Pure and Applied Mathematics Quarterly
Volume 8, Number 4
1117—1146, 2012

On Hermitian Forms over Dyadic Non-maximal Local Orders

Chia-Fu Yu

Abstract: We reduce a study of polarized abelian varieties over finite fields to the classification problem of skew-Hermitian modules over (possibly non-maximal) local orders. The main result of this paper gives a complete classification of these skew-Hermitian modules for the case where the ground ring is a dyadic non-maximal local order.
Keywords: hermitians forms, abelian varieties, local orders.

1. Introduction

Let p be a rational prime number. Let $R := \mathbb{Z}_2[X]/(X^2+p) = \mathbb{Z}_2[\pi]$, an order of the $\mathbb{Q}_2$-algebra $E := \mathbb{Q}_2[X]/(X^2+p)$, where $\mathbb{Z}_2$ is the ring of 2-adic integers, and π is the image of X in R. Denote by $a \mapsto \bar{a}$ the non-trivial involution on E and O_E the ring of integers in E. By a skew-Hermitian module over R we mean a $\mathbb{Z}_2$-free finite R-module M together with a $\mathbb{Z}_2$-valued non-degenerate alternating pairing

$$\psi : M \times M \to \mathbb{Z}_2$$

such that $\psi(ax, y) = \psi(x, \bar{a}y)$ for all $a \in R$ and $x, y \in M$. If M is self-dual with respect to the pairing ψ, then it is called a self-dual skew-Hermitian R-module. In this paper we study the classification of self-dual skew-Hermitian modules over R. As an elementary fact, the ring R is the maximal order if and only if $p = 2$ or $p \equiv 1 \pmod 4$. It is easier to handle the case where R is maximal; the classification is known even for any non-Archimedean local maximal order of characteristic not equal to 2, due to Jacobowitz [6]. We give an exposition of the

Received July 14, 2010
MSC (2010): 11E41, 14K15.

classification in Section 2, for the reader's convenience. The main part of this paper treats the case where R is not maximal, that is, the case $p \equiv 3 \pmod 4$. We now describe the main results.

Let $r \geq 1$ be an integer. Let S_r be the set of symmetric matrices in $\mathrm{GL}_r(\mathbb{F}_2)$. Define the equivalence relation $\sim$ on S_r by $A \sim B$, for $A, B \in S_r$, if there exists a matrix $P \in \mathrm{GL}_r(\mathbb{F}_2)$ such that $B = P^t AP$. Denote by $S_r/\sim$ the set of equivalence classes in S_r. Define integers m_r for $r \geq 0$ by $m_0 := 1$ and

$$m_r := \#S_r/\sim, \quad \forall\, r \geq 1. \tag{1.1}$$

Theorem 1.1. *Assume $p \equiv 7 \pmod 8$. There are*

$$\sum_{r=0}^{n} m_r \tag{1.2}$$

non-isomorphic self-dual skew-Hermitian R-modules of $\mathbb{Z}_2$-rank $2n$.

Theorem 1.2. *Assume $p \equiv 3 \pmod 8$. There are*

$$\sum_{r=0}^{n} m_r \tag{1.3}$$

non-isomorphic self-dual skew-Hermitian R-modules of $\mathbb{Z}_2$-rank $2n$.

The proofs are given in Sections 4 and 5. Though the statements of Theorems 1.1 and 1.2 look the same, the structures in the classification are different. It is easy to compute the integers m_r; see Lemma 4.7. The classification problem for ($\mathbb{Z}_2$-valued) skew-Hermitian R-modules is equivalent to the same problem for Hermitian R-modules. Indeed, let (M, ψ) be a skew-Hermitian module over R. Then there is a unique Hermitian form

$$\varphi : M \times M \to 2^m R$$

such that

$$\psi(x, y) := \mathrm{Tr}_{E/\mathbb{Q}_2}\, \pi\varphi(x, y), \quad \forall\, x, y \in M.$$

Here m is the largest integer such that $R^\vee \subset 2^m R$, where $R^\vee$ is the dual lattice of R for the pairing $(a, b) \mapsto \mathrm{Tr}_{E/\mathbb{Q}_2}(ab)$; in fact $m = 0$ or -1 depending on whether R is maximal or not, cf. § 5.1. Conversely, given a Hermitian R-module (M, φ) we get a ($\mathbb{Z}_2$-valued) skew-Hermitian R-module (M, ψ) by setting

$$\psi(x, y) := \mathrm{Tr}_{E/\mathbb{Q}_2}\, \pi\varphi(x, y), \quad \forall\, x, y \in M.$$

It is worth noting that when $p \equiv 3 \pmod 4$, the ground ring R is not hereditary (see Remark 3.4), nor the condition that $a + \bar{a} = 1$ for some $a \in R$ is not fulfilled. Therefore, results in the paper complement those of Riehm [12], and a general Witt type cancellation theorem [1, Theorem 3] obtained by Bayer-Fluckiger and Fainsilber; see Propositions 4.4 and 5.7.

The motivation of this work is to determine the Tate modules of certain abelian varieties over finite fields as Galois modules. The reader who is not familiar with abelian varieties may consult the reference [9] by Mumford. An abelian variety A over a field k of characteristic p is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over an algebraic closure $\bar{k}$ of k. Let $\Sigma_n(\mathbb{F}_p)$ denote the set of isomorphism classes of n-dimensional superspecial abelian varieties (A, λ) over $\mathbb{F}_p$ together with a principal polarization λ over $\mathbb{F}_p$ such that $\pi_A^2 = -p$, where π_A is the Frobenius endomorphism of A. Suppose (A, λ) is an element in $\Sigma_n(\mathbb{F}_p)$. For any prime $\ell \neq p$, the associated Tate module $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2n$ together with a continuous action ρ_A of the Galois group $\mathcal{G} := \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ and a Galois equivariant self-dual alternating pairing (the Weil pairing)

$$e_\ell : T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell(1),$$

where

$$\mathbb{Z}_\ell(1) := \lim_{\leftarrow} \mu_{\ell^m}(\overline{\mathbb{F}}_p)$$

is the Tate twist. Let $\sigma : x \mapsto x^p$ be the Frobenius automorphism of $\mathcal{G}$. Since $\sigma x = \pi_A x$ for all $x \in T_\ell(A)$, the action of the Galois group $\mathcal{G}$ on the Tate module $T_\ell(A)$ factors through the quotient

$$\mathbb{Z}_\ell[\mathcal{G}] \to \mathbb{Z}_\ell[X]/(X^2 + p) = \mathbb{Z}_\ell[\pi_A].$$

The pairing e_ℓ induces an involution $a \mapsto \bar{a}$ on $\mathbb{Z}_\ell[\pi_A]$ by the adjoint. It follows from $\pi_A \overline{\pi}_A = p$ and $\pi_A^2 = -p$ that this involution is non-trivial. Fix an isomorphism $\mathbb{Z}_\ell(1) \simeq \mathbb{Z}_\ell$ as $\mathbb{Z}_\ell$-modules. The problem of classifying Tate modules of superspecial abelian varieties in $\Sigma_n(\mathbb{F}_p)$ as $\mathcal{G}$-modules together to the Weil pairing amounts to

(1) classifying self-dual skew-Hermitian modules over the ring $\mathbb{Z}_\ell[X]/(X^2+p)$, and

(2) determining the image of $\Sigma_n(\mathbb{F}_p)$ in the set of isomorphism classes of skew-Hermitian modules over $\mathbb{Z}_\ell[X]/(X^2+p)$.

The second problem seems to be hard. Besides, in order to state the result of the second problem, one needs an explicit description of the classification. In this paper we limit ourselves to the first problem.

As mentioned before, if the ring $\mathbb{Z}_\ell[X]/(X^2+p)$ is the maximal order in the (commutative and semi-simple) $\mathbb{Q}_\ell$-algebra $\mathbb{Q}_\ell[X]/(X^2+p)$, then the classification is known. As well-known the ring $\mathbb{Z}_\ell[X]/(X^2+p)$ is maximal except when $\ell=2$ and $p\equiv 3 \pmod 4$, which is also the most complicated case. Theorems 1.1 and 1.2 solve the first problem in this exceptional case. An immediate consequence of Theorems 1.1 and 1.2 (also using Lemma 4.7) is the following result.

Theorem 1.3. *Notation as above. Assume* $p\equiv 3 \pmod 4$. *There are at most* $n+\lfloor n/2\rfloor$ *isomorphism classes of polarized* 2*-adic Tate modules* $(T_2(A),\rho_A,e_2)$ *for all elements* (A,λ) *in* $\Sigma_n(\mathbb{F}_p)$.

The paper is organized as follows. In Section 2 we give an exposition of the classification of Hermitian forms over non-Archimedean local maximal orders of characteristic not equal to 2, following Jacobowitz [6]. Section 3 gives the complete classification of R-modules. Sections 4 and 5 treat the classification of skew-Hermitian R-modules in the split case $p\equiv 7 \pmod 8$ and the inert case $p\equiv 3 \pmod 8$ separately.

Acknowledgments. The manuscript is prepared during the author's stay at l'Institut des Hautes Études Scientifiques. He acknowledges the institution for kind hospitality and excellent working conditions. The research was partially supported by grants NSC 97-2115-M-001-015-MY3 and AS-99-CDA-M01. The author acknowledges the referee for his/her careful reading and helpful comments which remove many errors and inaccuracies.

2. Hermitian forms over local fields

In this section we give an exposition of the classification of Hermitian forms over local maximal orders, for the reader's convenience. Our reference is Jacobowitz [6].

2.1. **Hermitian spaces.** Let F be a non-Archimedean local field of $\operatorname{char} F \neq 2$. Let O_F be the ring of integers of F, and π_F a uniformizer of O_F. Let E be a quadratic field extension of F; E is necessarily separable over F. Let O_E be the ring of integers in E, and π a uniformizer of O_E. Write $a \mapsto \bar{a}$ for the non-trivial automorphism of E over F, and let $\pi = \pi_F$ if the extension E/F is unramified. Let v be the normalized valuation on E such that $v(\pi) = 1$.

