THÉORIE DES NOMBRES
BESANÇON

Années 1996/97-1997/98

Genres et facteurs invariants de formes hermitiennes

P. CALAME

UNIVERSITÉ DE LAUSANNE FACULTÉ DES SCIENCES

Genres et facteurs invariants de formes hermitiennes

Philippe Calame

Ce travail a été effectué en vue de
l'obtention du Diplôme de mathématicien
de l'université de Lausanne,
sous la direction du Professeur
Jacques Boéchat.

Mai 1997

Introduction

Il est souvent intéressant et utile, en théorie des nombres, de comparer une propriété d'un objet sur un corps de nombres avec la propriété de l'objet dans ses localisés ; on mettra en relation, par exemple, le fait qu'un élément d'un corps de nombre soit un carré avec le fait qu'il le soit dans chacun de ses localisés. La théorie des formes quadratiques sur les corps de nombres, comme celles des formes hermitiennes, utilise avec succès ce procédé *local-global* avec, comme point central, le théorème de Hasse-Minkowski qui est certainement un des résultats les plus difficiles et les plus profonds de la théorie. Ce théorème nous dit essentiellement que l'isométrie de deux espaces quadratiques (ou hermitiens) sur un corps de nombres est caractérisée par leur isométrie sur tous les localisés : deux espaces sont globalement isométriques si et seulement s'ils sont localement isométriques.

Nous nous intéresserons aux réseaux, qui seront pour nous des espaces hermitiens sur l'anneau des entiers d'un corps de nombres. L'analogue du théorème de Hasse-Minkowski dans ce cadre n'est plus vrai, et nous pouvons définir une relation d'équivalence plus faible que l'isométrie, correspondant à l'isométrie locale : nous dirons alors que deux réseaux sont *dans le même genre* si tous leurs localisés sont isométriques.

Le but de ce travail est d'étudier les genres des réseaux. Nous commencerons par donner des invariants d'isométrie des réseaux ; nous montrerons qu'ils sont en fait des invariants de genre.
Si L est un réseau, on peut considérer son réseau dual $L^{\#}$ et les *facteurs invariants* de L dans $L^{\#}$; ces derniers comportent beaucoup d'informations sur les genres et en constituent de ce fait un invariant important.
D'autre part, si K est un corps de nombres et A son anneau des entiers, alors l'extension à K d'un A-réseau est un espace hermitien sur K qui, grâce au théorème de Hasse-Minkowski, est en fait un invariant de genre. Les signatures aux places infinies le sont alors aussi.
Dans ce travail, nous montrerons que le nombre de genres dont les représentants possèdent des facteurs invariants et des signatures donnés est fini et nous donnerons une méthode pour le calculer. La complication due au cas ramifié dyadique rend difficile l'écriture d'une formule générale explicite ; cependant, les résultats que nous obtiendrons nous permettront de trouver, de cas en cas et moyennant quelques calculs, une formule pour un choix particulier de facteurs invariants et de signatures.

Le premier chapitre sera consacré aux définitions générales ainsi qu'à la description sommaire des différents outils dont nous aurons besoin. Nous y définirons le genre et les facteurs invariants d'un réseau.

Le deuxième chapitre traitera de l'étude globale des espaces hermitiens sur un corps de nombres. Nous commencerons par étudier les espaces hermitiens sur les localisés. Nous déduirons ensuite du théorème de Hasse-Minkowski pour les formes quadratiques une

version identique pour les formes hermitiennes, ce qui nous conduira naturellement au théorème de Landherr.

Dans le troisième chapitre, nous étudierons les liens entre l'isométrie des réseaux sur un corps local et leurs facteurs invariants. Nous observerons tout d'abord que les facteurs invariants d'un réseau correspondent parfaitement à ses *décompositions de* Jordan. Nous distinguerons ensuite trois cas possibles de corps locaux : les cas non ramifié, ramifié non dyadique et ramifié dyadique. Le premier cas est vraiment très facile alors que les complications et les difficultés techniques sont beaucoup plus élevées pour le dernier.

Le dernier chapitre nous permettra de rassembler tous nos résultats et de passer du local au global. Nous calculerons le nombres de genres de réseaux de facteurs invariants et de signatures donnés.

Le travail se terminera par quatre annexes qui contiennent des applications calculatoires de la théorie exposée.

Dans la première, nous présenterons un outil de calcul, le *déterminant*, qui fournit une aide précieuse pour le calcul des facteurs invariants d'un réseau.

Dans les deux annexes suivantes, nous donnerons une liste explicite des genres de réseaux dans deux cas particulier : les genres de réseaux unimodulaires totalement définis positifs dans les extensions cyclotomiques, pour la deuxième annexe, et les genres de réseaux de rang 2 sur les entiers de Gauss, pour la troisième. Dans la quatrième et dernière annexe, nous verrons qu'un genre ne possède pas forcément de représentant libre, en montrant l'existence de contre-exemples pour certaines extensions quadratiques du corps des entiers rationnels. Nous en déduirons que leur anneau des entiers n'est pas principal.

Je tiens à remercier mon directeur de diplôme, le Professeur Jacques Boéchat, pour les discussions enrichissantes que nous avons eues et pour son aide à résoudre certains problèmes particuliers. Mes remerciements vont aussi à Maurice Mischler qui m'a proposé ce sujet et m'a soutenu durant la préparation du diplôme ainsi qu'au Professeur Henri Joris qui a accepté de relire ce travail.

Dorigny, mai 1997.

Table des matières

Chapitre 1

Généralités sur les corps de nombres et les formes hermitiennes

Dans ce premier chapitre, nous allons rappeler quelques notions qui nous seront utiles par la suite et définir ainsi le cadre dans lequel nous allons travailler.

Fixons tout d'abord quelques conventions.

Un anneau sera toujours commutatif et possédera toujours une unité.
D'autre part, on notera volontiers par une égalité les isomorphismes canoniques entre modules ou anneaux et par une inclusion les homomorphismes canoniques injectifs d'anneaux ou de modules.

§ 1. Produits de deux anneaux de Dedekind

Dans ce premier paragraphe, nous allons étudier le produit de deux copies d'un anneau de Dedekind et définir une notion de groupe d'idéaux fractionnaires pour ces types d'anneaux.

Mais rappelons tout d'abord la définition et quelques propriétés des anneaux de Dedekind.

On appelle *anneau de* Dedekind un anneau noethérien, intègre et intégralement clos tel que tout idéal premier non nul soit maximal.

Soit A un anneau de Dedekind. Notons K son corps des fractions.

On dit qu'un sous A-module $\mathfrak{a}$ de K est un *idéal fractionnaire* de A s'il existe $x \in K$ non nul tel que $x\,\mathfrak{a} \subset A$. On vérifie aisément qu'un sous A-module $\mathfrak{a}$ de K est un idéal fractionnaire de A si et seulement si $\mathfrak{a}$ est de type fini.

Pour la suite du texte, on dira idéal fractionnaire au lieu d'idéal fractionnaire non nul.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux fractionnaires, on appelle produit de $\mathfrak{a}$ et $\mathfrak{b}$ le sous A-module de K engendré par $\{\, xy \mid x \in \mathfrak{a},\ y \in \mathfrak{b} \,\}$ qui est encore un idéal fractionnaire de A et que l'on note $\mathfrak{a}\cdot\mathfrak{b}$. Il est bien connu que cette multiplication munit l'ensemble des idéaux fractionnaires $I(A)$ d'une structure de groupe abélien libre admettant l'ensemble des idéaux premiers non nuls de A comme base.
Si $\mathfrak{a} \in I(A)$ et si $\mathfrak{p}$ est un idéal premier de A, on appelle *valuation* $\mathfrak{p}$*-adique* de $\mathfrak{a}$ l'exposant de $\mathfrak{p}$ dans la décomposition de $\mathfrak{a}$ dans la base formée des idéaux premiers non nuls de A. On note $v_{\mathfrak{p}}(\mathfrak{a})$ la valuation $\mathfrak{p}$-adique de $\mathfrak{a}$. Il est clair que $v_{\mathfrak{p}} : I(A) \to \mathbb{Z}$ est un homomorphisme surjectif de groupes.
Si $x \in K^*$, on écrit $v_{\mathfrak{p}}(x)$ au lieu de $v_{\mathfrak{p}}(xA)$ ce qui définit un homomorphisme $v_{\mathfrak{p}} : K^* \to \mathbb{Z}$. Prolongeant $v_{\mathfrak{p}}$ à K en posant $v_{\mathfrak{p}}(0) = \infty$, on obtient une application $v_{\mathfrak{p}} : K \to \mathbb{Z} \cup \{\infty\}$ vérifiant $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$ et $v_{\mathfrak{p}}(x+y) \geqslant \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}$, avec les conventions

usuelles sur l'usage du symbole ∞. On obtient alors une valuation sur K que l'on appelle encore valuation $\mathfrak{p}$-adique (voir le paragraphe 3).

