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 $\{\, x\,y \mid x \in \mathfrak{a},\ y \in \mathfrak{b}\,\}$ 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 $\Phi(\mathfrak{a}) = \big(\mathfrak{a} \otimes_B A_1, \mathfrak{a} \otimes_B A_2\big)$ 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 $\mathbb{R}^{*2} = \{a\bar{a} \mid a \in \mathbb{C}^*\}$.

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

élément non trivial du groupe de Galois de l'extension E/K, alors que dans le deuxième cas B sera l'anneau $A \times A$ et $\sigma(x,y) = (y,x)$. On identifiera alors K (resp. A) avec la diagonale de $K \times K$ (resp. $A \times A$). Observons que $\sigma|_B$ est une involution de B d'anneau fixe A.

6.1 DÉFINITION. On appelle *B-réseau* tout B-module hermitien dans E non dégénéré.

On vérifie aisément que la somme orthogonale de deux B-réseaux est encore un B-réseau.

6.2 DÉFINITION. Soit (L,h) un B-réseau.

(i) On dit que (L,h) est *entier* si $h(L,L) \subset B$.

(ii) On dit que le B-réseau (M,k) est un *sous-réseau* de (L,h) si M est un sous-module de L et si $k = h|_{M\times M}$.

Il est clair que la A-algèbre K est plate car sans torsion. Notons que les homomorphismes canoniques $B \otimes_A K \to E$ et $E \otimes_A K \to E$ sont des isomorphismes ce qui nous permet de considérer l'extension d'un B-réseau à E.

Soit (L,h) un B-réseau. Notons (V,h) son extension à E.
Supposons que E soit un corps. Alors V est clairement libre de type fini sur E. D'autre part, le lemme 5.2 nous dit que (V,h) est non dégénéré de sorte que l'homomorphisme $\phi_h : V \to \mathrm{Hom}_E(V,E)$ est injectif. En comparant les dimensions des E-espaces vectoriels V et $\mathrm{Hom}_E(V,E)$, on montre alors que ϕ_h est un isomorphisme.

Si $E = K \times K$, les mêmes résultats sont vrais, mais nécessitent une preuve. Supposons alors que $E = K \times K$ et reprenons les notations du paragraphe 1.
Commençons par quelques remarques.

Pour tout $1 \leqslant i \leqslant 2$, notons $V_i = V \otimes_E K_i$ et $h_i = \pi_i \circ h$. Considérons $x, y \in V$. Ecrivons $x = x_1 + x_2$ et $y = y_1 + y_2$ avec $x_1, y_1 \in V_1$ et $x_2, y_2 \in V_2$. On a $h(x_1, y_1) = h((1,0)\,x_1, y_1) = h(x_1, (0,1)\,y_1) = h(x_1, 0) = 0$ et de même $h(x_2, y_2) = 0$. D'autre part, $h_1(x_2, y_1) = h_1((0,1)\,x_2, y_1) = \pi_1(0,1) \cdot h_1(x_2, y_1) = 0$ et aussi $h_2(x_1, y_2) = 0$. En résumé, on obtient $h(x,y) = h(x_1,y_1) + h(x_1,y_2) + h(x_2,y_1) + h(x_2,y_2) = \big(h_1(x_1,y_2), h_2(x_2,y_1)\big)$.

6.3 LEMME. *Supposons que $E = K \times K$ et que $B = A \times A$. Soient (L,h) un B-réseau et (V,h) son extension à E. Alors V est un E-module libre de rang fini et l'application K-linéaire $\phi_h : V \to \mathrm{Hom}_E(V,E)$ est un isomorphisme.*

Preuve. Soit $\phi_1 : V_1 \to \mathrm{Hom}_K(V_2, K)$ l'application K-linéaire définie par $\phi_1(x)(y) = h_2(y,x)$. Alors ϕ_1 est injective. En effet, supposons par l'absurde qu'il existe $x \in V_1$ non nul tel que $\phi_1(x) = 0$. Il existe $a \in K$ non nul avec $ax \in L_1$ et l'on a alors $h(y_1 + y_2, ax) = a\,\big(h_1(y_1,0), h_2(y_2,x)\big) = a\,\big(0, \phi_1(x)(y_2)\big) = 0$ pour tout $y_1 \in L_1$ et $y_2 \in L_2$ ce qui contredit la non dégénérescence de h sur L. On montre de même que $\phi_2 : V_2 \to \mathrm{Hom}_K(V_1, K)$ définie par $\phi_2(x)(y) = h_1(y,x)$ est une application K-linéaire injective.

Ainsi $\dim_K V_1 \leqslant \dim_K\big(\mathrm{Hom}_K(V_2,K)\big) = \dim_K V_2 \leqslant \dim_K\big(\mathrm{Hom}_K(V_1,K)\big) = \dim_K V_1$ de sorte que ϕ_1 et ϕ_2 sont des isomorphismes K-linéaires.
Notons $n = \dim_K V_1 = \dim_K V_2$. Alors $V = V_1 \oplus V_2 \simeq K_1^n \oplus K_2^n = (K_1 \oplus K_2)^n = E^n$ comme E-modules, donc V est libre.
D'autre part, on en déduit que $\phi_1 \oplus \phi_2 : V_1 \oplus V_2 \to \mathrm{Hom}_K(V_2,K) \oplus \mathrm{Hom}_K(V_1,K)$ est un isomorphisme K-linéaire. Mais $\phi_1 \oplus \phi_2 = \phi_h$ moyennant l'identification de leurs images $\mathrm{Hom}_K(V_2,K) \oplus \mathrm{Hom}_K(V_1,K) = \mathrm{Hom}_K(V_2,K_2) \oplus \mathrm{Hom}_K(V_1,K_1) = \mathrm{Hom}_E(V,E)$ donnée par la proposition 1.10. Ainsi ϕ_h est un isomorphisme. □

Reprenons le degré de généralité du début du paragraphe.

En regroupant nos résultats, nous avons prouvé :

6.4 COROLLAIRE. *Soient (L,h) un B-réseau et (V,h) son extension à E. Alors V est un E-module libre de rang fini et h est non dégénérée sur V.* □

6.5 DÉFINITION. Soient (L,h) un B-réseau et (V,h) son extension à E. On appelle *discriminant* de (L,h) le discriminant $\mathrm{d}V$ de (V,h) que l'on note $\mathrm{d}L$. On appelle *rang* de (L,h) le rang du E-module libre V et on le note $\mathrm{rang}\,(L,h)$ ou $\mathrm{rang}\,L$.

Intéressons-nous à la réciproque du corollaire 6.4.
Soient (V,h) un E-module hermitien libre et non dégénéré et L un sous-B-module projectif de V tel que $L \otimes_B E = V$. Il est clair que $h|_{L\times L}$ est une forme hermitienne dans E.

6.6 PROPOSITION. *Soient (V,h) un E-module hermitien libre et non dégénéré et L un sous B-module projectif de V tel que $L \otimes_B E = V$. Alors $(L, h|_{L\times L})$ est un B-réseau dont l'extension à E est (V,h).*

Preuve. Il suffit de montrer que $h|_{L\times L}$ est non dégénérée.

Remarquons tout d'abord que, si $x \in V$, il existe $b \in E^*$ avec $bx \in L$. En effet, soit $x \in V$. Comme $V = L \otimes_B E$, il existe $y \in L$ et $b \in E$ avec $x = by$. Ecrivons $b = ca^{-1}$ avec $c \in B$ et $a \in E^*$. On a ainsi $ax = cy \in L$.

Soit $x \in L$. Supposons que $h(x,y) = 0$ pour tout $y \in L$. Soit $z \in V$; considérons $a \in E^*$ avec $az \in L$. On a alors $h(x,z) = \sigma(a)^{-1}h(x,az) = 0$ et donc, vu la non dégénérescence de (V,h), on a $x = 0$. Ainsi $h|_{L\times L}$ est non dégénérée. □

Venons-en à la définition du dual d'un B-réseau.

6.7 DÉFINITION. Soient (L,h) un B-réseau et $V := L \otimes_B E$. On appelle *dual* de L le sous B-module $L^\#$ de V défini par $L^\# = \{x \in V \mid h(x,L) \in B\}$.

Le lemme suivant découle directement des définitions :

6.8 LEMME. *Un B-réseau (L,h) est entier si et seulement si $L \subset L^\#$.* □

Soient (L,h) un B-réseau et (V,h) son extension à E.

Vu le théorème 2.1 et le corollaire 2.3, il existe une E-base $x_1,\dots,x_n$ de V et des idéaux fractionnaires $\mathfrak{a}_1,\dots,\mathfrak{a}_n$ de B tels que $L = \mathfrak{a}_1x_1 \oplus \cdots \oplus \mathfrak{a}_nx_n$. Comme l'application $\phi_h : V \to \mathrm{Hom}_E(V,E)$ est un isomorphisme, il existe une E-base $y_1,\cdots,y_n$ de V duale de la base $x_1,\dots,x_n$ dans le sens où $h(x_i,y_j) = \delta_{ij}$. Soit $x \in V$. Ecrivons $x = \lambda_1y_1+\cdots+\lambda_ny_n$ avec $\lambda_1,\dots,\lambda_n \in E$. On a alors $h(x,L) = \lambda_1\,h(y_1,\mathfrak{a}_1x_1) + \cdots + \lambda_n\,h(y_n,\mathfrak{a}_nx_n) = = \lambda_1\,\sigma(\mathfrak{a}_1) + \cdots + \lambda_n\,\sigma(\mathfrak{a}_n)$ de sorte que $h(x,L) \in B$ si et seulement si l'on a les inclusions $\lambda_1\,\sigma(\mathfrak{a}_1),\dots,\lambda_n\,\sigma(\mathfrak{a}_n) \subset B$. Ainsi $L^\# = \sigma(\mathfrak{a}_1)^{-1}y_1 \oplus \cdots \oplus \sigma(\mathfrak{a}_n)^{-1}y_n$.

En résumé, nous avons prouvé :

6.9 PROPOSITION. *Soient (L,h) un B-réseau et (V,h) son extension à E. Considérons une E-base $x_1,\dots,x_n$ de V et des idéaux fractionnaires $\mathfrak{a}_1,\dots,\mathfrak{a}_n$ de E tels que $L = = \mathfrak{a}_1x_1 \oplus \cdots \oplus \mathfrak{a}_nx_n$. Soit $y_1,\dots,y_n$ la base de V, duale de $x_1,\dots,x_n$ dans le sens où $h(x_i,y_j) = \delta_{ij}$. Alors $L^\# = \sigma(\mathfrak{a}_1)^{-1}y_1 \oplus \cdots \oplus \sigma(\mathfrak{a}_n)^{-1}y_n$. En particulier $L^\#$ est un sous B-module projectif de V tel que $L^\# \otimes_B E = V$ et $(L^\#, h|_{L^\#\times L^\#})$ est un B-réseau dont (V,h) est l'extension à E.* □

6.10 DÉFINITION. Soient (L,h) un B-réseau. On appelle *facteurs invariants* de (L,h) les facteurs invariants de L dans $L^\#$.

Il est clair que deux réseaux isométriques ont mêmes facteurs invariants.

6.11 REMARQUES. La proposition 6.9 nous permet immédiatement de vérifier :

i) Pour tout B-réseau (L,h), on a $(L^\#)^\# = L$.

ii) Soient L et M deux B-réseaux. On a $(L \perp M)^\# = L^\# \perp M^\#$.

iii) Si (L,h) et un B-réseau et $\mathfrak{a}$ est un idéal fractionnaire de B, on a $(\mathfrak{a}L)^\# = \sigma(\mathfrak{a})^{-1}L^\#$.

6.12 DÉFINITION. Soit (L,h) un B-réseau. On dit que (L,h) est *unimodulaire* si ses facteurs invariants sont tous égaux à B.

Remarquons qu'un B-réseau est unimodulaire si et seulement si $L = L^\#$.

Définissons encore quelques invariants d'isométrie des réseaux.

6.13 DÉFINITION. Soit (L,h) un B-réseau dans E. On appelle *échelle* (resp. *norme*) de (L,h) le sous B-module $\mathcal{H}L$ (resp. $\mathcal{N}L$) de E engendré par $h(L,L)$ (resp. $h(L)$).

6.14 LEMME. *Soit (L,h) un B-réseau. Alors $\mathcal{H}L$ et $\mathcal{N}L$ sont des idéaux fractionnaires de B et l'on a $\mathcal{N}L \subset \mathcal{H}L$.*

Preuve. Il est clair que $\mathcal{H}L$ et $\mathcal{N}L$ sont de type fini sur B et que $\mathcal{N}L \subset \mathcal{H}L$.
Remarquons qu'il existe $x \in L$ avec $h(x,x) \neq 0$. En effet, raisonnons par l'absurde. Soient $x, y \in L$; posons $a = h(x,y)$ et considérons $b \in K^*$ avec $ba \in B$. On a alors $a + \sigma(a) = h(x+y, x+y) - h(x,x) - h(y,y) = 0$ et $0 = h(x + ba\,y, x + ba\,y) = 2ba\,\sigma(a)$, de sorte que $h(x,y) = 0$ pour tout $x, y \in L$, ce qui contredit le fait que (L,h) est non dégénérée. Ainsi $h(x,x) \in \mathcal{N}L \cap E^* \subset \mathcal{H}L \cap E^*$ et le résultat découle alors des définitions et de la proposition 1.7. □

§ 7. Localisation de modules hermitiens sur les corps de nombres

Soient K un corps de nombres, A son anneau des entiers, E une extension quadratique de K et B la clôture intégrale de A dans E. On considère l'unique élément non trivial σ du groupe de Galois de l'extension E/K.
Soit $\mathfrak{p}$ une place de K.
Nous souhaitons étendre les modules hermitiens sur E (resp. B) à $E \otimes_K K_\mathfrak{p}$ (resp. $B \otimes_A A_\mathfrak{p}$). Les résultats du paragraphe 3 nous permettent de nous placer dans le cadre du paragraphe 6.
Rappelons que la K-algèbre $K_\mathfrak{p}$ et la A-algèbre $A_\mathfrak{p}$ sont toutes deux plates car sans torsion. Les extensions que l'on souhaite considérer ont alors un sens et nous pouvons définir :

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

(i) Soit (V,h) un espace hermitien sur E. On appelle $\mathfrak{p}$-*localisé* de (V,h) l'extension de (V,h) à $E \otimes_K K_\mathfrak{p}$ que l'on note $(V_\mathfrak{p}, h_\mathfrak{p})$.

(ii) Soit (L,h) un B-réseau. On appelle $\mathfrak{p}$-*localisé* de (L,h) l'extension de (L,h) à $B \otimes_A A_\mathfrak{p}$ que l'on note $(L_\mathfrak{p}, h_\mathfrak{p})$.

Le lemme 5.2 nous permet alors d'énoncer :

7.2 LEMME. *Le $\mathfrak{p}$-localisé d'un espace hermitien non dégénéré sur E est non dégénéré. De même, le $\mathfrak{p}$-localisé d'un B-réseau est un $(B \otimes_A A_\mathfrak{p})$-réseau.* □

Nous sommes en mesure de donner une définition du genre d'un réseau.

7.3 DÉFINITION. Soient (L,h) et (M,k) deux B-réseaux. On dit que (L,h) et (M,k) sont *dans le même genre* si, pour toute place $\mathfrak{p}$ de K, les $\mathfrak{p}$-localisés $(L_\mathfrak{p}, h_\mathfrak{p})$ et $(M_\mathfrak{p}, k_\mathfrak{p})$ sont isométriques.

Il est clair que deux réseaux isométriques sont dans le même genre.

Montrons que deux réseaux dans le même genre ont les mêmes facteurs invariants.
Observons tout d'abord que la localisation commute avec la prise du dual et des facteurs invariants dans le sens où le dual du localisé d'un réseau est le localisé de son dual et les facteurs invariants de son localisé sont les localisés de ses facteurs invariants.

7.4 LEMME. *Soient (L,h) un B-réseau et $\mathfrak{p}$ une place finie de K. Alors $(L^\#)_\mathfrak{p} = (L_\mathfrak{p})^\#$.*

Preuve. Notons (V,h) l'extension de (L,h) à E. Il existe une base $x_1,\dots,x_n$ de V et des idéaux fractionnaires $\mathfrak{a}_1,\dots,\mathfrak{a}_n$ de B tels que $L = \mathfrak{a}_1x_1 \oplus \cdots \oplus \mathfrak{a}_nx_n$. Alors $x_1,\dots,x_n$ est une $(E \otimes_K K_\mathfrak{p})$-base de $V_\mathfrak{p}$ et l'on a $L_\mathfrak{p} = (\mathfrak{a}_1 \otimes_A A_\mathfrak{p})\,x_1 \oplus \cdots \oplus (\mathfrak{a}_n \otimes_A A_\mathfrak{p})\,x_n$.
D'autre part, soit $y_1,\dots,y_n$ la base duale de $x_1,\dots,x_n$. Vu le lemme 6.9, on a $L^\# = \sigma(\mathfrak{a}_1)^{-1}y_1 \oplus \cdots \oplus \sigma(\mathfrak{a}_n)^{-1}y_n$ et donc $(L^\#)_\mathfrak{p} = \big(\sigma(\mathfrak{a}_1)^{-1} \otimes_A A_\mathfrak{p}\big)\,y_1 \oplus \cdots \oplus \big(\sigma(\mathfrak{a}_n)^{-1} \otimes_A A_\mathfrak{p}\big)\,y_n$. Mais il est clair que $y_1,\dots,y_n$ est la $(E \otimes_K K_\mathfrak{p})$-base de $V_\mathfrak{p}$ duale de $x_1,\dots,x_n$ et que $\sigma(\mathfrak{a}_1)^{-1} \otimes_A A_\mathfrak{p} = \sigma(\mathfrak{a}_1 \otimes_A A_\mathfrak{p})^{-1}$. Ainsi $(L^\#)_\mathfrak{p} = (L_\mathfrak{p})^\#$. □

On notera alors volontiers $L^\#_\mathfrak{p}$ pour $(L^\#)_\mathfrak{p} = (L_\mathfrak{p})^\#$.

7.5 PROPOSITION. *Soient $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ les facteurs invariants d'un B-réseau (L,h) et $\mathfrak{p}$ une place finie de K. Alors $\mathfrak{r}_1 \otimes_A A_\mathfrak{p} \supset \cdots \supset \mathfrak{r}_n \otimes_A A_\mathfrak{p}$ sont les facteurs invariants du $\mathfrak{p}$-localisé $(L_\mathfrak{p}, h_\mathfrak{p})$.*

Preuve. Soit (V,h) l'extension de (L,h) à E. Vu le théorème des facteurs invariants, il existe une base $x_1,\dots,x_n$ de V et des idéaux fractionnaires $\mathfrak{a}_1,\dots,\mathfrak{a}_n$ de B tels que $L^\# = \mathfrak{a}_1x_1 \oplus \cdots \oplus \mathfrak{a}_nx_n$ et $L = \mathfrak{a}_1\mathfrak{r}_1x_1 \oplus \cdots \oplus \mathfrak{a}_n\mathfrak{r}_nx_n$. Alors $x_1,\dots,x_n$ est une base de $V_\mathfrak{p}$ sur $(E \otimes_K K_\mathfrak{p})$ et, en localisant, on obtient $(L_\mathfrak{p})^\# = (L^\#)_\mathfrak{p} = (\mathfrak{a}_1 \otimes_A A_\mathfrak{p})\,x_1 \oplus \cdots \oplus (\mathfrak{a}_n \otimes_A A_\mathfrak{p})\,x_n$ et $L_\mathfrak{p} = (\mathfrak{a}_1 \cdot \mathfrak{r}_1 \otimes_A A_\mathfrak{p})\,x_1 \oplus \cdots \oplus (\mathfrak{a}_n \cdot \mathfrak{r}_n \otimes_A A_\mathfrak{p})\,x_n$. On conclut alors en observant que $(\mathfrak{a}_1 \cdot \mathfrak{r}_1) \otimes_A A_\mathfrak{p} = (\mathfrak{a}_1 \otimes_A A_\mathfrak{p}) \cdot (\mathfrak{r}_1 \otimes_A A_\mathfrak{p})$. □

7.6 THÉORÈME. *Deux réseaux dans le même genre ont mêmes facteurs invariants.*

Preuve. Soient (L,h) et (L',h') deux réseaux dans le même genre de facteurs invariants respectifs $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ et $\mathfrak{r}'_1 \supset \cdots \supset \mathfrak{r}'_n$. Alors $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (L'_\mathfrak{p}, h'_\mathfrak{p})$ et donc, vu la proposition 7.5, on a $\mathfrak{r}_i \otimes_A A_\mathfrak{p} = \mathfrak{r}'_i \otimes_A A_\mathfrak{p}$ pour toute place finie $\mathfrak{p}$ de K. Ainsi $\mathfrak{r}_i = \mathfrak{r}'_i$ pour tout $1 \leqslant i \leqslant n$. □

Avant de conclure ce premier chapitre, montrons encore que l'échelle et la norme sont des invariants de genre.

Remarquons à cet effet que l'échelle et la norme du localisé d'un réseau sont respectivement les localisés de son échelle et de sa norme :

7.7 PROPOSITION. *Soient (L,h) un B-réseau et $\mathfrak{p}$ une place finie de K.*
Alors $\mathcal{H}L_\mathfrak{p} = \mathcal{H}L \otimes_A A_\mathfrak{p}$ et $\mathcal{N}L_\mathfrak{p} = \mathcal{N}L \otimes_A A_\mathfrak{p}$.

Preuve. Montrons que $\mathcal{H}L \otimes_A A_\mathfrak{p} = \mathcal{H}L_\mathfrak{p}$.

Si $x,y \in L$, alors $x \otimes 1$ et $y \otimes 1$ sont des éléments de $L_\mathfrak{p} = L \otimes_A A_\mathfrak{p}$ de sorte que, via l'inclusion canonique de B dans $B \otimes_A A_\mathfrak{p}$, on a $h(x,y) = h_\mathfrak{p}(x \otimes 1, y \otimes 1) \in \mathcal{H}L_\mathfrak{p}$. Ainsi $\mathcal{H}L \subset \mathcal{H}L_\mathfrak{p}$ et donc $\mathcal{H}L \otimes_A A_\mathfrak{p} \subset \mathcal{H}L_\mathfrak{p}$.

Réciproquement, si $x \otimes a$ et $y \otimes b$ sont des éléments de $L_\mathfrak{p} = L \otimes_A A_\mathfrak{p}$, on a par définition $h_\mathfrak{p}(x \otimes a, y \otimes b) = h(x,y) \otimes ab \in \mathcal{H}L \otimes_A A_\mathfrak{p}$ de sorte que, comme tout élément de $L_\mathfrak{p}$ est une somme finie d'éléments de la forme $x \otimes a$, on a $\mathcal{H}L_\mathfrak{p} \subset \mathcal{H}L \otimes_A A_\mathfrak{p}$.

On montre de même que $\mathcal{N}L \otimes_A A_\mathfrak{p} = \mathcal{N}L_\mathfrak{p}$. □

7.8 COROLLAIRE. *Deux réseaux dans le même genre ont même norme et échelle.*

Preuve. Soient (L, h) et (M, k) deux B-réseaux dans le même genre. Vu que $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq$ $\simeq (M_\mathfrak{p}, k_\mathfrak{p})$, on a $\mathcal{H}L \otimes_A A_\mathfrak{p} = \mathcal{H}L_\mathfrak{p} = \mathcal{H}M_\mathfrak{p} = \mathcal{H}M \otimes_A A_\mathfrak{p}$ pour toute place finie $\mathfrak{p}$ de K. Ainsi $\mathcal{H}L = \mathcal{H}M$. On obtient de même $\mathcal{N}L = \mathcal{N}M$. □

Nous définirons au chapitre suivant d'autres invariants de genre. Nous observerons en particulier que l'extension au corps des fractions, et par conséquent le discriminant, est un invariant de genre.

Chapitre 2
Equivalence de formes hermitiennes sur les corps de nombres

Le but de ce chapitre est de classifier les formes hermitiennes sur les corps de nombres à l'aide d'un système minimal d'invariants et de montrer l'analogue du théorème de Hasse-Minkowski pour les formes hermitiennes. Nous emploierons une méthode qui consiste à se ramener au cas des formes quadratiques. Notre demarche reprend les idées et la méthode que Landherr a proposées dans son article de 1935 [5].

Considérons une extension quadratique $^E/_K$ de corps de nombres dont les anneaux des entiers respectifs sont B et A et notons σ l'unique élément non trivial du groupe de Galois de $^E/_K$.

Avant d'étudier globalement les espaces hermitiens sur E, commençons par décrire les classes d'isométrie des $\mathfrak{p}$-localisés pour toute place $\mathfrak{p}$ de K. Nous profiterons aussi de donner quelques résultats sur les classes d'isométrie des $\mathfrak{p}$-localisés de B-réseaux, notamment dans le cas où $\mathfrak{p}$ est finie décomposée.

§ 1. Isométrie des $\mathfrak{p}$-localisés : le cas décomposé

Soit $\mathfrak{p}$ une place décomposée de K.
Alors $E \otimes_K K_\mathfrak{p} = K_\mathfrak{p} \times K_\mathfrak{p}$ et $B \otimes_A A_\mathfrak{p} = A_\mathfrak{p} \times A_\mathfrak{p}$; de plus, avec cette identification, on a $(\sigma \otimes \mathrm{Id})(x,y) = (y,x)$. Nous pouvons énoncer :

1.1 PROPOSITION. *Soient K un corps de caractéristique différente de 2, $E := K \times K$ et σ l'involution de E définie par $\sigma(x,y) = (y,x)$. Alors tout module hermitien libre non dégénéré sur E admet une base orthonormée.*

Preuve. Soit (V,h) un espace hermitien libre de rang n sur E.
Supposons que $n = 1$. On a $V = xE$ pour un $x \in V$ et $h(x,x) \neq 0$ car h est non dégénérée. Si l'on note $a := h(x,x) \in K^*$, il est alors clair que $V = (a^{-1},1)xE$ et on a $h\big((a^{-1},1)x, (a^{-1},1)x\big) = (a^{-1},1)(1,a^{-1})h(x,x) = a^{-1}a = 1$.

Généralement, si $n > 1$, considérons une E-base $\{x_1,\dots,x_n\}$ de V ; si $h(x_i,x_i) = 0$ pour tout $1 \leqslant i \leqslant n$, on peut supposer que $a := h(x_1,x_2) \neq 0$ de sorte qu'en remplaçant x_1 par $x_1 + ax_2$ si a est inversible et x_1 par $x_1 + x_2$ sinon, on peut supposer que $h(x_1,x_1) \neq 0$ et donc, comme pour le cas où $n = 1$, que $h(x_1,x_1) = 1$. Considérons $y_i := x_i - h(x_1,x_i)x_1$ pour chaque $2 \leqslant i \leqslant n$ et le sous-module $W := y_2E \oplus \cdots \oplus y_nE$; on vérifie que $V = x_1E \perp W \simeq <1> \perp W$ et on conclut par récurrence. □

La connaissance du $\mathfrak{p}$-localisé d'un espace hermitien en une place décomposée $\mathfrak{p}$ ne nous donne alors aucune information sur l'espace hermitien.

Soit (V,h) est un espace hermitien sur E. De façon générale, grâce au paragraphe 4 du chapitre 1, l'entier $\left(d, {}^{E}\!/_{K}\right)_{\mathfrak{p}}$ ne dépend pas du choix du représentant $d \in K^*$ de $\mathrm{d}V$, ce qui nous permet de le noter $\left(\mathrm{d}V, {}^{E}\!/_{K}\right)_{\mathfrak{p}}$. Dans le cas particulier qui nous intéresse, on a en fait $\left(\mathrm{d}V, {}^{E}\!/_{K}\right)_{\mathfrak{p}} = 1$.

Supposons de plus que la place $\mathfrak{p}$ soit finie et étudions les classes d'isométries de $\mathfrak{p}$-localisés de réseaux.

Modifions les notations jusqu'à la fin du paragraphe ; considérons un anneau principal A de corps des fractions K et posons $E = K \times K$ et $B = A \times A$. On notera σ l'involution de E donnée par $(x,y) \mapsto (y,x)$.

Reprenons les notations des paragraphes 1 et 6 du chapitre 1.

1.2 LEMME. *Soient (L,h) un B-réseau et (V,h) son extension à E. Alors il existe une base orthonormée $z_1,\dots,z_n$ de (V,h) et une suite d'idéaux fractionnaires $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ de A tels que $L = (A_1 \oplus \mathfrak{a}_1 A_2)z_1 \oplus \cdots \oplus (A_1 \oplus \mathfrak{a}_n A_2)z_n$.*

Preuve. Pour $1 \leqslant i \leqslant 2$, notons $L_i = L \otimes_B A_i$ et $V_i = V \otimes_E K_i$. Rappelons que si $x_i, y_i \in V_i$, on a $h(x_1+x_2, y_1+y_2) = \big(h_1(x_1,y_2), h_2(y_1,x_2)\big)$ où $h_i = \pi_i \circ h$. D'autre part, on a montré au début de la preuve du lemme 6.3 du chapitre 1 que l'application K-linéaire $\phi_2 : V_2 \to \mathrm{Hom}_K(V_1,K)$ définie par $\phi_2(x)(y) = h_1(y,x)$ est un isomorphisme.

Soient N_1 un sous A-module de V_1 avec $N_1 \otimes_A K = V_1$, libre de base $x_1,\dots,x_n$ et $N_2 := \{y \in V_2 \mid h_1(N_1,y) \subset A\} \subset V_2$. Comme ϕ_2 est un isomorphisme, il existe une base $y_1,\dots,y_n$ de V_2 avec $h_2(x_i,y_j) = \delta_{ij}$. On vérifie alors aisément que $N_2 = Ay_1 \oplus \cdots \oplus Ay_n$. En particulier $N_2 \otimes_A K = V_2$.

On a les mêmes propriétés si l'on considère un sous A-module Q_2 de V_2 avec $Q_2 \otimes_A K = V_2$ et si l'on définit $Q_1 = \{x \in V_1 \mid h_1(x,Q_2) \subset A\} \subset V_1$. En écrivant Q_1 et Q_2 dans des bases adéquates, il est immédiat que l'on a aussi $Q_2 = \{y \in V_2 \mid h_1(Q_1,y) \subset A\} \subset V_2$.

Posons $M_2 = \{x \in V_2 \mid h_1(L_1,x) \subset A\} \subset V_2$. Alors $M_2 \otimes_A K = V_2$.

