JOURNAL OF ALGEBRA 74, 341–373 (1982)

Unimodular Hermitian and Skew-Hermitian Forms

EVA BAYER

Section de Mathématiques, Université de Genève, 2-4, rue du Lièvre, CH-1211 Geneva 24, Switzerland

Communicated by A. Fröhlich

Received January 5, 1981; revised March 16, 1981

INTRODUCTION

Let K be an algebraic number field with a non-trivial involution, and let A be the ring of integers of K. We shall study the classification, up to isometry, of unimodular ε-hermitian forms $L \times L \to A$, where $\varepsilon = \pm 1$. The A-module L is always supposed to be projective, of finite rank.

In Section 1 we shall classify the A-modules which support a unimodular ε-hermitian form. For instance we shall show that if $\varepsilon = +1$, the number of isomorphism classes of such modules of fixed rank is h_K/h_F or $2h_K/h_F$, depending on whether K/F is ramified or not, where F is the fixed field of the involution, h_K and h_F being the class numbers of K and F.

Then we shall show (Section 2) that the unimodular ε-hermitian forms on a given rank one module are classified by $U_0/N(U)$, where U is the group of units of K and U_0 is the group of units of F. Unfortunately, the cardinality of $U_0/N(U)$ is unknown in general. We shall compute $\#[U_0/N(U)]$ in two particular cases: when K is totally imaginary and F totally real, and when K has odd class number.

In the rest of the paper *we shall assume that there exists an* $\alpha \in A$ *such that* $1 = \alpha + \bar{\alpha}$. This hypothesis is realized for the orders which arise in the knot-theoretical applications. In Section 4 we shall apply the strong approximation theorem for *indefinite forms* of G. Shimura, and results of C. T. C. Wall, to this situation. For instance, if $\varepsilon = +1$, we shall prove that two indefinite unimodular hermitian forms are isometric if and only if they have the same rank, signatures and isometric determinants (cf. Corollary 4.10. The determinant is a unimodular hermitian form of rank one, see Definition 1.9). In many cases these forms can be diagonalized (see Proposition 4.11.2 and 4.11.3). In general if (L, h) is a unimodular, indefinite hermitian form then $(L, h) \cong (L_1, h_1) \perp \cdots \perp (L_m, h_m)$ with $\operatorname{rank}(L_i) \leqslant 2$. (Proposition 4.11.1). For $\varepsilon = -1$ such a splitting is in general only possible with $\operatorname{rank}(L_i) \leqslant 4$ (see Proposition 4.12).

0021 8693/82/020341–33$02.00/0

The classification is particularly simple if no real embedding of F extends to an imaginary embedding of K (i.e., there are no signatures).

In this case, if (L, h) is a unimodular hermitian form then $(L, h) \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp (M, g)$, where $(M, g) \cong \det(L, h)$ is a rank one form.

This can be proved without using the strong approximation theorem of G. Shimura if $\operatorname{rank}(L) \geqslant 3$ (see Section 3).

We shall apply our results to isometric structures in Section 5 and to knot theory in Section 6.

1. Modules Which Support Unimodular Hermitian or Skew-Hermitian Forms

Let K be an algebraic number field with a non-trivial $\mathbb{Q}$-involution $x \to \bar{x}$. Let $F = \{x \in K \text{ such that } \bar{x} = x\}$ be the fixed field of this involution. Let A be the ring of integers of K, and let A_0 be the ring of integers of F. We shall denote C_K, C_F the corresponding ideal class groups.

Let L be a torsion-free A-module of finite rank, and let $h: L \times L \to A$ be an ε-hermitian form, where $\varepsilon = +1$ or -1.

Definition 1.1. We shall say that $h: L \times L \to A$ is *unimodular* if and only if

$$\operatorname{ad}(h): L \to \operatorname{Hom}_A(L, A),$$
$$x \mapsto h(\ , x),$$

is bijective.

Let $L = I_1 e_1 \oplus \cdots \oplus I_n e_n$, where the I_i's are A-ideals. The *Steinitz class* of L is the ideal class of $I = I_1 \cdots I_n$ in C_K.

It is easy to check that $h: L \times L \to A$ is unimodular if and only if

$$aI\bar{I} = A,$$

where

$$a = \det(h(e_i, e_j)_{i,j}).$$

(The proof is similar to [23, 82:14]).

We shall consider the following problem: Which A-modules L support a unimodular ε-hermitian form $h: L \times L \to A$? We shall see that the answer is different for $\varepsilon = +1$ and $\varepsilon = -1$.

The Hermitian Case

Let $N: C_K \to C_F$ be the norm map (see, for instance, [19, Sect. 26] for the definition).

We shall say that K/F is *unramified* if no prime of F, finite or infinite, ramifies in K. We say that K/F is *ramified* otherwise.

PROPOSITION 1.2. (1) *L supports a unimodular hermitian form if and only if the Steinitz class of L is in* $\mathrm{Ker}(N)$.

(2) *If K/F is ramified, then N is surjective.*

(3) *If K/F is unramified, then* $\mathrm{Coker}(N) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. (1) (Note that (1) is also proved in [19, Sect. 26].) Assume that L supports a unimodular hermitian form $h: L \times L \to A$. Let I and a be as in Definition 1.1. Then $aI\bar{I} = A$, so $aN(I) = A_0$. Therefore the Steinitz class of L is in $\mathrm{Ker}(N)$. Conversely, suppose that $aN(I) = A_0$ for some $a \in F$. The A-module L is isomorphic to $M = If_1 \oplus Af_2 \oplus \cdots \oplus Af_n$. It suffices to show that M supports a unimodular hermitian form. Let

$$\begin{aligned} h(f_i, f_j) &= 0 \quad \text{if } i \neq j, \\ &= 1 \quad \text{if } i = j \neq 1, \\ &= a \quad \text{if } i = j = 1. \end{aligned}$$

Then $\det(h(f_i, f_j)_{ij}) = a$. We have $A = aN(I)A = aI\bar{I}$, therefore $h: M \times M \to A$ is unimodular.

(2) Let H_0 be the Hilbert class field of F. We are assuming that K/F is ramified, so $H_0 \cap K = F$. Now [17, Lemma, p. 83] gives the desired result. By Galois theory we have the exact sequence

$$\mathrm{Gal}(H/K) \xrightarrow{f} \mathrm{Gal}(H_0/F) \longrightarrow \mathrm{Gal}(K/F) \longrightarrow 1.$$

The Artin symbols induce isomorphisms

$$\theta: C_K \to \mathrm{Gal}(H/K),$$
$$\theta_0: C_F \to \mathrm{Gal}(H_0/F),$$

(cf. [16]) and it is straightforward to check that the diagram

$$\begin{array}{ccc} C_K & \xrightarrow{N} & C_F \\ \theta \downarrow & & \downarrow \theta_0 \\ \mathrm{Gal}(H/K) & \xrightarrow{f} & \mathrm{Gal}(H_0/F) \end{array}$$

commutes. $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z}$, therefore we get the exact sequence

$$C_K \xrightarrow{N} C_F \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

COROLLARY 1.3. *Let* $h_K = \#C_K$, $h_F = \#C_F$.
The number of isomorphism classes of torsion free A-modules of rank n which support a unimodular hermitian form is

$$\frac{h_K}{h_F} \quad \text{if } K/F \text{ is ramified,}$$

$$\frac{2 \cdot h_K}{h_F} \quad \text{if } K/F \text{ is unramified.}$$

The Skew-Hermitian Case

Over the number field K, there is a bijection between nonsingular hermitian and non-singular skew-hermitian forms. Indeed, there exists a non-zero element μ of K such that $\bar{\mu} = -\mu$, and multiplication by μ gives the desired bijection.

Similarly, if there exists a rank one unimodular skew-hermitian form, then tensorisation with this form gives a bijection between unimodular hermitian and unimodular skew-hermitian forms of given rank. Therefore we shall begin by investigation the existence of such a rank one form. N. Stoltzfus has solved a similar problem in [27]. We shall use some of the techniques he developed. (C. Bushnell has also results for a similar problem, see [7]).

DEFINITION 1.4. Assume that K/F is unramified. Let U be the group of units of A. Let $u \in U$ such that $u\bar{u} = 1$. By Hilbert's Theorem 90 there exists an x in K such that $u = x(\bar{x})^{-1}$. Set

$$Sc(u) = \prod_{P \text{ inert}} (-1)^{v_P(x)}.$$

This gives a well-defined homomorphism

$$Sc\colon H^1(\mathbb{Z}/2\mathbb{Z}, U) \to \mathbb{Z}/2\mathbb{Z}$$

(cf. [27, p. 48]).
Let Δ *be the different of* K/F.

LEMMA 1.5 [27, p. 52–53]. *Suppose that either* K/F *is ramified, or* K/F *is unramified and* $Sc(-1) = 1$. *Then there exists a* $\gamma \in K^{\cdot}$, $\bar{\gamma} = -\gamma$, *and an A-ideal M such that*

$$\gamma M\bar{M} = \Delta.$$

PROPOSITION 1.6. *There exists a rank one skew-hermitian form if and only if* K/F *verifies one of the following*:

(a) K/F *is ramified and* $\Delta = J^2$ *for some A-ideal J.*

(b) K/F *is unramified and* $Sc(-1) = 1$.

Proof. Suppose that there exists a rank one skew-hermitian form; i.e., there exists an element $a \in K^{\cdot}$ with $\bar{a} = -a$, and an A-ideal I such that

$$aI\bar{I} = A.$$

(a) Suppose that K/F is ramified. Let γ, M as in Lemma 1.5: $\gamma M\bar{M} = \Delta$. Therefore we have

$$\Delta = (\gamma a)(IM)(\overline{IM})$$

and $\overline{\gamma a} = \gamma a$. If P is a prime ideal such that $v_P(\Delta) \neq 0$, then P is ramified (cf. [16, III, Sect. 2, Proposition 8]). In particular, $\bar{P} = P$. Therefore if P divides IM, then P also divides $\overline{IM}$. On the other hand, $\gamma a \in F$, so $v_P(\gamma a)$ must be even as P is ramified. Therefore $\Delta = J^2$ for an A-ideal J.

(b) Suppose that K/F is unramified. Notice that $v_P(a)$ is even for every inert prime P, because $aI\bar{I} = A$. Therefore

$$Sc(-1) = \prod_{P \text{ inert}} (-1)^{v_P(a)} = 1.$$

Conversely, if either (a) or (b) is satisfied, then $\Delta = J^2$ (with $J = A$ in the unramified case), and by Lemma 1.5, $\Delta = \gamma M\bar{M}$ with $\bar{\gamma} = -\gamma$. Therefore $\gamma(MJ^{-1})(\overline{MJ^{-1}}) = A$, and

$$B\colon (MJ^{-1}) \times (MJ^{-1}) \to A$$

$$(x, y) \to \gamma x \bar{y}$$

is a unimodular skew-hermitian form of rank one.

Suppose that either (a) *or* (b) *of Proposition* 1.6 *is satisfied.*

Then there exists a rank one unimodular skew-hermitian form B. The tensor product of a unimodular ε-hermitian form of rank n with B is a unimodular $(-\varepsilon)$-hermitian form of rank n. Therefore we have:

COROLLARY 1.7. *For every positive integer n there exists a bijection between hermitian unimodular forms of rank n and skew-hermitian unimodular forms of rank n.*

This bijection can be given by the form $B\colon (MJ^{-1}) \times (MJ^{-1}) \to A$ which is described at the end of the proof of Proposition 1.6.