By a Hermitian space over E we mean a finite-dimensional vector V over E, together with an F-bilinear pairing

$$h : V \times V \to E$$

such that $h(ax, by) = a\bar{b}h(x, y)$ and $h(y, x) = \overline{h(x, y)}$ for all $a, b \in E$ and $x, y \in V$. The pairing h is called a Hermitian form. It is called *non-degenerate* if the induced linear map $V \to V^* := \operatorname{Hom}_E(V, E)$ by $x \mapsto h(\cdot, x)$ is injective (and hence isomorphic). By a Hermitian module over O_E we mean a finite free O_E-module L together with a Hermitian form h on $V = E \otimes_{O_E} L$, not necessarily assumed that $h(L, L) \subset O_E$. It is called *non-degenerate* if the Hermitian E-space (V, h) is non-degenerate; it is *unimodular* if $h(L, L) \subset O_E$ and the induced map $L \to L^* := \operatorname{Hom}_{O_E}(L, O_E)$ is an isomorphism. A full rank O_E-submodule in a Hermitian E-space is usually called an O_E-lattice. A decomposition of a Hermitian module (resp. space) L into submodules (resp. subspaces) L_1 and L_2:

$$L = L_1 \oplus L_2$$

means that $L = L_1 + L_2$, $L_1 \cap L_2 = 0$ and $h(x, y) = 0$ for all $x \in L_1$ and $y \in L_2$. For a submodule (resp. subspace) L_1 of L, denote by $L_1^\perp$ the orthogonal complement of L_1 in L.

Lemma 2.1. *Any Hermitian space (V, h) over E has a decomposition*

$$V = V^\perp \oplus V_1,$$

where V_1 is any E-linear subspace complementary to the null subspace $V^\perp$. The Hermitian subspace V_1, if non-zero, is non-degenerate and the projection $V_1 \to V/V^\perp$ is isometric.

From now on, we assume that (V, h) is non-degenerate. The *determinant* or *discriminant* of V (resp. of a lattice L), denoted by dV (resp. dL), is defined as $\det(h(x_i, x_j))$, where $x_1, \ldots, x_n$ is an E-basis for V (resp. an O_E-basis for L). The determinant dV (resp. dL) is unique up to an element in $N_{E/F}(E^\times)$ (resp.

$N_{E/F}(O_E^\times)$). Write $dV_1 \simeq dV_2$ (resp. $dL_1 \simeq dL_2$) if there is an element $a \in N_{E/F}(E^\times)$ (resp. $a \in N_{E/F}(O_E^\times)$) such that $dV_2 = a \cdot dV_1$ (resp. $dL_2 = a \cdot dL_1$).

Theorem 2.2.

(1) *We have* $V = Ex_1 \oplus \cdots \oplus Ex_{n-1} \oplus Ex_n$ *with* $h(x_i, x_i) = 1$ *for* $i = 1, \ldots, n-1$ *and* $h(x_n, x_n) = dV$.
(2) *Two Hermitian spaces* V_1 *and* V_2 *over* E *are isometric if and only if* $\dim V_1 = \dim V_2$ *and* $dV_1 \simeq dV_2$.

Proof. This is Theorem 3.1 of [6]. The statement (1) follows from the fact that any non-degenerate quadratic form of rank ≥ 4 over F represents every non-zero element in F. The statement (2) follows from (1).

2.2. **General properties of Hermitian lattices.** Let (L, h) be a Hermitian lattice. For any elements $x_1, \ldots, x_n$ in L, denote by $< x_1, \ldots, x_n >_{O_E}$ the O_E-submodule generated by $x_1, \ldots, x_n$. If L has an orthogonal basis $x_1, \ldots, x_n$ with $h(x_i, x_i) = \alpha_i$, we will write

$$L =< x_1 > \oplus \cdots \oplus < x_n > \simeq (\alpha_1) \oplus \cdots \oplus (\alpha_n).$$

Definition 2.3.

(1) A vector $x \in L$ is called *maximal* if $x \notin \pi L$.
(2) Let $sL := \{h(x, y) | x, y \in L\}$, and let nL be the O_E-submodule in E generated by elements $h(x, x)$ for all $x \in L$. Clearly, one has $nL \subset sL$.
(3) We call L *normal* if $nL = sL$, and *subnormal* otherwise.
(4) A lattice L is called π^i*-modular*, where $i \in \mathbb{Z}$, if $h(x, L) = (\pi^i)$ for every maximal vector $x \in L$; L is called *modular* if it is π^i-modular for some $i \in \mathbb{Z}$.

Clearly, if L_1 and L_2 are both π^i-modular, then so is their direct sum $L_1 \oplus L_2$. Any rank one lattice is modular. The lattice $L =< x, y >$ with $v(h(x, y)) = i, v(h(x, x) > i$, and $v(h(y, y)) > i$ is a π^i-modular plane. We write

$$\begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$$

for the Hermitian plane (O_E^2, h) with $h(e_1, e_1) = a$, $h(e_1, e_2) = b$ and $h(e_2, e_2) = c$. For any $i \in \mathbb{Z}$, define the hyperbolic plane $H(i)$ to be

$$\begin{pmatrix} 0 & \pi^i \\ \bar{\pi}^i & 0 \end{pmatrix}.$$

Proposition 2.4. *There is an O_E-basis $x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_s$ such that*

$$V = < x_1 > \oplus \cdots \oplus < x_r > \oplus < y_1, z_1 > \oplus \cdots \oplus < y_s, z_s >$$

and all components are modular.

Proof. This is Proposition 4.3 of [6].

Proposition 2.5. *A π^i-modular lattice L has an orthogonal basis if any of the following conditions holds:*

(1) *L has odd rank.*
(2) *L is normal.*
(3) *$i = 0$ and there is an element $a \in E$ such that $v(a) = v(a + \bar{a}) = 0$.*

Proof. This is Proposition 4.4 of [6].

Definition 2.6.

(1) For any integer $j \in \mathbb{Z}$, define

$$L_{(j)} := \{x \in L \,|\, h(x, L) \subset (\pi^j)\}.$$

This defines a decreasing filtration $\{L_{(j)}\}$ on L.

(2) A decomposition $L = \oplus_{1 \le \lambda \le t} L_\lambda$ of L is called a *Jordan splitting* if each L_λ is modular and

$$sL_1 \supsetneq \ldots, \supsetneq sL_t.$$

Two Jordan splittings

$$L = \oplus_{1 \le \lambda \le t} L_\lambda, \quad K = \oplus_{1 \le \lambda \le T} K_\lambda$$

are said to be of the *same type* if $t = T$, and for each λ, one has

$$sL_\lambda = sK_\lambda, \quad \operatorname{rank} L_\lambda = \operatorname{rank} K_\lambda,$$

and either both L_λ and K_λ are normal or both are subnormal.

It follows from Proposition 2.4 that every lattice has a Jordan splitting. Any two Jordan splittings of a lattice L are of the same type (see [6, p. 449]). For a Jordan splitting $L = \oplus_\lambda L_\lambda$, define the integers $s(\lambda)$ and $u(\lambda) = u_L(\lambda)$ for $\lambda = 1, \dots, t$ by

$$sL_\lambda = (\pi^{s(\lambda)}), \quad nL_{(s(\lambda))} = (\pi^{u(\lambda)}),$$

and the fractional O_E-ideals $\mathfrak{f}(\lambda)$ for $\lambda = 1, \dots, t-1$ by

$$\mathfrak{f}(\lambda) := (\pi^{u(\lambda)+u(\lambda+1)-2s(\lambda)}).$$

Since any two splittings are of the same type, the invariant $\{s(\lambda)\}$, and hence the invariants $\{u(\lambda)\}$ and $\{\mathfrak{f}(\lambda)\}$ are independent of the choice of Jordan splittings.

Theorem 2.7. *Suppose E/F is unramified. Then*

(1) *There is an element a in E such that $v(a) = v(a + \bar{a}) = 0$.*
(2) *Any π^i-modular lattice L is isomorphic to $(\pi^i) \oplus \dots, \oplus(\pi^i)$.*
(3) *Any two lattices are isometric if and only if they are of the same type.*

Proof. This is Theorem 7.1 of [6].

Theorem 2.8. *Suppose that E/F is ramified and non-dyadic.*

(1) *Let L be a π^i-modular lattice of rank n.*
If $i = 2d$ is even, then

$$L \simeq (\pi^d) \oplus \cdots \oplus (\pi^d) \oplus (\pi^{-(n-1)d} dL).$$

If i is odd, then n is even and

$$L \simeq H(i) \oplus \cdots \oplus H(i).$$

(2) *Let L and K be two lattices with Jordan splittings $\oplus L_\lambda$ and $\oplus K_\lambda$, respectively. Then $L \simeq K$ if and only if L and K are of the same type and $dL_j \simeq dK_j$ for every index j for which $s(j)$ is even.*

Proof. These are Proposition 8.1 and Theorem 8.2 of [6].

Theorems 2.7 and 2.8 complete the classification in the cases where E/F is unramified, or E/F is ramified and non-dyadic. It remains to describe the ramified dyadic case.

2.3. **The ramified dyadic case: modular lattices.** In the remaining of this section we assume that E/F is ramified and dyadic.

Proposition 2.9. *Suppose that L is a π^i-modular lattice of rank ≥ 3. Then*

$$L \simeq L_0 \oplus H(i) \oplus \cdots \oplus H(i).$$

where L_0 is a π^i-modular lattice of rank one or two satisfying $nL_0 = nL$.

Proof. This is Proposition 10.3 of [6].

Proposition 2.10. *Let L_1 and L_2 be two π^i-modular lattices. If $L_1 \oplus H(i) \simeq L_2 \oplus H(i)$, then $L_1 \simeq L_2$.*

Proof. This is Proposition 9.3 of [6].

By Propositions 2.9 and 2.10, the classification of modular lattices is reduced to the case of planes. Furthermore we may assume that $i = 0$ or 1.

We need a classification of dyadic ramified extensions. For an element a in $O_F^\times$, denote by $\mathfrak{d}_F(a)$ the smallest O_F-ideal J such that $a \mod J$ is a square. If a is a square, then define $\mathfrak{d}_F(a)$ to be (0). Since the squaring $x \mapsto x^2$ is an automorphism on $O_F/(\pi_F)$, one has $\mathfrak{d}_F(a) \subset (\pi_F)$ for any $a \in O_F^\times$. It is known that the O_F-ideals occurring as $\mathfrak{d}_F(a)$ for some $a \in O_F^\times$ are precisely $(0), (4)$, and all (π_F^{2k+1}) with $0 < 2k+1 < v_F(4)$ where $v_F(\pi_F) = 1$. Furthermore, one has

$$\mathfrak{d}_F(1 + \pi_F^{2k+1}\delta) = (\pi_F^{2k+1})$$

for every $\delta \in O_F^\times$ and every integer k such that $0 < 2k+1 < v_F(4)$.