Appliquons le théorème des facteurs invariants à L_2 et à M_2. Comme A est principal, il existe une K-base $x_1,\dots,x_n$ de V et une suite d'idéaux fractionnaires $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ de A tels que $L_2 = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n x_n$ et $M_2 = Ax_1 \oplus \cdots \oplus Ax_n$. Il existe une base $y_1,\dots,y_n$ de V_2 telle que $h_1(y_i,x_j) = \delta_{ij}$. Vu les remarques ci-dessus, on a $L_1 = Ay_1 \oplus \cdots \oplus Ay_n$. En posant $z_i = x_i + y_i$, on obtient une E-base $z_1,\dots,z_n$ de V telle que $h(z_i,z_j) = \big(h_1(x_i,y_j), h_2(x_j,y_i)\big) = \big(h_1(x_i,y_j), h_1(y_i,x_j)\big) = \delta_{ij}$. Finalement, on a $L = L_1 \oplus L_2 = (A_1 \oplus \mathfrak{a}_1 A_2)z_1 \oplus \cdots \oplus (A_1 \oplus \mathfrak{a}_n A_2)z_n$. □

Soient (L,h) un B-réseau et (V,h) son extension à E.
Ecrivons $L = \big(A_1 \oplus \mathfrak{a}_1 A_2\big)z_1 \oplus \cdots \oplus \big(A_1 \oplus \mathfrak{a}_n A_2\big)z_n$ pour une E-base orthonormée $z_1,\dots,z_n$ de (V,h) et une suite d'idéaux fractionnaires $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ de A. Il est alors clair que l'on a $L^{\#} = \big(\mathfrak{a}_1{}^{-1} A_1 \oplus A_2\big)z_1 \oplus \cdots \oplus \big(\mathfrak{a}_n{}^{-1} A_1 \oplus A_2\big)z_n$
Ainsi les facteurs invariants de (L,h) sont $\mathfrak{a}_1 A_1 \oplus \mathfrak{a}_1 A_2 \supset \cdots \supset \mathfrak{a}_n A_1 \oplus \mathfrak{a}_n A_2$.
En particulier, la suite $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ est unique.

Nous avons entre autres prouvé :

1.3 COROLLAIRE. *Deux B-réseaux sont isométriques si et seulement s'ils ont les mêmes facteurs invariants.* □

Si X est un ensemble, nous noterons $\Delta(X)$ la diagonale de X, c'est-à-dire le sous-ensemble de $X \times X$ donné par $\{(x,y) \in X \times X \mid x = y\}$.

Le résultat suivant est clair.

1.4 PROPOSITION. Les idéaux fractionnaires $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ de B sont les facteurs invariants d'un B-réseau si et seulement si $v_{\mathfrak{p}}(\mathfrak{r}_i) \in \Delta(\mathbb{Z})$ pour tout $1 \leqslant i \leqslant n$. □

§ 2. Isométrie des $\mathfrak{p}$-localisés : le cas infini non décomposé

Soit $\mathfrak{p}$ une place infinie non décomposée de K. En d'autres termes, on a $\mathfrak{p} \in \mathcal{J}$.
Il s'ensuit alors que $K_{\mathfrak{p}} \simeq \mathbb{R}$, que $E \otimes_K K_{\mathfrak{p}} \simeq \mathbb{C}$ et que $\sigma \otimes \mathrm{Id}$ est transportée par ce dernier isomorphisme sur la conjugaison complexe que l'on notera $x \mapsto \overline{x}$.

Considérons un espace hermitien (V,h) sur $\mathbb{C}$.

Faisons tout d'abord une remarque préliminaire.
Si $x \in V$ est tel que $h(x,x) \neq 0$, alors, comme $\{a\overline{a} \mid a \in \mathbb{C}^*\} = \mathbb{R}^{*2}$, il existe $a \in \mathbb{C}^*$ avec $a\overline{a} = |h(x,x)|$ et donc $h(a^{-1}x, a^{-1}x) = a^{-1}\overline{a^{-1}}h(x,x) = \frac{h(x,x)}{|h(x,x)|} = \pm 1$.
Nous dirons qu'un espace hermitien (V,h) sur $\mathbb{C}$ est *défini positif* (resp. *défini négatif*) si $h(x,x) \in \mathbb{R}^{*2}$ (resp. $h(x,x) \in -\mathbb{R}^{*2}$) pour tout $x \in V \setminus \{0\}$. La remarque préliminaire nous permet facilement de constater que (V,h) est défini positif (resp. défini négatif) si et seulement si $V \simeq < 1 > \perp \cdots \perp < 1 >$ (resp. $V \simeq < -1 > \perp \cdots \perp < -1 >$).

2.1 PROPOSITION. *Si (V,h) est un espace hermitien non dégénéré sur $\mathbb{C}$, alors il existe des sous-espaces V_1 défini positif et V_2 défini négatif avec $V = V_1 \perp V_2$. De plus, les nombres* $\dim_{\mathbb{C}} V_1$ *et* $\dim_{\mathbb{C}} V_2$ *ne dépendent que de (V,h).*

Preuve. La première assertion découle immédiatement de la remarque préliminaire.
Prouvons la seconde. Soient $V = V_1 \perp V_2 = W_1 \perp W_2$ deux décompositions orthogonales de V avec V_1 et W_1 définis positifs et V_2 et W_2 définis négatifs. Comme $\mathbb{R}^{*2} \cap -\mathbb{R}^{*2} = \emptyset$, il suit des définitions que $V_1 \cap W_2 = \{0\}$ et donc que $\dim_{\mathbb{C}} V_1 \leqslant \dim_{\mathbb{C}} W_1$. Par un argument similaire, on obtient $\dim_{\mathbb{C}} W_1 \leqslant \dim_{\mathbb{C}} V_1$. □

2.2 DÉFINITION. Reprenons les notations de la proposition précédente. On appelle *indice positif* de (V,h) (resp. *indice négatif* de (V,h)) l'entier $I^+(V,h)$ (resp. $I^-(V,h)$) défini par $I^+(V,h) := \dim_{\mathbb{C}} V_1$ (resp. $I^-(V,h) := \dim_{\mathbb{C}} V_2$). Le couple $(I^+(V,h), I^-(V,h))$ s'appelle la *signature* de (V,h) et se note $I(V,h)$.

2.3 COROLLAIRE. *Soient (V,h) et (W,k) deux espaces hermitiens sur $\mathbb{C}$. Alors les conditions suivantes sont équivalentes :*

(i) $(V,h) \simeq (W,k)$

(ii) $I(V,h) = I(W,k)$

D'autre part, pour tout couple (a,b) *d'entiers positifs, il existe un espace hermitien* (V,h) *sur* $\mathbb{C}$ *de signature* (a,b). □

Remarquons, en utilisant le paragraphe 4 du chapitre 1, que si (V,h) est un espace hermitien sur $\mathbb{C}$, l'entier $\left(d, {}^{\mathbb{C}}/_{\mathbb{R}}\right)$ ne dépend pas du choix du représentant $d \in K^*$ de $\mathrm{d}V$, ce qui nous permet de le noter $\left(\mathrm{d}V, {}^{\mathbb{C}}/_{\mathbb{R}}\right)$. De plus, on a $\left(\mathrm{d}V, {}^{\mathbb{C}}/_{\mathbb{R}}\right) = (-1)^{I^-(V,h)}$.

Soient (V,h) un espace hermitien sur E. On note volontiers $I_{\mathfrak{p}}(V,h)$ (resp. $I^+_{\mathfrak{p}}(V,h)$ et $I^-_{\mathfrak{p}}(V,h)$) au lieu de $I(V_{\mathfrak{p}}, h_{\mathfrak{p}})$ (resp. $I^+(V_{\mathfrak{p}}, h_{\mathfrak{p}})$ et $I^-(V_{\mathfrak{p}}, h_{\mathfrak{p}})$).

Soient (L,h) un B-réseau et (V,h) son extension à E. Alors, par définition, on a $(L_{\mathfrak{p}}, h_{\mathfrak{p}}) = (V_{\mathfrak{p}}, h_{\mathfrak{p}})$ pour toute place $\mathfrak{p} \in \mathcal{J}$. On définira alors les *signatures* de (L,h) comme étant la famille des signatures des $\mathfrak{p}$-localisés pour tout $\mathfrak{p} \in \mathcal{J}$. Il est clair que les signatures sont des invariants de genres des B-réseaux :

2.4 PROPOSITION. *Deux B-réseaux dans le même genre ont mêmes signatures.* □

Concluons ce paragraphe par une définition :

2.5 DÉFINITION. Nous dirons qu'un espace hermitien ou qu'un réseau est *totalement défini positif* (resp. *totalement défini négatif*) si ses $\mathfrak{p}$-localisés sont définis positifs (resp. négatifs) pour tout $\mathfrak{p} \in \mathcal{J}$.

§ 3. Isométrie des $\mathfrak{p}$-localisés : le cas fini non décomposé

Soit $\mathfrak{p}$ une place de K. Supposons que $\mathfrak{p}$ soit finie non décomposée.
Alors $E \otimes_K K_{\mathfrak{p}} = E_{\mathfrak{P}}$ où $\mathfrak{P}$ est l'unique place de E au dessus de $\mathfrak{p}$. Nous sommes dans le cas où $E_{\mathfrak{P}}$ est une extension quadratique du corps local $K_{\mathfrak{p}}$ et nous pouvons énoncer :

3.1 PROPOSITION. *Soit K un corps local de caractéristique nulle et E une extension quadratique de K. Notons σ l'unique élément non trivial du groupe de Galois de l'extension ${}^{E}/_{K}$. Soit (V,h) un espace hermitien non dégénéré de dimension n sur E. Alors* $V \simeq < 1 > \perp \cdots \perp < 1 > \perp < \mathrm{d}V >$.

Preuve. Procédons par récurrence sur n. Le cas $n = 1$ étant clair, supposons $n > 1$.
Considérons l'espace quadratique (V,h') sur K associé à l'espace (V,h). Rappelons que (V,h') est de dimension $2n$ sur K et que l'on a $h(V) = h'(V)$. Comme un espace quadratique de dimension au moins 4 sur un corps local est universel (cf. [7], 63:18), on a $h(V) = h'(V) = K$ de telle sorte qu'il existe $x \in V$ avec $h(x,x) = 1$. Nous pouvons alors écrire $V = xE \perp (xE)^{\perp} \simeq < 1 > \perp (xE)^{\perp}$. Mais on a $\mathrm{d}V = \mathrm{d}(xE)^{\perp}$ et l'hypothèse de récurrence permet alors de conclure. □

3.2 REMARQUE. Le résultat obtenu ici est beaucoup plus simple que le résultat analogue pour les espaces quadratiques. Cela tient au fait que, pour les espaces quadratiques, les difficultés se concentrent dans les dimensions 2 et 3, car en dimension au moins 4, tout espace est universel. Ce fait nécessite l'introduction d'un invariant supplémentaire appelé le symbole de Hasse (cf. [7], page 167). Cette difficulté disparaît complètement dans le cadre des formes hermitiennes, car un espace hermitien de dimension 2 est déjà universel.

Conservons les notations du théorème. Soit (V,h) un espace hermitien sur E. Vu la proposition 4.2 du chapitre 1, l'entier $\left(d, {}^{E}/_{K}\right)$ ne dépend pas du choix du représentant $d \in K^*$ de $\mathrm{d}V$, ce qui nous permet de le noter $\left(\mathrm{d}V, {}^{E}/_{K}\right)$. Si (W,k) est un autre espace hermitien sur E, alors $\mathrm{d}V = \mathrm{d}W$ si et seulement si $\left(\mathrm{d}V, {}^{E}/_{K}\right) = \left(\mathrm{d}W, {}^{E}/_{K}\right)$.

Nous renvoyons l'étude des localisés des réseaux en les places finies non décomposées au chapitre 3.

§ 4. Le théorème de Hasse-Minkowski pour les formes hermitiennes

Considérons une extension quadratique ${}^{E}/_{K}$ de corps de nombres et notons σ l'unique élément non trivial du groupe de Galois de ${}^{E}/_{K}$.

Enonçons tout d'abord le théorème de Hasse-Minkowski pour les formes quadratiques. Il est prouvé dans [7], théorème 66:4.

4.1 THÉORÈME. (Théorème de Hasse-Minkowski) *Soit K un corps de nombres. Alors deux espaces quadratiques non dégénérés sur K sont isométriques si et seulement si tous leurs localisés sont isométriques.* □

Nous allons en prouver un analogue pour les formes hermitiennes en nous y ramenant.

4.2 THÉORÈME. *Soient (V,h) et (W,k) deux espaces hermitiens non dégénérés sur E. Les conditions suivantes sont équivalentes :*

(i) $(V,h) \simeq (W,k)$

(ii) $(V_{\mathfrak{p}}, h_{\mathfrak{p}}) \simeq (W_{\mathfrak{p}}, k_{\mathfrak{p}})$ *pour toute place* $\mathfrak{p}$ *de* K.

Preuve. Il suffit de prouver que l'assertion (ii) implique l'assertion (i).
Supposons donc que $(V_{\mathfrak{p}}, h_{\mathfrak{p}}) \simeq (W_{\mathfrak{p}}, k_{\mathfrak{p}})$ pour toute place $\mathfrak{p}$ de K.

Remarquons tout d'abord que (V,h) et (W,k) représentent les mêmes éléments, c'est-à-dire que $h(V) = k(W)$. En effet, on a $(V_{\mathfrak{p}}, h'_{\mathfrak{p}}) \simeq (W_{\mathfrak{p}}, k'_{\mathfrak{p}})$ pour toute place $\mathfrak{p}$, donc, grâce au théorème de Hasse-Minkowski, $(V,h') \simeq (W,k')$. En particulier, on a $h'(V) = k'(W)$ et donc $h(V) = h'(V) = k'(W) = k(W)$.

D'autre part, il est clair que l'hypothèse implique que $\dim_E V = \dim_E W$; notons n cet entier et raisonnons par récurrence sur n.

Si $n = 1$, alors la remarque ci-dessus garantit l'existence de $a \in K^*$ représenté par à la fois par (V,h) et (W,k) de sorte que $V \simeq < a > \simeq W$.

Supposons $n > 1$. De manière analogue, on obtient des décompositions $V \simeq < a > \perp \overline{V}$ et $W \simeq < a > \perp \overline{W}$ pour un $a \in K^*$ et des sous-espaces $\overline{V}$ et $\overline{W}$ de V et W respectivement. Il suffit alors de prouver que $(\overline{V}_\mathfrak{p}, h_\mathfrak{p}) \simeq (\overline{W}_\mathfrak{p}, k_\mathfrak{p})$ pour toute place $\mathfrak{p}$ et nous pourrons conclure par récurrence.
Si $\mathfrak{p}$ est décomposée, alors l'assertion est claire grâce à la proposition 1.1.
Supposons que $\mathfrak{p}$ soit finie non décomposée. Alors $a\,\mathrm{d}\overline{V}_\mathfrak{p} = \mathrm{d}V_\mathfrak{p} = \mathrm{d}W_\mathfrak{p} = a\,\mathrm{d}\overline{W}_\mathfrak{p}$, donc $\mathrm{d}\overline{V}_\mathfrak{p} = \mathrm{d}\overline{W}_\mathfrak{p}$ et la proposition 3.1 permet de conclure.
Finalement, supposons $\mathfrak{p}$ infinie non décomposée. Supposons en plus que $a_\mathfrak{p} \in \mathbb{R}^{*2}$, le cas où $a_\mathfrak{p} \in -\mathbb{R}^{*2}$ se traitant de manière analogue. Si $\overline{V}_\mathfrak{p} = V_1 \perp V_2$ et $\overline{W}_\mathfrak{p} = W_1 \perp W_2$ sont des décompositions respectives de $\overline{V}_\mathfrak{p}$ et $\overline{W}_\mathfrak{p}$ avec V_1 et W_1 définis positifs et V_2 et W_2 définis négatifs, alors $< a_\mathfrak{p} > \perp V_1$ et $< a_\mathfrak{p} > \perp W_1$ sont aussi définis positifs et donc $V_\mathfrak{p} \simeq (< a_\mathfrak{p} > \perp V_1) \perp V_2$ et $W_\mathfrak{p} \simeq (< a_\mathfrak{p} > \perp W_1) \perp W_2$ sont aussi de telles décompositions. Par conséquent, $I^-(\overline{V}_\mathfrak{p}, h_\mathfrak{p}) = I^-(V_\mathfrak{p}, h_\mathfrak{p}) = I^-(W_\mathfrak{p}, k_\mathfrak{p}) = I^-(\overline{W}_\mathfrak{p}, k_\mathfrak{p})$ et nous pouvons conclure grâce au corollaire 2.3. □

4.3 REMARQUE. Il est en fait possible de voir ce dernier théorème comme corollaire immédiat du théorème de Hasse-Minkowski, en utilisant le résultat suivant dont la preuve se trouve dans [8], chapitre 10, théorème 1.1 :

Deux espaces hermitiens sur E possédant les mêmes associés (à isométrie près) sont isométriques.

Ce résultat n'est pas tout-à-fait évident. C'est le moyen utilisé par W. Scharlau dans son livre [4] pour ramener la théorie des formes hermitiennes à celle des formes quadratiques. Notre approche a l'avantage d'être un petit peu plus directe dans le cas particulier qui nous intéresse, mais elle a le défaut de cacher un phénomème plus général.

Le théorème de Hasse-Minkowski nous permet de donner d'autres invariants de genre pour les réseaux comme l'extension à E et en particulier le discriminant.
Notons B l'anneau des entiers de E.

4.4 COROLLAIRE. *Soient (L, h) et (M, k) deux B-réseaux dont on note (V, h) et (W, k) les extensions respectives à E. Supposons (L, h) et (M, k) dans le même genre. Alors $(V, h) \simeq (W, k)$. En particulier $\mathrm{d}L = \mathrm{d}M$.*

Preuve. Comme (L, h) et (M, k) sont dans le même genre, on a $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (M_\mathfrak{p}, k_\mathfrak{p})$ donc $(V_\mathfrak{p}, h_\mathfrak{p}) \simeq (W_\mathfrak{p}, k_\mathfrak{p})$ pour toute place $\mathfrak{p}$ de K et par conséquent $(V, h) \simeq (W, k)$. □

§ 5. Un système d'invariants pour les formes hermitiennes

Reprenons les notations du paragraphe 4.

Cherchons maintenant un système d'invariants qui permette de classifier les formes hermitiennes sur E. Il est clair que la dimension, le discriminant et les signatures des $\mathfrak{p}$-localisés pour les $\mathfrak{p} \in \mathcal{J}$ sont des invariants. Supposons que (V, h) et (W, k) soient deux espaces hermitiens de même dimension avec $\mathrm{d}V = \mathrm{d}W$ et $I_\mathfrak{p}(V, h) = I_\mathfrak{p}(W, k)$ pour toute place $\mathfrak{p} \in \mathcal{J}$.

Soit alors $\mathfrak{p}$ une place de K.
Si $\mathfrak{p}$ est décomposée, alors $V_\mathfrak{p} \simeq W_\mathfrak{p}$ grâce à la proposition 1.1.
Comme $\mathrm{d}V_\mathfrak{p} = (\mathrm{d}V)_\mathfrak{p} = (\mathrm{d}W)_\mathfrak{p} = \mathrm{d}W_\mathfrak{p}$, on a $V_\mathfrak{p} \simeq W_\mathfrak{p}$ si $\mathfrak{p}$ est finie non décomposée, par la proposition 3.1.
Finalement, si $\mathfrak{p}$ est infinie non décomposée, la condition $I_\mathfrak{p}(V,h) = I_\mathfrak{p}(W,k)$ nous garantit, par le corollaire 2.3, que $V_\mathfrak{p} \simeq W_\mathfrak{p}$.
En résumé, nous avons montré que $V_\mathfrak{p} \simeq W_\mathfrak{p}$ pour toute place $\mathfrak{p}$ de K.

Grâce au théorème 4.2, nous avons prouvé le théorème de Landherr :

5.1 THÉORÈME. (Théorème de Landherr) *Soient (V,h) et (W,k) deux formes hermitiennes sur E. Alors les conditions suivantes sont équivalentes :*

(i) $(V,h) \simeq (W,k)$

(ii) $\dim_E V = \dim_E W$, $\mathrm{d}V = \mathrm{d}W$ *et* $I_\mathfrak{p}(V,h) = I_\mathfrak{p}(W,k)$ *pour tout* $\mathfrak{p} \in \mathcal{J}$. □

Considérons un espace hermitien (V,h) sur E et ses invariants $\dim_E V$, $\mathrm{d}V$ et $I_\mathfrak{p}(V,h)$ pour les places $\mathfrak{p} \in \mathcal{J}$. Quels sont les relations entre ces derniers ?

Il est clair que, si $\mathfrak{p} \in \mathcal{J}$, alors $V_\mathfrak{p} \simeq <1> \perp \cdots \perp <1> \perp <-1> \perp \cdots \perp <-1>$ avec $\dim_\mathbb{C}(<1> \perp \cdots \perp <1>) = I_\mathfrak{p}^+(V,h)$ et $\dim_\mathbb{C}(<-1> \perp \cdots \perp <-1>) = I_\mathfrak{p}^-(V,h)$ et donc $\mathrm{d}V_\mathfrak{p} = (-1)^{I_\mathfrak{p}^-(V,h)}$. D'autre part, $I_\mathfrak{p}^+(V,h) + I_\mathfrak{p}^-(V,h) = \dim_E V$.

La proposition suivante nous dit que ce sont en fait les seules relations que l'on a en toute généralité :

5.2 PROPOSITION. *Soient n un entier et $d \in K^*$. Considérons pour toute place $\mathfrak{p} \in \mathcal{J}$ un couple $(a_\mathfrak{p}, b_\mathfrak{p})$ d'entiers non négatifs avec $a_\mathfrak{p} + b_\mathfrak{p} = n$ et $d_\mathfrak{p} = (-1)^{b_\mathfrak{p}}$. Alors il existe un espace hermitien (V,h) sur E de dimension n tel que l'on ait $\mathrm{d}V = d$ et $I_\mathfrak{p}(V,h) = (a_\mathfrak{p}, b_\mathfrak{p})$ pour tout $\mathfrak{p} \in \mathcal{J}$.*

Preuve. Nous utiliserons le fait suivant : si P est un ensemble de places infinies réelles et si $f : P \to \{\pm 1\}$ est une application, il existe $x \in K^*$ tel que le signe de $x_\mathfrak{p}$ soit $f(\mathfrak{p})$ pour tout $\mathfrak{p} \in P$. Cela découle directement du théorème d'approximation faible (cf. [2], chapitre 2, théorème 8, p. 66).

Procédons par récurrence sur n.
Si $n = 1$, alors $V := <d>$ répond à la question.
Supposons $n > 1$. Soient $\mathcal{A} := \{\mathfrak{p} \in \mathcal{J} \mid a_\mathfrak{p} = 0\}$ et $\mathcal{B} := \mathcal{J} \setminus \mathcal{A}$. Vu la remarque ci-dessus, il existe $x \in K^*$ tel que $x_\mathfrak{p}$ soit positif (resp. négatif) pour tout $\mathfrak{p} \in \mathcal{B}$ (resp. $\mathfrak{p} \in \mathcal{A}$). Posons $d' = \frac{d}{x}$, $(a'_\mathfrak{p}, b'_\mathfrak{p}) = (a_\mathfrak{p}, b_\mathfrak{p} - 1)$ si $\mathfrak{p} \in \mathcal{A}$ et $(a'_\mathfrak{p}, b'_\mathfrak{p}) = (a_\mathfrak{p} - 1, b_\mathfrak{p})$ si $\mathfrak{p} \in \mathcal{B}$. On vérifie aisément que $d'_\mathfrak{p} = (-1)^{b'_\mathfrak{p}}$ pour tout $\mathfrak{p} \in \mathcal{J}$.
Par hypothèse de récurrence, il existe un espace hermitien (W,k) de dimension $n-1$ avec $\mathrm{d}W = d'$ et $I_\mathfrak{p}(W,k) = (a'_\mathfrak{p}, b'_\mathfrak{p})$ pour tout $\mathfrak{p} \in \mathcal{J}$. L'espace hermitien (V,h) défini par $V = <x> \perp W$ répond à la question. □

5.3 COROLLAIRE. *Soit n un entier strictement positif. Considérons pour toute place $\mathfrak{p}$ de K un module hermitien $(V_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ libre de dimension n sur $E \otimes_K K_\mathfrak{p}$. Alors il existe un*

espace hermitien (V,h) sur E tel que $(V_\mathfrak{p},h_\mathfrak{p}) \simeq (V_{(\mathfrak{p})},h_{(\mathfrak{p})})$ si et seulement si les conditions suivantes sont satisfaites :

(i) L'ensemble des places $\mathfrak{p}$ telles que $\left(\mathrm{d}V_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = -1$ est fini.

(ii) On a $\prod_\mathfrak{p} \left(\mathrm{d}V_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = 1$.

Preuve. Supposons l'existence d'un espace hermitien (V,h) avec $(V_\mathfrak{p},h_\mathfrak{p}) \simeq (V_{(\mathfrak{p})},h_{(\mathfrak{p})})$. En particulier, on a $\left(\mathrm{d}V_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = \left(\mathrm{d}V_\mathfrak{p}, {}^{E}\!/_{K}\right)_\mathfrak{p} = \left(\mathrm{d}V, {}^{E}\!/_{K}\right)_\mathfrak{p}$ et on conclut grâce à la proposition 4.4 du chapitre 1.
Supposons maintenant les assertions (i) et (ii) vérifiées. Vu la proposition 4.5 du chapitre 1, il existe $d \in K^*$ avec $\left(d, {}^{E}\!/_{K}\right)_\mathfrak{p} = \left(\mathrm{d}V_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p}$ pour toute place $\mathfrak{p}$. Grâce à la proposition 5.2, il existe un espace hermitien (V,h) sur E de discriminant d et de signatures $I_\mathfrak{p}(V_{(\mathfrak{p})},h_{(\mathfrak{p})})$ pour tout $\mathfrak{p} \in \mathcal{J}$. En utilisant les propositions 1.1 et 3.1 ainsi que le corollaire 2.3, on conclut que $(V_\mathfrak{p},h_\mathfrak{p}) \simeq (V_{(\mathfrak{p})},h_{(\mathfrak{p})})$ pour toute place $\mathfrak{p}$ de K. □

§ 6. Représentation et isotropie

Dans ce dernier paragraphe, nous conservons les notations du paragraphe 4.

Considérons le problème de la représentabilité d'un espace hermitien par un autre.
Rappelons qu'un espace hermitien (W,k) est dit *représenté* par l'espace hermitien (V,h) s'il existe un homomorphisme E-linéaire $f : W \to V$ avec $h\big(f(x),f(y)\big) = k\big(x,y\big)$ pour tout x, $y \in W$. Comme tous les espaces que nous considérons sont non dégénérés, un tel f ne peut être qu'injectif. Ainsi (W,k) est représenté par (V,h) si et seulement si (W,k) est isométrique à un sous-espace de (V,h). En particulier, si $\dim_E W = \dim_E V$, alors (W,k) est représenté par (V,h) si et seulement si $(W,k) \simeq (V,h)$. Nous nous limiterons donc au cas où $\dim_E W < \dim_E V$.

6.1 PROPOSITION. *Soient (V,h) et (W,k) deux espaces hermitiens de dimensions respectives n et m avec $m < n$. La condition nécessaire et suffisante pour que (W,k) soit représenté par (V,h) est que $I_\mathfrak{p}^+(W,k) \leqslant I_\mathfrak{p}^+(V,h)$ et $I_\mathfrak{p}^-(W,k) \leqslant I_\mathfrak{p}^-(V,h)$ pour tout $\mathfrak{p} \in \mathcal{J}$.*

Preuve. La nécessité est claire.
Prouvons la suffisance. Considérons l'élément $d := \frac{\mathrm{d}V}{\mathrm{d}W} \in K^*$ et pour toute place $\mathfrak{p} \in \mathcal{J}$, le couple $(a_\mathfrak{p},b_\mathfrak{p}) := \big(I_\mathfrak{p}^+(V,h)-I_\mathfrak{p}^+(W,k), I_\mathfrak{p}^-(V,h)-I_\mathfrak{p}^-(W,k)\big)$. Si $\mathfrak{p} \in \mathcal{J}$, on a $a_\mathfrak{p}+b_\mathfrak{p} = n-m$ et $d_\mathfrak{p} = \frac{\mathrm{d}V_\mathfrak{p}}{\mathrm{d}W_\mathfrak{p}} = \frac{(-1)^{I_\mathfrak{p}^-(V,h)}}{(-1)^{I_\mathfrak{p}^-(W,k)}} = (-1)^{b_\mathfrak{p}}$ et donc, grâce à la proposition 5.2, il existe un espace hermitien (U,l) de dimension $n-m$ avec $dU = d$ et $I_\mathfrak{p}(U,l) = (a_\mathfrak{p},b_\mathfrak{p})$ pour toute place $\mathfrak{p} \in \mathcal{J}$. Il est alors clair que $W \perp U$ a les mêmes invariants que V et donc, grâce au théorème 5.1, que $W \perp U \simeq V$. □

Soient (V,h) un espace hermitien sur E et $a \in K^*$. Il est clair que $a \in h(V)$ si et seulement si $< a >$ est représenté par (V,h).

On prouve alors facilement le corollaire suivant :

6.2 COROLLAIRE. *Soient (V,h) un espace hermitien sur E de dimension au moins 2 et $a \in K^*$. Alors $a \in h(V)$ si et seulement si $a_\mathfrak{p} \in h(V_\mathfrak{p})$ pour tout $\mathfrak{p} \in \mathcal{J}$.* □

On appelle *plan hyperbolique* tout espace hermitien sur E isotrope de dimension 2.
Si (H,l) est un plan hyperbolique, on vérifie que $H \simeq < 1 > \perp < -1 >$. En particulier, il n'y en a essentiellement qu'un seul et ses invariants sont $\dim_E H = 2$, $\mathrm{d}H = -1$ et $I^+_\mathfrak{p}(H,l) = I^-_\mathfrak{p}(H,l) = 1$ pour toute place $\mathfrak{p} \in \mathcal{J}$.
Soit (V,h) un espace hermitien sur E. Il est facile de voir que (V,h) est isotrope si et seulement s'il représente un plan hyperbolique.

