Lattices and Orders in Quaternion Algebras with Involution

Håkan Granath

July 18, 2005

Abstract

We study maximal orders Λ in quaternion algebras having an involution over a quadratic field extension K/F. We construct a quadratic quaternary lattice in the algebra which parametrises the optimally embedded orders in F-subalgebras. We show that the Clifford algebra of the dual of this lattice can naturally be embedded in the order. We also develop a theory relating quaternion orders to hermitian planes. Using these techniques, we classify up to genus the optimally embedded suborders of Λ. Finally, we show that the units of norm 1 in Λ maps surjectively to the spinorial kernel of the orthogonal group of the lattice.

Key words: quaternion order, Clifford algebra, hermitian form, orthogonal groups
2000 Mathematics Subject Classification: 11R52, 16H05, 11E88, 11E39

In this paper we study maximal orders Λ in quaternion algebras A with a so called type 2 involution over a quadratic field extension K/F, and particular the optimally embedded orders in F-subalgebras of such algebras A. Our main results concern the construction of a certain quaternary quadratic lattice (L, q). This lattice parametrises the optimally embedded suborders in the given order. The correspondence between lattice elements and suborders is naturally described in terms of Clifford algebras. In particular, the discriminant of the suborder is essentially given by the corresponding value of the quadratic form q.

Another technique that we develop is a one to one correspondence between orders and hermitian planes. Given a quadratic order R, a quaternion algebra Λ is called R-primitive if there exists an embedding of R into Λ. We show that in the local case there is a one to one correspondence between such orders and hermitian planes over R.

We give two applications of the above described results. First, combining the two techniques, we can characterize the suborders up to genus, i.e. any optimally embedded suborder of Λ can locally described up to isomorphism.

As a second application will prove in general that the norm one group of Λ maps surjectively onto the spinorial kernel group of the lattice L. This is a problem that was studied by James in [7]. He constructed in some situations an explicit lattice having this property. Our proof is however completely general, and in particular we do not need to make any restrictions at dyadic places.

The original motivation for this work was for studying compact Shimura surfaces, see [5]. There the Λ^1-orbits in the lattice L corresponds to certain modular curves on the surfaces.

1 Preliminaries

1.1 Algebras and orders

Let P be a Dedekind domain, and F its field of quotients. We assume that all residue fields of P are perfect and that $\mathrm{char}(F) \neq 2$. Let K be a separable quadratic extension of F. The non-trivial automorphism of K is denoted by $x \mapsto \overline{x}$, and R is the ring of integers in K. Let $R^{\#} = \{x \in K \mid \mathrm{tr}(xR) \subseteq P\}$, and the discriminant D is the P-ideal $D = [R^{\#} : R]$. There exist an ideal $\mathcal{D}$ in R, the different, such that $N_{K/F}(\mathcal{D}) = D$.

If L is a lattice over P, then we say that an element $\beta \in L$ is *primitive*, if for every $x \in F$ such that $x\beta \in L$ we have $x \in P$. Similarly, we say that an integral quadratic or hermitian form f is primitive if xf, where $x \in F$, is integral only if $x \in P$.

Let B be a quaternion algebra over F, i.e. a central simple algebra of dimension 4 over F. In case K is a field, then the following lemma is the Skolem-Noether theorem. In the case $K \cong F \times F$, see lemma 2.5 in [5] for a proof.

Lemma 1. *If ρ_1 and ρ_2 are embeddings of K into B, then there exists an invertible element $u \in B$ such that $\rho_1(x) = u\rho_2(x)u^{-1}$ for all $x \in K$.*

Let $\mathcal{O} \subset B$ be an order over P. The dual lattice is $\mathcal{O}^{\#} = \{x \in B \mid \mathrm{tr}(x\mathcal{O}) \subseteq P\}$, and the reduced discriminant $d(\mathcal{O})$ of $\mathcal{O}$ is the P-ideal which satisfies $[\mathcal{O}^{\#} : \mathcal{O}] = d(\mathcal{O})^2$.

Recall that the $\mathcal{O}$ is called *hereditary*, if every (left) $\mathcal{O}$-module is projective. An order is hereditary if and only if the discriminant $d(\mathcal{O})$ is square free. The order $\mathcal{O}$ is said to be a *Gorenstein order*, if $\mathcal{O}^{\#}$ is projective as left (or equivalently right) $\mathcal{O}$-module. $\mathcal{O}$ is called *Bass order* if every order $\mathcal{O}'$ containing $\mathcal{O}$ is a Gorenstein order. Finally, an order $\mathcal{O}$ is a Gorenstein (Bass) order if and only if $\mathcal{O}_{\mathfrak{p}}$ is a Gorenstein (Bass) order for every prime ideal $\mathfrak{p}$.

Assume that F is a local field, i.e. it is complete under some discrete valuation v, and let π be a prime element of F (we assume that $v(\pi) = 1$). If K is split, then $R = P \times P$, with $\overline{(x, y)} = (y, x)$ for $x, y \in P$. Assume that K is a field. We have $R = P[\Pi]$, where the prime element Π is given as follows. If F is non-dyadic, then $\Pi = \sqrt{\theta}$ where $v(\theta) = 0$ if the extension K/F is unramified and $v(\theta) = 1$ if it is ramified. Consider the dyadic case. If K/F is unramified, then $\Pi = 2^{-1}(1 + \sqrt{\theta})$ where $\theta \equiv 1 + 4\rho \pmod{4\pi}$ and ρ is a unit in P. If the extension is ramified there are two cases: In the so called ramified unit case we have $\Pi = \pi^{-k}(1 + \sqrt{\theta})$, where $\theta = 1 + \pi^{2k+1}\rho$, $\rho \in P^*$ and k is a rational integer with $0 \leq k < v(2)$. In the so called ramified prime case, we have $\Pi = \sqrt{\theta}$, where $v(\theta) = v(\pi)$. There exist an element $\delta \in R$ such that $\overline{\delta} = -\delta$ and $\mathcal{D} = (\delta)$. We have $\delta = \Pi$ in the non-dyadic case, $\delta = \sqrt{\theta}$ in the dyadic unramified case, $\delta = 2\Pi$ in the dyadic ramified prime case, and $\delta = 2\pi^{-k}\sqrt{\theta}$ in the dyadic ramified unit case.

