $1 \leqslant i \leqslant k$ et $1 \leqslant j \leqslant m_i$ on note

$$\sigma_{ij} \ : \ L/K \to \bar{K}/K$$

l'homomorphisme défini par $\sigma_{ij}(\alpha) = \alpha_{ij}$. En composant σ_{ij} avec le plongement $K(\alpha_{ij}) \hookrightarrow L_{ij}$ on obtient des homomorphismes

$$L \overset{\sigma_{ij}}{\to} K(\alpha_{ij}) \hookrightarrow L_{ij}$$

qu'on notera encore σ_{ij} pour simplifier la notation. Alors on a

$$\sigma_{ij} = \tau_{ij} \circ \sigma_{i1}, \qquad j = 1, \dots, m_i.$$

Pour tout $i = 1, \dots, k$ on définit une valeur absolue w_i de L en posant:

$$\|x\|_{w_i} = \|\sigma_{ij}(x)\|_{ij}, \qquad x \in L$$

et on vérifie les propriétés suivantes:

i) w_i ne depend pas du choix de $j = 1, \dots, m_i$.

Preuve. On a $\|\sigma_{ij}(x)\|_{ij} = \|\tau_{ij}(\sigma_{i1}(x))\|_{ij} = \|\sigma_{i1}(x)\|_{i1}$ ce qui montre qu'on peut poser $j = 1$ dans la définition de w_i.

ii) Le complété de L pour w_i est isomorphe à L_{ij}.

Preuve. rappelons que $\sigma_{ij}(L)$ est dense dans L_{ij}.

iii) Les valeurs absolues $w_1, \dots, w_k$ sont deux à deux distincts.

Preuve. Comme les polynômes $f_i(X)$ sont deux à deux distincts, les extensions $L_{1,1}/K_v, L_{2,1}/K_v, \dots, L_{k,1}/K_v$ sont deux à deux non-isomorphes ce qui entraîne que les valeurs absolues $w_1, \dots, w_k$ sont deux à deux non-équivalentes.

Théorème 2.3.1. *Les valeurs absolues $w_1, \dots, w_k$ sont précisement celles qui prolongent v. On a*

$$\sum_{w|v} [L_w : K_v] = [L : K].$$

Preuve. Il est clair que $w_1, \dots, w_k$ prolongent v. Réciproquement, soit w une valeur absolue sur L qui prolonge v. Alors L_w est une extension de K_v et il existe un homomorphisme $\sigma \ : \ L_w/K_v \to \bar{K}_v/K_v$. L'élément $\sigma(\alpha)$ est une raçine de $f(X)$ dans $\bar{K}_v$ i.e. il existe i et j tels que $\sigma(\alpha) = \alpha_{ij}$. Donc σ fournit un isomorphisme

$$\sigma \ : \ L_w/K \to L_{ij}/K_v.$$

Par l'unicité du prolongement (théorème 2.2.7) la valeur absolue sur L_w est donnée par

$$\|x\|_{L_w} = \|\sigma(x)\|_{ij}.$$

En particulier, si $x \in L$ on a

$$\|x\|_{L_w} = \|\sigma_{ij}(x)\|_{ij} = \|x\|_{w_i},$$

d'où $w = w_i$ i.e. $w_1, \dots, w_k$ sont toutes les valeurs absolues au-dessus de v.

Comme $[L_{w_i} : K_v] = [L_{ij} : K_v] = m_i$ on a

$$\sum_{i=1}^{k} [L_{w_i} : K_v] = \sum_{i=1}^{k} m_i = deg(f(X)) = [L : K].$$

Le théorème est démontré.

COROLLAIRE 2.3.2. *Pour tout $\sigma \in Hom_{K_v}(L_w, \bar{K}_v)$ la restriction $\sigma|_L$ de σ à L est un homomorphisme $L/K \to \bar{K}/K$ et l'application*

$$\bigcup_{w|v} Hom_{K_v}(L_w, \bar{K}_v) \to Hom_K(L, \bar{K}),$$
$$\sigma \mapsto \sigma|_L$$

ainsi définie, est une bijection.

PREUVE. Comme $card(Hom_K(L, \bar{K})) = [L : K]$ et $card(Hom_{K_v}(L_w, \bar{K}_v)) = [L_w : K_v]$ les ensembles $Hom_K(L, \bar{K})$ et $\cup_{w|v} Hom_{K_v}(L_w, \bar{K}_v)$ ont même cardinal.Donc il suffit montrer la surjectivité. Tout élément de $Hom_K(L, \bar{K})$ est de la forme $\sigma_{ij} : L/K \to K(\alpha_{ij})$, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant m_i$. Par continuité, σ_{ij} se prolonge à un isomorphisme $\phi_{ij} : L_{w_i} \simeq L_{ij} \subset \bar{K}_{\mathfrak{p}}$ qui vérifie, donc, la condition $\phi_{ij}|_L = \sigma_{ij}$.

COROLLAIRE 2.3.3. *Soit v une valeur absolue sur K. Alors pour tout $x \in L$ on a*

$$Tr_{L/K}(x) = \sum_{w|v} Tr_{L_w/K_v}(x),$$
$$N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x).$$

PREUVE. Comme

$$Tr_{L/K}(x) = \sum_{\sigma \in Hom_K(L, \bar{K})} \sigma(x),$$
$$N_{L/K}(x) = \prod_{\sigma \in Hom_K(L, \bar{K})} \sigma(x),$$

le corollaire découle du corollaire 2.3.3.

COROLLAIRE 2.3.4. *Soit v une valeur absolue sur K est soit L/K une extension séparable. Alors pour tout $x \in L$ on a*

$$\prod_{w|v} \|x\|_w^{[L_w : K_v]} = \|N_{L/K}(x)\|_v .$$

PREUVE. Par le théorème 2.2.7 on a

$$|x\|_w^{[L_w : K_v]} = \|N_{L_w/K_v}(x)\|_v$$

et la formule voulue découle du corollaire 2.3.3.

3.2. Extensions galoisiennes.

Nous supposons maintenant que L/K est une extension galoisienne finie. On note $G = Gal(L/K)$ 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:

$$\|x\|_{(g_1g_2)w} = \|(g_1g_2)^{-1}(x)\|_w = \|g_2^{-1}(g_1^{-1}x)\|_w = \|g_1^{-1}(x)\|_{g_2w} = \|x\|_{g_1(g_2w)}.$$

Donc on a

$$(g_1g_2)w = g_1(g_2w),$$

ce qui signifie que le groupe G opère sur S_v.

Définition. *On appelle groupe de décomposition de w et on note G_w le stabilisateur de w dans G:*

$$G_w = \{g \in G \,|\, gw = w\}.$$

On déduit de cette définition les propriétés suivantes:

i) Pour tout $g \in G$ on a $G_{gw} = gGg^{-1}$;

ii) Soit $\{x_n\} \subset L$ une suite de Cauchy pour w. Si $g \in G$, alors $\{g(x_n)\}$ est une suite de Cauchy pour w.

Preuve. On a

$$\|g(x_n) - g(x_m)\|_w = \|g(x_n - x_m)\|_w = \|x_n - x_m\|_{g^{-1}w} = \|x_n - x_m\|_w,$$

d'où la propriété ii).

iii) On a une inclusion naturelle

$$G_w \to Gal(L_w/K_v).$$

Preuve. Par ii) tout automorphisme $g \in G_w$ se prolonge par continuité à L_w.

Théorème 2.3.5. *i) Le groupe de Galois G opère sur S_v transitivement i.e. pour tous $w, w' \in S_v$ il existe $g \in G$ tel que $w' = gw$.*

ii) L'inclusion $G_w \to Gal(L_w/K_v)$ est un isomorphisme.

Preuve. Soit $G = \cup_{i=1}^r g_i G_w$ la décomposition de G selon G_w et soit $w_i = g_i w$. Comme l'ordre de $Gal(L_w/K_v)$ est égal à $[L_w : K_v]$, on a:

$$|G| = r|G_w| = \sum_{i=1}^{r} |G_{w_i}| \leq \sum_{i=1}^{r} [L_{w_i} : K_v] \leq$$
$$\leq \sum_{w|v} [L_w : K_v] = [L : K] = |G|.$$

Donc on a des égalités partout. En particulier:

a) $|G_{w_i}| = [L_{w_i} : K_v]$ ce qui montre que les inclusions $G_{w_i} \to Gal(L_{w_i}/K_v)$ 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 on déduit que G opère transitivement sur S_v.

§4. Valeurs absolues non-archimédiennes

Dans ce paragraphe nous étudions les valeurs absolues non-archimédiennes qui joue un rôle très important en théorie des nombres.

DÉFINITION. *Soient K un corps et $\|\cdot\|$ une valeur absolue sur K. On dit que $\|\cdot\|$ est non-archimédienne ou ultramétrique si au lieu de la condition*

$$\|x+y\| \leq \|x\| + \|y\|$$

elle vérifie la condition plus forte:

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

Voici deux propriétés élémentaires des valeurs absolues non-archimédiennes qui découlent directement de cette définition:

i) Soit $\|\cdot\|$ une valeur absolue non-archimédienne. Si $\|x\| > \|y\|$, alors

$$\|x+y\| = \|x\|.$$

PREUVE. 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) $\|\cdot\|$ est non-arcimédienne si et seulement si $\|x\| \leq 1$ implique $\|1+x\| \leq 1$.

PREUVE. C'est clair.

iii) Une valeur absolue $|\cdot\|$ est non-archimédienne si et seulement si

$$\|n1_K\| \leq 1, \qquad \textit{pour tout } n \in \mathbb{N}.$$

PREUVE. Soit $\|x\| \leq 1$. Alors

$$\|1+x\|^n = \|(1+x)^n\| = \|\sum_{k=0}^{n} C_n^k x^k\| \leq \sum_{k=0}^{n} \|C_n^k 1_K\| \|x\|^k \leq \sum_{k=0}^{n} \|x\|^k \leq n+1.$$

Donc $\|1+x\| \leq (n+1)^{1/n}$. En passant à la limite quand $n \to \infty$ on obtient que $\|1+x\| \leq 1$ ce qui montre que $\|\cdot\|$ est non-archimédienne.

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.

PREUVE. Ça découle directement de iii).

PROPOSITION 2.4.1. *Soit K un corps muni d'une valeur absolue non-archimédienne $\|\cdot\|$. Alors l'ensemble*

$$O = \{x \in K \mid \|x\| \leq 1\}$$

est un anneau appelé l'anneau de valuation. Le groupe des unité de O coïncide avec

$$U = \{x \in K \mid \|x\| = 1\}.$$

L'ensemble

$$\mathfrak{m} = \{x \in K \mid \|x\| < 1\}$$

est un idéal maximal de O et un seul. Le corps des fractions de O coïncide avec K dans lequel O est intégralement clos.

PREUVE. Soient $x, y \in O$. Alors

$$\|x \pm y\| \leq max\{\|x\|, \|y\|\} \leq 1,$$
$$\|xy\| = \|x\| \, \|y\|,$$

d'où on déduit que O est un anneau.

Soit $x \in O$. Alors $x^{-1} \in O$ 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 tous $x, y \in \mathfrak{m}$ on a

$$\|x \pm y\| \leq max\{\|x\|, \|y\|\} < 1.$$

Si $x \in O$ et $y \in \mathfrak{m}$, alors

$$\|xy\| = \|x\| \, \|y\| < 1.$$

Donc, $\mathfrak{m}$ est un idéal de O et on a

$$U \cup \mathfrak{m} = O.$$

Soit I un idéal de O. Si $I \nsubseteq \mathfrak{m}$, alors $I \cap U \neq \varnothing$ i.e. I contient une unité de O, d'où $I = O$. Donc $\mathfrak{m}$ est l'idéal maximal de O.

Soit $x \in K$. Si $\|x\| \leq 1$, on a $x \in O$ juste par définition. Sinon $\|x\| > 1$, d'où $\|1/x\| < 1$ et $x^{-1} \in O$. Donc K est le corps des fractions de O.

On montre que O est intégralement clos dans K. Soit $x \in K$ un élément entier sur O. Alors

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 = 0, \qquad a_i \in O.$$

Supposons que $x \neq O$. 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 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. *Le corps $k = O/\mathfrak{m}$ est appelé le corps résiduel de O.*

Dans la suite nous allons utiliser les notations et les conventions suivantes.

a) Si K est complet pour une valeur absolue, on ne s'interesse que de cette valeur absolue qu'on note $\|\cdot\|_K$. En particulier, si $\|\cdot\|_K$ est non-archimédienne, on notera O_K l'anneau de valuation, $\mathfrak{m}_K$ l'idéal maximal de O_K, U_K le groupe des unités et $k_K = O_K/\mathfrak{m}_K$ le corps résiduel.

b) Si K n'est pas complet on s'interesse des toutes les valeurs absolues sur K qu'on note $\|\cdot\|_v$ où on laisse v parcourir une famille d'indices. En particulier, si $\|\cdot\|_v$ est non-archimédienne, on note A_v l'anneau de valuation, $\mathfrak{m}_{A_v}$ l'idéal maximal de A_v, $U(A_v)$ le groupe des unités et $k_v = A_v/\mathfrak{m}_{A_v}$ le corps résiduel. On notera K_v le complété de K pour $\|\cdot\|_v$, O_v l'anneau de valuation de K_v et $\mathfrak{m}_v$ l'idéal maximal de O_v.

Etudions maintenant la convergence des séries dans un corps complet K. Une série

$$(*) \qquad \sum_{k=0}^{\infty} a_k$$

est convergente 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

$$\|a_n\|_K = \|S_n - S_{n-1}\|_K \underset{n\to\infty}{\to} 0.$$

Dans le cas général la réciproque est fausse, i.e. la condition $a_n \to 0$ n'est pas suffisante pour que la série (*) converge (on peut, par exemple, prendre $K = \mathbb{R}$). Neanmoins, si la valeur absolue $\|\cdot\|_K$ est non-archimédienne, la situation est très agréable:

PROPOSITION 2.4.2. *Soit K un corps complet pour une valeur absolue non-archimédienne. Alors une série*

$$\sum_{k=1}^{\infty} a_k, \qquad a_k \in K$$

est convergente si et seulement si $a_k \underset{k\to\infty}{\to} 0$.

PREUVE. i) Soit

$$S_n = \sum_{k=0}^{n} a_k.$$

Si $m \geqslant n$, alors

$$\|S_m - S_n\|_K = \|\sum_{k=n+1}^{m} a_k\|_K \leqslant \max_{n+1\leqslant k\leqslant m} \|a_k\|_K.$$

Soit $\epsilon > 0$. Si $a_k \to 0$, il existe N tel que $\|a_k\|_K < \epsilon$ pour tout $k > N$. Alors, pour tous $m, n \geqslant N$ on a

$$\|S_m - S_n\|_K < \epsilon.$$

Donc S_n est une suite de Cauchy ce qui entraîne la convergence car K est complet.

PROPOSITION 2.4.3 (LEMME DE HENSEL). *Soit K un corps complet pour une valeur absolue non-archimédienne. Soit $f(X)$ un polynôme à coéfficients dans O_K. Si α_0 est un élément de O_K vérifiant*

$$\|f(\alpha_0)\|_K < \|f'(\alpha_0)\|_K\,,$$

alors la suite

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

convèrge à une racine de $f(X)$.

PREUVE. Posons $C = \|f(\alpha_0)\|_K$ et $\gamma = \left\|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right\|_K < 1$. On va démontrer par récurrence que pour tout $i \geqslant 1$ on a

i) $\|f(\alpha_i)\|_K \leqslant C\gamma^i$;

ii) $\|f'(\alpha_i)\|_K = \|f'(\alpha_0)\|_K$.

Soit $\alpha_{i+1} = \alpha_i + h$ avec $h \in O_K$. Alors le développement en série de Taylor donne

$$f(\alpha_{i+1}) = f(\alpha_i) + hf'(\alpha_i) + h^2 g\,,$$

où $g \in O$ est un élément qui dépend de h et de α_i et dont la forme explicite n'est pas importante pour la suite. En prenant $h = f(\alpha_i)/f'(\alpha_i)$ on obtient

$$f(\alpha_{i+1}) = f(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)^2}g\,.$$

Si les formules i) et ii) sont vraie au rang i, alors

$$\|f(\alpha_{i+1})\|_K \leqslant \|f(\alpha_i)\|_K \left\|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right\|_K \leqslant C\gamma^{i+1}\,.$$

D'autre part, on a

$$f'(\alpha_{i+1}) \;=\; f'(\alpha_i) - f"(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \cdots = f'(\alpha_i)\left(1 - f"(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)^2} + \cdots\right)$$

et comme

$$\|f'(\alpha_i)\|_K = \|f'(\alpha_0)\|_K$$

et

$$\|f(\alpha_i)\|_K \leqslant C\gamma^i$$

on obtient que

$$\left\|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right\|_K \leqslant \left\|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right\|_K < 1$$

i.e. que

$$1 - f"(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)^2} + \cdots$$

est une unité dans O_K. Donc,

$$\|f(\alpha_{i+1})\|_K = \|f(\alpha_i)\|_K = \|f(\alpha_0)\|_K$$

et les formules i) et ii) sont établies.

Pour déduire la propositions de ces formules on remarque que comme

$$\left\| \frac{f(\alpha_i)}{f'(\alpha_i)} \right\|_K \leqslant \frac{C}{\|f'(\alpha_0)\|_K} \gamma^i \underset{i\to\infty}{\longrightarrow} 0$$

la suite $\frac{f(\alpha_i)}{f'(\alpha_i)}$ tend vers 0. Donc, la suite $\{\alpha_i\}$ est convergente. Si on note $\alpha = \lim_{i\to\infty} \alpha_i$, sa limite, on obtient

$$f(\alpha) = \lim_{i\to\infty} f(\alpha_i) = 0$$

car

$$\|f(\alpha_i)\|_K \leqslant C\gamma^i \underset{i\to\infty}{\longrightarrow} 0\,.$$

La proposition est démontrée.

Voici un cas particulier très util du lemme de Hensel.

COROLLAIRE 2.4.4. *Soit $f(X) \in O_K[X]$ un polynôme à coéfficients dans O_K est soit $\bar{f}(X) \in k_K[X]$ la réduction de $f(X)$ modulo $\mathfrak{m}_K$. Si $\bar{\alpha} \in k_K$ est une racine simple de $\bar{f}(X)$, alors il existe une racine $\alpha \in O_K$ de $f(X)$ telle que $\bar{\alpha} = \alpha \pmod{\mathfrak{m}_K}$ et une seule.*

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 O_K. D'autre part, comme $\bar{f}(\bar{\alpha}) = 0$, on a $\|f(\alpha_0)\|_K \leqslant 1$ 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 $\bar{\alpha} = \beta \pmod{\mathfrak{m}_K}$. On a

$$f(X) = (X - \alpha)g(X),$$

avec $\bar{g}(\alpha) \neq 0$ car $\bar{\alpha}$ est une racine simple de $\bar{f}(X)$. En prenant $X = \beta$ on obtient $(\beta - \alpha)g(\beta) = f(\beta) = 0$, d'ou $g(\beta) = 0$. Mais alors

$$\bar{g}(\bar{\alpha}) = \bar{g}(\bar{\beta}) = 0,$$

ce qui donne une contradiction.

§5. Valuations discrètes

DÉFINITION. *Soit K un corps. On appelle valuation discrète sur K une application surjective*

$$v \;:\; K^* \to \mathbb{Z},$$

satisfaisant aux propriétés suivantes:

i) v est un homomorphisme, i.e.

$$v(xy) = v(x) + v(y)$$

pour tous $x, y \in K^*$.

ii) Pour tous $x, y \in K^*$ *on a*

$$v(x+y) \geqslant \min\{v(x), v(y)\}.$$

On prolonge v *sur* K *en posant* $v(0) = +\infty$.