Enonçons encore brièvement deux théorèmes caractérisant respectivement les modules projectifs de type fini et les modules plats sur un anneau de Dedekind.

Rappelons tout d'abord quelques définitions et résultats.
Soit A un anneau, non nécessairement de Dedekind. Un A-module M est dit *projectif* s'il existe un A-module N tel que $M \oplus N$ soit libre. Remarquons que si M est projectif de type fini, on peut choisir un tel N de sorte que $M \oplus N$ soit libre de type fini.
Un A-module M est dit *plat* si pour toute application A-linéaire injective $f : B \to C$ l'homomorphisme $f \otimes \mathrm{Id} : M \otimes_A B \to M \otimes_A C$ induit par $x \otimes y \mapsto x \otimes f(y)$ est injectif.
Il est bien connu qu'un module projectif et nécessairement plat.

Pour la suite du chapitre, projectif signifiera projectif de type fini.

1.1 THÉORÈME. *Soient A un anneau de Dedekind et K son corps des fractions. Soit M un A-module de type fini. Alors les conditions suivantes sont équivalentes :*

(i) M est projectif.

(ii) M est sans torsion.

(iii) M est isomorphe à un sous A-module d'un K-espace vectoriel V de dimension finie.

(iv) L'homomorphisme $M \to M \otimes_A K$ induit par $x \mapsto x \otimes 1$ est injectif.

Preuve. La preuve se trouve dans [2]. L'équivalence entre (ii), (iii) et (iv) est la proposition 4.1 de la page 88. L'implication de (ii) par (i) est claire, alors que sa réciproque est l'assertion (b) du théorème 13 de la page 95. □

En particulier, tout idéal fractionnaire d'un anneau de Dedekind est projectif.

1.2 THÉORÈME. *Soit A un anneau de Dedekind. Un A-module est plat si et seulement s'il est sans torsion*

Preuve. Notons K le corps des fractions de A. Soit M un A-module.
Supposons M plat. Alors l'homomorphisme canonique $M \to M \otimes_A K$ est injectif et ainsi l'égalité $x = x \otimes 1 = ax \otimes \frac{1}{a}$, vérifiée pour tout $x \in M$ et pour tout $a \in A$ non nul, nous montre que M est sans torsion.
Réciproquement, supposons M sans torsion. Alors tous ses sous-modules de type fini sont sans torsion donc, vu le théorème 1.1, projectifs et en particulier plats. On conclut alors en observant qu'un module est plat si tous ses sous-modules de type fini le sont. Ce fait découle en effet de l'équivalence entre les assertions (a) et (b) du théorème 3, page 147, dans [1]. □

Soient A un anneau de Dedekind et K son corps des fractions. Etudions l'anneau $A \times A$. Posons $B = A \times A$ et $E = K \times K$.

Considérons les homomorphismes d'anneaux $\pi_1, \pi_2 : E \to K$ définis respectivement par $\pi_1(x, y) = x$ et $\pi_2(x, y) = y$. Chacun d'eux munit K d'une structure de E-algèbre que

l'on note K_1 et K_2 respectivement. Il est clair que $E = K_1 \oplus K_2$ en tant que E-module.

Le même phénomène se produit au niveau des anneaux : les homorphismes π_1 et π_2 induisent des structures de B-algèbre sur A notées respectivement A_1 et A_2. On a aussi $B = A_1 \oplus A_2$ comme B-module.

1.3 REMARQUE. L'homomorphisme canonique $E \otimes_B A_i \to K_i$ induit par $x \otimes y \mapsto \pi_i(x)y$ est clairement un isomorphisme d'algèbres sur E.

1.4 PROPOSITION. *Soit M un B-module de type fini. Les conditions suivantes sont équivalentes :*

(i) M est projectif.

(ii) L'homomorphisme $M \to M \otimes_B E$ induit par $x \mapsto x \otimes 1$ est injectif.

Preuve. Il suffit de vérifier que l'assertion (ii) implique l'assertion (i). Comme A_1 est projectif sur B, l'application $M \otimes_B A_1 \to (M \otimes_B E) \otimes_B A_1$ est injective ; or, par la remarque 1.3, $(M \otimes_B E) \otimes_B A_1 = M \otimes_B (E \otimes_B A_1) = M \otimes_B K_1 = (M \otimes_B A_1) \otimes_A K_1$; ainsi, grâce au théorème 1.1, $M \otimes_B A_1$ est projectif sur A. Il existe alors un A-module N et un entier positif n avec $(M \otimes_B A_1) \oplus N \simeq A_1^n$ comme A-modules et donc aussi en tant que B-modules. On a ainsi un isomorphisme de B-modules $(M \otimes_B A_1) \oplus (N \oplus A_2^n) \simeq A_1^n \oplus A_2^n = B^n$ de sorte que $M \otimes_B A_1$ est B-projectif. On montre de même que $M \otimes_B A_2$ est B-projectif et on conclut en observant que $M = (M \otimes_B A_1) \oplus (M \otimes_B A_2)$. □

1.5 REMARQUE. Soit $\mathfrak{a}$ un sous B-module de E. Alors l'homomorphisme $i : \mathfrak{a} \otimes_B E \to E$ induit par $x \otimes y \mapsto xy$ est injectif. En effet, il suffit de remarquer que tout élément de $\mathfrak{a} \otimes_B E$ peut s'écrire sous la forme $x \otimes y$ avec $y \in E^*$.

1.6 DÉFINITION. On appelle *idéal fractionnaire* de B tout sous B-module $\mathfrak{a}$ de type fini de E tel que $\mathfrak{a} \otimes_B E = E$.

Notons $I(B)$ l'ensemble des idéaux fractionnaires de B. Vu la proposition 1.4, tout idéal fractionnaire de B est projectif.

Soit $\mathfrak{a}$ un sous B-module de E. Pour $1 \leqslant i \leqslant 2$, on a $\mathfrak{a} \otimes_B A_i \subset E \otimes_B A_i = K_i$ et on a $\pi_i(\mathfrak{a}) = \mathfrak{a} \otimes_B A_i$ via ces identifications.

1.7 PROPOSITION. *Soit $\mathfrak{a}$ un sous B-module de type fini de E. Alors les conditions suivantes sont équivalentes :*

(i) $\mathfrak{a}$ est un idéal fractionnaire de B.

(ii) $\mathfrak{a} \otimes_B A_1$ et $\mathfrak{a} \otimes_B A_2$ sont des idéaux fractionnaires de A.

(iii) $\mathfrak{a} \cap E^* \neq \emptyset$.

Preuve. Montrons que l'assertion (i) implique (ii).
Supposons que $\mathfrak{a}$ soit un idéal fractionnaire de B. Soit $1 \leqslant i \leqslant 2$. Alors $\mathfrak{a} \otimes_B A_i$ est un sous A-module de type fini de K tel que $(\mathfrak{a} \otimes_B A_i) \otimes_{A_i} K_i = (\mathfrak{a} \otimes_B E) \otimes_E K_i = = E \otimes_E K_i = K_i$ de sorte que $\mathfrak{a} \otimes_B A_i$ est un idéal fractionnaire de A.