Write $E = F(\sqrt{\theta})$, where θ is a non-square unit or a prime element. We have the following two cases [6, p. 451]:

(a) θ is a prime element, or
(b) θ is a unit and $\mathfrak{d}_F(\theta) = (\pi_F^{2k+1})$ with $0 < 2k+1 < v_F(4)$. In this case,

$$E = F((1 + \pi_F^{2k+1}\delta)^{1/2})$$

for some unit $\delta \in O_F^\times$.

Note that the case $\mathfrak{d}_F(\theta) = (4)$ occurs only when E/F is unramified. We refer the case (a) as *ramified prime*, ("R-P"), and the case (b) as *ramified unit*, ("R-U").

We use a notation from [6, p. 450]: to indicate an unspecified element a in E with $v(a) \geq v(b)$, we shall write $a = \{b\}$; to indicate an unspecified element a with $v(a) = v(b)$, write $a = [b]$.

Proposition 2.11.

(1) *If L is π^i-modular, then $nL \supset nH(i)$.*

(2) *If $a \in F$ is any element in $nH(i)$, then the π^i-modular lattice* $\begin{pmatrix} 0 & \pi^i \\ \bar{\pi}^i & a \end{pmatrix}$ *is isomorphic to $H(i)$.*

Proof. This is Proposition 9.1 of [6].

Proposition 2.12. *Let L be a π^i-modular plane, where $i = 0$ or 1, with $nL = nH(i)$.*

(1) *If L is isotropic, then $L \simeq H(i)$.*
(2) *Either in R-P with $i = 1$ or in R-U with $i = 0$, the lattice L must be isotropic; particularly one has $L \simeq H(i)$. In the other two cases, if L is anisotropic, then $(h(x, x)) = nL$ for any maximal vector $x \in L$.*
(3) *If K is another π^i-modular plane, with $nK = nL$ and $dK \simeq dL$, then one has $K \simeq L$.*

Proof. This is Proposition 9.2 of [6].

Propositions 2.11 and 2.12 handle the case where L is a π^i-modular plane with $nL = nH(i)$, the minimal case. The other case $nL \neq nH(i)$ is treated in the following proposition.

Proposition 2.13. *Let L be a π^i-modular plane, where $i = 0$ or 1, with $nL = (\pi^{2m}) \supsetneq nH(i)$.*

(1) *If L is normal, then* $L \simeq (1) \oplus (dL) \simeq \begin{pmatrix} 1 & 1 \\ 1 & \{1\} \end{pmatrix}$.

(2) *If L is subnormal, then*

$$L \simeq \begin{pmatrix} \pi_F^m & \pi^i \\ \bar{\pi}^i & \{a\} \end{pmatrix},$$

where $a = 4\pi_F^{-m+i}$ in R-P, and $a = 4\pi_F^{-2k-m+i-1}$ in R-U.

PROOF. This is Proposition 10.2 of [6].

Using Propositions 2.9–2.13, one can obtain the following characterization for modular lattices (see [6, Proposition 10.4]).

Theorem 2.14. *Let L and K be two π^i-modular lattices for some $i \in \mathbb{Z}$. Then $L \simeq K$ if and only if* $\operatorname{rank} L = \operatorname{rank} K$, $nL = nK$, *and $dL \simeq dK$.*

2.4. **The ramified dyadic case: the invariants.** Let L and K be two Hermitian lattices, and let $I \subset O_E$ be a proper ideal. We write $dL/dK \simeq 1 \pmod{I}$ if $v(dL) = v(dK)$ and there are O_E-bases x_i and y_i for L and K, respectively, such that

$$\det(h_L(x_i, x_j))/\det(h_K(y_i, y_j)) \equiv 1 \pmod{I}.$$

The following theorem [6, Theorem 11.4] gives a complete classification of Hermitian forms over local maximal orders by the invariants.

Theorem 2.15. *Let L and K be two Hermitian lattices. Suppose*

$$L = \oplus_{1 \le \lambda \le t} L_\lambda \quad \text{and} \quad K = \oplus_{1 \le \lambda \le T} K_\lambda$$

are any Jordan splittings of L and K, respectively. Then L and K are isometric if and only if the following four necessary conditions hold:

(1) *L and K are of the same type.*
(2) *$dL \simeq dK$.*
(3) *$u_L(\lambda) = u_K(\lambda)$ for all $\lambda = 1, \dots, t$.*
(4) *For all $j = 1, \dots, t-1$, one has*

$$d(L_1 \oplus \cdots \oplus L_j)/d(K_1 \oplus \cdots \oplus K_j) \simeq 1 \pmod{\mathfrak{f}(j)}.$$

3. Unpolarized cases

In this section we assume that $p \equiv 3 \pmod 4$. Recall that $R = \mathbb{Z}_2[X]/(X^2 + p) = \mathbb{Z}_2[\pi]$ and $E = R \otimes_{\mathbb{Z}_2} \mathbb{Q}_2 = \mathbb{Q}_2[\pi]$. Let O_E be the ring of integers of E; O_E is either a complete discrete valuation ring or is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Put $\alpha := (\pi - 1)/2$. Then $\alpha \in O_E$ and

$$O_E = \mathbb{Z}_2[\alpha] = \mathbb{Z}_2[X]/(X^2 + X + (p+1)/4).$$

Put $\omega := \pi - 1$, and one has

$$R = \mathbb{Z}_2[\omega] = \mathbb{Z}_2[X]/(X^2 + 2X + (p+1)) \quad \text{and} \quad 2\alpha = \omega.$$

We shall classify R-modules M which are free $\mathbb{Z}_2$-modules of finite rank. Write $< x_1, \ldots, x_m >_R$ for the R-submodule of M generated by elements $x_1, \ldots, x_m$.

We divide the classification into two cases:

Case (a): $p \equiv 3 \pmod 8$. In this case, the algebra E is an unramified quadratic extension of $\mathbb{Q}_2$. We have (at least) two indecomposable $\mathbb{Z}_2$-free finite R-modules: R and O_E as R-modules. The R-module structure of O_E is given as follows: write $O_E =< 1, \alpha >_{\mathbb{Z}_2}$, then

$$\omega 1 = 2\alpha \quad \text{and} \quad \omega\alpha = -2\alpha - (p+1)/2. \tag{3.1}$$

If M is an R-module of the form $R^{\oplus r} \oplus O_E^{\oplus s}$ for some non-negative integers r and s, then the integers r and s are uniquely determined by M. Indeed, we have $r + s = \dim_E M \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$, and $M/(2,\omega)M = (\mathbb{F}_2)^r \oplus (\mathbb{F}_2 \oplus \mathbb{F}_2)^s$.

Case (b): $p \equiv 7 \pmod 8$. In this case, the algebra E is isomorphic to $\mathbb{Q}_2 \times \mathbb{Q}_2$. Let α_1 and α_2 are the roots of the quadratic polynomial $X^2 + X + (p+1)/4$ in $\mathbb{Z}_2$. By switching the order, we may assume that α_1 is a unit and $\alpha_2 \in 2\mathbb{Z}_2$. By the Chinese Remainder Theorem, we have the isomorphisms

$$O_E = \mathbb{Z}_2[\alpha] \simeq O_E/(\alpha - \alpha_1) \times O_E/(\alpha - \alpha_2) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Clearly, $X^2 + 2X + (p+1) = (X - 2\alpha_1)(X - 2\alpha_2)$ and $(\omega - 2\alpha_1)(\omega - 2\alpha_2) = 0$ in R. There are (at least) three indecomposable $\mathbb{Z}_2$-free finite R-modules:

$$R, \quad R/(\omega - 2\alpha_1), \quad \text{and} \quad R/(\omega - 2\alpha_2).$$

Among them, one has

$$O_E \simeq R/(\omega - 2\alpha_1) \oplus R/(\omega - 2\alpha_2)$$

as R-modules. If M is an R-module of the form $R^r \oplus [R/(\omega - 2\alpha_1)]^s \oplus [R/(\omega - 2\alpha_2)]^t$ for some non-negative integers r, s and t, then the integers r, s and t are uniquely determined by M. Indeed, we have

$$\operatorname{rank}_{\mathbb{Z}_2} M = 2r + s + t, \quad M/(2,\omega)M = \mathbb{F}_2^r \oplus \mathbb{F}_2^s \oplus \mathbb{F}_2^t,$$

and

$$M/(\omega - 2\alpha_1)M = [R/(\omega - 2\alpha_1)]^{r+s} \oplus (\mathbb{F}_2)^t.$$

Conversely, we shall show that the indecomposable finite R-modules described in Cases (a) and (b) exhaust all possibilities.

Theorem 3.1. *Let M be a $\mathbb{Z}_2$-free finite R-module. Then*

(1) *Assume $p \equiv 3 \pmod 8$ (Case (a)). The R-module M is isomorphic to $R^r \oplus O_E^s$ for some non-negative integers r and s. Moreover, the integers r and s are uniquely determined by M.*

(2) *Assume $p \equiv 7 \pmod 8$ (Case (b)). The R-module M is isomorphic to*

$$R^r \oplus [R/(\omega - 2\alpha_1)]^s \oplus [R/(\omega - 2\alpha_2)]^t$$

for some non-negative integers r, s and t. Moreover, the integers r, s and t are uniquely determined by M.

Proof. We have seen that the integers r, s (and t for (2)) are uniquely determined by the R-module M. We now prove the first part of each statement.

(1) Assume $p \equiv 3 \pmod 8$. In this case we have $M \otimes_{\mathbb{Z}_2} \mathbb{Q}_2 = M \otimes_R E \simeq E^n \simeq \mathbb{Q}_2^{2n}$, and hence $M \simeq \mathbb{Z}_2^{2n}$ and $\overline{M} := M/2M \simeq \mathbb{F}_2^{2n}$. Let

$$\overline{M} := M/2M = (\mathbb{F}_2[\omega]/\omega^2)^r \oplus (\mathbb{F}_2)^{2s} \tag{3.2}$$

be the decomposition as $R/2R = \mathbb{F}_2[\omega]/(\omega^2)$-modules. We first show that if $s = 0$, then $M \simeq R^r$. Since $r = \dim M \otimes_R \mathbb{F}_2 = \dim_E M \otimes_R E$ and R is a local Noetherian domain, the module M is free.