Remarque. L'hypothèse de surjectivité n'est pas importante et sert à normaliser v. En effet, si $v : K^* \to \mathbb{Z}$ est un homomorphisme non-nul, alors son image $v(K^*)$ est un sous-groupe de $\mathbb{Z}$. Donc, il existe $n > 0$ tel que $v(K^*) = n\mathbb{Z}$ et en posant $v'(x) = v(x)/n$ un obtient un homomorphisme surjectif $v' : K^* \to \mathbb{Z}$.

Soit K un corps muni d'une valuation discrète v. On fixe un réel $\rho \in]0;1[$ et on pose

$$\|x\|_v = \rho^{v(x)}, \qquad x \in K.$$

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) $\|x+y\|_v \leqslant \rho^{\min\{v(x),v(y)\}} = \max\{\|x\|_v, \|y\|_v\}$.

Donc, $\| \cdot \|_v$ 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

$$\|x\|_1 = \|x\|_v^c, \qquad \textit{pour tout } x \in K.$$

et la proposition 2.1.3 implique que $\| \cdot \|_1$ et $\| \cdot \|_v$ sont équivalentes i.e. qu'elles induisent la même topologie sur K.
La propriété i), §4 s'écrit:

$$v(x+y) = v(x), \qquad \textit{si } v(x) < v(y).$$

Rappelons la définition d'un anneau de valuation discrète donnée dans le chapitre I,§7.

Définition. *Soit* A *un anneau intègre. On dit que* A *est un anneau de valuation discrète s'il est principal et possède un idéal premier non-nul et un seul.*

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 $u \in U(A)$ est une unité. Tout élément non-nul $a \in A$ s'écrit

$$a = u\pi^k, \qquad u \in U(A), \ k \in \mathbb{N}$$

et on a

$$A = \mathfrak{m} \cup U(A), \qquad \mathfrak{m} \cap U(A) = \varnothing.$$

Nous allons établir le lien entre les anneaux de valuation discrète et les valuations discrètes qui ont été définies dans ce paragraphe.

THÉORÈME 2.5.1. *1) Soit K un corps muni d'une valuation discrète v. Alors*

$$A_v = \{x \in K \mid v(x) \geqslant 0\}$$

est un anneau de valuation discrète. Plus précisement:

i) $U(A_v) = \{x \in K \mid v(x) = 0\}$ *coïncide avec le groupe des unités de* A_v.

ii) $\mathfrak{m}_{A_v} = \{x \in K \mid v(x) > 0\}$ *est l'idéal maximal de* A_v;

iii) un élément $\pi \in A_v$ *est une uniformisante 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 $x \in K$ s'écrit de façon unique sous la forme

$$x = \pi^n u, \qquad u \in U(A),\ n \in \mathbb{Z}.$$

Posons

$$v(x) = n.$$

Alors v est une valuation discrète sur K telle que $A_v = A$ et $\mathfrak{m}_{A_v} = (\pi)$.

PREUVE. Comme

$$A_v = \{x \in K \mid \|x\|_v \leq 1\},$$

la proposition 2.4.1 montre que A_v est l'anneau de valuation de v. La même proposition implique que $U(A_v) = \{x \in A_v \mid v(x) = 0\}$ 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

$$x = u\pi^{v(x)}, \qquad u \in U(A_v).$$

Soit I un idéal non-nul de A_v. Posons

$$n = \min\{v(x) \mid x \in I\}.$$

Alors I 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 $u_0 \in U(A_v)$, on obtient que $\pi^n = u_0^{-1}x_0 \in I$, d'où

$$(\pi^n) \subseteq I.$$

Réciproquement, si $x \in I$, 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 $I = (\pi^n)$ 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

$$x = u\pi^n, \qquad n \in \mathbb{N},\ u \in U(A).$$

Donc, tout élément x du corps des fractions K de A sécrit de façon unique sous la forme

$$x = u\pi^n, \qquad n \in \mathbb{Z},\ u \in U(A).$$

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 2.5.2. *La valuation discrète v admet un prolongement sur K_v et un seul. Le corps K_v est muni, ainsi, d'une valuation discrète pour laquelle il est complet. L'anneau de valuation 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 $O_v/\mathfrak{m}_v$ est canoniquement isomorphe à $k_v = A_v/\mathfrak{m}_{A_v}$.*

Preuve. Par le théorème 2.1.4, il existe un unique prolongement de $\| \cdot \|_v$ à K_v qu'on note encore $\| \cdot \|_v$ à K_v pour simplifier la notation. Soit $x \in K_v$ un élément non-nul. Il existe une suite $\{x_n\} \subset K$ 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

$$v(x_n) = v(x_{n+1}) \qquad \textit{pour tout } n \geqslant N.$$

Posons

$$(*) \qquad v(x) = v(x_N) = \lim_{n\to\infty} v(x_n) \in \mathbb{Z}.$$

Alors

$$\|x\|_v = \rho^{v(x)}, \qquad x \in K_v.$$

On en déduit que

$$v(x+y) \geqslant \min\{v(x), v(y)\},$$
$$v(xy) = v(x) + v(y),$$

ce qui montre que la formule (*) fournit un prolongement de v à K_v. Il est unique car le prolongement de $\| \cdot \|_v$ à K_v est unique par le théorème 2.1.4.

Soit O_v l'anneau de valuation de K_v. Si $x = \lim_{n\to\infty} x_n \in O_v$, 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 $A_v \subseteq O_v$ et $\mathfrak{m}_{A_v} = \mathfrak{m}_v \cap A_v$, on a une inclusion

$$A_v/\mathfrak{m}_{A_v} \subseteq O_v/\mathfrak{m}_v.$$

Pour montrer que c'est un isomorphisme on remarque que si $y \in O_v$, il existe $x \in A_v$ tel que $v(x-y) \geqslant 1$ (A_v est dense dans 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 $O_v/\mathfrak{m}_v$ est $y + \mathfrak{m}_v$. La proposition est démontrée.

§6. Valuations discrètes d'un anneau de Dedekind

6.1. Valuations discrètes associées aux idéaux premiers.

Nous revenons à l'étude des anneaux de Dedekind. Ce paragraphe peut être vu comme la suite du §8, chapitre I.

Soit A un anneau de Dedekind et soit K son corps des fractions. Soit $\mathfrak{p}$ un idéal premier non-nul de A. On note $A_\mathfrak{p}$ la localisation de A en $\mathfrak{p}$:

$$A_\mathfrak{p} = \left\{ \frac{a}{s} \in K \mid a \in A, s \notin \mathfrak{p} \right\}$$

(voir chapitre I, §7). Comme $A \subseteq A_\mathfrak{p}$, le corps des fractions de $A_\mathfrak{p}$ coïncide avec K. Rappelons (voir théorème 1.7.4) que $A_\mathfrak{p}$ est un anneau de valuation discrète. Son idéal maximal est $\mathfrak{m}_{A_\mathfrak{p}} = \mathfrak{p}A_\mathfrak{p}$ et son corps résiduel $A_\mathfrak{p}/\mathfrak{m}_{A_\mathfrak{p}}$ est isomorphe à $k_\mathfrak{p} = A/\mathfrak{p}$.

Soit $\pi_\mathfrak{p} \in \mathfrak{p} \setminus \mathfrak{p}^2$. Alors $\pi_\mathfrak{p}$ est une uniformisante de $A_\mathfrak{p}$ i.e.

$$\mathfrak{m}_{A_\mathfrak{p}} = (\pi_\mathfrak{p})$$

(voir chapitre I, §6, vi)). On note

$$v_\mathfrak{p} \ : \ K^* \to \mathbb{Z}$$

la valuation discrète de K associée à $A_\mathfrak{p}$. Tout $x \in K^*$ s'écrit de façon unique sous la forme

$$x = \pi_\mathfrak{p}^n u_\mathfrak{p}, \quad u_\mathfrak{p} \in U(A_\mathfrak{p})$$

et on a

$$v_\mathfrak{p}(x) = n.$$

Donnons maintenant les propriétés principales de ces valuations discrètes.

i) Soit $a \in K^*$ et soit

$$(*) \qquad (a) = \prod \mathfrak{p}^{n_\mathfrak{p}(a)}$$

la factorisation de l'idéal fractionnaire principal (a) en produit d'idéaux premiers. Alors pour tout $\mathfrak{p}$ on a

$$v_\mathfrak{p}(a) = n_\mathfrak{p}(a).$$

PREUVE. a) Supposons d'abord que $a \in A$. On reécrit (*) sous la forme

$$(**) \qquad (a) = \mathfrak{p}_1^{n_{\mathfrak{p}_1}(a)} \cdot \mathfrak{p}_2^{n_{\mathfrak{p}_2}(a)} \cdots \mathfrak{p}_k^{n_{\mathfrak{p}_k}(a)}.$$

Rappelons que $A_{\mathfrak{p}_1} = S_{\mathfrak{p}_1}^{-1}A$, où $S_{\mathfrak{p}_1} = A \setminus \mathfrak{p}_1$. Donc, si $i \neq 1$ l'intersection $\mathfrak{p}_i \cap S_{\mathfrak{p}_1}$ est non-vide et par la proposition 1.7.1 on a $S_{\mathfrak{p}_1}^{-1}\mathfrak{p}_i = A_{\mathfrak{p}_1}$ (on peut démontrer cette égalité directement en remarquant que si $s \in \mathfrak{p}_i \cap S_{\mathfrak{p}_1}$, alors $1 = s/s \in S_{\mathfrak{p}_1}^{-1}\mathfrak{p}_i$, d'où $A_{\mathfrak{p}_1} \subseteq S_{\mathfrak{p}_1}^{-1}\mathfrak{p}_i$.) Alors, en multipliant (**) par $S_{\mathfrak{p}_1}^{-1}$ on obtient:

$$aA_{\mathfrak{p}_1} = (A_{\mathfrak{p}_1}\mathfrak{p}_1)^{n_{\mathfrak{p}_1}(a)} = (\pi_{\mathfrak{p}_1})^{n_{\mathfrak{p}_1}(a)}.$$

Donc, a et $\pi_{\mathfrak{p}_1}^{n_{\mathfrak{p}_1}(a)}$ engendrent le même idéal principal dans $A_{\mathfrak{p}_1}$ ce qui montre qu'il existe $u_{\mathfrak{p}_1} \in U(A_{\mathfrak{p}_1})$ tel que

$$a = \pi_{\mathfrak{p}_1}^{n_{\mathfrak{p}_1}(a)} u_\mathfrak{p}.$$

On en déduit que $v_{\mathfrak{p}_1}(x) = n_{\mathfrak{p}_1}(a)$. b) Dans le cas général, si $a \in K^*$, alors il s'écrit $a = b/c$ avec $b, c \in A$. On a $n_\mathfrak{p}(a) = n_\mathfrak{p}(b) - n_\mathfrak{p}(c)$ et $v_\mathfrak{p}(a) = v_\mathfrak{p}(b) - v_\mathfrak{p}(c)$. Par a), on a $n_\mathfrak{p}(b) = v_\mathfrak{p}(b)$ et $n_\mathfrak{p}(c) = v_\mathfrak{p}(c)$, d'où $n_\mathfrak{p}(a) = v_\mathfrak{p}(a)$.

ii) Soit $a \in K^*$. Alors $v_\mathfrak{p}(a) = 0$ pour presque tout $\mathfrak{p}$.

PREUVE. C'est une conséquence immédiate de i).

iii) On a

$$A = \bigcap_\mathfrak{p} A_\mathfrak{p}.$$

Autrement dit, $x \in A$ si et seulement si $v_\mathfrak{p}(x) \geqslant 0$ pour tout $\mathfrak{p}$.

PREUVE. L'inclusion $A \subseteq \cap_\mathfrak{p} A_\mathfrak{p}$ est triviale. Réciproquement, soit $x \in K^*$ et soit

$$(x) = \mathfrak{p}_1^{n_{\mathfrak{p}_1}(x)} \cdot \mathfrak{p}_2^{n_{\mathfrak{p}_2}(x)} \cdots \mathfrak{p}_k^{n_{\mathfrak{p}_k}(x)}.$$

Si $v_\mathfrak{p}(x) \geqslant 0$ pour tout $\mathfrak{p}$, alors $(x) \subseteq A$, d'où $x \in A$.

v) Soient $a, b \in A$. Alors $a \mid b$ si et seulement si $v_\mathfrak{p}(a) \leqslant v_\mathfrak{p}(b)$ pour tout $\mathfrak{p}$.

PREUVE. Soit $c = b/a \in K$. Alors $c \in A$ si et seulement si $v_\mathfrak{p}(b) - v_\mathfrak{p}(a) = v_\mathfrak{p}(c) \geqslant 0$, d'où le résultat.

Le lemme suivant peut être vu comme un analogue du lemme chinois pour les valuations:

LEMME 2.6.1 (LEMME D'APPROXIMATION). *Pour tout $i = 1, \dots, k$ soient $\mathfrak{p}_i$ des idéaux premiers de A distincts deux à deux, $x_i \in K$ et $n_i \geqslant 0$. Alors il existe $x \in K$ tel que*

$$v_{\mathfrak{p}_i}(x - x_i) \geqslant n_i$$

pour tout $i = 1, \dots, k$ et

$$v_{\mathfrak{q}}(x) \geqslant 0 \qquad si\ \mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_k.$$

PREUVE. a) Supposons d'abord que $x \in A$. Alors, par le lemme chinois le système

$$\begin{cases} x \equiv x_1 \pmod{\mathfrak{p}_1^{n_1}} \\ x \equiv x_1 \pmod{\mathfrak{p}_2^{n_2}} \\ \cdots\cdots\cdots\cdots \\ x \equiv x_k \pmod{\mathfrak{p}_k^{n_k}} \end{cases}$$

est résoluble dans A. Comme $x - x_i \in \mathfrak{p}_i^{n_i}$, on a $v_{\mathfrak{p}_i}(x - x_i) \geqslant n_i$.

b) Considérons maintenant la 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:

$$\begin{cases} v_{\mathfrak{p}_i}(y - b_i) \geqslant n_i + v_{\mathfrak{p}_i}(s) \quad pour\ i = 1, \dots, k \\ v_{\mathfrak{q}}(y) \geqslant v_{\mathfrak{q}}(s) \quad si\ \mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_k. \end{cases}$$

Comme $v_{\mathfrak{q}}(s) = 0$ pour presque tout $\mathfrak{q}$, c'est un système finiavec les conditions du type envisagé dans a) (il faut ajouter à la famille $\{\mathfrak{p}_i\}$ les idéaux $\mathfrak{q}$ tels que $v_{\mathfrak{q}}(s) > 0$). Donc il est résoluble. Soit y une solution et soit $x = y/s$. Alors

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

et

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

Le lemme est démontré.

Voici deux cas particuliers de ce lemme.

COROLLAIRE 2.6.2. *Pour tout $i = 1, \dots, k$ soient $\mathfrak{p}_i$ des idéaux premiers de A distincts deux à deux, $x_i \in A_{\mathfrak{p}_i}$ et $n_i \geqslant 0$. Alors il existe $x \in A$ tel que*

$$v_{\mathfrak{p}_i}(x - x_i) \geqslant n_i$$

pour tout $i = 1, \dots, k$.

PREUVE. Comme $v_{\mathfrak{p}_i}(x_i) \geqslant 0$, on a

$$v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(x - x_i + x_i) \geqslant \min\{v_{\mathfrak{p}_i}(x - x_i), v_{\mathfrak{p}_i}(x_i)\} \geqslant 0.$$

Comme $v_{\mathfrak{q}}(x) \geqslant 0$ pour tout $\mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_k$, on obtient que $v_{\mathfrak{p}}(x) \geqslant 0$ pour tout $\mathfrak{p}$ et la propriété iv) implique que $x \in A$.

COROLLAIRE 2.6.3. *Soit $\mathfrak{p}$ un idéal premier de A. Alors pour tous $a \in A_{\mathfrak{p}}$ et $n \geqslant 0$ il existe $x \in A$ tel que*

$$v_{\mathfrak{p}}(x - a) \geqslant n.$$

PREUVE. C'est le cas de $k = 1$ du corollaire 2.6.2.

En utilisant le lemme d'approximation nous allons démontrer la proposition suivante:

PROPOSITION 2.6.4. *Si $\mathfrak{p} \neq \mathfrak{q}$, alors les valuations $v_{\mathfrak{p}}$ et $v_{\mathfrak{q}}$ ne sont pas équivalentes.*

PREUVE. Soit $\pi_{\mathfrak{p}}$ une uniformisante de $A_{\mathfrak{p}}$. Par le corollaire 2.3.2 il existe $x \in A$ tel que $v_{\mathfrak{p}}(x - \pi_{\mathfrak{p}}) \geqslant 2$ et $v_{\mathfrak{q}}(x - 1) \geqslant 1$. Donc

$$v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}((x - \pi_{\mathfrak{p}}) + \pi_{\mathfrak{p}}) = v_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$$

et

$$v_{\mathfrak{q}}(x) = v_{\mathfrak{q}}((x - 1) + 1) = v_{\mathfrak{q}}(1) = 0.$$

Posons $x_n = x^n$. Alors $v_{\mathfrak{p}}(x^n) = n$ ce qui montre que x^n tend vers 0 pour la topologie définie par $v_{\mathfrak{p}}$. Par contre, $v_{\mathfrak{q}}(x^n) = 0$ ce qui signifie que $x^n \nrightarrow 0$ pour la topologie de $v_{\mathfrak{q}}$. Donc, ces deux topologies sont différentes.

Soit $\mathfrak{p}$ un idéal premier de A et soit $v = v_{\mathfrak{p}}$ 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 $K_{\mathfrak{p}}$ au lieu de $K_{v_{\mathfrak{p}}}$ pour simplifier la notation.

La proposition suivante résume ses propriétés principales.

PROPOSITION 2.6.5. *i) Le corps $K_{\mathfrak{p}}$ est complet pour la valuation discrète $\mathfrak{v}_{\mathfrak{p}}$.*
ii) L'anneau de valuation $O_{\mathfrak{p}}$ de $K_{\mathfrak{p}}$ coïncide avec l'adhérence de A dans $K_{\mathfrak{p}}$.
iii) Le corps résiduel de $O_{\mathfrak{p}}$ est isomorphe à $k_{\mathfrak{p}} = A/\mathfrak{p}$.

PREUVE. i) est démontrée dans la proposition 2.5.2.

ii) Soit $x \in O_{\mathfrak{p}}$. Par la proposition 2.5.2 $A_{\mathfrak{p}}$ est dense dans $O_{\mathfrak{p}}$ i.e. pour tout $n \geqslant 0$ il existe $y_n \in A_{\mathfrak{p}}$ tel que $v_{\mathfrak{p}}(x - y_n) \geqslant n$. D'autre part, par le corollaire 2.6.3 il existe $x_n \in A$ tel que $v_{\mathfrak{p}}(y_n - x_n) \geqslant n$. Donc,

$$\begin{aligned} v_{\mathfrak{p}}(x_n - x) &= v_{\mathfrak{p}}((x_n - y_n) + (y_n - x)) \geqslant \\ &\geqslant \min\{v_{\mathfrak{p}}(x_n - y_n), v_{\mathfrak{p}}(y_n - x)\} \geqslant n \end{aligned}$$

ce qui montre que $\{x_n\}$ converge vers x. Donc, A est dense dans $O_{\mathfrak{p}}$.

iii) Par la proposition 2.5.2 le corps résiduel de $O_{\mathfrak{p}}$ est isomorphe à $A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$. D'autre part, $A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ est isomorphe à $k_{\mathfrak{p}} = A/\mathfrak{p}$ par le théorème 1.7.4.

6.2. Extensions.

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 $w_{\mathfrak{P}}$ la valuation discrète de L qui correspond à $\mathfrak{P}$ et $L_{\mathfrak{P}}$ le complété de L pour $w_{\mathfrak{P}}$.