Let L be an A-module of rank n and let I be a representant of the Steinitz class of L.

Set $\tilde{I} = I(MJ^{-1})^n$.

COROLLARY 1.8. *L supports a unimodular skew-hermitian form if and only if the ideal class of $\tilde{I}$ is in* Ker(N).

Note that the number of isomorphism classes of such modules is given by Corollary 1.3.

DEFINITION 1.9 (cf. [14, p. 667]). Let $h: L \times L \to A$ be an ε-hermitian form of rank n. The *determinant* of (L, h) is the rank one $(\varepsilon)^n$-hermitian form

$$\det(L, h): \Lambda^n L \times \Lambda^n L \to A$$

$$\det(L, h)(x_1 \Lambda \cdots \Lambda x_n, y_1 \Lambda \cdots \Lambda y_n) = \det(h(x_i, y_j)_{i,j})$$

(where $\Lambda^n L$ is the nth exterior power of L).

Note that if (L, h) is unimodular, then so is $\det(L, h)$. Isometric forms have isometric determinants. The determinant of an orthogonal sum is the tensor product of the determinants:

$$\det\{(L, h) \perp (L', h')\} = \det(L, h) \otimes \det(L', h').$$

Suppose that neither (a) *or* (b) *of Proposition* 1.6 *is satisfied*:

Then all unimodular skew-hermitian forms have even rank: indeed, the determinant of a unimodular skew-hermitian form of odd rank is a rank one unimodular skew-hermitian form, and such a form does not exist in this case.

Let $\mu \in K^{\cdot}$ such that $\bar{\mu} = -\mu$. Then $K = F(\mu)$. Let $\theta = \mu^2$. Let P be a prime ideal of F. We shall denote $(\ ,\ )_P$ the Hilbert symbol.

Let $\tilde{F} = \{x \in F^{\cdot}$ such that $(x, \theta)_P = 1$ if P is unramified, and if P is finite non-dyadic ramified$\}$ (a prime P is dyadic if $N_{F/\mathbf{Q}}(P)$ is even).

PROPOSITION 1.10 (Levine, [19, Lemma 24.3 and Theorem 25.1]). *Let L be an A-module of even rank. There exists a unimodular skew-hermitian form $h: L \times L \to A$ if and only if there exists an $a \in \tilde{F}$ such that $aI\bar{I} = A$, where I is a representant of the Steinitz class of L.*

Let us consider

$$\phi: \operatorname{Ker}(N) \to F^{\cdot}/U_0 N_{K/F}(K^{\cdot}),$$

$$[I] \mapsto [a],$$

where $aI\bar{I} = A$.

It is easy to check that ϕ is well defined.

Let $\pi: F^{\cdot} \to F^{\cdot}/U_0 N_{K/F}(K^{\cdot})$ be the projection.

Let $k = \#\pi(\tilde{F})$, $m = \#(C_K/C_K^G)$, where

$$C_K^G = \{c \in C_K \text{ such that } \bar{c} = c\}.$$

COROLLARY 1.11. *The number of isomorphism classes of A-modules of given even rank which supports a unimodular skew-hermitian form is* $k \cdot m$.

Proof. Let X be the set of Steinitz classes of A-modules L of rank $2n$ such that L supports a unimodular skew-hermitian form. Proposition 1.10 implies that

$$X = \{c \in C_K \text{ such that there exists } I \in c \text{ with } aI\bar{I} = A \text{ for some } a \in \tilde{F}\}.$$

We have $X \subset \mathrm{Ker}(N)$. $\phi: X \to \pi(\tilde{F})$ is onto by [19, Lemma 24.3].

We have the exact sequence:

$$1 \longrightarrow \mathrm{Ker}(\phi) \longrightarrow X \xrightarrow{\phi} \pi(\tilde{F}) \longrightarrow 1$$

Therefore it suffices to prove that $\#\mathrm{Ker}(\phi) = m$.

An ideal class which is in $\mathrm{Ker}(\phi)$ can be represented by an ideal I such that $I\bar{I} = A$. Then $I = J\bar{J}^{-1}$ for some A-ideal J. We have the exact sequence:

$$1 \to C_K^G \to C_K \to \mathrm{Ker}(\phi) \to 1$$
$$[J] \mapsto [J\bar{J}^{-1}].$$

2. CLASSIFICATION OF RANK ONE UNIMODULAR ε-HERMITIAN FORMS

In the preceding section we have seen which A-ideals support a unimodular ε-hermitian form. Now we want to classify the unimodular ε-hermitian forms on a given ideal.

Let I be an A-ideal and let $h_i: I \times I \to A$, $h_i(x, y) = a_i x\bar{y}$, $i = 1, 2$ be two unimodular ε-hermitian forms. Then $a_1 I\bar{I} = a_2 I\bar{I} = A$, therefore $u = a_1 a_2^{-1} \in U_0$, where U_0 is the group of units of A_0 (we have $\bar{u} = u$ because $\bar{a}_1 = \varepsilon a_1$, $\bar{a}_2 = \varepsilon a_2$). Let U be the group of units of A. An isomorphism $f: I \to I$ is given by multiplication with an element $v \in U$, and f is an isometry between h_1 and h_2 if and only if $a_2 = N(v) \cdot a_1$, where $N(v) = v\bar{v}$.

Therefore h_1 and h_2 are isometric if and only if $u = N(v)$ for some $v \in U$.

So we have proved:

PROPOSITION 2.1. *The set of isometry classes of unimodular ε-hermitian forms $h: I \times I \to A$ (for I fixed) is in bijection with*

$$U_0/N(U),$$

where $N(U) = \{u\bar{u}, u \in U\}$.

EXAMPLE 2.2. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Then $U_0 = \{+1, -1\}$, so $\#[U_0/N(U)]$ is 1 or 2. It is easy to check that if $D < 0$, then $\#[U_0/N(U)] = 2$. For $D > 0$ both cases are possible.

We are going to compute the cardinality of $U_0/N(U)$ in two cases:

PROPOSITION 2.3. *Let $d = [F : Q]$. If every infinite prime of F ramifies in K (i.e., K is totally imaginary and F is totally real), then*

$$\#[U_0/N(U)] = 2^d/Q$$

with $Q = 1$ or 2.

Proof. Let μ be the group of roots of unity in K. If $\zeta \in \mu$, then $\bar{\zeta} = \zeta^{-1}$. Indeed, this is clear if $\zeta = \pm 1$. If $\bar{\zeta} = \pm 1$, then $\bar{\zeta} \neq \zeta$ because the fixed field F is totally real. Consider a complex embedding of $\mathbb{Q}(\zeta)$. Then the images of ζ and of $\bar{\zeta}$ are inverse to each other, therefore $\bar{\zeta} = \zeta^{-1}$.

Conversely if $u \in U$ such that $u\bar{u} = 1$, then $u \in \mu$. Indeed, U and U_0 have the same rank by the theorem of Dirichlet [24, 4.4 Théorème 1]. So there exists an integer k such that $u^k \in U_0$. Therefore $(u\bar{u})^k = u^{2k} = 1$, so $u \in \mu$. We have:

$$[U_0 : N(U)] = \frac{[U_0 : U_0^2]}{[N(U) : U_0^2]}.$$

We have $[U_0 : U_0^2] = 2^d$ by the theorem of Dirichlet.

Let $Q = [N(U) : U_0^2]$. We want to show that $Q = 1$ or 2. We have seen that $N(\mu) = 1$, therefore $Q = [U : \mu \cdot U_0]$.

Let us consider $\varphi\colon U \to U$, $\varphi(u) = \bar{u}u^{-1}$. Then $\varphi(U)$ is contained in μ. Indeed, if $v \in \varphi(U)$ then $N(v) = 1$ and we have seen that this implies $v \in \mu$.

Clearly $[\mu : \varphi(U)] \cdot [\varphi(U) : \mu^2] = 2$.

But $Q = [\varphi(U) : \mu^2]$, therefore $Q = 1$ or 2.

Remark 2.4. Suppose that a non-dyadic finite prime of F ramifies in K. Then $Q = 1$. It suffices to show that $\mu \neq \varphi(U)$. We shall prove that $-1 \notin \varphi(U)$. Indeed, if $-1 \in \varphi(U)$, then there exists $u \in U$ such that $\bar{u} = -u$. Then $K = F(u)$. The discriminant of K/F divides the discriminant of u which is $4u^2$. Therefore K/F has no non-dyadic finite ramified primes, which contradicts our assumption.

EXAMPLE 2.5. Let $K = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity. Then $Q = 1$ if $m = p^k$ or $2 \cdot p^k$, p prime, and $Q = 2$ otherwise (cf. [17, Chap. 3, Theorem 4.1]).

Therefore the number of isometry classes of unimodular ε-hermitian forms on a given ideal is

$$\begin{array}{ll} 2^d & \text{if} \quad m = p^k \text{ or } 2 \cdot p^k, \\ 2^{d-1} & \text{otherwise,} \end{array}$$

where $2d = [K : \mathbb{Q}]$.

Let r be the number of finite primes, and s the number of infinite primes of F which ramify in K.

PROPOSITION 2.6. *Suppose that K has odd class number. Then*

$$\begin{aligned} \#[U_0/N(U)] &= 2^{r+s-1} && \text{if } K/F \text{ is ramified} \\ &= 1 && \text{if } K/F \text{ is unramified.} \end{aligned}$$

Proof. This proof is based on an idea of P. Schneider, and is inspired by a note of K. Iwasawa [12].

We have $U_0/N(U) \cong H(\mathbb{Z}/2\mathbb{Z}, U)$ (cf. [8, p. 108, Theorem 5]). Let us denote $G = \mathbb{Z}/2\mathbb{Z}$ in order to simplify the notation.

Let J be the *idèle* group of K (see e.g. [16] for the definition), P the principal idèles and $C = J/P$ the *idèle* class group.

Let E be the group of *idèle* units (i.e., E is the kernel of the canonical homomorphism of J onto the group of ideals of K). We have the exact sequence

$$1 \to PE/P \to J/P \to J/PE \to 1.$$

J/PE is isomorphic to C_K: the ideal class group of K, and $PE/P \cong E/U$ (cf. [12], Section 3).

Therefore we have:

$$1 \to E/U \to C \to C_K \to 1. \tag{1}$$

We are assuming that the cardinality of C_K is odd, therefore

$$H^1(G, C_K) = H^2(G, C_K) = 1.$$

By a theorem of Tate, we have $H^1(G, C) = 1$, $H^2(G, C) \cong G$ (cf. [8, p. 178, Theorem 8.3, and p. 180, Theorem 9.1]).

The cohomology exact sequence associated to (1) gives

$$H^1(G, E/U) = 1, \qquad H^2(G, E/U) \cong G.$$

Let us consider the cohomology exact sequence associated to

$$1 \to U \to E \to E/U \to 1$$

we have:

$$1 \to H^2(G, U) \to H^2(G, E) \to G$$
$$\to H^1(G, U) \to H^1(G, E) \to 1. \tag{2}$$

Let us compute $H^2(G, E)$.

Let R be the set of finite primes of F which ramify in K, and let S be the set of infinite primes of F which ramify in K. For $P_0 \in R \cup S$, let P be the prime of K above P_0. Let us denote F_{P_0} the completion of F at P_0, and K_P the completion of K at P. If $P_0 \in R$, let U_{P_0} respectively U_P the group of units in F_{P_0} respectively K_P.

Let E_0 be the group of *idèle* units of F.