Now suppose $s > 0$. Choose an element $a \neq 0 \in (\mathbb{F}_2)^{2s}$ and let $x \in M$ be an element such that $\bar{x} = a$. As $\overline{\omega x} = 0$, the element $\omega x/2 \in M$. Put $M_1 :=< x, \omega x/2 >_{\mathbb{Z}_2}$; it is an R-module and is isomorphic to O_E. Let ω' denote the conjugate of ω; one has $\omega' = -2 - \omega$ and $\omega\omega' = (1 + p)$. Note that $(1 + p)/4$ is a unit. Since $\bar{x} \notin \omega'\overline{M}$, one has $x \notin \omega' M$. We show that $\overline{\omega x/2} \neq 0$. Suppose not, then $\omega x = 4y$ for some $y \in M$. Applying ω', we get $x = \omega' y'$ for some $y' \in M$, contradiction. We show that the $\mathbb{F}_2$-vector space $\overline{M}_1 := M_1/2M =< \bar{x}, \overline{\omega x/2} >$ is 2-dimensional. Suppose that $x + \omega x/2 = 2z$ for some $z \in M$. Since $(1 + \omega/2) = -\omega'/2$, we get $x = -[4/(\omega\omega')] \cdot \omega z \in \omega M$ and $\bar{x} \in \omega\overline{M} = \omega'\overline{M}$, contradiction. Therefore, the quotient $\overline{M}/\overline{M}_1$ has dimension decreased by 2. On

the other hand, the $\mathbb{Z}_2$-rank of M/M_1 also decreases by 2. This shows that M/M_1 is free as $\mathbb{Z}_2$-modules. If the integer s in (3.2) for M/M_1 is positive, then we can find an R-submodule $M_2 =< x_2, \omega x_2/2 >_{\mathbb{Z}_2} \simeq O_E$ not contained in the vector space $E \otimes_{O_E} M_1$ such that $M/(M_1 + M_2)$ is free as $\mathbb{Z}_2$-modules. Continuing this process, we get R-submodules $M_1, \dots, M_{s'}$, which are isomorphic to O_E, such that $M_1 + \cdots + M_{s'} = M_1 \oplus \cdots \oplus M_{s'}$ and $M/(M_1 + \cdots + M_{s'})$ is a free R-module. It follows that $M \simeq O_E^{s'} \oplus R^{r'}$. Since s' and r' are uniquely determined by M as before, the integers s' and r' are actually equal to s and r in (3.2), respectively. This proves (1).

(2) Assume $p \equiv 7 \pmod 8$. Let

$$M_1 := \{x \in M \mid (\omega - 2\alpha_1)x = 0\},$$

and

$$M_2 := \{x \in M \mid (\omega - 2\alpha_2)x = 0\}.$$

Using the relation

$$2 = (\omega - 2\alpha_1)(2\alpha_2 + 1)^{-1} - (\omega - 2\alpha_2)(2\alpha_2 + 1)^{-1},$$

one shows that $2M \subset M_1 + M_2$, and hence the quotient $M/(M_1 + M_2)$ is an $\mathbb{F}_2$-vector space, say of dimension r. Let $x_1, \dots, x_r$ be elements of M such that the images $\bar{x}_1, \dots, \bar{x}_r$ form an $\mathbb{F}_2$-basis for $M/(M_1 + M_2)$. Put $F_0 :=< x_1, \dots, x_r >_R$, which is isomorphic to R^r, as $\bar{x}_i's$ form a basis for $F_0/(M_1 + M_2) = F_0/(2, \omega)F_0 \simeq \mathbb{F}_2^r$. Now $(\omega - 2\alpha_2)F_0 \subset M_1$, we choose elements $y_1, \dots, y_s$ in M_1 so that the images $\bar{y}_1, \dots, \bar{y}_s$ form an $R/(\omega - 2\alpha_1)$-basis for $M_1/(\omega - 2\alpha_2)F_0$, and put $F_1 =< y_1, \dots, y_s >_R$. We have

$$M_1 = (\omega - 2\alpha_2)F_0 \oplus F_1, \quad \text{and} \quad F_0 \cap F_1 = 0.$$

Similarly, we have a free $R/(\omega - 2\alpha_2)$-submodule F_2 of M_2, of rank t, such that

$$M_2 = (\omega - 2\alpha_1)F_0 \oplus F_2, \quad \text{and} \quad F_0 \cap F_2 = 0.$$

We have $(F_0 + F_1) \cap F_2 = F_0 \cap F_2 = 0$ and $M = F_0 + F_1 + F_2$, and hence $M = F_0 \oplus F_1 \oplus F_2$. This proves (2). ∎

Corollary 3.2. *Assume $p \equiv 3 \pmod 4$. Let A be an n-dimensional superspecial abelian variety A over $\mathbb{F}_p$ with $\pi_A^2 = -p$. Then the Tate module $T_2(A)$ of A is isomorphic to $R^r \oplus O_E^s$ for some non-negative integers r and s such that $r + s = n$. Moreover, the integers r and s are uniquely determined by $T_2(A)$.*

PROOF. Note that the Tate space $V_2(A) = T_2(A) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ is a free E-module of rank n; this follows from the fact that $\mathrm{tr}(a; V_2(A)) = n\,\mathrm{tr}(a; E)$ for all $a \in R$. It follows that the numbers s and t in Theorem 3.1 (2) above are the same. Therefore, the corollary follows. ∎

Lemma 3.3. *Assume $p \equiv 3 \pmod 4$. Let $n \geq 1$ be an integer. For any non-negative integers r and s with $r+s = n$, there exists an n-dimensional superspecial abelian variety A_r over $\mathbb{F}_p$ with $\pi_A^2 = -p$ such that the Tate module $T_2(A_r)$ of A_r is isomorphic to $R^r \oplus O_E^s$.*

PROOF. Choose a supersingular elliptic curve E_0 over $\mathbb{F}_p$ such that the endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(E_0)$ is equal to the ring $O_{\mathbb{Q}(\sqrt{-p})}$ of integers in the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$, and a supersingular elliptic curve E_1 over $\mathbb{F}_p$ such that the endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(E_0)$ is equal to $\mathbb{Z}[\sqrt{-p}]$ (see Waterhouse [17, Theorem 4.2 (3), p. 539]). Put $A_r = E_1^r \times E_0^s$, then the superspecial abelian variety A_r has the desired property. ∎

Remark 3.4. We recall that a (not necessarily commutative) ring Λ is said to be *left hereditary* if every left ideal of Λ is a projective Λ-module [11, Section 2f, p. 27]. One defines in a similar manner for the notion of *right hereditary*. If Λ is both left and right Noetherian, then Λ is left hereditary if and only if it is right hereditary [11, p. 29]. In this case Λ is simply called hereditary. Suppose that A is a Dedekind domain with quotient field K so that $A \neq K$ and B is a finite-dimensional semi-simple K-algebra. A hereditary A-order in B is an A-order Λ which is hereditary; note that Λ is both left and right Noetherian as it is finite as an A-module. Write $B = \prod_{i=1}^r B_i$ as the product of its simple factors and let A_i be the integral closure of A in the center K_i of B_i. Under the assumption that each A_i is a finite A-module, any hereditary A-order Λ in B has the form $\Lambda = \prod_{i=1}^r \Lambda_i$, where Λ_i is a hereditary A_i-order in B_i; cf. [11, Theorems 40.7, p. 369]. The finiteness assumption is used to make sure that any A_i-order in B_i is also an A-order. This assumption is fulfilled if A is Japanese or B is separable over K, that is, the center of B is a finite product of separable field extensions of K. We refer the reader to [8] for the definition of Japanese rings. Note that Theorem 40.7 of [11] is proved under the stronger assumption that B is separable over K; however, the proof only uses the finiteness assumption as stated.

As a special case, if B is separable and commutative over K, then the maximal A-order in B (it exists under the finiteness assumption) is the unique hereditary A-order in B.

From the discussion above, the non-maximal order $R = \mathbb{Z}_2[\pi]$ is not hereditary.

4. Proof of Theorem 1.1.

4.1. In this section we assume that $p \equiv 7 \pmod 8$. Thus, the algebra E is isomorphic to $\mathbb{Q}_2 \times \mathbb{Q}_2$. Write $\sigma_i : E \to \mathbb{Q}_2$ for the ith projection for $i = 1, 2$. Let (M, ψ) be a self-dual skew-Hermitian R-module of $\mathbb{Z}_2$-rank $2n$ and let $V := M \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. For $i = 1, 2$, let

$$V^i := \{x \in V;\, ax = \sigma_i(a)x,\ \forall a \in E\} \quad \text{and} \quad M^i := V^i \cap M \tag{4.1}$$

be the σ_i-components of V and M, respectively. It follows from the property $\psi(ax, y) = \psi(x, \bar{a}y)$ that each V^i is an isotropic subspace over $\mathbb{Q}_2$. Thus, $\dim V^i \leq n$ for $i = 1, 2$ and hence $\dim V^1 = \dim V^2$. This shows that V is a free E-module of rank n. Therefore, by Theorem 3.1, there are unique non-negative integers r and s with $r + s = n$ such that

$$M \simeq R^{\oplus r} \oplus O_E^{\oplus s} \tag{4.2}$$

as R-modules. Note that $r = 0$ if and only if $M = M^1 + M^2$, and we always have $M/(M^1 + M^2) \simeq (\mathbb{Z}/2\mathbb{Z})^r$.

Define a self-dual skew-Hermitian R-module (L_h, ψ_h) as follows. The R-module L_h is $O_E = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Put $e_1 = (1, 0)$ and $e_2 = (0, 1)$, and set $\psi_h(e_1, e_2) = 1$.

4.2. Suppose that there exist elements $x \in M^1$ and $y \in M^2$ such that $\psi(x, y) = 1$. Then the submodule $M_1 =< x, y >_R$ generated by x and y is isomorphic to L_h as skew-Hermitian R-modules and we have the decomposition

$$M = M_1 \oplus M_1^{\perp} \tag{4.3}$$

as skew-Hermitian R-modules, where $M_1^{\perp}$ is the orthogonal complement of M_1. Therefore, if $s = n$, then $M \simeq L_h^{\oplus n}$ as skew-Hermitian R-modules.