Rappelons la définition suivante:

DÉFINITION. *On dit que* $\mathfrak{P}$ *est au-dessus de* $\mathfrak{P}$ *ou que* $\mathfrak{P}$ *divise* $\mathfrak{p}$ *si* $\mathfrak{P} \cap A = \mathfrak{p}$; *notation* $\mathfrak{P} \mid \mathfrak{p}$.

Si $\mathfrak{p}$ est un idéal premier de A, on a

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})},$$

où $e(\mathfrak{P}/\mathfrak{p})$ est l'indice de ramification de $\mathfrak{P}$ (voir chapitre I, §8).

Soit $x \in K^*$. Alors

$$xA = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$$

(voir §3, ii)). Donc, on a

$$xB = (xA)B = \prod_{\mathfrak{p}} \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})\, v_{\mathfrak{p}}(x)}.$$

En comparant cette formule à la formule

$$xB = \prod_{\mathfrak{P}} \mathfrak{P}^{w_{\mathfrak{P}}(x)}$$

on obtient que pour tout $x \in K$

$$(*) \qquad v_{\mathfrak{p}}(x) = \frac{1}{e(\mathfrak{P}/\mathfrak{p})}\, w_{\mathfrak{P}}(x).$$

Soit $\rho_{\mathfrak{p}} \in]0;1[$ et soit

$$\|x\|_{\mathfrak{p}} = \rho_{\mathfrak{p}}^{v_{\mathfrak{p}}(x)}, \qquad x \in K$$

la valeur absolue sur K associée à $v_{\mathfrak{p}}$. En posant $\rho_{\mathfrak{P}} = \rho_{\mathfrak{p}}^{1/e(\mathfrak{P}/\mathfrak{p})}$ et

$$\|x\|_{\mathfrak{P}} = \rho_{\mathfrak{P}}^{v_{\mathfrak{P}}(x)}, \qquad x \in L$$

on obtient une valeur absolue sur L qui prolonge $\|\cdot\|_{\mathfrak{p}}$. On dira par abus de language que $w_{\mathfrak{P}}$ prolonge $v_{\mathfrak{p}}$ avec l'indice $e(\mathfrak{P}/\mathfrak{p})$.

THÉORÈME 2.6.6. *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* $\|\cdot\|_{\mathfrak{p}}$. *On a:*

$$\sum_{\mathfrak{P}|\mathfrak{p}} [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = [L : K].$$

PREUVE. Par la proposition 2.6.4 les valeurs absolues $\|\cdot\|_{\mathfrak{P}}$ sont deux à deux non-équivalentes. Réciproquement, soit $\|\cdot\|$ une valeur absolue qui prolonge $\|\cdot\|_{\mathfrak{p}}$. Comme $\|\cdot\|_{\mathfrak{p}}$ est non-archimédienne, $|\cdot\|_w$ l'est aussi (voir iv), §4). Soit B_w l'anneau de valuation de w et soit $\mathfrak{m}$ son idéal maximal. Par la proposition 2.4.1 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 $\mathfrak{P} = B \cap \mathfrak{m}$.

Alors $\mathfrak{P} \cap A = \mathfrak{p}$, i.e. $\mathfrak{P}$ est un idéal premier de B qui divise $\mathfrak{p}$. Donc B_w contient l'anneau de valuation discrète $B_{\mathfrak{P}}$. Il est facile de voir (exercice) que tout anneau de valuation discrète est un sous-anneau *maximal* de son corps des fractions. Donc $B_w = B_{\mathfrak{P}}$. Soit $\pi_{\mathfrak{P}}$ une uniformisante de $B_{\mathfrak{P}}$. Si $x = \pi_{\mathfrak{P}}^m \in B_w$, $u \in U(B_w)$, alors

$$\|x\| = \|\pi_{\mathfrak{P}}\|^m, \qquad m = w_{\mathfrak{P}}(x).$$

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 $\|\cdot\| = \|\cdot\|_{\mathfrak{P}}$.

La formule $\sum_{\mathfrak{P}|\mathfrak{p}} [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = [L : K]$ est un cas particulier du théorème 2.3.1.

Nous pouvons expliciter autres résultats du §3 pour notre cas. En particulier on a les formules suivantes:

$$N_{L/K}(x) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x),$$
$$Tr_{L/K}(x) = \sum_{\mathfrak{P}|\mathfrak{p}} Tr_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x), \qquad x \in L.$$

Supposons maintenant que L/K est galoisienne. Soit $G = Gal(L/K)$. 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 $\mathfrak{p}$. Il est facile à montrer (juste par définition) que pour tout $g \in G$ l'ensemble $g(\mathfrak{P})$ 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 $S_{\mathfrak{p}}$.

Soit $v = v_{\mathfrak{p}}$ et soit S_v l'ensemble des valeurs absolues w de L qui prolongent v. Par le théorème 2.6.6 tout $w \in S_v$ s'écrit comme $w = w_{\mathfrak{P}}$ avec $\mathfrak{P} \mid \mathfrak{p}$ et l'application $\mathfrak{P} \mapsto w_{\mathfrak{P}}$ établie une bijection entre $S_{\mathfrak{P}}$ et S_v. Soit $x \in L^*$. Si

$$xB = \prod_{\mathfrak{P}} \mathfrak{P}^{w_{\mathfrak{P}}(x)},$$

alors

$$g^{-1}(x)B = \prod_{\mathfrak{P}} g^{-1}(\mathfrak{P})^{w_{\mathfrak{P}}(x)},$$

d'où

$$w_{\mathfrak{P}}(g^{-1}(x)) = w_{g(\mathfrak{P})}(x).$$

Donc, $g w_{\mathfrak{P}} = w_{g(\mathfrak{P})}$ ce qui montre que la bijection $\mathfrak{P} \mapsto w_{\mathfrak{P}}$ est compatible avec l'action de G.

Pour simplifier la notation on note $G_{\mathfrak{P}}$ le groupe de décomposition de $w_{\mathfrak{P}}$. Donc on a

$$G_{\mathfrak{P}} = \{g \in G \,|\, g(\mathfrak{P}) = \mathfrak{P}\}.$$

THÉORÈME 2.6.7. *Soit L/K une extension galoisienne et soit $\mathfrak{p}$ un idéal premier non-nul de A. Alors:*

i) Le groupe de Galois $G = Gal(L/K)$ opère transitivement sur $S_\mathfrak{p}$. Pour tout $\mathfrak{P} \mid \mathfrak{p}$ le groupe de décomposition $G_\mathfrak{P}$ est isomorphe à $Gal(L_\mathfrak{P}/K_\mathfrak{p})$.

ii) Les entiers $e(\mathfrak{P}/\mathfrak{p})$ et $f(\mathfrak{P}/\mathfrak{p})$ 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

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

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

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

PREUVE. i) est un cas particulier du théorème 2.3.5.

ii) Soit

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

la factorisantion 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 $l_{\mathfrak{P}_1} = B/\mathfrak{P}_1$ et $l_{\mathfrak{P}_i} = B/\mathfrak{P}_i$, d'où on obtient que $f(\mathfrak{P}_1/\mathfrak{p}) = f(\mathfrak{P}_i/\mathfrak{p})$. 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 on obtient que $e_1 = e_i$. La formule $e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = [L : K]$ résulte maintenant du théorème 1.8.6. Le théorème est démontré.

Le corps $K_\mathfrak{p}$ ou plutôt la famille des corps $K_\mathfrak{p}$ où $\mathfrak{p}$ parcourt les idéaux premiers de A contient beaucoup d'informaton sur K. C'est pourquoi les §§7-10 de ce chapitre seront consacrés à l'étude des corps complets. Dans le §7 on considère le cas de $K = \mathbb{Q}$ qui fournit un bon exemple des constructions précédentes. Nous reviendrons à l'étude des anneaux de Dedekind généraux dans le dernier paragraphe de ce chapitre.

§7. Les nombres p-adiques

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 $\| \cdot \|_\infty$:

$$\|x\|_\infty = |x|.$$

Il est clair qu'elle est archimédienne.

Nous allons montrer qu'à tout nombre premier p on peut associer une valuation discrète sur $\mathbb{Q}$. 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 a et b sont des entiers premiers à p. On définit une fonction

$$v_p \ : \ \mathbb{Q}^* \to \mathbb{Z}$$

en posant

$$v_p(x) = n.$$

PROPOSITION 2.7.1. *La fonction v_p est une valuation discrète sur $\mathbb{Q}$.*

PREUVE. La proposition résulte du théorème 1.7.4 appliqué à $A = \mathbb{Z}$ et $\mathfrak{p} = (p)$ et du théorème 2.5.1. On peut aussi donner la preuve directe suivante.

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

$$v_p(xy) = n + m = v_p(x) + v_p(y).$$

D'autre part, si $m \geqslant n$, alors

$$x + y = p^n\,\frac{ad + bcp^{m-n}}{bd},$$

d'où

$$v_p(x+y) = v_p(p^n) + v_p(ad + bcp^{m-n}) - v_p(bd) \geqslant n = \min\{v_p(x), v_p(y)\},$$

car $v_p(ad + bcp^{m-n}) \geqslant 0$ et $v_p(bd) = 0$. Donc, v_p est une valuation discrète.

Par définition, l'anneau de valuation de v_p est

$$\mathbb{Z}_{(p)} = \{x = p^n a/b \,|\, n \geqslant 0,\, p \nmid a, b\}.$$

Le nombre premier p est une uniformisante de $\mathbb{Z}_{(p)}$ et

$$\mathfrak{m}_{(p)} = \{x = p^n a/b \,|\, n \geqslant 1,\, p \nmid a, b\} = p\mathbb{Z}_{(p)}$$

est l'idéal maximal de $\mathbb{Z}_{(p)}$.

Le corps résiduel $\mathbb{Z}_{(p)}/\mathfrak{m}_{(p)}$ de v_p est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

On peut normaliser la valeur absolue associée à v_p en prenant $\rho = 1/p$ et en posant, donc,

$$\|x\|_p = \left(\frac{1}{p}\right)^{v_p(x)}.$$

DÉFINITION. *La valeur absolue non-archimédienne $\|\cdot\|_p$ est appelé la valeur absolue p-adique sur $\mathbb{Q}$.*

Nous admettons le théorème suivant:

THÉORÈME 2.7.2 (OSTROWSKI). *i) Toute valeur absolue archimédienne sur $\mathbb{Q}$ est équivalente à la valeur absolue usuelle $\|\cdot\|_\infty$.*

ii) Si $\|\cdot\|$ est une valeur absolue non-archimédienne non-triviale sur $\mathbb{Q}$, alors il existe un unique nombre premier p tel que $\|\cdot\|$ est équivalente à $\|\cdot\|_p$.

PREUVE. voir [K], chapitre I, théorème 1.

Donc, le théorème d'Ostrowski donne une classification complète des valeurs absolues sur $\mathbb{Q}$.

Il est bien connu qu'en completant $\mathbb{Q}$ pour la valeur absolue usuelle on obtient le corps des réels $\mathbb{R}$.

DÉFINITION. *On appelle le corps des nombres p-adiques et on note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la valeur absolue p-adique.*

On note $\mathbb{Z}_p$ l'anneau de valuation de $\mathbb{Q}_p$. Par la proposition 2.6.5, $\mathbb{Z}_p$ coïncide avec l'adhérence de $\mathbb{Z}$ dans $\mathbb{Q}_p$. 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 $\mathbb{F}_p$.

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 $v_p(x - x_n) \underset{n\to\infty}{\to} +\infty$.

ii) Une série

$$\sum_{k=1}^{\infty} a_k, \qquad a_k \in \mathbb{Q}_p$$

est convergente si et seulement si $v_p(a_k) \to +\infty$.

iii) Tout élément de $x \in \mathbb{Q}_p$ peut être représenter par une suite de Cauchy $\{x_n\} \subset Q$ 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 $v_p(x_n - x'_n) \to +\infty$.

LEMME 2.7.3. *Pour tout $x \in \mathbb{Z}_p$ il existe une unique suite de Cauchy $\{x_n\} \subset \mathbb{Q}$ qui satisfait aux conditions suivantes:*

i) $\{x_n\}$ représente x, i.e. $\lim_{n\to\infty} x_n = x$;

ii) $0 \leqslant x_n \leqslant p^n$ pour tout $n \geqslant 1$;

iii) $x_n \equiv x_{n+1} \pmod{p^n}$ pour tout $n \geqslant 1$.

PREUVE. 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 $v_p(x_n - y_n) \geqslant n$, on a

$$v_p(x_n - x) = v_p((x_n - y_n) + (y_n - x)) \geqslant \min\{v_p(x_n - y_n), v_p(y_n - x)\} \geqslant n,$$

d'où $\lim_{n\to\infty} x_n = x$. Le même argument montre que $v_p(x_n - x_{n+1}) \geqslant n$ 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 2.7.3. 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 $v_p(x) = -n < 0$, alors $v_p(xp^n) = 0$, 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:

$$x = \sum_{k=-n}^{\infty} a_k p^k, \qquad 0 \leqslant a_k \leqslant p-1.$$

§8. Corps locaux

8.1. Corps complets pour une valuation discrète.

Dans cette section nous expliciterons les résultats des §2 et §6 pour les corps complets pour une valuation discrète.

Dans ce paragraphe K désigne un corps complet pour une valuation discrète

$$v_K \ : \ K^* \to \mathbb{Z}.$$

On note O_K et on appelle anneau des entiers de K son anneau de valuation

$$O_K = \{x \,|\, v_K(x) \geqslant 0\}.$$

On appelle groupe des unités de K et on note U_K le groupe des unités de O_K:

$$U_K = \{x \,|\, v_K(x) = 0\}.$$

On note π_K une uniformisante de O_K et $\mathfrak{m}_K$ son idéal maximal. Donc on a

$$\mathfrak{m}_K = \{x \in K \,|\, v_K(x) > 0\},$$
$$\mathfrak{m}_K = (\pi_K).$$

On choisit $\rho \in]0;1[$ on on fixe une valeur absolue sur K en posant

$$\|x\|_K = \rho^{v_K(x)}.$$

THÉORÈME 2.8.1. *Soit L/K une extension finie séparable. Alors,*

i) La fermèture intégrale de O_K dans L est un anneau de valuation discrète qu'on note B.

ii) La valeur absolue $\| \cdot \|_K$ admet un prolongement $\| \cdot \|_L$ à L et un seul. Ce prolongement est induit par la valuation discrète de B.

iii) Le corps L est complet pour la topologie définie par $\| \cdot \|_L$. Son anneau des entiers O_L coïncide avec B.

PREUVE. Comme O_K est un anneau de Dedekind, on peut appliquer le théorème 2.6.6. On obtient ainsi que les prolongements de $\| \cdot \|_K$ à L sont induits par les valuations discrètes associées aux idéaux premiers non-nul de B. Comme par le théorème 2.2.7 il n'existe qu'un seul prolongement de $\| \cdot \|_K$ à L on obtient que B possède un unique idéal premier $\mathfrak{m}_L$. Comme B est un anneau de Dedekind, ceci implique que $\mathfrak{m}_L$ est principal (voir chapitre I,§6, vi)) ce qui montre que B est un anneau de valuation discrète. Les autres assertions sont évidentes.

Nous allons utiliser les notations et les définitions suivantes. Soit π_L une uniformisante de L.

Les idéaux $\mathfrak{m}_K = (\pi_K)$ et $\mathfrak{m}_L = (\pi_L)$ sont les uniques idéaux premiers non-nuls des anneaux O_K et O_L et on note $k_K = O_K/\mathfrak{m}_K$ et $k_L = O_L/\mathfrak{m}_L$ les corps résiduels correspondants. Alors k_L est une extension finie de k_K. Le degré $f = [k_L : k_K]$ est appelé le degré résiduel de L/K.

On note e où $e(L/K)$ l'indice de ramification de l'idéal (π_L):

$$(*) \qquad \pi_K O_L = \pi_L^e O_L.$$

Cet entier e sera appelé l'indice de ramification de l'extension L/K.

La formule(*) signifie tout simplement que π_K s'écrit sous la forme:

$$\pi_K = \pi_L^e u, \qquad u \in U_L.$$

Si on note v_L la valuation discrète de L on obtient que

$$e = v_L(\pi_K).$$

Plus généralement, si $x \in K$, alors

$$v_L(x) = e v_K(x).$$

COROLLAIRE 2.8.2. *On a*

$$ef = [L : K].$$

PREUVE. C'est un cas particulier du théorème 1.8.6.

Les propriétés suivantes sont des cas particuliers des corollaires 2.2.9-2.2.11:

i) Soit L/K une extension galoisienne. Alors pour tous $x \in L$ et $g \in Gal(L/K)$ les éléments x et $g(x)$ ont même valuation. En particulier

$$g(O_L) = O_L.$$

ii) Soit L/K une extension galoisienne. Alors l'action de $G = Gal(L/K)$ sur L est continue.

iii) Les applications $N_{L/K}$ et $Tr_{L/K}$ sont continues.

Par le théorème 2.2.7 le prolongement de $\| \cdot \|_K$ à L est donné par la formule explicite suivante:

$$(*) \qquad \|x\|_L = \|N_{L/K}(x)\|_K^{1/n}, \qquad n = [L : K].$$

Nous pouvons donner aussi une formule explicite pour v_L:

PROPOSITION 2.8.3. *Soit L/K une extension finie de degré n. Alors*

$$v_L(x) = \frac{1}{f} v_K(N_{L/K}(x)) .$$

PREUVE. On a

$$\|x\|_K = \rho_K^{v_K(x)}, \qquad x \in K$$

et

$$\|x\|_L = \rho_L^{v_L(x)}, \qquad x \in L.$$

Comme $0 < \rho_K, \rho_L < 1$, il existe $c > 0$ tel que $\rho_K = \rho_L^c$. Alors la formule (*) donne:

$$v_L(x) = \frac{c}{n}\, v_K(N_{L/K}(x)), \qquad x \in L.$$

Pour déterminer la constante c posons $x = \pi_K$. Alors $e = v_L(\pi_K) = \frac{c}{n}\, v_K(\pi_K^n) = c$. Comme $e/n = f$, la formule s'en déduit.

PROPOSITION 2.8.4. *Soient $K \subseteq L \subseteq M$ une tour d'extensions finies. Alors*

$$e(M/L)\, e(L/K) = e(M/K),$$
$$f(M/L)\, f(M/K) = f(M/K).$$

PREUVE. Ces formules découlent directement des définitions et ont été déjà mentionnées dans le §8 du chapitre I.

8.2. Corps locaux.

DÉFINITION. *On appelle corps local un corps muni d'une valuation discrète pour laquelle il est complet à corps résiduel fini.*

Exemples. 1) Le corps des nombres p-adiques est un corps local à corps résiduel $\mathbb{F}_p$.

2) Soit K une extension finie de $\mathbb{Q}_p$. Alors K est muni d'une valuation discrète pour laquelle il est complet (théorème 2.8.1). Par le corrollaire 2.8.2 le corps résiduel

k_K est une extension finie de $\mathbb{F}_p$, ce qu montre qu'il est un corps fini de caractéristique p. Donc, K est un corps local.

3) Soit k un corps fini et soit $k[[X]]$ l'anneaux 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 d'abord que le groupe des unités $k[[X]]^*$ de $k[[X]]$ est

$$(*) \qquad k[[X]]^* = \{\sum_{i=0}^{\infty} a_i X^i \,|\, a_0 \neq 0\}.$$

En effet, $\sum_{i=0}^{\infty} a_i X^i$ est inversible si et seulement s'il existe $\sum_{j=0}^{\infty} b_i X^i$ 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

$$\begin{aligned} &a_0 b_0 = 1, \\ &a_0 b_1 + a_1 b_0 = 0, \\ &a_0 b_2 + a_1 b_1 + a_2 b_2 = 0, \\ &\cdots\cdots\cdots\cdots\cdots . \end{aligned}$$

En particulier, si $\sum_{i=0}^{\infty} a_i X^i$ 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.