Compte tenu de ces observations, les conditions d'isotropie s'expriment ainsi :

6.3 COROLLAIRE. *Soit (V,h) un espace hermitien sur E de dimension au moins 3. Alors les conditions suivantes sont équivalentes :*

(i) (V,h) *est isotrope*

(ii) $(V_\mathfrak{p}, h_\mathfrak{p})$ *est isotrope pour tout* $\mathfrak{p} \in \mathcal{J}$

(iii) $I^+_\mathfrak{p}(V,h),\ I^-_\mathfrak{p}(V,h) \geqslant 1$ *pour tout* $\mathfrak{p} \in \mathcal{J}$. □

Chapitre 3
Isométrie de réseaux sur les corps locaux

Le but de ce chapitre est de classifier les réseaux sur les corps locaux et de voir dans quelle mesure les facteurs invariants d'un réseau déterminent sa classe d'isométrie.

Nous exploiterons certains réultats de l'article de Jacobowitz [4] et nous nous contenterons le plus souvent de les citer sans démonstration.

Dans le premier paragraphe, nous introduirons quelques notions au sujet des corps locaux. Dès le deuxième paragraphe, K désignera un corps local d'anneau de valuation A, d'uniformisante π et nous considérerons une extension quadratique $E := K(\sqrt{\theta})$ de K d'anneau de valuation B et d'uniformisante p. Notons σ l'unique élément non trivial du groupe de Galois de l'extension E/K.
Nous supposerons K de caractéristique nulle.

§ 1. Quelques résultats sur les corps locaux

Dans tout le paragraphe, $(K, \mathfrak{p})$ désignera un corps local de caractéristique nulle et A sera son anneau de valuation. Nous noterons v_K la valuation $\mathfrak{p}$-adique de $(K, \mathfrak{p})$.

1.1 DÉFINITION. On appelle *uniformisante* de $(K, \mathfrak{p})$ tout générateur de l'unique idéal premier de A.

Il est clair que $\pi \in K$ est une uniformisante de K si et seulement si $v_K(\pi) = 1$ et que le quotient de deux uniformisantes de K est une unité de A.
D'autre part, les idéaux fractionnaires de A sont tous de la forme $\pi^i A$ avec $i \in \mathbb{Z}$.

Commençons par étudier les unités qui ne sont pas des carrés et introduisons la notion de défaut quadratique qui décrit en quelque sorte l'écart entre une unité et un carré.

1.2 DÉFINITION. Soit $x \in A^*$. On appelle *défaut quadratique* de x l'intersection de tous les idéaux $\mathfrak{a}$ de A tels qu'il existe $y \in A$ avec $x - y^2 \in \mathfrak{a}$.

On peut vérifier que le défaut quadratique de x est le plus petit idéal de A tel que x soit congru à un carré modulo cet idéal.
Le lemme suivant est central dans cette discussion. Il dit en fait que toute unité dont la différence à 1 est suffisamment divisible par π est un carré. Ce lemme, que Jacobowitz appelle le *lemme de Hensel* dans [4], est le théorème 63:1 dans [7] :

1.3 LEMME. *Pour tout $x \in A$, il existe $y \in A$ tel que $1 + 4\pi x = (1 + 2\pi y)^2$.* □

En particulier, une unité $x \in A^*$ est un carré si et seulement si son défaut quadratique est nul.

La propostion suivante est prouvée dans [7], 63:2 :

1.4 PROPOSITION. *Soit $x \in A^*$ de défaut quadratique $\mathfrak{a}$. Supposons que x ne soit pas un carré. Alors $0 \leqslant v_K(\mathfrak{a}) \leqslant v_K(4)$ et de plus l'entier $v_K(\mathfrak{a})$ est impair ou vaut $v_K(4)$.* □

De plus, il existe toujours une unité de défaut quadratique $4A$ (cf. [7], 63:4).

Décrivons maintenant brièvement le comportement d'une extension quadratique de corps locaux. Nous pouvons énoncer :

1.5 THÉORÈME. *Soient E une extension quadratique de K et B la clôture intégrale de A dans E. Alors il existe exactement une place $\mathfrak{P}$ de E au dessus de $\mathfrak{p}$ et $(E, \mathfrak{P})$ est un corps local dont l'anneau de valuation est B.*

Preuve. Un partie de la démonstration se trouve dans [7]. L'existence et l'unicité de la place $\mathfrak{P}$ découle du théorème 14:1 et le fait que $(E, \mathfrak{P})$ soit un corps local de la proposition 32:3. Il reste à prouver que B en est l'anneau de valuation.

Il est clair que B est un anneau de Dedekind. Soit $\mathfrak{Q}$ un idéal premier non nul de B. Alors $\mathfrak{Q} \cap A$ est un idéal premier non nul de A donc $\mathfrak{Q} \cap A = \mathfrak{p}$ et $\mathfrak{p} \subset \mathfrak{Q}$. Ainsi $\mathfrak{Q}$ induit une place de E au-dessus de $\mathfrak{p}$, donc $\mathfrak{Q} = \mathfrak{P}$. On en déduit que $B = \{ x \in K \mid v_{\mathfrak{P}}(x) \geqslant 0 \}$ ce qui montre que B est l'anneau de valuation du corps local $(E, \mathfrak{P})$. □

En particulier, la place $\mathfrak{p}$ est non décomposée ; elle est ainsi ramifiée ou inerte.

Nous dirons que l'extension E/K est *ramifiée* si la place $\mathfrak{p}$ est ramifiée et *non ramifiée* si la place $\mathfrak{p}$ est inerte. Nous dirons que l'extension E/K est *dyadique* si K est un corps local dyadique ou, de manière équivalente, si E est un corps local dyadique.

Soit E/K une extension quadratique de corps locaux. Supposons K et E d'uniformisantes respectives π et p. Il existe $\theta \in K$ avec $E = K(\sqrt{\theta})$; comme θ est défini à un carré près, on peut le choisir unitaire ou de valuation 1.

Il est clair que $v_E(\pi) = 2$ si l'extension E/K est ramifiée et $v_E(\pi) = 1$ si elle est non ramifiée. Soit $x \in K^*$. Ecrivons $x = \pi^k \eta$ avec $k \in \mathbb{Z}$ et $\eta \in A^*$. Alors $v_E(x) = k\, v_E(\pi)$ et $v_K(x) = k\, v_K(\pi)$ de sorte que $v_E(x) = 2\, v_K(x)$ si l'extension est ramifiée et $v_E(x) = v_K(x)$ si elle est non ramifiée.

Supposons que $v_K(\theta) = 1$. Alors $\sqrt{\theta} \in B$ est de valuation strictement positive et ainsi $1 \leqslant v_E(\sqrt{\theta}) = \frac{1}{2} v_E(\theta) \leqslant v_K(\theta) = 1$ de sorte que $\frac{1}{2} v_E(\theta) = v_K(\theta)$ et donc l'extension E/K est ramifiée.

Supposons que $v_K(\theta) = 0$, autrement dit que θ soit une unité. Vu la proposition 63:3 dans [7], l'extension E/K est non ramifiée si et seulement si θ est une unité de défaut

quadratique $4A$. Si l'extension est non dyadique, alors, vu la proposition 1.4, θ ne peut être qu'une unité de défaut quadratique $4A$ et donc l'extension est non ramifiée.
En résumé, nous avons montré :

1.6 PROPOSITION. *Soient K un corps local de caractéristique nulle, A son anneau de valuation et $\theta \in A$ une unité ou une uniformisante telle que $E := K(\sqrt{\theta})$ soit une extension quadratique de K.*

(i) Si E/K est non ramifiée, alors θ est une unité de défaut quadratique $4A$.

(ii) Si E/K est ramifiée non dyadique, alors θ est une uniformisante de K.

(iii) Si E/K est ramifiée dyadique, on a deux possibilités : θ est une uniformisante de K ou θ est une unité de défaut quadratique $\pi^{2k+1}A$ avec $0 < 2k+1 < v_E(4)$. □

§ 2. Modularité et décompositions de Jordan

Le but de ce paragraphe est de définir une classe particulière de réseaux appelés réseaux modulaires qui possèdent des propriétés agréables. Ensuite, nous montrerons comment tout réseau peut s'écrire comme somme orthogonale de réseaux modulaires.

Soit L un B-module projectif de type fini. Comme B est principal, L est libre de rang que l'on notera n.
Si $x \in E \otimes_B L$, il existe $a \in E^*$ avec $ax \in L$ et donc $B_x L := \{a \in E \mid ax \in L\}$ est un idéal fractionnaire non nul de E. Il est clair que $x \in L$ si et seulement si $B_x L \supset B$.
On dit que $x \in L$ est un *vecteur maximal* de L si $B_x L = B$.
Notons que tout vecteur d'une B-base de L est maximal. Si $x \in L$ est un vecteur maximal, alors il existe une B-base $x_1, \ldots, x_n$ de L avec $x = x_1$.

2.1 DÉFINITION. Soient (L, h) un B-réseau et $\mathfrak{a}$ un idéal fractionnaire non nul de E. On dit que (L, h) est $\mathfrak{a}$-*modulaire* si $h(x, L) = \mathfrak{a}$ pour tout vecteur maximal $x \in L$.

Si $\beta \in E^*$, on dit parfois β-modulaire au lieu de βB-modulaire.

2.2 REMARQUES. Soit (L, h) un réseau $\mathfrak{a}$-modulaire.

i) Il est clair que $\mathcal{H}L = \mathfrak{a}$.

ii) Si $\mathfrak{b}$ est un idéal fractionnaire non nul de E, alors $(\mathfrak{b}L, h)$ est un réseau $\mathfrak{b}^2\mathfrak{a}$-modulaire. En effet, écrivons $\mathfrak{b} = \beta B$ pour un $\beta \in E^*$. Alors, tout vecteur maximal y de $\mathfrak{b}L$ s'écrit $y = \beta x$ où x est un vecteur maximal de L et on a $h(y, \mathfrak{b}L) = h(y, \beta L) = = h(\beta x, \beta L) = \beta\sigma(\beta)h(x, L) = \mathfrak{b}^2\mathfrak{a}$.

iii) On a $L^\# = \mathfrak{a}^{-1}L$.
En effet, la relation $h(L, L) \subset \mathfrak{a}$ implique $h(\mathfrak{a}^{-1}L, L) \subset B$ et donc $\mathfrak{a}^{-1}L \subset L^\#$. Réciproquement, si $x \in L^\#$, il existe $\alpha \in E^*$ avec αx vecteur maximal de L. On a alors $\mathfrak{a} = h(\alpha x, L) = \alpha h(x, L) \subset \alpha B$, donc $\alpha^{-1} \in \mathfrak{a}^{-1}$ et ainsi $x = \alpha^{-1}(\alpha x) \in \mathfrak{a}^{-1}L$.

iv) Grâce à ii) et iii) il est clair que $(L^\#, h)$ est $\mathfrak{a}^{-1}$-modulaire.

2.3 REMARQUES. On a également les propriétés suivantes :

i) Soient $(L_1, h_1), (L_2, h_2)$ des B-réseaux $\mathfrak{a}$-modulaires. Notons $h = h_1 \perp h_2$. Alors $(L_1 \perp L_2, h)$ est aussi $\mathfrak{a}$-modulaire.
En effet, soit $x \in L_1 \perp L_2$ un vecteur maximal. On a clairement $h(x, L_1 \perp L_2) \subset \mathfrak{a}$. D'autre part, il existe $y \in L_1$ et $z \in L_2$ avec $x = y + z$. On peut supposer y maximal. Il existe $u \in L_1$ avec $h_1(y,u)B = \mathfrak{a}$. Comme $h(x,u) = h_1(y,u)$, on a $h(x,u)B = \mathfrak{a}$.

ii) Soit (L, h) un B-réseau défini par $L = xB \oplus yB \simeq \begin{pmatrix} \alpha & \beta \\ \sigma(\beta) & \gamma \end{pmatrix}$ avec $v_E(\beta) < v_E(\alpha)$ et $v_E(\beta) < v_E(\gamma)$. Alors (L, h) est β-modulaire.
En effet, soit $z := ax + by$ un vecteur maximal de L. Il est clair que $h(z, L) \subset \beta B$. D'autre part, on peut supposer que a ou b est une unité : supposons par exemple que $a \in B^*$. On a alors $v_E\big(h(ax+by, y)\big) = v_E\big(a\,h(x,y) + b\,h(y,y)\big) = v_E\big(a\beta + b\gamma\big) = v_E(\beta)$ car $v_E(\beta) = v_E(a\beta) < v_E(b\gamma)$ et donc $h(z, L) = \beta B$.

2.4 LEMME. *Soient (L, h) un B-réseau et J un sous-réseau $\mathcal{H}L$-modulaire de L. Alors J est une composante de (L, h).*

Preuve. On a clairement $E \otimes_B L = E \otimes_B J \perp (E \otimes_B J)^\perp$.
Montrons que $L = J \perp (L \cap (E \otimes_B J)^\perp)$.
Il suffit de vérifier que $L \subset J \perp (L \cap (E \otimes_B J)^\perp)$.
Soit $x \in L$. Ecrivons $x = y + z$ avec $y \in E \otimes_B J$ et $z \in (E \otimes_B J)^\perp$. On a alors $h(y, J) = h(x, J) \subset h(L, L) = \mathcal{H}L$ et donc $(\mathcal{H}L)^{-1}y \subset J^\# = (\mathcal{H}L)^{-1}J$ de sorte que $y \in J \subset L$ et que $z = x - y \in L \cap (E \otimes_B J)^\perp$. □

2.5 DÉFINITION. On appelle *triplet de* Jordan tout triplet de la forme (t, r, s) où $t \in \mathbb{N}$, $r := (r_1, \ldots, r_t) \in \mathbb{N}^t$ et $s := (s_1, \ldots, s_t) \in \mathbb{Z}^t$ avec $s_1 < \cdots < s_t$.

2.6 DÉFINITION. Soit (t, r, s) un triplet de Jordan.
Soit (L, h) un B-réseau. On appelle *décomposition de* Jordan *de (L, h) de type (t, r, s)* toute suite $L_1, \ldots, L_t$ de sous-réseaux de L avec $L = L_1 \perp \cdots \perp L_t$ et L_i p^{s_i}-modulaire de rang r_i pour tout $1 \leqslant i \leqslant t$.

Nous allons maintenant montrer que tout réseau admet une décomposition de Jordan. Nous aurons besoin du lemme suivant :

2.7 LEMME. *Soit (L, h) un B-réseau. Alors il existe une composante modulaire J de (L, h) de rang 1 ou 2 telle que $\mathcal{H}J = \mathcal{H}L$ et $\mathcal{N}J = \mathcal{N}L$.*

Preuve. Supposons que $\mathcal{N}L = \mathcal{H}L$. Alors il existe $x \in L$ avec $v_E\big(h(x,x)\big)$ minimal, en d'autres termes avec $h(x,x)B = \mathcal{N}L$. Il est immédiat que $J := xB$ est un réseau modulaire vérifiant $\mathcal{H}J = \mathcal{H}L$ et $\mathcal{N}J = \mathcal{N}L$. On conclut grâce au lemme 2.4.

Supposons que $\mathcal{N}L \neq \mathcal{H}L$. Alors il existe $x, y \in L$ avec $v_E\big(h(x,y)\big)$ minimal, en d'autres termes avec $h(x,y)B = \mathcal{H}L$. Remarquons que $xB + yB$ est un sous-réseau $\mathcal{H}L$-modulaire de L par la remarque 2.3 ii) et donc une composante de L grâce au lemme 2.4.

Si $\mathcal{N}(xB+yB)=\mathcal{N}L$, alors $J:=xB+yB$ répond à la question.
Si $\mathcal{N}(xB+yB)\neq\mathcal{N}L$, alors l'égalité $\mathcal{N}L=\mathcal{N}(xB+yB)+\mathcal{N}(xB+yB)^{\perp}$ montre l'existence de $z\in(xB+yB)^{\perp}$ avec $v_E\big(h(z,z)\big)$ minimal, en d'autres termes avec $h(z,z)B=\mathcal{N}L$.
Ainsi $J:=(x+z)B+yB$ répond à la question. □

Soit (L,h) un B-réseau. Une utilisation récursive du lemme ci-dessus montre que (L,h) s'écrit comme somme orthogonale de plans et droites modulaires dont l'un ou l'une a même norme et échelle que L. En regroupant les termes adéquatement, on obtient, grâce à la remarque 2.3 i), une décomposition de Jordan de (L,h) dont l'une des composantes, en l'occurence la première, a même norme et échelle que L.

En résumé, nous avons prouvé le résultat suivant :

2.8 PROPOSITION. *Soit (L,h) un B-réseau. Alors (L,h) admet une décomposition de Jordan $L_1,\dots,L_t$ avec $\mathcal{H}L_1=\mathcal{H}L$ et $\mathcal{N}L_1=\mathcal{N}L$.* □

Intéressons-nous maintenant au lien entre les facteurs invariants d'un réseau et le type d'une de ses décompositions de Jordan.

Soit (L,h) un B-réseau et $L_1,\dots,L_t$ une décomposition de Jordan de L de type (t,r,s). Alors $L=L_1\perp\cdots\perp L_t$ et donc $L^{\#}=L_1^{\#}\perp\cdots\perp L_t^{\#}=p^{-s_1}L_1\perp\cdots\perp p^{-s_t}L_t$ grâce à la remarque 2.2 iii). Ainsi les facteurs invariants de (L,h) sont

$$p^{s_1}B=\cdots=p^{s_1}B\supset p^{s_2}B=\cdots=p^{s_2}B\supset\cdots\supset p^{s_t}B=\cdots=p^{s_t}B,$$

chaque $p^{s_i}B$ apparaissant r_i fois.

En particulier, grâce à l'unicité des facteurs invariants de (L,h), on en déduit que toutes les décompositions de Jordan d'un réseau sont du même type, ce qui nous permet de définir le *type* d'un B-réseau comme étant le type d'une de ses décompositions de Jordan. Il est clair que deux réseaux isométriques ont le même type.
D'autre part, le calcul ci-dessus nous montre que le type et les facteurs invariants sont essentiellement les mêmes invariants d'isométrie des réseaux :

2.9 PROPOSITION. *Deux B-réseaux ont le même type si et seulement s'ils ont les mêmes facteurs invariants.* □

On observera qu'un réseau est B-modulaire si et seulement s'il est unimodulaire.

Soit (t,r,s) un triplet de Jordan.
Notons $\mathcal{C}(t,r,s)$ l'ensemble des classes d'isométries de réseaux de type (t,r,s).
Si $\lambda\in\{\pm1\}$, notons $\mathcal{C}_\lambda(t,r,s)$ l'ensemble des classes d'isométrie de réseaux de type (t,r,s) et de discriminant d avec $\left(d,{}^{E}/_{K}\right)=\lambda$. Il est clair que $\mathcal{C}(t,r,s)$ est la réunion disjointe de $\mathcal{C}_{-1}(t,r,s)$ et de $\mathcal{C}_{+1}(t,r,s)$.

§ 3. Décompositions de Jordan saturées

Le type d'un réseau est-il un invariant suffisant pour déterminer la classe d'isométrie d'un B-réseau ? Ce n'est pas le cas en toute généralité, les problèmes ne survenant d'ailleurs que si l'extension est ramifiée. Il faut donc essayer de définir d'autres invariants. On souhaiterait choisir la norme des réseaux d'une décomposition de Jordan. Mais il existe des réseaux admettant deux décompositions de Jordan $L_1, \dots, L_t$ et $L'_1, \dots, L'_t$ avec $\mathcal{N}L_i \neq \mathcal{N}L'_i$ pour certains $1 \leqslant i \leqslant t$.
Nous allons éviter cet inconvénient grâce à la notion plus forte de décomposition de Jordan saturée. Nous prouverons que tout réseau possède une décomposition saturée et nous donnerons des conditions nécessaires et suffisantes pour qu'une décomposition de Jordan arbitraire d'un réseau soit saturée.

Soient (L, h) un B-réseau et $\mathfrak{a}$ un idéal fractionnaire non nul de E.
Posons $L^{\mathfrak{a}} = \{x \in L \mid h(x, L) \in \mathfrak{a}\}$. Il est clair que $L^{\mathfrak{a}}$ est un sous-réseau de L tel que $\mathcal{H}L^{\mathfrak{a}} \subset \mathfrak{a}$.

Soient (L_1, h_1) et (L_2, h_2) des B-réseaux.
Si $L_1 \simeq L_2$, alors $L_1^{\mathfrak{a}} \simeq L_2^{\mathfrak{a}}$.
On vérifie aisément que $(L_1 \perp L_2)^{\mathfrak{a}} = L_1^{\mathfrak{a}} \perp L_2^{\mathfrak{a}}$ comme sous-réseaux de $(L_1 \perp L_2, h_1 \perp h_2)$.

Si $s \in \mathbb{Z}$, nous noterons L^s au lieu de $L^{(p^s B)}$.

Supposons que (L, h) soit un réseau $\mathfrak{b}$-modulaire. Si $\mathfrak{b} \subset \mathfrak{a}$, alors $L^{\mathfrak{a}} = L$. Si $\mathfrak{b} \supset \mathfrak{a}$ avec $\mathfrak{b} \neq \mathfrak{a}$, on vérifie que $L^{\mathfrak{a}} = \mathfrak{a}\mathfrak{b}^{-1}L$.

Soient (L, h) un B-réseau, $L_1, \dots, L_t$ une décomposition de Jordan de (L, h) de type (t, r, s) et $1 \leqslant j \leqslant t$. Alors

$$\text{(i)} \quad L^{s_j} = p^{s_j - s_1} L_1 \perp \cdots \perp p^{s_j - s_{j-1}} L_{j-1} \perp L_j \perp \cdots \perp L_t.$$

Il s'ensuit que $\mathcal{N}L_i \subset \mathcal{N}L^{s_i}$ pour tout $1 \leqslant i \leqslant t$ et que $\mathcal{N}L^{s_1} \supset \cdots \supset \mathcal{N}L^{s_t}$.

3.1 DÉFINITION. Considérons un B-réseau (L, h) et $L_1, \dots, L_t$ une décomposition de Jordan de (L, h) de type (t, r, s). On dit que $L_1, \dots, L_t$ est *saturée* si $\mathcal{N}L^{s_i} = \mathcal{N}L_i$ pour tout $1 \leqslant i \leqslant t$.

3.2 THÉORÈME. *Tout B-réseau possède une décomposition de Jordan saturée.*

Preuve. Soit (L, h) un B-réseau. Soit t le nombre de composantes de n'importe quelle décomposition de Jordan de (L, h). Montrons par récurrence sur $1 \leqslant j \leqslant t$ qu'il existe une décomposition de Jordan $L_1, \dots, L_t$ avec $\mathcal{N}L^{s_i} = \mathcal{N}L_i$ pour tout $1 \leqslant i \leqslant j$.

Supposons $j = 1$. Alors on a $L^{s_1} = L$ grâce à la formule (i) et le résultat découle de la proposition 2.8.

Soit $1 < j \leqslant t$. Soit $L_1, \dots, L_t$ une décomposition de Jordan de (L, h) avec $\mathcal{N}L^{s_i} = \mathcal{N}L_i$ pour tout $1 \leqslant i \leqslant j-1$. Il s'agit de trouver une décomposition de Jordan $L'_1, \dots, L'_t$ de (L, h) avec $\mathcal{N}L^{s_i} = \mathcal{N}L'_i$ pour tout $1 \leqslant i \leqslant j$.
Remarquons tout d'abord que la formule (i) implique que $\mathcal{N}(L_j \perp \cdots \perp L_t) \subset \mathcal{N}L^{s_j}$.

Supposons $\mathcal{N}(L_j \perp \cdots \perp L_t) = \mathcal{N}L^{s_j}$. Alors, en vertu de la proposition 2.8, $L_j \perp \cdots \perp L_t$ possède une décomposition de Jordan $J_j, \ldots, J_t$ avec $\mathcal{N}J_j = \mathcal{N}(L_j \perp \cdots \perp L_t)$. Ainsi $L_1, \ldots, L_{j-1}, J_j, \ldots, J_t$ est une décomposition de Jordan de (L, h) avec $\mathcal{N}L^{s_j} = \mathcal{N}J_j$.

Supposons $\mathcal{N}(L_j \perp \cdots \perp L_t) \neq \mathcal{N}L^{s_j}$. Alors, vu la formule (i), il existe $1 \leqslant k \leqslant j-1$ avec $\mathcal{N}L^{s_j} = \mathcal{N}(p^{s_j - s_k}L_k)$. Posons $J = p^{s_j}(L_j \perp L_k)^{\#} = L_j \perp p^{s_j - s_k}L_k$.
Comme $\mathcal{N}L_j \subset \mathcal{N}L^{s_j} = \mathcal{N}(p^{s_j-s_k}L_k)$, on a $\mathcal{N}J = \mathcal{N}L^{s_j}$. Or L_j est p^{s_j}-modulaire et $p^{s_j-s_k}L_k$ est $p^{2s_j-s_k}$-modulaire avec $s_j < 2s_j - s_k$. La proposition 2.8 nous garantit l'existence d'une décomposition de Jordan $J = J_1 \perp J_2$ avec J_1 p^{s_j}-modulaire de norme $\mathcal{N}L^{s_j}$ et J_2 $p^{2s_j-s_k}$-modulaire.
On vérifie que $L_j \perp L_k = (p^{-s_j}J)^{\#} = (p^{-s_j}J_1)^{\#} \perp (p^{-s_j}J_2)^{\#} = J_1 \perp p^{s_k-s_j}J_2$ avec $p^{s_k-s_j}J_2$ p^{s_k}-modulaire. Vu que $\mathcal{N}L_k = \mathcal{N}L^{s_k} \supset \mathcal{N}L^{s_j} \supset \mathcal{N}L_j$, on a $\mathcal{N}L_k = \mathcal{N}(L_j \perp L_k)$. Mais $\mathcal{N}J_1 = \mathcal{N}L^{s_j} = \mathcal{N}(p^{s_j-s_k}L_k) \supsetneq \mathcal{N}L_k = \mathcal{N}(L_j \perp L_k)$ et donc $\mathcal{N}(p^{s_k-s_j}J_2) = \mathcal{N}L_k = \mathcal{N}L^{s_k}$.
Ainsi $L_1, \ldots, L_{k-1}, p^{s_k-s_j}J_2, L_{k+1}, \ldots, L_{j-1}, J_1, L_{j+1}, \ldots, L_t$ est une décomposition de Jordan de (L, h) avec la propriété requise. □

Soient (L, h) un B-réseau et $L_1, \ldots, L_t$ une décomposition de Jordan de (L, h) de type (t, r, s). Posons $n = (n_1, \ldots, n_t)$ avec $n_i = v_E(\mathcal{N}L_i)$ pour tout $1 \leqslant i \leqslant t$. Le quadruplet (t, r, s, n) s'appelle le *type fondamental* de $L_1, \ldots, L_t$.

Le résultat suivant est clair :

3.3 PROPOSITION. *Deux décompositions de Jordan saturées d'un réseau ont même type fondamental.* □

Cette proposition nous permet de définir le *type fondamental* d'un réseau comme étant le type fondamental de n'importe quelle décomposition de Jordan saturée de ce réseau. Il est clair que le type fondamental est un invariant d'isométrie des réseaux.

Soient (L, h) un B-réseau et $L_1, \ldots, L_t$ une décomposition de Jordan de (L, h) de type fondamental (t, r, s, n). Quelles conditions faut-il poser sur les n_i pour que la décomposition soit saturée ? Vu la définition 3.1 et la formule (i), $L_1, \ldots, L_t$ est saturée si et seulement si $\mathcal{N}L_j \subset \mathcal{N}p^{s_j-s_1}L_1, \ldots, \mathcal{N}p^{s_j-s_{j-1}}L_{j-1}\mathcal{N}L_{j+1}\ldots, \mathcal{N}L_t$ pour tout $1 \leqslant j \leqslant t$, c'est-à-dire si et seulement si $n_j \leqslant n_{j+1}, \ldots, n_t$ et $n_j \leqslant 2s_j - 2s_1 + n_1, \ldots, 2s_j - 2s_{j-1} + n_{j-1}$ pour tout $1 \leqslant j \leqslant t$ ou, de manière équivalente, si et seulement si $n_1 \leqslant \cdots \leqslant n_t$ et $n_{j+1} - n_j \leqslant 2s_{j+1} - 2s_j$ pour tout $1 \leqslant j \leqslant t-1$. Ainsi nous avons prouvé :

3.4 PROPOSITION. *Soient (L, h) un B-réseau et $L_1, \ldots, L_t$ une décomposition de Jordan de (L, h) de type fondamental (t, r, s, n).*
Alors $L_1, \ldots, L_t$ est saturée si et seulement si $n_1 \leqslant \cdots \leqslant n_t$ et $n_{j+1} - n_j \leqslant 2s_{j+1} - 2s_j$ pour tout $1 \leqslant j \leqslant t-1$. □

3.5 DÉFINITION. On appelle *quadruplet de* Jordan tout quadruplet (t, r, s, n) où $t \in \mathbb{N}$, $r := (r_1, \ldots, r_t) \in \mathbb{N}^t$, $s := (s_1, \ldots, s_t) \in \mathbb{Z}^t$ et $n := (n_1, \ldots, n_t) \in (2\mathbb{Z})^t$ avec $s_1 < \cdots < s_t$, $n_1 \leqslant \cdots \leqslant n_t$ et $n_{j+1} - n_j \leqslant 2(s_{j+1} - s_j)$ pour tout $1 \leqslant j \leqslant t-1$.

La proposition 3.4 nous dit qu'une décomposition de Jordan est saturée si et seulement si son type fondamental est un quadruplet de Jordan.

Soit (t, r, s, n) un quadruplet de Jordan.
Notons $\mathcal{C}(t, r, s, n)$ l'ensemble des classes d'isométries de réseaux possédant (t, r, s, n) comme type fondamental.
Si $\lambda \in \{\pm 1\}$, notons $\mathcal{C}_\lambda(t, r, s, n)$ l'ensemble des classes d'isométries de réseaux de type fondamental (t, r, s, n) et de discriminant d avec $\left(d, {}^{E}\!/_{K}\right) = \lambda$. Il est clair que $\mathcal{C}(t, r, s, n)$ est la réunion disjointe de $\mathcal{C}_{-1}(t, r, s, n)$ et de $\mathcal{C}_{+1}(t, r, s, n)$.