4.3. Recall that the polarization type of a non-degenerate alternating pairing ψ' on a free module M' over a PID R' of rank r is a tuple $(d_1, \ldots, d_r)$ of elements in R' with $d_1 | \ldots | d_r$ such that there exists a Lagrangian R'-basis x_i, y_i for $i = 1, \ldots, r$ such that $\psi'(x_i, y_i) = d_i$. The elements d_i are unique up to a unit in R'. The choice of the Lagrangian basis $\{x_i, y_i\}$ gives rise to a splitting of $M' = M'_1 \oplus M'_2$ into isotropic submodules $M'_1 :=< x_1, \ldots, x_r >_{R'}$ and $M'_2 :=< y_1, \ldots, y_r >_{R'}$. Conversely, if M' splits into the direct sum of two isotropic submodules M'_1 and M'_2. then a Lagrangian basis $\{x_i, y_i\}$ can be chosen so that $x_i \in M'_1$ and $y_i \in M'_2$ for all $i = 1, \ldots, r$.

Lemma 4.1.

(1) *The polarization type of the pairing ψ on the R-submodule $M^1 + M^2$ viewed as a $\mathbb{Z}_2$-module is $(1, \ldots, 1, 2, \ldots, 2)$, with multiplicity s and r for 1 and 2 respectively.*

(2) *There is a decomposition as skew-Hermitian R-modules*

$$M \simeq M_1 \oplus L_h^{\oplus s}, \tag{4.4}$$

where M_1 is a free R-submodule of rank r which is self-dual with respect to the pairing ψ.

Proof. The polarization type of the pairing ψ on the submodule $M^1 + M^2$ viewed as a $\mathbb{Z}_2$-module has the form $(2^{a_1}, \ldots, 2^{a_n})$ with integers $0 \leq a_1 \leq \cdots \leq a_n$. Since $|M/(M^1 + M^2)| = 2^r$, one has $\sum_{i=1}^n a_i = r$. If $a_1 > 0$, then $a_i = 1$ for all i and $r = n$. Below we show that $s = 0$ implies $a_1 > 0$. This proves the case where $s = 0$.

If $a_1 = 0$, then there exist elements $x \in M^1$ and $y \in M^2$ such that $\psi(x, y) = 1$. Using § 4.2, one has a decomposition of M into skew-Hermitian R-modules

$$M \simeq M' \oplus L_h \tag{4.5}$$

with $M' \simeq R^r \oplus O_E^{s-1}$ as an R-module, particularly $s > 0$.

Suppose $s > 0$ and we prove the statement by induction on s. Then $a_1 = 0$ and by the same argument we have $M \simeq M' \oplus L_h$ as above. By the induction hypothesis, the polarization type of ψ on $M^1 + M^2$ is $(1, \ldots, 1, 2, \ldots, 2)$ with multiplicity s for 1, and we get a decomposition of M into skew-Hermitian R-modules

$$M \simeq M_1 \oplus L_h^{\oplus s},$$

where M_1 is a free R-submodule of rank r which is self-dual with respect to the pairing ψ. This proves both (1) and (2). ∎

4.4. Now we classify self-dual skew-Hermitian R-modules (M, ψ) in the case where $M \simeq R^r$, where r is a positive integer. Let N be the smallest O_E-module in V containing M, and let $N' = M^1 + M^2$. We have

$$N = N^1 \oplus N^2, \quad N' = 2N.$$

The polarization type of ψ on $2N$ is $(2, \dots, 2)$. Put $\psi_N := 2\psi$. Then we have $\psi_N(N, N) \subset \mathbb{Z}_2$ and N is self-dual with respect to the pairing ψ_N. Put $\overline{N} = N/2N$ and let $\overline{\psi}_N : \overline{N} \times \overline{N} \to \mathbb{F}_2$ be the induced non-degenerate pairing. We have

$$2N \subset M \subset N, \quad \dim_{\mathbb{F}_2} \overline{M} = r \tag{4.6}$$

and that $\overline{M}$ is isotropic for $\overline{\psi}_N$, where $\overline{M} := M/2N$. Note that M generates N over O_E, or equivalently, $\overline{M}$ generates $\overline{N}$ over $O_E/2O_E = \mathbb{F}_2 \times \mathbb{F}_2$.

Suppose M_1 is another self-dual skew-Hermitian R-module such that $M_1 \simeq R^r$. Define N_1 and ψ_{N_1} similarly. Since (N_1, ψ_{N_1}) is isomorphic to (N, ψ_N) by Lemma 4.1 (2), we choose an isomorphism $\alpha : (N_1, \psi_{N_1}) \simeq (N, \psi_N)$ of skew-Hermitian R-modules. The image $M' = \alpha(M_1)$ is an R-module which satisfies the same property (4.6) as M does.

Now we fix the self-dual skew-Hermitian R-module (N, ψ_N). Let X_r the set of all R-submodules M of N such that

- $2N \subset M \subset N$ and $\dim_{\mathbb{F}_2} \overline{M} = r$, where $\overline{M} := M/2N$,
- $\overline{M}$ is isotropic with respect to the pairing $\overline{\psi}_N$, and
- M generates N over O_E.

We need to determine the isomorphism classes of elements M in X_r. Let $\overline{X}_r$ be the set of maximally isotropic $\mathbb{F}_2$-subspaces $\overline{M}$ of $\overline{N}$ such that $\overline{M}$ generates $\overline{N}$ over $\mathbb{F}_2 \times \mathbb{F}_2$. Since the R-module structure of $\overline{N}$ is simply an $\mathbb{F}_2$-module, the reduction map $M \mapsto \overline{M}$ gives rise to a bijection $X_r \simeq \overline{X}_r$.

If two elements M_1 and M_2 in X_r are isomorphic as skew-Hermitian R-modules, then any isomorphism between them lifts to an R-linear automorphism of (N, ψ_N). Therefore, the set of isomorphism classes of elements in X_r is in bijection with the orbit set $\mathrm{Aut}_R(N, \psi_N) \backslash X_r$. As the R-action on N extends uniquely to an

O_E-action on N, we have $\mathrm{Aut}_R(N,\psi_N) = \mathrm{Aut}_{O_E}(N,\psi_N)$. The action of the group $\mathrm{Aut}_{O_E}(N,\psi_N)$ on X_r factors through $\mathrm{Aut}_{\overline{O}_E}(\overline{N},\overline{\psi}_N)$, and the reduction map yields a bijection

$$\mathrm{Aut}_{O_E}(N,\psi_N)\backslash X_r \simeq \mathrm{Aut}_{\overline{O}_E}(\overline{N},\overline{\psi}_N)\backslash \overline{X}_r.$$

Proposition 4.2. *Let r be a positive integer. There are*

$$\#\ \mathrm{Aut}_{\overline{O}_E}(\overline{N},\overline{\psi}_N)\backslash \overline{X}_r.$$

non-isomorphic self-dual skew-Hermitian R-modules M such that $M \simeq R^r$ as R-modules.

We now describe the set $\mathrm{Aut}_{\overline{O}_E}(\overline{N},\overline{\psi}_N)\backslash \overline{X}_r$. Let $\overline{N} = \overline{N}^1 \oplus \overline{N}^2$ be the decomposition induced by $\overline{O}_E = \mathbb{F}_2 \times \mathbb{F}_2$, and let $p_i : \overline{N} \to \overline{N}^i$ be the ith projection for $i = 1, 2$. Fix a basis $e_1, \ldots, e_r$ for $\overline{N}^1$ and a basis $f_1, \ldots, f_r$ for $\overline{N}^2$ such that $\overline{\psi}_N(e_i, f_j) = \delta_{i,j}$ for all $i, j = 1, \ldots, r$. Using the basis $\{e_i, f_i\}_{i=1,\ldots,r}$ we identify the $\mathbb{F}_2$-vector space $\overline{N}$ with the $\mathbb{F}_2$-space $\mathbb{F}_2^{2r}$ of column vectors. Let $\overline{M}$ be an $\mathbb{F}_2$-vector space of $\overline{N}$ of dimension r. Choose a basis $v_1, \ldots, v_r$ for $\overline{M}$. The subspace $\overline{M}$ generates $\overline{N}$ over $\mathbb{F}_2 \times \mathbb{F}_2$ if and only if $p_i(\overline{M}) = \overline{N}^i$ for $i = 1, 2$. In this case, after a unique change of basis we may assume that $v_i = e_i + u_i$ for $i = 1, \ldots, r$ and $u_1, \ldots, u_r$ forms a basis for $\overline{N}^2$. Write $u_j = \sum_i u_{ij} f_i$ and let $U := (u_{ij}) \in \mathrm{GL}_r(\mathbb{F}_2)$. The matrix U is uniquely determined by $\overline{M}$. One computes

$$\overline{\psi}_N(e_i + u_i, e_j + u_j) = \overline{\psi}_N(e_i, u_j) - \overline{\psi}_N(e_j, u_i) = u_{ij} - u_{ji}.$$

It follows that $\overline{M}$ is isotropic for $\overline{\psi}_N$ if and only if the matrix U is symmetric. This shows $\overline{X}_r \simeq S_r$. Recall that S_r denotes in the set of all symmetric matrices in $\mathrm{GL}_r(\mathbb{F}_2)$ (Section 1). With respect to the basis $\{e_i, f_i\}$ the automorphism group $\mathrm{Aut}_{\overline{O}_E}(\overline{N},\overline{\psi}_N)$ of is

$$\left\{ \begin{pmatrix} A^{-1} & 0 \\ 0 & A^t \end{pmatrix} ;\ A \in \mathrm{GL}_r(\mathbb{F}_2) \right\} \simeq \mathrm{GL}_r(\mathbb{F}_2), \quad \begin{pmatrix} A^{-1} & 0 \\ 0 & A^t \end{pmatrix} \mapsto A^{-1}.$$

From the formula

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & A^t \end{pmatrix} \begin{pmatrix} I_r \\ U \end{pmatrix} = \begin{pmatrix} I_r \\ A^t U A \end{pmatrix} A^{-1}$$

the action of the group $\mathrm{GL}_r(\mathbb{F}_2) \simeq \mathrm{Aut}_{\overline{O}_E}(\overline{N}, \overline{\psi}_N)$ on S_r, transported from the action on $\overline{X}_r$, is given by

$$A \cdot U = A^{-t} U A^{-1}, \quad \forall\, A \in \mathrm{GL}_r(\mathbb{F}_2),\ U \in S_r.$$

We have shown the following proposition.

Proposition 4.3. *Notation as above. There is a bijection*

$$\mathrm{Aut}_{\overline{O}_E}(\overline{N}, \overline{\psi}_N) \backslash \overline{X}_r \simeq \mathrm{GL}_r(\mathbb{F}_2) \backslash S_r.$$

Note that $S_r/\sim$, the set of equivalence classes (see Section 1), is the orbit set $\mathrm{GL}_r(\mathbb{F}_2)\backslash S_r$.