La formule (*) montre que tout $f(X) \in k[[X]]$ s'écrit de façon unique sous la forme

$$f(X) = X^n u(X), \qquad u(X) \in k[[X]]^*.$$

On en déduit que $k[[X]]$ est un anneaux de valuation discrète. Son idéal maximal $Xk[[X]]$ est engendré par X. L'application

$$\begin{aligned} &k[[X]] \to k, \\ &f(X) \mapsto a_0 \end{aligned}$$

est un homomorphisme surjectif. Son noyau est $Xk[[X]]$ ce qui fournit un isomorphisme

$$k[[X]]/Xk[[X]] \simeq k.$$

Donc, le corps résiduel de $k[[X]]$ est isomorphe à k.

On note $k((X))$ le corps des fractions de $k[[X]]$. La formule (*) implique que 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. Donc, $k((X))$ est un corps local de caractéristique $p = car(k)$.

Soit K un corps local. Le corps résiduel $k_K = O_K/\mathfrak{m}_K$ est fini et on note p sa caractéristique. Alors k_K est une extension finie de $\mathbb{F}_p$ et on pose $f = [k_K : \mathbb{F}_p]$ et $q = p^f$. Par le théorème 0.4.4 on a $card(k_K) = q$. On normalise souvent la valeur absolue $\| \cdot \|_K$ en posant $\rho = q^{-1}$, i.e.

$$\|x\|_K = \left(\frac{1}{q}\right)^{v_K(x)}.$$

Si $x \in O_K$, on note $\bar{x}$ la classe de x dans k_K :

$$\bar{x} = x + \mathfrak{m}_K = x \pmod{\pi_K}.$$

Définition. *On appelle système de représentants de k_K dans O_K une partie $S \subset O_K$ telle que pour tout $\xi \in k_K$ il existe un élément $s \in S$ vérifiant $\bar{s} = \xi$, et un seul.*

Exemples. 1) Soit $K = \mathbb{Q}_p$. Alors $S = \{0, 1, \ldots, p-1\}$ est un système de représentants de $\mathbb{F}_p$ dans $\mathbb{Z}_p$ car $\mathbb{F}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$.

2) Soit $K = k((X))$. Alors $S = k$ est un système de représentants de k dans $k[[X]]$.

PROPOSITION 2.8.5. *Soit S un système de représentants. Alors tout $a \in O_K$ s'écrit de façon unique comme série convergente:*

$$a = \sum_{i=0}^{\infty} s_i \pi_K^i, \qquad s_i \in S.$$

Tout $x \in K$ s'écrit de même:

$$x = \sum_{i=i_0}^{\infty} s_i \pi_K^i, \qquad i_0 \in \mathbb{Z},\ s_i \in S.$$

PREUVE. Soit $a \in O_K$. Alors il existe un unique $s_0 \in S$ tel que $\bar{s}_0 = \bar{a}$, i.e.

$$a \equiv s_0 \pmod{\pi_K}.$$

Alors a s'écrit:

$$a = s_0 + a_1 \pi_K, \qquad a_1 \in O_K.$$

En appliquant ce qui précède à a_1 on obtient:

$$a_1 = s_1 + a_2 \pi_K, \qquad s_1 \in S, a_2 \in O_K,$$

d'où

$$a = s_0 + s_1 \pi_K + a_2 \pi_K^2$$

et ainsi de suite. Comme pour tout n on a

$$a = s_0 + s_1 \pi_K + \cdots + s_n \pi_K^n + a_{n+1} \pi_K^{n+1}$$

avec $v_K(a_{n+1}\pi_K^{n+1}) \geqslant n+1$, la série

$$\sum_{i=0}^{\infty} s_i \pi_K^i$$

converge vers a. Inversement, toute série de la forme $\sum_{i=0}^{\infty} s_i \pi_K^i$ est convergente puisque son terme général tend vers 0 (proposition 2.4.2).

Si $x \in K$, alors $x = \pi_K^{v_K(x)} u$ avec $u \in U_K$ et en développant u on obtient

$$x = \sum_{i=i_0}^{\infty} s_i \pi_K^i, \qquad i_0 = v_K(x).$$

la proposition est démontrée.

Remarque. En appliquant ces résultats à $K = \mathbb{Q}_p$ avec $\pi_K = p$ et $S = \{0, 1, \ldots, p-1\}$ on retrouve les résultats du §7.
Nous voulons montrer qu'un corps local possède un système de représentants particulier formé par des racines de l'unité.

THÉORÈME 2.8.6. *Soit K un corps local et soit $q = card(k_K)$. Alors*
i) Tout $\xi \in k_K$ possède un relèvement $[\xi] \in O_K$ vérifiant $[\xi]^q = [\xi]$ et un seul;
ii) Pour tous $\xi, \eta \in k_K$ on a

$$[\xi]\,[\eta] = [\xi\eta];$$

iii) La famille $S_m = \{[\xi] \,|\, \xi \in k_K\}$ est un système de représentants de k_K dans O_K.

PREUVE. i) Soit $f(X) = X^q - X \in O_K[X]$ et soit $\bar{f}(X) \in k_K[X]$ la réduction de $f(X)$ modulo $\mathfrak{m}_K$. Comme $\bar{f}'(X) = \bar{q}X^{q-1} - \bar{1} = -\bar{1}$, le polynôme $\bar{f}(X)$ est séparable.

Soit $\xi \in k_K$. Alors ξ est une raçine de $\bar{f}(X)$ (voir le théorème 0.4.4) et par le corollaire 2.4.4 il existe une unique raçine $[\xi] \in O_K$ de $f(X)$ telle que $\xi = [\xi] \pmod{\pi_K}$. On en déduit i).

ii) Comme $\xi = [\xi] \pmod{\pi_K}$ et $\eta = [\eta] \pmod{\pi_K}$, on a $\xi\eta = [\xi]\,[\eta] \pmod{\pi_K}$, i.e. $[\xi]\,[\eta]$ est un représentant de $\xi\eta$ dans O_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 2.8.7. *Soit K un corps local et soit $q = card(k_K)$. Alors K contient toutes les raçines $(q-1)$-ièmes de l'unité.*

PREUVE. Les éléments $[\xi]$, $\xi \neq 0$ sont les raçines $(q-1)$-ièmes de l'unité.

DÉFINITION. *Le système de représentants S_m est appelé le système de représentants multiplicatif ou le système de Teichmüller.*

Nous pouvons maintenant "classifier" les corps locaux. Commençons par les corps de caractéristique 0.

THÉORÈME 2.8.8. *Soit K un corps local de caractéristique 0 à corps résiduel de caractéristique $p > 0$. Alors K est isomorphe à une extension finie de $\mathbb{Q}_p$.*

PREUVE. Par le théorème 0.4.1, K contient un sous-corps isomorphe à $\mathbb{Q}$. Donc, en remplaçant K par un corps isomorphe on peut supposer que $\mathbb{Q} \subset K$. La réstriction de $\|\cdot\|_K$ à $\mathbb{Q}$ est une valeur absolue non-archimédienne sur $\mathbb{Q}$. Par le théorème d'Ostrowski (théorème 2.7.2) il existe un nombre premier l tel que la réstriction de $\|\cdot\|_K$ à $\mathbb{Q}$ est équivalente à $\|\cdot\|_l$. Comme K est complet, il contient le complété $\mathbb{Q}_l$ de $\mathbb{Q}$. Donc, K est une extension de $\mathbb{Q}_l$. Le corps résiduel k_K est une extension de $\mathbb{F}_l = k_{\mathbb{Q}_l}$, d'où $l = p = car(k_K)$. Soient $f = [k_K : \mathbb{F}_p]$ et $e = v_K(p)$. Alors le corollaire 2.8.2 implique que K est une extension finie de $\mathbb{Q}_p$ de degré fe.

Dans le cas de caractéristique p la situation est plus simple:

THÉORÈME 2.8.9. *Soit K un corps local de caractéristique p à corps résiduel k. Alors K est isomorphe à $k((X))$.*

PREUVE. Pour tout $\xi \in k$ soit $[\xi]$ le représentant de Teichmüller de ξ. Comme K est de caractéristique p, on a

$$([\xi] + [\eta])^q = [\xi]^q + [\eta]^q = [\xi] + [\eta]$$

(voir la proposition 0.4.2).Comme

$$\xi + \eta = [\xi] + [\eta] \pmod{\pi_K}$$

l'unicité du relèvement démontrée dans le théorème 2.8.6, i) implique que

$$[\xi + \eta] = [\xi] + [\eta].$$

Donc l'application

$$\begin{aligned} k &\to K, \\ \xi &\mapsto [\xi] \end{aligned}$$

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 2.6.1 tout élément de K s'écrit de manière unique

$$\sum_{i=i_0}^{\infty} a_i \pi_K^i$$

avec $a_i \in k$ d'ou on déduit que l'application

$$\begin{aligned} k((X)) &\to K, \\ \sum_{i=i_0}^{\infty} a_i X^i &\mapsto \sum_{i=i_0}^{\infty} a_i \pi_K^i \end{aligned}$$

est un isomorphisme.

PROPOSITION 2.8.10. *Soit L/K un extension finie des corps locaux. Alors il existe $a \in O_L$ tel que $O_L = O_K[a]$.*

PREUVE. Soit l le corps résiduel de L. Comme l'extension l/k est séparable, il existe $\bar{\alpha} \in l$ tel que $l = k[\bar{\alpha}]$. On prend le relèvement $\alpha \in O_L$ de $\bar{\alpha}$ vérifiant $\alpha^{q_L - 1} = 1$, où $q_L = |l|$. Posons $a = \alpha + \pi_L$, où π_L est une uniformisante de L. Soit $B = O_K[a]$. Alors B contient un système de représentants de l car $a^i \equiv \alpha^i \pmod{\pi}_L$. D'autre part, B contient l'élément

$$x = a^{q-1} - 1 = (\alpha + \pi_L)^{q-1} - 1 = (q-1)\alpha^{q-2}\pi_L + \cdots$$

qui est une uniformisante de L car $v_L(x) = 1$. On en déduit que $B = O_L$.

§9 . Extensions non-ramifiées

Dans ce paragraphe K désigne un corps complet pour une valuation discrète.

Définition. *On dit qu'une extension finie L/K est non-ramifiée si $f(L/K) = [L : K]$ et si l'extension des corps résiduels k_L/k_K est séparable.*

dans le cas général la condition de séparabilité de k_L/k_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 qui découlent directement de cette définition.

i) L/K est non-ramifiée si et seulement si $e(L/K) = 1$ et k_L/k_K est séparable.

Preuve. On a $f(L/K)e(L/K) = [L : K]$.

ii) L/K est non-ramifiée si et seulement si π_K est une uniformisante de L et k_L/k_K est séparable.

Preuve. On a $v_L(\pi_K) = e(L/K)v_K(\pi_K) = 1$.

iii) Soit $K \subseteq L \subseteq M$ une tour d'extensions. Alors M/K est non-ramifiée si et seulement si L/K et M/L sont non-ramifiées.

Preuve. On a $e(M/K) = e(M/L)e(L/K)$, d'où le résultat.

Soit L/K une extension non-ramifiée et soit k_L/k_K l'extension résiduelle corréspondante. Elle est séparable (théorème 0.4.6), donc il existe $\bar{\alpha} \in k_L$ tel que $k_L = k_K(\bar{\alpha})$. Pour étuduer la structure des extensions non-ramifiées nous avons besoin de la proposition suivante.

Proposition 2.9.1. *i) Soit L/K une extension non-ramifiée. Soient $k_L = k_K(\bar{\alpha})$ et $\bar{f}(X) \in k_K[X]$ le polynôme minimal de $\bar{\alpha}$. Soit $f(X) \in O_K[X]$ un polynôme unitaire dont la réduction $\bmod \pi_K$ est $\bar{f}(X)$. Alors*

i) $f(X)$ a une racine $\alpha \in O_L$ telle que $\bar{\alpha} = \alpha \pmod{\pi_L}$ et une seule.

ii) On a $L = K(\alpha)$.

Preuve. Comme k_L/k_K est séparable, $\bar{\alpha}$ est une racine simple du polynôme $\bar{f}(X)$ et la partie i) de la proposition découle du corollaire 2.4.4.

Pour montrer que $L = K(\alpha)$, posons $L' = L(\alpha)$. Alors L' est une extension non-ramifiée de K contenant α. Donc le corps résiduel $k_{L'}$ contient $\bar{\alpha}$ ce qui donne

$$[k_L : k_K] \geqslant [k_{L'} : k_K] \geqslant [k_L : k_K].$$

On en déduit que $k_{L'} = k_L$, d'où $L' = L$.

L'assertion réciproque s'énonce ainsi:

Proposition 2.9.2. *Soit K un corps local et soit $l = k_K(\bar{\alpha})$ une extension finie séparable de k_K. Soient $\bar{f}(X)$ le polynôme minimal de $\bar{\alpha}$ et $f(X)$ un polynôme unitaire dont la réduction est égale à $\bar{f}(X)$. Alors,*

$$L = K[X]/(f(X))$$

est une extension non-ramifiée de K dont le corps résiduel k_L est isomorphe à l.

PREUVE. Comme $\bar{f}(X)$ est irréductible, $f(X)$ l'est aussi et L est une extension de K de degré

$$[L : K] = deg(f) = deg(\bar{f}) = [l : k_K].$$

Soit $\alpha = X \pmod{f(X)}$ la classe de X dans L. Alors $L = K(\alpha)$ et α est une racine du polynôme $f(X)$ (voir théorème 0.2.3). En particulier, α est entier sur O_K et $\bar{\alpha} \in k_K$ est une racine de $\bar{f}(X)$. Donc,

$$[L : K] =\geqslant [k_L : k_K] \geqslant [k_K(\bar{\alpha}) : k_K] = deg\bar{f}(X) = [L : K]$$

ce qui entraine que

$$[k_L : k_K] = [k_K(\bar{\alpha}) : k_K] = deg\bar{f}(X) == [L : K].$$

Donc, L/K est non-ramifiée est son corps résiduel est isomorphe à $l = k_K(\bar{\alpha})$.

On fixe une clôture algébrique $\bar{K}$ de K. Soient L/K et M/K deux extensions finies de K. On note $Hom_K(L, M)$ l'ensemble formé par les homomorphismes

$$\sigma \ : \ L/K \to M/K$$

qui fixent K. Soit $\sigma \in Hom_K(L, M)$. Comme $\sigma(O_L) \subseteq O_M$ en passant aux corps résiduels on obtient un homomorphisme

$$\bar{\sigma} \ : \ k_L/k_K \to k_M/k_K \, .$$

Donc, on a définit une application

$$f \ : \ Hom_K(L, M) \to Hom_{k_K}(k_L, k_M) \, ,$$
$$f(\sigma) = \bar{\sigma}.$$

La proposition suivante joue le rôle clé dans ce paragraphe.

PROPOSITION 2.9.3. *Si L/K est non-ramifiée, alors f est une bijection. En particulier, si L/K est une extension galoisienne non-ramifiée, alors on a un isomorphisme canonique*

$$Gal(L/K) \simeq Gal(k_L/k_K).$$

PREUVE. Soit $k_L = k_K(\bar{\alpha})$ et soit $\bar{f}(X)$ le polynôme minimal de $\bar{\alpha}$. Soit $f(X) \in O_K[X]$ un polynôme dont la réduction est égale à $\bar{f}(X)$. Alors par la proposition 2.9.1 on a $L = K(\alpha)$, où α est une racine de $f(X)$ vérifiant $\bar{\alpha} = \alpha \pmod{\pi_L}$. 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 $Hom_K(L, M)$ et les racines β du polynôme $f(X)$ dans M. Montrons d'abord que f est surjective. Soit $\bar{\sigma} \in Hom_{k_K}(k_L, k_M)$. Alors $\bar{\beta} = \bar{\sigma}(\bar{\alpha})$ est une racine de $\bar{f}(X)$ et par la proposition 2.7.1 il existe une unique racine β de $f(X)$ telle que $\bar{\beta} = \beta \pmod{\pi_L}$. En posant $\sigma(\alpha) = \beta$ on obtient un homomorphisme $\sigma \in Hom_K(L, M)$ tel que $f(\sigma) = \bar{\sigma}$. Donc f est surjectif.

Pour montrer l'injectivité on remarque que si σ_1 et σ_2 sont deux éléments de $Hom_K(L, M)$ tels que $\bar{\sigma}_1 = \bar{\sigma}_2$, alors $\sigma_1(\alpha)$ et $\sigma_2(\alpha)$ sont deux racines de $f(X)$ tels que $\sigma_1(\alpha) \equiv \sigma_2(\alpha) \pmod{\pi_L}$. Mais dans ce cas $\sigma_1(\alpha) = \sigma_2(\alpha)$ par la prop. 2.9.1.

PROPOSITION 2.9.4. *Soient L_1 et L_2 deux extensions non-ramifiées de K. Alors le composite L_1L_2 est non-ramifié sur K.*

PREUVE. Soient k_i et k_2 les corps résiduels des L_1 et L_2 et soit l le composite k_1k_2. Soit L une extension non-ramifiée de K à corps résiduel l. On a

$$Hom_K(L_i, L) \equiv Hom_{k_K}(k_i, l)$$

et comme $k_i \subseteq l$ on obtient que $L_i \subseteq L$. Alors $L_1L_2 \subseteq L$, et comme L/K est non-ramifiée, L_1L_2/K l'est aussi.

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 $f(L/K) = 1$.

THÉORÈME 2.9.5. *Soit K un corps local. Alors pour tout n il existe une extension non-ramifiée de K de degré n et une seule. Cette extension est galoisienne et son groupe de Galois est cyclique d'ordre n.*

PREUVE. i) Soit k_K le corps résiduel de K. Par le théorème 0.4.5 il existe une unique extension l/k_K de degré n et par la proposition 2.9.2 on peut construire une extension on-ramifiée L/K à corps résiduel $k_L = l$. L'existence de L est donc établie.

ii) Par le théorème 0.4.6 l'extension k_L/k_K est galoisienne et $Gal(k_L/k_K)$ est cyclique d'ordre n. En appliquant la proposition 2.9.3 on obtient

$$(*) \qquad Hom_K(L, L) \simeq Hom_{k_K}(k_L, k_L) = Gal(k_L/k_K).$$

Donc, il existe n automorphismes de L/K ce qui entraîne que L/K est galoisienne. La formule (*) donne aussi

$$Gal(L/K) = Hom_K(L, L) \simeq Gal(k_L/k_K)$$

ce qui montre qu'elle est cyclique d'ordre n.

iii) 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 avec le corps résiduel $k_M = l$. Alors, en utilisant toujours la proposition 2.9.3, on a

$$Hom_K(L, M) \simeq Hom_{k_K}(l, l).$$

Comme $Hom_{k_K}(l, l)$ est non-vide (par exemple il contient id_l) il existe un homomorphisme $\sigma : L/K \to M/K$. On a déjà montré que L/K est galoisienne, d'où

$$L = \sigma(L) \subseteq M.$$

Comme L/K et M/K ont même degré, on en déduit que $L = M$.

Soit L/K une extension non-ramifiée finie. Dans la preuve du théorème 2.9.4 on a établie un isomorphisme

$$Gal(L/K) \simeq Gal(k_L/k_K).$$

Le groupe de Galois de k_L/k_K est engendré par l'automorphisme F_{k_L/k_K} défini par

$$F_{k_L/k_K}(x) = x^q,$$

où $q = card(k_K)$ (voir théorème 0.4.6). On appelle automorphisme de Frobenius de L/K et on note $F_{L/K}$ l'élément de $Gal(L/K)$ qui correspond à F_{k_L/k_K}. On a

$$F_{L/K}(x) \equiv x^q \pmod{\pi_L} \qquad \textit{pour tout } x \in O_L.$$

Nous pouvons donner une construction explicite des extensions non-ramifiées des corps locaux.