§ 4. Cas d'une extension non ramifiée

Supposons dans ce paragraphe que l'extension ${}^{E}\!/_{K}$ soit non ramifiée.
Vu la proposition 1.6, θ est une unité de défaut quadratique $4A$ et on a $v_E(\pi) = 1$, ce qui nous permet de supposer que $p = \pi$.
D'autre part, on a $\left(\pi, {}^{E}\!/_{K}\right) = -1$ (cf. [7], 63:3).

Commençons par déterminer la structure des B-réseaux modulaires. Le résultat suivant est prouvé dans [4], paragraphe 7, page 453 :

4.1 PROPOSITION. *Soit (L, h) un réseau p^s-modulaire. Alors $L \simeq < \pi^s > \perp \cdots \perp < \pi^s >$. En particulier, $\mathcal{N}L = \mathcal{H}L$ et $\left(\mathrm{d}L, {}^{E}\!/_{K}\right) = (-1)^{s \cdot \operatorname{rang} L}$.* □

Le critère de la proposition 3.4 montre que toute décomposition de Jordan est saturée.

D'autre part, on en déduit aisément que deux B-réseaux sont équivalents si et seulement s'ils sont du même type.

Le résultat suivant est une conséquence immédiate de la proposition 4.1 :

4.2 THÉORÈME. *Soit (t, r, s) un triplet de Jordan. Alors $\left|\mathcal{C}(t, r, s)\right| = 1$.*
De plus, si $\lambda \in \{\pm 1\}$, alors $\left|\mathcal{C}_\lambda(t, r, s)\right| \leqslant 1$ et on a $\left|\mathcal{C}_\lambda(t, r, s)\right| = 1$ si et seulement si $\lambda = (-1)^{r_1 s_1 + \cdots + r_t s_t}$. □

§ 5. Cas d'une extension ramifiée non dyadique

Supposons dans ce paragraphe que l'extension ${}^{E}\!/_{K}$ soit ramifiée non dyadique.
Vu la proposition 1.6, on a $v_K(\theta) = 1$ et donc $v_E(\sqrt{\theta}) = 1$, ce qui nous permet de supposer que $\pi = \theta$ et que $p = \sqrt{\pi}$.
On a $\left(\pi, {}^{E}\!/_{K}\right) = -1$ car $\pi = -p\,\sigma(p)$. D'autre part, il existe une unité $\Delta \in A^*$ de défaut quadratique $4A$ et l'on a $\left(\Delta, {}^{E}\!/_{K}\right) = -1$ (cf [7] 63:4 et 63:11a). Ainsi 1 et Δ sont des représentants des classes de K^* modulo $\{x\,\sigma(x) \mid x \in E^*\}$.

Commençons par déterminer la structure des B-réseaux modulaires.

Soit $s \in \mathbb{Z}$.

Considérons le B-réseau $(H(s), h)$ défini par $H(s) = xB \oplus yB \simeq \begin{pmatrix} 0 & p^s \\ \sigma(p^s) & 0 \end{pmatrix}$.
On vérifie aisément que $(H(s), h)$ est p^s-modulaire de norme $p^{s+1}B$ et de discriminant $\mathrm{d}H(s) = -1$.

Le résultat suivant est prouvé dans [4], proposition 8.1, page 453 :

5.1 PROPOSITION. *Soit (L, h) un B-réseau p^s-modulaire de rang r.*

(i) Supposons s pair. Il existe $\delta \in A^*$ avec $L \simeq < \pi^{\frac{s}{2}} > \perp \cdots \perp < \pi^{\frac{s}{2}} > \perp < \pi^{\frac{s}{2}} \delta >$. En particulier, $\mathcal{N}L = \mathcal{H}L$ et $\left(\mathrm{d}L, {}^{E}/_{K}\right) = \left(-1, {}^{E}/_{K}\right)^{\frac{rs}{2}} \left(\delta, {}^{E}/_{K}\right)$.

(ii) Supposons s impair. Alors $L \simeq H(s) \perp \cdots \perp H(s)$. En particulier, r est pair, $\mathcal{N}L = p\mathcal{H}L$ et $\left(\mathrm{d}L, {}^{E}/_{K}\right) = \left(-1, {}^{E}/_{K}\right)^{\frac{r}{2}}$. □

Soient $s \in \mathbb{Z}$ et $r \in \mathbb{N}$.

Supposons s pair. Il existe exactement deux B-réseaux p^s-modulaires de rang r à isométrie près, chacun de discriminant différent. En effet, les B-réseaux L_1 et L_2 définis respectivement par $L_1 \simeq < \pi^{\frac{s}{2}} > \perp \cdots \perp < \pi^{\frac{s}{2}} >$ et $L_2 \simeq < \pi^{\frac{s}{2}} > \perp \cdots \perp < \pi^{\frac{s}{2}} > \perp < \pi^{\frac{s}{2}} \Delta >$ sont clairement deux réseaux p^s-modulaires de rang r non isométriques, car de discriminant différent. De plus, la proposition ci-dessus nous dit que tout réseau p^s-modulaire de rang r est isométrique à L_1 ou à L_2.
Si s est impair, il est clair qu'il existe exactement un B-réseau p^s-modulaire de rang r si r est pair, alors qu'il n'en existe aucun si r est impair.
En particulier, deux réseaux p^s-modulaires de rang r sont isométriques si et seulement s'ils ont le même discriminant.

D'autre part, la norme d'un réseau p^s-modulaire est entièrement déterminée par s. En utilisant la proposition 3.4, on voit que toute décomposition de Jordan est saturée.

Soit (t, r, s) un triplet de Jordan. Posons $P(t, r, s) = \{i \in \mathbb{N} \mid 1 \leqslant i \leqslant t \text{ et } s_i \in 2\mathbb{Z}\}$ et $I(t, r, s) = \{i \in \mathbb{N} \mid 1 \leqslant i \leqslant t \text{ et } s_i \notin 2\mathbb{Z}\}$.
Le théorème suivant donne des conditions équivalentes à l'isométrie de réseaux. Il est prouvé dans [4], théorème 8.2, page 454.

5.2 THÉORÈME. *Soient (L, h) et (L', h') des B-réseaux admettant les décompositions de Jordan respectives $L_1, \ldots, L_t$ de type (t, r, s) et $L'_1, \ldots, L'_{t'}$ de type (t', r', s'). Alors les conditions suivantes sont équivalentes :*

(i) (L, h) et (L', h') sont isométriques

(ii) $(t, r, s) = (t', r', s')$ et $\mathrm{d}L_j = \mathrm{d}L'_j$ pour tout $j \in P(t, r, s)$

(iii) $(t, r, s) = (t', r', s')$ et $L_j \simeq L'_j$ pour tout $1 \leqslant j \leqslant t$. □

On peut alors immédiatement calculer le nombre de classes d'isométrie de réseaux d'un type donné.

5.3 COROLLAIRE. *Soit (t, r, s) un triplet de Jordan. Alors :*

(i) On a $C(t, r, s) = \emptyset$ si et seulement s'il existe $j \in I(t, r, s)$ avec r_j impair.

(ii) Si $\mathcal{C}(t,r,s) \neq \emptyset$, *on a* $\left|\mathcal{C}(t,r,s)\right| = 2^{|P(t,r,s)|}$. □

Essayons de déterminer maintenant le nombre de réseaux de type et de discriminant donnés.

5.4 THÉORÈME. *Soient* (t,r,s) *un triplet de Jordan tel que* $\mathcal{C}(t,r,s) \neq \emptyset$ *et* $\lambda \in \{\pm 1\}$.

(i) Si $P(t,r,s) = \emptyset$, *alors* $\left|\mathcal{C}_\lambda(t,r,s)\right| \leqslant 1$ *et on a* $\left|\mathcal{C}_\lambda(t,r,s)\right| = 1$ *si et seulement si* $\lambda = \left(-1, {}^{E}\!/_{K}\right)^{\frac{1}{2}(r_1+\cdots+r_t)}$.

(ii) Si $P(t,r,s) \neq \emptyset$, *alors* $\left|\mathcal{C}_\lambda(t,r,s)\right| = 2^{|P(t,r,s)|-1}$.

Preuve. L'assertion (i) découle de la proposition 5.1.

Prouvons (ii). Fixons $j \in P(t,r,s)$. Posons $t' = t-1$ et définissons $r' \in \mathbb{N}^{t'}$ et $s' \in \mathbb{Z}^{t'}$ par $r' = (r_1, \ldots, r_{j-1}, r_{j+1}, \ldots, r_t)$ et $s' = (s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_t)$.
Comme $\mathcal{C}(t,r,s) \neq \emptyset$, on a $\mathcal{C}(t',r',s') \neq \emptyset$ grâce au corollaire 5.3.

Définissons une application $\Phi : \mathcal{C}_\lambda(t,r,s) \to \mathcal{C}(t',r',s')$ de la manière suivante :
Soit (L,h) un réseau de $\mathcal{C}_\lambda(t,r,s)$. Si $L_1, \ldots, L_t$ une décomposition de Jordan de (L,h), le réseau $L' := L_1 \perp \cdots \perp L_{j-1} \perp L_{j+1} \perp \cdots \perp L_t$ est de type (t',r',s') et sa classe ne dépend que de la classe de L grâce au théorème 5.2. Nous pouvons alors poser $\Phi(L) = L'$.
Montrons que Φ est une bijection.

Soient L et L' deux réseaux de $\mathcal{C}_\lambda(t,r,s)$ avec $\Phi(L) \simeq \Phi(L')$. Soient $L_1, \ldots, L_t$ et $L'_1, \ldots, L'_t$ des décompositions de Jordan respectives de L et L'. On a par définition $L_1 \perp \cdots \perp L_{j-1} \perp L_{j+1} \perp \cdots \perp L_t \simeq L'_1 \perp \cdots \perp L'_{j-1} \perp L'_{j+1} \perp \cdots \perp L'_t$. D'autre part, on a $\left(\mathrm{d}L_j, {}^{E}\!/_{K}\right) = \lambda \cdot \left(\Phi(L), {}^{E}\!/_{K}\right) = \lambda \cdot \left(\Phi(L'), {}^{E}\!/_{K}\right) = \left(\mathrm{d}L'_j, {}^{E}\!/_{K}\right)$. Comme L_j et L'_j sont tous deux p^{s_j}-modulaires de rang r_j, on a $L_j \simeq L'_j$ et donc finalement $L \simeq L'$, ce qui prouve l'injectivité de Φ.

Soit L' un réseau de $\mathcal{C}(t',r',s')$. Comme s_j est pair, il existe un B-réseau p^{s_j}-modulaire J vérifiant $\left(\mathrm{d}J\,\mathrm{d}L', {}^{E}\!/_{K}\right) = \lambda$. Alors $L' \perp J$ est un réseau de $\mathcal{C}_\lambda(t,r,s)$ tel que $\Phi(L' \perp J) \simeq L'$ et ainsi Φ est surjective.

Finalement $\left|\mathcal{C}_\lambda(t,r,s)\right| = \left|\mathcal{C}(t',r',s')\right| = 2^{|P(t',r',s')|} = 2^{|P(t,r,s)|-1}$ par le corollaire 5.3. □

5.5 COROLLAIRE. *Soient* (t,r,s) *un triplet de Jordan et* $\lambda \in \{\pm 1\}$.
Alors $\left|\mathcal{C}_\lambda(t,r,s)\right| \leqslant 2^{\max(0,|P(t,r,s)|-1)}$. □

§ 6. Cas d'une extension ramifiée dyadique : réseaux modulaires

Supposons dans ce paragraphe que l'extension ${}^{E}\!/_{K}$ soit ramifiée dyadique.
On a donc $v_E(\pi) = 2$.
Vu la proposition 1.6, on a essentiellement deux possibilités pour θ :
i) $v_K(\theta) = 1$.
On peut alors supposer que $\pi = \theta$ et que $p = \sqrt{\pi}$. Dans ce cas, on dit que l'extension est *ramifiée première*, en abrégé R-P.

ii) θ est une unité de défaut quadratique $\pi^{2k+1}A$ avec $0 < 2k+1 < v_K(4)$.
Ecrivons alors $\theta = 1 + \pi^{2k+1}\delta$ avec $\delta \in A^*$. On a $\left(\frac{1+\sqrt{\theta}}{\pi^k}\right) \cdot \sigma\left(\frac{1+\sqrt{\theta}}{\pi^k}\right) = \frac{1-\theta}{\pi^{2k}} = -\pi\delta$ de sorte que $v_E\left(\frac{1+\sqrt{\theta}}{\pi^k}\right) = \frac{1}{2}v_E(-\pi\delta) = 1$. On peut alors supposer que $p = \frac{1+\sqrt{\theta}}{\pi^k}$. Dans ce cas, l'extension est *ramifiée k-unitaire*, en abrégé R-U_k.

Remarquons que l'on a $p\,\sigma(p) = -\pi$ dans le cas R-P et $p\,\sigma(p) = -\delta\pi$ dans le cas R-U_k.

Il existe une unité $\Delta \in A^*$ de défaut quadratique $4A$ (cf. [7], 63:4). Ecrivons alors $\Delta = 1 + 4\eta$ avec $\eta \in A^*$. Si l'extension E/K est ramifiée première, on a $\left(\Delta, E/K\right) = -1$ (cf. [7], 63:11a).

Montrons qu'il existe $\omega \in A^*$ tel que $\left(\omega, E/K\right) = -1$. Si l'extension est ramifiée première, on choisira $\omega = \Delta$. Supposons alors l'extension ramifiée unitaire ; il existe un $a \in K$ non nul tel que $\left(a, E/K\right) = -1$. Il suffit alors de choisir $\omega = a\,(p\,\sigma(p))^{-v_K a}$.
Considérons alors une unité ϵ de défaut quadratique maximal parmi les unités qui ne sont pas une norme. Remarquons que si l'extension est ramifiée première, on peut encore choisir $\epsilon = \Delta$ (cf. [7], 63:1).
Ainsi 1 et ϵ sont des représentants des classes de K^* modulo $\{x\,\sigma(x) \mid x \in E^*\}$ et toute unité de défaut quadratique strictement contenu dans celui de ϵ est une norme.

Dans ce paragraphe, nous établirons la structure des réseaux modulaires.

Le théorème suivant est le principal théorème de classification des réseaux modulaires. Il est prouvé dans [4], proposition 10.4, page 460 :

6.1 THÉORÈME. *Soient $s \in \mathbb{Z}$ et (L,h), (L',h') deux réseaux p^s-modulaires.*
Alors $L \simeq L'$ si et seulement si rang L = rang L', $\mathrm{d}L = \mathrm{d}L'$ *et* $\mathcal{N}L = \mathcal{N}L'$. □

Déterminons maintenant les relations entre le rang, le discriminant, l'échelle et la norme d'un réseau modulaire et dressons la liste complète de tous les réseaux modulaires.

Soit $s \in \mathbb{Z}$. Considérons le B-réseau $\big(H(s),h\big)$ défini par

$$H(s) = xB \oplus yB \simeq \begin{pmatrix} 0 & p^s \\ \sigma(p^s) & 0 \end{pmatrix}.$$

On vérifie aisément que $\big(H(s),h\big)$ est p^s-modulaire de discriminant $\mathrm{d}H(s) = -1$. Pour le calcul de sa norme, nous avons besoin d'un résultat technique simple prouvé dans [4] au début du paragraphe 9, page 454 :

6.2 LEMME. *Soient $s \in \mathbb{Z}$ et $x \in p^sB$.*

(i) Dans le cas R-P *:*
Si s est pair, on a $x + \sigma(x) \in 2p^sB$ et $\mathcal{N}H(s) = 2p^sB$.
Si s est impair, on a $x + \sigma(x) \in 2p^{s+1}B$ et $\mathcal{N}H(s) = 2p^{s+1}B$.

(ii) Dans le cas R-U_k *:*
Si s est pair, on a $x + \sigma(x) \in 2p^{s-2k}B$ et $\mathcal{N}H(s) = 2p^{s-2k}B$.
Si s est impair, on a $x + \sigma(x) \in 2p^{s-2k-1}B$ et $\mathcal{N}H(s) = 2p^{s-2k-1}B$. □

Le théorème suivant permet de nous limiter à n'étudier que les réseaux modulaires de rang 1 ou 2. C'est la proposition 9.3 de la page 457 dans [4].

6.3 THÉORÈME. *Soient $s \in \mathbb{Z}$ et (L,h) un réseau p^s-modulaire.*
Alors il existe un sous-réseau p^s-modulaire J de L de rang 1 ou 2 et de même norme que (L,h) tel que $L \simeq J \perp H(s) \perp \cdots \perp H(s)$. □

6.4 REMARQUE. Le théorème 6.3 peut être vu comme corollaire immédiat du théorème de classification 6.1. Cependant, il permet de ramener la preuve du théorème 6.1 aux cas de réseaux de rang 1 ou 2. C'est d'ailleurs la méthode utilisée par R. Jacobowitz dans son article [4]. Il n'est alors possible d'adopter le point de vue ci-dessus que si l'on dispose d'une preuve directe du théorème de classification 6.1.

Le théorème 6.3 nous permet immédiatement de classifier les réseaux modulaires de rang impair.

6.5 THÉORÈME. *Soient $r \in \mathbb{N}$ impair et $s \in \mathbb{Z}$.*

(i) Si s est impair, il n'existe aucun B-réseau p^s-modulaire de rang r.

(ii) Si s est pair, il existe alors exactement deux classes de réseaux p^s-modulaires de rang r. Si L_1 et L_2 en sont des représentants respectifs, on a $\mathcal{N}L_1 = \mathcal{N}L_2 = p^sB$ et $\left(\mathrm{d}L_1, {}^{E}\!/_{K}\right) = -\left(\mathrm{d}L_2, {}^{E}\!/_{K}\right)$.

Preuve. Si (L,h) est un B-réseau p^s-modulaire de rang r impair, alors, vu le théorème 6.3, il existe un sous-réseau p^s-modulaire J de rang 1 avec $L \simeq J \perp H(s) \perp \cdots \perp H(s)$ et $\mathcal{N}J = \mathcal{N}L$. Mais il est clair que $\mathcal{N}J = \mathcal{H}J = p^sB$ de sorte que s est pair. Cela prouve d'une part l'assertion (i) et d'autre part que $\mathcal{N}L = p^sB$.
Considérons les B-réseaux (L_1,h_1) et (L_2,h_1) p^s-modulaires de rang r définis respectivement par $L_1 \simeq < \pi^{\frac{s}{2}} > \perp H(s) \perp \cdots \perp H(s)$ et $L_2 \simeq < \epsilon\pi^{\frac{s}{2}} > \perp H(s) \perp \cdots \perp H(s)$. On a clairement $\left(\mathrm{d}L_1, {}^{E}\!/_{K}\right) = -\left(\mathrm{d}L_2, {}^{E}\!/_{K}\right)$ et vu le théorème 6.1, tout réseau p^s-modulaire de rang r est isométrique à L_1 ou à L_2. □

Soient $r \in \mathbb{N}$ pair et $s \in \mathbb{Z}$. La classification des réseaux p^s-modulaires de rang r est plus délicate que celle des réseaux modulaires de rang impair. La norme des réseaux jouera un rôle essentiel dans ce travail et nous allons tout d'abord déterminer les valeurs qu'elle peut prendre. Le lemme suivant est prouvé dans [4], proposition 9.1 a), page 455.

6.6 LEMME. *Soient $s \in \mathbb{Z}$ et L un réseau p^s-modulaire de rang 2.*
Alors $\mathcal{H}L \supset \mathcal{N}L \supset \mathcal{N}H(s)$. □

Pour classifier effectivement les réseaux p^s-modulaires de rang r, nous devons distinguer deux cas, selon que l'extension ${}^{E}\!/_{K}$ est ramifiée première ou unitaire.

Supposons tout d'abord que l'extension ${}^{E}\!/_{K}$ soit ramifiée première.

Soient $s \in \mathbb{Z}$ et $m \in \mathbb{Z}$ avec $s < 2m \leqslant s + v_E(2)$.

Considérons le B-réseau $\big(H(s,2m),h\big)$ défini par

$$H(s,2m) = xB \oplus yB \simeq \begin{pmatrix} \pi^m & p^s \\ \sigma(p^s) & 0 \end{pmatrix}.$$

Comme $s < 2m$, le critère de la remarque 2.3 ii) nous montre que $\big(H(s,2m),h\big)$ est p^s-modulaire. De plus, il est clair que $\big(\mathrm{d}H(s,2m), {}^{E}\!/_{K}\big) = \big(-1, {}^{E}\!/_{K}\big)$.

Déterminons maintenant la norme de $H(s,2m)$. Soit $z := ax + by \in H(s,2m)$.
On a $h(z,z) = a\,\sigma(a)\pi^m + a\,\sigma(b)p^s + \sigma(a\,\sigma(b)p^s)$ et donc, en utilisant le lemme 6.2,

$$\begin{aligned} v_E\big(h(z,z)\big) &\geqslant \min\big\{\, 2m + v_E\big(a\,\sigma(a)\big),\ v_E\big(a\,\sigma(b)p^s + \sigma(a\,\sigma(b)p^s)\big)\,\big\} \\ &\geqslant \min\big\{\, 2m,\ s + v_E(2)\,\big\} \\ &= 2m \end{aligned}$$

de sorte que $\mathcal{N}H(s,2m) = p^{2m}B$.

Remarquons, dans le cas où s est pair, que $H\big(s, s + v_E(2)\big) \simeq H(s)$.

Considérons le B-réseau $\big(J(s,2m),h\big)$ défini par

$$J(s,2m) = xB \oplus yB \simeq \begin{pmatrix} \pi^m & p^s \\ \sigma(p^s) & 4\pi^{s-m}(-1)^{s+1}\eta \end{pmatrix}.$$

Rappelons que η est une unité telle que $\Delta = 1 + 4\eta$.

On a
$$\begin{aligned} v_E\big(4\pi^{s-m}(-1)^{s+1}\eta\big) &= v_E(4\pi^{s-m}) \\ &= 2\,v_E(2) + 2\,(s-m) \\ &= 2\,\big(v_E(2) + s\big) - 2m \\ &\geqslant 2\,(2m) - 2m \\ &= 2m \end{aligned}$$

et ainsi, comme $s < 2m$, le critère de la remarque 2.3 ii) nous montre que $\big(J(s,2m),h\big)$ est p^s-modulaire.

De plus
$$\begin{aligned} \mathrm{d}J(s,2m) &= \pi^m 4\pi^{s-m}(-1)^{s+1}\eta - (-\pi)^s \\ &= \pi^m 4\pi^{s-m}(-1)^s\,\frac{1-\Delta}{4} - (-\pi)^s \\ &= (-\pi)^s(1 - \Delta - 1) \\ &= -\Delta(-\pi)^s, \end{aligned}$$

donc $\big(\mathrm{d}J(s,2m), {}^{E}\!/_{K}\big) = \big(\Delta, {}^{E}\!/_{K}\big)\big(-1, {}^{E}\!/_{K}\big) = -\big(-1, {}^{E}\!/_{K}\big)$.

Déterminons maintenant la norme de $J(s,2m)$. Soit $z := ax + by \in J(s,2m)$. On a $h(z,z) = a\,\sigma(a)\pi^m + a\,\sigma(b)p^s + \sigma(a\,\sigma(b)p^s) + b\,\sigma(b)4\pi^{s-m}(-1)^{s+1}\eta$.
Mais $v_E\big(a\,\sigma(a)\pi^m\big)$ et $v_E\big(b\,\sigma(b)4\pi^{s-m}(-1)^{s+1}\eta\big)$ sont supérieurs ou égaux à $2m$, donc, en utilisant le lemme 6.2,

$$\begin{aligned} v_E\big(h(z,z)\big) &\geqslant \min\big\{\, 2m,\ v_E\big(a\,\sigma(b)p^s + \sigma(a\,\sigma(b)p^s)\big)\,\big\} \\ &\geqslant \min\big\{\, 2m,\ s + v_E(2)\,\big\} \\ &= 2m \end{aligned}$$

de sorte que $\mathcal{N}J(s,2m) = p^{2m}B$.

Nous sommes alors en mesure d'énoncer le théorème suivant :

6.7 THÉORÈME. *Supposons $^{E}/_{K}$ ramifiée première. Soient $r \in \mathbb{N}$ pair et $s \in \mathbb{Z}$.*

(i) Pour tout $n \in \mathbb{Z}$ pair avec $s \leqslant n \leqslant s + v_E(2)$, il existe exactement deux classes d'isométrie de B-réseaux p^s-modulaires de rang r et de norme p^nB. Si L_1 et L_2 en sont des représentants respectifs, on a $\left(\mathrm{d}L_1, {}^{E}/_{K}\right) = -\left(\mathrm{d}L_2, {}^{E}/_{K}\right)$.

(ii) Si $n = s + v_E(2) + 1$ est pair et donc s est impair, il existe exactement une classe d'isométrie de B-réseaux p^s-modulaires de rang r et de norme p^nB, celle du réseau $H(s) \perp \cdots \perp H(s)$.

(iii) Pour toutes les autres valeurs paires de n, il n'existe aucune classe d'isométrie de B-réseaux p^s-modulaires de rang r et de norme p^nB.

Preuve. Soit $n \in \mathbb{Z}$ pair.
Supposons que $n = s$. Considérons les B-réseaux (L_1, h_1) et (L_2, h_2) p^s-modulaires de rang r définis respectivement par $L_1 \simeq < \pi^{\frac{n}{2}} > \perp < \pi^{\frac{n}{2}} > \perp H(s) \perp \cdots \perp H(s)$ et $L_2 \simeq < \epsilon\pi^{\frac{n}{2}} > \perp < \pi^{\frac{n}{2}} > \perp H(s) \perp \cdots \perp H(s)$. On a clairement $\mathcal{N}L_1 = \mathcal{N}L_2 = p^nB$ et $\left(\mathrm{d}L_1, {}^{E}/_{K}\right) = -\left(\mathrm{d}L_2, {}^{E}/_{K}\right)$ de sorte que, vu le théorème 6.1, tout réseau p^s-modulaire de rang r de norme p^nB est isométrique à L_1 ou à L_2.

Supposons que $s < n \leqslant s + v_E(2)$. Considérons les B-réseaux (L_1, h_1) et (L_2, h_2) p^s-modulaires de rang r définis respectivement par $L_1 \simeq H(s,n) \perp H(s) \perp \cdots \perp H(s)$ et $L_2 \simeq J(s,n) \perp H(s) \perp \cdots \perp H(s)$. Vu les calculs précédents, on a $\mathcal{N}L_1 = \mathcal{N}L_2 = p^nB$ et $\left(\mathrm{d}L_1, {}^{E}/_{K}\right) = -\left(\mathrm{d}L_2, {}^{E}/_{K}\right)$ de sorte que, vu le théorème 6.1, tout réseau p^s-modulaire de rang r de norme p^nB est isométrique à L_1 ou à L_2.

Supposons que $n = s + v_E(2) + 1$, en particulier que s est impair. Soit (L, h) un B-réseau p^s-modulaire de rang r. Vu le théorème 6.3, il existe un sous-réseau p^s-modulaire L' de rang 2 et de norme p^nB avec $L \simeq L' \perp H(s) \perp \cdots \perp H(s)$.
Ecrivons $L' = xB + yB$ avec $x, y \in L'$. On peut supposer que $h(x,y) = p^s$. On a $h(x,x),\ h(y,y) \in 2p^{s+1}B$, donc il existe $a,\ b \in A$ avec $h(x,x) = 2p^{s+1}a$ et $h(y,y) = 2p^{s+1}b$. Ainsi $\mathrm{d}L' = 4\pi^{s+1}ab - (p\,\sigma(p))^s = 4\pi^s\pi ab - (-\pi)^s = -(-\pi)^s(1 - 4\pi ab)$. Mais $(1 - 4\pi ab)$ est un carré dans A (cf [7], 63:1), donc $\left(\mathrm{d}L', {}^{E}/_{K}\right) = \left(-1, {}^{E}/_{K}\right)$. Vu le théorème 6.1, on a $L' \simeq H(s)$.

Finalement, l'assertion (iii) découle des lemmes 6.2 et 6.6. □

6.8 COROLLAIRE. *Supposons $^{E}/_{K}$ ramifiée première. Soient $r \in \mathbb{N}$ pair et $s \in \mathbb{Z}$.*

(i) Supposons s pair. Alors il existe exactement $v_E(2) + 2$ classes d'isométrie de B-réseaux p^s-modulaire de rang r. Il y en a exactement $v_K(2) + 1$ dont le symbole de Hilbert du discriminant est $+1$.

(ii) Supposons s impair. Alors il existe exactement $v_E(2) + 1$ classes d'isométrie de B-réseaux p^s-modulaire de rang r. Il y en a exactement $v_K(2) + \alpha$ dont le symbole de Hilbert du discriminant est $+1$ où $\alpha \in \{0,1\}$ et $\alpha = 1$ si et seulement si $\left(-1, {}^{E}/_{K}\right)^{\frac{r}{2}} = 1$. □

Supposons maintenant que l'extension $^E/_K$ soit ramifiée k-unitaire.

Soient $s \in \mathbb{Z}$ et $m \in \mathbb{Z}$ avec $s < 2m \leqslant s + v_E(2) - 2k - 1$.

Considérons le B-réseau $\big(H(s,2m), h\big)$ défini par

$$H(s,2m) = xB \oplus yB \simeq \begin{pmatrix} \pi^m & p^s \\ \sigma(p^s) & 0 \end{pmatrix}.$$

Comme $s < 2m$, le critère de la remarque 2.3 ii) nous montre que $\big(H(s,2m), h\big)$ est p^s-modulaire. De plus $\big(\mathrm{d}H(s,2m), {}^E/_K\big) = \big(-1, {}^E/_K\big)$.

Déterminons maintenant la norme de $H(s,2m)$. Soit $z := ax + by \in H(s,2m)$.
On a $h(z,z) = a\,\sigma(a)\pi^m + a\,\sigma(b)p^s + \sigma(a\,\sigma(b)p^s)$ et donc, en utilisant le lemme 6.2,

$$\begin{aligned} v_E\big(h(z,z)\big) &\geqslant \min\big\{\, v_E\big(2m + a\,\sigma(a)\big),\ v_E\big(a\ \sigma(b)p^s + \sigma(a\,\sigma(b)p^s)\big)\,\big\} \\ &\geqslant \min\big\{\, 2m,\ s - 2k - 1 + v_E(2)\,\big\} \\ &= 2m \end{aligned}$$

de sorte que $\mathcal{N}H(s,2m) = p^{2m}B$.

Considérons le B-réseau $\big(J(s,2m), h\big)$ défini par

$$J(s,2m) = xB \oplus yB \simeq \begin{pmatrix} \pi^m & p^s \\ \sigma(p^s) & 4\pi^{s-m-2k-1}(-\delta)^s\delta^{-1}\eta \end{pmatrix},$$

avec δ et η comme au début du paragraphe.