Proposition 4.4 (Witt Cancellation)**.** *Let M_1 and M_2 be two self-dual skew-Hermitian R-modules. Suppose there is an isomorphism*

$$M_1 \oplus L_h^{\oplus s} \simeq M_2 \oplus L_h^{\oplus s}$$

of skew-Hermitian R-modules for some integer $s \geq 0$. Then M_1 is isometric to M_2.

Proof. By Lemma 4.1 (2), we have decompositions $M_1 = M_1' \oplus L_h^{\oplus s'}$ and $M_2 = M_2' \oplus L_h^{\oplus s''}$ as skew-Hermitian modules such that M_1' and M_2' are free as R-modules. Note that $s'' = s'$. Replacing M_1 and M_2 by M_1' and M_2', respectively, we may assume that $M_1 \simeq M_2 \simeq R^r$ as R-modules. Write ψ_i for the pairings on $M_i \oplus L_h^{\oplus s}$, for $i = 1, 2$. Let N_i be the smallest O_E-module in the vector space $E \otimes_R M_i$ containing M_i. Then $N_i \oplus L_h^{\oplus s}$ is the smallest O_E-module in the vector space $E \otimes_R (M_i \oplus L_h^{\oplus s})$ containing $M_i \oplus L_h^{\oplus s}$. Put $\psi_i' := 2\psi_i$, which is a $\mathbb{Z}_2$-valued skew-Hermitian form on $N_i \oplus L_h^{\oplus s}$. The pairing ψ_i' induces a non-degenerate pairing $\overline{\psi_i'}$ on the $\mathbb{F}_2$-vector space

$$(N_i \oplus L_h^{\oplus s})/(2N_i \oplus L_h^{\oplus s}) \simeq N_i/2N_i =: \overline{N}_i,$$

and the subspace

$$(M_i \oplus L_h^{\oplus s})/(2N_i \oplus L_h^{\oplus s}) \simeq M_i/2N_i =: \overline{M}_i$$

is a maximal isotropic subspace with respect to $\overline{\psi_i'}$.

Let $\alpha : M_1 \oplus L_h^{\oplus s} \simeq M_2 \oplus L_h^{\oplus s}$ be an isomorphism of skew-Hermitian R-modules. The map α lifts to an isomorphism $\beta : N_1 \oplus L_h^{\oplus s} \simeq N_2 \oplus L_h^{\oplus s}$, and β induces an isomorphism $\bar{\beta} : \overline{N}_1 \simeq \overline{N}_2$ of symplectic $\mathbb{F}_2$-spaces such that $\bar{\beta}(\overline{M}_1) = \overline{M}_2$.

We lift Lagrangian bases $\{x_i\}$ for $\overline{N}_1$) and $\{\bar{\beta}(x_i)\}$ for $\overline{N}_2$ to Lagrangian bases X_i for N_1 and Y_i for N_2, respectively. The map $\gamma : N_1 \simeq N_2$ which sends X_i to Y_i is an isomorphism of skew-Hermitian R-modules. Since $\gamma(2N_1) = 2N_2$ and $\gamma(\overline{M}_1) = \overline{M}_2$, it gives an isomorphism from M_1 to M_2. This proves the proposition. ∎

Remark 4.5. Proposition 4.4 (also Proposition 5.7) is not covered by a general Witt type cancellation theorem [1, Theorem 3] proved by Bayer-Fluckiger and Fainsilber, as the condition $a + \bar{a} = 1$ for some $a \in R$ is not fulfilled.

Corollary 4.6. *Let M be a self-dual skew-Hermitian R-module of $\mathbb{Z}_2$-rank $2n$. Then there are unique non-negative integers r and s with $r+s = n$ and a self-duel skew-Hermitian R-module M_1 which is free of rank r such that*

$$M \simeq M_1 \oplus L_h^{\oplus s}.$$

Moreover, M_1 is uniquely determined by M up to isomorphism.

Proof. This follows immediately from Lemma 4.1 (2) and Proposition 4.4. ∎

By Corollary 4.6 and Propositions 4.2 and 4.3, Theorem 1.1 is proved.

4.5. It is well-known that the set $S_r/\sim$ parametrizes equivalence classes of non-degenerate symmetric $\mathbb{F}_2$-spaces (W, φ) of dimension r. We use the notation (1) to indicate the one-dimensional non-degenerate symmetric space $\mathbb{F}_2$ with the pairing $\varphi(e_1, e_1) = 1$, and write

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

for the two-dimensional non-degenerate symmetric space $\mathbb{F}_2 \oplus \mathbb{F}_2$ with the pairing

$$\varphi(e_1, e_1) = \varphi(e_2, e_2) = 0, \quad \varphi(e_1, e_2) = 1.$$

Lemma 4.7. *Let (W, φ) be a symmetric space over $\mathbb{F}_2$ of dimension $r \geq 1$. If r is odd, then*

$$(W, \varphi) \simeq (1) \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

If r is even, then either

$$(W,\varphi) \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ or}$$

$$(W,\varphi) \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus (1) \oplus (1).$$

In particular, we have

$$\#S_r/\sim = \begin{cases} 1, & \text{if } r \text{ is odd,} \\ 2, & \text{if } r \text{ is even.} \end{cases}$$

Proof. Denote by $N(W)$ the set of vectors $x \in W$ such that $\varphi(x,x) = 0$. It is easy to show that $N(W)$ is a subspace. Let $N(W)_n$ be the null subspace of $N(W)$ and $W_2 \subset N(W)$ be a complement of $N(W)_n$. Then W_2 is a maximal non-degenerate subspace in $N(W)$ and it is easy to show

$$W_2 \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $W_1 := W_2^{\perp} \subset W$ be the orthogonal complement of W_2; one has $W = W_1 \oplus W_2$ and $N(W) = N(W_1) \oplus W_2$. It follows that $N(W)_n = N(W_1) = W(W_1)_n$ in W_1. We have $\dim W_1 \leq \dim N(W_1) + 1$, as if one has $y \neq x$ with $\varphi(x,x) = 1$ and $\varphi(y,y) = 1$ then $\varphi(x+y, x+y) = 0$. It follows that $\dim N(W_1) \leq 1$, otherwise W_1 would be degenerate. Therefore, $\dim W_1 \leq 2$. As there are no vectors $x, y \in W_1$ such that $\varphi(x,x) = \varphi(y,y) = 0$ and $\varphi(x,y) = 1$, the symmetric space (W_1, φ) is isomorphic to the direct sum of copies of (1). Therefore, the lemma follows. ∎

5. Proof of Theorem 1.2.

5.1. In this section we assume that $p \equiv 3 \pmod 8$. Thus, the algebra E is an unramified quadratic field extension of $\mathbb{Q}_2$. Recall that

$$R = \mathbb{Z}_2[\omega] = \mathbb{Z}_2[X]/(X^2 + 2X + p + 1) \subset O_E = \mathbb{Z}_2[\alpha]/(X^2 + X + (p+1)/4),$$

$\omega = \pi - 1$, $\alpha = \omega/2$ and $\pi \in R$ is an element with $\pi^2 = -p$. Let (M, ψ) be a skew-Hermitian R-module of $\mathbb{Z}_2$-rank $2n$, and let $V := M \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. There is a unique non-degenerate E-valued skew-Hermitian form

$$\langle\, ,\, \rangle : V \times V \to E \tag{5.1}$$

such that $\langle ax, by\rangle = a\bar{b}\langle x, y\rangle$ for all $a, b \in E$ and $x, y \in V$, and $\psi(x, y) = \mathrm{Tr}_{E/\mathbb{Q}_2}\langle x, y\rangle$ for all $x, y \in V$. Since $E/\mathbb{Q}_2$ is unramified, the inverse different $\mathcal{D}^{-1}_{E/\mathbb{Q}_2}$ is equal to O_E. Put $(\ ,\ ) := \pi\langle\ ,\ \rangle$, which is a Hermitian form on V. Note that $\langle M, M\rangle \subset O_E$ if and only if $(M, M) \subset O_E$, as the element $\pi = 1 + \omega$ lands in $1 + 2O_E = R^\times \subset O_E^\times$.

Lemma 5.1.

(1) *One has $(M, M) \subset 2^{-1}R$. Under the assumption that M is self-dual with respect to the pairing ψ, the condition $(M, M) \subset O_E$ holds if and only if M is invariant under the O_E-action.*
(2) *The R-lattice M is self-dual with respect to the pairing ψ if and only if M is self-dual with respect to the pairing $2(\ ,\ )$.*

Proof. (1) The element $\langle x, y\rangle$ for $x, y \in M$ satisfies the property $\mathrm{Tr}_{E/\mathbb{Q}_2}(\langle x, y\rangle R) \subset \mathbb{Z}_2$. Therefore, it lands in the dual lattice $R^\vee$ of R for the pairing $(a, b) \mapsto \mathrm{Tr}_{E/\mathbb{Q}_2}(ab)$. It is easy to check that $R^\vee = 2^{-1}R$, and hence the first part is proved.

Let $\widetilde{M}$ be the O_E-submodule in V generated by M. If M is invariant under the O_E-action, then $\langle M, M\rangle \subset O_E^\vee = O_E$. Conversely, if $\langle M, M\rangle \subset O_E$, then $\langle \widetilde{M}, \widetilde{M}\rangle \subset O_E$. This yields $\psi(\widetilde{M}, \widetilde{M}) \subset \mathbb{Z}_2$. As M is self-dual, one has $\widetilde{M} = M$. This proves (1).

(2) For any element $x \in V$, one has

$$(x, M) \in 2^{-1}R \iff \psi(x, M) \in \mathbb{Z}_2.$$

Therefore, the assertion follows. ∎

From now on, we assume that M is self-dual with respect to the pairing ψ.

Lemma 5.2. *One has $N_{E/\mathbb{Q}_2}(R^\times) = \mathbb{Z}_2^\times$.*

Proof. We use the following basic fact in number theory; see [10, Corollary, p. 7]. Suppose E/F is a unramified finite extension of non-Archimedean local fields. For any integer $i \geq 1$, let $U_E^{(i)} := 1 + \pi_E^i O_E \subset O_E^\times$ and $U_F^{(i)} := 1 + \pi_F^i O_F \subset O_F^\times$ be the ith principal congruence subgroups of $O_E^\times$ and $O_F^\times$, respectively. Then we have $N_{E/F}(U_E^{(i)}) = U_F^{(i)}$.