THÉORÈME 2.9.6. *Soit K un corps local et soit $q = card(k_K)$. Soit ζ_{q^n-1} une racine primitive $q^n - 1$-ième de l'unité. Alors $K(\zeta_{q^n-1})$ est une extension non-ramifiée de K de degré n.*

PREUVE. Soit L/K une extension non-ramifiée de degré n. Alors $card(k_L) = q^n$ et par le corollaire 2.8.7 L contient ζ_{q^n-1}. Donc $K(\zeta_{q^n-1}) \subseteq L$. D'autre part, par le théorème 2.8.6 le corps résiduel de $K(\zeta_{q^n-1})$ contient toutes les racines q^n-1-ièmes de l'unité i.e. coïncide avec k_L. Donc $L = K(\zeta_{q^n-1})$.

§10 . Extensions totalement ramifiées

Dans ce paragraphe K est un corps complet pour une valuation discrète.

DÉFINITION. *On dit qu'une extension L/K est totalement ramifiée si $f(L/K) = 1$.*

Il résulte de cette définition que:
i) L/K est totalement ramifiée si et seulement si $k_L = k_K$.
ii) L/K est totalement ramifiée si et seulement si $e(L/K) = [L : K]$.
iii) si $K \subseteq L \subseteq M$, alors M/K est totalement ramifiée si et seulement si M/L et L/K sont totalement ramifiées.

DÉFINITION. *On dit que*

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in O_K[X]$$

est un polynôme d'Eisenstein, si
i) $a_i \equiv 0 \pmod{\pi_K}$;
ii) $a_0 \neq 0 \pmod{\pi_K^2}$.

PROPOSITION 2.10.1. *Si $f(X)$ est un polynôme d'Eisenstein, alors il est irréductible sur K.*

PREUVE. La preuve est exactement la même que dans le cas des polynômes d'Eisenstein sur $\mathbb{Z}$, avec p remplacé par π_K.

THÉORÈME 2.10.2. *1) Soit $f(X) \in O_K[X]$ un polynôme d'Eisenstein et soit α une racine de $f(X)$. Alors $L = K(\alpha)$ 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

$$O_L = O_K[\pi_L].$$

PREUVE. 1) Soit α une racine d'un polynôme d'Eisenstein

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in O_K[X].$$

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

$$nv_L(\alpha) = v_L(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \geqslant \min_i\{v_L(a_i) + iv_L(\alpha)\}.$$

Comme $v_L(a_i) > 0$, on en déduit que $v_L(\alpha) > 0$. Comme $v_L(a_i) \geqslant v_L(a_0)$, on obtient

$$v_L(a_i) + iv_L(\alpha) > v_L(a_0), \quad si\ i = 1, \ldots, n-1,$$

d'où

$$nv_L(\alpha) = v_L(a_0).$$

On a $v_L(a_0) = v_L(\pi_K) = e(L/K)$ et $v_L(\alpha) \geqslant v_L(\pi_L) = 1$. Donc,

$$n \leqslant nv_L(\alpha) = e(L/K),$$

ce qui signifie que $n = e(L/K)$ 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 $\sigma_i(\pi_L)$ et on a

$$v_M(\sigma_i(\pi_L)) = v_M(\pi_L) > 0.$$

Soit $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ le polynôme minimal de π_L. Comme

$$f(X) = \prod_i (X - \sigma_i(\pi_L))$$

on obtient que $v_M(a_i) > 0$, d'où $v_K(a_i) > 0$ i.e.

$$a_i \equiv 0 \pmod{\pi_K}.$$

D'autre part, on a

$$v_L(a_0) = v_L(a_1\pi_L + \cdots a_{n-1}\pi^{n-1} + \pi_L^n).$$

Comme

$$v_L(a_i\pi_L^i) = v_L(a_i) + v_L(\pi^i) \geqslant e(L/K)v_K(a_i) + i \geqslant n + i$$

on a

$$v_L(\pi_L^n) = n < v_L(a_i\pi_L^i)$$

d'où

$$v_L(a_0) = v_L(\pi_L^n) = n.$$

Donc, $v_K(a_0) = v_L(a_0)/e(L/K) = 1$ et on a monté que $f(X)$ est un polynôme d'Eisenstein.

Pour montrer que $O_L = O_K[\pi_L]$, posons

$$B = O_K[[\pi_L]] = \{\sum_{i=0}^{\infty} c_i\pi_L^i \mid c_i \in O_K\}.$$

Comme $k_L = k_K$, l'anneau B contient un système de représentants de k_L et une uniformisante de L, d'où $B = O_L$ (proposition 2.8.5). Pour montrer que $B = O_K[\pi_L]$, on remarque que la formule

$$\pi_L^n = -a_{n-1}\pi_L^{n-1} - \cdots - a_1\pi_L - a_0, \quad a_i \in O_K,$$

permet d'écrire une série $\sum c_i\pi_L^i$ comme un polynôme de π_L à coefficients dans O_K.

Pour les corps **locaux** on peut montrer que toute extension finie peut être construite à partir des extensions non-ramifiées et totalement ramifiées façon suivante:

THÉORÈME 2.10.3. *Soit L/K une extension finie des 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.

PREUVE. 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

$$Hom_K(L_0, L) \simeq Hom_{k_K}(k_L, k_L),$$

on obtient qu'il existe un homomorphisme σ $L_0/K \to L/K$ 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 ramifié. Si M/L est une sous-extension non-ramifiée de L/K, alors $k_M \subseteq k_L$, d'où $M \subseteq L_0$. Donc, L_0/K est l'unique sous-extension de L/K vérifiant i)-ii).

Soit L/K une extension finie galoisienne. Dans les notations du théorème 2.10.1 on pose

$$I_{L/K} = Gal(L/L_0).$$

Alors $I_{L/K}$ est un sous-groupe distingué de $Gal(L/K)$ et

$$Gal(L/K)/I_{L/K} \simeq Gal(L_0/L).$$

DÉFINITION. *La groupe $I_{L/K}$ est appelé le groupe d'inértie de l'extension L/K.*

Nous allons maintenant étudier les extensions totalement ramifiées des corps locaux.

§11 . Différente

11.1. L'espace dual. Soit K un corps. Rappelons que si V et W sont deux espaces vectoriels sur K, alors l'ensemble $Hom_K(V,W)$ des applications linéaires $f : V \to W$ est un espace vectoriel sur K. L'addition et la multiplication par scalaires dans $Hom_K(V,W)$ sont données par

$$(f_1 + f_2)(v) = f_1(v) + f_2(v),$$
$$(af)(v) = af(v).$$

Si V et W sont de dimensions finies n et m, alors $Hom_K(V,W)$ est de dimension nm et s'identifie, après le choix des bases à l'espace vectoriel des (m,n)-matrices à coefficients dans K.

DÉFINITION. *On appelle espace dual de V et on note V^* l'espace vectoriel*

$$V^* = Hom_K(V,K).$$

Voici quelques propriétés élémentaires de V^* :

i) V^* est de dimension $n = dim(V)$.

ii) Soit $v_1, \dots, v_n$ une base de V. On définit des applications linéaires $f_i : V \to K$ par

$$f_i(v_j) = \begin{cases} 1, & si\ i = j \\ 0, & sinon. \end{cases}$$

Alors $f_1, \dots, f_n$ est une base de V^*.

PREUVE. Comme V^* est de dimension n, il suffit de montrer que $f_1, \dots, f_n$ forment un système libre. Soit

$$a_1 f_1 + \dots a_n f_n = 0, \quad a_i \in K.$$

Alors, pour tout i on a

$$0 = (a_1 f_1 + \dots a_n f_n)(v_i) = \sum_j f_i(v_j) = a_i.$$

Donc, $a_i = 0$ pour tout i.

DÉFINITION. *$f_1, \dots, f_n$ est appelé la base duale de $v_1, \dots, v_n$.*

DÉFINITION. *Soit V un K-espace vectoriel de dimension finie. On appelle forme bilinéaire sur V une application*

$$B : V \times V \to K,$$
$$(u,v) \mapsto B(u,v)$$

vérifiant les conditions suivantes:

i) $B(u_1 + u_2, v) = B(u_1, v) + B(u_2, v)$ et $B(u, v_1 + v_2) = B(u, v_1) + B(u, v_2)$.

ii) si $\lambda \in K$ et $u, v \in V$, alors

$$B(\lambda u, v) = B(u, \lambda v) = \lambda B(u, v);$$

On dit que B est symétrique, si
iii) $B(u,v) = B(v,u)$ *pour tous* $u, v \in V$.

Soit $v_1, \ldots, v_n$ une base de V et soit

$$M(B,\bar{v}) = \begin{pmatrix} B(v_1,v_1) & B(v_1,v_2) & \ldots & B(v_1,v_n) \\ B(v_2,v_1) & B(v_2,v_2) & \ldots & B(v_2,v_n) \\ \vdots & \vdots & \ddots & \vdots \\ B(v_n,v_1) & B(v_n,v_2) & \ldots & B(v_n,v_n) \end{pmatrix}.$$

Si $u = \sum_{i=1}^n x_i v_i$ et $v = \sum_{i=1}^n y_i v_i$, alors

$$B(u,v) = \sum_{i,j=1}^{n} B(v_i,v_j) x_i y_j.$$

En termes matriciels cette formule s'écrit

$$B(u,v) = (x_1, \ldots, x_n) M(B,\bar{v}) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

En particulier, B est symétrique si et seulement si $M(B,\bar{v})$ est une matrice symétrique.

DÉFINITION. *On appelle discriminant de B dans la base $v_1, \ldots, v_n$ le déterminant*

$$disc(B,\bar{v}) = det(M(B,\bar{v})).$$

Soit B une forme bilinéaire. Pour tout $u \in V$, on définit une application

$$f_u \ : \ V \to K$$

par

$$f_u(v) = B(u,v).$$

On vérifie facilement que f_u est une forme linéaire sur V et que l'application

$$u \mapsto f_u$$

est un homomorphisme d'espaces vectoriels:

$$i_V \ : \ V \to V^* = Hom_K(V,K).$$

DÉFINITION. *On dit qu'une forme bilinéaire B est non-dégénérée si pour tout $u \neq 0$ il existe $v \neq 0$ tel que $B(u,v) \neq 0$.*

PROPOSITION 2.11.1. *Les assertions suivantes sont équivalentes:*
i) B est non-dégénérée;
ii) $disc(B) \neq 0$;
iii) l'application $i_V : V \to V^*$ est un isomorphisme;

PREUVE. *i)* $\Leftrightarrow$ *iii)*. Comme $\dim(V) = \dim(V^*)$, l'application i_V est un isomorphisme si et seulement si $\ker(i_V) = \{0\}$. Soit $u \in \ker(i_V)$. Alors $f_u = 0$ i.e. pour tout $v \in V$ on a $B(u, v) = 0$. On en déduit que i) et iii) sont équivalentes.

i) $\Leftrightarrow$ *ii)*. On utilise la formule

$$B(u, v) = (x_1, \dots, x_n) M(B, \bar{v}) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Soit $u = \sum x_i v_i \in V$ un vecteur non-nul. Si $disc(B, \bar{v}) \neq 0$, alors $M(B, \bar{v})$ est inversible et

$$(x_1, \dots, x_n) M(B, \bar{v}) \neq (0, \dots, 0).$$

Donc, on peut trouver $y_1, \dots, y_n$ tels que

$$B(u, v) = (x_1, \dots, x_n) M(B, \bar{v}) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \neq 0,$$

ce qui signifie que B est non-dégénérée. Donc, *ii)* $\Rightarrow$ *i)*.

Réciproquement, s'il existe $v \in V$ tel que $B(u, v) \neq 0$, alors

$$(*) \qquad (x_1, \dots, x_n) M(B, \bar{v}) \neq (0, \dots, 0).$$

Si B est non-dégénérée, alors (*) est vraie pour tout $(x_1, \dots, x_n) \neq (0, \dots, 0)$. En transposant (*), on obtient que le système d'équations linéaires

$$M(B, \bar{v})^t \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

n'a pas de solutions non-nuls, d'où

$$\det(M(B, \bar{v})) = \det(M(B, \bar{v})^t) \neq 0.$$

Donc, *i)* $\Rightarrow$ *ii)*.

Soit B une forme non-dégénérée et soit $v_1, \dots, v_n$ une base de V. Alors $V \simeq V^*$ et il existe $v'_1, \dots, v'_n$ tels que $i_V(v'_j) = f_j$. Comme $f_1, \dots, f_n$ est une base de V^*, les vecteurs $v'_1, \dots, v'_n$ forment une base de V. On a

$$B(v'_i, v_j) = \begin{cases} 1, & si\ i = j \\ 0, & sinon. \end{cases}$$

DÉFINITION. *La base $v'_1, \ldots, v'_n$ est appelée la base duale de la base $v'_1, \ldots, v'_n$.*

11.2. La différente. Dans toute cette section A désigne un anneau de Dedekind, de corps des fractions K. Soient L/K une extension fini séparable et B la fermeture intégrale de A dans L. Nous allons étudier l'application

$$\langle\ ,\ \rangle\ :\ L \times L \to K,$$
$$\langle x, y\rangle = Tr_{L/K}(xy).$$

PROPOSITION 2.11.2. *$\langle\ ,\ \rangle$ est une forme bilinéaire symétrique sur L.*

PREUVE. On a

$$\langle x_1 + x_2, y\rangle = Tr_{L/K}((x_1 + x_2)y) = Tr_{L/K}(x_1y + x_2y) =$$
$$Tr_{L/K}(x_1y) + Tr_{L/K}(x_2y) = \langle x_1, y\rangle + \langle x_2, y\rangle.$$

Si $a \in K$, alors pour tout $z \in L$ on a $Tr_{L/K}(az) = aTr_{L/K}(z)$, d'où

$$\langle ax, y\rangle = Tr_{L/K}(axy) = aTr_{L/K}(xy) = a\langle x, y\rangle.$$

Les autres propriétés sont aussi évidentes.

Si $M \subseteq L$ est un A-module de type fini, on pose

$$M' = \{x \in L \,|\, \langle x, y\rangle \in A \text{ pour tout } y \in M\}.$$

Alors,
i) M' est un A-module;
ii) Si $M \subseteq N$, alors $N' \subseteq M'$.

PREUVE. Si $x_1, x_2 \in M'$, alors

$$\langle x_1 \pm x_2, y\rangle = \langle x_1, x_2\rangle \pm \langle x_2, y\rangle \in A \quad \text{pour tout } y \in M,$$
$$\langle ax_1, y\rangle = a\langle x_1, y\rangle \in A \text{pour tous } a \in A, y \in M.$$

Donc, M' est un A-module.

Supposons que $M \subseteq N$. Tout $x \in N'$ vérifie $\langle x, y\rangle \in A$, $y \in N$. On en déduit que $x \in M'$, d'où $N' \subseteq M'$.

Soit $\omega_1, \ldots, \omega_n$ une base de L/K et soit $\omega'_1, \ldots, \omega'_n$ la base duale.

PROPOSITION 2.11.3. *Soit*

$$M = A\omega_1 + \ldots + A\omega_n$$

le A-module libre engendré par $\omega_1, \ldots, \omega_n$. Alors

$$M' = A\omega'_1 + \cdots + A\omega'_n.$$

PREUVE. Soit $x = \sum c_i\omega'_i \in L$. Pour tout j on a

$$\langle x, \omega_j\rangle = \sum_i \langle \omega'_i, \omega_j\rangle = c_j.$$

Donc $x \in M'$ si et seulement si $c_j \in A$ pour tout j, d'où la proposition.

Avant de passer à la définition de la différente, démontrons

LEMME 2.11.4. *Pour tout $\alpha \in B$ le polynôme minimal de α sur K est à coéfficients dans A. En particulier, $Tr_{L/K}(\alpha) \in A$.*

PREUVE. Soit $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ un polynôme unitaire et tel que $g(\alpha) = 0$. Pour tout plongement $\sigma : L/K \to \bar{K}/K$ on a $g(\sigma(\alpha)) = \sigma g(\alpha) = 0$ ce qui signifie que $\sigma(\alpha)$ est entier sur A. Donc,

$$Tr_{L/K}(\alpha) = \sum_{\sigma} \sigma(\alpha)$$

est entier sur A. D'autre part, $Tr_{L/K}(\alpha) \in K$ et A est intégralement clos, d'où $Tr_{L/K}(\alpha) \in A$.

Soit $f(X)$ le polynôme minimal de α sur K. Alors

$$f(X) = \prod_{\sigma} (X - \sigma(\alpha)),$$

et le même argument montre que $f(X)$ est à coéfficients dans A.

Soit B la fermeture intégrale de A dans L. En général, B n'est pas libre sur A, mais on peut démontrer la proposition suivante:

PROPOSITION 2.11.5. *i) Il existe des A-modules libres $M_1, M_2 \subset L$ tels que*

$$M_1 \subseteq B \subseteq M_2.$$

ii) B' est un idéal fractionnaire de B qui contient B.
iii) $(B')^{-1}$ est un idéal de B.

PREUVE. i) Soit $\omega_1, \ldots, \omega_n$ une base de L/K. Par la proposition 1.3.1 il existe $a \in A$ tel que $a\omega_1, \ldots, a\omega_n$ sont entiers sur A. Soit M_1 le A-module engendré par $a\omega_1, \ldots, a\omega_n$. Alors M_1 est A-libre et on a $M_1 \subseteq B$. La construction d'un module libre M_2 contenant B est donnée dans la preuve du théorème 1.4.2 (voir la formule (*)).

ii) Par construction, B' est un A-module. Si $x, y \in B$, alors le lemme 2.9.4 donne

$$\langle x, y \rangle = Tr_{L/K}(xy) \in A,$$

d'où $B \subseteq B'$. Pour montrer que B' est un idéal fractionnaire il suffit de trouver $b \neq 0$ tel que $bB' \subseteq B$. Soit $x_1, \ldots, x_n$ une base de M_2. Par la proposition 1.3.1 il existe $b \in B$ tel que $bx_1, \ldots, bx_n \in B$, d'où $bB' \subseteq bM_2 \in B$.

iii) $(B')^{-1}$ est l'idéal fractionnaire défini par

$$(B')^{-1} = \{x \in L \,|\, xB' \subseteq B\}$$

(voir §5 du chapitre I). Soit $x \in (B')^{-1}$. Comme $B \subseteq B'$, on a $x \in xB \subseteq xB' \subseteq B$, d'où $(B')^{-1} \subseteq B$.

La proposition est démontrée.

DÉFINITION. *L'idéal $(B')^{-1}$ est appelé la différente de B sur A; notation*

$$\mathcal{D}_{B/A} = (B')^{-1}.$$

D'abord, nous allons démontrer quelques propriétés formelles de la différente.

THÉORÈME 2.11.6. *Soit $K \subseteq L \subseteq M$ une tour d'extensions séparables. Soient B la fermeture intégrale de A dans L et C la fermeture intégrale de B dans M. Alors*

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}.$$

Remarque. L'écriture $\mathcal{D}_{C/B}\mathcal{D}_{B/A}$ signifie l'idéal de C engendré par les produits xy, $x \in \mathcal{D}_{C/B}$, $y \in \mathcal{D}_{B/A}$.

PREUVE. On va plutôt montrer que

$$\mathcal{D}_{C/A}^{-1} = \mathcal{D}_{C/B}^{-1}\mathcal{D}_{B/A}^{-1}.$$

Démontrons d'abord l'inclusion

$$(*) \qquad \mathcal{D}_{C/B}\mathcal{D}_{B/A} \subseteq \mathcal{D}_{C/A}^{-1}.$$

L'idéal $\mathcal{D}_{C/B}^{-1}\mathcal{D}_{B/A}^{-1}$ est engendré par les produits xy $x \in \mathcal{D}_{C/B}^{-1}$, $y \in \mathcal{D}_{B/A}^{-1}$. Soit $z \in C$. Alors $Tr_{M/L}(xz) \in B$, d'où

$$Tr_{M/K}((xy)z) = Tr_{L/K}(yTr_{M/L}(xz)) \in A.$$

Donc $xy \in \mathcal{D}_{C/A}^{-1}$ et l'inclusion (*) est démontrée.