We have

$$H^2(G, E) = E_0/N_{K/F}(E)$$
$$= \prod_{P_0 \in R} \{U_{P_0}/N_{K_P/F_{P_0}}(U_P)\} \times \prod_{P_0 \in S} \{F^{\cdot}_{P_0}/N_{K_P/F_{P_0}}(K^{\cdot}_P)\}.$$

We have

$$\#\{U_{P_0}/N_{K_P/F_{P_0}}(U_P)\} = 2 \qquad \text{if} \quad P_0 \in R$$

(see for instance [16, IX, Sect. 3, Lemma 4]), and clearly

$$\#\{F^{\cdot}_{P_0}/N_{K_P/F_{P_0}}(K^{\cdot}_P)\} = 2 \qquad \text{if} \quad P_0 \in S.$$

Therefore we have

$$\#H^2(G, E) = 2^{r+s}.$$

If K/F is unramified then $r = s = 0$, therefore (2) implies $\#H^2(G, U) = 1$.

If K/F is ramified, (2) gives

$$1 \to H^2(G, U) \to H^2(G, E) \to G.$$

But by Hilbert reciprocity

$$H^2(G, U) \to H^2(G, E)$$

cannot be surjective if $r \neq 0$ or $s \neq 0$.

Therefore we have

$$1 \to H^2(G, U) \to H^2(G, E) \to G \to 1,$$

so $\#H^2(G, U) = 2^{r+s-1}$.

Remark 2.7. (1) We have

$$\frac{\#H^2(\mathbb{Z}/2\mathbb{Z}, U)}{\#H^1(\mathbb{Z}/2\mathbb{Z}, U)} = 2^{s-1}$$

(see [5, Lemma 3.1]). Therefore $\#[U_0/N(U)] \geqslant 2^{s-1}$.

(2) Let k_1 be the number of real embeddings, and $2k_2$ the number of imaginary embeddings of F. Then Dirichlet's theorem implies that $\#[U_0/U_0^2] = 2^{k_1+k_2}$ (see, for instance, [24, 4.4 Théorème 1]).

As $U_0 \subset N(U)$, we obtain:

$$\#[U_0/N(U)] \leqslant 2^{k_1+k_2}.$$

3. Isotropic Forms

The aim of this section is to prove the following:

Proposition 3.1. *Assume that there exists an* $\alpha \in A$ *such that* $1 = \alpha + \bar{\alpha}$, *and that no infinite prime of* F *ramifies in* K.

Let (L, h) *be a unimodular hermitian form, with* $\operatorname{rank}_A(L) \geqslant 3$. *Then*

$$(L, h) \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp (M, g)$$

where $(M, g) = det(L, h)$ *is a rank one form.*

(See Definition 1.9 for the definition of the determinant.)

It follows immediately from Proposition 3.1 that

Corolary 3.2. *Let* K/F *be as in Proposition* 3.1. *Then unimodular hermitian forms of rank* $\geqslant 3$ *are classified by rank and determinant.*

The corresponding result for skew-hermitian forms is

Proposition 3.3 (A. Bak and W. Scharlau). *Let* K/F *be as in Proposition* 3.1. *Let* (L, h) *be a unimodular skew-hermitian form of rank* $2m$. *Then*

$$(L, h) \cong \mathbb{H}^{m-1} \perp \mathbb{H}(I)$$

where I *is an* A*-ideal.*

(See Definition 3.6 for the definition of $\mathbb{H}$ and $\mathbb{H}(I)$.)

If there exist unimodular skew-hermitian forms of odd rank, then there exists a bijection between unimodular hermitian and unimodular skew-hermitian forms of given rank (see Corollary 1.7), therefore we can apply Proposition 3.1.

Remark. (1) The hypothesis $1 = \alpha + \bar{\alpha}$ for some $\alpha \in A$ is satisfied for the orders A arrizing from the knot-theoretical applications (see Sections 5 and 6).

(2) In Section 4 we shall give another proof of Proposition 3.1 using the Strong approximation theorem of G. Shimura. The proof we give in Section 3 only uses the ordinary strong approximation theorem for ideals, and Landherr's theorem.

DEFINITION 3.4. Let V be a finite dimensional K-vector space, and let $h\colon V \times V \to K$ be a non-singular hermitian form. Let $e_1, \ldots, e_n$ be a basis of V. The *discriminant* of (V, h) will be the class of $\det(h(e_i, e_j))_{ij})$ in $F^{\cdot}/N_{K/F}(K^{\cdot})$, where $N_{K/F}(x) = x\bar{x}$.

Let P be a prime of F. Let F_P be the completion of F at P, and $K_P = F_P \otimes K$. We shall denote $(V, h)_P$ the tensorisation of (V, h) with K_P.

If P is an infinite prime of F which ramifies in K, then $F_P = \mathbb{R}$ and $K_P = \mathbb{C}$. We shall denote σ_P the signature of $(V, h)_P$.

Let $\mu \in K^{\cdot}$ such that $\bar{\mu} = -\mu$. If $h\colon V \times V \to K$ is a non-singular skew-hermitian form, then we define d, σ_P as the discriminant and signatures of the hermitian form $(V, \mu \cdot h)$.

Let $\theta = \mu^2 \in F^{\cdot}$. If P is a prime of F, we shall denote $(\ ,\ )_P$ the Hilbert symbol.

LEMMA 3.5 (Landherr's Theorem, cf. [15]). *Two non-singular ε-hermitian forms $h\colon V \times V \to K$, $g\colon W \times W \to K$ are isometric if and only if they have the same dimension, discriminant and signatures.*

Let $P_1, \ldots, P_s$ be the infinite primes of F which ramify in K. *There exists a non-singular ε-hermitian form of dimension n, discriminant d and signatures $\sigma_1, \ldots, \sigma_s$ if and only if*

$$(d, \theta)_{P_i} = (-1)^{(n-\sigma_i)/2}, \qquad i = 1, \ldots, s.$$

Assume that no infinite prime of F ramifies in K. Then there are no signatures, and Landherr's theorem implies that non-singular ε-hermitian forms are classified by dimension and discriminant.

Let (V, h) be a non-singular ε-hermitian form of dimension $n \geqslant 3$, and of discriminant d. Let (W, g) be an ε-hermitian form of dimension $n-2$ and discriminant $(-d)$.

Then (V, h) is isometric to the orthogonal sum of (W, g) with a hyperbolic plane (i.e., a 2-dimensional form given by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ \epsilon & 0 \end{smallmatrix}\right)$.)

Therefore (V, h) represents zero. If $h: L \times L \to A$ is an ε-hermitian form such that $(L, h) \otimes K = (V, h)$, then clearly (L, h) also represents zero.

Therefore we shall begin by recalling some definitions and lemmas concerning forms which represent zero.

DEFINITION 3.6. (1) An ε-hermitian form $h: L \times L \to A$ is *isotropic* if there exists an x in L such that $h(x, x) = 0$. We shall say that x is an *isotropic vector.*

(2) Let I be an A-ideal. We shall denote $\mathbb{H}(I)$ the ε-hermitian form

$$h: (Ie \oplus \bar{I}^{-1}f) \times (Ie \oplus \bar{I}^{-1}f) \to A$$

such that

$$h(e, e) = h(f, f) = 0,$$
$$h(e, f) = 1.$$

If $I = A$, we shall write $\mathbb{H}$ instead of $\mathbb{H}(A)$.

(3) An ε-hermitian form $h: L \times L \to A$ is *even* if there exists a sesquilinear form $g: L \times L \to A$ such that $h(x, y) = g(x, y) + \varepsilon\overline{g(x, y)}$.

For instance $\mathbb{H}(I)$ is even.

Remark 3.7. If there exists an $\alpha \in A$ such that $\alpha + \bar{\alpha} = 1$, then every ε-hermitian form is even. This is clear for $\varepsilon = +1$. For $\varepsilon = -1$, note that if $\bar{a} = -a$ then $a = \alpha a - \overline{(\alpha a)}$.

The following lemma is well-known (see for instance [9]):

LEMMA 3.8. *Let $h: L \times L \to A$ be an isotropic, even, unimodular ε-hermitian form. Let $x \in L \otimes K$ be an isotropic vector, and let $I = \{\lambda \in K$ such that $\lambda \cdot x \in L\}$. Then $\mathbb{H}(I)$ is an orthogonal summand of (L, h).*

Proof. Let $V = L \otimes K$. Set $x_1 = x$, $I_1 = I$, and let $x_2, ..., x_n \in V$ such that $L = Ix_1 \oplus \cdots \oplus I_n x_n$, where $I_2, ..., I_n$ are A-ideals.

Let $y_1, ..., y_n$ be the dual basis of $x_1, ..., x_n$. Let $L^{\#} = \{v \in V \mid h(v, L) \subseteq A\}$. Then $L^{\#} = \bar{I}^{-1}y_1 \oplus \cdots \oplus \bar{I}_n^{-1}y_n$ (the proof is as in [23, 82F]).

As (L, h) is unimodular, $L = L^{\#}$. Therefore $Ix \oplus \bar{I}^{-1}y_1$ is contained in L. Now $h(y_1, y_1) = \beta + \varepsilon\bar{\beta}$ for some $\beta \in A$ because h is even.

Let $y = y_1 - \beta x$. Then $h(y, y) = 0$, therefore the restriction of h to $Ix \oplus \bar{I}^{-1}y$ is isometric to $\mathbb{H}(I)$. Clearly $\mathbb{H}(I)$ is unimodular, so it is an orthogonal summand of (L, h).

LEMMA 3.9 (A. Bak and W. Scharlau, [1, Lemma 7.2]). *If IJ^{-1} is a product of inert primes and of ideals of the form $P\bar{P}$, then $\mathbb{H}(I)$ and $\mathbb{H}(J)$ are isometric.*

Remark. The isometry relations between hyperbolic forms are completely worked out in [1], and also in [6], in a more general situation.

Note that the proof of Lemma 3.9 only uses the strong approximation theorem for ideals, [23, 21:2].

PROPOSITION 3.10. *Let (L, h) be an even, isotropic, unimodular hermitian form of rank* 3. *Then* $\mathbb{H}$ *is an orthogonal summand of* (L, h).

COROLLARY 3.11. *The isometry class of* (L, h) *is completely determined by* $\det(L, h)$.

Proof of Proposition 3.10. Let e_1 be an isotropic vector, and let $I = \{\lambda \in K$ such that $\lambda e_1 \in L\}$. By Lemma 3.8 there exists another isotropic vector e_2 such that $\mathbb{H}(I) = Ie_1 \oplus \bar{I}^{-1}e_2$ is an orthogonal summand of (L, h), say

$$(L, h) \cong \mathbb{H}(I) \perp Je_3.$$

CLAIM. *Let P be a prime ideal of odd norm such that $\bar{P} \neq P$. Then $\mathbb{H}(IP)$ is an orthogonal summand of (L, h).*

This claim implies the proposition. Indeed, by the strong approximation theorem [23, 21:2] we may assume that $I^{-1} \subset A$, has odd norm, and that no ramified prime divides I^{-1}.

Therefore $I^{-1} = M \cdot N$, where M is a product of prime ideals satisfying the hypotheses of the claim, and N is a product of inert primes. Applying the claim several times we see that $\mathbb{H}(N^{-1})$ is an orthogonal summand of (L, h). By Bak–Scharlau (see Lemma 3.9) we have $\mathbb{H}(N^{-1}) \cong \mathbb{H}$, as N is a product of inert primes.

Proof of Claim. If $x \in K$, we shall denote (x) the principal A-ideal which is generated by x.