Montrons que (ii) implique (iii).
Supposons que $\mathfrak{a} \otimes_B A_1$ et $\mathfrak{a} \otimes_B A_2$ soient des idéaux fractionnaires de A. Alors, pour tout $1 \leqslant i \leqslant 2$, il existe $x_i \in \mathfrak{a} \otimes_B A_i \subset K_i$ non nul. Considérons $x = x_1 + x_2 \in K_1 \oplus K_2$. Alors $x \in \mathfrak{a} \cap E^*$. En effet, il est clair que $x \in (\mathfrak{a} \otimes_B A_1) \oplus (\mathfrak{a} \otimes_B A_2) = \mathfrak{a}$; de plus, grâce à l'identification $E = K_1 \oplus K_2$, on a $x = (x_1, x_2)$ qui alors est évidemment inversible.
Vérifions finalement que l'assertion (iii) implique l'assertion (i).
Supposons que $\mathfrak{a} \cap E^* \neq \emptyset$. Considérons alors $x \in \mathfrak{a} \cap E^*$. Si $y \in E$, on peut écrire $y = x(x^{-1}y) = x \otimes x^{-1}y \in \mathfrak{a} \otimes_B E$. □

Soient $\mathfrak{a}$, $\mathfrak{b} \in I(B)$. Alors le sous B-module de E engendré par $\{ xy \mid x \in \mathfrak{a},\ y \in \mathfrak{b} \}$ est un idéal fractionnaire de B que l'on note $\mathfrak{a} \cdot \mathfrak{b}$ et que l'on appelle *produit* de $\mathfrak{a}$ et de $\mathfrak{b}$. Il est clair que cette multiplication munit $I(B)$ d'une structure de monoïde commutatif.

1.8 THÉORÈME. *Le monoïde $I(B)$ est un groupe abélien libre de base l'ensemble des idéaux de la forme $A_1 \oplus \mathfrak{p}A_2$ et $\mathfrak{p}A_1 \oplus A_2$ où $\mathfrak{p}$ est un idéal premier non nul de A. De plus, l'application $\Phi : I(B) \to I(A) \times I(A)$ définie par $\Phi(\mathfrak{a}) = (\mathfrak{a} \otimes_B A_1, \mathfrak{a} \otimes_B A_2)$ est un isomorphisme.*

Preuve. En utilisant l'identification de $\mathfrak{a} \otimes_B A_i$ avec $\pi_i(\mathfrak{a})$, on peut aisément vérifier que $(\mathfrak{a} \cdot \mathfrak{b}) \otimes_B A_1 = (\mathfrak{a} \otimes_B A_1) \cdot (\mathfrak{b} \otimes_B A_1)$ pour tout $\mathfrak{a}, \mathfrak{b} \in I(B)$ ce qui montre que Φ est un homomorphisme de monoïdes.
Considérons $\Psi : I(A) \times I(A) \to I(B)$ définie par $\Psi(\mathfrak{a}_1, \mathfrak{a}_2) = \mathfrak{a}_1 A_1 \oplus \mathfrak{a}_2 A_2$. Il est clair que $\Psi \circ \Phi = \mathrm{Id}$ et que $\Phi \circ \Psi = \mathrm{Id}$ donc Φ est une bijection et ainsi un isomorphisme de monoïdes. Finalement $I(B)$ est un groupe abélien libre de base consistant en les idéaux de la forme $A_1 \oplus \mathfrak{p}A_2$ et $\mathfrak{p}A_1 \oplus A_2$ où $\mathfrak{p}$ est un idéal premier non nul de A. □

Le théorème 1.8 nous permet de définir pour tout idéal premier non nul $\mathfrak{p}$ de A une valuation $\mathfrak{p}$-adique :

1.9 DÉFINITION. Soient $\mathfrak{p}$ un idéal premier non nul de A et $\mathfrak{a} \in I(B)$. On appelle *valuation $\mathfrak{p}$-adique* de $\mathfrak{a}$ le couple formé des exposants respectifs de $\mathfrak{p}A_1 \oplus A_2$ et $A_1 \oplus \mathfrak{p}A_2$ dans la décomposition de $\mathfrak{a}$ dans la base décrite dans le théorème 1.8 et on la note $v_{\mathfrak{p}}(\mathfrak{a})$.

Il est clair que $v_{\mathfrak{p}} : I(B) \to \mathbb{Z} \times \mathbb{Z}$ est un homomorphisme surjectif de groupes et que, pour tout $\mathfrak{a} \in I(B)$, on a $v_{\mathfrak{p}}(\mathfrak{a}) = \big(v_{\mathfrak{p}}(\mathfrak{a} \otimes_B A_1), v_{\mathfrak{p}}(\mathfrak{a} \otimes_B A_2)\big)$.

Etudions encore quelques groupes d'homomorphismes.

1.10 PROPOSITION. *Soient V et W deux E-modules. Pour $1 \leqslant i \leqslant 2$, notons $V_i = V \otimes_E K_i$ et $W_i = W \otimes_E K_i$. Alors* $\mathrm{Hom}_E(V, W) = \mathrm{Hom}_K(V_1, W_1) \oplus \mathrm{Hom}_K(V_2, W_2)$.

Preuve. Comme $V = V_1 \oplus V_2$ et $W = W_1 \oplus W_2$, on a $\mathrm{Hom}_E(V, W) = \bigoplus_{1 \leqslant i,j \leqslant 2} \mathrm{Hom}_E(V_i, W_j)$.
Soient $1 \leqslant i, j \leqslant 2$. Calculons $\mathrm{Hom}_E(V_i, W_j)$.
Si $i = j$, alors, V_i et W_i étant des K_i-modules, on a $\mathrm{Hom}_E(V_i, W_i) \subset \mathrm{Hom}_K(V_i, W_i)$, l'inclusion réciproque découlant de la surjectivité de la projection π_i définissant l'action

de E sur K_i. Supposons $i \neq j$. Considérons, par exemple, $f \in \mathrm{Hom}_E(V_1, W_2)$. Soit $x \in V_1$. Alors $f(x) = f((1,0)x) = (1,0)f(x) = (1,0)\big((0,1)f(x)\big) = 0$ de sorte que $f = 0$. □

§ 2. Le théorème des facteurs invariants

Soient A un anneau de Dedekind et K son corps des fractions.
Fixons un K-espace vectoriel V de dimension finie n.

Etudions plus particulièrement les relations entre deux sous-modules projectifs de V. Le résultat fondamental s'appelle le théorème des facteurs invariants. C'est le théorème 81:11 dans [7].

2.1 THÉORÈME. (Théorème des facteurs invariants) *Soient V un K-espace vectoriel de dimension finie n et L et M deux sous A-modules projectifs de V tels que $L \otimes_A K = M \otimes_A K = V$. Alors il existe une base $x_1, \dots, x_n$ de V, des idéaux fractionnaires $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ de A et une suite $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ d'idéaux fractionnaires de A tels que $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n x_n$ et $M = \mathfrak{a}_1\mathfrak{r}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n\mathfrak{r}_n x_n$. De plus, la suite $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ ne dépend que des sous-modules L et M.* □

2.2 DÉFINITION. Reprenons les notations du théorème 2.1. Les idéaux $\mathfrak{r}_1, \dots, \mathfrak{r}_n$ s'appellent les *facteurs invariants* de M dans L.

Nous souhaitons étendre le théorème des facteurs invariants à l'anneau $A \times A$. Notons alors $B = A \times A$ et $E = K \times K$. Nous allons nous ramener au cas ci-dessus.