On a
$$\begin{aligned} v_E\big(4\pi^{s-m-2k-1}(-\delta)^s\delta^{-1}\eta\big) &= v_E\big(4\pi^{s-m-2k-1}\big) \\ &= 2\,v_E(2) + 2(s - m - 2k - 1) \\ &= 2\,v_E(2 + s - 2k - 1) - 2m \\ &\geqslant 2\,(2m) - 2m \\ &= 2m \end{aligned}$$

et ainsi, comme $s < 2m$, le critère de la remarque 2.3 ii) nous montre que $\big(J(s,2m), h\big)$ est p^s-modulaire.

De plus
$$\begin{aligned} \mathrm{d}J(s,2m) &= \pi^m 4\pi^{s-m-2k-1}(-\delta)s\delta^{-1}\eta - (-\delta\pi)^s \\ &= -(-\delta\pi)^s(-4\pi^{-2k-1}\delta^{-1}\eta + 1) \\ &= -(-\delta\pi)^{s-2k-1}(-\delta)^{2k}(4\eta - \pi^{2k+1}\delta). \end{aligned}$$

Mais $\Delta - \theta = 1 + 4\eta - (1 + \pi^{2k+1}\delta) = 4\eta - \pi^{2k+1}\delta$ de sorte que $\big(\mathrm{d}J(s,2m), {}^E/_K\big) = \big(-1, {}^E/_K\big)\big(\Delta - \theta, {}^E/_K\big)$. Or l'espace quadratique V défini par $V \simeq < \Delta - \theta > \perp < \theta >$ représente $\Delta = \Delta - \theta + \theta$ et $v_E(\mathrm{d}V) = v_E(\Delta - \theta) = v_E(4\eta - \pi^{2k+1}\delta) = 2k + 1$ est impair, donc l'espace quadratique V ne représente pas 1 (cf [7] 63:10).
Ainsi $\big(\Delta - \theta, {}^E/_K\big) = -1$ de sorte que finalement $\big(\mathrm{d}J(s,2m), {}^E/_K\big) = -\big(-1, {}^E/_K\big)$.

Déterminons maintenant la norme de $J(s,2m)$. Soit $z := ax + by \in J(s,2m)$. On a $h(z,z) = a\,\sigma(a)\pi^m + a\,\sigma(b)p^s + \sigma(a\,\sigma(b)p^s) + b\,\sigma(b)\,4\pi^{s-m-2k-1}(-\delta)^s\delta^{-1}\eta$.
Mais $v_E\big(a\,\sigma(a)\pi^m\big)$ et $v_E\big(b\,\sigma(b)4\pi^{s-m-2k-1}(-\delta)^s\delta^{-1}\eta\big)$ sont supérieurs ou égaux à $2m$ de sorte qu'en utilisant le lemme 6.2, on a

$$\begin{aligned} v_E\big(h(z,z)\big) &\geqslant \min\big\{\, 2m,\ v_E\big(a\,\sigma(b)p^s + \sigma(a\,\sigma(b)p^s)\big)\,\big\} \\ &\geqslant \min\big\{\, 2m,\ s + v_E(2)\,\big\} \\ &= 2m \end{aligned}$$

et ainsi $\mathcal{N}J(s,2m) = p^{2m}B$.

Nous sommes alors en mesure d'énoncer le théorème suivant :

6.9 THÉORÈME. *Supposons E/K ramifiée k-unitaire. Soient $r \in \mathbb{N}$ pair et $s \in \mathbb{Z}$.*

(i) Pour tout $n \in \mathbb{Z}$ pair avec $s \leqslant n \leqslant s + v_E(2) - 2k - 1$, il existe exactement deux classes d'isométrie de B-réseaux p^s-modulaires de rang r et de norme p^nB. Si L_1 et L_2 en sont des représentants respectifs, on a $\big(\mathrm{d}L_1, E/K\big) = -\big(\mathrm{d}L_2, E/K\big)$.

(ii) Si $n = s + v_E(2) - 2k$ est pair et donc s est pair, il existe exactement une classe d'isométrie de B-réseaux p^s-modulaires de rang r et de norme p^nB, celle du réseau $H(s) \perp \cdots \perp H(s)$.

(iii) Pour toutes les autres valeurs paires de n, il n'existe aucune classe d'isométrie de B-réseaux p^s-modulaires de rang r et de norme p^nB.

Preuve. Les assertions (i) et (iii) se prouvent comme leur analogue du théorème 6.7.

Prouvons alors (ii). Soit $n \in \mathbb{Z}$ pair avec $n = s + v_E(2) - 2k$. En particulier s est pair. Soit (L,h) un B-réseau p^s-modulaire de rang r. Vu le théorème 6.3, il existe un sous-réseau p^s-modulaire L' de rang 2 et de norme p^nB avec $L \simeq L' \perp H(s) \perp \cdots \perp H(s)$. Grâce au théorème de classification 6.1, il suffit de montrer que $\big(\mathrm{d}L', E/K\big) = \big(-1, E/K\big)$.
Vu la remarque 2.2 i), $p^{-\frac{s}{2}}L'$ est B-modulaire. De plus, on a $\mathcal{N}p^{-\frac{s}{2}}L' = p^{-2k+v_E(2)}B$. D'autre part, il est clair que $\big(\mathrm{d}L', E/K\big) = \big(\mathrm{d}(p^{-\frac{s}{2}}L'), E/K\big)$. Ainsi, quitte à remplacer L' par $p^{-\frac{s}{2}}L'$, on peut supposer que $s = 0$.
Ecrivons $L' = xB + yB$ avec $x, y \in J$. On peut supposer que $h(x,y) = 1$. On a $h(x,x),\ h(y,y) \in 2\pi^{-k}B$, donc il existe $a,\ b \in A$ avec $h(x,x) = 2\pi^{-k}a$ et $h(y,y) = 2\pi^{-k}b$. Posant $y' = -bpx + y$, on a évidemment que $L' = xB + y'B$ avec $h(x,y') \in B^*$. D'autre part, on a $h(y',y') = b^2p\,\sigma(p)\,2a\pi^{-k} - b\big(p + \sigma(p)\big) + 2b\pi^{-k} = -\delta b^2\,2a\pi^{-k+1}$ de sorte que $v_E\big(h(y',y')\big) > v_E\big(h(y,y)\big)$. En itérant ce procédé, on se ramène au cas où $v_E(b) \geqslant k+2$. Ainsi $\mathrm{d}L' = 4\pi^{-2k}ab - 1 = -(1 - 4\pi^{-2k}ab)$. Or $v_K(\pi^{-2k}ab) = \frac{1}{2}v_E(\pi^{-2k}ab) \geqslant \frac{1}{2}(-k+k+2) = 1$ de sorte que $1 - 4\pi^{-2k}ab$ est un carré dans A (cf [7], 63:1). On obtient finalement $\big(\mathrm{d}L', E/K\big) = \big(-1, E/K\big)$. □

6.10 COROLLAIRE. *Supposons E/K ramifiée k-unitaire. Soient $r \in \mathbb{N}$ pair et $s \in \mathbb{Z}$.*

(i) Supposons s pair. Alors il existe exactement $v_E(2) - 2k + 1$ classes d'isométrie de B-réseaux p^s-modulaire de rang r. Il y en a exactement $v_K(2) - k + \alpha$ dont le symbole de Hilbert du discriminant est $+1$ où $\alpha \in \{0,1\}$ et $\alpha = 1$ si et seulement si $\big(-1, E/K\big)^{\frac{r}{2}} = 1$.

(ii) Supposons s impair. Alors il existe exactement $v_E(2) - 2k$ classes d'isométrie de B-réseaux p^s-modulaire de rang r. Il y en a exactement $v_K(2) - k$ dont le symbole de Hilbert du discriminant est $+1$. □

§ 7. Cas d'une extension ramifiée dyadique : calcul du nombre de classes

Les hypothèses et notations de ce paragraphe sont les mêmes que celles du paragraphe précédent.

Dans ce paragraphe, nous déterminerons $\big|\mathcal{C}(t,r,s)\big|$ pour tout triplet de Jordan (t,r,s).

Si $L_1,\dots,L_t$ est une décomposition de Jordan saturée d'un B-réseau de type fondamental (t,r,s,n), nous noterons $L_{(j)} = L_1 \perp \cdots \perp L_j$ pour tout $1 \leqslant j \leqslant t$.
Le théorème central de ce chapitre est prouvé dans [4], théorème 11.4, page 463. Il donne des conditions équivalentes à l'isométrie de B-réseaux.

7.1 THÉORÈME. *Soient $L_1,\dots,L_t$ et $L_1,\dots,L'_{t'}$ des décompositions de Jordan saturées de type fondamental respectif (t,r,s,n) et (t',r',s',n'). Alors les B-réseaux $L_1 \perp \cdots \perp L_t$ et $L'_1 \perp \cdots \perp L'_{t'}$ sont isométriques si et seulement si les trois conditions suivantes sont satisfaites :*

(i) $(t,r,s,n) = (t',r',s',n')$.

(ii) $\mathrm{d}L_1 \cdots \mathrm{d}L_t = \mathrm{d}L'_1 \cdots \mathrm{d}L'_{t'}$.

(iii) Pour tout $1 \leqslant j \leqslant t-1$, $\dfrac{\mathrm{d}L_{(j)}}{\mathrm{d}L'_{(j)}}$ *est représenté par une unité* $\kappa \in A^*$ *telle que* $\kappa - 1 \in p^{n_{j+1}+n_j-2s_j}B$. □

Essayons d'exprimer les deux dernières conditions d'une façon plus agréable permettant le calcul de $\big|\mathcal{C}(t,r,s,n)\big|$ pour tout quadruplet de Jordan (t,r,s,n).
Posons $f_j = n_{j+1} + n_j - 2s_j$ pour tout $1 \leqslant j \leqslant t-1$ et $f_t = v_E(4) + 2$.
Soit $\pi^c A$ le défaut quadratique de l'unité $\epsilon \in A^*$. Rappelons qu'il est maximal parmi les défauts quadratiques des unités qui ne sont pas une norme.
Posons $U(t,r,s,n) = \big\{\, j \mid 1 \leqslant j \leqslant t,\ f_j > 2c \,\big\}$. Nous noterons U au lieu de $U(t,r,s,n)$ lorsqu'aucune confusion n'est possible.
La proposition 1.4 nous dit que $c \leqslant v_K(4)$ de sorte que $t \in U$.
Le théorème 7.1 peut alors se réécrire ainsi :

7.2 COROLLAIRE. *Soient $L_1,\dots,L_t$ et $L'_1,\dots,L'_t$ des décompositions de Jordan saturées de type fondamental (t,r,s,n). Alors $L_1 \perp \cdots \perp L_t \simeq L'_1 \perp \cdots \perp L'_t$ si et seulement si $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$ pour tout $j \in U(t,r,s,n)$.*

Preuve. Supposons que $L_1 \perp \cdots \perp L_t \simeq L'_1 \perp \cdots \perp L'_t$. Soit $j \in U$. Montrons que $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$. C'est clair si $j = t$. Supposons alors $j < t$. Vu le théorème 7.1, il existe $\kappa \in A^*$ représentant $\frac{\mathrm{d}L_{(j)}}{\mathrm{d}L'_{(j)}}$ telle que $\kappa - 1 \in p^{f_j}B$ donc $\kappa - 1 \in \pi^{\frac{f_j}{2}}A \subset \pi^{c+1}A$. Par définition de c, on a $\kappa \in \big\{\, a\,\sigma(a) \mid a \in A^* \,\big\}$ et ainsi $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$.

Réciproquement, supposons que $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$ pour tout $j \in U$. Comme $t \in U$, on a $\mathrm{d}(L_1 \perp \cdots \perp L_t) = \mathrm{d}(L'_1 \perp \cdots \perp L'_t)$. Montrons que, pour tout $1 \leqslant j < t$, il existe $\kappa \in A^*$ représentant $\frac{\mathrm{d}L_{(j)}}{\mathrm{d}L'_{(j)}}$ telle que $\kappa - 1 \in p^{f_j}B$. Si $j \in U$, on peut alors choisir $\kappa = 1$. Si $j \notin U$, on a $f_j \leqslant 2c$ de sorte que $\epsilon - 1 \in p^{f_j}B$. On choisira alors $\kappa = 1$ si $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$ et $\kappa = \epsilon$ sinon. □

Soit (t,r,s,n) un quadruplet de Jordan. Calculons $\big|\mathcal{C}(t,r,s,n)\big|$. Nous supposerons que $\mathcal{C}(t,r,s,n) \neq \emptyset$, ce qui revient à supposer que pour tout $1 \leqslant i \leqslant t$, il existe un B-réseau p^{s_i}-modulaire de norme $p^{n_i}B$.

Si $1 \leqslant j \leqslant t$, on dit que n_j est *maximal* si $n_j = s_j + v_E(2) + 1$ dans le cas R-P ou si $n_j = s_j + v_E(2) - 2k$ dans le cas R-U_k. Notons $S(t,r,s,n)$ ou plus simplement S l'ensemble des $j \in U$ tels que n_j soit maximal. Remarquons que n_j est maximal si et seulement s'il n'existe qu'une seule classe d'isométrie de réseaux p^{s_j}-modulaires de norme $p^{n_j}B$; si L en est un représentant, alors $\mathrm{d}L = -1$.
Soit $j \in S$. Considérons le plus petit entier strictement positif $k(j)$ vérifiant l'une ou l'autre des trois conditions suivante : $j = k(j)$, $j - k(j) \in U$ ou $n_{j-k(j)}$ n'est pas maximal. Remarquons que si $j \in S$, on a n_i maximal pour tout $j - k(j) + 1 \leqslant i \leqslant j$.
Posons $V = V(t,r,s,n) = \big\{\, j \in S \mid j - k(j) \in U \cup \{0\} \,\big\}$ et $T = T(t,r,s,n) = U \setminus V$.

7.3 REMARQUE. Soient $j \in V$ et l le plus grand entier de $T \cup \{0\}$ avec $l \leqslant j$. Alors $n_{l+1}, \ldots, n_t$ sont tous maximaux.
Raisonnons par l'absurde. Soit m le plus grand entier avec $l < m < j$ et n_m non maximal. Comme $j \in U$ et $j > m$, on peut considérer le plus petit entier q avec $q \in U$ et $q > m$. Soit $m < i < q$. Par définition de m et q, on a n_i maximal, $i \neq 0$ et $i \notin U$ de sorte que $m = q - k(q)$. Comme $l + 1 \leqslant q \leqslant j$, on a $q \notin T$ donc $q \in V$ et $m = q - k(q) \in U$. Vu que n_m n'est pas maximal, $m \in T$ ce qui contredit la définition de l.

Nous pouvons alors énoncer :

7.4 THÉORÈME. *Soit (t,r,s,n) un quadruplet de Jordan tel que $\mathcal{C}(t,r,s,n) \neq \emptyset$. Alors* $\big|\mathcal{C}(t,r,s,n)\big| = 2^{|T(t,r,s,n)|}$.

Preuve. Soient (L,h) un réseau de type fondamental (t,r,s,n) et $L_1, \ldots, L_t$ et $L'_1, \ldots, L'_t$ deux décompositions de Jordan saturées de (L,h).
Si $j \in T$, on a $j \in U$ donc, vu le corollaire 7.2, $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$ de sorte que l'on peut définir une application $\Phi : \mathcal{C}(t,r,s,n) \to \{\pm 1\}^T$ par $\Phi\big(L\big)(j) = \big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big)$.

Montrons que Φ est injective.

Soient (L,h) et (L',h') deux réseaux de type fondamental (t,r,s,n) avec $\Phi\big(L\big) = \Phi\big(L'\big)$. Soient $L_1, \ldots, L_t$ et $L'_1, \ldots, L'_t$ deux décompositions de Jordan saturées de (L,h) et (L',h') respectivement. Vu le corollaire 7.2, il suffit de montrer que pour tout $j \in U$, on a $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$. Soit $j \in U$.
Si $j \in T$, on a $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = \Phi\big(L\big)(j) = \Phi\big(L'\big)(j) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$.
Supposons que $j \notin T$. Alors $j \in V$.
Soit l le plus grand entier de $T \cup \{0\}$ avec $l \leqslant j$. Vu la remarque 7.3, n_i est maximal pour tout $l + 1 \leqslant i \leqslant j$. Si $l = 0$, on a alors $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = (-1)^j = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$ et si $l \in T$, on a $\big(\mathrm{d}L_{(j)}, {}^{E}\!/_{K}\big) = (-1)^{j-l} \cdot \big(\mathrm{d}L_{(l)}, {}^{E}\!/_{K}\big) = (-1)^{j-l} \cdot \Phi\big(L\big)(l) = (-1)^{j-l} \cdot \Phi\big(L'\big)(l) = = (-1)^{j-l} \cdot \big(\mathrm{d}L'_{(l)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L'_{(j)}, {}^{E}\!/_{K}\big)$.

Montrons que Φ est surjective.

Si $|T| = 0$, c'est clair. Supposons alors que $m := |T| \geqslant 1$ et écrivons $T = \{t_1, \dots, t_m\}$ avec $t_1 < \cdots < t_m$. Posons $t_0 = 0$.
Soit $\tau \in \{\pm 1\}^T$. Considérons $1 \leqslant j \leqslant m$.
Suposons qu'il existe des réseaux $L_1, \dots, L_{t_{j-1}}$ avec L_i p^{s_i}-modulaire de norme $p^{n_i}B$ pour tout $1 \leqslant i \leqslant t_{j-1}$ et $\big(\mathrm{d}L_{(t_i)}, {}^{E}\!/_{K}\big) = \tau(t_i)$ pour tout $1 \leqslant i \leqslant j-1$.
Montrons qu'il existe des B-réseaux $L_{t_{j-1}+1}, \dots, L_{t_j}$ avec L_i p^{s_i}-modulaire de norme $p^{n_i}B$ pour tout $t_{j-1}+1 \leqslant i \leqslant t_j$ et $\big(\mathrm{d}L_{(t_j)}, {}^{E}\!/_{K}\big) = \tau(t_j)$.
Supposons que $t_j \notin S$. Vu les théorèmes 6.5, 6.7 et 6.9, il existe des réseaux $L_{t_{j-1}+1}, \dots, L_{t_j}$ avec L_i p^{s_i}-modulaire de norme $p^{n_i}B$ pour tout $t_{j-1}+1 \leqslant i \leqslant t_j$ et tels que $\big(\mathrm{d}L_{t_j}, {}^{E}\!/_{K}\big) = \tau(t_j)\big(\mathrm{d}L_{(t_j-1)}, {}^{E}\!/_{K}\big)$. On a clairement $\big(\mathrm{d}L_{(t_j)}, {}^{E}\!/_{K}\big) = \tau(t_j)$.
Supposons maintenant que $t_j \in S$. Comme $t_j \in T$, on a $t_j \notin V$ et donc $k(t_j) < t_j$ et $t_j - k(t_j) \notin U$ de sorte que, par définition de $k(t_j)$, $t_j - k(t_j)$ n'est pas maximal et, comme $t_{j-1} \in U$, $t_{j-1} < t_j - k(t_j)$. Vu les théorèmes 6.5, 6.7 et 6.9, il existe des réseaux $L_{t_{j-1}+1}, \dots, L_{t_j}$ avec L_i p^{s_i}-modulaire de norme $p^{n_i}B$ pour tout $t_{j-1}+1 \leqslant i \leqslant t_j$, $\big(\mathrm{d}L_{j-k(t_j)}, {}^{E}\!/_{K}\big) = \big(\mathrm{d}L_{(j-k(t_j)-1)}, {}^{E}\!/_{K}\big)(-1)^{k(t_j)}\tau(t_j)$ et $\big(\mathrm{d}L_i, {}^{E}\!/_{K}\big) = -1$ pour tout entier i vérifiant $t_j - k(t_j) + 1 \leqslant i \leqslant t_j$. On a alors, par construction, $\big(\mathrm{d}L_{(t_j)}, {}^{E}\!/_{K}\big) = \tau(t_j)$.

En résumé, on a prouvé l'existence de B-réseaux $L_1, \dots, L_{t_m}$ avec L_i p^{s_i}-modulaire de norme $p^{n_i}B$ pour tout $1 \leqslant i \leqslant t_m$ et $\big(\mathrm{d}L_{(t_i)}, {}^{E}\!/_{K}\big) = \tau(t_i)$ pour tout $1 \leqslant i \leqslant t$. Utilisons une dernière fois les théorèmes 6.5, 6.7 et 6.9 pour trouver des réseaux $L_{t_m+1}, \dots, L_t$ avec L_i p^{s_i}-modulaire de norme $p^{n_i}B$ pour tout $t_m + 1 \leqslant i \leqslant t$. Il est alors clair que l'on a $\Phi\big(L_1 \perp \cdots \perp L_t\big) = \tau$ de sorte que Φ est surjective.

Comme Φ est une bijection, on a $\big|\mathcal{C}(t,r,s,n)\big| = \big|\{\pm 1\}^{T(t,r,sn)}\big| = 2^{|T(t,r,s,n)|}$. □

7.5 COROLLAIRE. *Soient (t,r,s,n) un quadruplet de Jordan tel que $\mathcal{C}(t,r,s,n) \neq \emptyset$ et $\lambda \in \{\pm 1\}$. Alors*

(i) Si $T(t,r,s,n) = \emptyset$, alors $\big|\mathcal{C}_\lambda(t,r,s,n)\big| \leqslant 1$ et on a $\big|\mathcal{C}_\lambda(t,r,s,n)\big| = 1$ si et seulement si $\lambda = \big(-1, {}^{E}\!/_{K}\big)^{\frac{1}{2}(r_1+\cdots+r_t)}$.

(ii) Si $T(t,r,s,n) \neq \emptyset$, alors $\big|\mathcal{C}_\lambda(t,r,s,n)\big| = 2^{|T(t,r,s,n)|-1}$.

Preuve. Supposons tout d'abord que $T(t,r,s,n) = \emptyset$. Vu les définitions, on a n_i maximal pour tout $1 \leqslant i \leqslant t$ donc $r_1 + \cdots + r_t$ est pair et $\big(\mathrm{d}L, {}^{E}\!/_{K}\big) = \big(-1, {}^{E}\!/_{K}\big)^{\frac{1}{2}(r_1+\cdots+r_t)}$ pour tout réseau L de $\mathcal{C}_\lambda(t,r,s,n)$, ce qui prouve (i).
Supposons que $T(t,r,s,n) \neq \emptyset$. Reprenons les notations de la preuve du théorème 7.4 et considérons plus particulièrement l'application $\Phi : \mathcal{C}(t,r,s,n) \to \{\pm 1\}^T$. Soit L un réseau de $\mathcal{C}(t,r,s,n)$. On a $t \in U$ par définition. Soit l le plus grand élément de T. Vu la remarque 7.3, on a $n_{l+1}, \dots, n_t$ maximaux donc $\big(\mathrm{d}L, {}^{E}\!/_{K}\big) = (-1)^{t-l} \cdot \Phi\big(L\big)(l)$. En résumé, L est dans $\mathcal{C}_\lambda(t,r,s,n)$ si et seulement si $\Phi\big(L\big)(l) = (-1)^{t-l} \cdot \lambda$. □

Soit (t,r,s) un triplet de Jordan tel que $\mathcal{C}(t,r,s) \neq \emptyset$. Calculons $\big|\mathcal{C}(t,r,s)\big|$.
Notons $N(t,r,s)$ ou plus simplement N lorsqu'aucune confusion n'est possible l'ensemble des $n = (n_1, \dots, n_t) \in (2\mathbb{Z})^t$ tels que les conditions suivantes sont satisfaites :

i) $s_i = n_i$ est pair si r_i est impair,

ii) $s_i \leqslant n_i \leqslant v_E\big(\mathcal{N}H(s_i)\big)$ si r_i est pair,

iii) $n_1 \leqslant \cdots \leqslant n_t$,

iv) $n_{i+1} - n_i \leqslant 2\,(s_{i+1} - s_i)$ pour tout $1 \leqslant i \leqslant t-1$.

Les théorèmes 6.5, 6.7 et 6.9 nous montrent clairement que $n \in N(t,r,s)$ si et seulement si (t,r,s,n) est un quadruplet de Jordan tel que $\mathcal{C}(t,r,s,n) \neq \emptyset$.

7.6 THÉORÈME. *Soit (t,r,s) un triplet de Jordan tel que $\mathcal{C}(t,r,s) \neq \emptyset$.*
Alors on a

$$\left|\mathcal{C}(t,r,s)\right| = \sum_{n \in N(t,r,s)} \left|\mathcal{C}(t,r,s,n)\right| = \sum_{n \in N(t,r,s)} 2^{|T(t,r,s,n)|}.$$

Preuve. Il suffit de prouver que $\mathcal{C}(t,r,s) = \bigsqcup_{n \in N(t,r,s)} \mathcal{C}(t,r,s,n)$, ce qui découle directement des définitions. □

Soit (t,r,s) un triplet de Jordan. On dit que $n \in N(t,r,s)$ est *maximal* si $n_1, \ldots, n_t$ sont tous maximaux. Il existe au plus un $n \in N(t,r,s)$ maximal ; s'il en existe un, on dit que $N(t,r,s)$ est *maximal*. Notons $N^*(t,r,s)$ l'ensemble des éléments non maximaux de $N(t,r,s)$.
Le résultat suivant se prouve comme le théorème 7.6 :

7.7 THÉORÈME. *Soient (t,r,s) un triplet de Jordan tel que $\mathcal{C}(t,r,s) \neq \emptyset$ et $\lambda \in \{\pm 1\}$.*
Alors on a

$$\left|\mathcal{C}_\lambda(t,r,s)\right| = \alpha + \sum_{n \in N^*(t,r,s)} 2^{|T(t,r,s,n)|-1}$$

où $\alpha \in \{0,1\}$ et $\alpha = 1$ si et seulement si $N(t,r,s)$ est maximal et $\lambda = (-1)^{\frac{1}{2}(r_1+\cdots+r_t)}$. □

7.8 REMARQUE. Les deux derniers théorèmes 7.6 et 7.7 nous donnent des résultats précis mais peu utilisables dans ce degré de généralité. Ils nous permettent par contre de calculer les nombres $\left|\mathcal{C}(t,r,s)\right|$ et $\left|\mathcal{C}_\lambda(t,r,s)\right|$ dans des situations concrètes où l'extension et le triplet de Jordan nous sont donnés explicitement. Cependant, la théorie se simplifie nettement si l'on suppose que la suite $s_1 < \cdots < s_t$ est suffisamment croissante. Mais, avant d'aborder ces cas dans le prochain paragraphe, donnons quelques estimations plus simples de ces nombres.

Notons $P = P(t,r,s)$ (resp. $I = I(t,r,s)$) le nombre d'entiers $1 \leqslant i \leqslant t$ tels que r_i et s_i sont pairs (resp. r_i est pair et s_i impair).

7.9 PROPOSITION. *Soit (t,r,s) un triplet de Jordan. Alors :*

(i) Dans le cas R-P *on a* $\left|\mathcal{C}(t,r,s)\right| \leqslant 2^{t-P-I} \cdot \left(v_E(2)+2\right)^P \cdot \left(v_E(2)+1\right)^I$.

(ii) Dans le cas R-U$_k$ *on a* $\left|\mathcal{C}(t,r,s)\right| \leqslant 2^{t-P-I} \cdot \left(v_E(2)-2k+1\right)^P \cdot \left(v_E(2)-2k\right)^I$.

Preuve. Considérons $\Phi : \prod_{1\leqslant i\leqslant t} C\big(1,(r_i),(s_i)\big) \to C(t,r,s)$ définie par $\Phi\big(L_1,\dots,L_t\big) = L_1 \perp \cdots \perp L_t$. Clairement Φ est surjective. Le résultat découle alors du théorème 6.5 et des corollaires 6.8 et 6.10. □

Donnons encore une estimation de $\big|\mathcal{C}_\lambda(t,r,s)\big|$:

7.10 PROPOSITION. *Soit (t,r,s) un triplet de Jordan et $\lambda \in \{\pm 1\}$. Alors :*

(i) Dans le cas R-P *on a* $\big|\mathcal{C}_\lambda(t,r,s)\big| \leqslant 2^{t-1}\cdot(v_K(2)+1)^{P+I}$.

(ii) Dans le cas R-U$_k$ *on a* $\big|\mathcal{C}_\lambda(t,r,s)\big| \leqslant 2^{t-1}\cdot(v_K(2)-k+1)^{P+I}$.

Preuve. Les deux assertions se prouvant de la même manière, nous nous contenterons de démontrer la première.
Notons $\Omega = \big\{f \in \{\pm 1\}^{\{1,\dots,t\}} \big|\ f(1)\cdots f(t) = \lambda\big\}$ et considérons, pour tout $f \in \Omega$, l'ensemble $\mathcal{A}(f)$ de toutes les classes de $\mathcal{C}_\lambda(t,r,s)$ dont les réseaux admettent des décompositions de Jordan de la forme $L_1,\dots,L_t$ avec $\big(\mathrm{d}L_i, {}^{E}\!/_{K}\big) = f(i)$ pour tout $1 \leqslant i \leqslant t$.
Il est alors clair que $\mathcal{C}_\lambda(t,r,s) = \bigcup_{f\in\Omega} \mathcal{A}(f)$ et donc $\big|\mathcal{C}_\lambda(t,r,s)\big| \leqslant \sum_{f\in\Omega} \big|\mathcal{A}(f)\big|$.
Considérons l'application $\Psi : \prod_{1\leqslant i\leqslant t} \mathcal{C}_{f(i)}\big(1,(r_i),(s_i)\big) \to \mathcal{A}(f)$ définie par $\Psi\big(L_1,\dots,L_t\big) = L_1 \perp \cdots \perp L_t$. Elle est clairement surjective. Or le théorème 6.5 et les corollaires 6.8 et 6.10, nous disent que $\big|\mathcal{C}_{f(i)}\big(1,(r_1),(s_1)\big)\big|$ est inférieur à 1 si r_i est impair et à $v_K(2)+1$ si r_i est pair de sorte que finalement $\big|\mathcal{A}(f)\big| \leqslant \big(v_K(2)+1\big)^{P+I}$.
Ainsi $\big|\mathcal{C}_\lambda(t,r,s)\big| \leqslant |\Omega|\cdot\big(v_K(2)+1\big)^{P+I}$ et on conclut en observant que $|\Omega| = 2^{t-1}$. □

§ 8. Cas d'une extension ramifiée dyadique : un exemple idyllique

Les hypothèses et notations de ce paragraphe sont les mêmes que celles du paragraphe précédent.
Soit (t,r,s) un triplet de Jordan. Supposons que la suite $s_1 < \cdots < s_t$ soit suffisamment croissante, c'est à dire que $s_{i+1} - s_i \geqslant v_E(4)+1$ pour tout $1 \leqslant i \leqslant t-1$. Nous allons étudier les B-réseaux de type (t,r,s).