In the local case, let $J(\mathcal{O})$ denote the Jacobson radical of the quaternion order $\mathcal{O}$. $\mathcal{O}$ is said to be an *Azumaya order*, if $\mathcal{O}/J(\mathcal{O})$ is a non-trivial central simple algebra over the residue field $\widehat{P} = P/(\pi)$. If $\mathcal{O}$ is a Gorenstein order which is not Azumaya, then the Eichler invariant $e(\mathcal{O})$ is defined by

$$e(\mathcal{O}) = \begin{cases} -1 & \text{if } \mathcal{O}/J(\mathcal{O}) \text{ is a quadratic field extension if } \widehat{P}, \\ 1 & \text{if } \mathcal{O}/J(\mathcal{O}) \cong \widehat{P} \times \widehat{P}, \\ 0 & \text{if } \mathcal{O}/J(\mathcal{O}) \cong \widehat{P}. \end{cases}$$

We recall the construction of even Clifford algebras. Let L be a P-lattice on the F-vector space V such that $FL = V$. Let $q : V \to F$ be a quadratic form such that $q(L) \subseteq P$. Consider the tensor algebra $\mathcal{T}_0(L) = \bigoplus_{k=0}^{\infty} L^{\otimes 2k}$. If I_0 is the ideal in $\mathcal{T}_0(L)$ generated by all elements $x \otimes x - q(x)$, where $x \in L$, then $C_0(L, q) = \mathcal{T}_0(L)/I_0$ is called the *even Clifford algebra* of (L, q). The following result can be shown by a direct calculation (see [8], Satz 7).

Proposition 2. *If $\mathcal{O} = C_0(L, q)$, then the reduced discriminant of $\mathcal{O}$ is given by $d(\mathcal{O}) = d(q)$.*

1.2 Orders in the local case

Assume that F is a local field. In this case, there are only two isomorphism classes of quaternion algebras over F. If $\mathcal{O}$ is a maximal order in $M_2(F)$, then there exists an invertible element $u \in M_2(F)$ such that $\mathcal{O} = uM_2(P)u^{-1}$ (see [9], theorem 17.3). If B is a skew field, then B has a unique maximal order $\mathcal{O}$. It has a P-basis $1, E_1, E_2, E_3$, where

$$E_1^2 = -\epsilon - E_1, \quad E_2^2 = \pi, \quad E_3 = E_1E_2, \quad E_2E_1 + (E_1 + 1)E_2 = 0, \qquad (1)$$

where $\epsilon \in P$, $1 - 4\epsilon \in P^* \setminus P^{*2}$. The norm form is:

$$\mathrm{nr}(\lambda) = a_0^2 - a_0a_1 + \epsilon a_1^2 - \pi(a_2^2 - a_2a_3 + \epsilon a_3^2), \qquad (2)$$

where $\lambda = a_0 + a_1E_1 + a_2E_2 + a_3E_3$ for $a_i \in P$. Using this, one easily get that $\mathcal{O} = \{x \in B \mid \mathrm{nr}(x) \in P\}$. We let Ω_F denote this unique maximal order in the unique skew field over F.

The proofs of the following results can be found in [1]:

Proposition 3. *If $e(\mathcal{O}) = -1$, then $\mathcal{O}$ is a Bass order. Furthermore, there is a unique chain of orders*

$$\mathcal{O} = \mathcal{O}_0 \subset \mathcal{O}_1 \subset \cdots \subset \mathcal{O}_n$$

such that $[\mathcal{O}_{i+1} : \mathcal{O}_i] = (\pi^2)$ and $e(\mathcal{O}_i) = -1$ for $i = 0, 1, \ldots, n-1$, and $\mathcal{O}_n$ is a maximal order.

Proposition 4. *If $e(\mathcal{O}) = 0$ and $\mathcal{O}$ is a Bass order, then there is a unique chain of orders*

$$\mathcal{O} = \mathcal{O}_0 \subset \mathcal{O}_1 \subset \cdots \subset \mathcal{O}_n$$

such that $[\mathcal{O}_{i+1} : \mathcal{O}_i] = (\pi)$, $e(\mathcal{O}_i) = 0$ for $i = 0, 1, \ldots, n-1$, and $d(\mathcal{O}_n) = (\pi)$.

If $\mathcal{O}$ is a Bass order with $e(\mathcal{O}) = -1$ or 0, then the first hereditary order in the chain of orders in proposition 3 or proposition 4 respectively, is called the *hereditary closure* of $\mathcal{O}$ and is denoted $H(\mathcal{O})$.