Let $x_1 \in K$ such that $(x_1^{-1}) \cap A = P$. This is possible by the strong approximation theorem.

Let μ be a non-zero element of A such that $\bar{\mu} = -\mu$. We have

$$x_1 = \frac{\alpha}{\beta} + \frac{\gamma}{\delta}\mu$$

with $\alpha, \beta, \gamma, \delta \in A_0$.

As $P \neq \bar{P}$, we have $\alpha \neq 0$, $\gamma \neq 0$.

Using the strong approximation theorem we may assume that I and J relatively prime to P, to (β), that $I^{-1} \subset A$, $J \subset A$ and that I and J are relatively prime.

Let $a = h(e_3, e_3)$ and set

$$x_2 = -\beta a/2\alpha$$

Direct computation shows that $x = x_1 e_1 + x_2 e_2 + e_3$ is an isotropic vector. Let

$$\begin{aligned} I_x &= Kx \cap L \\ &= \{(x_1 e_1 + x_2 e_2 + e_3) \cdot m \text{ such that} \\ &\qquad x_1 m \in I, x_2 m \in \bar{I}^{-1}, m \in J\} \end{aligned}$$

then

$$I_x \cong x_1^{-1} I \cap x_2^{-1} \bar{I}^{-1} \cap J.$$

$I_x I^{-1} \cong (x_1^{-1}) \cap x_2^{-1} I^{-1} \bar{I}^{-1} \cap J I^{-1}$.

We have $JI^{-1} \subset A$, therefore

$$I_x I^{-1} \cong ((x_1^{-1}) \cap A) \cap (x_2^{-1} I^{-1} \bar{I}^{-1} \cap A) \cap JI^{-1}.$$

We have:

$$x_2^{-1} I^{-1} \bar{I}^{-1} \cap A \subset (1/a)\, I^{-1} \bar{I}^{-1} \subset JI^{-1}$$

because

$$(1/a)A = J\bar{J} \subset J$$

and

$$I^{-1} \bar{I}^{-1} \subset I^{-1}$$

So

$$I_x I^{-1} \cong P \cap (x_2^{-1} I^{-1} \bar{I}^{-1} \cap A)$$

(recall that $(x_1^{-1}) \cap A = P$).

Now, P and $x_2^{-1} I^{-1} \bar{I}^{-1} \cap A$ are relatively prime. To see this, it suffices to prove that $v_P(x_2^{-1}) \leqslant 0$.

We have:

$$N_{K/F}(x_1^{-1}) = \frac{\beta^2 \delta^2}{\alpha^2 \delta^2 - \mu^2 \beta^2 \gamma^2},$$

$$N_{K/F}(x_2^{-1}) = \frac{4\alpha^2}{\beta^2 a^2}.$$

Let $P_0 = P \cap A_0$.

We have: $v_{P_0}(N(x_1^{-1})) = 1$, because $N_{K/F}(P) = P_0$.

As $v_{P_0}(N(x_1^{-1})) = 1$, $v_{P_0}(\alpha^2\delta^2 - \mu^2\beta^2\gamma^2)$ is odd.

Therefore $v_{P_0}(\alpha^2\delta^2) = v_{P_0}(\mu^2\beta^2\gamma^2)$ (note that P_0 is not ramified, therefore $v_{P_0}(\mu^2)$ is even), and

$$v_{P_0}(\alpha^2\delta^2 - \mu^2\beta^2\gamma^2) > v_{P_0}(\alpha^2\delta^2).$$

We have $v_{P_0}(\beta^2\delta^2) = v_{P_0}(\alpha^2\delta^2 - \mu^2\beta^2\gamma^2) + 1$, therefore

$$v_{P_0}(\beta^2) + v_{P_0}(\delta^2) > v_{P_0}(\alpha^2) + v_{P_0}(\delta^2) + 1,$$

so

$$v_{P_0}(\beta^2) > v_{P_0}(\alpha^2).$$

$v_{P_0}(a) = 0$ by assumption, therefore $v_{P_0}(x_2^{-1}) < 0$.

Set $M = (x_2^{-1}I^{-1}\bar{I}^{-1} \cap A)$. We have just seen that P and M are relatively prime, so $I_x I^{-1} \cong P \cdot M$.

Therefore $\mathbb{H}(IPM)$ is an orthogonal summand of (L, h) (see Lemma 3.8). But M is a product of inert primes and of ideals of the form $Q\bar{Q}$. Therefore, by Bak–Scharlau (Lemma 3.9) we have $\mathbb{H}(IPM) \cong \mathbb{H}(IP)$.

Proof of Corollary 3.11. This follows immediately from Proposition 3.10, noting that $\det(\mathbb{H}) = \langle -1 \rangle$, and that the determinant of an orthogonal sum is the tensor product of the determinants (see Definition 1.9).

Proof of Proposition 3.1. Let $\operatorname{rank}_A(L) = 3$. Consider the lattice $(N, f) = \langle 1 \rangle \perp \langle 1 \rangle \perp (\det(L, h))$.

By the discussion following Lemma 3.5 (L, h) and (N, f) are both isotropic. By Remark 3.7, (L, h) and (N, f) are both even. Clearly $\det(N, f) = \det(L, h)$. Therefore by Corollary 3.11, (L, h) and (N, f) are isometric. This proves Proposition 3.1 for $\operatorname{rank}_A(L) = 3$.

Suppose $\operatorname{rank}_A(L) > 3$. We shall prove that $\langle 1 \rangle$ is an orthogonal summand of (L, h), and then continue by induction.

As in the case $\operatorname{rank}_A(L) = 3$ we see that (L, h) is isotropic and even. By Lemma 3.8 there exists an A-ideal I such that $\mathbb{H}(I)$ is an orthogonal summand of (L, h). By the strong approximation theorem we may assume that no ramified ideal divides I. By Lemma 3.9, we may assume that if P divides I, then $\bar{P}$ does not divide I. Then we see that $\mathbb{H}(I)$ is isometric to the hermitian form $(N, g) = (Ae \oplus I\bar{I}^{-1}f,\ ee = 1,\ ff = -1,\ ef = 0)$.

Indeed, let $x = e + f$. Then $\{\lambda \in K$ such that $\lambda x \in (Ae \oplus I\bar{I}^{-1}f)\} = A \cap I\bar{I}^{-1} = I$.

As (N, g) is even, Lemma 3.8 implies that $(N, g) \cong \mathbb{H}(I)$.

Clearly $\langle 1 \rangle$ is an orthogonal summand of (N, g). Therefore $\langle 1 \rangle$ is an orthogonal summand of (L, h).

Remark 3.12. Note that the last part of the above proof implies that if

$1 = \alpha + \bar{\alpha}$ for some $\alpha \in A$ and if $\varepsilon = +1$, then $\mathbb{H}(I) \cong \mathbb{H}(J)$ if and only if $\det(\mathbb{H}(I)) \cong \det(\mathbb{H}(J))$.

For the proof of Proposition 3.3 we shall need the following remark:

Remark 3.13. If there exists $\alpha \in A$ such that $\alpha + \bar{\alpha} = 1$, then no dyadic prime of F ramifies in K. Indeed, the minimal polynomial of α over F is $X^2 - X + \alpha\bar{\alpha}$, so the discriminant of α is $d = 1 - 4\alpha\bar{\alpha}$. The discriminant of K/F divides d, and d has odd norm, therefore no prime of even norm of F can ramify in K.

Proof of Proposition 3.3. Let $V = L \otimes K$, and let $e_1, ..., e_{2m}$ be a basis of V. Set $a = \det(h(e_i, e_j)_{ij}) \in F^{\cdot}$. Then $(\alpha, \theta)_P = +1$ if P is unramified or finite non-dyadic ramified (see [19, Lemma 24.3], or [31, Proposition 6]). We have no infinite ramified primes, and Remark 3.13 implies that there are no dyadic ramified primes. Therefore $(a, \theta)_P = +1$ for every prime P. So $a \in N_{K/F}(K^{\cdot})$ by the Hasse cyclic norm theorem, [23, 65:23].

By Landherr's theorem (Lemma 3.5) this implies that (V, h) is hyperbolic (recall that there are no signatures). Therefore (L, h) is also hyperbolic: $(L, h) \cong \mathbb{H}(I_1) \perp \cdots \perp \mathbb{H}(I_m)$ (apply Lemma 3.8 several times). Then [21, Theorem 7.1] gives the desired result.

4. Indefinite Forms

In this section we shall assume that there exists an $\alpha \in A$ such that $\alpha + \bar{\alpha} = 1$. The orders arising from the knot theoretical applications satisfy this hypothesis (see Sections 5 and 6). We shall apply results of G. Shimura and C. T. C. Wall to this situation.

We have seen in Section 3 that the hypothesis $1 = \alpha + \bar{\alpha}$ with $\alpha \in A$ implies that no dyadic prime of F ramifies in K, and that every ε-hermitian form $h: L \times L \to A$ is even (see Remarks 3.7 and 3.13).

Let P be a prime of F. Let F_P be the completion of F at P, and let $K_P = F_P \otimes K$. We shall use the notation (V, h) for non-singular ε-hermitian forms $h: V \times V \to K$, where V is a finite dimensional K-vector space. We shall denote $(V, h)_P$ the tensorisation of (V, h) with K_P. A *lattice* L in (V, h) will be a torsion-free A-module of finite rank such that $L \otimes_A K = V$, and such that the restriction of h to L is A-valued and *unimodular*.

Definition 4.1. (V, h) is *definite* if for every infinite prime P of F we have:

(a) P ramifies in K;

(b) $(V, h)_P$ is anisotropic.

(V, h) is *indefinite* otherwise.

DEFINITION 4.2. Let L, M be two lattices in (V, h). We shall say that L and M are in the same *genus* if for every prime P of F there exists an automorphism ψ_P of $(V, h)_P$ such that $\psi_P(L_P) = M_P$. If $\det(\psi_P) = 1$, then L and M are in the same *SU-genus.*

LEMMA 4.3 [31, Proposition 6]. *Let L and M be two lattices in (V, h). Then L and M are in the same genus.*

Remark 4.4. For this lemma the hypothesis that no dyadic prime of F ramifies in K is essential. When applying results of [31], note that (with our hypothesis) for $\varepsilon = +1$ there are no "bad primes," and for $\varepsilon = -1$ the "bad primes" are exactly the finite primes of F which ramify in K (cf. [31, p. 433–434]).

LEMMA 4.5. *Let (V, h) be indefinite,* $\dim(V) \geqslant 2$. *Let L and $N = N_1 \perp N_2$ be lattices in (V, h) such that* $\operatorname{rank}(N_2) \geqslant 1$. *Then N_1 is an orthogonal summand of L.*

Proof. The following argument has been used by L. Gerstein [10, p. 412, (V)]. By Lemma 4.3, L and N are in the same genus. So or every prime P of F there exists an automorphism ψ_P of $(V, h)_P$ such that $\psi_P(L_P) = N_P$. Let $\beta_P = \det(\psi_P)$, then $\beta_P \cdot \overline{\beta_P} = 1$. We have $\beta_P = 1$ for almost all P.

Let $W = N_2 \otimes K$, and let g be the restriction of h to W. There exists an automorphism ϕ_P of $(W, g)_P$ such that $\det(\phi_P) = \beta_P^{-1}$.

Let M be the A-lattice in W suchq that

$$M_P = \phi_P(N_{2P}) \qquad \text{if} \quad \beta_P \neq 1,$$
$$= N_{2P} \qquad \text{if} \quad \beta_P = 1$$

(cf. [23, 81:14], noting that $M_P = N_{2P}$ for almost all P).