Since $R^\times = 1 + 2O_E$ and $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$, the lemma follows. ∎

5.2. We define three self-dual skew-Hermitian R-modules L_0, L_1, H as follows.

(i) The R-module L_0 is O_E and the pairing ψ_0 is defined by $\psi_0(1, \omega/2) = 1$. Write ω' for the conjugate of ω. To see this defines a skew-Hermitian R-module, one checks that

$$\psi_0(\omega'/2, 1) = \psi_0((-2-\omega)/2, 1) = \psi_0(-\omega/2, 1) = \psi_0(1, \omega/2). \tag{5.2}$$

(ii) The R-module L_1 is R and the pairing ψ_1 is defined by $\psi_1(1, \omega) = 1$. Similarly, one checks that $\psi_1(1, \omega) = \psi_1(\omega', 1)$ as (5.2).

(iii) The R-module H is $R \oplus R$ with standard basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$. The pairing ψ_H is defined by

$$\begin{aligned} \psi_H(e_1, \omega e_1) = \psi_H(e_1, e_2) = \psi_H(e_2, \omega e_2) = \psi_H(\omega e_1, \omega e_2) = 0, \\ \psi_H(e_1, \omega e_2) = \psi_H(e_2, \omega e_1) = 1. \end{aligned} \tag{5.3}$$

Note that using the relation $\psi_H(\omega x, y) = \psi_H(x, \omega' y)$ the pairing ψ_H is uniquely determined by any values of

$$\psi_H(e_1,\ \omega e_1),\ \psi_H(e_1, e_2),\ \psi_H(e_1, \omega e_2),\ \text{and}\ \psi_H(e_2, \omega e_2).$$

One checks that

$$\psi_H(\omega' e_1, e_2) = \psi_H((-2-\omega)e_1, e_2) = \psi_H(e_2, \omega e_1) = 1 = \psi_H(e_1, \omega e_2).$$

So (5.3) defines a skew-Hermitian R-module.

By Theorem 3.1, there are unique non-negative integers r and s with $r + s = n$ such that

$$M \simeq R^r \oplus O_E^s$$

as R-modules. If one has a decomposition

$$M \simeq L_1^{\oplus r_1} \oplus H^{\oplus r_2} \oplus L_0^{\oplus s'}$$

as skew-Hermitian R-modules for some non-negative integers r_1,r_2 and s', then $r_1 + 2r_2 = r$ and $s' = s$.

5.3. Let $M_0 \subset M$ be the R-submodule defined by

$$M_0 := \{x \in M \,|\, \omega x \in 2M\}. \tag{5.4}$$

Write $\overline{M} := M/2M$ and $\overline{M}_0 := M_0/2M$. Let

$$\overline{\psi} : \overline{M} \times \overline{M} \to \mathbb{F}_2$$

be the induced non-degenerate alternating pairing. We have a filtration

$$\omega\overline{M} \subset \overline{M}_0 \subset \overline{M},$$

and have the following properties

- $\dim_{\mathbb{F}_2} \omega\overline{M} = \dim_{\mathbb{F}_2} \overline{M}/\overline{M}_0 = r$ and $\dim_{\mathbb{F}_2} \overline{M}_0 = 2s + r$, and
- $\omega\overline{M}$ is an isotropic subspace with respect to the pairing $\overline{\psi}$.

For any element x in M, write $\overline{x}$ for the image of x in $\overline{M}$.

Lemma 5.3. *Let M be a self-dual skew-Hermitian R-module.*

(1) *If there exists an element $x \in M$ such that $\overline{\psi}(\overline{x}, \omega\overline{x}) \neq 0$, then the R-submodule M_1 generated by x, with the pairing $\psi|_{M_1}$ restricted on M_1, is isomorphic to (L_1, ψ_1) as skew-Hermitian R-modules. Moreover, we have the decomposition*

$$M = M_1 \oplus M_1^{\perp}$$

as skew-Hermitian R-modules.

(2) *If there exists an element $x \in M_0 \subset M$ such that $\overline{\psi}(\overline{x}, \overline{\omega/2x}) \neq 0$, then the R-submodule M_1 generated by x and $\omega/2x$, with the pairing $\psi|_{M_1}$ restricted on M_1, is isomorphic to (L_0, ψ_0) as skew-Hermitian R-modules. Moreover, we have the decomposition*

$$M = M_1 \oplus M_1^{\perp}$$

as skew-Hermitian R-modules.

Proof. (1) We have $\psi(x, \omega x) = a \in \mathbb{Z}_2^{\times}$. By Lemma 5.2, there is an element $\lambda \in R^{\times}$ such that $N(\lambda) = a^{-1}$. Replacing x by λx, we get $\psi(x, \omega x) = 1$. Since M_1 is self-dual and R-invariant, the orthogonal complement $M_1^{\perp}$ is R-invariant and we have $M = M_1 \oplus M_1^{\perp}$. This proves (1).

(2) Using the same argument as (1), we can choose an element $x \in M_1$ such that $\psi(x, \omega/2x) = 1$ and we have the decomposition $M = M_1 \oplus M_1^{\perp}$. It is clear that we have an isometry $(M_1, \psi|_{M_1}) \simeq (L_0, \psi_0)$. This proves (2). ∎

Lemma 5.4. *There is a decomposition as skew-Hermitian R-modules*

$$M \simeq M_1 \oplus L_0^{\oplus s} \tag{5.5}$$

where M_1 is a free R-submodule of rank r which is self-dual with respect to the pairing ψ.

PROOF. Let $M_0 \subset M$ be the submodule defined as (5.4). It is clear that $\overline{\psi}(\omega\overline{M}, \overline{M}_0) = 0$. It follows from the non-degeneracy of $\overline{\psi}$ that there are vectors $x_1, \dots, x_r \in \omega\overline{M}$ and $y_1, \dots, y_r \in \overline{M}$ such that

$$\overline{\psi}(x_i, x_j) = \overline{\psi}(y_i, y_j) = 0, \quad \text{and} \quad \overline{\psi}(x_i, y_j) = \delta_{i,j}$$

for all $i, j = 1, \dots, r$. Put $W_1 :=< y_1, \dots, y_r >_{\mathbb{F}_2}$ and $W_2 := (\omega\overline{M} \oplus W_1)^{\perp}$. We have $\overline{M} = \omega\overline{M} \oplus W_1 \oplus W_2$. It follows from

$$\overline{\psi}(\omega W_2, \overline{M}) = \overline{\psi}(W_2, (-2-\omega)\overline{M}) = 0$$

that $\omega W_2 = 0$, and hence $W_2 \subset \overline{M}_0$. It follows from the dimension counting that $\overline{M}_0 = \omega\overline{M} \oplus W_2$. This shows that the pairing $\overline{\psi}$ is non-degenerate on $\overline{M}_0/\omega\overline{M}$. We can choose elements $z_1, \dots, z_s$ in M_0 such that the O_E-submodule $M_2 =< z_1, \dots, z_s >_{O_E} \subset M_0$ is mapped onto W_2. The module M_2 is self-dual with respect to ψ. By Lemma 5.1, M_2 is a unimodular Hermitian module over O_E for the pairing $(\ ,\ )$, and hence M_2 is a direct sum of O_E-rank one Hermitian submodule, as $E/\mathbb{Q}_2$ is unramified. Therefore, $M_2 \simeq L_0^{\oplus s}$ as skew-Hermitian R-modules. Put $M_1 := M_2^{\perp}$. We have $M = M_1 \oplus M_2$ as skew-Hermitian modules, and M_1 is a free R-submodule of rank r which is self-dual with respect to the pairing ψ. ∎

5.4. Now we classify self-dual skew-Hermitian R-modules (M, ψ) in the case where $M \simeq R^r$, where r is a positive integer. Let N be the smallest O_E-module in V containing M, and let N' be the largest O_E-submodule in M. We have $N' = 2N \supset 2M$. Since $N'/2M$ is a maximal isotropic $\mathbb{F}_2$-subspace of dimension r with respect to $\overline{\psi}$, the polarization type of ψ on N' is $(2, \dots, 2)$. Put $\psi_N := 2\psi$. We have $\psi_N(N, N) \subset \mathbb{Z}_2$, and N is self-dual with respect to the pairing ψ_N. Note that $(N, \psi_N) \simeq (L_0, \psi_0)^{\oplus r}$ by Lemma 5.4. Put $\overline{N} = N/2N$ and let $\overline{\psi}_N : \overline{N} \times \overline{N} \to \mathbb{F}_2$ be the induced non-degenerate pairing. We have

$$2N \subset M \subset N, \quad \dim_{\mathbb{F}_2} \overline{M} = r \tag{5.6}$$

and $\overline{M}$ is isotropic for $\overline{\psi}_N$, where $\overline{M} := M/2N$. Note that M generates N over O_E, or equivalently, the subspace $\overline{M}$ generates $\overline{N}$ over $\overline{O}_E := O_E/2O_E = \mathbb{F}_4$.

Suppose M_1 is another self-dual skew-Hermitian R-module such that $M_1 \simeq R^r$. Define N_1 and ψ_{N_1} similarly. As $(N_1, \psi_{N_1}) \simeq (N, \psi_N)$, we choose an isomorphism $\alpha : (N_1, \psi_{N_1}) \simeq (N, \psi_N)$ of skew-Hermitian R-modules. The image $M' = \alpha(M_1)$ is an R-module which satisfies the same property as M does (5.6).

Now we fix the self-dual skew-Hermitian R-module (N, ψ_N). Similarly to § 4.4, let X_r be the set of all R-submodules M of N such that

- $2N \subset M \subset N$ and $\dim_{\mathbb{F}_2} \overline{M} = r$,
- $\overline{M}$ is isotropic with respect to the pairing $\overline{\psi}_N$, and
- M generates N over O_E.

We need to determine the isomorphism classes of elements M in X_r. Let $\overline{X}_r$ be the set of maximally isotropic $\mathbb{F}_2$-subspaces $\overline{M}$ of $\overline{N}$ such that $\overline{M}$ generates $\overline{N}$ over $\mathbb{F}_4$. Since the R-module structure of $\overline{N}$ is simply an $\mathbb{F}_2$-module, the reduction map $M \mapsto \overline{M}$ gives rise to a bijection $X_r \simeq \overline{X}_r$.