8.1 PROPOSITION. *Soit $L_1,\dots,L_t$ une décomposition de Jordan de type fondamental (t,r,s,n) de L. Supposons que $s_{i+1} - s_i \geqslant v_E(2)+1$ pour tout $1 \leqslant i \leqslant t-1$. Alors $L_1,\dots,L_t$ est saturée.*

Preuve. Grâce aux lemmes 6.6 et 6.2, on a $s_i \leqslant n_i \leqslant s_i + v_E(2)+1$ pour tout $1 \leqslant i \leqslant t$ de sorte que si $1 \leqslant j \leqslant t-1$, on a $n_{j+1} - n_j \geqslant s_{j+1} - s_j - v_E(2) - 1 \geqslant v_E(2)+1-v_E(2)-1 \geqslant 0$ et $n_{j+1} - n_j \leqslant s_{j+1} + v_E(2) + 1 - s_j \leqslant s_{j+1} + (s_{j+1} - s_j) - s_j = 2\,(s_{j+1} - s_j)$ et donc, vu la proposition 3.4, $L_1,\dots,L_t$ est saturée. □

8.2 THÉORÈME. *Soient $L_1,\dots,L_t$ et $L'_1,\dots,L'_t$ deux décompositions de Jordan de type fondamental (t,r,s,n). Supposons que $s_{i+1} - s_i \geqslant v_E(4)+1$ pour tout $1 \leqslant i \leqslant t-1$. Alors $L_1 \perp \cdots \perp L_t \simeq L'_1 \perp \cdots \perp L'_t$ si et seulement si $L_i \simeq L'_i$ pour tout $1 \leqslant i \leqslant t$.*

Preuve. Rappelons les notations du chapitre précédent. On a $f_i = n_{i+1} + n_i - 2s_i$ pour tout $1 \leqslant i \leqslant t-1$, $f_t = v_E(4) + 2$ et $U = U(t,r,s,n) = \{ i \mid 1 \leqslant i \leqslant t,\ f_i > 2c \}$. On a clairement $t \in U$. Soit $1 \leqslant i \leqslant t-1$. Alors $f_i = n_{i+1} + n_i - 2s_i \geqslant n_{i+1} - s_i \geqslant s_{i+1} - s_i \geqslant$ $\geqslant v_E(4)+1 > 2\,v_K(4) \geqslant 2c$ (cf. [7], 63:1). Ainsi $U = \{ j \mid 1 \leqslant j \leqslant t \}$. Or la proposition 8.1 nous dit que les décompositions $L_1, \ldots, L_t$ et $L'_1, \ldots, L'_t$ sont saturées. On conclut alors grâce au corollaire 7.2 et au théorème 6.1. □

8.3 REMARQUE. Ce théorème nous donne, dans ce cas particulier, un critère simple d'isométrie des B-réseaux. Il nous montre que les difficultés dans la classification des B-réseaux de type (t,r,s) provient essentiellement des relations qu'il peut y avoir entre les réseaux $L_1, \ldots, L_t$ d'une décomposition de Jordan lorsque les s_i sont trop proches les uns des autres.

Rappelons quelques notations du paragraphe précédent : on note $P = P(t,r,s)$ (resp. $I = I(t,r,s)$) le nombre d'entiers $1 \leqslant i \leqslant t$ tels que r_i et s_i sont pairs (resp. r_i est pair et s_i impair).

8.4 COROLLAIRE. *Soit (t,r,s) un triplet de Jordan tel que $\mathcal{C}(t,r,s,) \neq \emptyset$. Supposons que $s_{i+1} - s_i \geqslant v_E(4) + 1$ pour tout $1 \leqslant i \leqslant t-1$. Alors :*

(i) Dans le cas R-P *on a* $\big|\mathcal{C}(t,r,s)\big| = 2^{t-P-I} \cdot \big(v_E(2)+2\big)^P \cdot \big(v_E(2)+1\big)^I$.

(ii) Dans le cas R-U_k *on a* $\big|\mathcal{C}(t,r,s)\big| = 2^{t-P-I} \cdot \big(v_E(2)-2k+1\big)^P \cdot \big(v_E(2)-2k\big)^I$.

Preuve. Considérons $\Phi : \prod_{1 \leqslant j \leqslant t} \mathcal{C}\big(1,(r_i),(s_i)\big) \to \mathcal{C}(t,r,s)$ définie par $\Phi\big(L_1,\ldots,L_t\big) =$ $= L_1 \perp \cdots \perp L_t$. Le théorème 8.2 nous dit que Φ est une bijection. On peut alors conclure grâce au théorème 6.5 et aux corollaires 6.8 et 6.10. □

Calculons finalement $\big|\mathcal{C}_\lambda(t,r,s)\big|$ pour $\lambda \in \{\pm 1\}$.

8.5 PROPOSITION. *Soient (t,r,s) un triplet de Jordan tel que $\mathcal{C}(t,r,s,) \neq \emptyset$ et $\lambda \in \{\pm 1\}$. Supposons que $s_{i+1} - s_i \geqslant v_E(4) + 1$ pour tout $1 \leqslant i \leqslant t-1$. Alors :*

(i) Plaçons-nous dans le cas où l'extension E/K est ramifiée première.
Si $I < t$, on a $\big|\mathcal{C}_\lambda(t,r,s)\big| = 2^{t-P-I-1} \cdot \big(v_E(2)+2\big)^P \cdot \big(v_E(2)+1\big)^I$.
Si $I = t$, alors $\big|\mathcal{C}_\lambda(t,r,s)\big| = \frac{1}{2}\big((v_E(2)+1)^I - 1\big) + \alpha$ *où $\alpha \in \{0,1\}$ avec $\alpha = 1$ si et seulement si* $\lambda = \big(-1, E/K\big)^{\frac{1}{2}(r_1+\cdots+r_t)}$.

(ii) Plaçons-nous dans le cas où l'extension E/K est ramifiée unitaire.
Si $P < t$, on a $\big|\mathcal{C}_\lambda(t,r,s)\big| = 2^{t-P-I-1} \cdot \big(v_E(2)-2k+1\big)^P \cdot \big(v_E(2)-2k\big)^I$.
Si $P = t$, alors $\big|\mathcal{C}_\lambda(t,r,s)\big| = \frac{1}{2}\big((v_E(2)-2k+1)^P - 1\big) + \alpha$ *où $\alpha \in \{0,1\}$ avec $\alpha = 1$ si et seulement si* $\lambda = \big(-1, E/K\big)^{\frac{1}{2}(r_1+\cdots+r_t)}$.

Preuve. Les deux assertions se prouvant de la même manière, nous ne démontrerons que la première.
Soit $1 \leqslant i \leqslant t$. Notons $\widetilde{\mathcal{C}}^i_\lambda(t,r,s)$ l'ensemble des classes de réseaux L de type fondamental (t,r,s,n) avec n_i non maximal vérifiant $\big(\mathrm{d}L, E/K\big) = \lambda$. Soit $\overline{\mathcal{C}}^i_\lambda(t,r,s)$ le complémentaire

de $\widetilde{\mathcal{C}}^i_\lambda(t,r,s)$ dans $\mathcal{C}_\lambda(t,r,s)$, $C(r_i,s_i) = \{\, n \in 2\mathbb{Z} \mid s_i \leqslant n \leqslant s_i + v_E(2) \,\}$ si r_i est pair et $C(r_i,s_i) = \{\, s_i \,\}$ si r_i est impair et donc, grâce au théorme 6.5, s_i est pair.
Posons $t' = t-1$, $r' = (r_1,\dots,r_{i-1},r_{i+1},\dots,r_t)$ et $s' = (s_1,\dots,s_{i-1},s_{i+1},\dots,s_t)$.

Le théorème 8.2 permet de définir une application $\Phi : \widetilde{\mathcal{C}}^i_\lambda(t,r,s) \to \mathcal{C}(t',r',s') \times C(r_i,s_i)$ par $\Phi\big(L_1 \perp \cdots \perp L_t\big) = \big(L_1 \perp \cdots \perp L_{i-1} \perp L_{i+1} \perp \cdots \perp L_t, v_E(\mathcal{N}L_i)\big)$.

Montrons que Φ est bijective.

Soient L et L' deux réseaux de $\widetilde{\mathcal{C}}^i_\lambda(t,r,s)$ avec $\Phi(L) \simeq \Phi(L')$. Soient $L_1,\dots,L_t$ et $L'_1,\dots,L'_t$ des décompositions de Jordan respectives de L et L'. Il est alors clair par définition que $L_1 \perp \cdots \perp L_{i-1} \perp L_{i+1} \perp \cdots \perp L_t \simeq L'_1 \perp \cdots \perp L'_{i-1} \perp L'_{i+1} \perp \cdots \perp L'_t$ et donc, comme $\mathrm{d}L = \mathrm{d}L' = \lambda$, que $\mathrm{d}L_i = \mathrm{d}L'_i$. D'autre part, on a $v_E(\mathcal{N}L_i) = v_E(\mathcal{N}L'_i)$ de sorte que $L_i \simeq L'_i$ grâce au théorème 6.1. Ainsi $L \simeq L'$ et Φ est injective.

Soient L un réseau de $\mathcal{C}(t',r',s')$ et $n \in C(r_i,s_i)$. Comme n_i est non maximal, les théorèmes 6.5 et 6.7 nous assurent l'existence d'un réseau J p^{s_i}-modulaire de norme p^nB tel que $\big(\mathrm{d}J, {}^E\!/_K\big) = \lambda \cdot \big(\mathrm{d}L, {}^E\!/_K\big)$. Il est clair que $L \perp J$ est un réseau de $\widetilde{\mathcal{C}}^i_\lambda(t,r,s)$ tel que $\Phi\big(L \perp J\big) = \big(L,n\big)$ ce qui prouve que Φ est surjective.

Supposons maintenant que $I < t$. Choisissons $1 \leqslant i \leqslant t$ avec r_i impair ou s_i pair. Il est alors clair que $\mathcal{C}_\lambda(t,r,s) = \widetilde{\mathcal{C}}^i_\lambda(t,r,s)$. On a ainsi $|\mathcal{C}_\lambda(t,r,s)| = |\mathcal{C}(t',r',s')| \cdot |C(r_i,s_i)|$ et il suffit alors d'utiliser le corollaire 8.4 en distingant les cas $i \in P$ et $i \notin P$ pour conclure.

Supposons finalement que $I = t$. Prouvons la formule par récurrence sur t.

Si $t = 1$, le résultat découle du théorème 6.7. Supposons $t > 1$.

Choisissons $i = t$. Alors $\mathcal{C}_\lambda(t,r,s)$ est la réunion disjointe de $\overline{\mathcal{C}}^t_\lambda(t,r,s)$ et $\widetilde{\mathcal{C}}^t_\lambda(t,r,s)$. Posons $\lambda' = \big(-1, {}^E\!/_K\big)^{\frac{r_t}{2}}\lambda$. On vérifie aisément que l'application $\Psi : \overline{\mathcal{C}}^t_\lambda(t,r,s) \to \mathcal{C}_{\lambda'}(t',r',s')$ définie par $\Psi\big(L_1 \perp \cdots \perp L_t\big) = \big(L_1 \perp \cdots \perp L_{t-1}\big)$ est une bijection de sorte que, par hypothèse de récurrence, on a $|\overline{\mathcal{C}}^t_\lambda(t,r,s)| = |\mathcal{C}_{\lambda'}(t',r',s')| = \frac{1}{2}\big((v_E(2)+1)^{t-1}-1\big) + \alpha$ où $\alpha \in \{\pm 1\}$ avec $\alpha = 1$ si et seulement si $\lambda' = \big(-1, {}^E\!/_K\big)^{\frac{1}{2}(r_1+\cdots+r_{t-1})}$, en d'autres termes si et seulement si $\lambda = \big(-1, {}^E\!/_K\big)^{\frac{1}{2}(r_1+\cdots+r_t)}$. D'autre part, vu la première partie de la preuve, on sait que $|\widetilde{\mathcal{C}}^t_\lambda(t,r,s)| = |\mathcal{C}(t',r',s')| \cdot |C(r_t,s_t)| = (v_E(2)+1)^{t-1} \cdot \frac{1}{2}v_E(2)$.

Finalement $|\mathcal{C}_\lambda(t,r,s)| = (v_E(2)+1)^{t-1} \cdot \frac{1}{2}v_E(2) + \frac{1}{2}\big((v_E(2)+1)^{t-1}-1\big) + \alpha =$
$= \frac{1}{2}(v_E(2)+1)^{t-1} \cdot (v_E(2)+1) - \frac{1}{2} + \alpha = \frac{1}{2}\big((v_E(2)+1)^t - 1\big) + \alpha.$ □

Chapitre 4
Genres, facteurs invariants et signatures

Dans ce chapitre, nous essayerons de voir dans quelle mesure les facteurs invariants et les signatures d'un réseau détermine son genre et plus précisément de compter le nombre de genres dont les réseaux possèdent des facteurs invariants et des signatures donnés.

Soient K un corps de nombres dont A est l'anneau des entiers, E une extension quadratique de K et B la clôture intégrale de A dans E. Alors B est l'anneau des entiers de E. Il existe $\theta \in K$ non carré tel que $E = K(\sqrt{\theta})$. L'unique élément non trivial σ du groupe de Galois de l'extension $^{E}/_{K}$ est alors donné par $\sigma(x + y\sqrt{\theta}) = x - y\sqrt{\theta}$.

§ 1. Vers un système d'invariants pour les genres

Le lemme suivant découle directement du paragraphe 4 du chapitre 3 et du corollaire 1.3 du chapitre 2 :

1.1 LEMME. *Soient (L, h) et (M, k) deux B-réseaux et $\mathfrak{p}$ une place finie non ramifiée de K. Alors $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (M_\mathfrak{p}, k_\mathfrak{p})$ si et seulement si $(L_\mathfrak{p}, h_\mathfrak{p})$ et $(M_\mathfrak{p}, k_\mathfrak{p})$ ont les mêmes facteurs invariants.* □

1.2 THÉORÈME. *Soient (L, h) et (M, k) deux B-réseaux. Alors (L, h) et (M, k) sont dans le même genre si et seulement si les trois conditions suivantes sont satisfaites :*

(i) (L, h) *et* (M, k) *ont mêmes facteurs invariants.*

(ii) (L, h) *et* (M, k) *ont mêmes signatures.*

(iii) $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (M_\mathfrak{p}, k_\mathfrak{p})$ *pour toute place ramifiée* $\mathfrak{p}$ *de* K.

Preuve. Observons tout d'abord que, par la proposition 1.1 du chapitre 2, on a toujours $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (M_\mathfrak{p}, k_\mathfrak{p})$ pour toute place infinie $\mathfrak{p}$ avec $\mathfrak{p} \notin \mathcal{J}$. D'autre part, vu le lemme 1.1, l'assertion (i) est équivalente à dire que $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (M_\mathfrak{p}, k_\mathfrak{p})$ pour toute place finie non ramifiée $\mathfrak{p}$ de K. Finalement, grâce au corollaire 2.3 du chapitre 2, l'assertion (ii) revient à dire que $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (M_\mathfrak{p}, k_\mathfrak{p})$ pour toute place $\mathfrak{p} \in \mathcal{J}$. □

En utilisant le théorème 1.2 ci-dessus, et le corollaire 4.4 du chapitre 2, on obtient :

1.3 COROLLAIRE. *Soient (L, h) et (M, k) deux B-réseaux. Alors (L, h) et (M, k) sont dans le même genre si et seulement si les trois conditions suivantes sont satisfaites :*

(i) $(L \otimes_B E, h \otimes_B E) \simeq (M \otimes_B E, k \otimes_B E)$

(ii) (L, h) *et* (M, k) *ont mêmes facteurs invariants*

(iii) $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (M_\mathfrak{p}, k_\mathfrak{p})$ *pour toute place ramifiée* $\mathfrak{p}$ *de* K. □

Le lemme suivant est essentiel ; il est prouvé dans [7], 81:14 :

1.4 LEMME. *Soit V un E-espace vectoriel de dimension finie. Considérons pour toute place finie $\mathfrak{P}$ de E un sous $B_\mathfrak{P}$-module $L_{(\mathfrak{P})}$ de type fini de $V \otimes_E E_\mathfrak{P}$ tel que $L_{(\mathfrak{P})} \otimes_{B_\mathfrak{P}} E_\mathfrak{P} = V \otimes_E E_\mathfrak{P}$. Les conditions suivantes sont équivalentes :*

(i) Il existe un sous B-module de type fini L de V tel que $L \otimes_B B_\mathfrak{P} = L_{(\mathfrak{P})}$ pour toute place finie $\mathfrak{P}$ de E.

(ii) Il existe une partie cofinie Ω de places finies de E et un sous B-module de type fini L de V tel que $L \otimes_B B_\mathfrak{P} = L_{(\mathfrak{P})}$ pour tout $\mathfrak{P} \in \Omega$. □

1.5 THÉORÈME. *Soit n un entier strictement positif. Considérons pour toute place $\mathfrak{p}$ de K un $(B \otimes_A A_\mathfrak{p})$-réseau $(L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ de rang n. Alors, il existe un B-réseau (L, h) tel que $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ pour toute place $\mathfrak{p}$ de K si et seulement si les deux conditions suivantes sont satisfaites :*

(i) Il existe une partie cofinie Ω de places finies de K telle que pour tout $\mathfrak{p} \in \Omega$ le réseau $(L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ soit unimodulaire et $\left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = 1$.

(ii) On a $\prod_\mathfrak{p} \left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = 1$.

Preuve. Supposons l'existence d'un B-réseau (L, h) avec $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ pour toute place $\mathfrak{p}$ de K. Les deux assertions résultent de la proposition 7.5 du chapitre 1 ainsi que de la proposition 4.5 du chapitre 1.

Supposons maintenant les assertions (i) et (ii) vérifiées. Vu le corollaire 5.3 du chapitre 2, il existe un espace hermitien (V, h) sur E tel que $\mathrm{d}V_\mathfrak{p} = \mathrm{d}L_{(\mathfrak{p})}$ pour toute place $\mathfrak{p}$ de K et dont les signatures sont $I(L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ pour toute place $\mathfrak{p} \in \mathcal{J}$.

Soit M un sous B-module de type fini de V avec $M \otimes_B E = V$. La proposition 7.5 du chapitre 1 nous dit qu'il existe une partie cofinie Ω' de places finies de K telles que $(M_\mathfrak{p}, h_\mathfrak{p})$ soit unimodulaire pour tout $\mathfrak{p} \in \Omega'$. Soit Γ l'ensemble des places finies non ramifiées de K qui sont dans $\Omega \cap \Omega'$. Alors, grâce au lemme 1.1, on a $(L_{(\mathfrak{p})}, h_{(\mathfrak{p})}) \simeq (M_\mathfrak{p}, h_\mathfrak{p})$ pour toute place $\mathfrak{p} \in \Gamma$.

Soit $\mathfrak{p}$ une place finie de K. Si $\mathfrak{p} \notin \Gamma$, il existe, grâce aux propositions 1.1 et 3.1 du chapitre 2, un sous $(B \otimes_A A_\mathfrak{p})$-module $M_{(\mathfrak{p})}$ de type fini de $V_\mathfrak{p}$ tel que $(M_{(\mathfrak{p})}, h_\mathfrak{p}) \simeq (L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$. Si $\mathfrak{p} \in \Gamma$, posons $M_{(\mathfrak{p})} = M_\mathfrak{p}$. On a ainsi $(M_{(\mathfrak{p})}, h_\mathfrak{p}) \simeq (L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ pour toute place finie $\mathfrak{p}$ de K.

Soit $\mathfrak{P}$ une place finie de E. Soit $\mathfrak{p}$ l'unique place finie de K telle que $\mathfrak{P}|\mathfrak{p}$. Posons $N_{(\mathfrak{P})} = M_{(\mathfrak{p})} \otimes_{(B \otimes_A A_\mathfrak{p})} B_\mathfrak{P}$. Alors $N_{(\mathfrak{P})} = \big(M \otimes_B (B \otimes_A A_\mathfrak{p})\big) \otimes_{(B \otimes_A A_\mathfrak{p})} B_\mathfrak{P} = M \otimes_B B_\mathfrak{P}$ pour tout $\mathfrak{p} \in \Gamma$, et l'ensemble des places finies $\mathfrak{P}$ de E telles que $\mathfrak{p} \notin \Gamma$ est fini. Ainsi, grâce au lemme 1.4, il existe un sous B-module de type fini L de V tel que $L \otimes_B B_\mathfrak{P} = N_{(\mathfrak{P})}$ pour toute place $\mathfrak{P}$ de E.

Alors (L,h) est le B-réseau cherché. En effet, soit $\mathfrak{p}$ une place de K.

Supposons $\mathfrak{p}$ infinie. Alors $L_\mathfrak{p} = V_\mathfrak{p}$ et l'isométrie entre $L_\mathfrak{p}$ et $L_{(\mathfrak{p})}$ résulte du corollaire 2.3 ou de la proposition 1.1, tous deux du chapitre 2, selon que $\mathfrak{p} \in \mathcal{J}$ ou non.

Supposons $\mathfrak{p}$ finie décomposée. Notons $\mathfrak{P}_1$ et $\mathfrak{P}_2$ les places de B au-dessus $\mathfrak{p}$. Alors $L_\mathfrak{p} = L \otimes_B (B \otimes_A A_\mathfrak{p}) = L \otimes_B (B_{\mathfrak{P}_1} \oplus B_{\mathfrak{P}_1}) = (L \otimes_B B_{\mathfrak{P}_1}) \oplus (L \otimes_B B_{\mathfrak{P}_2}) = N_{(\mathfrak{P}_1)} \oplus N_{(\mathfrak{P}_2)} = (M_{(\mathfrak{p})} \otimes_{(B \otimes_A A_\mathfrak{p})} B_{\mathfrak{P}_1}) \oplus (M_{(\mathfrak{p})} \otimes_{(B \otimes_A A_\mathfrak{p})} B_{\mathfrak{P}_2}) = M_{(\mathfrak{p})} \otimes_{(B \otimes_A A_\mathfrak{p})} (B_{\mathfrak{P}_1} \oplus B_{\mathfrak{P}_2}) = M_{(\mathfrak{p})}$.

Supposons $\mathfrak{p}$ finie non décomposée. Notons $\mathfrak{P}$ l'unique place de E au-dessus de $\mathfrak{p}$. Alors $L_\mathfrak{p} = L \otimes_B (B \otimes_A A_\mathfrak{p}) = L \otimes_B B_\mathfrak{P} = N_{(\mathfrak{P})} = M_{(\mathfrak{p})} \otimes_{(B \otimes_A A_\mathfrak{p})} B_\mathfrak{P} = M_{(\mathfrak{p})}$.

Finalement, on obtient $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$. □

1.6 COROLLAIRE. *Soient $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ une suite décroissante d'idéaux fractionnaires de B avec $v_\mathfrak{p}(\mathfrak{r}_i \otimes_A A_\mathfrak{p}) \in \Delta(\mathbb{Z})$ pour toute place finie décomposée $\mathfrak{p}$ et $(a_\mathfrak{p}, b_\mathfrak{p})_{\mathfrak{p} \in \mathcal{J}}$ une famille de couple d'entiers positifs avec $a_\mathfrak{p} + b_\mathfrak{p} = n$. Considérons pour toute place finie ramifiée $\mathfrak{p}$ de K un $(B \otimes_A A_\mathfrak{p})$-réseau $(L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ de facteurs invariants $\mathfrak{r}_1 \otimes_A A_\mathfrak{p} \supset \cdots \supset \mathfrak{r}_n \otimes_A A_\mathfrak{p}$. Alors les conditions suivantes sont équivalentes :*

(i) Il existe un B-réseau (L,h) de facteurs invariants $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$, de signatures $(a_\mathfrak{p}, b_\mathfrak{p})_{\mathfrak{p} \in \mathcal{J}}$ et tel que $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ pour toute place $\mathfrak{p}$ ramifiée.

(ii) On a $\displaystyle\prod_{\mathfrak{p} \in \mathcal{R}} \left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = \prod_{\mathfrak{p} \in \mathcal{I}} (-1)^{v_\mathfrak{p}(\mathfrak{r}_1) + \cdots + v_\mathfrak{p}(\mathfrak{r}_n)} \cdot \prod_{\mathfrak{p} \in \mathcal{J}} (-1)^{b_\mathfrak{p}}.$

Preuve. Vu le théorème 4.2 du chapitre 3 et la proposition 1.4 du chapitre 2, il existe pour toute place finie non ramifiée $\mathfrak{p}$ un unique $(B \otimes_A A_\mathfrak{p})$-réseau $(L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ dont les facteurs invariants sont $\mathfrak{r}_1 \otimes_A A_\mathfrak{p} \supset \cdots \supset \mathfrak{r}_n \otimes_A A_\mathfrak{p}$. On a alors $\left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = 1$ si $\mathfrak{p}$ se décompose et $\left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = (-1)^{v_\mathfrak{p}(\mathfrak{r}_1) + \cdots + v_\mathfrak{p}(\mathfrak{r}_n)}$ si $\mathfrak{p}$ est inerte.
D'autre part, vu le corollaire 2.3 du chapitre 2, il existe pour tout $\mathfrak{p} \in \mathcal{J}$ un unique $(B \otimes_A A_\mathfrak{p})$-réseau $(L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ de signature $(a_\mathfrak{p}, b_\mathfrak{p})$. On a alors $\left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = (-1)^{b_\mathfrak{p}}$.
Grâce à la proposition 1.1 du chapitre 2, on peut considérer finalement, pour toute place infinie décomposée $\mathfrak{p}$, l'unique $(B \otimes_A A_\mathfrak{p})$-réseau de rang n que l'on note $(L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$. Il est clair que $\left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = 1$.
On remarque alors aisément que l'assertion (i) revient à supposer qu'il existe un B-réseau (L,h) avec $(L_\mathfrak{p}, h_\mathfrak{p}) \simeq (L_{(\mathfrak{p})}, h_{(\mathfrak{p})})$ pour toute place $\mathfrak{p}$ de K.
D'autre part, l'assertion (ii) est équivalente à supposer que $\displaystyle\prod_\mathfrak{p} \left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = 1$.

On conclut alors grâce au théorème 1.5. □

§ 2. Nombre de genres de facteurs invariants et de signatures donnés

Introduisons quelques définitions et notations supplémentaires.

Soit $\mathfrak{r}$ une suite décroissante $\mathfrak{r}_1 \supset \cdots \supset \mathfrak{r}_n$ d'idéaux fractionnaires de B.
Remarquons, en utilisant la proposition 1.4 du chapitre 2, qu'il n'y a aucun B-réseau de facteurs invariants $\mathfrak{r}$ s'il existe $1 \leqslant i \leqslant n$ et une place finie décomposée $\mathfrak{p}$ de K telle que $v_\mathfrak{p}(\mathfrak{r}_i \otimes_A A_\mathfrak{p}) \notin \Delta(\mathbb{Z})$.
Nous dirons alors que $\mathfrak{r}$ est une *suite adéquate* de B si l'on a $v_\mathfrak{p}(\mathfrak{r}_i \otimes_A A_\mathfrak{p}) \in \Delta(\mathbb{Z})$ pour tout $1 \leqslant i \leqslant n$ et pour toute place $\mathfrak{p}$ finie et décomposée de K.

Soit $\mathfrak{r}$ une suite adéquate de B.
Si $\mathfrak{p}$ est une place finie non décomposée de K, nous noterons $\mathfrak{r}_\mathfrak{p}$ le triplet de Jordan (t, r, s) déterminé par la suite décroissante $\mathfrak{r}_1 \otimes_A A_\mathfrak{p} \supset \cdots \supset \mathfrak{r}_n \otimes_A A_\mathfrak{p}$ de la manière suivante : définissons t et s en écrivant $\{v_\mathfrak{p}(\mathfrak{r}_1), \ldots, v_\mathfrak{p}(\mathfrak{r}_n)\} = \{s_1, \ldots, s_t\}$ avec $s_1 < \cdots < s_t$ et posons $r_j = \big|\{1 \leqslant i \leqslant n \mid s_j = v_\mathfrak{p}(\mathfrak{r}_i)\}\big|$ pour tout $1 \leqslant j \leqslant t$.
Vu le paragraphe 2 du chapitre 3, il est clair qu'un $(B \otimes_A A_\mathfrak{p})$-réseau est de type $\mathfrak{r}_\mathfrak{p}$ si et seulement si ses facteurs invariants sont $\mathfrak{r}_1 \otimes_A A_\mathfrak{p} \supset \cdots \supset \mathfrak{r}_n \otimes_A A_\mathfrak{p}$.

Nous appellerons *famille de signatures* de K toute famille $\Sigma = (a_\mathfrak{p}, b_\mathfrak{p})_{\mathfrak{p} \in \mathcal{J}}$ de couples d'entiers positifs avec $a_\mathfrak{p} + b_\mathfrak{p} = n$.

Soient $\mathfrak{r}$ une suite adéquate de B et Σ une famille de signature de K.

On note $\mathcal{G}(\mathfrak{r}, \Sigma)$ l'ensemble de tous les genres des B-réseaux possédant les facteurs invariants $\mathfrak{r}$ et les signatures Σ. Nous allons déterminer le cardinal de $\mathcal{G}(\mathfrak{r}, \Sigma)$. Mais avant cela, nous avons encore besoin de quelques notations techniques.
Posons $\lambda_\mathfrak{r} = \prod_{\mathfrak{p} \in \mathcal{I}} (-1)^{v_\mathfrak{p}(\mathfrak{r}_1) + \cdots + v_\mathfrak{p}(\mathfrak{r}_n)}$ et $\lambda_\Sigma = \prod_{\mathfrak{p} \in \mathcal{J}} (-1)^{b_\mathfrak{p}}$.