Then $N_1 \perp M$ is in the SU-genus of , therefore by the strong approximation theorem of Shimura [26, Theorem 5.19], $N_1 \perp M$ and L are isometric.

We have seen in Section 1 that if there exist unimodular skew-hermitian lattices of odd rank, then the classification of hermitian and skew-hermitian lattices is the same. Therefore we shall only consider the cases $\varepsilon = +1$ and $\varepsilon = -1$, $\operatorname{rank}_A(L)$ even.

Recall that $\mu \in K^{\cdot}$ is such that $\bar{\mu} = -\mu$, $\theta = \mu^2$, and that $(\ ,\ )_P$ is the Hilbert symbol.

LEMMA 4.6 (19, Lemma 24.3] or [31, Proposition 6]). *Let (V, h) be a non-singular ε-hermitian form of discriminant d.*

$\varepsilon = +1$. *(V, h) contains a unimodular lattice if and only if*

$$(d, \theta)_P = +1$$

for every prime P of F which does not ramify in K.

$\varepsilon = -1$, $\dim(V) = 2m$. *(V, h) contains a unimodular lattice if and only if $(d, \theta)_P = +1$ for every prime P of F which does not ramify in K, and if $(d, \theta)_P = (-1, \theta)_P^m$ for every finite prime P of F which ramifies in K.*

COROLLARY 4.7. *Let L be an indefinite, unimodular lattice in (V, h) and let Mbe a unimodular lattice in (W, g).*

Assume that $\dim(W) < \dim(V)$, and that $(W, g)_P$ is an orthogonal summand of $(V, h)_P$ for every infinite prime P of F which ramifies in K. Then M is an orthogonal summand of L.

Proof. By Landherr's theorem (W, g) is an orthogonal summand of (V, h): $(V, h) = (W, g) \perp (U, f)$. Lemma 4.6 implies that (U, f) also contains a unimodular lattice, say M'. Apply Lemma 4.5 with $N_1 = M$, $N_2 = M'$. Let C_0 be the subgroup of C_K which consists of the ideal classes containing ideals I such that $\bar{I} = I$.

Let $g: C_F \to C_K$ be the homomorphism which is induced by the extension of ideals.

PROPOSITION 4.8. *(V, h) as in Lemma 4.6, indefinite, $\dim(V) \geqslant 2$. The number of isometry classes of unimodular lattices in (V, h) is*

(1) *$\#(C_K/C_0)$ if $\varepsilon = +1$,*

(2) *$\#(C_K/g(C_F))$ if $\varepsilon = -1$.*

Remark. If $\dim(V)$ is odd, then Proposition 4.8 follows immediately from [26, Theorem 5.24(i)] and from Lemma 4.3.

Proof of Proposition 4.8. Let L be a unimodular lattice in (V, h). For every prime ideal P of F, set $E_{0P} = \{x \in A_P \text{ such that } x\bar{x} = 1\}$, and let E_P be the set of $\det(\psi)$, where $\psi: V_P \to V_P$ is an automorphism of $(V, h)_P$ such that $\psi(L_P) = L_P$. Clearly E_P only depends of the genus of L. As (V, h) contains exactly one genus of unimodular lattices (cf. Lemma 4.3), E_P depends only of (V, h).

We have $E_{0P} = E_P$ if P is unramified (see [26, 5.22]). Following [26, 5.22] we shall say that a ramified prime ideal P is irregular if $E_{0P} \neq E_P$. We shall denote Y the product of the factor groups E_{0P}/E_P for all irregular prime ideals P. Let x be an element of K such that $x\bar{x} = 1$. We shall denote $f(x)$ the element of Y whose components are the cosets xE_P. Let X be the group of A-ideals I such that $I\bar{I} = A$, and let $X_0 = \{aA, a \in K^{\cdot} \text{ such that } a\bar{a} = 1\} \subset X$.

(1) Let $\varepsilon = +1$. Then there are no irregular prime ideals. Indeed, let P be a finite prime of F which ramifies in K. By Remark 3.13 P is non-dyadic. Then $(L, h)_P$ can be diagonalized (cf. [13, Proposition 8.1.a]). Let $A_P \cdot e$ be an orthogonal summand of $(L, h)_P$, and let M be the orthogonal complement of $A_P \cdot e$. Let $x \in E_{0P}$. Then x is a unit of A_P. Let us define $\psi: L_p \to L_p$ by $\psi(e) = xe$, and $\psi(m) = m$ if $m \in M$. Clearly ψ extends to an automorphism of $(V, h)_P$, and $\psi(L_P) = L_P$. We have $\det(\psi) = x$, so $x \in E_P$. This implies that $E_{0P} = E_P$. (Notice that we have used an argument of [31, p. 433].)

Therefore [31, Proposition 5.27(i) and (iii)] imply that the set of isometry classes of unimodular lattices in (V, h) is in bijection with X/X_0.

Let $\varphi: C_K/C_0 \to X/X_0$ be the homomorphism which is induced by $\varphi(J) = \bar{J}J^{-1}$. It is easy to check that φ is an isomorphism. (Note that if $I\bar{I} = A$, then there exists an A-ideal J such that $I = \bar{J}J^{-1}$. This implies that φ is onto.)

(2) Let $\varepsilon = -1$. Let P be a finite prime of F which ramifies in K. Then P is irregular. Indeed, by Remark 3.13 P is non-dyadic. Then [31, p. 434, "bad tame case"] implies that $(L, h)_P$ is hyperbolic. Let $x \in E_{0P}$. By Hilbert's theorem 90 there exists $y \in K_P^{\cdot}$ such that $x = \bar{y}y^{-1}$. Then [31, Theorem 4] implies that $x \in E_P$ if and only if $v_P(y) \equiv 0 \bmod 2$. Therefore $E_{0P}/E_P \cong \mathbb{Z}/2\mathbb{Z}$, so P is irregular.

Let $Z = \{(aA, f(a)),\ a \in K \text{ such that } a\bar{a} = 1\} \subset X \times Y$.

Let $P_1, \ldots, P_r$ be the finite primes of F which ramify in K. Notice that

$$Z = \{(\bar{y}y^{-1}A, ((-1)^{v_{P_i}(y)})_{i=1,\ldots,r}),\ y \in K^{\cdot}\}.$$

Now [26, Proposition 5.27(iii)] implies that the set of isometry classes of unimodular lattices in (V, h) is in bijection with $(X \times Y)/Z$.

Let

$$\varphi: C_K/g(C_F) \to (X \times Y)/Z$$

be the homomorphism which is induced by

$$\varphi(J) = (J\bar{J}^{-1}, ((-1)^{v_{P_i}(J)})_{i=1,\ldots,r}) \subset X \times Y.$$

Then φ is an isomorphism. It is clear that φ is well defined and onto. If $\varphi(J) \in Z$, then $J\bar{J}^{-1} = (\bar{y}y^{-1})A$, and $v_{P_i}(J) \equiv v_{P_i}(y) \bmod 2$, $i = 1, \ldots, r$. Therefore J is isomorphic to $I = y \cdot J$, we have $\bar{I} = I$, and $v_P(I)$ is even for every ramified prime P. Therefore $I = I_0 A$ for some A_0-ideal I_0.

Proposition 4.9. $\varepsilon = +1$. *Let* (V, h) *as in Lemma* 4.6, $\dim(V) = 1$. *The number of isometry classes of unimodular lattices in* (V, h) *is* $\#(C_K/C_0)$.

Proof. $(W, g) = \langle 1 \rangle \perp \langle -1 \rangle \perp (V, h)$ is indefinite.

Let L be a lattice in (W, g), and let M' be a lattice in (V, h). Then $\langle 1 \rangle \perp \langle -1 \rangle \perp M'$ is a lattice in (W, g).

LEMMA 4.5. *With* $N_1 = \langle 1 \rangle \perp \langle -1 \rangle$, $N_2 = M'$ *implies that* L *is isometric to* $\langle 1 \rangle \perp \langle -1 \rangle \perp M$, *where* M *is some lattice in* (V, h).

Therefore $M \to \langle 1 \rangle \perp \langle -1 \rangle \perp M$ induces a surjective map from the set of isometry classes of lattices in (V, h) onto the set of isometry classes of lattices in (W, g).

If $L_1 = \langle 1 \rangle \perp \langle -1 \rangle \perp M_1$ is isometric to

$$L_2 = \langle 1 \rangle \perp \langle -1 \rangle \perp M_2$$

then

$$M_1 = -\det(L_1) \cong -\det(L_2) = M_2$$

therefore this map is injective. Proposition 4.8 now gives the desired result.

COROLLARY 4.10. $\varepsilon = +1$. *Two indefinite, unimodular lattices are isometric if and only if they have the same rank, signatures and isometric determinants.*

Proof. Let $(V, h) = \langle 1 \rangle$. By Proposition 4.9, there are $k = \#(C_K/C_0)$ isometry classes of lattices in (V, h). Let $L_1,..., L_k$ be a complete set of representatives.

Let us consider two indefinite lattices which have the same rank, determinant and signatures. By Landherr's theorem (Lemma 3.5) we may assume that these lattices, say M and N, are lattices in the same hermitian form (W, g). We can assume that $\dim_K(W) \geqslant 2$, otherwise the statement is obvious.

Let $M_i = M \otimes_A L_i$, $i = 1,..., k$, with $M_1 = M$. The M_i's are lattices in (W, g), and $\det(M_i)$ is not isometric to $\det(M_j)$ if $i \neq j$.

We know by Proposition 4.8 that there are exactly k isometry classes of lattices in (W, g), so every lattice in (W, g) is isometric to one of the M_i's.

Therefore N is isometric to one of the M_i's. But N cannot be isometric to M_i with $i \neq 1$, because $\det(N)$ is not isometric to $\det(M_i)$ if $i \neq 1$. Therefore N and M are isometric.

Relation between the Invariants

There exists a rank n unimodular lattice with determinant (L, h) and signatures $\sigma_1,..., \sigma_s$ if and only if

$$(d, \theta)_{P_i} = (-1)^{(n - \sigma_i)/2}$$

for the infinite primes P_i of F which ramify in K, where d is the discriminant of $(V, h) = (L, h) \otimes K$.

Proof. The necessity of this condition follows from Lemma 3.5.

Conversely, let (W, g) be an n-dimensional hermitian form with discriminant d and signatures $\sigma_1, \ldots, \sigma_s$ (this form exists by Lemma 3.5). There are $k = \#(C_K/C_0)$ isometry classes of unimodular lattices in (W, g) by Proposition 4.8. These lattices have non-isometric determinants. These determinants are lattices in (V, h), and Proposition 4.9 implies that (V, h) contains exactly k isometry classes of lattices, so one of the determinants must be (L, h).

PROPOSITION 4.11. $\varepsilon = +1$. *Let* (L, h) *be an indefinite, unimodular lattice. Then*

(1) (L, h) *is isometric to an orthogonal sum of lattices of rank* 1 *and* 2.

(2) *If at least one finite prime of* F *ramifies in* K, *then* (L, h) *can be diagonalized.*

(3) *If no infinite prime of* F *ramifies in* K, *then*

$$(L, h) \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp (M, g)$$

where $\operatorname{rank}(M) = 1$.

Proof. Let $(V, h) = (L, h) \otimes K$.