2.3 THÉORÈME. *Soient V un E-module libre de rang fini n, L et M deux sous B-modules projectifs de type fini de V tels que $L \otimes_B E = M \otimes_B E = V$. Alors il existe une base $x_1, \dots, x_n$ de V et des idéaux fractionnaires $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ de B et une unique suite $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ d'idéaux fractionnaires de B tels que $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n x_n$ et $M = \mathfrak{a}_1\mathfrak{r}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n\mathfrak{r}_n x_n$.*

Preuve. Pour chaque $1 \leqslant i \leqslant 2$, posons $V_i = V \otimes_E K_i$, $L_i = L \otimes_B A_i$ et $M_i = M \otimes_B A_i$. Il est clair que V_i est un K-espace vectoriel de dimension n et que L_i est un A-module projectif. On a $L_i = L \otimes_B A_i \subset V \otimes_B A_i = V \otimes_E (E \otimes_B A_i) = V \otimes_E K_i = V_i$. De plus $L_i \otimes_A K = (L \otimes_B A_i) \otimes_{A_i} K_i = (L \otimes_B E) \otimes_E K_i = V \otimes_E K_i = V_i$. Bien évidemment, M_i a les mêmes propriétés. Vu le théorème 2.1, il existe une base $x_{i,1}, \dots, x_{i,n}$ de V_i et des idéaux fractionnaires $\mathfrak{a}_{i,1}, \dots, \mathfrak{a}_{i,n}$ et $\mathfrak{r}_{i,1} \supset \cdots \supset \mathfrak{r}_{i,n}$ de A tels que $L_i = \mathfrak{a}_{i,1}x_{i,1} \oplus \cdots \oplus \mathfrak{a}_{i,n}x_{i,n}$ et $M_i = \mathfrak{a}_{i,1}\mathfrak{r}_{i,1}x_{i,1} \oplus \cdots \oplus \mathfrak{a}_{i,n}\mathfrak{r}_{i,n}x_{i,n}$.
Mais les K-isomorphismes $K_1 x_{1,j} \oplus K_2 x_{2,j} \to E$ définis par $a\,x_{1,j} + b\,x_{2,j} \mapsto (a,b)$ sont en fait E-linéaires de sorte que $V = V \otimes_E (K_1 \oplus K_2) = (V \otimes_E K_1) \oplus (V \otimes_E K_2) = V_1 \oplus V_2 = K_1 x_{1,1} \oplus \cdots \oplus K_1 x_{1,n} \oplus K_2 x_{2,1} \oplus \cdots \oplus K_2 x_{2,n} \simeq E^n$ comme E-modules.
Grâce aux identifications correspondantes, on obtient les isomorphismes $L = L \otimes_B B = L \otimes_B (A_1 \oplus A_2) = L_1 \oplus L_2 = (\mathfrak{a}_{1,1}x_{1,1} \oplus \cdots \oplus \mathfrak{a}_{1,n}x_{1,n}) \oplus (\mathfrak{a}_{2,1}x_{2,1} \oplus \cdots \oplus \mathfrak{a}_{2,n}x_{2,n}) \simeq (\mathfrak{a}_{1,1}A_1 \oplus \mathfrak{a}_{2,1}A_2) \oplus \cdots \oplus (\mathfrak{a}_{1,n}A_1 \oplus \mathfrak{a}_{2,n}A_2)$ et de même $M = M \otimes_B (A_1 \oplus A_2) = M_1 \oplus M_2 \simeq (\mathfrak{a}_{1,1}A_1 \oplus \mathfrak{a}_{2,1}A_2)(\mathfrak{r}_{1,1}A_1 \oplus \mathfrak{r}_{2,1}A_2) \oplus \cdots \oplus (\mathfrak{a}_{1,n}A_1 \oplus \mathfrak{a}_{2,n}A_2)(\mathfrak{r}_{1,n}A_1 \oplus \mathfrak{r}_{2,n}A_2)$ avec les

inclusions évidentes $\mathfrak{r}_{1,1}A_1 \oplus \mathfrak{r}_{2,1}A_2 \supset \cdots \supset \mathfrak{r}_{1,n}A_1 \oplus \mathfrak{r}_{2,n}A_2$, ce qui montre l'existence de la suite des $\mathfrak{r}_i$.

Prouvons maintenant son unicité. Soient $x_1, \ldots, x_n$ et $x'_1, \ldots, x'_n$ deux E-bases de V, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{a}'_1, \ldots, \mathfrak{a}'_n$ des idéaux fractionnaires de B et $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ et $\mathfrak{r}'_1 \supset \cdots \supset \mathfrak{r}'_n$ deux suites décroissantes d'idéaux fractionnaires de B tels que $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n x_n = \mathfrak{a}'_1 x'_1 \oplus \cdots \oplus \mathfrak{a}'_n x'_n$ et $M = \mathfrak{a}_1\mathfrak{r}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n\mathfrak{r}_n x_n = \mathfrak{a}'_1\mathfrak{r}'_1 x'_1 \oplus \cdots \oplus \mathfrak{a}'_n\mathfrak{r}'_n x'_n$. On voit alors que $L_i = (\mathfrak{a}_1 \otimes_B A_i)\, x_1 \oplus \cdots \oplus (\mathfrak{a}_n \otimes_B A_i)\, x_n$ et $M_i = (\mathfrak{a}_1 \cdot \mathfrak{r}_1 \otimes_B A_i)\, x_1 \oplus \cdots \oplus (\mathfrak{a}_n \cdot \mathfrak{r}_n \otimes_B A_i)\, x_n$. Mais, pour tout $1 \leqslant j \leqslant n$, on a $(\mathfrak{a}_j \cdot \mathfrak{r}_j) \otimes_B A_i = (\mathfrak{a}_j \otimes_B A_i) \cdot (\mathfrak{r}_j \otimes_B A_i)$; de plus il est clair que $\mathfrak{r}_1 \otimes_B A_i \supset \cdots \supset \mathfrak{r}_n \otimes_B A_i$ de sorte qu'en utilisant l'unicité des facteurs invariants de L_i dans M_i, on obtient $\mathfrak{r}_j \otimes_B A_i = \mathfrak{r}'_j \otimes_B A_i$. Ainsi, pour tout $1 \leqslant j \leqslant n$, on a $\mathfrak{r}_j = \mathfrak{r}_j \otimes_B (A_1 \oplus A_2) = (\mathfrak{r}_j \otimes_B A_1) \oplus (\mathfrak{r}_j \otimes_B A_2) = (\mathfrak{r}'_j \otimes_B A_1) \oplus (\mathfrak{r}'_j \otimes_B A_2) = \mathfrak{r}'_j$. □

On peut définir, comme dans le cas d'un anneau de Dedekind, la notion de facteurs invariants :

2.4 DÉFINITION. Reprenons les notations du théorème 2.3. Les idéaux $\mathfrak{r}_1, \ldots, \mathfrak{r}_n$ s'appellent également les *facteurs invariants* de M dans L.

§ 3. Places, complétions et corps de nombres

Dans ce paragraphe, nous ne prouvons aucun résultat et renvoyons le lecteur aux ouvrages de Fröhlich et Taylor [2] (chapitres II.2 , II.3 et III.1) et de O'Meara [4] (chapitres I et II).

Soit K un corps. On appelle *valeur absolue* sur K toute application $\beta : K \to \mathbb{R}$ telle que $\beta(x) > 0$ si $x \neq 0$, $\beta(0) = 0$, $\beta(xy) = \beta(x)\,\beta(y)$ et $\beta(x+y) \leqslant \beta(x) + \beta(y)$ pour tout $x, y \in K$. On dit que la valeur absolue β est *discrète* si $\beta(K^*)$ est un sous groupe discret de $\mathbb{R}^{*2}$. Notons que si β est discrète, on a $\beta(x+y) \leqslant \max\{\beta(x), \beta(y)\}$ pour tout $x, y \in K$.