Rappelons que l'on note $\mathcal{R}$ l'ensemble des places de K ramifiées dans E/K.
Si $\lambda \in \{\pm 1\}$, nous poserons $\Omega(\lambda) = \big\{f \in \{\pm 1\}^\mathcal{R} \mid \prod_{\mathfrak{p} \in \mathcal{R}} f(\mathfrak{p}) = \lambda\big\}$.
Supposons $\mathcal{R} = \emptyset$; remarquons que $\Omega(\lambda)$ contient l'application vide si $\lambda = 1$ alors que $\Omega(\lambda) = \emptyset$ sinon.

Finalement, nous noterons $\mathcal{C}^\mathfrak{p}(\mathfrak{r}_\mathfrak{p})$ l'ensemble des classes d'isométrie des $B_\mathfrak{p}$-réseaux de type $\mathfrak{r}_\mathfrak{p}$ alors que $\mathcal{C}^\mathfrak{p}_\lambda(\mathfrak{r}_\mathfrak{p})$ sera l'ensemble des classes d'isométrie des $B_\mathfrak{p}$-réseaux de type $\mathfrak{r}_\mathfrak{p}$ et de discriminant d vérifiant $\big(d, E/K\big)_\mathfrak{p} = \lambda$.

2.1 THÉORÈME. *Soient $\mathfrak{r}$ une suite adéquate de B et Σ une famille de signatures de K. Alors l'ensemble $\mathcal{G}(\mathfrak{r}, \Sigma)$ est fini et l'on a*

$$\big|\mathcal{G}(\mathfrak{r}, \Sigma)\big| = \sum_{f \in \Omega(\lambda_\mathfrak{r} \lambda_\Sigma)} \left(\prod_{\mathfrak{p} \in \mathcal{R}} \big|\mathcal{C}^\mathfrak{p}_{f(\mathfrak{p})}(\mathfrak{r}_\mathfrak{p})\big| \right).$$

Preuve. Posons $\Omega = \Omega(\lambda_\mathfrak{r} \lambda_\Sigma)$. Pour tout $f \in \Omega$, notons $\mathcal{A}(f)$ l'ensemble des genres des B-réseaux (L, h) de $\mathcal{G}(\mathfrak{r}, \Sigma)$ avec $f(\mathfrak{p}) = \big(\mathrm{d}L_\mathfrak{p}, E/K\big)_\mathfrak{p}$ pour tout $\mathfrak{p} \in \mathcal{R}$.
Remarquons que $\mathcal{G}(\mathfrak{r}, \Sigma)$ est la réunion disjointe des $\mathcal{A}(f)$ lorsque f parcourt Ω. En effet, il est clair que $\mathcal{A}(f) \cap \mathcal{A}(g) = \emptyset$ lorsque $f \neq g$. Considérons un réseau (L, h) de $\mathcal{G}(\mathfrak{r}, \Sigma)$. Soit $\mathfrak{p}$ une place non ramifiée de K. Si $\mathfrak{p} \in \mathcal{I}$, alors, vu le théorème 4.2 du chapitre 3, on a $\big(\mathrm{d}L_\mathfrak{p}, E/K\big)_\mathfrak{p} = (-1)^{v_\mathfrak{p}(\mathfrak{r}_1) + \cdots + v_\mathfrak{p}(\mathfrak{r}_n)}$. Si $\mathfrak{p} \in \mathcal{J}$, alors $\big(\mathrm{d}L_\mathfrak{p}, E/K\big)_\mathfrak{p} = (-1)^{b_\mathfrak{p}}$. Dans tous les autres cas, on a $\big(\mathrm{d}L_\mathfrak{p}, E/K\big)_\mathfrak{p} = 1$.
Finalement, définissons $f \in \{\pm 1\}^\mathcal{R}$ en posant $f(\mathfrak{p}) = \big(\mathrm{d}L_\mathfrak{p}, E/K\big)_\mathfrak{p}$ pour tout $\mathfrak{p} \in \mathcal{R}$. Vu la formule du produit de Hilbert, on a $f \in \Omega$. Ainsi (L, h) est un réseau de $\mathcal{A}(f)$.
En résumé, nous avons montré que $\big|\mathcal{G}(\mathfrak{r}, \Sigma)\big| = \sum_{f \in \Omega} \big|\mathcal{A}(f)\big|$.

Soit $f \in \Omega$. Calculons $\big|\mathcal{A}(f)\big|$.
Considérons l'application $\Phi : \mathcal{A}(f) \to \prod_{\mathfrak{p} \in \mathcal{R}} \mathcal{C}^\mathfrak{p}_{f(\mathfrak{p})}(\mathfrak{r}_\mathfrak{p})$ définie par $\Phi(L, h) = \big((L_\mathfrak{p}, h_\mathfrak{p})\big)_{\mathfrak{p} \in \mathcal{R}}$.

Montrons que Φ est injective. Soient (L,h) et (L',h') deux réseaux de $\mathcal{A}(f)$ tels que $(L_\mathfrak{p},h_\mathfrak{p}) \simeq (L'_\mathfrak{p},h'_\mathfrak{p})$ pour toute place $\mathfrak{p} \in \mathcal{R}$. Par définition, L et L' ont mêmes facteurs invariants et mêmes signatures en toute place $\mathfrak{p} \in \mathcal{J}$. Comme $(L_\mathfrak{p},h_\mathfrak{p}) \simeq (L'_\mathfrak{p},h'_\mathfrak{p})$ pour toute place ramifiée $\mathfrak{p}$, le théorème 1.2 nous dit alors que (L,h) et (L',h') sont dans le même genre.

Montrons que Φ est surjective. Considérons pour tout $\mathfrak{p} \in \mathcal{R}$ un $(B \otimes_A A_\mathfrak{p})$-réseau $(L_{(\mathfrak{p})},h_{(\mathfrak{p})})$ de facteurs invariants $\mathfrak{r}_\mathfrak{p}$ et tel que $\left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = f(\mathfrak{p})$. Alors, par définition de f, on a $\prod_{\mathfrak{p}\in\mathcal{R}} \left(\mathrm{d}L_{(\mathfrak{p})}, {}^{E}\!/_{K}\right)_\mathfrak{p} = \lambda_\mathfrak{r}\lambda_\Sigma$ et on conclut grâce au corollaire 1.6.

On a finalement $\left|\mathcal{A}(f)\right| = \prod_{\mathfrak{p}\in\mathcal{R}} \left|\mathcal{C}^\mathfrak{p}_{f(\mathfrak{p})}(\mathfrak{r}_\mathfrak{p})\right|$. □

Donnons quelques approximations de cette formule :

2.2 PROPOSITION. *Soient* $\mathfrak{r}$ *une suite adéquate de* B *et* Σ *une famille de signatures de* K. *Alors*

$$\left|\mathcal{G}(\mathfrak{r},\Sigma)\right| \leqslant \prod_{\mathfrak{p}\in\mathcal{R}} \left|\mathcal{C}^\mathfrak{p}(\mathfrak{r}_\mathfrak{p})\right|.$$

Preuve. Considérons l'application $\Phi : \mathcal{G}(\mathfrak{r},\Sigma) \to \prod_{\mathfrak{p}\in\mathcal{R}} \mathcal{C}^\mathfrak{p}(\mathfrak{r}_\mathfrak{p})$ définie par $\Phi\big((L,h)\big) = \big((L_\mathfrak{p},h_\mathfrak{p})\big)_{\mathfrak{p}\in\mathcal{R}}$. Le théorème 1.2 nous assure que Φ est injective, ce qui nous permet de conclure. □

Les deux formules ci-dessus sont difficilement applicables pour des calculs généraux. Pour en donner une approximation plus calculable, il faut introduire beaucoup plus de notations.

Soit $\mathfrak{r}$ une suite adéquate de B et $\mathfrak{p}$ une place ramifiée de K. Notons (t,r,s) le triplet de Jordan $\mathfrak{r}_\mathfrak{p}$ et posons $t_\mathfrak{p}(\mathfrak{r}) = t$.

Si $\mathfrak{p}$ est dyadique, notons $R_\mathfrak{p}(\mathfrak{r})$ le nombre d'entiers $1 \leqslant i \leqslant i$ tels que r_i sont pairs et $S_\mathfrak{p}(\mathfrak{r})$ le nombre d'entiers $1 \leqslant i \leqslant t$ tels que s_i est pair.

Notons $\mathcal{R}_1$ l'ensemble des places ramifiées non dyadiques, $\mathcal{R}_2$ l'ensemble des places ramifiées dyadiques premières et $\mathcal{R}_3$ l'ensemble des places ramifiées dyadiques unitaires. Pour tout $\mathfrak{p} \in \mathcal{R}_3$, soit $k_\mathfrak{p} \in \mathbb{Z}$ tel que $\theta_\mathfrak{p}$ soit de défaut quadratique $\mathfrak{p}^{2k_\mathfrak{p}+1}$.

2.3 THÉORÈME. *Soient* $\mathfrak{r}$ *une suite adéquate de* B *et* Σ *une famille de signatures de* K. *Alors*

$$\left|\mathcal{G}(\mathfrak{r},\Sigma)\right| \leqslant 2^{|\mathcal{R}|-1} \prod_{\mathfrak{p}\in\mathcal{R}_1} 2^{\max(0,S_\mathfrak{p}(\mathfrak{r})-1)} \cdot \prod_{\mathfrak{p}\in\mathcal{R}_2} 2^{t_\mathfrak{p}(\mathfrak{r})-1}\left(v_\mathfrak{p}(2)+1\right)^{R_\mathfrak{p}(\mathfrak{r})} \cdot \prod_{\mathfrak{p}\in\mathcal{R}_3} 2^{t_\mathfrak{p}(\mathfrak{r})-1}\left(v_\mathfrak{p}(2)-k_\mathfrak{p}+1\right)^{R_\mathfrak{p}(\mathfrak{r})}.$$

Preuve. Reprenons les notations du théorème 2.1. Rappelons que $\mathcal{G}(\mathfrak{r},\Sigma) = \bigsqcup_{f\in\Omega} \mathcal{A}(f)$ et que $\left|\mathcal{A}(f)\right| = \prod_{\mathfrak{p}\in\mathcal{R}} \left|\mathcal{C}^\mathfrak{p}_{f(\mathfrak{p})}(\mathfrak{r}_\mathfrak{p})\right|$. On utilise ensuite le corollaire 5.5 et la proposition 7.10, tous deux du chapitre 3, pour borner $\left|\mathcal{A}(f)\right|$ indépendemment de $f \in \Omega$ et on conclut en observant que $|\Omega| = 2^{|\mathcal{R}|-1}$. □

§ 3. Formules pour le nombre de genres dans quelques cas particuliers

Dans ce paragraphe, nous reprenons les notations des paragraphes précédents.
Nous allons donner une formule d'expression plus simple dans certains cas particuliers.
Nous supposerons tout d'abord qu'aucune place finie ne ramifie dans l'extension $^E/_K$. Nous pouvons alors énoncer :

3.1 THÉORÈME. *Soit $^E/_K$ une extension quadratique de corps de nombres telle qu'aucune place finie ne ramifie. Soient $\mathfrak{r}$ une suite adéquate de B et Σ une famille de signatures de K.*

(i) On a $\big|\mathcal{G}(\mathfrak{r},\Sigma)\big| \leqslant 1$. En particulier, deux réseaux sont dans le même genre si et seulement s'ils ont mêmes facteurs invariants et signatures.

(ii) On a $\big|\mathcal{G}(\mathfrak{r},\Sigma)\big| = 1$ si et seulement si $\lambda_{\mathfrak{r}} = \lambda_\Sigma$.

Preuve. L'assertion (i) découle du théorème 1.2 alors que (ii) n'est qu'un cas particulier du corollaire 1.6. □

Supposons ensuite qu'un seul premier ne ramifie dans l'extension $^E/_K$.
Le résultat ci-dessous est un corollaire du théorème 2.1 :

3.2 PROPOSITION. *Soit $^E/_K$ une extension de corps de nombres telle qu'une seule place finie $\mathfrak{p}$ ramifie. Soient $\mathfrak{r}$ une suite adéquate de B et Σ une famille de signature de K. Alors*

$$\big|\mathcal{G}(\mathfrak{r},\Sigma)\big| = \big|\mathcal{C}^{\mathfrak{p}}_{\lambda_{\mathfrak{r}}\lambda_\Sigma}(\mathfrak{r}_{\mathfrak{p}})\big|. \qquad \square$$

Annexe 1
Un outil de calcul : le déterminant d'un réseau

Nous reprenons les notations et hypothèses du chapitre 4.

Dans cette première annexe, nous allons considérer des B-réseaux libres définis par une matrice hermitienne et montrer que l'idéal engendré par le déterminant de cette matrice n'est autre que le produit des facteurs invariants. Ce résultat sera très pratique pour classer ce type de réseaux, car la valeur du déterminant nous aidera beaucoup pour déterminer leurs facteurs invariants.
D'autre part, nous profiterons d'identifier le plus grand idéal des facteurs invariants comme étant l'échelle du réseau considéré. Pour simplifier l'expression, nous parlerons de *premier facteur invariant* au lieu du plus grand idéal des facteurs invariants.

Introduisons quelques définitions qui prendraient naturellement place dans le cadre du paragraphe 6 du chapitre 1, dont nous reprenons d'ailleurs les notations.

1. DÉFINITION. Soient (L,h) un B-réseau et $\mathfrak{r}_1 \supset \ldots \supset \mathfrak{r}_n$ ses facteurs invariants. On appelle *volume* de (L,h) l'idéal $\mathcal{V}(L) = \mathfrak{r}_1 \cdots \mathfrak{r}_n$ de B.

On observera qu'un B-réseau est unimodulaire si et seulement s'il est entier de volume B.

Soient (L,h) un B-réseau libre, $x_1,\ldots,x_n$ et $y_1,\ldots,y_n$ deux B-bases de L. Alors les déterminants $\det\big(h(x_i,x_j)\big)$ et $\det\big(h(y_i,y_j)\big)$ sont égaux à un élément inversible de B près et définissent ainsi le même idéal fractionnaire de B. En conséquence :

2. DÉFINITION. Soit (L,h) un B-réseau libre. On appelle *déterminant* de (L,h) l'idéal fractionnaire de B, noté $\det(L,h)$ ou $\det L$, engendré par $\det\big(h(x_i,x_j)\big)$ où $x_1,\ldots,x_n$ est une B-base de L.

Soit (L,h) un réseau libre sur un anneau des entiers d'un corps de nombres. Nous allons montrer que son volume et son discriminant sont égaux et que le premier facteur invariant coïncide avec son échelle. Nous prouverons d'abord que c'est le cas pour ses localisés en les places finies et nous en déduirons le résultat général.

Traitons tout d'abord le cas décomposé.

Nous sommes dans le cadre du paragraphe 1 du chapitre 2 : considérons un anneau principal A de corps des fractions K et posons $E = K \times K$ et $B = A \times A$. Nous noterons

σ l'involution de E donnée par $(x,y) \mapsto (y,x)$. Rappelons que pour tout $1 \leqslant i \leqslant 2$, la projection $(x_1,x_2) \mapsto x_i$ munit A d'une structure de B-algèbre notée A_i.

3. PROPOSITION. *Soit (L,h) un B-réseau de premier facteur invariant $\mathfrak{r}_1$. Alors on a les égalités $\mathcal{V}(L) = \det L$ et $\mathcal{H}L = \mathfrak{r}_1$.*

Preuve. Notons (V,h) l'extension de (L,h) à E. Vu le lemme 1.2 du chapitre 2, il existe une base orthonormée $z_1,\dots,z_n$ de V et une suite d'idéaux fractionnaires $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$ de A avec $L = (A_1 \oplus \mathfrak{a}_1A_2)z_1 \oplus \cdots \oplus (A_1 \oplus \mathfrak{a}_nA_2)z_n$. Notons que les facteurs invariants de L sont alors $\mathfrak{a}_1A_1 \oplus \mathfrak{a}_1A_2 \supset \cdots \supset \mathfrak{a}_nA_1 \oplus \mathfrak{a}_nA_2$. Comme A est principal, il existe $a_1,\dots,a_n \in A$ avec $a_iA = \mathfrak{a}_i$ pour tout $1 \leqslant i \leqslant n$. Alors $(1,a_1)z_1,\dots,(1,a_n)z_n$ est une B-base de L et un calcul rapide nous montre que $\det L = (a_1\cdots a_n)B = a_1B\cdots a_nB = (\mathfrak{a}_1A_1 \oplus \mathfrak{a}_1A_2)\cdots(\mathfrak{a}_nA_1 \oplus \mathfrak{a}_nA_2) = \mathcal{V}(L)$.
Il est finalement clair que $\mathcal{H}L = (a_1,a_1)B = \mathfrak{a}_1A_1 \oplus \mathfrak{a}_1A_2 = \mathfrak{r}_1$. □

Occupons-nous ensuite du cas non décomposé.

Nous sommes dans le cadre du chapitre 3 : considérons un corps local K d'anneau de valuation A, d'uniformisante π et une extension quadratique $E := K(\sqrt{\theta})$ de K d'anneau de valuation B et d'uniformisante p. Notons σ l'unique élément non trivial du groupe de Galois de l'extension E/K.

Rappelons que tout B-réseau est libre car B est principal.

4. LEMME. *Soient n un entier positif, $\mathfrak{a}$ un idéal fractionnaire de B et (L,h) un B-réseau $\mathfrak{a}$-modulaire de rang n. Alors $\det L = \mathfrak{a}^nB$.*

Preuve. Notons (V,h) l'extension de (L,h) à E. Soient $x_1,\dots,x_n$ une B-base de L et $y_1,\dots,y_n$ la E-base de V duale de $x_1,\dots,x_n$ dans le sens où $h(x_i,y_j) = \delta_{ij}$. Rappelons que $L^\#$ est libre sur B de base $y_1,\dots,y_n$. Un calcul simple, comme celui de l'exemple 42:5 dans [7], nous montre que $\det L^\# = (\det L)^{-1}$. D'autre part, on vérifie aisément que $\det(\mathfrak{a}L) = \mathfrak{a}^{2n}\det L$, grâce au fait que $\sigma(\mathfrak{a}) = \mathfrak{a}$. Vu le point iii) de la remarque 2.2 du chapitre 3, on a $\det L = \det(\mathfrak{a}L^\#) = \mathfrak{a}^{2n}(\det L)^{-1}$. Ainsi $\det L = \mathfrak{a}^n$. □

Soit (L,h) un B-réseau de type (t,r,s). En utilisant l'existence d'une décomposition de Jordan pour (L,h), nous avons vu au pragraphe 2 du chapitre 3 que les facteurs invariants de (L,h) sont $p^{s_1}B = \cdots = p^{s_1}B \supset \cdots \supset p^{s_t}B = \cdots = p^{s_t}B$.

Le lemme 4 nous permet alors d'énoncer :

5. PROPOSITION. *Soit (L,h) un B-réseau de premier facteur invariant $\mathfrak{r}_1$. Alors on a les égalités $\mathcal{V}(L) = \det L$ et $\mathcal{H}L = \mathfrak{r}_1$.* □

Traitons enfin le cas d'un réseau sur un anneau des entiers d'un corps de nombres.

Soient K un corps de nombres, A son anneau des entiers, E une extension quadratique de K et B la clôture intégrale de A dans E. On considère l'unique élément non trivial σ du groupe de Galois de l'extension E/K.

6. THÉORÈME. *Soit (L, h) un B-réseau libre de premier facteur invariant $\mathfrak{r}_1$. Alors $\mathcal{V}(L) = \det L$ et $\mathcal{H}L = \mathfrak{r}_1$.*

Preuve. Soit $\mathfrak{p}$ une place finie de K. Vu la proposition 7.5 du chapitre 1, on a $\mathcal{V}(L_\mathfrak{p}) = \mathcal{V}(L) \otimes_A A_\mathfrak{p}$; de plus, il est clair que que $\det L_\mathfrak{p} = \det L \otimes_A A_\mathfrak{p}$; les propositions 3 et 5 permettent alors de montrer que $\mathcal{V}(L) = \det L$. On prouve d'une manière semblable l'égalité $\mathcal{H}L = \mathfrak{r}_1$. □

7. COROLLAIRE. *Un B-réseau libre est unimodulaire si et seulement s'il est de déterminant B.*

La connaissance de l'échelle et du déterminant d'un réseau nous donne alors beaucoup d'informations sur les facteurs invariants : en particulier si le réseau est de rang 2, elle suffit à la détermination exacte et complète de ces derniers. Nous utiliserons ce fait dans l'annexe 3.

Annexe 2
Réseaux unimodulaires dans les extensions cyclotomiques

Dans cette annexe, nous donnerons la liste complète des réseaux unimodulaires totalement définis positifs sur les extensions cyclotomiques.

Commençons par quelques définitions et propriétés générales à propos des extensions cyclotomiques.

Soit $m \in \mathbb{N}$ avec $m \geqslant 3$. Nous noterons ζ_m le nombre complexe $e^{\frac{2\pi i}{m}}$.
Le corps de nombres $E_m := \mathbb{Q}(\zeta_m)$ s'appelle le *corps m-cyclotomique.*
Remarquons que si $m \equiv 2 \bmod 4$, alors $E_m = E_{\frac{m}{2}}$. Nous pourrons alors supposer que m est impair ou divisible par 4.
Notons Φ_m le polynôme minimal de ζ_m sur $\mathbb{Q}$. Il est bien connu que Φ_m est de degré $\varphi(m)$ où φ est la *fonction caractéristique* d'Euler définie par $\varphi(m) = \left|(\mathbb{Z}/m\mathbb{Z})^*\right|$.
On rappelle que $\varphi(mn) = \varphi(m)\varphi(n)$ si n et m sont premiers entre eux et que $\varphi(p^l) = = p^{l-1}(p-1)$ si p est un nombre premier et l un entier positif.
Notons B_m l'anneau des entiers de E_m. On a $B_m = \mathbb{Z}[\zeta_m]$ (cf. [10], théorème 2.6).

Considérons l'unique involution σ de E_m carcatérisée par $\sigma(\zeta_m) = \zeta_m^{-1}$. Notons K_m le corps fixe pour cette involution ; en d'autres termes, on a $K_m = \left\{x \in E_m \,|\, \sigma(x) = x\right\}$. On vérifie aisément que $K_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

L'extension quadratique ${}^{E_m}\!/_{K_m}$ s'appelle l'*extension m-cyclotomique.*

Notons A_m l'anneau des entiers de K_m. On a $A_m = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$ (cf. [10], proposition 2.16).

Etudions les places de K_m et leur comportement dans l'extension ${}^{E_m}\!/_{K_m}$.

Remarquons que tous les plongements de K_m sont réels alors que ceux de E_m sont tous complexes. On en déduit qu'il existe exactement $\frac{1}{2}\varphi(m)$ places infinies de K_m qui sont alors toutes non décomposées.

Les places finies de K_m sont étudiées dans [10] et le résultat suivant en est la proposition 2.15 de la page 16.

1. PROPOSITION. *Soit $m \geqslant 3$ un entier impair ou divisible par 4.*

(i) Supposons que m ne soit pas une puissance d'un nombre premier. Alors aucune place finie de K_m ne ramifie dans ${}^{E_m}\!/_{K_m}$.

(ii) Supposons que m soit une puissance d'un nombre premier p. Alors il existe une et une seule place finie $\mathfrak{p}$ de K_m qui soit ramifiée dans l'extension ${}^{E_m}\!/_{K_m}$. De plus c'est l'unique place de K_m telle que l'on ait l'inclusion des idéaux $pA_m \subset \mathfrak{p}$. □

Supposons que m soit une puissance d'un nombre premier p, disons $m = p^l$.

Pour simplifier l'écriture, notons A, B, K, E et ζ au lieu de A_m, B_m, K_m, E_m et ζ_m.

Notons $\mathfrak{p}$ la place finie ramifiée de K et $\mathfrak{P}$ l'unique place de E au dessus de $\mathfrak{p}$. Remarquons que l'extension ramifiée ${}^{E_{\mathfrak{P}}}/_{K_{\mathfrak{p}}}$ est dyadique si et seulement si $p = 2$.

Supposons $p = 2$ et $l \geqslant 3$.

Il est clair que -1 est un carré dans E et que l'on a $E = K(\sqrt{-1})$.

Alors -1 est aussi un carré dans $E_{\mathfrak{P}}$ et $E_{\mathfrak{P}} = K_{\mathfrak{p}}(\sqrt{-1})$. Ainsi l'extension ${}^{E_{\mathfrak{P}}}/_{K_{\mathfrak{p}}}$ est ramifiée k-unitaire pour un entier k vérifiant $0 < 2k+1 < v_K(4)$.

Déterminons cet entier.

Comme $(1-\zeta)^{\varphi(m)} B = pB$, on a $\mathfrak{P} = (1-\zeta)\,B$ de sorte que $\mathfrak{p} = (1-\zeta)\,\sigma(1-\zeta)\,A = \\ = \big(2-(\zeta+\zeta^{-1})\big)\,A$. On peut alors choisir les uniformisantes $\pi = 2-(\zeta+\zeta^{-1})$ et $\tilde{\pi} = 1-\zeta$ de $K_{\mathfrak{p}}$ et $E_{\mathfrak{P}}$ respectivement.

Mais $\pi = 2-(\zeta+\zeta^{-1}) = (1-\zeta)+\sigma(1-\zeta) \in 2\tilde{\pi}^{-2k} B_{\mathfrak{P}}$ grâce au lemme 6.2 du chapitre 3, de sorte que $2 = v_E(\pi) \geqslant v_E(2\tilde{\pi}^{-2k}) = v_E(2) - 2k$. Ainsi $k \geqslant v_K(2) - 1$. D'autre part, comme $2k+1 < v_K(4)$, on a $k \leqslant v_K(2) - 1$. En résumé, on a $k = v_K(2) - 1$.

Pour déteminer le nombre de genres cherché, nous devons encore calculer le symbole de Hilbert $\big(-1, {}^{E}/_{K}\big)_{\mathfrak{p}}$.

2. LEMME. *Soit $m \in \mathbb{Z}$ de la forme $m = 2^l$ avec $l \in \mathbb{N}$ et $l \geqslant 2$.*

(i) Si $l = 2$, alors $\big(-1, {}^{E_m}/_{K_m}\big)_{\mathfrak{p}} = -1$.

(ii) Si $l > 2$, alors $\big(-1, {}^{E_m}/_{K_m}\big)_{\mathfrak{p}} = 1$.

Preuve. Comme ci-dessus, notons A, B, E et K au lieu de A_m, B_m, E_m et K_m respectivement.

Utilisons la formule du produit de Hilbert. Soit $\mathfrak{q}$ une place de K_m avec $\mathfrak{q} \neq \mathfrak{p}$. Si $\mathfrak{q}$ est décomposée, alors $\big(-1, {}^{E}/_{K}\big)_{\mathfrak{q}} = 1$. Supposons $\mathfrak{q}$ finie non décomposée et soit Ω la place de E au dessus de $\mathfrak{q}$. Alors l'extension locale ${}^{E_\Omega}/_{K_{\mathfrak{q}}}$ est non ramifiée de sorte que toute unité de $A_{\mathfrak{q}}$ est une norme (cf [7], 63:16) et donc $\big(-1, {}^{E}/_{K}\big)_{\mathfrak{q}} = 1$.

Supposons finalement la place $\mathfrak{q}$ infinie. Alors $\mathfrak{q}$ est non décomposée et donc $\big(-1, {}^{E}/_{K}\big)_{\mathfrak{q}} = \\ = -1$, car $-1 \in \mathbb{R}^*$ n'est pas une norme de l'extension ${}^{\mathbb{C}}/_{\mathbb{R}}$.

Ainsi $\big(-1, {}^{E}/_{K}\big)_{\mathfrak{q}} = (-1)^{|\mathcal{J}|}$. On conclut en observant que $|\mathcal{J}| = \frac{1}{2}\varphi(m) = 2^{l-2}$. □

Notons $\mathcal{M}^+(r)$ l'ensemble des genres des réseaux unimodulaires totalement définis positifs de rang r.

Nous pouvons enfin énoncer :

3. THÉORÈME. *Soient $m \geqslant 3$ un entier avec m impair ou divisible par 4 et $r \in \mathbb{N}$. Alors le B_m-réseau (L, h) défini par $L = x_1 A_m \oplus \cdots \oplus x_r A_m \simeq < 1 > \perp \cdots \perp < 1 >$ est unimodulaire et totalement défini positif.*

(i) Supposons que $m = 4$ et que r soit divisible par 4. Alors $\big|\mathcal{M}^+(r)\big| = 2$. De plus

(L,h) et (M,k) sont des représentants de $\mathcal{M}^+(r)$ où

$$M = y_1A_m \oplus \cdots \oplus y_rA_m \simeq \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & i \\ 0 & 1 & 2 & 1 \\ 0 & -i & 1 & 2 \end{pmatrix} \perp \cdots \perp \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & i \\ 0 & 1 & 2 & 1 \\ 0 & -i & 1 & 2 \end{pmatrix}.$$

(ii) Supposons que $m = 2^l$ avec $l \geqslant 3$ et que r soit pair. Alors $|\mathcal{M}^+(r)| = 2$. De plus (L,h) et (M,k) sont des représentants de $\mathcal{M}^+(r)$ où

$$M = y_1A_m \oplus \cdots \oplus y_rA_m \simeq \begin{pmatrix} 2-\sqrt{2} & 1 \\ 1 & 2+\sqrt{2} \end{pmatrix} \perp \cdots \perp \begin{pmatrix} 2-\sqrt{2} & 1 \\ 1 & 2+\sqrt{2} \end{pmatrix}.$$

(iii) Dans tous les autres cas, c'est-à-dire si m n'est pas une puissance de 2 ou si r est impair ou encore si $m = 4$ et $r \equiv 2 \bmod 4$, alors $|\mathcal{M}^+(r)| = 1$.

Preuve. Comme ci-dessus, notons A, B, E et K pour A_m, B_m, E_m et K_m respectivement. On vérifie aisément que le B-réseau (L,h) est unimodulaire et totalement défini positif de sorte que $|\mathcal{M}^+(r)| \geqslant 1$.

Supposons tout d'abord que m ne soit pas une puissance d'un nombre premier. Le théorème 3.1 du chapitre 4 nous dit qu'il y a au plus un genre de B-réseaux unimodulaires totalement définis positifs de rang r. Ainsi $|\mathcal{M}^+(r)| = 1$.

Supposons ensuite que $m = p^l$ où $p \in \mathbb{Z}$ est un nombre premier. Vu la proposition 3.2 du chapitre 4, on a $|\mathcal{M}^+(r)| = |\mathcal{C}^{\mathfrak{p}}_{+1}(1,(0),(r))|$.