1.3 Primitive orders

We say that the order $\mathcal{O}$ over P is *R-primitive* if there exists an embedding of R into $\mathcal{O}$. If an order is R-primitive for some R, then it is a Bass order (see [1], prop. 1.4). The following result follows from proposition 1.12 and remark 1.16 in [2]:

Proposition 5. *Assume that P is a local ring and that $\mathcal{O}$ is an R-primitive order which is not Azumaya. If K/F is unramified, then $e(\mathcal{O}) = -1$. If K/F is split, then $e(\mathcal{O}) = 1$. If K/F is ramified and $\mathcal{O}$ is not hereditary, then $e(\mathcal{O}) = 0$. Furthermore, assume that $d(\mathcal{O}) = (\pi^n)$, where $n \in \mathbb{Z}$. Then:*

i) If $e(\mathcal{O}) = -1$, then $\mathcal{O} = R + J(H(\mathcal{O}))^m$, where $m = n/2$ if $H(\mathcal{O})$ is an Azumaya algebra, and $m = n - 1$ otherwise.

ii) If $e(\mathcal{O}) = 0$, then $\mathcal{O} = R + J(H(\mathcal{O}))^m$, where $m = n - 1$.

If $\mathcal{O}_1$ and $\mathcal{O}_2$ are two R-primitive orders, then by conjugating one of these orders if necessary, we may (by lemma 1) arrange so that they both contain the same copy of R. Hence the situation is

$$\begin{array}{ccc} \mathcal{O}_1 & \subset & B \\ \cup & & \cup \\ R & \subset & \mathcal{O}_2 \, . \end{array} \tag{3}$$

Lemma 6. *Assume that F is a local field, and that K is a field. Let $\mathcal{O}_i$ be two non-maximal R-primitive orders in a quaternion algebra B. Then $H(\mathcal{O}_1) \cong H(\mathcal{O}_2)$.*

Proof. If B is a skew field, then there is nothing to prove since B contains a unique hereditary order. Assume that $B \cong M_2(F)$. If K/F is an unramified field extension, then $e(\mathcal{O}_i) = -1$, for $i = 1, 2$, by proposition 5. Hence we get that $H(\mathcal{O}_i) \cong M_2(P)$ by proposition 3 and we are done. If K is a ramified field, then we get, for $i = 1, 2$, that $e(\mathcal{O}_i) = 0$, and hence that $H(\mathcal{O}_i)$ is a non-maximal hereditary order by proposition 4. Such orders must have Eichler invariant equal to 1, and hence they are isomorphic to $\left(\begin{smallmatrix} P & P \\ \pi P & P \end{smallmatrix}\right)$. $\square$

We have the following result, which is a version of the Eichler-Hasse-Noether-Chevalley-Schilling theorem (cf. [4], Satz 7):

Proposition 7. *Let R be a maximal order in a separable maximal commutative subalgebra K of B, and let $\mathcal{O}_1, \mathcal{O}_2$ be two isomorphic orders in B containing R. Then there exists a non-trivial ideal $\mathfrak{i} \subseteq R$ such that $\mathfrak{i}\mathcal{O}_1 = \mathcal{O}_2\mathfrak{i}$.*

Proof. We only need to check this locally. If K is split, then we may identify B with $M_2(F)$. We can assume, by lemma 1, that the embedding of $R \cong P \times P$ is given by $R = \left(\begin{smallmatrix} P & 0 \\ 0 & P \end{smallmatrix}\right)$. We get that the orders $\mathcal{O}_j$ are of the form $\mathcal{O}_j = \left(\begin{smallmatrix} P & a_j P \\ b_j P & P \end{smallmatrix}\right)$, for $j = 1, 2$, where $a_j, b_j \in F$. Since $\mathcal{O}_1 \cong \mathcal{O}_2$, we get that $(a_1 b_1) = (a_2 b_2) \subseteq P$. It is now clear that if we choose an invertible element $g \in R$ of the form $g = x\left(\begin{smallmatrix} a_2 & 0 \\ 0 & a_1 \end{smallmatrix}\right)$, where $x \in F$, then $g\mathcal{O}_1 = \mathcal{O}_2 g$.

Assume now that K is a field. If the orders $\mathcal{O}_j$ are hereditary, then the claim follows by theorem 1.8 in [3] (it states that the embedding numbers $e_*(R, \mathcal{O}_j)$ (defined therein) are equal to 1, which gives the claim).

Assume that the orders are not hereditary. By proposition 5, we have that $e(\mathcal{O}_1) = e(\mathcal{O}_2) \neq 1$. We get, by proposition 5, that there exists an integer m such that

$$\mathcal{O}_j = R + J(H(\mathcal{O}_j))^m,$$

for $i = 1, 2$. We have that $H(\mathcal{O}_1) \cong H(\mathcal{O}_2)$, by lemma 6, but we know that the assertion holds in the hereditary case, and hence we have that $gH(\mathcal{O}_1) = H(\mathcal{O}_2)g$ for some invertible element $g \in R$. Consequently, we get $gJ(H(\mathcal{O}_1)) = J(H(\mathcal{O}_2))g$, and we are done. □

We are now ready to prove the main result of this section.

Theorem 8. *Assume that F is a local field and let $\mathcal{O}_1, \mathcal{O}_2 \subset B$ be two R-primitive orders. If $d(\mathcal{O}_1) = d(\mathcal{O}_2)$, then $\mathcal{O}_1 \cong \mathcal{O}_2$.*

Proof. If the orders are maximal, then there is nothing to prove. Assume that the orders are non-maximal. We can assume without loss of generality that the situation is as in diagram (3). By lemma 6, we have that $H(\mathcal{O}_1) \cong H(\mathcal{O}_2)$, and hence there exists, by proposition 7, an invertible element $g \in R$ such that $gH(\mathcal{O}_1)g^{-1} = H(\mathcal{O}_2)$. We get, for a suitable integer m as in proposition 5, that $g\mathcal{O}_1 g^{-1} = g(R + J(H(\mathcal{O}_1))^m)g^{-1} = R + J(H(\mathcal{O}_2))^m = \mathcal{O}_2$. □

1.4 Involutions

Let now A be a quaternion algebra over K and B as before a quaternion algebra over F. The following elementary lemma gives the relation between the discriminants of A and B respectively, when $A \cong K \otimes_F B$. For a proof, see [5], lemma 4.3.