Deux valeurs absolues β_1 et β_2 sur K sont dites *équivalentes* si elles induisent la même topologie sur K. On appelle *place* de K toute classe d'équivalence de valeurs absolues sur K. Si $\mathfrak{p}$ est une place de K, on a deux possibilités : soit toute valeur absolue de $\mathfrak{p}$ est discrète, soit aucune valeur absolue de $\mathfrak{p}$ ne l'est. Dans le premier cas, on dira que la place $\mathfrak{p}$ est *finie* alors que dans le deuxième cas, on parlera de place *infinie*. Si $\mathfrak{p}$ est une place finie de K et $\beta_1, \beta_2 \in \mathfrak{p}$, alors $\mathfrak{v}_{(\mathfrak{p})} := \{x \in K \mid \beta_1(x) \leqslant 1\} = \{x \in K \mid \beta_2(x) \leqslant 1\}$ est un anneau principal que l'on appelle l'*anneau de valuation* de K en $\mathfrak{p}$. Cet anneau possède un unique idéal premier donné par $\mathfrak{m}_{(\mathfrak{p})} := \{x \in K \mid \beta_1(x) < 1\} = \{x \in K \mid \beta_2(x) < 1\}$. Le quotient $K_{(\mathfrak{p})} = \mathfrak{v}_{(\mathfrak{p})}/\mathfrak{m}_{(\mathfrak{p})}$ s'appelle *le corps résiduel* de K en $\mathfrak{p}$.

On appelle *valuation* sur K toute application $v : K \to \mathbb{Z} \cup \{\infty\}$ telle que $v(xy) = v(x) + v(y)$, $v(x+y) \geqslant \min\{v(x), v(y)\}$ pour tout $x, y \in K$ et $v(x) = \infty$ si et seulement si $x = 0$. Toute valuation v sur K induit une famille de valeurs absolues discrètes équivalentes données par $x \mapsto a^{v(x)}$ pour tout $a \in \mathbb{R}$ avec $0 < a < 1$ et définit donc une place finie que l'on note encore v. La réciproque est également vraie : toute valeur absolue discrète sur K provient d'une valuation sur K.

Soient E/K une extension de corps, $\mathfrak{p}$ une place de K et $\mathfrak{P}$ une place de E. On dit que $\mathfrak{P}$

est *au-dessus* de $\mathfrak{p}$ si la restriction de toute valuation de $\mathfrak{P}$ est une valuation de $\mathfrak{p}$ et l'on note $\mathfrak{P}|\mathfrak{p}$. Dans ce cas $\mathfrak{p}$ est finie si et seulement si $\mathfrak{P}$ est finie.

Soient K un corps et $\mathfrak{p}$ une place de K. Alors il existe une extension K' de K et une place $\mathfrak{p}'$ de K' telle que K est dense dans K' et pour toute valeur absolue $\beta \in \mathfrak{p}'$, on a (K', β) complet et $\beta|_K \in \mathfrak{p}$. De plus, cette extension $(K', \mathfrak{p}')$ est unique à isomorphisme près. On dit que K' est le *complété* de K en $\mathfrak{p}$ et on note $K_\mathfrak{p}$ pour K' et $\mathfrak{p}$ pour $\mathfrak{p}'$. Si $x \in K$, on notera $x_\mathfrak{p}$ l'image de x dans $K_\mathfrak{p}$ par l'inclusion de K dans $K_\mathfrak{p}$.

On appelle *corps local* tout couple $(K, \mathfrak{p})$ formé d'un corps K et d'une place finie $\mathfrak{p}$ de K telle que (K, β) soit complet pour tout $\beta \in \mathfrak{p}$ et dont le corps résiduel est fini. Nous noterons encore $\mathfrak{p}$ l'unique idéal maximal $\mathfrak{m}_{(\mathfrak{p})}$ de l'anneau de valuation $\mathfrak{v}_{(\mathfrak{p})}$ de K. On dit que le corps local $(K, \mathfrak{p})$ est *dyadique* si $2 \in \mathfrak{m}_{(\mathfrak{p})}$ ou, de manière équivalente, si $K_{(\mathfrak{p})}$ est de caractéristique 2 et *non dyadique* dans le cas contraire.

Si K est le corps des fractions d'un anneau de Dedekind A et $\mathfrak{p}$ un idéal premier de A, on identifiera $\mathfrak{p}$ avec la place finie de K induite par la valuation $\mathfrak{p}$-adique.

Soient A un anneau de Dedekind, K son corps des fractions, E une extension quadratique de K et B la clôture intégrale de A dans E.

Soient $\mathfrak{p}$ et $\mathfrak{P}$ des idéaux premiers de K et E respectivement. Alors la place $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$ si et seulement si l'on a l'inclusion des idéaux $\mathfrak{p}B \subset \mathfrak{P}$.

Si $\mathfrak{p}$ est une place de K, alors il existe au moins une place de E au-dessus de $\mathfrak{p}$, mais au plus deux. On dit que la place $\mathfrak{p}$ *se décompose* ou *est décomposée* s'il existe exactement deux places de E au-dessus de $\mathfrak{p}$. Dans le cas contraire, on dit que $\mathfrak{p}$ est *non décomposée.*
Soient $\mathfrak{p}$ une place finie non décomposée de K et $\mathfrak{P}$ l'unique place de E au-dessus de $\mathfrak{p}$. On est dans l'une des deux situations suivantes :

i) On a l'égalité $\mathfrak{p}B = \mathfrak{P}^2$ en tant qu'idéaux. Dans ce cas, on dit que $\mathfrak{p}$ est *ramifiée* dans l'extension E/K.

ii) On a l'égalité $\mathfrak{p}B = \mathfrak{P}$ en tant qu'idéaux. Dans ce cas, on dit que $\mathfrak{p}$ est *inerte* dans l'extension E/K.

On notera $\mathcal{R}$ (resp. $\mathcal{I}$) l'ensemble des places ramifiées (resp. inertes).
Notons $\mathcal{J}$ l'ensemble des places infinies non décomposées de K.

On appelle *corps de nombres* toute extension finie du corps $\mathbb{Q}$ des rationnels.

Soit K un corps de nombres. On appelle *anneau des entiers* de K la clôture intégrale A de $\mathbb{Z}$ dans K. On sait que A est un anneau de Dedekind de corps des fractions K.

On appelle *plongement* de K tout homomorphisme d'anneaux $\mathbb{Q}$-linéaire de K dans $\mathbb{C}$. On dit qu'un plongement f de K est *réel* si $f(K) \subset \mathbb{R}$ et *complexe* dans le cas contraire. Comme l'extension $K/\mathbb{Q}$ est séparable, il y a exactement $n = \dim_\mathbb{Q} K$ plongements de K. De plus, on peut les grouper en r_1 plongements réels $f_1, \ldots, f_{r_1}$ et $2r_2$ plongements complexes $g_1, \sigma \circ g_1, \ldots, g_{r_2}, \sigma \circ g_{r_2}$ où σ est la conjugaison complexe de $\mathbb{C}$. On a alors $n = r_1 + 2r_2$. Les applications $x \mapsto |f_i(x)|$ et $x \mapsto |g_i(x)|$ sont des valeurs absolues et définissent en fait $r_1 + r_2$ places distinctes. D'autre part, tout idéal premier $\mathfrak{p}$ induit une valuation $\mathfrak{p}$-adique et donc une place que l'on notera encore $\mathfrak{p}$. Selon un théorème d'Ostrowski, ces

places sont toutes distinctes et que toute place de K est l'une d'entre elles. Les $r_1 + r_2$ places définies à l'aide des plongements de K sont infinies alors que celles induites par les valuations $\mathfrak{p}$-adiques sont finies.

Soient K un corps de nombres, A son anneau des entiers et $\mathfrak{p}$ une place de K.