Si $p \neq 2$, alors le théorème 5.4 du chapitre 3 nous dit que $|\mathcal{C}^{\mathfrak{p}}_{+1}(1,(0),(r))| \leqslant 1$. Ainsi $|\mathcal{M}^+(r)| = 1$.

Si $m = 2^l$ et r est impair, on obtient aussi $|\mathcal{M}^+(r)| = 1$ en utilisant le théorème 6.5 du chapitre 3.

Supposons $m = 2^l$ et r pair. Comme l'extension ${}^{E_m}\!/_{K_m}$ est ramifiée dyadique k-unitaire avec $k = v_{\mathfrak{p}}(2) - 1$, on peut donc utiliser le corollaire 6.10 du chapitre 3. On a $|\mathcal{M}^+(r)| = |\mathcal{M}^+(r)| = v_{\mathfrak{p}}(2) - k + \alpha = 1 + \alpha$ où $\alpha \in \{0,1\}$ et $\alpha = 1$ si et seulement si $\left(-1, {}^{E}\!/_{K}\right)_{\mathfrak{p}}^{\frac{r}{2}} = 1$.

Supposons $m = 4$. Alors $\left(-1, {}^{E}\!/_{K}\right)_{\mathfrak{p}} = -1$ grâce au lemme 2 de sorte que $|\mathcal{M}^+(r)| = 1$ si r n'est pas divisible par 4 et $|\mathcal{M}^+(r)| = 2$ si r est un multiple de 4.

Pour montrer que le réseau (M,k) possède les propriétés requises, il suffit de traiter le cas où $r = 4$. On vérifie alors que la matrice associée à (M,k) est de déterminant 1 et que toutes ses valeurs propres sont réelles et strictement positives. On en déduit aisément, en particulier grâce au corollaire 7 de l'annexe 1, que le réseau (M,k) est unimodulaire totalement défini positif. D'autre part, soit $z \in M$. Vu le lemme 6.2 du chapitre 3, on a $v_{\mathfrak{p}}\big(x + \sigma(x)\big) > 0$ pour tout $x \in B$ de sorte qu'un calcul rapide nous montre que $v_{\mathfrak{p}}\big(h(z,z)\big) > 0$. Ainsi $\mathcal{N}(M,k) \neq \mathcal{N}(L,h)$ et le corollaire 7.8 du chapitre 1 nous permet de conclure.

Si $m > 4$, alors, vu le lemme 2, on a $\left(-1, {}^{E}\!/_{K}\right)_{\mathfrak{p}} = 1$ et donc $|\mathcal{M}^+(r)| = 2$ pour tout entier r pair. On procède essentiellement de la même manière que ci-dessus pour montrer que le réseau (M,k) possède les propriétés requises. Il faut cependant être attentif lorsque l'on vérifie qu'il est totalement défini positif, car certains coefficients de la matrice le

définissant peuvent être modifiés par la localisation : en fait, on obtiendra l'une ou l'autre des matrices

$$\begin{pmatrix} 2-\sqrt{2} & 1 \\ 1 & 2+\sqrt{2} \end{pmatrix} \qquad \begin{pmatrix} 2+\sqrt{2} & 1 \\ 1 & 2-\sqrt{2} \end{pmatrix}$$

selon que le plongement induisant la place infinie envoie $\sqrt{2}$ sur $\sqrt{2}$ ou $-\sqrt{2}$. Il faut alors vérifier que toutes les deux sont définies positives. □

4. REMARQUE. Notre résultat contredit le résultat qu'obtient Hashimoto dans [3] (proposition 3.8). Il ne trouve en effet qu'un seul genre de B_m-réseau unimodulaire de rang r lorsque $m = 2^l$ avec $l \geqslant 3$ et $r \equiv 2 \bmod 4$. Nous suivons cependant tous deux essentiellement le même raisonnement, à la différence près qu'Hashimoto utilise pour arriver à sa conclusion l'égalité $\left(-1, {}^{E_m}/_{K_m}\right)_{\mathfrak{p}} = -1$ qui, comme nous l'avons prouvé, est fausse. La différence que nous obtenons selon que l'entier $m = 2^l$ soit 4 où strictement supérieur à 4 s'explique par le fait que $\sqrt{2} \in E_m$ dès que $m > 4$.

5. REMARQUE. Indiquons brièvement comment comparer nos résultats avec ceux de la théorie des formes quadratiques entières sur $\mathbb{Z}$. Il est possible d'associer aux réseaux définis par les deux matrices

$$X_4 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & i \\ 0 & 1 & 2 & 1 \\ 0 & -i & 1 & 2 \end{pmatrix} \qquad \text{et} \qquad Y_2 = \begin{pmatrix} 2-\sqrt{2} & 1 \\ 1 & 2+\sqrt{2} \end{pmatrix}$$

sur A_4 et A_8 respectivement, des formes quadratiques entières sur $\mathbb{Z}$, en prenant respectivement la moitié de la trace $\mathrm{Tr}_{K_4/\mathbb{Q}}$ ou le quart de la trace $\mathrm{Tr}_{K_8/\mathbb{Q}}$. Nous obtenons dans le deux cas une forme quadratique unimodulaire définie positive de rang 8 : il s'agit en fait de la forme E_8 qui est l'unique forme quadratique unimodulaire définie positive de rang inférieur ou égal à 8 non isométrique à l'identité (cf. [8], appendice 4, pages 398 et suivantes).

D'autre part, ces matrices nous permettent d'exhiber deux réseaux qui ne sont pas isométriques bien qu'ils soient dans le même genre. En effet, considérons les $\mathbb{Z}[i]$-réseaux (L, h) et (M, k) de rang 5 définis par $L \simeq X_4 \perp < 1 >$ et $M \simeq < 1 > \perp \cdots \perp < 1 >$. Vu le théorème 3, ces deux réseaux sont dans le même genre. Mais ils ne sont pas isométriques ; en effet, dans le cas contraire, leurs traces respectives seraient isométriques et donc les réseaux quadratiques de rang 10 sur $\mathbb{Z}$ définis respectivement par $E_8 \perp < 1 > \perp < 1 >$ et $< 1 > \perp \cdots \perp < 1 >$ le seraient aussi, ce qui est faux (cf. [7], dernières remarques de la page 335).

Annexe 3

Genres des réseaux entiers de rang 2 sur les entiers de Gauss

L'objectif de cette troisième annexe est de dresser la liste complète de tous les genres des réseaux entiers de rang 2 sur les entiers de Gauss.

Considérons l'extension quadratique de corps de nombres ${}^{\mathbb{Q}(i)}/_{\mathbb{Q}}$ où $i = \sqrt{-1}$. Ce n'est autre que l'extension 4-cyclotomique définie dans l'annexe 2 dont nous reprenons ci-dessous quelques résultats. Les anneaux d'entiers respectifs de $\mathbb{Q}$ et $\mathbb{Q}(i)$ sont $\mathbb{Z}$ et $\mathbb{Z}[i]$; ce dernier s'appelle l'anneau des *entiers de Gauss*. Nous noterons σ l'automorphisme involutif de $\mathbb{Q}(i)$ donné par $\sigma(x+iy) = x - iy$.

Rappelons que l'unique place infinie de $\mathbb{Q}$ est non décomposée dans l'extension ${}^{\mathbb{Q}(i)}/_{\mathbb{Q}}$. Ainsi les espaces hermitiens sur $\mathbb{Q}(i)$ ont exactement une signature.
D'autre part, 2 est l'unique place finie de $\mathbb{Q}$ ramifiée dans ${}^{\mathbb{Q}(i)}/_{\mathbb{Q}}$ et l'extension locale ${}^{\mathbb{Q}_2(i)}/_{\mathbb{Q}_2}$ est ramifiée dyadique 0-unitaire, en d'autres termes -1 est une unité de défaut quadratique 1. D'autre part, il est bien connu qu'une place finie p de $\mathbb{Q}$ se décompose dans ${}^{\mathbb{Q}(i)}/_{\mathbb{Q}}$ si et seulement si $p \equiv 1 \bmod 4$.

Déterminons le défaut quadratique maximal que peut avoir une unité α de $\mathbb{Z}_2$ telle que $\left(\alpha, {}^{\mathbb{Q}_2(i)}/_{\mathbb{Q}_2}\right) = -1$. Notons c la valuation de ce défaut quadratique.
On a $v_2(4) = 2$ de sorte que, vu la proposition 1.4 du chapitre 3, on a $1 \leqslant c \leqslant 2$. Montrons que $c = 1$. Remarquons que 5 est une unité de défaut quadratique $4\mathbb{Z}_2$; en effet, vu l'exemple 63:3 dans [7], il suffit de prouver que l'extension ${}^{\mathbb{Q}_2(\sqrt{5})}/_{\mathbb{Q}_2}$ est non ramifiée, ce qui découle du fait bien connu que la place induite par l'idéal premier $2\mathbb{Z}$ est inerte dans l'extension ${}^{\mathbb{Q}(\sqrt{5})}/_{\mathbb{Q}}$. Mais un calcul simple utilisant la formule du produit de Hilbert nous montre que $\left(5, {}^{\mathbb{Q}(i)}/_{\mathbb{Q}}\right) = 1$ de sorte que si α est une autre unité de défaut quadratique $4\mathbb{Z}_2$, on a aussi $\left(\alpha, {}^{\mathbb{Q}(i)}/_{\mathbb{Q}}\right) = 1$ car $\frac{\alpha}{5}$ est un carré dans $\mathbb{Q}_2(i)$ (cf. [7], 63:4). Ainsi $c = 1$.

Donnons à présent la liste des genres des $\mathbb{Z}[i]$-réseaux entiers de rang 2 :

Pour tout $m, n \in \mathbb{Z}$ avec $m, n \neq 0$ et $n > 0$ si $m < 0$, considérons le réseau $A(m,n)$ défini par

$$A(m,n) = x\,\mathbb{Z}[i] \oplus y\,\mathbb{Z}[i] \simeq \begin{pmatrix} mn & 0 \\ 0 & m \end{pmatrix}.$$

Il est clair que $\mathcal{H}A(m,n) = \mathcal{N}A(m,n) = m\,\mathbb{Z}[i]$ et que les facteurs invariants de $A(m,n)$ sont $m\,\mathbb{Z}[i] \supset mn\,\mathbb{Z}[i]$. La signature de $A(m,n)$ est $(2,0)$ si $m, n > 0$, $(1,1)$ si $m > 0$ et $n < 0$ et finalement $(0,2)$ si $m < 0$ et $n > 0$.

Pour tout $m, n, k \in \mathbb{Z}$ avec $m \neq 0$, n impair, $k \geqslant 2$ et $n > 0$ si $m < 0$, considérons le réseau $B(m,n,k)$ défini par

$$B(m,n,k) = x\,\mathbb{Z}[i] \oplus y\,\mathbb{Z}[i] \simeq \begin{pmatrix} 2^k nm & mn(1+i)^{k+1} \\ mn(1-i)^{k+1} & (2n+1)m \end{pmatrix}.$$

Observons que $\det B(m,n,k) = m^2 2^k n\,\mathbb{Z}[i]$ et que $\mathcal{H}B(m,n,k) = \mathcal{N}B(m,n,k) = m\,\mathbb{Z}[i]$. Ainsi les facteurs invariants de $B(m,n,k)$ sont $m\,\mathbb{Z}[i] \supset m2^k n\,\mathbb{Z}[i]$. La signature de $B(m,n,k)$ est $(2,0)$ si $m,n > 0$, $(1,1)$ si $m > 0$ et $n < 0$ et finalement $(0,2)$ si $m < 0$ et $n > 0$.

Pour tout $m, n \in \mathbb{Z}$ avec $m \neq 0$ et $n \geqslant 2$ si $m < 0$, considérons le réseau $C(m,n)$ défini par

$$C(m,n) = x\,\mathbb{Z}[i] \oplus y\,\mathbb{Z}[i] \simeq \begin{pmatrix} 2mn & m(1+2i) \\ m(1-2i) & 2m \end{pmatrix}.$$

On vérifie facilement que $\det C(m,n) = m^2(4n-5)\,\mathbb{Z}[i]$, que $\mathcal{H}C(m,n) = m\,\mathbb{Z}[i]$ et que $\mathcal{N}C(m,n) = 2m\,\mathbb{Z}[i]$. On en déduit aisément que les facteurs invariants de $C(m,n)$ sont $m\,\mathbb{Z}[i] \supset m(4n-5)\,\mathbb{Z}[i]$. La signature de $C(m,n)$ est $(2,0)$ si $m > 0$ et $n \geqslant 2$, $(1,1)$ si $m > 0$ et $n \leqslant 1$ et finalement $(0,2)$ si $m < 0$ et $n \geqslant 2$.

Pour tout $m, n \in \mathbb{Z}$ avec $m \neq 0$ et $n \geqslant 1$ si $m < 0$, considérons le réseau $D(m,n)$ défini par

$$D(m,n) = x\,\mathbb{Z}[i] \oplus y\,\mathbb{Z}[i] \simeq \begin{pmatrix} 2mn & m(1+i) \\ m(1-i) & 2m \end{pmatrix}.$$

Quelques calculs nous montrent que $\det D(m,n) = 2m^2(2n-1)\,\mathbb{Z}[i]$, que $\mathcal{H}D(m,n) = m(1+i)\,\mathbb{Z}[i]$ et que $\mathcal{N}D(m,n) = 2m\,\mathbb{Z}[i]$. Alors les facteurs invariants de $D(m,n)$ sont $m(1+i)\,\mathbb{Z}[i] \supset m(1+i)(2n-1)\,\mathbb{Z}[i]$. La signature de $D(m,n)$ est $(2,0)$ si $m > 0$ et $n \geqslant 1$, $(1,1)$ si $m > 0$ et $n \leqslant 0$ et finalement $(0,2)$ si $m < 0$ et $n \geqslant 1$.

Montrons que les réseaux définis ci-dessus forment un système complet de représentants des genres des $\mathbb{Z}[i]$-réseaux entiers de rang 2.

Nous allons procéder comme suit : pour chaque valeur possible des facteurs invariants $\mathfrak{r}$, nous allons déterminer le nombre de genres de réseaux de facteurs invariants $\mathfrak{r}$ et observer que la liste ci-dessus possède exactement le même nombre de réseaux de facteurs invariants $\mathfrak{r}$. Nous pourrons conclure grâce au fait que les réseaux de la liste sont deux à deux dans des genres différents.

Commençons par donner une formule calculable pour le nombre de genres. Soit $\mathfrak{r} = (\mathfrak{r}_1, \mathfrak{r}_2)$ une suite adéquate de $\mathbb{Z}[i]$, avec $\mathfrak{r}_1, \mathfrak{r}_2 \subset \mathbb{Z}[i]$.
Soit $\mathcal{G}(\mathfrak{r})$ l'ensemble de genres de $\mathbb{Z}[i]$-réseaux de facteurs invariants $\mathfrak{r}$. Rappelons que l'on note $\lambda_{\mathfrak{r}} = \prod_{\mathfrak{p} \in \mathcal{I}} (-1)^{v_{\mathfrak{p}}(\mathfrak{r}_1)+v_{\mathfrak{p}}(\mathfrak{r}_2)}$.

On a $\left|\mathcal{G}(\mathfrak{r})\right| = \left|\mathcal{G}(\mathfrak{r},(2,0))\right| + \left|\mathcal{G}(\mathfrak{r},(0,2))\right| + \left|\mathcal{G}(\mathfrak{r},(1,1))\right| = 2\left|\mathcal{C}_{\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right| + \left|\mathcal{C}_{-\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right|$.

Observons ensuite la forme des facteurs invariants d'un réseaux.

Soit (L,h) un $\mathbb{Z}[i]$-réseau de facteurs invariants $\mathfrak{r}_1 \supset \mathfrak{r}_2$. Vu la proposition 1.4 du chapitre 2, on a $v_{\mathfrak{p}}(\mathfrak{r}_j) \in \Delta(\mathbb{Z})$ pour toute place finie décomposée $\mathfrak{p}$ de $\mathbb{Q}$ de sorte que,

comme $\mathbb{Z}[i]$ est principal, on peut écrire $\mathfrak{r}_1$ sous la forme $m(1+i)^k\,\mathbb{Z}[i]$ et $\mathfrak{r}_2$ sous la forme $mn(1+i)^{k+l}\,\mathbb{Z}[i]$ où $m, n \in \mathbb{N}$ sont impairs. Or, si k est impair, le 2-localisé (L_2, h_2) ne peut être que $(1+i)^k$-modulaire de sorte que $l = 0$. Comme $\mathcal{I}$ est l'ensemble des premiers congrus à 3 modulo 4, on vérifie aisément que l'on a $\lambda_{\mathfrak{r}} = 1$ si $n \equiv 1 \bmod 4$ et $\lambda_{\mathfrak{r}} = -1$ si $n \equiv 3 \bmod 4$.

Les quatre possibilités ci-dessous couvrent alors tous les choix possibles de facteurs invariants de $\mathbb{Z}[i]$-réseaux de rang 2.

Soient $\mathfrak{r}$ les facteurs invariants d'un $\mathbb{Z}[i]$-réseau (L, h).

i) Supposons que les facteurs invariants $\mathfrak{r}$ soient de la forme $m\,\mathbb{Z}[i] \supset mn\,\mathbb{Z}[i]$ avec $m, n \in \mathbb{N}$ et n impair. Alors le 2-localisé (L_2, h_2) est $2^{v_2(m)}$-modulaire et donc, grâce au corollaire 6.10 du chapitre 3, on a $\left|\mathcal{C}_{+1}(\mathfrak{r}_2)\right| = 1$ et $\left|\mathcal{C}_{-1}(\mathfrak{r}_2)\right| = 2$. On obtient ainsi $\left|\mathcal{G}(\mathfrak{r})\right| = 4$ si $n \equiv 1 \bmod 4$ et $\left|\mathcal{G}(\mathfrak{r})\right| = 5$ si $n \equiv 3 \bmod 4$.

Si $n \equiv 1 \bmod 4$, les réseaux $A(m, n)$, $A(m, -n)$, $A(-m, -n)$ et $C\big(m, \frac{1}{4}(5-n)\big)$ sont clairement dans $\mathcal{G}(\mathfrak{r})$. De plus, ils sont dans des genres distincts. En effet, la norme coïncide avec l'échelle pour les trois premiers ce qui n'est pas le cas pour le dernier ; en outre les trois premiers sont de signature distincte.

Si $n \equiv 3 \bmod 4$, les réseaux $A(m, n)$, $A(m, -n)$, $A(-m, -n)$ et $C\big(m, \frac{1}{4}(n+5)\big)$ et $C\big(-m, \frac{1}{4}(n+5)\big)$ sont clairement dans $\mathcal{G}(\mathfrak{r})$. De plus, ils sont dans des genres distincts. En effet, la norme coïncide avec l'échelle pour les trois premiers ce qui n'est pas le cas pour les deux autres ; d'autre part, les trois premiers, comme les deux derniers, sont de signature différente.

ii) Supposons que les facteurs invariants $\mathfrak{r}$ soient de la forme $m\,\mathbb{Z}[i] \supset 2mn\,\mathbb{Z}[i]$ avec $m, n \in \mathbb{N}$ et n impair. Alors le 2-localisé (L_2, h_2) est une somme orthogonale de deux réseau unimodulaires de rang 1 dont la différence des valuations des échelles est égale à 2. Or $2 \leqslant 2c$ de sorte que, grâce au théorème 7.7 et au corollaire 7.5 du chapitre 3, on a $\left|\mathcal{C}_{\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right| = \left|\mathcal{C}_{-\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right| = 1$. On obtient ainsi $\left|\mathcal{G}(\mathfrak{r})\right| = 3$.

On observe alors que les réseaux $A(m, 2n)$, $A(m, -2n)$ et $A(-m, -2n)$ sont dans $\mathcal{G}(\mathfrak{r})$ et de genres distincts, car de signature différente.

iii) Supposons que les facteurs invariants $\mathfrak{r}$ soient de la forme $m\,\mathbb{Z}[i] \supset 2^k mn\,\mathbb{Z}[i]$ avec $m, n \in \mathbb{N}$, n impair et $k \geqslant 2$. Par un même raisonnement que sous ii), on obtient, en utilisant le fait que $2^k > 2c$, les égalités $\left|\mathcal{C}_{\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right| = \left|\mathcal{C}_{-\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right| = 2$. Ainsi $\left|\mathcal{G}(\mathfrak{r})\right| = 6$.

Mais les réseaux $A(m, 2^k n)$, $A(m, -2^k n)$, $A(-m, 2^k n)$, $B(m, n, k)$, $B(m, -n, k)$ et $B(-m, n, k)$ sont clairement dans $\mathcal{G}(\mathfrak{r})$. De plus, ils sont dans des genres distincts. En effet, les trois premiers, comme les trois derniers, sont de signature différente. Montrons ensuite que $A(m, 2^k n)$ n'est pas dans le même genre que $B(m, n, k)$, bien qu'ils aient la même signature. Tous les deux admettent une décomposition de Jordan du type $(2, (1,1), (2v_2(m), 2v_2(m)+2k))$. Si J_1, J_2 (resp. J_1', J_2') en est une pour $A(m, 2^k n)$ (resp. $B(m, n, k)$), on a d'une part $\big(\mathrm{d}J_1, {}^{\mathbb{Q}_2(i)}\!/_{\mathbb{Q}_2}\big) = \big(m, {}^{\mathbb{Q}_2(i)}\!/_{\mathbb{Q}_2}\big)$ et d'autre part $\big(\mathrm{d}J_1', {}^{\mathbb{Q}_2(i)}\!/_{\mathbb{Q}_2}\big) = \big((2n+1)m, {}^{\mathbb{Q}_2(i)}\!/_{\mathbb{Q}_2}\big) = -\big(m, {}^{\mathbb{Q}_2(i)}\!/_{\mathbb{Q}_2}\big)$ car $\big(2n+1, {}^{\mathbb{Q}_2(i)}\!/_{\mathbb{Q}_2}\big) = -1$ vu que $2n+1 \equiv 3 \bmod 4$. On conclut en observant que $2k > 2c$ et en appliquant le corollaire 7.2 du chapitre 3.

On procède de même pour montrer que $A(m, -2^k n)$ (resp. $A(-m, 2^k n)$) n'est dans le même genre que $B(m, -n, k)$ (resp. $B(-m, n, k)$).

iv) Supposons que les facteurs invariants $\mathfrak{r}$ soient de la forme $m(1+i)\,\mathbb{Z}[i] \supset mn(1+i)\,\mathbb{Z}[i]$ avec $m, n \in \mathbb{N}$ et n impair. Alors le 2-localisé (L_2, h_2) est $(1+i)^s$-modulaire avec s impair et le corollaire 6.10 du chapitre 3 nous permet d'affirmer que $\left|\mathcal{C}_{\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right| = \left|\mathcal{C}_{-\lambda_{\mathfrak{r}}}(\mathfrak{r}_2)\right| = 1$. Ainsi $\left|\mathcal{G}(\mathfrak{r})\right| = 3$.

Mais les réseaux $D\big(m, \frac{1}{2}(n+1)\big)$, $D\big(-m, \frac{1}{2}(n+1)\big)$ et $D\big(m, \frac{1}{2}(1-n)\big)$ sont clairement dans $\mathcal{G}(\mathfrak{r})$. De plus, ils sont dans des genres différents, car de signature distincte.

Annexe 4

Existence de genres ne contenant pas de réseau libre

Le but de cette dernière annexe est de montrer qu'un genre n'admet pas forcément un réseau libre comme représentant. Nous allons construire une famille de contre-exemples très semblables en considérant des réseaux de rang 1 sur les anneaux des entiers de certains corps quadratiques. Nous obtiendrons en corollaire une démonstration du fait que les anneaux d'entiers en question ne sont pas principaux.

Commençons par donner brièvement quelques résultats sur les corps quadratiques.

On appelle *corps quadratique* toute extension de degré 2 du corps $\mathbb{Q}$ des rationnnels.
Si K est un corps quadratique, il existe un entier $m \in \mathbb{Z}$ sans facteurs carrés avec $m \neq 0, 1$ tel que $K = \mathbb{Q}(\sqrt{m})$. De plus, si m et n sont deux tels entiers distincts, alors $\mathbb{Q}(\sqrt{m}) \neq \neq \mathbb{Q}(\sqrt{n})$.
Les places de $\mathbb{Q}$ ont le comportement suivant dans l'extension ${}^{\mathbb{Q}(\sqrt{m})}/_{\mathbb{Q}}$: l'unique place infinie de $\mathbb{Q}$ est décomposée dans l'extension si et seulement si $m > 0$. Les places finies de $\mathbb{Q}$ qui sont ramifiées sont les places correspondant aux premiers p qui divisent m ainsi qu'à 2 lorsque $m \equiv 3 \bmod 4$.
Posons $\alpha_m = \sqrt{m}$ si $m \equiv 2, 3 \bmod 4$ et $\alpha_m = \frac{1+\sqrt{m}}{2}$ si $m \equiv 1 \bmod 4$. Il est bien connu que l'anneau des entiers de $\mathbb{Q}(\sqrt{m})$ est $\mathbb{Z}[\alpha_m]$.

Notons $\mathcal{M}(m)$ l'ensemble des genres des $\mathbb{Z}[\alpha_m]$-réseaux unimodulaires de rang 1.

1. LEMME. *Soit $m \in \mathbb{Z}$ sans facteurs carrés avec $m \neq 0, 1$. Soit R le nombre de facteurs premiers de l'entier m si $m \equiv 1 \bmod 4$ et de l'entier $2m$ si $m \equiv 2, 3 \bmod 4$.*

(i) Si $m > 0$, alors $|\mathcal{M}(m)| = 2^{R-1}$.

(ii) Si $m < 0$, alors $|\mathcal{M}(m)| = 2^{R}$.

Preuve. Remarquons tout d'abord que R est le nombre de places finies de $\mathbb{Q}$ qui sont ramifiées dans l'extension ${}^{\mathbb{Q}(\sqrt{m})}/_{\mathbb{Q}}$. D'autre part, si p est une telle place, notons $\mathcal{C}_\lambda(p)$ l'ensemble des classes d'isométrie de $\mathbb{Z}_p[\alpha_m]$-réseaux unimodulaires de rang 1 et de discriminant d vérifiant $\left(d, {}^{\mathbb{Q}_p(\sqrt{m})}/_{\mathbb{Q}_p}\right) = \lambda$ où $\lambda \in \{\pm 1\}$.
Vu les théorèmes 5.4 et 6.5, tous deux du chapitre 3, on a $|\mathcal{C}_{+1}(p)| = |\mathcal{C}_{-1}(p)| = 1$ pour toute place finie ramifiée p.
Notons $\mathfrak{r}$ la suite adéquate de longueur 1 de $\mathbb{Z}[\alpha_m]$ donnée par $\mathfrak{r}_1 = \mathbb{Z}[\alpha_m]$. Utilisons le théorème 2.1 du chapitre 4 et ses notations ; pour toute famille de signature Σ, on a $|\mathcal{G}(\mathfrak{r}, \Sigma)| = |\Omega(\lambda_\Sigma)| = 2^{R-1}$.

Supposons $m > 0$. Il n'y a alors aucune place infinie non décomposée de sorte que Σ ne peut être que la famille vide et donc $|\mathcal{M}(m)| = |\mathcal{G}(\mathfrak{r}, 0)| = 2^{R-1}$.

Si $m < 0$, il existe une unique place infinie non décomposée et on obtient alors $|\mathcal{M}(m)| = |\mathcal{G}(\mathfrak{r}, (1,0))| + |\mathcal{G}(\mathfrak{r}, (0,1))| = 2^{R-1} + 2^{R-1} = 2^R$. □

Soit (L, h) un $\mathbb{Z}[\alpha_m]$-réseau libre de rang 1. On peut alors supposer que $L = \mathbb{Z}[\alpha_m]$. D'autre part, h est entièrement caractérisée par l'élément $h(1,1)$ qui est à la fois dans $\mathbb{Z}$ et générateur de $\mathcal{V}L = \mathbb{Z}[\alpha_m]$ de sorte que $h(1,1) = \pm 1$. Ainsi, il y a au plus deux classes d'isométrie, donc au plus deux genres de $\mathbb{Z}[\alpha_m]$-réseaux unimodulaires de rang 1 admettant un représentant libre.

On en déduit alors le théorème suivant :

2. THÉORÈME. *Soit $m \in \mathbb{Z}$ sans facteurs carrés avec $m \neq 0, 1$. Soit R le nombre de facteurs premiers de l'entier m si $m \equiv 1 \bmod 4$ et de l'entier $2m$ si $m \equiv 2, 3 \bmod 4$. Supposons que $m > 0$ et $R > 2$ ou que $m < 0$ et $R > 1$. Alors il existe au moins un genre de $\mathbb{Z}[\alpha_m]$-réseaux unimodulaires de rang 1 n'admettant aucun représentant libre. En particulier, l'anneau $\mathbb{Z}[\alpha_m]$ n'est pas principal.* □

Bibliographie

[1] P.M. COHN, *Algebra*, Vol. 2 John Wiley & Sons London 1977.

[2] A. FRÖHLICH et M.J. TAYLOR, *Algebraic number theory*, Cambridge University Press Cambridge 1991.

[3] K. HASHIMOTO, *Elliptic conjugacy classes of the Siegel modular group and unimodular hermitian forms over the ring of cyclotomic integers*, J. Fac. Sci. Univ. Tokyo Sect IA, Math 33 pp. 57–82 1986.

[4] R. JACOBOWITZ, *Hermitian forms over local fields*, Am. J. Math. 84 pp. 441–465 1962.

[5] W. LANDHERR, *Äquivalenz Hermitescher Formen über einem beliebigen algebraischen Zahlkörper*, Abh. Math. Sem. Hamb. 11 pp. 245–248 1936.

[6] M. MISCHLER, *Un lien entre les $\mathbb{Z}$-réseaux unimodulaires et les formes hermitiennes : les F-réseaux*, Publ. Fac. Sci. Unil Lausanne 1996.

[7] O.T. O'MEARA, *Introduction to quadratic forms*, Springer-Verlag Berlin 1963.

[8] W. SCHARLAU, *Quadratic and Hermitian Forms*, Springer-Verlag Berlin 1985.

[9] G. SHIMURA, *Arithmetic of unitary groups*, Ann. of Math. 79 No 2 pp. 369–409 1964.

[10] L. WASHINGTON, *Introduction to Cyclotomics Fields*, Springer-Verlag Berlin 1982.