Lemma 9. *A is ramified at a prime spot $\mathfrak{q}$ of K if and only if $\mathfrak{q} \neq \overline{\mathfrak{q}}$ and $\mathfrak{p} = \mathfrak{q}\overline{\mathfrak{q}}$ is a split prime spot of F such that $B_{\mathfrak{p}}$ is ramified.*

An *involution of type* 2 on A is a map $\tau : A \to A$ such that $\tau^2(a) = a$, $\tau(a+b) = \tau(a) + \tau(b)$, $\tau(ab) = \tau(a)\tau(b)$ and $\tau(xa) = \overline{x}\tau(a)$ for all $a, b \in A$ and $x \in K$. Observe that if τ is any involution of type 2, then it commutes with the canonical involution on A, i.e. $\tau(a^*) = \tau(a)^*$ for all $a \in A$. Using lemma 9, we get (see [5], prop. 4.4):

Proposition 10. *The following properties are equivalent:*

i) *A has an involution of type 2;*

ii) *A contains a subalgebra which is a quaternion algebra over F;*

iii) *A is ramified at a finite number of pairs of conjugated (different) prime spots of K.*

We have the following well-known result (see [10], theorem 7.4, p. 301):

Lemma 11. *Let τ and ν be two involutions of type 2 on A. Then there exists an invertible element $\gamma \in A$ such that $\tau(\gamma)^* = \gamma$ and $\nu(a) = \gamma^{-1}\tau(a)\gamma$ for all $a \in A$. Furthermore, if γ_1 is another invertible element in A satisfying $\tau(\gamma_1)^* = \gamma_1$ and $\nu(a) = \gamma_1^{-1}\tau(a)\gamma_1$ for all $a \in A$, then there exists $r \in F$ such that $\gamma_1 = r\gamma$.*

Let τ be an involution of type 2 on A and $\Lambda \subset A$ a maximal R-order. We let A_τ and Λ_τ denote the algebra respectively the order consisting of elements fixed under the involution, i.e.

$$A_\tau = \{x \in A \mid \tau(x) = x\}$$

and $\Lambda_\tau = \Lambda \cap A_\tau$. It is clear that, in general, the isomorphism class of Λ_τ do depend on τ. We remark that by statement iii) in proposition 10, it is natural to define $d_P(\Lambda) = d(\Lambda) \cap P$, when A allows an involution of type 2.

Let ν and τ be two involutions. By lemma 11, there exists an element $\gamma = \gamma_{\nu,\tau} \in A$ such that $\tau(\gamma)^* = \gamma$ and $\nu(x) = \gamma^{-1}\tau(x)\gamma$ for all $x \in A$. We say that ν and τ are of the same *local type* if the integers $v_\mathfrak{p}(\mathrm{nr}(\gamma))$ are even for all primes $\mathfrak{p}$ dividing $d(\Lambda)$.

The choice of involution will be important in our constructions. We say that an involution τ on A is *optimal* with respect to a maximal order Λ if $d(\Lambda_\tau) = d_P(\Lambda)$. Locally, for any maximal order there exists an optimal involution. Globally, this is in general not true. To see this, consider for example any algebra A which is ramified at an odd number of pairs of prime spots in K. But it need not be possible even if A is ramified at an even number of pairs of prime spots. Consider for example the case where $F = \mathbb{Q}$ and $A \cong M_2(K)$, but $\Lambda \ncong M_2(R)$ (such orders exist if the class number of K is even). If τ is optimal, then $\Lambda_\tau \cong M_2(\mathbb{Z})$, which gives that $\Lambda \supseteq R\Lambda_\tau \cong M_2(R)$, so we get a contradiction. However, it turns out that it is most important to have good behaviour of Λ_τ at those prime spots that divide D. We say that an involution τ of type 2 on a maximal order Λ is *special*, if for all primes $\mathfrak{p}$ such that $\mathfrak{p} \mid D$, we have $(\Lambda_\tau)_\mathfrak{p} \cong M_2(P_\mathfrak{p})$. Note that for $\mathfrak{p}$ ramified in K we have $(A_\tau)_\mathfrak{p} \cong M_2(F_\mathfrak{p})$, by proposition 10, so the condition of the definition is equivalent to requiring that $(\Lambda_\tau)_\mathfrak{p}$ is maximal. Note also that the involution is special if and only if $d(\Lambda_\tau)$ and D are relatively prime. Another way to formulate this, is to say that $\tau : A_\mathfrak{p} \to A_\mathfrak{p}$ is optimal with respect to $\Lambda_\mathfrak{p}$ for all primes $\mathfrak{p}$, which are ramified in K. In the next section we will see that there always exist an involution which is special with respect to any given maximal order.

We now formulate a local result on optimal involutions in a special case, which we will need later.