Using the same argument as in § 4.4, the set of isomorphism classes of elements in X_r is in bijection with the orbit set $\mathrm{Aut}_{O_E}(N, \psi_N)\backslash X_r$, and the reduction map induces the bijection

$$\mathrm{Aut}_{O_E}(N, \psi_N)\backslash X_r \simeq \mathrm{Aut}_{\mathbb{F}_4}(\overline{N}, \overline{\psi}_N)\backslash \overline{X}_r \tag{5.7}$$

Proposition 5.5. *Let r be a positive integer. There are*

$$\#\,\mathrm{Aut}_{\mathbb{F}_4}(\overline{N}, \overline{\psi}_N)\backslash \overline{X}_r$$

non-isomorphic self-dual skew-Hermitian R-modules M such that $M \simeq R^r$ as R-modules.

We now describe the orbit set $\mathrm{Aut}_{\overline{O}_E}(\overline{N}, \overline{\psi}_N)\backslash \overline{X}_r$. Let $V_0 = \mathbb{F}_4^r$, viewed as the space of column vectors, together with the standard non-degenerate Hermitian form $(\ ,\ )_0$ defined by

$$((x_i), (y_i))_0 = \sum_{i=1}^{r} x_i \bar{y}_i,$$

where $y \mapsto \bar{y}$ is the non-trivial automorphism on $\mathbb{F}_4$. Choose an element $\epsilon \in \mathbb{F}_4^\times$ such that $\epsilon + \bar{\epsilon} = 0$ (in fact $\epsilon = 1$) and put $\langle x, y\rangle_0 := \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}\, \epsilon(x, y)_0$, for $x, y \in V_0$. Then we have an isomorphism $(V_0, \langle\ ,\ \rangle_0) \simeq (\overline{N}, \overline{\psi}_N)$ as skew-Hermitian modules over $\mathbb{F}_4$ and we may identify $(\overline{N}, \overline{\psi}_N)$ with $(V_0, \langle\ ,\ \rangle_0)$. Let $U(r)$ be the unitary group over $\mathbb{F}_2$ associated to the Hermitian space $(V_0, (\ ,\ )_0)$; one has

$$U(r)(\mathbb{F}_2) = \mathrm{Aut}_{\mathbb{F}_4}(V_0, (\ ,\ )_0) = \mathrm{Aut}_{\mathbb{F}_4}(V_0, \langle\ ,\ \rangle_0)$$

Write any matrix U in $\mathrm{GL}_r(\mathbb{F}_4)$ as $(u_1, \ldots, u_r)$, where $u_i \in V_0$. The map

$$U = (u_1, \ldots, u_r) \mapsto W =< u_1, \ldots, u_r >_{\mathbb{F}_2}$$

induces a bijection between $\mathrm{GL}_r(\mathbb{F}_4)/\mathrm{GL}_r(\mathbb{F}_2)$ and the set Z_r of r-dimensional $\mathbb{F}_2$-subspace $W \subset V_0$ which spans V_0 over $\mathbb{F}_4$. Note that $\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(x,y)_0 = 0$ if and only if $(x,y)_0 \in \mathbb{F}_2$. It follows that a subspace $W \in Z_r$ is isotropic with respect to $\langle\,,\,\rangle_0$ if and only if $\bar{U}^t U \in \mathrm{GL}_r(\mathbb{F}_2)$ for any matrix U mapping to W. Let $Y_r \subset \mathrm{GL}_r(\mathbb{F}_4)$ be the subset consisting of matrices U such that $\bar{U}^t U \in \mathrm{GL}_r(\mathbb{F}_2)$. The action of the group $U(r)(\mathbb{F}_2)$ on the set $\mathrm{GL}_r(\mathbb{F}_4)/\mathrm{GL}_r(\mathbb{F}_2)$, transported from the action of the group $\mathrm{Aut}_{\overline{O}_E}(\overline{N},\overline{\psi}_N) = \mathrm{Aut}_{\mathbb{F}_4}(V_0,\langle\,,\,\rangle_0)$ on the set $\overline{X}_r$, is simply the left translation. Thus, there is a bijection

$$\mathrm{Aut}_{\overline{O}_E}(\overline{N},\overline{\psi}_N)\backslash\overline{X}_r \simeq U(r)(\mathbb{F}_2)\backslash Y_r/\mathrm{GL}_r(\mathbb{F}_2). \tag{5.8}$$

Lemma 5.6. *The map $\pi : Y_r \to \mathrm{GL}_r(\mathbb{F}_2)$ defined by $U \mapsto \bar{U}^t U$ induces the bijection*

$$U(r)(\mathbb{F}_2)\backslash Y_r/\mathrm{GL}_r(\mathbb{F}_2) \simeq S_r/\sim .$$

Proof. Since the matrix $\bar{U}^t U$ is Hermitian, one has $\pi(Y_r) \subset S_r$. Each non-empty fiber of π is a principal homogeneous space of $U(r)(\mathbb{F}_2)$. Thus, the induced map $\pi : U(r)(\mathbb{F}_2)\backslash Y_r \to S_r$ is injective. One easily checks $\pi(UP) = P^t\pi(U)P$ for $P \in \mathrm{GL}_r(\mathbb{F}_2)$. Thus, we have the injection map

$$U(r)(\mathbb{F}_2)\backslash Y_r/\mathrm{GL}_r(\mathbb{F}_2) \to S_r/\sim .$$

It suffices to show that the map $\pi : Y_r \to S_r/\sim$ is surjective. By Lemma 4.7, any matrix A in S_r is equivalent to a matrix with diagonal boxes either (1) or $\widetilde{I}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus it suffices to find a matrix $U \in \mathrm{GL}_2(\mathbb{F}_4)$ such that $\bar{U}^t U = \widetilde{I}_2$. Note that $\mathbb{F}_4 = \mathbb{F}_2[\beta]$ with $\beta^2 + \beta + 1 = 0$. Take

$$U = \begin{pmatrix} \beta & \beta+1 \\ 1 & \beta+1 \end{pmatrix}$$

and get $\bar{U}^t U = \widetilde{I}_2$. This proves the lemma. ∎

Proposition 5.7 (Witt Cancellation)**.** *Let M_1 and M_2 be two self-dual skew-Hermitian R-modules. Suppose there is an isomorphism*

$$M_1 \oplus L_0^{\oplus s} \simeq M_2 \oplus L_0^{\oplus s}$$

of skew-Hermitian R-modules for some integer $s \geq 0$. Then M_1 is isometric to M_2.

PROOF. The proof is the same as that of Proposition 4.4. Note that one can lift the isomorphism $\overline{\beta} : (\overline{N}_1, \overline{\psi}_1) \simeq (\overline{N}_2, \overline{\psi}_2)$ to an isomorphism $\gamma : (N_1, \psi_1) \simeq (N_2, \psi_2)$. This is because $\mathrm{Isom}_R((N_1, \psi_1), (N_2, \psi_2))$ is the set of $\mathbb{Z}_2$-points of a smooth scheme over $\mathbb{Z}_2$ (in fact a trivial torsor of a smooth group scheme over $\mathbb{Z}_2$). ∎

Corollary 5.8. *Let M be a self-dual skew-Hermitian R-module of $\mathbb{Z}_2$-rank $2n$. Then there are unique non-integers r and s with $r + s = n$ and a self-duel skew-Hermitian R-module M_1 which is free of rank r such that*

$$M \simeq M_1 \oplus L_0^{\oplus s}.$$

Moreover, M_1 is uniquely determined, up to isomorphism, by M.

PROOF. This follows immediately from Lemma 5.4 and Proposition 5.7. ∎

Theorem 1.2 follows from Corollary 5.8, Proposition 5.5, (5.8), and Lemma 5.6.

REFERENCES

[1] E. Bayer-Fluckiger and L. Fainsilber, Non-unimodular Hermitian forms. *Invent. Math.* **123** (1996), no. 2, 233–240.

[2] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I. With applications to finite groups and orders.* Pure and Applied Mathematics. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1981, 819 pp.

[3] L. Fainsilber and J. Morales, An injectivity result for Hermitian forms over local orders. *Illinois J. Math.* **43** (1999), no. 2, 391–402.

[4] T. Ibukiyama and T. Katsura, On the field of definition of superspecial polarized abelian varieties and type numbers. *Compositio Math.* **91** (1994), 37–46.

[5] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers. *Compositio Math.* **57** (1986), 127–152.

[6] R. Jacobowitz, Hermitian forms over local fields. *Amer. J. Math.* **84** (1962), 441–465.

[7] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, The book of involutions. American Mathematical Society, Colloquium Publications, 44. *Amer. Math. Soc.*, 1998, 593 pp.

[8] H. Matsumura, *Commutative algebra.* Second edition. Mathematics Lecture Note Series, 56. Benjamin/Cummings Publishing, 1980, 313 pp.

[9] D. Mumford, *Abelian Varieties.* Oxford University Press, 1974.

[10] V. Platonov and A. Rapinchuk, Algebraic groups and number theory. *Pure and Applied Mathematics, 139.* Academic Press, Inc., Boston, MA, 1994.

[11] I. Reiner, *Maximal orders.* London Mathematical Society Monographs, No. **5**. Academic Press, London-New York, 1975, 395 pp.

[12] C. Riehm, Hermitian forms over local hereditary orders. *Amer. J. Math.* **106** (1984), no. 4, 781–800.

[13] W. Scharlau, *Quadratic and Hermitian forms*. Grundlehren der Mathematischen Wissenschaften **270**. Springer-Verlag, Berlin, 1985.

[14] G. Shimura, Arithmetic of Hermitian forms. *Doc. Math.* **13** (2008), 739–774.

[15] J. Tate, Classes d'isogenie de variétés abéliennes sur un corps fini (d'après T. Honda). *Sém. Bourbaki Exp.* 352 (1968/69). Lecture Notes in Math., vol. 179, Springer-Verlag, 1971.

[16] J. Tate, Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2** (1966), 134–144.

[17] W. C. Waterhouse, Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560.

[18] C.-F. Yu, Superspecial abelian varieties over finite prime fields. *J. Pure Appl. Algebra* **216** (2012), 1418–1427.

Chia-Fu Yu
Institute of Mathematics, Academia Sinica and NCTS (Taipei Office)
6th Floor, Astronomy Mathematics Building
No. 1, Roosevelt Rd. Sec. 4
Taipei, Taiwan, 10617
E-mail: chiafu@math.sinica.edu.tw