Soit maintenant $x \in \mathcal{D}_{C/A}^{-1}$. Alors, pour tout $y \in C$ on a

$$Tr_{M/K}(xy) \in A.$$

Comme $Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}$, on obtient que pour tout $b \in B$

$$Tr_{L/K}(Tr_{M/L}(xy)b) = Tr_{M/K}(x(yb)) \in A,$$

d'où $Tr_{M/L}(xy) \in \mathcal{D}_{B/A}^{-1}$. Donc, pour tout $z \in \mathcal{D}_{B/A}$ on a

$$Tr_{M/L}((xz)y) = zTr_{M/L}(xy) \in B,$$

d'où $xz \in \mathcal{D}_{C/B}^{-1}$. Donc, on a montré que

$$\mathcal{D}_{C/A}^{-1}\mathcal{D}_{B/A} \subseteq \mathcal{D}_{C/B}^{-1}$$

i.e. que

$$(**) \qquad \mathcal{D}_{C/A}^{-1} \subseteq \mathcal{D}_{B/A}^{-1}\mathcal{D}_{C/B}^{-1}.$$

Les inclusions (*) et (**) donnent le théorème.

Maintenant nous allons calculer la différente dans un cas particulier important.

THÉORÈME 2.11.7. *Soient α un élément entier sur A et $B = A[\alpha]$. Alors $\mathcal{D}_{B/A}$ coïncide avec l'idéal principal engendré par $f'(\alpha)$:*

$$\mathcal{D}_{B/A} = (f'(\alpha)).$$

PREUVE. Soit $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ le polynôme minimal de α sur K. Alors $a_i \in A$ (lemme 2.9.4) et $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ est une base de B sur A. En particulier, B est libre sur A de rang n.

Soient $\alpha_1, \ldots, \alpha_n$ les racines de $f(X)$. On a la formule suivante:

$$(*) \qquad \sum_{i=1}^{n} \frac{f(X)}{X - \alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r$$

pour tout$r = 0, 1, \ldots, n-1$. Pour démontrer cette formule on peut remarquer que X^r et $\sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)}$ sont des polynômes de degré $\leqslant n-1$ qui ont mêmes valeurs en $\alpha_1, \ldots \alpha_n$ car

$$\left(\frac{f(X)}{X - \alpha_i}\right)\Big|_{X=\alpha_j} = \begin{cases} 0, & si\ i \neq j \\ f'(\alpha_i), & si\ i = j. \end{cases}$$

Si $g(X) = c_0 + c_1X + \cdots + c_kX^k$ est un polynôme à coefficients dans L, posons

$$Tr_{L/K}(g(X)) = \sum_{i=1}^{k} Tr_{L/K}(c_i)X^i.$$

Alors, la formule (*) s'écrit

$$Tr_{L/K}\left(\frac{f(X)}{X - \alpha} \frac{\alpha^r}{f'(\alpha)}\right) = X^r.$$

Posons

$$\frac{f(X)}{X - \alpha} = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}, \quad b_i \in B.$$

Alors on a

$$Tr_{L/K}\left(\frac{b_i}{f'(\alpha)}\, \alpha^r\right) = \begin{cases} 0, & si\ i \neq r, \\ 1, & si\ i = r. \end{cases}$$

Donc, les éléments $b_i/f'(\alpha)$, $0 \leqslant i \leqslant n-1$ forment la base duale de $1, \alpha, \ldots, \alpha^{n-1}$ et par la proposition 2.9.3 on a

$$\mathcal{D}_{B/A}^{-1} = \frac{1}{f'(\alpha)} (b_0A + b_1A + \cdots + b_{n-1}A).$$

Il reste à montrer que

$$(**) \qquad b_0A + b_1A + \cdots + b_{n-1}A = A[\alpha].$$

Comme b_i sont entiers sur A et appartiennent à L, on a $b_i \in B = A[\alpha]$, d'où

$$b_0A + b_1A + \cdots + b_{n-1}A \subseteq A[\alpha].$$

D'autre part, la formule

$$f(X) = (b_0 + b_1 X + \cdots + b_{n-1} X^{n-1})(X - \alpha)$$

donne, par récurrence

$$\begin{aligned}
&b_{n-1} = 1 \quad \Rightarrow \quad A = b_{n-1} A \\
&b_{n-2} - \alpha = a_{n-1} \quad \Rightarrow \quad \alpha = b_{n-2} - a_{n-1} \in A + b_{n-2} A, \\
&b_{n-3} - \alpha b_{n-2} = a_{n-2} \quad \Rightarrow \quad \alpha^2 \in A + b_{n-2} A + b_{n-3} A, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

On en déduit que $A[\alpha] \subseteq b_0 A + b_1 A + \cdots + b_{n-1} A$, d'où (**). Donc, $\mathcal{D}_{B/A}^{-1} = f'(\alpha)^{-1} B$ et le théorème est démontré.

11.3. Discriminant.

DÉFINITION. *Soit L/K une extension séparable et soit $\mathfrak{b} \subseteq B$ un idéal non-nul. On appelle discriminant de B et on note $\mathfrak{d}_{B/A}(\mathfrak{b})$ l'idéal de A engendré par les éléments*

$$D_{L/K}(\omega_1, \ldots, \omega_n),$$

où $\omega_1, \ldots, \omega_n$ parcourt les bases de L/K qui sont contenues dans $\mathfrak{b}$.

En particulier, si $\mathfrak{b}$ est un A-module libre, alors $\mathfrak{d}_{B/A}(\mathfrak{b})$ est l'idéal principal engendré par $D_{L/K}(\omega_1, \ldots, \omega_n)$, où $\omega_1, \ldots, \omega_n$ est une base de $\mathfrak{b}$.

On pose $\mathfrak{d}_{B/A} = \mathfrak{d}_{B/A}(B)$.

PROPOSITION 2.11.8. *Soit $\mathfrak{b}$ un idéal fractionnaire de B. Alors,*

$$\mathfrak{d}_{B/A}(\mathfrak{b}) = \mathcal{N}_{B/A}(\mathfrak{b})^2 \, \mathfrak{d}_{B/A},$$

où $\mathcal{N}_{B/A}$ désigne l'application "norme" (voir chapitre I, §10).

PREUVE. a) Supposons d'abord que $\mathfrak{b}$ est principal. Soit $\mathfrak{b} = (\beta)$. Si $\omega_1, \ldots, \omega_n \in \mathfrak{b}$ est une base de L/K, alors $\beta\omega_1, \ldots, \beta\omega_n$ l'est aussi et on a:

$$\begin{vmatrix} \sigma_1(\beta\omega_1) & \ldots & \sigma_1(\beta\omega_n) \\ \sigma_2(\beta\omega_1) & \ldots & \sigma_2(\beta\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta\omega_1) & \ldots & \sigma_n(\beta\omega_n) \end{vmatrix} = \prod_{i=1}^{n} \sigma_i(\beta) \begin{vmatrix} \sigma_1(\omega_1) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \ldots & \sigma_2(\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \ldots & \sigma_n(\omega_n) \end{vmatrix},$$

d'où:

$$D_{L/K}(\beta\omega_1, \ldots, \beta\omega_n) = N_{L/K}(\beta)^2 \, D_{L/K}(\omega_1, \ldots, \omega_n).$$

Comme $N_{L/K}(\beta)$ engendre $\mathcal{N}_{B/A}((\beta))$ (proposition 1.9.1) on obtient la formule voulue.

b) Considérons maintenant le cas général. Il suffit de montrer que pour tout idéal paremier $\mathfrak{p}$ de A on a:

$$\mathfrak{d}_{B/A}(\mathfrak{b})_{\mathfrak{p}} = \mathcal{N}_{B/A}(\mathfrak{b})_{\mathfrak{p}} (\mathfrak{d}_{B/A})_{\mathfrak{p}}$$

(rappelons que $M_\mathfrak{p}$ désigne la localisation de M en $\mathfrak{p}$.). On a

$$\mathfrak{d}_{B/A}(\mathfrak{b})_\mathfrak{p} = \mathfrak{d}_{B_\mathfrak{p}/A_\mathfrak{p}}(\mathfrak{b}_\mathfrak{p}),$$
$$\mathcal{N}_{B/A}(\mathfrak{b})_\mathfrak{p}(\mathfrak{d}_{B/A})_\mathfrak{p} = \mathcal{N}_{B_\mathfrak{p}/A_\mathfrak{p}}(\mathfrak{b}_\mathfrak{p})\mathfrak{d}_{B_\mathfrak{p}/A_\mathfrak{p}}.$$

Comme l'anneau $B_\mathfrak{p}$ est principal, l'idéal $\mathfrak{b}_\mathfrak{p}$ est principal et l'égalité voulue découle de la partie a) de la démonstration.

Nous pouvons maintenant démontrer le résultat principal de cette section.

THÉORÈME 2.11.9. *On a*

$$\mathfrak{d}_{B/A} = \mathcal{N}_{B/A}(\mathcal{D}_{B/A}).$$

PREUVE. Si $\omega'_1, \dots, \omega'_n$ est la base de L/K qui est duale de $\omega_1, \dots, \omega_n$, alors le calcul direct du produit des déterminants montre que

$$D_{L/K}(\omega_1, \dots, \omega_n)\, D_{L/K}(\omega_1, \dots, \omega_n) = 1.$$

On en déduit que $\mathfrak{d}_{B/A}\mathfrak{d}_{B/A}(B') = A$. La proposition précedente donne:

$$\mathfrak{d}_{B/A}(B') = \mathfrak{d}_{B/A}(\mathcal{D}^{-1}_{B/A}) = \mathcal{N}_{B/A}(\mathcal{D}_{B/A})^{-2}\,\mathfrak{d}_{B/A},$$

d'où

$$\mathfrak{d}^2_{B/A}\mathcal{N}_{B/A}(\mathcal{D}_{B/A})^{-2} = A.$$

Le théorème s'en déduit.

11.4. Le cas de valuation discrète.

Soient K un corps complet pour une valuation discrète et L/K une extension finie. Alors O_L est la fermeture intégrale de O_K dans L.

DÉFINITION. *On appelle différente de L/K (résp. discriminant de L/K) et on note $\mathcal{D}_{L/K}$ (résp. $\mathfrak{d}_{L/K}$) la différente (résp. discriminant) de O_L sur O_K.*

THÉORÈME 2.11.10. *Soit L/K une extension finie des corps locaux et soit $e = e(L/K)$ l'indice de ramification. Alors,*

i) L/K est non-ramifiée si et seulement si $\mathcal{D}_{L/K} = O_L$;

ii) Si L/K est totalement ramifiée et si $f(X)$ est le polynôme minimal de π_L, alors

$$\mathcal{D}_{L/K} = (f'(\pi_L));$$

PREUVE. i) Soit L/K une extension non-ramifiée et soit $k_L = k_K(\bar{\alpha})$. Soit $\bar{f}(X)$ le polynôme minimal de $\bar{\alpha}$ et soit $f(X) \in O_K[X]$ un relèvement de $\bar{f}(X)$. Alors $O_L = O_K[\alpha]$ où α est la racine de $f(X)$ au-dessus de $\bar{\alpha}$ (voir la proposition 2.9.1). On a $\bar{f}'(\bar{\alpha}) \neq 0$, d'où $f'(\alpha) \in U(L)$. Donc, par le théorème 2.11.7 on a

$$\mathcal{D}_{L/K} = (f'(\alpha)) = O_L.$$

Réciproquement, supposons que $\mathcal{D}_{L/K} = O_L$. Par le théorème 2.11.9 on a $\mathfrak{d}_{L/K} = \mathcal{N}_{L/K}(O_L) = O_K$. Soit $\omega_1, \dots, \omega_n$ une base de O_L sur O_K. Alors on a:

$$D_{L/K}(\omega_1, \dots, \omega_n) \in U_K.$$

Soit $\bar{\omega}_i = \omega_i \pmod{\pi_L}$. Alors $\bar{\omega}_1, \dots, \bar{\omega}_n$ engendrent k_L sur k_K et on a

$$D_{k_L/k_K}(\bar{\omega}_1, \dots, \bar{\omega}_n) = \overline{D_{L/K}(\omega_1, \dots, \omega_n)} \neq 0.$$

On en déduit que $\bar{\omega}_1, \dots, \bar{\omega}_n$ est une base séparable de k_L/k_K (proposition 0.3.4). Donc k_L/k_K est une extension séparable de degré n, d'où on déduit que L/K est non-ramifiée.

ii) Si L/K est totalement ramifiée, alors par le théorème 2.10.2 on a $O_L = O_K[\pi_L]$, d'où

$$\mathcal{D}_{L/K} = (f'(\pi_L)).$$

Pour les corps locaux on peut démontrer un résultat plus précis.

PROPOSITION 2.11.11. *Soit L/K une extension fini des corps locaux et soit $e = e(L/K)$. Alors π_L^{e-1} divise $\mathcal{D}_{L/K}$.*

PREUVE. Soit L_0/K la sous-extension non-ramifiée maximale de L/K (voir théorème 2.10.3). Alors, par le théorème 2.11.6 on a

$$\mathcal{D}_{L/K} = \mathcal{D}_{L/L_0}\mathcal{D}_{L_0/K} = \mathcal{D}_{L/L_0}.$$

Soit $f(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_1X + a_0$ le polynôme minimal de π_L sur L_0. Comme $f(X)$ est un polynôme d'Eisenstein (théorème 2.10.2), on a $v_L(a_i) \geqslant e$, d'où

$$v_L(f'(\pi_L)) = v_L(e\pi_L^{e-1} + (e-1)a_{e-1}\pi_L^{e-2} + \cdots + a_1) \geqslant$$
$$\geqslant \min_i\{v_L(e\pi_L^{e-1}), v_L(ia_i\pi_L^{i-1})\} \geqslant e - 1.$$

Donc, π_L^{e-1} divise $\mathcal{D}_{L/L_0} = (f'(\pi_L))$.

11.5. Le cas global.

Nous revenons au cas général. Soient A un anneau de Dedekind de corps des fractions K, L/K une extension séparable et B la fermeture intégrale de A dans L. Pour tout idéal premier non-nul $\mathfrak{P}$ de B on pose $\mathfrak{p} = \mathfrak{P} \cap A$. On note $O_\mathfrak{P}$ (résp. $O_\mathfrak{p}$) l'anneau des entiers de $L_\mathfrak{P}$ (résp. de $K_\mathfrak{p}$). Soit $\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$ la différente de $O_\mathfrak{P}$ sur $O_\mathfrak{p}$. Comme $O_\mathfrak{P}$ est un anneau de valuation discrète, la différente est un idéal principal, i.e. on a

$$\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}} = \mathfrak{P}^{n_\mathfrak{P}}O_\mathfrak{P}, \qquad n_\mathfrak{P} \in \mathbb{N}.$$

Le théorème suivant montre que la connaissance de ces différentes "locales" permet de retrouver la différente $\mathcal{D}_{B/A}$.

THÉORÈME 2.11.12. *On a*

$$\mathcal{D}_{B/A} = \prod_\mathfrak{P} \mathfrak{P}^{n_\mathfrak{P}}.$$

PREUVE. La preuve n'est pas difficile, mais elle est relativement longue et routine. Voir, par exemple *S. lang, Algebraic Number Theory*, §1 du chapitre III).

Le corollaire suivant est très important.

COROLLAIRE 2.11.13. *Soit L/K une extension finie. Un idéal $\mathfrak{P}$ de B est ramifié (i.e. $e(\mathfrak{P}/\mathfrak{p}) > 1$) si et seulement si $\mathfrak{P} \mid \mathcal{D}_{B/A}$. En particulier, presque tous les idéaux premiers de B sont non-ramifiés dans L/K.*

CHAPITRE III. Corps de nombres

§1. Corps de nombres

DÉFINITION. *On appelle corps de nombres une extension finie K du corps $\mathbb{Q}$. On note O_K et on appelle anneau des entiers de K la fermeture intégrale de $\mathbb{Z}$ dans K.*

L'anneau O_K est le principal objet d'études de la théorie des nombres.
Nous commençons par la structure *additive* de O_K.

PROPOSITION 3.1.1. *Soit $n = [K : \mathbb{Q}]$. Alors O_K est un $\mathbb{Z}$-module libre de rang n.*

PREUVE. C'est un cas particulier du corollaire 1.4.3.

Le théorème suivant est fondamental.

THÉORÈME 3.1.2. *O_K est un anneau de Dedekind.*

PREUVE. Comme $\mathbb{Z}$ est principal, il est un anneau de Dedekind (proposition 1.5.1) et le théorème résulte de la proposition 1.8.5.

Nous pouvons, donc, appliquer à l'étude de O_K les méthodes et les résultats des chapitres I,II. Soit $\mathfrak{p}$ un idéal premier non-nul de O_K. Alors $\mathfrak{p} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ i.e. il existe un nombre premier p tel que $(p) = \mathfrak{p} \cap Z$. On dit que $\mathfrak{p}$ divise p ou que $\mathfrak{p}$ est au-dessus de p; notation $\mathfrak{p} \mid p$. La factorisation de p dans O_K s'écrit:

$$pO_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e_\mathfrak{p}},$$

où $e_\mathfrak{p} = e(\mathfrak{p}/p)$ sont les indices de ramification. Les corps résiduels $k_\mathfrak{p} = O_K/\mathfrak{p}$ sont des extensions finies de $\mathbb{F}_p$ et on note $f_\mathfrak{p} = [k_\mathfrak{p} : \mathbb{F}_p]$ les degrés résiduels correspondants.

Nous allons maintenant étudier les valeurs absolues sur K. Rappelons qu'on peut associer une valuation discrète $v_\mathfrak{p}$ et une valeur absolue $\| \cdot \|_\mathfrak{p}$ à tout idéal premier non-nul $\mathfrak{p}$ de O_K. Les théorèmes 3.1.3 et 3.1.4 généralisent le théorème d'Ostrowski.

THÉORÈME 3.1.3. *i) Soit $\| \cdot \|$ une valeur absolue non-archimédienne sur K. Alors il existe un unique idéal premier $\mathfrak{p}$ de O_K tel que $\| \cdot Vert$ est équivalente à $\| \cdot \|_\mathfrak{p}$.*

ii) Si $\mathfrak{p} \mid p$, alors le complété $K_\mathfrak{p}$ de K pour $\| \cdot \|_\mathfrak{p}$ est une extension finie de $\mathbb{Q}_p$ de degré $n_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p}$. Plus précisement, on a

$$e(K_\mathfrak{p}/\mathbb{Q}_p) = e_\mathfrak{p},$$
$$f(K_\mathfrak{p}/\mathbb{Q}_p) = f_\mathfrak{p}.$$

iii) On a

$$\sum_{\mathfrak{p}|p} [K_\mathfrak{p} : \mathbb{Q}_p] = [K : \mathbb{Q}].$$

PREUVE. i) La restriction de $\|\cdot\|$ sur $\mathbb{Q}$ est une valeur absolue non-archimédienne qui, par le théorème d'Ostrowski, est équivalente à la valeur absolue p-adique $\|\cdot\|_p$ pour certain p. Alors, par le théorème 2.6.6 $\|\cdot\|$ est équivalente à $\|\cdot\|_{\mathfrak{p}}$, où $\mathfrak{p}$ est un idéal premier au-dessus de p.

ii) La formule $e(K_{\mathfrak{p}}/\mathbb{Q}_p) = e_{\mathfrak{p}}$ découle de la définition de l'indice de ramification des corps locaux. Par la proposition 2.6.5 le corps résiduel de $K_{\mathfrak{p}}$ est isomorphe à $k_{\mathfrak{p}}$, d'où $f(K_{\mathfrak{p}}/\mathbb{Q}_p) = f_{\mathfrak{p}}$. Donc $[K_{\mathfrak{p}} : \mathbb{Q}_p] = e_{\mathfrak{p}} f_{\mathfrak{p}}$ (corollaire 2.8.2).

iii) découle de théorème 2.6.6.