Lemma 12. *If F is a local field and π is a prime element such that $\pi \mid d(\Lambda)$, then any involution τ on Λ is optimal. Furthermore, there exists an isomorphism $\Omega_F \times \Omega_F \to \Lambda$ such that the induced involution on $\Omega_F \times \Omega_F$ is given by $\tau(x, y) = (y, x)$ for all $(x, y) \in \Omega_F \times \Omega_F$.*

Proof. By lemma 9, we can identify Λ with $\Omega_F \times \Omega_F$ and let ι be the involution given by $\iota(x, y) = (y, x)$ for all $(x, y) \in \Omega_F \times \Omega_F$. By lemma 11, there exists $\gamma = (b, b^*)$ such that $\tau(\lambda) = \gamma^{-1}\iota(\lambda)\gamma$ for all $\lambda \in \Lambda$. We get that $\Lambda_\tau = \{(x, y) \in \Omega_F \times \Omega_F \mid yb = bx\} \cong \Omega_F$, so τ is optimal.

We clearly have $R\Lambda_\tau \subseteq \Lambda$, but on the other hand we have that $R\Lambda_\tau$ is a maximal order, hence we get $\Lambda = R\Lambda_\tau$. The claim follows. □

1.5 Existence of special involutions

We now show that the requirement that the involution is special can always be fulfilled, i.e. for every maximal order Λ in A there exist an involution which is special with respect to Λ.

Proposition 13. *Let A be a quaternion algebra over K and assume that it exists an involution of type 2 on A. If Λ is a maximal order in A, then there exists an involution of type 2 on A which is special with respect to Λ.*

Proof. Let τ be some involution of type 2 on A. Let $\mathfrak{p}$ be a prime ideal ramified in K. Let $\Pi_\mathfrak{p}$ and $\theta_\mathfrak{p}$ be as in section 1.2, so $\Pi_\mathfrak{p} = \sqrt{\theta_\mathfrak{p}}$ in the non-dyadic and in the dyadic ramified prime case, and $\Pi_\mathfrak{p} = u_\mathfrak{p}^{-1}(1+\sqrt{\theta_\mathfrak{p}})$ for some element $u_\mathfrak{p} \in P_\mathfrak{p}$ in the dyadic ramified unit case. We have $R_\mathfrak{p} = P_\mathfrak{p} + \Pi_\mathfrak{p} P_\mathfrak{p}$ and if $x \in 2R_\mathfrak{p}$, then $x = x_1 + x_2\sqrt{\theta_\mathfrak{p}}$ where $x_1, x_2 \in P_\mathfrak{p}$. From lemma 9, we know that $A_\mathfrak{p} \cong M_2(K_\mathfrak{p})$ and hence we get that the maximal order $\Lambda_\mathfrak{p}$ is isomorphic to $M_2(R_\mathfrak{p})$. We fix such an isomorphism. We let $\iota_\mathfrak{p}$ denote the natural involution on $M_2(K_\mathfrak{p})$, which is given by element-wise conjugation on the entries of the matrices $x \in M_2(K_\mathfrak{p})$. By lemma 11, there exists an element $\gamma_\mathfrak{p} \in A_\mathfrak{p}$ such that $\tau(\gamma_\mathfrak{p})^* = \gamma_\mathfrak{p}$ and $\iota_\mathfrak{p}(x) = \gamma_\mathfrak{p}^{-1}\tau(x)\gamma_\mathfrak{p}$ for all $x \in A_\mathfrak{p}$. Let $t_\mathfrak{p}$ be an integer such that $\mathfrak{p}^{t_\mathfrak{p}}\gamma_\mathfrak{p}^{-1} \in 4p\Lambda_\mathfrak{p}$.

If we let $W = \{x \in A \mid \tau(x)^* = x\}$, then $\gamma_\mathfrak{p} \in W_\mathfrak{p}$ for all $\mathfrak{p}$. Choose now an element $\beta \in W$ such that $\beta - \gamma_\mathfrak{p} \in \mathfrak{p}^{t_\mathfrak{p}}\Lambda_\mathfrak{p}$ for all ramified primes $\mathfrak{p}$. Define an involution of type 2 on A by

$$\nu(x) = \beta^{-1}\tau(x)\beta.$$

We want to show that ν is a special involution with respect to Λ. Let

$$\Lambda_\nu = \{\lambda \in \Lambda \mid \nu(\lambda) = \lambda\}.$$

Let again $\mathfrak{p}$ be a prime ideal ramified in K. If we let $\omega_\mathfrak{p} = \gamma_\mathfrak{p}^{-1}\beta$, then $\nu(\lambda) = \omega_\mathfrak{p}^{-1}\iota_\mathfrak{p}(\lambda)\omega_\mathfrak{p}$ for all $\lambda \in \Lambda_\mathfrak{p}$ and $\iota_\mathfrak{p}(\omega_\mathfrak{p})^* = \omega_\mathfrak{p}$. Now $\omega_\mathfrak{p} - 1 = \gamma_\mathfrak{p}^{-1}(\beta - \gamma_\mathfrak{p}) \in \mathfrak{p}^{t_\mathfrak{p}}\gamma_\mathfrak{p}^{-1}\Lambda_\mathfrak{p} \subseteq 2p(2\Lambda_\mathfrak{p})$, so $\omega_\mathfrak{p} = a_\mathfrak{p} + 2\sqrt{\theta_\mathfrak{p}}b_\mathfrak{p}$, where $a_\mathfrak{p} \in P_\mathfrak{p}^*$ and $b_\mathfrak{p} \in \mathfrak{p}M_2(P_\mathfrak{p})$ with $b_\mathfrak{p}^* = -b_\mathfrak{p}$. We have $(\Lambda_\nu)_\mathfrak{p} = \{\lambda \in \Lambda_\mathfrak{p} \mid \iota_\mathfrak{p}(\lambda)\omega_\mathfrak{p} = \omega_\mathfrak{p}\lambda\}$. We write $\lambda = x + \Pi_\mathfrak{p} y$ with $x, y \in M_2(R_\mathfrak{p})$,