Si $\mathfrak{p}$ est finie, on définit l'anneau $A_\mathfrak{p}$ comme l'adhérence de A dans $K_\mathfrak{p}$. Alors $(K_\mathfrak{p}, \mathfrak{p})$ est un corps local d'anneau de valuation $A_\mathfrak{p}$. Le corps $K_\mathfrak{p}$ s'appelle *le corps des nombres $\mathfrak{p}$-adiques* de K et l'anneau $A_\mathfrak{p}$ *l'anneau des entiers $\mathfrak{p}$-adiques* de A. Remarquons que $A_\mathfrak{p}$ est un A-module sans torsion, donc plat.
L'application $\Phi : I(A) \to I(A_\mathfrak{p})$ définie par $\Phi(\mathfrak{a}) = \mathfrak{a} \otimes_A A_\mathfrak{p} = \mathfrak{a}A_\mathfrak{p}$ est un homorphisme surjectif de groupes. De plus $\Phi(\mathfrak{p})$ est l'unique idéal premier de $A_\mathfrak{p}$, noté encore $\mathfrak{p}$, et $\Phi(\mathfrak{q}) = A_\mathfrak{p}$ pour tout idéal premier $\mathfrak{q}$ de A distinct de $\mathfrak{p}$.

Si $\mathfrak{p}$ est infinie, on a $K_\mathfrak{p} \simeq \mathbb{R}$ ou $K_\mathfrak{p} \simeq \mathbb{C}$ selon que la place $\mathfrak{p}$ provienne d'un plongement réel ou complexe. On définira alors $A_\mathfrak{p} = K_\mathfrak{p}$.

Soient ${}^E\!/_K$ une extension quadratique de corps de nombres, A et B les anneaux des entiers respectifs de K et E. Alors B est la clôture intégrale de A dans E. Notons σ l'unique élément non trivial du groupe de Galois de l'extension ${}^E\!/_K$.
Soit $\mathfrak{p}$ une place de K.
On a alors un isomorphisme $\Phi : E \otimes_K K_\mathfrak{p} \to \prod_{\mathfrak{P}|\mathfrak{p}} E_\mathfrak{P}$ induit par $\Phi(x \otimes y) = (x_\mathfrak{P} \cdot y)_\mathfrak{P}$.
Les mêmes phénomèmes se produisent au niveau des anneaux d'entiers. On a le même isomorphisme canonique $\Phi : B \otimes_A A_\mathfrak{p} \to \prod_{\mathfrak{P}|\mathfrak{p}} B_\mathfrak{P}$.

Soit $\mathfrak{p}$ une place de K.

i) Si $\mathfrak{p}$ se décompose et si $\mathfrak{P}_1$ et $\mathfrak{P}_2$ sont les deux places au-dessus de $\mathfrak{p}$, alors $E_{\mathfrak{P}_1} = E_{\mathfrak{P}_2} = K_\mathfrak{p}$, $B_{\mathfrak{P}_1} = B_{\mathfrak{P}_2} = A_\mathfrak{p}$ et donc $E \otimes_K K_\mathfrak{p} = K_\mathfrak{p} \times K_\mathfrak{p}$ et $B \otimes_A A_\mathfrak{p} = A_\mathfrak{p} \times A_\mathfrak{p}$; de plus, avec cette identification, on a $(\sigma \otimes \mathrm{Id})(x, y) = (y, x)$.

ii) Si $\mathfrak{p} \in \mathcal{J}$, on a $K_\mathfrak{p} \simeq \mathbb{R}$ et $E \otimes_K K_\mathfrak{p} \simeq \mathbb{C}$; de plus, avec ces identifications, l'involution $\sigma \otimes \mathrm{Id}$ est la conjugaison complexe.

iii) Si $\mathfrak{p}$ est ramifiée (resp. inerte) et si $\mathfrak{P}$ est l'idéal premier au-dessus de $\mathfrak{p}$, alors la place $\mathfrak{p}A_\mathfrak{p}$ est ramifiée (resp. inerte) dans l'extension quadratique ${}^{E_\mathfrak{P}}\!/_{K_\mathfrak{p}}$ donc $E \otimes_K K_\mathfrak{p} = E_\mathfrak{P}$ et $B \otimes_A A_\mathfrak{p} = B_\mathfrak{P}$; de plus, avec cette identification, $\sigma \otimes \mathrm{Id}$ est l'élément non trivial du groupe de Galois de ${}^{E_\mathfrak{P}}\!/_{K_\mathfrak{p}}$.

Soit $\mathfrak{p}$ un idéal premier non nul de A. Nous sommes alors dans le cadre du paragraphe 1 et nous pouvons considérer l'application $\Psi : I(B) \to I(B \otimes_A A_\mathfrak{p})$ définie par $\Psi(\mathfrak{a}) = \mathfrak{a} \otimes_A A_\mathfrak{p}$. Cette application est un homomorphisme de groupes. Si $\mathfrak{p}$ est décomposé et si $\mathfrak{P}_1$ et $\mathfrak{P}_2$ sont les idéaux premiers de B au-dessus de $\mathfrak{p}$, alors, grâce aux identifications $B \otimes_A A_\mathfrak{p} = B_{\mathfrak{P}_1} \times B_{\mathfrak{P}_2} = A_\mathfrak{p} \times A_\mathfrak{p}$, on a $\Psi(\mathfrak{a}) = \mathfrak{a}B_{\mathfrak{P}_1} \oplus \mathfrak{a}B_{\mathfrak{P}_2}$ et $v_\mathfrak{p}\big(\Psi(\mathfrak{a})\big) = \big(v_{\mathfrak{P}_1}(\mathfrak{a}), v_{\mathfrak{P}_2}(\mathfrak{a})\big)$. Dans le cas contraire, si $\mathfrak{P}$ est l'unique idéal premier au-dessus de $\mathfrak{p}$, alors $\Psi(\mathfrak{a}) = \mathfrak{a}B_\mathfrak{P}$ et ainsi $v_\mathfrak{p}\big(\Psi(\mathfrak{a})\big) = v_\mathfrak{P}(\mathfrak{a})$ en utilisant cette fois l'identification $B \otimes_A A_\mathfrak{p} = B_\mathfrak{P}$.
En particulier, si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux fractionnaires de B avec $\mathfrak{a} \otimes_A A_\mathfrak{p} = \mathfrak{b} \otimes_A A_\mathfrak{p}$ pour toute place finie $\mathfrak{p}$ de K, on a $v_\mathfrak{P}(\mathfrak{a}) = v_\mathfrak{P}(\mathfrak{b})$ pour tout idéal premier non nul $\mathfrak{P}$ de B et donc $\mathfrak{a} = \mathfrak{b}$.

§ 4. Symbole et formule du produit de Hilbert

4.1 DÉFINITION. Soient K un corps et $a, b \in K^*$. On définit le *symbole de* Hilbert $(a,b)_K$ de a et b comme étant un entier égal à $+1$ s'il existe une solution $(x,y) \in K^2$ de l'équation $ax^2 + by^2 = 1$ et égal à -1 sinon.

Remarquons à titre d'exemple que $(a,b)_{\mathbb{C}} = 1$ pour tout $a, b \in \mathbb{C}^*$. Si $a, b \in \mathbb{R}^*$, alors $(a,b)_{\mathbb{R}}$ vaut 1 si $a > 0$ ou $b > 0$; ce même symbole vaut -1 dans les autres cas.

Soit E/K une extension quadratique de corps de caractéristique nulle. Si θ et θ' sont des éléments de K^* tels que $E = K(\sqrt{\theta}) = K(\sqrt{\theta'})$, alors $\frac{\theta}{\theta'}$ est un carré et l'on a ainsi $(a,\theta)_K = (a,\theta')_K$ pour tout $a \in K$. On notera alors $\left(a, E/K\right)$ au lieu de $(a,\theta)_K$.

Etudions le symbole de Hilbert sur des extensions quadratiques E/K de corps complets de caractéristique nulle.

Intéressons-nous tout d'abord à l'extension $\mathbb{C}/\mathbb{R}$. Soit $a \in \mathbb{R}^*$. Il est clair que $\left(a, \mathbb{C}/\mathbb{R}\right)$ est le signe de a. L'application $a \mapsto \left(a, \mathbb{C}/\mathbb{R}\right)$ est ainsi un homomorphisme surjectif de groupes de $\mathbb{R}^*$ sur $\{\pm 1\}$. Son noyau est alors $\mathbb{R}^{*2} = \{a\overline{a} \mid a \in \mathbb{C}^*\}$.