Passons maintenant aux valeurs absolues archimédiennes. On note $Hom_{\mathbb{Q}}(K, \mathbb{C})$ l'ensemble des plongements $\sigma : K/\mathbb{Q} \hookrightarrow \mathbb{C}/\mathbb{Q}$ de K dans $\mathbb{C}$. Comme $K/\mathbb{Q}$ est séparable, on a $card(Hom_{\mathbb{Q}}(K, \mathbb{C})) = [L : K]$.

On dit que $\sigma \in Hom_{\mathbb{Q}}(K, \mathbb{C})$ est réel si $\sigma(K) \subseteq \mathbb{R}$. Sinon on dit que σ est complexe. Rappelons que $\mathbb{C}/\mathbb{R}$ est une extension galoisienne de degré 2 et que la conjugaison complexe $z \mapsto \bar{z}$ est l'unique automorphisme non-trivial de $\mathbb{C}/\mathbb{R}$. Si σ est un plongement complexe alors $\bar{\sigma}$ définit par

$$\bar{\sigma}(x) = \overline{\sigma(x)}$$

l'est aussi et il est facile à voir que $\bar{\sigma} \neq \sigma$. En particulier, le nombre des plongements complexes est pair et on le note $2r_2$. Soit r_1 le nombre des plongements réels. Donc on a

$$r_1 + 2r_2 = [L : K].$$

THÉORÈME 3.1.4. *i) Soit $\|\cdot\|_v$ une valeur absolue archimédienne sur K. Alors il existe un plongement σ $K/\mathbb{Q} \hookrightarrow \mathbb{C}/\mathbb{Q}$ tel que $\|\cdot\|_v$ est équivalente à*

$$\|x\|_\sigma = |\sigma(x)|, \qquad x \in K,$$

où $|\cdot|$ désigne la valeur absolue usuelle sur $\mathbb{C}$. On dit que v est réelle (résr. complexe) si σ est réel (résp. complexe).

ii) Soit K_v le complété de K pour $\|\cdot\|_v$. Alors:

$$K_v = \begin{cases} \mathbb{R}, & \text{si } v \text{ est réelle}, \\ \mathbb{C}, & \text{si } v \text{ est complexe}. \end{cases}$$

iii) Deux plongements définissent la même valeur absolue si et seulement si ils sont conjugués sur $\mathbb{R}$. A équivalence près, K possède exactement $r_1 + r_2$ valeurs absolues archimédiennes.

PREUVE. Soit $\|\cdot\|_v$ une valeur absolue archimédienne sur K. Par le théorème d'Ostrowski la réstriction de $\|\cdot\|_v$ à $\mathbb{Q}$ est équivalente à la valeur absolue usuelle $|\cdot|$. Alors , par le théorème 2.3.1 il existe $\sigma \in Hom_{\mathbb{Q}}(K, \mathbb{C})$ tel que $\|\cdot\|$ soit équivalente à $\|\cdot\|_\sigma$. On en déduit i).

Deux plongements définissent la même valeur absolue si et seulement si il sont conjugués sur le complété de $\mathbb{Q}$ i.e. sur $\mathbb{R}$, d'où l'assertion iii).

Si σ est réel, alors on a $\mathbb{Q} \subseteq \sigma(K) \subseteq \mathbb{R}$, ce qui montre que l'adhérence de $\sigma(K)$ dans $\mathbb{C}$ est $\mathbb{R}$. Si σ est complexe, alors l'adhérence de $\sigma(K)$ dans $\mathbb{C}$ est une extension non-triviale de $\mathbb{R}$ ce qui montre qu'elle coïncide avec $\mathbb{C}$. Le théorème est démontré.

Nous allons normaliser les valeurs absolues de K de façon suivante. Si $\|\cdot\|_v$ est la valeur non-archimédienne qui est associée a un idéal $\mathfrak{p}$ on note q_v le cardinal du corps résiduel $k_\mathfrak{p}$ est on pose:

$$\|x\|_v = \left(\frac{1}{q_v}\right)^{v_\mathfrak{p}(x)}.$$

Comme

$$(*) \qquad \|p\|_v = \left(\frac{1}{q_v}\right)^{v_\mathfrak{p}(p)} = \left(\frac{1}{p^{f_v}}\right)^{e_v} = \frac{1}{p^{[K_v:\mathbb{Q}_p]}} = \|p\|_p^{[K_v:\mathbb{Q}_p]},$$

on voit que $\|\ \|_v^{[K_v:\mathbb{Q}_p]}$ est le prolongement de la valeur absolue p-adique à K_v.

Si $\|\cdot\|_v$ est la valeur archimédienne qui est associé à un plongement $\sigma \in Hom_\mathbb{Q}(K,\mathbb{C})$, on pose

$$\|x\|_v = \begin{cases} |\sigma(x)|, & \textit{si } \sigma \textit{ est réel,} \\ |\sigma(x)|^2, & \textit{si } \sigma \textit{ est complexe.} \end{cases}$$

Remarquons, que dans le cas complexe le carré de la valeur absolue ne satisfait pas à l'inégalité triangulaire et ne peut pas, donc, être considéré comme une valeur absolue. Neanmoins nous verrons que cette convention est très commode. Par exemple, on a le théorème suivant:

Théorème 3.1.5 (formule du produit). *Pour tout $x \in K$ on a*

$$\prod_v \|x\|_v = 1,$$

où v parcourt toutes les valeurs absolues normalisées (non-archimédiennes et archimédiennes) de K.

Preuve. a) On considère d'abord le cas $K = \mathbb{Q}$. Soit

$$x = \pm \prod_p p^{n_p}, \qquad n_p \in \mathbb{Z}$$

un nombre rationnel. Comme

$$\|x\|_p = \left(\frac{1}{p}\right)^{n_p},$$

et

$$\|x\|_\infty = |x|,$$

la formule résulte du théorème d'Ostrowski.

b) Considérons maintenant le cas général. Pour les valeurs non-archimédienne au-dessus de p la formule (*) et le corollaire 2.3.4 donnent:

$$\prod_{v|p} \|x\|_v = \|N_{K/\mathbb{Q}}(x)\|_p.$$

Pour les valeurs archimédiennes ona de même:

$$\prod_{v|\infty} \|x\|_v = \|N_{K/\mathbb{Q}}(x)\|_\infty.$$

Donc,

$$\prod_v \|x\|_v = \|N_{K/\mathbb{Q}}(x)\|_\infty \prod_p \|N_{K/\mathbb{Q}}(x)\|_p = 1.$$

Soit $\mathfrak{a}$ un idéal non-nul de O_K et soit

$$\mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{a})}$$

la factorisation de $\mathfrak{a}$. Comme $card(O_K/\mathfrak{p}^k) = q_\mathfrak{p}^k$, où $q_\mathfrak{p}$ est le cardinal du corps résiduel $k_\mathfrak{p}$, le lemme chinois implique que le quotient $O_K/\mathfrak{a}$ est fini. On pose

$$\mathbf{N}\mathfrak{a} = card(O_K/\mathfrak{a}).$$

On note $\mathcal{D}_K$ (résp. D_K) la différente (résp. le discriminant) de O_K sur $\mathbb{Z}$.

Si L/K est une extension galoisienne, on pose $G = Gal(L/K)$. Pour tout idéal premier $\mathfrak{P} \mid \mathfrak{p}$ de O_L on note $G_\mathfrak{P}$ le groupe de décomposition en $\mathfrak{P}$. On a

$$G_\mathfrak{P} \simeq Gal(L_\mathfrak{P}/K_\mathfrak{p}).$$

En particulier, si $\mathfrak{P}$ est non-ramifié, le groupe $G_\mathfrak{P}$ est engendré par l'automorphisme de Frobenius qu'on note $F_\mathfrak{P}$ (voir §9). Pour tout $x \in O_L$ on a:

$$F_\mathfrak{P}(x) \equiv x^{q_\mathfrak{p}} \pmod{\mathfrak{P}}.$$

Rappelons que par le corollaire 2.11.13 préque tous les idéaux premiers sont non-ramifiés.

§2. Groupe de classes

Dans ce paragraphe on montre le théorème suivant qui est fondamental en théorie des nombres:

THÉORÈME 3.2.1. *Soit K un corps de nombres. Alors le groupe de classes d'idéaux $Cl(O_K)$ est fini.*

PREUVE. On commence par un petit lemme technique:

LEMME 3.2.2. *Soit K un corps de nombres de degré n sur $\mathbb{Q}$ et soit $\omega_1, \ldots, \omega_n$ une base de O_K sur $\mathbb{Z}$. Il existe une constante C telle que pour tout $N \geqslant 1$ et pour tout $x = \sum_{i=1}^\infty a_i\omega_i \in O_K$ vérifiant*

$$|a_i| \leqslant 2(N+1), \qquad i = 1, \ldots, n$$

on ait

$$N_{K/\mathbb{Q}}(x) \leqslant CN^n\,.$$

Preuve du lemme 3.2.2. Soient $\sigma_i : K/\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}/\mathbb{Q}$, $i = 1, \ldots, n$ les plongements de $K/\mathbb{Q}$ dans $\bar{\mathbb{Q}}/\mathbb{Q}$. Par le théorème 0.3.2 on a

$$\left|N_{K/\mathbb{Q}}(x)\right| = \prod_{i=1}^{n} |a_1\sigma(\omega_1) + \ldots + a_n\sigma(\omega_n)| \leqslant \sum_{1\leqslant i_1,\ldots,i_n\leqslant n} b_{i_1,\ldots,i_n}|a_{i_1}|\,|a_{i_2}|\,|a_{i_n}|,$$

où

$$b_{i_1,\ldots,i_n} = |\sigma_1(\omega_{i_1})\sigma_2(\omega_2)\cdot\ldots\cdot\sigma_n(\omega_n)|\,.$$

En posant $B = \sum_{1\leqslant i_1,\ldots,i_n\leqslant n} b_{i_1,\ldots,i_n}$ et $C = 2^{2n}B$ on obtient

$$\left|N_{K/\mathbb{Q}}(x)\right| \leqslant B(2(N+1))^n = 2^nB(N+1)^n \leqslant 2^nB(2N)^n = CN^n.$$

Le lemme est démontré.

Passons à la démonstration du théorème 3.2.1. Soit $\mathfrak{a}$ un idéal non-nul de O_K. Comme $\mathfrak{a}^{-1}$ est un idéal fractionnaire, il existe un élément non-nul $\alpha \in O_K$ tel que $\mathfrak{b} = \alpha\mathfrak{a}^{-1} \subseteq O_K$. Soit

$$S = \{x = \sum_{i=1}^{n} a_i\omega_i \,|\, 0 \leqslant a_i \leqslant (\mathbf{N}\mathfrak{b})^{1/n} + 1\}.$$

Alors pour le cardinal de S on a

$$card(S) = ([(\mathbf{N}\mathfrak{b})]^{1/n} + 2)^n \geqslant (\mathbf{N}\mathfrak{b})^{1/n} + 1)^n \geqslant \mathbf{N}\mathfrak{b} + 1.$$

Considérons la projection canonique

$$O_K \to O_K/\mathfrak{b}.$$

Comme $card(O_K/\mathfrak{b}) = \mathbf{N}\mathfrak{b} < card(S)$, il existe $y, z \in S$, $y \neq z$ tels que $y \equiv z \pmod{\mathfrak{b}}$ i.e. $x = y - z \in \mathfrak{b}$. Soit $x = \sum_{i=1}^{n} a_i\omega_i$. Alors les coefficients a_i vérifient

$$|a_i| \leqslant 2((\mathbf{N}\mathfrak{b})^{1/n} + 1)$$

et le lemme 3.2.2 donne:

$$\left|N_{K/\mathbb{Q}}(x)\right| C(\mathbf{N}\mathfrak{b}).$$

Comme $x \in \mathfrak{b}$, on a $\mathfrak{b} \mid (x)$ et il existe un idéal $\mathfrak{c}$ de O_K tel que $(x) = \mathfrak{b}\mathfrak{c}$. On a

$$(\mathbf{N}\mathfrak{c})\,(\mathbf{N}\mathfrak{b}) = \mathbf{N}(\mathfrak{b}\mathfrak{c}) = \mathbf{N}((x)) = \left|N_{K/\mathbb{Q}}(x)\right| \leqslant C(\mathbf{N}\mathfrak{b}),$$

d'où

$$(*) \qquad \mathbf{N}\mathfrak{c} \leqslant C.$$

Comme $\mathfrak{b} = \alpha\mathfrak{a}^{-1}$ et $\mathfrak{c} = x\mathfrak{b}^{-1}$, les idéaux $\mathfrak{a}$ et $\mathfrak{c}$ sont équivalents i.e. appartiennent à la même classe dans $Cl(O_K)$. Donc, nous avons montré que dans chaque classe d'idéaux il existe un représentant $\mathfrak{c}$ vérifiant (*). Pour terminer la démonstration il suffit de montrer qu'il n'existe qu'un nombre fini d'idéaux vérifiant (*).

Soit p un nombre premier. Si $\mathfrak{c} \mid p$, alors $\mathbf{N}\mathfrak{c} \geqslant p$ ce qui signifie que si un idéal $\mathfrak{c}$ vérifie (*), alors $p \leqslant C$. Le théorème résulte maintenant du fait que pour tout p il n'existe qu'un nombre fini d'idéaux $\mathfrak{c}$ divisant p.

DÉFINITION. *Le cardinal h_K de $Cl(O_K)$ est appelé le nombre de classes de K.*

C'est un invariant très important. Rappelons que $h_K = 1$ si et seulement si O_K est principal. En général, h_K mésure la "complexité" de l'arithmétique de O_K. Dans les cas "simples" on peut calculer h_K en utilisant au lieu du théorème 3.2.1 sa version effective suivante:

THÉORÈME 3.2.3. *Soient K un corps de nombres, n sons degré, r_2 le nombre des valeurs absolues normalisées complexes de K. Soit D_K le discriminant de $K/\mathbb{Q}$. Alors toute classe d'idéaux contient un idéal $\mathfrak{a}$ tel que*

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

PREUVE. Voir [S], §4.3, proposition 1 et corollaire 1.

§3. Le théorème de Dirichlet

Soit K un corps de nombres. On appelle groupe des unités de K et on note U_K le groupe des unités de O_K. Dans ce paragraphe on étudie la structure de U_K. On note S_f (résp. S_∞ les valeurs absolues normalisées non-archimédiennes (résp. archimédiennes) de K.

PROPOSITION 3.3.1. *i) Un élément $x \in K$ est une unité de K si et seulement si*

$$\|x\|_v = 1, \qquad \textit{pour tout } v \in S_f.$$

ii) Soit $x \in U_K$. Alors

$$\sum_{v \in S_\infty} \log(\|x\|_v) = 0,$$

PREUVE. i) Par la propriété iii), §6, chapitre II, $x \in O_K$ si et seulement si $\|x\|_v \leq 1$ pour tout $v \in S_f$. Comme $\|x^{-1}\|_v = \|x\|_v^{-1}$, on en déduit que $x \in U_K$ si et seulement si $\|x\|_v = 1$.

ii) Comme $\|x\|_v = 1$ pour $v \in S_f$, la formule du produit (théorème 3.1.5) s'écrit:

$$\prod_{v \in S_\infty} \|x\|_v = 1.$$

En prenant les logarithmes, on obtient ii).

DÉFINITION. *Soit V un $\mathbb{R}$-espace vectoriel de dimension finie m. On appelle réseau de V un $\mathbb{Z}$-module libre $L \subset V$ de rang m.*

Soient $v_1, \ldots, v_{r_1}$ les valeurs absolues réelles et $v_{r_1+1}, \ldots, v_{r_1+r_2}$ les valeurs absolues complexes de K. Considérons l'application:

$$\mathcal{L}_K \ : \ U_K \to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2},$$
$$\mathcal{L}_K(x) = (\log(\|x\|_{v_1}), \ldots, \log(\|x\|_{v_{r_1}}), \log(\|x\|_{v_{r_1+1}}), \ldots, \log(\|x\|_{v_{r_1+r_2}}).$$

THÉORÈME 3.3.2 (DIRICHLET). *L'application $\mathcal{L}_K$ est un homomorphisme. Son noyau coïncide avec le groupe μ_K des racines de l'unité contenues dans K. L'image de $\mathcal{L}_K$ est un réseau du hyperplan*

$$H = \{(x_1, \dots, x_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{R}^{r_2} \mid \sum_{i=1}^{r_1+r_2} x_i = 0\}.$$

de $\mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$. En particulier, U_K est isomorphe à la somme directe $\mu_K \times \mathbb{Z}^{r_1+r_2}$.

PREUVE. Comme pour tout v on a

$$\log(\|xy\|_v) = \log(\|x\|_v) + \log(\|y\|_v),$$

l'application $\mathcal{L}_K$ est un homomorphisme et par la proposition 3.3.1 son image est contenue dans H.

Si $x \in \mu_K$, alors $\sigma(x)$ est une racine de l'unité dans $\mathbb{C}$ pour tout plongement σ, d'où $\|x\|_v = 1$ et $\log(\|x\|_v) = 0$. Donc, $\mu_K \subseteq \ker(\mathcal{L}_K)$.

Réciproquement, si $\mathcal{L}_K(x) = 0$, alors $|\sigma(x)| = 1$ pour tout $\sigma \in Hom_{\mathbb{Q}}(K, \mathbb{C})$. Soit

$$f(X) = a_0 + a_1 X + \cdots + X^n \in \mathbb{Z}[X]$$

le polynôme minimal de x. Comme

$$f(X) = \prod_{\sigma}(X - \sigma(x)),$$

on obtient qu'il existe une constante C telle que pour tout $x \in U_K$ les coefficients de $f(X)$ sont bornés par C :

$$(*) \qquad |a_i| \leq C.$$

Comme il n'existe qu'un nombre fini de polynômes $f(X) \in \mathbb{Z}[X]$ vérifiant (*), on obtient que $\ker(L_K)$ est fini. Par le théorème 0.4.3 ceci implique que $\ker(L_K) = \mu_K$.

Il reste à montrer que l'image de $\mathcal{L}_K$ est un *réseau* de H. C'est la partie la plus difficile de la démonstration qui nécessite une étude plus profonde des plongements de K dans $\mathbb{C}$. Voir [S], chapitre IV.

§4. Corps quadratiques

Dans ce paragraphe nous appliquons la théorie générale à l'étude des corps quadratiques.

DÉFINITION. *On appelle corps quadratique un corps de nombre K de degré 2 sur $\mathbb{Q}$.*

PROPOSITION 3.4.1. *Soit K un corps quadratique. Alors il existe un entier $d \in \mathbb{Z}$ sans facteurs carrés tel que*

$$K = \mathbb{Q}(\sqrt{d}).$$

PREUVE. Soit $K = \mathbb{Q}(\alpha)$. Comme $[K : \mathbb{Q}] = 2$, le polynôme minimal de α sur $\mathbb{Q}$ est de degré 2 i.e. il existe $a, b \in \mathbb{Q}$ tels que

$$\alpha^2 + a\alpha + b = 0.$$

Posons $c = a^2 - 4b \in \mathbb{Q}$. Alors $\alpha = \frac{-a \pm \sqrt{c}}{2}$, d'où $K = (\sqrt{c})$. Il est facile de voir que c s'ecrit de manière unique sous la forme $c = c_1^2 d$, où $c_1 \in \mathbb{Q}$ et $d \in \mathbb{Z}$ est un entier sans facteurs carrés. Alors $\mathbb{Q}(\sqrt{c}) = \mathbb{Q}(\sqrt{d})$, d'où la proposition.