In the non-dyadic case and in the dyadic ramified prime case, then $\iota_\mathfrak{p}(\lambda)\omega_\mathfrak{p} = \omega_\mathfrak{p}\lambda$ if and only if $yb_\mathfrak{p} + b_\mathfrak{p}y = a_\mathfrak{p}y + b_\mathfrak{p}x - xb_\mathfrak{p} = 0$. It is straightforward to verify that we can define a $P_\mathfrak{p}$-linear map $g_\mathfrak{p} : M_2(P_\mathfrak{p}) \to (\Lambda_\nu)_\mathfrak{p}$ by

$$g_\mathfrak{p}(x) = x + a_\mathfrak{p}^{-1}\sqrt{\theta_\mathfrak{p}}(xb_\mathfrak{p} - b_\mathfrak{p}x).$$

We get $\mathrm{nr}_{\Lambda_\mathfrak{p}/R_\mathfrak{p}}(g_\mathfrak{p}(x)) = xx^* + da_\mathfrak{p}^{-2}\,\mathrm{nr}_{\Lambda_\mathfrak{p}/R_\mathfrak{p}}(b_\mathfrak{p}x - xb_\mathfrak{p})$, which gives that

$$\mathrm{nr}_{\Lambda_\mathfrak{p}/R_\mathfrak{p}}(g_\mathfrak{p}(x)) \equiv \det(x) \pmod{\mathfrak{p}}$$

for all $x \in M_2(P_\mathfrak{p})$. But the determinant form on $M_2(P_\mathfrak{p})$ has discriminant 1, and hence the norm form on $(\Lambda_\nu)_\mathfrak{p}$ has discriminant 1 too. Hence $(\Lambda_\nu)_\mathfrak{p} \cong M_2(P_\mathfrak{p})$ and we are done.

In the dyadic ramified unit case, then $\iota_\mathfrak{p}(\lambda)\omega_\mathfrak{p} = \omega_\mathfrak{p}\lambda$ is equivalent to $b_\mathfrak{p}y + yb_\mathfrak{p} = 0$ and $(a+2b)y = u_\mathfrak{p}(xb_\mathfrak{p} - b_\mathfrak{p}x)$. We can define a map $g_\mathfrak{p} : M_2(P_\mathfrak{p}) \to (\Lambda_\nu)_\mathfrak{p}$ by

$$g_\mathfrak{p}(x) = x + u_\mathfrak{p}(a_\mathfrak{p} + 2b_\mathfrak{p})^{-1}\sqrt{\theta_\mathfrak{p}}(xb_\mathfrak{p} - b_\mathfrak{p}x).$$

and proceed as above. □

2 On orders associated to hermitian planes

2.1 Hermitian planes

A hermitian plane (V, h) is 2-dimensional vector space V over K together with a map $h : V \times V \to K$ which is K-linear in the first variable and satisfies $h(y, x) = \overline{h(x, y)}$ for all $x, y \in V$. There is a well known way (see [11]) to construct quaternion algebras from hermitian planes. Our aim in this section is to extend this construction to orders and examine some of its properties.

Proposition 14. *Let (V, h) be a non-degenerate hermitian plane over K. Then*

$$Q_h = \{f \in \operatorname{End}_K(V) \mid h(f^* x, y) = h(x, fy) \ \forall x, y \in V\}$$

is a quaternion algebra. Furthermore, Q_h is split if and only if $-\det(h)$ is trivial in $F^*/\operatorname{nr}_{K/F}(K^*)$, i.e. if and only if h is isotropic.

For a proof, see [11], p. 23–25.

Let M be a projective R-module of rank 2. Any such M will be called an *R-plane*. Let $V = K \otimes_R M$, so V is a 2-dimensional vector space containing M as a lattice. If $h : M \times M \to R$ is a hermitian form, then we construct a P-order $\mathcal{O}_h$, by

$$\mathcal{O}_h = \{\lambda \in \operatorname{End}_R(M) \mid h(x, \lambda y) = h(\lambda^* x, y) \text{ for all } x, y \in M\}, \tag{4}$$

i.e. we have $\mathcal{O}_h = Q_h \cap \operatorname{End}_R(M)$. Note that $\operatorname{End}_R(M)$ is a maximal order in $\operatorname{End}_K(V)$. It is clear that the isomorphism class of $\mathcal{O}_h$ only depends on the similarity class of h.

We know that an R-primitive order is a Bass order. Conversely, it is true, if P is a local ring, that any Bass order $\mathcal{O}$ is R-primitive for some maximal order R in some quadratic extension of F (see proposition 1.11 in [2]). We will see later in this section that if P is a local ring, then the order $\mathcal{O}_h$ in (4) is in fact R-primitive. As a consequence we get, for an arbitrary base ring P, that $\mathcal{O}_h$ is a Bass order.

2.2 A one to one correspondence

To a similarity class of hermitian R-planes we have, by (4), associated a P-order. Now we want to give a construction going in the opposite direction. Given an R-primitive order, we want to construct a similarity class of hermitian R-planes.