Considérons maintenant un corps local $(K, \mathfrak{p})$ de caractéristique nulle et E une extension quadratique de K. Notons σ l'unique élément non trivial du groupe de Galois de E/K. On a des propriétés analogues que l'on regroupe dans le lemme ci-dessous dont la preuve se trouve dans [7], proposition 63:13.

4.2 LEMME. *L'application $K^* \to \{\pm 1\}$ définie par $a \mapsto \left(a, E/K\right)$ est un homomorphisme surjectif de groupes, dont le noyau est $\{a\,\sigma(a) \mid a \in E^*\}$. En particulier, nous avons $\left|K^*/\{a\,\sigma(a) \mid a \in E^*\}\right| = 2$.* □

Donnons maintenant quelques résultats à propos des liens entre les symboles de Hilbert sur les divers localisés d'un corps de nombres.

Voici la *formule du produit de* Hilbert, aussi connue sous le nom de *loi de réciprocité de* Hilbert. Elle est prouvée dans [7], au chapitre VII.

4.3 THÉORÈME. (Formule du produit de Hilbert) *Considérons un corps de nombres K et $a, b \in K$. Alors $(a_{\mathfrak{p}}, b_{\mathfrak{p}})_{K_{\mathfrak{p}}} = 1$ pour presque toute place $\mathfrak{p}$ de K et*

$$\prod_{\mathfrak{p}} (a_{\mathfrak{p}}, b_{\mathfrak{p}})_{K_{\mathfrak{p}}} = 1.$$ □

Soient E/K une extension de corps de nombres, $\theta \in K$ avec $E = K(\sqrt{\theta})$ et $\mathfrak{p}$ une place de K. On posera $\left(a, E/K\right)_{\mathfrak{p}} = (a_{\mathfrak{p}}, \theta_{\mathfrak{p}})_{K_{\mathfrak{p}}}$ pour tout $a \in K$.
Supposons que $\mathfrak{p}$ est décomposée. Alors $\theta_{\mathfrak{p}}$ est un carré dans $K_{\mathfrak{p}}$. En effet, soit $\mathfrak{P}$ une place de E au-dessus de $\mathfrak{p}$. On a $(\sqrt{\theta})_{\mathfrak{P}}^2 = \theta_{\mathfrak{P}} \in E_{\mathfrak{P}}$ de sorte que $\theta_{\mathfrak{P}}$ est un carré dans $E_{\mathfrak{P}}$. Mais $E_{\mathfrak{P}} = K_{\mathfrak{p}}$ et, par cette identification, $\theta_{\mathfrak{p}} = \theta_{\mathfrak{P}}$ ce qui permet de conclure.

On a ainsi $\left(a, {}^{E}/_{K}\right)_{\mathfrak{p}} = 1$ pour tout $a \in K$.

Supposons $\mathfrak{p}$ non décomposée. Soit $\mathfrak{P}$ l'unique place de E au dessus de $\mathfrak{p}$. Rappelons que $E_{\mathfrak{P}}$ est une extension quadratique de $K_{\mathfrak{p}}$. On vérifie aisément que $E_{\mathfrak{P}} = K_{\mathfrak{p}}(\theta_{\mathfrak{p}})$. On a ainsi $\left(a, {}^{E}/_{K}\right)_{\mathfrak{p}} = \left(a_{\mathfrak{p}}, {}^{E_{\mathfrak{P}}}/_{K_{\mathfrak{p}}}\right)$ pour tout $a \in K$.

La formule du produit de Hilbert peut alors se réécrire ainsi :

4.4 PROPOSITION. *Soient ${}^{E}/_{K}$ une extension quadratique de corps de nombres et $a \in K$. Alors on a $\left(a, {}^{E}/_{K}\right)_{\mathfrak{p}} = 1$ sauf pour un nombre fini de place $\mathfrak{p}$ et*

$$\prod_{\mathfrak{p}} \left(a, {}^{E}/_{K}\right)_{\mathfrak{p}} = 1. \qquad \square$$

Donnons les conditions de réalisations du symbole de Hilbert :

4.5 PROPOSITION. *Soit ${}^{E}/_{K}$ une extension quadratique de corps de nombres. Considérons pour chaque place $\mathfrak{p}$ de K un entier $\lambda_{\mathfrak{p}} \in \{\pm 1\}$. Alors les conditions nécessaires et suffisantes pour qu'il existe $a \in K$ tel que $\left(a, {}^{E}/_{K}\right)_{\mathfrak{p}} = \lambda_{\mathfrak{p}}$ pour toute place $\mathfrak{p}$ sont les suivantes :*

(i) On a $\lambda_{\mathfrak{p}} = 1$ pour toute place décomposée $\mathfrak{p}$.

(ii) L'ensemble des places $\mathfrak{p}$ telles que $\lambda_{\mathfrak{p}} = -1$ est fini.

(iii) On a $\prod_{\mathfrak{p}} \lambda_{\mathfrak{p}} = 1$.

Preuve. La nécessité découle de la proposition 4.4 et des quelques remarques ci-dessus. Prouvons la suffisance. Notons $\mathcal{A}$ l'ensemble des places $\mathfrak{p}$ de K avec $\lambda_{\mathfrak{p}} = -1$. Alors $\mathcal{A}$ est fini et contient un nombre pair d'éléments. D'autre part, tout $\mathfrak{p} \in \mathcal{A}$ est non décomposé de sorte que $\theta_{\mathfrak{p}}$ n'est pas un carré dans $K_{\mathfrak{p}}$. Vu le corollaire 71:19a dans [7], il existe $a \in K$ tel que $\left(a, {}^{E}/_{K}\right)_{\mathfrak{p}} = -1$ si $\mathfrak{p} \in \mathcal{A}$ et $\left(a, {}^{E}/_{K}\right)_{\mathfrak{p}} = 1$ sinon. $\square$

§ 5. Formes et modules hermitiens

Soient $B \subset E$ une extension d'anneaux commutatifs et σ un automorphisme d'anneau involutif de E. Soit K l'anneau fixe de σ, c'est-à-dire le sous-anneau de E défini par $K = \{x \in E \mid \sigma(x) = x\}$. Posons $A = B \cap K$.

5.1 DÉFINITION. Soit M un B-module projectif de type fini.

(i) On appelle *forme hermitienne* sur M dans E toute application $h : M \times M \to E$ telle que $h(x,y) = \sigma\big(h(y,x)\big)$ et telle que $x \mapsto h(x,y)$ soit B-linéaire pour tout $y \in M$ fixé. On dit que le couple (M,h) est un *B-module hermitien dans E.*

(ii) On dit qu'une forme hermitienne h sur M est *non dégénérée* si, $y \in M$ étant fixé, $h(x,y) = 0$ pour tout $x \in M$ n'a lieu que si $y = 0$. Dans ce cas, on dit que (M,h) est un B-module hermitien *non dégénéré* dans E.

Si $B = E$, on omettra de préciser que la forme hermitienne est *dans* E. Si de plus B est un corps, on parle plus volontiers d'*espace hermitien* sur B.

Lorsque l'involution σ est l'identité de E, le terme hermitien est remplacé par celui de *quadratique* et l'on parlera de *forme*, de *module* et d'*espace quadratique*. Le terme hermitien est usuellement réservé au cas où l'isomorphisme σ n'est pas l'identité.

Soit (M, h) un B-module hermitien dans E.

Alors h induit une application A-linéaire $\phi_h : M \to \mathrm{Hom}_B(M, E)$ définie par $\phi_h(x)(y) = h(y, x)$. Il est clair que h est non dégénérée si et seulement si ϕ_h est injective.