Par le théorème 0.2.3 tout élément $x \in K$ s'écrit de façon unique sous la forme $x = a + b\sqrt{d}$, avec $a, b \in \mathbb{Q}$. L'extension $K/\mathbb{Q}$ est galoisienne et on a

$$Gal(K/\mathbb{Q}) = \{id, \sigma\},$$

où l'automorphisme σ est défini par $\sigma(\sqrt{d}) = -\sqrt{d}$. Nous allons maintenant déterminer l'anneau des entiers de K.

PROPOSITION 3.4.2. *i) Si $d \equiv 2$ ou $3 \pmod 4$, alors*

$$O_K = \mathbb{Z} + \mathbb{Z}\sqrt{d};$$

ii) Si $d \equiv 1 \pmod 4$, alors

$$O_K = \mathbb{Z} + \mathbb{Z}\omega,$$

où $\omega = \dfrac{-1 + \sqrt{d}}{2}$.

PREUVE. Soit $x = a + b\sqrt{d}$, $b \neq 0$. Alors $\sigma(x) = a - b\sqrt{d}$ et le polynôme minimal de x sur $\mathbb{Q}$ s'écrit

$$f(X) = (X - x)(X - \sigma(x)) = X^2 - (x + \sigma(x))X + x\sigma(x) = X^2 - 2aX + (a^2 - b^2 d).$$

Donc, $x \in O_K$ si et seulement si $2a \in \mathbb{Z}$ et $a^2 - b^2 d \in \mathbb{Z}$. En particulier, si $x \in O_K$, alors

$$(2b)^2 d = 4b^2 d = (2a)^2 - 4(a^2 - b^2 d) \in \mathbb{Z}.$$

Comme d est sans facteurs carrés on en déduit que $2b \in \mathbb{Z}$. Posons $m = 2a$ et $n = 2b \in \mathbb{Z}$. Alors

$$(*) \qquad m^2 - n^2 d = 4(a^2 - b^2 d) \equiv 0 \pmod 4.$$

Remarquons que pour tout $m \in \mathbb{Z}$ on a $m^2 \equiv 0 \pmod 4$ ou $m^2 \equiv 1 \pmod 4$.

i) Si $d \equiv 2$ *ou* $3 \pmod 4$, on voit facilement que (*) n'est possible que si $m, n \equiv 0 \pmod 2$, d'où on obtient que $a, b \in \mathbb{Z}$.

ii) Si $d \equiv 1 \pmod 4$, alors le même raisonnement montre que (*) est satisfaite si m et n ont même parité. Donc dans ce cas on a

$$x = a + b\sqrt{d} = \frac{m - n}{2} + n\omega,$$

avec $(m - n)/2 \in \mathbb{Z}$, d'où le résultat.

PROPOSITION 3.4.3. *Le discriminant absolue de $K = \mathbb{Q}(\sqrt{d})$ est*

$$D_K = \begin{cases} 4d, & si\ d \equiv 2, 3 \pmod 4, \\ d, & si\ d \equiv 1 \pmod 4. \end{cases}$$

PREUVE. On a $Tr_{K/\mathbb{Q}}(1) = 2$ et $Tr_{K/\mathbb{Q}}(\sqrt{d}) = 0$. Si $d \equiv 2, 3 \pmod 4$, alors

$$D_K = \begin{vmatrix} Tr_{K/\mathbb{Q}}(1) & Tr_{K/\mathbb{Q}}(\sqrt{d}) \\ Tr_{K/\mathbb{Q}}(\sqrt{d}) & Tr_{K/\mathbb{Q}}(d) \end{vmatrix} = 4d.$$

Si $d \equiv 1 \pmod 4$, alors

$$D_K = \begin{vmatrix} Tr_{K/\mathbb{Q}}(1) & Tr_{K/\mathbb{Q}}(\omega) \\ Tr_{K/\mathbb{Q}}(\omega) & Tr_{K/\mathbb{Q}}(\omega^2) \end{vmatrix} = d.$$

Etudions maintenant la décomposition des nombres premiers dans l'extension $K/\mathbb{Q}$.

DÉFINITION. *Soit p un nombre premier impair et soit $d \neq 0 \pmod p$ un entier. On dit que d est un résidu quadratique modulo p si la congruence*

$$X^2 \equiv d \pmod p$$

est résoluble dans $\mathbb{Z}$. Sinon, on dit que d est un non-résidu quadratique modulo p.

THÉORÈME 3.4.4. *Soit $K = \mathbb{Q}(\sqrt{d})$ et soit p un nombre premier.*

i) Si $p \nmid D_K$ et si d est un résidu quadratique modulo p, alors p se décompose dans O_K en produit des deux idéaux:

$$pO_K = \mathfrak{p}_1\mathfrak{p}_2\,, \qquad \mathfrak{p}_1 \neq \mathfrak{p}_2.$$

ii) Si $p \nmid D_K$ et si d est un non-résidu quadratique modulo p, alors p est inerte dans O_K i.e. pO_K est un idéal premier de O_K.

iii) Si $p \mid D_K$, alors p se ramifie dans O_K i.e.

$$pO_K = \mathfrak{p}^2.$$

PREUVE. i) Comme $K/\mathbb{Q}$ est galoisienne, la factorisation d'un nombre premier p dans O_K s'écrit:

$$p\,O_K = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_g)^{e_g},$$

où $e_p f_p g_p = [L : K] = 2$ (théorème 2.6.7).

Si $p \nmid D_K$, alors $K/\mathbb{Q}$ est non-ramifiée au-dessus de p et on a $e_p = 1$, $f_p g_p = 2$. Si la congruence $X^2 \equiv d \pmod p$ est résoluble, le polynôme $X^2 - \bar{d}$ a une racine ξ dans $\mathbb{F}_p$. Comme $p \neq 2$, on a $-\xi \neq \xi$ ce qui montre que ξ est une raçine simple. Alors par le Corollaire 2.4.3 au lemme de Hensel l'équation $X^2 = d$ a une raçine dans $\mathbb{Q}_p$ d'où $K_\mathfrak{p} = \mathbb{Q}_p$ pour tout idéal premier $\mathfrak{p}$ au-dessus de p. Donc $f_p = 1$ et $g_p = 2$.

ii) Si $p \nmid D_K$, et la congruence $X^2 \equiv d \pmod p$, n'est pas résoluble, l'équation $X^2 = d$ n'a pas de solutions dans K. Donc $K_\mathfrak{p} \neq \mathbb{Q}_p$, d'où $[K_\mathfrak{p} : \mathbb{Q}_p] = e_p f_p = 2$. Comme $e_p = 1$, on en déduit que $f_p = 2$ et $g_p = 1$.

iii) Si $p \mid D_K$, les idéaux au-dessus de p sont ramifié, d'où $e_p > 1$. Comme $e_p f_p g_p = 2$, on obtient $f_p = 1$ et $g_p = 1$, d'où le théorème.

Remarque. Avec la même méthode on peut traiter le cas $p = 2$.

DÉFINITION. *On dit que $K = \mathbb{Q}(\sqrt{d})$ est un corps quadratique réel (résp. imaginaire) si $d > 0$ (résp. si $d < 0$).*

PROPOSITION 3.4.5. *Si $K = Q(\sqrt{d})$ est un corps quadratique imaginaire, alors*

$$U_K = \begin{cases} \{\pm 1\}, & si\ d \neq -1, -3, \\ \{\pm 1, \pm i\}, & si\ d = -1, \\ \mu_6, & si\ d = -3. \end{cases}$$

PREUVE. Si $d \equiv 2, 3 \pmod 4$, une unité $u \in U_K$ s'écrit $u = a + b\sqrt{d}$ et $N_{K\mathbb{Q}}(u) = a^2 - b^2 d$ est une unité de $\mathbb{Z}$. Donc $a^2 + b^2 d = 1$, d'où on déduit que $b = 0$ et $a = \pm 1$ si $d \neq -1$.

Si $d = -1$, on a $a^2 + b^2 = 1$, d'où on obtient que $U_K = \{\pm 1, \pm i\}$.

Si $d \equiv 1 \pmod 4$, une unité $u \in U_K$ s'écrit $u = \dfrac{a + b\sqrt{d}}{2}$ avec $a \equiv b \pmod 2$. Alors

$$N_{K/\mathbb{Q}}(u) = \frac{a^2 - b^2 d}{4}$$

ce qui donne l'équation $a^2 + b^2|d| = 1$. Un raisonnement élémentaire montre que si $d \neq -3$, alors $a = \pm 2$ et $b = 0$, d'où $U_K = \{\pm 1\}$. Si $d = -3$, on a 6 solutions $(\pm 2, 0)$ et $(\pm 1, \pm 1)$ qui donnent les racines 6-ièmes de l'unité. Le théorème est démontré.

PROPOSITION 3.4.6. *Si K est un corps quadratique réel, alors U_K est la somme directe du groupe μ_2 d'ordre 2 et d'un groupe cyclique infini:*

$$U_K \simeq \mu_2 \times \mathbb{Z}.$$

PREUVE. Comme ± 1 sont les seules racines de l'unité dans $\mathbb{R}$, on a $\mu_K = \{\pm 1\}$. Comme $d > 0$, les racines du polynôme $X^2 - d = 0$ dans $\mathbb{C}$ sont réelles ce qui montre que $r_1 = 2$ et $r_2 = 0$. Par le théorème de Dirichlet on obtient que U_K est isomorphe à $\mu_2 \times Z$.

Remarque. On peut donner une preuve élémentaire de la proposition 3.4.6.

Bien qu'il existe beaucoup de résultats sur la structure du groupe de classes $Cl(O_K)$ d'un corps quadratique, c'est un objet qui est difficile à étudier. Voici quelques exemples:

i) Il y a des formules explicites (assez compliquées) pour le nombre de classes h_K.

ii) Pour les corps quadratiques imaginaires $\mathbb{Q}(\sqrt{d})$ Siegel a montré que

$$\frac{\log(h_K)}{\log |D_K|^{1/2}} \underset{d \to -\infty}{\longrightarrow} 1.$$

En particulier, pour tout C il n'existe qu'un nombre fini de K tels que $h_K \leq C$.

iii) Les seuls corps quadratiques imaginaires K avec $h_K = 1$ sont $\mathbb{Q}(\sqrt{d})$, $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. C'est une conjecture de Gauss qui a été démontrée par Heegner, Stark et Baker dans les années 60.

iv) Gauss a conjecturé qu'il existe une infinité de corps quadratiques réel avec $h_K = 1$. Ce problème reste ouvert.

§5. Corps cyclotomiques

Dans ce paragraphe nous appliquons la théorie générale à l'étude des corps cyclotomiques.

DÉFINITION. *On appelle corps cyclotomique et on note K_n le corps*

$$K_n = \mathbb{Q}(\zeta_n)$$

où ζ_n est une racine primitive n-ième de l'unité.

Il est bien connu que K_n est une extension galoisienne finie de $\mathbb{Q}$. Soit $G_n = Gal(K_n/\mathbb{Q})$. Alors G permute les racines n-ièmes de l'unité i.e. pour tout $g \in G$ il existe $i(g) \in \mathbb{Z}$ tel que

$$g(\zeta_n) = \zeta_n^{i(g)}.$$

Comme $\zeta_n^n = 1$, l'action de $g \in G$ sur K_n est completement définie par la classe de $i(g)$ modulo n. L'application

$$G \to (\mathbb{Z}/n\mathbb{Z})^*,$$
$$g \mapsto i(g) \pmod{n}$$

est un isomorphisme de G_n sur le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. En particulier, G_n est abélien.

Définition. *On dit qu'une extension galoisienne L/K est abélienne, si $Gal(L/K)$ est un groupe abélien.*

Le rôle des corps cyclotomiques dans la théorie des nombres s'éxplique par le théorème suivant:

Théorème 3.5.1 (Kronecker-Weber). *Soit K une extension abélienne de $\mathbb{Q}$. Alors il existe n tel que $K \subseteq K_n$.*

Preuve. Bien qu'il s'agit d'un résultat classique, sa preuve "élémentaire" est assez compliquée. On peut aussi déduire ce théorème de la théorie des corps de classes.

Nous allons étudier la décomposition des nombres premiers dans K_n. Pour simplifier, on suppose que $n = p$ est un nombre premier $\neq 2$ et on pose $K = \mathbb{Q}(\zeta_p)$.

Proposition 3.5.2. *i) Soient l un nombre premier et $\mathbb{Q}_l$ le corps des nombres l-adiques. Si $l \neq p$, alors $\mathbb{Q}_l(\zeta_p)$ est une extension non-ramifiée de $\mathbb{Q}_l$. On a*

$$[\mathbb{Q}_l(\zeta_p) : \mathbb{Q}_l] = f,$$

où f est le plus petit nombre naturel vérifiant la congruence $l^f \equiv 1 \pmod{p}$.

ii) L'extension $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ est totalement ramifiée de degré $p-1$.

Preuve. i) Comme $p \neq l$, la congruence

$$(*) \qquad l^x \equiv 1 \pmod{p}$$

est résoluble (par exemple, on peut prendre $x = p-1$ et utiliser le petit théorème de Fermat). Soit f le plus petit nombre naturel vérifiant (*). Par le théorème 2.9.6, $\mathbb{Q}_l(\zeta_{l^f-1})$ est une extension non-ramifiée de $\mathbb{Q}_l$ de degré f. Comme $p \mid l^f - 1$, on a $\zeta_p = \zeta_{l^f-1}^k$, où $l^f - 1 = pk$ ce qui montre que $\mathbb{Q}_l(\zeta_p) \subseteq \mathbb{Q}_l(\zeta_{l^f-1})$. On en déduit i).

ii) Soit $\pi = \zeta_p - 1$. Comme $\zeta_p^p = 1$, l'élément π est une racine du polynôme

$$f(X) = \frac{(1+X)^p - 1}{X} = X^{p-1} + C_p^{p-1}X^{p-2} + \cdots + C_p^2 X + p.$$

Comme p divise C_p^k, on voit que $f(X)$ est un polynôme d'Eisenstein et ii) découle du théorème 2.10.2.

THÉORÈME 3.5.3. *Soit l un nombre premier et soit (l) l'idéal principal de O_K qui est engendré par l. Alors:*

i) Si $l \neq p$, la factorisation de (l) s'écrit:

$$(l) = \mathfrak{l}_1 \cdot \ldots \cdot \mathfrak{l}_{g_l}.$$

Les idéaux $\mathfrak{l}_i$ sont non-ramifiés et leur degré résiduel $f_l = f(\mathfrak{l}_i/l)$ est la plus petite solution de la congruence $l^x \equiv 1 \pmod{p}$. En plus,

$$g_l f_l = p - 1.$$

ii) La factorisation de (p) s'écrit:

$$(p) = \mathfrak{p}^{p-1},$$

où $\mathfrak{p}$ est l'unique idéal premier au-dessus de p. Plus précisement, on a

$$\mathfrak{p} = (1 - \zeta_p).$$

PREUVE. i) Comme $K/\mathbb{Q}$ est galoisienne, la factorisation de (l) s'écrit

$$(l) = (\mathfrak{l}_1 \mathfrak{l}_2 \cdots \cdot \ldots \cdot \mathfrak{l}_{g_l})^{e_l}.$$

i) Si $l \neq p$, la proposition 3.2.5 implique que $e_l = 1$ et que le degré résiduel f_l est la plus petite solution de la congruence $l^x \equiv 1 \pmod{p}$. Comme $e_l f_l g_l = [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$, on en déduit i).

ii) Si $l = p$, alors la proposition 3.2.5 donne $e_p = p - 1$, d'où $f_p = g_p = 1$. On a

$$X^{p-1} + X^{p-2} + \cdots + 1 = (X^p - 1)/(X - 1) = \prod_{k=1}^{p-1} (X - \zeta_p^k).$$

En posant $X = 1$ on obtient:

$$p = \prod_{k=1}^{p-1} (1 - \zeta_p^k) = (1 - \zeta_p)^{p-1} \prod_{k=1}^{p-1} u_k,$$

où

$$u_k = \frac{1 - \zeta_p^k}{1 - \zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{k-1}.$$

Il est facile à montrer que u_k sont des unités. En effet, si $k < p$, alors il existe i tel que $ki \equiv 1 \pmod{p}$, d'où

$$u_k^{-1} = \frac{1 - \zeta_p^{ki}}{1 - \zeta_p^k} = 1 + \zeta_p^i + \cdots + \zeta_p^{i(k-1)}.$$

Donc, on a

$$(p) = (\zeta_p - 1)^{p-1}$$

et par l'unicité de factorisation on obtient que $\mathfrak{p} = (\zeta_p - 1)$.

Nous pouvons maintenant calculer la différente et le discriminant de $\mathbb{Q}(\zeta_p)$.

PROPOSITION 3.5.4. *On a*

$$\mathcal{D}_K = (\zeta_p - 1)^{p-2}$$

et

$$d_K = p^{p-2}$$

PREUVE. On a

$$\mathcal{D}_K = \prod_{\mathfrak{l}} \mathcal{D}_{K_\mathfrak{l}},$$

où $\mathfrak{l}$ parcourt tous les idéaux premiers de O_K. Si $\mathfrak{l} \neq \mathfrak{p}$, alors par le théorème 3.5.3 $K_\mathfrak{l}/\mathbb{Q}_l$ est non-ramifiée et le théorème 2.11.810 donne $\mathcal{D}_{K_\mathfrak{l}} = O_\mathfrak{l}$. Si $\mathfrak{l} = \mathfrak{p}$, le même théorème donne:

$$\mathcal{D}_{K_\mathfrak{p}} = (f'(\pi)),$$

où $\pi = \zeta - 1$. On a

$$f'(X) = (p-1)X^{p-2} + (p-2)C_p^{p-1}X^{p-3} + \cdots + C_p^2.$$

Comme $v_K((p-1)\pi^{p-2}) = p-2$ et

$$v_K(C_p^{p-k}) \geq v_K(p) = e_p = p-1,$$

on obtient que $\mathcal{D}_{K_\mathfrak{p}} = (\pi^{p-2}) = (\zeta_p - 1)^{p-2}$. On en déduit la première formule.

D'autre part, on a:

$$(D_K) = (\mathcal{N}_{K/\mathbb{Q}}(\mathcal{D}_K)) = \mathcal{N}_{K/\mathbb{Q}}(\zeta_p - 1)^{p-2} = p^{p-2}.$$

La proposition est démontrée.

Cette proposition nous permet de déterminer l'anneau des entiers de O_K.

PROPOSITION 3.5.5. *On a*

$$O_K = \mathbb{Z}[\zeta_p],$$

i.e. $1, \zeta_p, \ldots, \zeta_p^{p-2}$ *forment une base de* O_K *sur* $\mathbb{Z}$.

PREUVE. L'inclusion $\mathbb{Z}[\zeta_p] \subseteq O_K$ est evidente car $1, \zeta_p, \ldots, \zeta_p^{p-2}$ sont des entiers sur $\mathbb{Z}$. Donc pour montrer que $\mathbb{Z}[\zeta_p] = O_K$ il suffit que prouver que ces deux réseaux ont même discriminant. Comme

$$X^p - 1 = f(X)(X-1),$$

on a

$$pX^{p-1} = f'(X)(X-1) + f(X).$$

En posant $X = \zeta_p - 1$ on obtient

$$f'(\zeta_p) = \frac{p}{\zeta_p(\zeta_p - 1)}.$$

Comme $N_{K/\mathbb{Q}}(\zeta_p) = 1$ et $N_{K/\mathbb{Q}}(\zeta_p - 1) = p$, la proposition 0.3.5 donne

$$D_K(1, \zeta_p, \ldots, \zeta_p^{p-2}) = \pm N_{K/\mathbb{Q}}(f'(\zeta_p)) = \pm p^{p-2}.$$

d'où l'égalité voulue.