Let $\mathcal{O}$ be an R-primitive order with a fixed choice of an embedding of R into $\mathcal{O}$. We want to construct a hermitian form $h_{\mathcal{O}}$, on some R-plane M, in such a way that the similarity class of $h_{\mathcal{O}}$ is well defined. Now $\mathcal{O}$ can be naturally considered as an R-plane by multiplication from the left, and we will in fact construct a hermitian form on this R-plane. Consider the natural embedding of $\mathcal{O}$ into $\operatorname{End}_R(\mathcal{O})$ given by

$$\lambda \mapsto \hat{\lambda} = (v \mapsto v\lambda^*),$$

for all $\lambda \in \mathcal{O}$. This induces the following commutative diagram of ring embeddings

$$\begin{tikzcd} A \arrow[r] & \mathrm{End}_K(A) \\ \mathcal{O} \arrow[r] \arrow[u] & \mathrm{End}_R(\mathcal{O}) \,. \arrow[u] \end{tikzcd} \tag{5}$$

With these identifications, it is clear that we have

$$\mathcal{O} = A \cap \mathrm{End}_R(\mathcal{O}). \tag{6}$$

Now we claim that there exists a map

$$\xi : A \to K \tag{7}$$

satisfying $\xi(F) = F$, $\xi(la) = l\xi(a)$ for all $l \in K$, $a \in A$, and $\xi(a^*) = \overline{\xi(a)}$ for all $a \in A$. We can construct ξ as follows. Let $u \in A$ be such that $\bar{l} = ulu^{-1}$ for all $l \in K$. Such an element u exists by lemma 1. Now we get that $A = K \oplus Ku$ and we let ξ be projection on the first summand. It is straightforward to verify that this map has the required properties. The map ξ is uniquely determined up to a non-zero factor of F. We choose one such map ξ satisfying $\xi(\mathcal{O}) \subseteq R$ and we define the hermitian form

$$h_{\mathcal{O}} : \mathcal{O} \times \mathcal{O} \to R$$

by

$$h_{\mathcal{O}}(x, y) = \xi(xy^*).$$

Using this construction, we get in particular:

Proposition 15. *If $\mathcal{O}$ is an R-primitive order, then $\mathcal{O}$ is isomorphic to $\mathcal{O}_h$ for some R-plane (M, h).*

Proof. We want to show that we can choose (M, h) as the hermitian R-plane $(\mathcal{O}, h_{\mathcal{O}})$, or in other words that the composition $\mathcal{O} \mapsto h_{\mathcal{O}} \mapsto \mathcal{O}_{h_{\mathcal{O}}}$ induces the identity on the set of isomorphism classes of R-orders. It is clear that $h_{\mathcal{O}}(x, \hat{\lambda}(y)) = h_{\mathcal{O}}(\hat{\lambda}^*(x), y)$ for all $x, y, \lambda \in \mathcal{O}$. Furthermore, we claim that the copy of A in $\mathrm{End}_K(A)$ given by diagram (5), equals

$$\{f \in \mathrm{End}_K(A) \mid h_{\mathcal{O}}(x, f(y)) = h_{\mathcal{O}}(f^*(x), y) \text{ for all } x, y \in A\}. \tag{8}$$

Namely, A is clearly an F-subalgebra of the algebra defined by (8). On the other hand, both these algebras are 4-dimensional vector spaces over F, and hence equal. Now, using equality (6), we get that $\mathcal{O}_{h_{\mathcal{O}}} = \mathcal{O}$ as desired. □

The following lemma is the key step to prove that we get a one-to-one correspondence between similarity classes of R-planes and isomorphism classes of R-primitive orders in the local case. If (M, h) is a R-plane, then $n(h)$ denotes the P-ideal generated by all elements $h(u, u)$ for $u \in M$.

Lemma 16. *If $v \in M$, then $\mathcal{O}_h(v) = M$ if and only if $n(h) = (h(v, v))$.*

Proof. First we show that the condition is necessary. Assume that $\mathcal{O}_h(v) = M$. Take an element $w \in M$. Then there exists by hypothesis an element $\lambda_w \in \mathcal{O}_h$ such that $\lambda_w(v) = w$. We get $h(w,w) = h(\lambda_w(v), \lambda_w(v)) = h(v, \lambda_w^* \lambda_w(v)) = \mathrm{nr}(\lambda_w)h(v,v) \in (h(v,v))$. Hence $n(h) = (h(v,v))$, since w was arbitrary.

Now we want to show that the condition is sufficient. If $v \in M$ is any element with $n(h) = (h(v,v))$, then clearly $\mathcal{O}_h(v) \subseteq M$. To show that we have equality, it is sufficient to show that we have equality for all localisations. Hence we can assume that P is a local ring. It is furthermore sufficient to show that $\mathcal{O}_h(v) = M$ for some element v with $n(h) = (h(v,v))$. Let namely $u \in M$ be some other element satisfying $n(h) = (h(u,u))$. By hypothesis, we have $u = \lambda_u(v)$ for some element $\lambda_u \in \mathcal{O}_h$. But then we get, as above, that $(h(u,u)) = \mathrm{nr}(\lambda_u)(h(v,v))$ and hence λ_u is a unit in $\mathcal{O}_h$. Therefore, $\mathcal{O}_h(u) = (\mathcal{O}_h\lambda_u)(v) = \mathcal{O}_h(v) = M$. Scaling h with a suitable constant, we can assume that h is a primitive hermitian form on $M = R \oplus R$. We identify M with 2×1 R-matrices, and a hermitian form h is then given by $h(x,y) = \overline{y}^t Hx$, for some 2×2 matrix H with $\overline{H}^t = H$. With these identifications, we get

$$\mathcal{O}_h = \{\lambda \in M_2(R) \mid \overline{\lambda}^t H = H\lambda^*\}.$$

We want to show that there exists an element $v \in M$ such that $\mathcal{O}_h(v) = M$. There are several cases:

Assume that K is a split algebra, so $R = P \times P$. Let e_1 and e_2 be the orthogonal idempotents of R, so $\overline{e}_1 = e_2$. It is clear that we can find a basis of M such that h is similar to the form given by the matrix $H = \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)$, $x \in P$. We get

$$\mathcal{O}_h = \{e_1X + e_2Y \mid X, Y \in M_2(P) \text{ and } Y^tH = HX^*\},$$

which gives $\mathcal{O}_h = \{e_1\left(\begin{smallmatrix} a & -xb \\ c & d \end{smallmatrix}\right) + e_2\left(\begin{smallmatrix} d & -xc \\ b & a \end{smallmatrix}\right) \mid a,b,c,d \in P\}$. The claim follows by choosing $v = \begin{pmatrix} 1 & 0 \end{pmatrix}^t$.