(1) If P is an infinite prime of F which ramifies in K, we have $(V, h)_P = \langle e_{1P} \rangle \perp \langle e_{2P} \rangle \perp \cdots \perp \langle e_{nP} \rangle$ with $e_{iP} = \pm 1$. We may assume that $\dim(V) \geqslant 3$, therefore we can relabel the e_{iP}'s in such a way that $e_{1P} \cdot e_{2P} = +1$. Repeat this procedure at each infinite ramified prime. There exists a 2-dimensional form (W, g) with discriminant 1 and such that

$$(W, g)_P = \langle e_{1P} \rangle \perp \langle e_{2P} \rangle$$

for every infinite ramified prime P (see Lemma 3.5). By Lemma 4.6 (W, g) contains a unimodular lattice M. Apply Corollary 4.7, and then continue inductively.

(2) Let $P_1, \ldots, P_s$ be the infinite primes of F which ramify in K. Let $e_i = \pm 1$ such that $\langle e_i \rangle$ is an orthogonal summand of $(V, h)_{P_i}$. Let Q be a finite prime of F which ramifies in K, and let $d \in F^{\cdot}$ such that $(d, \theta)_{P_i} = e_i$, $i = 1, \ldots, s$, $(d, \theta)_Q = e_1, \ldots, e_s$, and that $(d, \theta)_P = +1$ if P is a prime of F different of $P_1, \ldots, P_s$ and Q (such a $d \in F^{\cdot}$ exists by [23, Theorem 71:19]). Let (W, g) be a 1-dimensional hermitian form with discriminant d. (W, g) contains a unimodular lattice by Lemma 4.6. Apply Corollary 4.7 and continue inductively.

(3) In this case Corollary 4.7 implies that any unimodular lattice of rank $<n$ is an orthogonal summand of (L, h). In particular this is true for $\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle$.

Remark. (1) L. Gerstein has proved that every indefinite, not necessarily unimodular, hermitian lattice is isometric to an orthogonal sum of lattices of rank at most 4 (cf. [10]).

(2) If the conditions of (2) or (3) are not satisfied, it is easy to show that there exist rank 2 lattices which cannot be diagonalized.

PROPOSITION 4.12. $\varepsilon = -1$. *Let* (L, h) *be an indefinite unimodular lattice of rank* $2m$.

(1) (L, h) *is isometric to an orthogonal sum of lattices of rank at most* 4.

(2) *Let* $Q_1, \ldots, Q_r$ *be the finite primes of* F *which ramify in* K. *If* $\prod_{i=1,\ldots,r} (-1, \theta)_{Q_i} = +1$, *then* (L, h) *is isometric to an orthogonal sum of lattices of rank* 2.

(3) *If no infinite prime of* F *ramifies in* K, *then*

$$(L, h) \cong \mathbb{H} \perp \cdots \perp \mathbb{H} \perp \mathbb{H}(I)$$

for some A*-ideal* I (see Definition 3.6 for the definition of $\mathbb{H}$ and $\mathbb{H}(I)$).

Proof. Let $(V, h) = (L, h) \otimes K$.

(1) If P is an infinite prime of F which ramifies in K, let $(V, \mu h)_P = \langle e_{1P} \rangle \perp \cdots \perp \langle e_{2mP} \rangle$, where $e_{iP} = \pm 1$ $(\bar{\mu} = -\mu)$. We can assume that $\dim(V) > 4$. Let us relabel the e_{i_P}'s in such a way that $e_{1P} \cdot e_{2P} \cdot e_{3P} \cdot e_{4P} = +1$. Repeat this for every infinite ramified prime. Let (W, g') be a hermitian form of dimension 4, discriminant 1, such that

$$(W, g')_P = \langle e_{1P} \rangle \perp \langle e_{2P} \rangle \perp \langle e_{3P} \rangle \perp \langle e_{4P} \rangle,$$

if P is an infinite ramified prime (this is possible by Lemma 3.5). Let $g = \mu \cdot g'$. We have $1 = (1, \theta)_P = (-1, \theta)_P^2 = 1$, therefore (W, g) contains a unimodular lattice (see Lemma 4.6). Corollary 4.7 implies that this lattice is an orthogonal summand of (L, h). Finish the proof by induction.

(2) For every infinite prime P of F which ramifies in K, let

$$(V, \mu h) = \langle e_{1P} \rangle \perp \cdots \perp \langle e_{2mP} \rangle,$$

$e_{iP} = \pm 1$. We may assume that $e_{1P} \cdot e_{2P} = +1$, because $\dim(V) > 2$. Let $d \in F^{\cdot}$ such that $(d, \theta)_{Q_i} = (-1, \theta)_P = 1$ for all other primes P of F. Such a $d \in F^{\cdot}$ exists by [23, Theorem 71:19]. Let (W, g) be a 2-dimensional skewhermitian form with discriminant d and such that

$$(W, \mu g) = \langle e_{1P} \rangle \perp \langle e_{2P} \rangle$$

(cf. Lemma 3.5). (W, g) contains a unimodular lattice by Lemma 4.6. Apply Corollary 4.7 and continue inductively.

(3) As there are no signatures, Corollary 4.7 implies that $(L, h) \cong \mathbb{H} \perp \cdots \perp \mathbb{H} \perp (M, g)$, with $\mathrm{rank}(M) = 2$. It remains to prove that (M, g) is hyperbolic. By Lemma 3.8 it suffices to prove that (W, g) is hyperbolic, where $W = M \otimes K$. By Lemma 4.6 the discriminant of (W, g) is -1. Therefore Landherr's theorem implies that (W, g) is hyperbolic.

Remark. If the conditions of (2) or (3) are not satisfied then it is easy to prove that there exist indecomposable skew-hermitian lattices of rank 4.

PROPOSITION 4.13 (C. T. C. Wall). *Let (L, h) and (L', h') be indefinite, unimodular ε-hermitian forms such that there exists a unimodular ε-hermitian form (M, g) with*

$$(L, h) \perp (M, g) \cong (L', h') \perp (M, g);$$

then $(L, h) \cong (L', h')$.

Proof. If $\mathrm{rank}(L) \geqslant 3$, this is [31, Theorem 10]. The proof is the same if $\mathrm{rank}(L) = 2$. It suffices to check that Corollary of Theorem 7 is still true if $\mathrm{rank}(L) = 2$. Let P be a finite prime of F which ramifies in K. Then P is non-dyadic by Remark 3.13. If (N, f) is a unimodular (-1)-hermitian lattice, then $(N, f)_P$ is hyperbolic by [31, p. 434, bad tame case]. Therefore we can apply Theorem 4 if $\varepsilon = -1$. If $\varepsilon = +1$, there is nothing to prove as there are no bad primes. The statement is obvious if $\mathrm{rank}(L) = 1$ (take determinants).

5. ISOMETRIC STRUCTURES

An *isometric structure* will be a triple (L, S, z) where L is a free $\mathbb{Z}$-module of finite rank, $S: L \times L \to \mathbb{Z}$ is a $\mathbb{Z}$-bilinear, e-symmetric form ($e = \pm 1$) such that $\det(S) = \pm 1$, and $z: L \to L$ is an endomorphism such that $S(zu, v) = S(u, (1 - z)v)$ for $u, v \in L$.

Two isometric structures (L_1, S_1, z_1) and (L_2, S_2, z_2) are *isomorphic* if there exists an isomorphism $F: L_1 \to L_2$ such that $S_2(F(u), F(v)) = S_1(u, v)$ for $u, v \in L_1$ and such that $Fz_1 = z_2 F$.

Let φ be the minimal polynomial of z. We shall assume that φ is *irreducible.*

Set $K = \mathbb{Q}[X]/(\varphi)$, $A = \mathbb{Z}[X]/(\varphi) = \mathbb{Z}[\alpha]$, where α is a root of φ.

Note that $(-1)^{\deg \varphi} \varphi(1 - X) = \varphi(X)$ [27, p. 13]. Therefore K has a non-trivial $\mathbb{Q}$-involution which sends α to $\bar{\alpha} = 1 - \alpha$.

We shall show that the classification of e-symmetric ($e = \pm 1$) isometric structures with minimal polynomial φ is equivalent to the classification of A-

valued unimodular $(-e)$-hermitian forms on torsion free A-modules of finite rank.

Let (L, S, z) be an isometric structure. Setting $\alpha \cdot v = z(v)$ provides L with an A-module structure. It is a torsion free A-module of rank

$$\frac{\operatorname{rank}_{\mathbb{Z}}(L)}{\operatorname{degree}(\varphi)}.$$

There exists a unique e-hermitian form

$$g: L \times L \to A^*$$

where $A^* = \{x \in K \text{ such that } \operatorname{Tr}_{K/\mathbb{Q}}(xA) \subseteq \mathbb{Z}\}$, given by the formula

$$\operatorname{Tr}_{K/\mathbb{Q}}(g(xu, v)) = S(xu, v) \qquad \text{for} \quad u, v \in L, \ x \in K.$$

(cf. [3, Sect. 1]).

g is unimodular; i.e., $\operatorname{ad}(g): L \to \operatorname{Hom}_A(L, A^*)$, $\operatorname{ad}(g)(u) = g(\ , u)$ is an isomorphism.

Conversely, any pair consisting of a torsion free A-module L and a unimodular e-hermitian form $g: L \times L \to A^*$ determines a unique isometric structure. It is easy to check that this correspondence sends isomorphic isometric structures to isometric e-hermitian forms and conversely.

One can eliminate the inconvenient of dealing with forms taking values in A^* using the following lemma:

LEMMA 5.1. *There exists a* $\gamma \cdot A$, $\bar{\gamma} = -\gamma$, *such that*

$$\gamma \cdot A^* = A.$$

Proof. We have $A = \mathbb{Z}[\alpha]$, therefore $A^* = (1/\varphi'(\alpha))A$ (cf. [16, III, Sect. 1, Corollary of Proposition 2]). Let $\gamma = \varphi'(\alpha)$. It remains to check that $\bar{\gamma} = -\gamma$.

Let $2d = \operatorname{degree}(\varphi) = [K : \mathbb{Q}]$. (The involution is non-trivial therefore $[K : \mathbb{Q}]$ must be even.)

Let $s: K \to \mathbb{Q}$, $s(\sum_{i=0}^{2d-1} x_i \alpha^i) = x_{2d-1}$ as in [30]. It is easy to check that $s(\bar{x}) = -s(x)$.

The proof of Proposition 2 [16, III, Sect. 1] shows that

$$s(x) = \operatorname{Tr}_{K/\mathbb{Q}}(\gamma^{-1} x).$$

We have

$$\begin{aligned} \operatorname{Tr}_{K/\mathbb{Q}}(\bar{\gamma}^{-1} x) &= \operatorname{Tr}_{K/\mathbb{Q}}(\gamma^{-1} \bar{x}) = s(\bar{x}) = s(\bar{x}) = -s(x) \\ &= \operatorname{Tr}_{K/\mathbb{Q}}(-\gamma^{-1} x) \qquad \text{for all} \quad x \in K, \end{aligned}$$

therefore

$$\bar{\gamma}^{-1} = -\gamma^{-1}, \qquad \text{so} \quad \bar{\gamma} = -\gamma.$$

Let $h = \gamma \cdot g$. Then $h: L \times L \to A$ is a unimodular, $(-e)$-hermitian form. Assume that $A = \mathbb{Z}[\alpha]$ is the whole ring of integers of K. Then the results of Sections 1–4 can be used to classify isometric structures with minimal polynomial φ (note that $\varepsilon = -e$).

EXAMPLE 5.2. Let $\lambda(x) = (1-x)^{2d}\,\varphi(1/(1-x))$, where $2d = \text{degree}(\varphi)$. Then $\lambda \in \mathbb{Z}[x]$. We have

$$\lambda(x) = 1 + (1-x)\,f(x) \qquad \text{with} \qquad f(x) \in \mathbb{Z}[x];$$

therefore, $\lambda(1) = 1$.