Notons $h(M) = \{h(x, x) \mid x \in M\} \subset K$. Un élément $a \in K$ est dit *représenté* par (M, h) si $a \in h(M)$. Le module hermitien (M, h) dans E est dit *universel* si $h(M) = K$ et *isotrope* s'il existe $x \in M$ non nul avec $h(x, x) = 0$.

Supposons (M, h) non dégénéré. Si N est un sous B-module de M et si $h|_{N \times N}$ est non dégénérée, on dit que $(N, h|_{N \times N})$ est un *sous-module hermitien* de (M, h) que l'on note simplement (N, h) ou N.

Deux B-modules hermitiens (M, h) et (N, k) dans E sont dits *isométriques* s'il existe un isomorphisme B-linéaire $f : M \to N$ avec $k\big(f(x), f(y)\big) = h\big(x, y\big)$ pour tout $x, y \in M$ et l'on note $(M, h) \simeq (N, k)$. Un tel f s'appelle une *isométrie* de (M, h) sur (N, k).

Si (N_1, h_1) et (N_2, h_2) sont deux B-modules hermitiens dans E, on définit une forme hermitienne $h_1 \perp h_2$ sur $N_1 \oplus N_2$ dans E par $(x_1 + x_2, y_1 + y_2) \mapsto h_1(x_1, y_1) + h_2(x_2, y_2)$. Il est clair que $h_1 \perp h_2$ est non dégénérée si h_1 et h_2 sont non dégénérées. Le module hermitien $(N_1 \oplus N_2, h_1 \perp h_2)$ s'appelle alors la *somme orthogonale* de (N_1, h_1) et (N_2, h_2) et se note $N_1 \perp N_2$.

Si N_1 et N_2 sont deux sous B-modules hermitiens de (M, h) avec $M = N_1 \oplus N_2$ et $h(N_1, N_2) = 0$, on dit que M se *décompose orthogonalement* en N_1 et N_2. Il est alors clair que l'application de $N_1 \perp N_2$ sur M définie par $(n_1, n_2) \mapsto n_1 + n_2$ est une isométrie et l'on note alors $M = N_1 \perp N_2$.

Soit A' une A-algèbre plate. Posons $B' = B \otimes_A A'$ et $E' = E \otimes_A A'$. Alors σ s'étend en une involution $\sigma \otimes \mathrm{Id}$ de E' que l'on note encore σ. De plus les homomorphismes canoniques $A' \to B' \to E'$ sont injectifs et, grâce aux identifications qui en découlent, on a $A' = \{x \in B' \mid \sigma(x) = x\}$.
Soit (M, h) un B-module hermitien dans E. Alors $M' := M \otimes_A A' = M \otimes_B (B \otimes_A A') = M \otimes_B B'$ est un B'-module projectif et h induit clairement une application A'-bilinéaire $h' : (M \otimes_A A') \times (M \otimes_A A') \to E'$ par $(x \otimes a, y \otimes b) \mapsto h(x, y) \otimes ab$. On vérifie aisément que h' est une forme hermitienne sur M' dans E'. On dit alors que (M', h') est l'extension de (M, h) à B' et l'on note $(M \otimes_B B', h \otimes_B B')$ pour (M', h').
On a évidemment la transitivité de l'extension : si A'' est une A'-algèbre plate, alors A'' est un A-module plat. De plus, si $B'' := B \otimes_A A''$, on a $\big((M \otimes_B B') \otimes_{B'} B'', (h \otimes_B B') \otimes_{B'} B''\big) = (M \otimes_B B'', h \otimes_B B'')$.

5.2 LEMME. *Soient A' une A-algèbre plate et $B' := B \otimes_A A'$. Alors l'extension à B' d'un module hermitien non dégénéré est non dégénérée.*

Preuve. Soit (M,h) un B-module hermitien non dégénéré dans E. Remarquons que B' est un B-module plat et notons (M',h') son extension à B'. Observons ensuite, en utilisant la projectivité de M, que $\phi : \mathrm{Hom}_B(M,E) \otimes_B B' \to \mathrm{Hom}_{B'}(M \otimes_B B', E \otimes_B B')$ défini par $\psi \otimes a \mapsto \big(x \otimes b \mapsto \psi(x) \otimes ab\big)$ est un isomorphisme B'-linéaire. On conclut alors en constatant que $(\phi_h \otimes \mathrm{Id})$ est injective et que $\phi \circ (\phi_h \otimes \mathrm{Id}) = \phi_{h'}$. □

Une matrice $X \in \mathrm{M}_n(E)$ est dite *σ-hermitienne* si $X_{ij} = \sigma(X_{ji})$ pour tout i,j. Notons $\mathrm{Herm}_n(E,\sigma)$ le sous-module des matrices σ-hermitiennes carrées de dimension n.
Soient M un B-module libre et $x_1,\dots,x_n$ une B-base de M.
Alors l'application qui associe à une forme hermitienne h sur M dans E la matrice $\big(h(x_i,x_j)\big)$ est une bijection entre l'ensemble des formes hermitiennes sur M dans E et $\mathrm{Herm}_n(E,\sigma)$. Si $X \in \mathrm{Herm}_n(E,\sigma)$, l'écriture $(M,h) = x_1B \oplus \cdots \oplus x_nB \simeq X$ signifiera que M est un B-module libre de base $x_1,\dots,x_n$ et que h est la forme hermitienne donnée par la matrice X.
La base $x_1,\dots,x_n$ est dite *orthogonale* pour h si la matrice associée est diagonale. On note alors volontiers $M \simeq < h(x_1,x_1) > \perp \cdots \perp < h(x_n,x_n) >$. De plus, elle est dite *orthonormée* si la matrice associée est la matrice unité.

Supposons maintenant que $B = E$ et que A soit un corps de caractéristique nulle. Soit (M,h) un B-espace hermitien libre. Si $x_1,\dots,x_n$ et $y_1,\dots,y_n$ sont deux B-bases de M, alors les déterminants $\det\big(h(x_i,x_j)\big)$ et $\det\big(h(y_i,y_j)\big)$ des matrices associées sont tous les deux nuls ou tous les deux non nuls. Ils sont tous deux non nuls si et seulement si (M,h) est non dégénéré. Si tel est le cas, ils définissent le même élément de $A^*/\{a\,\sigma(a) \mid a \in B^*\}$ que l'on appelle le *discriminant* de (M,h) et que l'on note $\mathrm{d}(M,h)$ ou plus simplement $\mathrm{d}M$. Par abus de notation, $\mathrm{d}M$ désignera aussi n'importe quel élément de A^* dont la réduction modulo $\{a\,\sigma(a) \mid a \in B^*\}$ donne $\mathrm{d}M$ au sens strict.

Supposons que $B = E$ soit un corps de caractéristique nulle. Si N est un sous-espace hermitien d'un espace hermitien non dégénéré (M,h), alors le *complément orthogonal* de N dans M défini par $N^\perp = \{x \in M \mid h(x,N) = 0\}$ est aussi un sous-espace hermitien de V et l'on a $M = N \perp N^\perp$. En particulier, tout espace hermitien admet une base orthogonale.

Supposons que A soit un corps dont $B = E$ est une extension quadratique et notons σ l'unique élément du groupe de Galois de l'extension B/A. Soit (M,h) un espace hermitien de dimension n sur A. Définissons $h' : M \times M \to A$ par $h'(x,y) = \frac{1}{2}\big(h(x,y) + h(y,x)\big)$ pour tout $x,y \in V$. Il est clair que (M,h') est un espace quadratique de dimension $2n$ sur A que l'on appelle l'*espace associé* à (M,h) ou la *trace* de (M,h). On vérifie que $h(M) = h'(M)$. Il est clair que les associés de deux B-espaces hermitiens isométriques sont isométriques.

§ 6. Réseaux et facteurs invariants

Soient A un anneau de Dedekind et K son corps des fractions. Supposons K de caractéristique nulle.
Dans ce paragraphe, on désignera par E une extension quadratique de K ou l'anneau $K \times K$. Dans le premier cas, B sera la clôture intégrale de A dans E et σ l'unique