It is easy to check that $\lambda(x) = x^{2d}\lambda(x^{-1})$. Let $\tau = 1 - \alpha^{-1}$. Then $\lambda(\tau) = 0$. We have $\bar{\tau} = \tau^{-1}$.

If $\varphi(0) = \pm 1$, then the leading coefficient of λ is ± 1. Then we have

$$A = \mathbb{Z}[x]/(\varphi) = \mathbb{Z}[x]/(\lambda).$$

Notice that $\varphi(x) = x^{2d}\lambda(1 - x^{-1})$.

Assume that $\lambda = \lambda_m$ is the mth cyclotomic polynomial. Then A is integrally closed (see for instance [16, IV, Sect. 1, Theorem 4]).

The condition $\lambda_m(1) = 1$ is satisfied if and only if m is not a prime power (see [18, p. 206]).

The number of isomorphism classes of skew-symmetric isometric structures with characteristic polynomial φ is then

$$h_- \cdot 2^d \qquad \text{if} \quad m = 2 \cdot p^k,$$

$$h_- \cdot 2^{d-1} \qquad \text{otherwise},$$

where $h_- = h_K/h_F$ (cf. Corollary 1.3 and Example 2.5).

For the value of h_- see the tables in [11] or [25].

If $e = +1$ we must check the condition of Proposition 1.6 (recall that symmetric isometric structures correspond to skew-hermitian forms!)

The different Δ of K/F is $(\tau - \bar{\tau}) \cdot A$ (cf. [16, III, Sect. 1, Corollary of Proposition 2]).

Then $N_{K/\mathbb{Q}}(\tau - \tau^{-1}) = \lambda(1) \cdot \lambda(-1)$ must be a square. If $m = p^k$, we have $\lambda_m(1) = 1$, $\lambda_m(-1) = p$: therefore we have no symmetric isometric structures with characteristic polynomial φ in this case. If $m \neq 2 \cdot p^k$, p^k, then $\lambda_m(1) = \lambda_m(-1) = 1$. So $\tau - \tau^{-1}$ is a unit, $\Delta = A$, therefore the condition of Proposition 1.6 is satisfied. The number of isomorphism classes of symmetric isometric structures with characteristic polynomial φ is then $h_- \cdot 2^{d-1}$.

Note that if we have two polynomials φ_0 and φ_1 such that $(1-x)^{2d_0}\lambda_0(1/(1-x))=\lambda_m(x)$, $(1-x)^{2d_1}\varphi_1(1/(1-x))=\lambda_m(x)$, where λ_m and λ_n are cyclotomic polynomials such that m/n is not a prime power, then the resultant $R(\varphi_0,\varphi_1)=\pm 1$ (see [27, Proposition 3.4]).

Let $h(\varphi)$ be the number of isomorphism classes of isometric structures with characteristic polynomial φ.

Then [27, Theorem 3.2] implies that $h(\varphi_1\cdot\varphi_2)=h(\varphi_1)\cdot h(\varphi_2)$. We can then compute $h(\varphi_1\cdot\varphi_2)$ using the above formulas.

Remark 5.3. Let $K=\mathbb{Q}[x]/(\varphi)=\mathbb{Q}(\alpha)$, and let F be the fixed field of the Q-involution of K which sends α to $1-\alpha$.

Let $\varphi=\prod_{i=1}^{m} g_i$ with $g_i\in\mathbb{R}[x]$, irreducible. Then the number of infinite primes of F which ramify in K is equal to the number of g_i's such that degree$(g_i)=2$ and $g_i(1-x)=g_i(x)$.

6. Applications to Knot Theory

Let $\Sigma^{2q-1}\subset S^{2q+1}$ be a simple $(2q-1)$-knot, $q\geqslant 3$. Let $M^{2q}\subset S^{2q+1}$ be a Seifert surface of Σ^{2q-1}, and let

$$B\colon Hq(M^{2q},\mathbb{Z})/\text{torsion}\times Hq(M^{2q},\mathbb{Z})/\text{torsion}\to\mathbb{Z}$$

be the associated Seifert form (cf. [20] for the definitions).

We shall say that M^{2q} is *minimal* if M^{2q} is $(q-1)$-connected and if $\det(B)\neq 0$. Such a Seifert surface exists by [21] and [28, p. 485]. $Hq(M^{2q},\mathbb{Z})$ is then a torsion-free $\mathbb{Z}$-module of finite rank. Let $e=(-1)^q$, and $S=B+eB^t$. Then $\det(S)=\pm 1$. Let $z=S^{-1}B$. Then $(Hq(M^{2q},\mathbb{Z}),S,z)$ is an isometric structure (see Section 5). It is easy to check that isomorphic Seifert forms correspond to isomorphic isometric structures and conversely.

Therefore we have:

(1) The isotopy classes of minimal Seifert surfaces correspond biunivoquely to the isomorphism classes of isometric structures (see Levine [20]).

$\det(B)$ is an invariant of the isotopy class of Σ^{2q-1}. Assume that $\det(B)$ is a prime number, or ± 1. Then Σ^{2q-1} has, up to isotopy, only one minimal Seifert surface (see [29, Corollary 4.7]).

Therefore (1) also gives the classification of simple $(2q-1)$-knots in this case. This is for instance the case for simple fibred knots ($\det(B)=\pm 1$).

Let φ be the minimal polynomial and ϕ the characteristic polynomial of z. φ and ϕ are invariants of the isotopy class of Σ^{2q-1}. Note that $\phi(0)=\pm\det(B)$. ϕ is related to the Alexander polynomial Δ of Σ^{2q-1}.

We have:

$$\phi(x) = (-e)^D x^{2D} \Delta(1 - x^{-1}),$$

where $2D = \text{degree}(\Delta)$.

Assume that φ is *irreducible*, and that $A = \mathbb{Z}[x]/(\varphi)$ is *integrally closed.* Then $\phi = \varphi^n$.

Using (1), and Section 5, we can then apply the results of Sections 1–4 to the classification of minimal Seifert surfaces, and also of simple $(2q-1)$-knots if $\phi(0)$ is a prime or ± 1.

For instance Section 1 implies the following:

Let $e = -1$ (i.e., q is odd). For each positive integer n, the number of isomorphism classes of A-modules of rank n which can be realized as $Hq(M^{2q}, \mathbb{Z})$ for a minimal Seifert surface M^{2q} is

$$\begin{array}{ll} h_K/h_F & \text{if } K/F \text{ is ramified,} \\ 2h_K/h_F & \text{if } K/F \text{ is unramified,} \end{array}$$

where $K = Q[x]/(\varphi) = Q(\alpha)$, and F is the fixed field of the Q-involution given by $\bar{\alpha} = 1 - \alpha$.

This follows from Corollary 1.3. For the A-module structure of these modules see Proposition 1.2. The corresponding result for $e = +1$ is more complicated: see Section 1.

Section 2 concerns the classification of minimal Seifert surfaces with a given irreducible Alexander polynomial. Here we shall only write down the results for the quadratic and the cyclotomic case.

EXAMPLE 6.1. Let $\varphi(x) = x^2 - x + a$, irreducible, such that $1 - 4a$ is square free. Let $\Delta(x) = (-e)(ax^2 - (2a-1)x + a)$.

If $e = -1$, the number of isotopy classes of minimal Seifert surfaces of Alexander polynomial Δ is

$$\begin{array}{ll} 2 \cdot h_K & \text{if } 1 - 4a < 0 \\ & \text{and if } 1 - 4a > 0, \text{ and the fundamental} \\ & \text{unit has norm } +1, \\ h_K & \text{if } 1 - 4a > 0 \text{ and the fundamental} \\ & \text{unit has norm } -1. \end{array}$$

If $e = +1$, then this number is zero. Indeed, the condition of Proposition 1.6 implies that $1 - 4a = \pm x^2$ with $x \in \mathbb{Z}$.

If a is a prime or ± 1, then this also gives the number of isotopy classes of simple $(2q-1)$-knots with Alexander polynomial Δ.

For the value of h_K see [4].

EXAMPLE 6.2. Let λ_m be a cyclotomic polynomial with $m = 2 \cdot p^k$ or m composite. Let $2d = \text{degree}(\lambda_m)$.

For $e = -1$, the number of isotopy classes of minimal Seifert surfaces (or of simple fibred $(2q-1)$-knots) with Alexander polynomial λ_m is

$$\begin{array}{ll} h_- \cdot 2^d & \text{if } m = 2 \cdot p^k, \\ h_- \cdot 2^{d-1} & \text{if } m \text{ is composite,} \end{array}$$

where $h_- = h_K/h_F$.

For $e = +1$, this number is

$$\begin{array}{ll} 0 & \text{if } m = 2 \cdot p^k, \\ h_- \cdot 2^{d-1} & \text{if } m \text{ is composite,} \end{array}$$

(cf. Example 5.2).

For the value of h_- see the tables in [11] or [25].

For $n > 1$ we have:

PROPOSITION 6.3. *Let φ be such that no infinite prime of F ramifies in K (see Remark 5.3 for the equivalent condition on φ). Let Σ^{2q-1}, Σ_1^{2q-1} be simple $(2q-1)$-knots with minimal polynomial φ.*

Let φ^n be the characteristic polynomial of Σ^{2q-1} and φ^m the characteristic polynomial of Σ_1^{2q-1}.

Assume that $m < n$. Then there eists a simple $(2q-1)$-knot Σ_2^{2q-1} such that

$$\Sigma^{2q-1} \sim \Sigma_1^{2q-1} + \Sigma_2^{2q-1},$$

where $\sim$ denotes "isotopic" and $+$ denotes connected sum (cf. Corollary 4.7).

This proposition is true without assuming that the determinant of the Seifert form is prime or ± 1. To see this, recall that isomorphic isometric structures correspond to isotopic knots (see [20]).

Proposition 6.3 can be used to obtain counterexamples of unique factorisation of higher-dimensional knots (see [2] for explicit counterexamples).

Assume that φ is such that at least one infinite prime of F does not ramify in K (see Remark 5.3 for the equivalent condition on φ).

In this case we also have a similar (but weaker) result to Proposition 6.3: see Corollary 4.7. Further, we have:

PROPOSITION 6.4: q odd $(e = -1)$. *Let Σ^{2q-1} be a simple $(2q-1)$-knot with minimal polynomial φ. Then*

(1) $\Sigma^{2q-1} \sim \Sigma_1^{2q-1} + \cdots + \Sigma_m^{2q-1}$, *where the* Σ_i^{2q-1} *are simple knots with characteristic polynomial* φ *or* φ^2.

(2) *If at least one finite prime of F ramifies in K, then*

$$\Sigma^{2q-1} \sim \Sigma_1^{2q-1} + \cdots + \Sigma_n^{2q-1}$$

such that the characteristic polynomial of Σ_i^{2q-1} *is* φ *for* $i = 1,..., n$ (*see Proposition* 4.11).

The analogue of Proposition 6.4 for q even $(e = +1)$ follows from Proposition 4.12.

Remark 6.5. Propositions 6.3 and 6.4 are also true if we replace "simple knot" by "minimal Seifert surface."

PROPOSITION 6.6. *Let* M^{2q}, M_1^{2q} *and* M_2^{2q} *be minimal Seifert surfaces with minimal polynomial* φ, *and assume that* $M_1^{2q} + M^{2q} \sim M_2^{2q} + M^{2q}$. *Then* $M_1^{2q} \sim M_2^{2q}$ (*cf. Proposition* 4.13).

Note that this is also true for simple fibred knots.

One can also use the results of Section 4 to compute class numbers. We shall illustrate this with some examples.

EXAMPLE 6.7. Let $\varphi(x) = x^2 - x + a$ irreducible, such that $1 - 4a$ is square free. Assume that $1 - 4a < 0$. Let $e = -1$ (q odd). Then for every positive integer n, the number of isotopy classes of minimal Seifert surfaces with minimal polynomial φ and characteristic polynomial φ^n is

$2 \cdot h_K$	if the norm of the fundamental unit is $+1$,
h_K	if the norm of the fundamental unit is -1

(cf. Example 6.1 and Proposition 4.11.3).

If $e = +1$ then the characteristic polynomial must be of the form φ^{2m} (see Example 6.1). We have:

For every positive integer m, the number of isotopy classes of minimal Seifert surfaces with minimal polynomial φ and characteristic polynomial φ^{2m} is h_K (cf. Proposition 4.8.2).

For instance if $a = -1$, $\varphi(x) = x^2 - x - 1$, then $h_K = 1$ and the norm of the fundamental unit is -1 (see the tables in [4]). Therefore the class number is 1 both for $e = -1$ and $e = +1$.

EXAMPLE 6.8. Let $\lambda(x) = x^4 - 5x^3 + 9x^2 - 5x + 1$, $\varphi(x) = x^4\lambda(1 - x^{-1})$. λ and are irreducible (λ is irreducible mod 2).

q odd. For every positive integer n there exist exactly two isotopy classes of simple fibred $(2q-1)$-knots with minimal polynomial φ and Alexander polynomial λ^n.

q even. Then the Alexander polynomial must be of the form λ^{2m}, because $\lambda(-1)$ is not a square (see [22, Theorem 1(d)] or Proposition 1.6).

For every positive integer m there exists exactly one isotopy classes of simple fibred $(2q-1)$-knots with minimal polynomial φ and Alexander polynomial λ^{2m}.

Indeed, $A=\mathbb{Z}[x]/(\varphi)=\mathbb{Z}[x]/(\lambda)$. Then A is integrally closed (see [19, p. 95]). The fixed field of the involution is $F=\mathbb{Q}(\sqrt{-3})$. Therefore K and F are both totally imaginary, so no infinite prime of F ramifies in K. We have $h_K=1$ (apply [16, V, Sect. 4, Theorem 4]). The different Δ of K/F is $(\tau-\tau^{-1})A$, where τ is a root of λ.

But $N_{K/\mathbb{Q}}(\tau-\tau^{-1})=\lambda(1)\cdot\lambda(+1)=21$, therefore exactly two finite primes of F ramify in K. Proposition 2.6 implies $\#[U_0/N(U)]=2$ (in fact one can check that $-1\notin N(U)$, so $\{+1,-1\}$ is a set of representatives of $U_0/N(U)$).

For $e=-1$ (q odd) apply Proposition 4.11.3, Proposition 2.1 and Corollary 1.3 (one can also apply Proposition 4.8). For $e=+1$ (q even), apply Proposition 4.8.

EXAMPLE 6.9. Let $\lambda(x)=x^4+x^3-3x^2+x+1$, $\varphi(x)=x^4\lambda(1-x^{-1})$. Then λ and φ are irreducible, because λ is irreducible mod 2.

q odd. The number of isotopy classes of simple fibred $(2q-1)$-knots with minimal polynomial φ and Alexander polynomial λ^n is $n+1$.

q even. Then the Alexander polynomial must be of the form λ^{2m} because $\lambda(-1)$ is not a square.

The number of isotopy classes of simple fibred $(2q-1)$-knots with minimal polynomial φ and Alexander polynomial λ^{2m} is m if m is odd, and $m+1$ if m is even.

Indeed, we see that $A=\mathbb{Z}[x]/(\varphi)=\mathbb{Z}[x]/(\lambda)$ is integrally closed [19, p. 95].

The fixed field of the involution is $F=\mathbb{Q}(\sqrt{21})$. It is straightforward to check that λ has two real and two imaginary roots, therefore exactly one infinite prime of F ramifies in K. We have $h_K=1$. Inded, [16, V, Sect. 4, Theorem 4] implies that every ideal class contains an ideal of norm at most 4. But there are no ideals of norm 2 or 4 because λ is irreducible mod 2. It remains to check that the prime ideals of norm 3 are principal. The different Δ of K/F is $(\tau-\tau^{-1})A$, where τ is a root of λ, and we have $N_{K/\mathbb{Q}}(\tau-\tau^{-1})=\lambda(1)\,\lambda(-1)=-3$. So $\Delta=P$, with $N_{K/\mathbb{Q}}(P)=3$. Let $P_0=P\cap A_0$, then $P_0A=P^2$. The discriminant of F is 21, therefore $3A_0=P_0^2$. So we have $3A = P^4$. This implies that P is the only A-ideal of norm 3. But P is principal, as $P = (\tau - \tau^{-1})A$. So we have proved that $h_K = 1$.

Let $e = -1$ (q odd). We shall apply Proposition 4.8 with $\varepsilon = -e = +1$.

Let us determine the number of isometry classes of nonsingular hermitian forms $h: V \times V \to K$, $\dim(V) = n$, which contain a unimodular lattice. The number of possible signatures is $n + 1$. Let d be the discriminant of (V, h). We must have $(d, \theta)_P = +1$ for P unramified (see Lemma 4.6), and $(d, \theta)_P$ for P infinite is determined by the choice of the signature. Exactly one finite prime P_0 of F ramifies in K.

Therefore $(d, \theta)_{P_0}$ is also determined by Hilbert reciprocity. $e = +1$ (q even). Let (V, h) be a non-singular skew-hermitian form containing a unimodular lattice, $\dim(V) = 2m$. Let d be the discriminant of (V, h). By Lemma 4.6 we have $(d, \theta)_P = +1$ if P is unramified, and $(d, \theta)_{P_0} = (-1, \theta)^m_{P_0}$ for the unique finite ramified prime P_0. We have $N_{F/Q}(P_0) = 3$, therefore $(-1, \theta)_{P_0} = -1$ (cf. [27, Claim, p. 40]). If m is odd we have $(d, \theta)_{P_0} = -1$. So by Hilbert reciprocity we have $(d, \theta)_P = -1$ for the unique infinite ramified prime P. So we have exactly m possible signatures. If m is even, then $(d, \theta)_{P_0} = (-1, \theta)^m_{P_0} = +1$, so $(d, \theta)_{P_0} = +1$ for the infinite ramified prime P. So there are $m + 1$ possible signatures. Apply Proposition 4.8.

Acknowledgments

I want to thank A. Fröhlich, M. Kervaire and W. Scharlau for many useful conversations. I also thank K. Ribet and P. Schneider who have helped me with the computation of $U_0/N(U)$. I thank the Department of Mathematics of the University of Münster and Professor W. Scharlau for their hospitality during the academic year 1979/80. I thank the "Fonds National Suisse de la recherche scientifique" for their support during the redaction of this paper.

References

1. A. Bak and W. Scharlau, Grothendieck and Witt groups of orders and finite groups, *Invent. Math.* **23** (1974), 207–240.
2. E. Bayer, Factorisation is not unique for higher dimensional knots, *Comm. Math. Helv.* **55** (1980), 583–592.
3. E. Bayer and F. Michel, Finitude du nombre des classes d'isomorphisme des structures isométriques entières, *Comm. Math. Helv.* **54** (1979), 378–396.
4. Z. I. Borevitch and I. R. Chafarevitch, "Théorie des nombres," Gauthier–Villars, Paris.
5. A. Brumer and M. Rosen, Class number and ramification in number fields, *Nagoya Math. J.* **23** (1963), 97–101.
6. C. Bushnell, Modular quadratic and hermitian forms over Dedekind rings, I, *J. Reine Angew. Math.* **286/287** (1976), 169–186.
7. C. Bushnell, Modular quadratic and hermitian forms over Dedekind rings, II, *J. Reine Angew. Math.* **288** (1976), 24–36.

8. J. W. S. CASSELS AND A. FRÖHLICH, "Algebraic Number Theory," Academic Press, New York, 1967.
9. A. FRÖHLICH, On the K-theory of unimodular forms over rings of algebraic integers, *Quart. J. Math. Oxford (2)* **22** (1971), 401–424.
10. L. GERSTEIN, Integral decomposition of hermitian forms, *Amer. J. Math.* **92** (1970), 398–417.
11. H. HASSE, "Über die Klassenzahl abelscher Zahlkörper," Akademie-Verlag, Berlin.
12. K. IWASAWA, A note on the group of units of an algebraic number fields, *J. Math. Pures Appl.* **35** (1956), 189–192.
13. R. JACOBOWITZ, Hermitian forms over local fields, *Amer. J. Math.* **84** (1962), 441–465.
14. M. KNEBUSCH, A. ROSENBERG, AND R. WARE, Grothendieck and Witt rings of hermitian forms over Dedekind rings, *Pacific J. Math.* **43**, No. 3 (1972), 657–673.
15. W. LANDHERR, Äquivalenz Hermitescher Formen über einen beliebigen algebraischen Zahlkörper, *Abh. Math. Sem. Univ. Hamburg* **11** (1935), 245–248.
16. S. LANG, "Algebraic Number Theory," Addison–Wesley, Reading, Mass.,
17. S. LANG, "Cyclotomic Fields," Springer-Verlag, Berlin/New York,
18. S. LANG, "Algebra," Addison–Wesley, Reading, Mass.,
19. J. P. LEVINE, "Algebraic Structure of Knot Modules," Lecture Notes in Mathematics 772, Springer-Verlag, Heidelberg/Berlin/New York, 1980.
20. J. P. LEVINE, An algebraic classification of some knots of codimension two, *Comm. Math. Helv.* **45** (1970), 185–198.
21. J. P. LEVINE, Unknotting spheres in codimension two, *Topology* **4** (1965), 9–16.
22. J. P. LEVINE, Polynomial invariants of knots of codimension two, *Ann. of Math.* **84** (1966), 537–554.
23. O. T. O'MEARA, "Introduction to Quadratic Forms," Springer-Verlag, Berlin/New York,
24. P. SAMUEL, "Théorie algébrique des nombres," Collection Méthodes, Hermann, Paris,
25. G. SCHRUTKA VON RECHTENSTAMM, Tabelle der (relativ-) Klassenzahlen von Kreiskörpern, *Abh. Deutsche Akad. Wiss. Berlin 1964*, *Math. Nat. Kl. Nr 2.*
26. G. SHIMURA, Arithmetic of unitary groups, *Ann. of Math.* **79**, No. 2 (1964), 369–409.
27. N. W. STOLTZFUS, Unraveling the integral knot concordance group, *Mem. Amer. Math. Soc.* **12**, No. 192 (1977).
28. H. F. TROTTER, Homology of group systems with applications to knot theory, *Ann. of Math.* **76** (1962), 464–498.
29. H. F. TROTTER, On S-equivalence of Seifert matrices, *Invent. Math.* **20** (1973), 173–207.
30. H. F. TROTTER, Knot modules and Seifert matrices, *in* "Knot Theory," Lecture Notes in Mathematics 685, Springer-Verlag, Heidelberg/Berlin/New York, 1975.
31. C. T. C. WALL, On the classification of hermitian forms. I. Rings of algebraic integers, *Compos. Math.* **22** (1970), 425–451.