Assume that K is a local field with, as before, valuation v and prime elements π and Π of P and R respectively. We are now going to use the classification of hermitian planes in [6] to verify the claim.

Assume first that M has an orthogonal basis, so we can choose a basis such that H is given by $H = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $v(\alpha) \le v(\beta)$. We get

$$\mathcal{O}_h = \{\begin{pmatrix} a & -\overline{c}\beta/\alpha \\ c & \overline{a} \end{pmatrix} \mid a, c \in R\},$$

so if we choose $v = \begin{pmatrix} 1 & 0 \end{pmatrix}^t$, then $\mathcal{O}_h(v) = M$ and we are done. If K is an unramified field extension of F, then every hermitian plane has an orthogonal basis (see [6], p. 453). Hence we assume from now on that K is ramified.

Consider first the non-dyadic case. In this case, we can choose π and Π such that $\Pi = \sqrt{\pi}$. By proposition 8.1 in [6], if h does not have an orthogonal basis, then h is similar to a hyperbolic plane, which is given by the matrix

$$H(i) = \begin{pmatrix} 0 & \Pi^i \\ \overline{\Pi}^i & 0 \end{pmatrix}$$

for $i = 0, 1$. We get

$$\mathcal{O}_h = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in P,\ c, d \in R,\ \overline{\Pi}^i\overline{c} = -\Pi^i c,\ \Pi^i\overline{b} = -\overline{\Pi}^i b\}. \tag{9}$$

If $i = 0$, then we get $\mathcal{O}_h = \{\left(\begin{smallmatrix} a & \Pi b \\ \Pi c & d \end{smallmatrix}\right) \mid a, b, c, d \in P\}$, so $\mathcal{O}_h(v) = M$ if $v = \begin{pmatrix}1 & 1\end{pmatrix}^t$. If $i = 1$, then we get $\mathcal{O}_h = M_2(P)$, and we can choose $v = \begin{pmatrix}1 & \Pi\end{pmatrix}^t$.

Now we consider the dyadic case. Let Π be as in section 1.1. According to (9.1) in [6], we have, for $i = 0, 1$, that $n(H(i)) = (2\pi^i)$ in the ramified prime case, and $n(H(i)) = (2\pi^{-k})$ in the ramified unit case. In the former case, the situation is analogous to the non-dyadic case using (9). In the latter case, it is straightforward to check, using (9), that we get $\mathcal{O}_h(v) = M$ if we choose $v = \begin{pmatrix}1 & \Pi\end{pmatrix}^t$ when $i = 0$ and $v = \begin{pmatrix}1 & 1\end{pmatrix}^t$ when $i = 1$.

There are even more subnormal planes h to consider in the dyadic case. According to propositions 9.1, 9.2 and 10.2 in [6], they are given by the following: Let $i = 0$ or $i = 1$, and assume that h is Π^i-modular. We have $n(h) \supseteq n(H(i))$. Assume that $n(h) = (\pi^m)$. Then h can be given by the matrix

$$H = \begin{pmatrix} \pi^m & \Pi^i \\ \overline{\Pi}^i & \alpha \end{pmatrix},$$

where $v(\alpha) \geq m$. It is straightforward to verify that

$$\mathcal{O}_h = \{\begin{pmatrix} a & \Pi^i(a - \overline{a})/\pi^m - \alpha\overline{c}/\pi^m \\ c & \overline{a} + (\Pi^i c + \overline{\Pi}^i\overline{c})/\pi^m \end{pmatrix} \mid a, c \in R\}$$

and hence $v = \begin{pmatrix}1 & 0\end{pmatrix}^t$ will do. □

Assume now that there exists an element $v \in M$ satisfying $\mathcal{O}_h(v) = M$. Then, for any element $s \in R$, there exists a unique element $\lambda_s \in \mathcal{O}_h$ such that $\lambda_s(v) = sv$. Hence we get an embedding of R into $\mathcal{O}_h$ by the map

$$s \mapsto \lambda_s,$$

and consequently $\mathcal{O}_h$ is R-primitive. Furthermore, consider the map $\xi : \mathcal{O}_h \to R$ defined by

$$\xi(\lambda) = h(v, \lambda(v)).$$

This map ξ clearly satisfies all the requirements we made concerning the mapping (7). Using this, it is clear that the composition of maps $h \mapsto \mathcal{O}_h \mapsto h_{\mathcal{O}_h}$ is the identity on the set of similarity classes of hermitian R-planes.

If P is a local ring, then the existence of an element $v \in M$ as in lemma 16 is clear. As a special case of proposition 7, we get in the local case that if $\rho_j : R \to \mathcal{O}$, $j = 1, 2$, are two embeddings, then there exists an element γ in the normaliser $N(\mathcal{O})$ of $\mathcal{O}$ such that $\gamma\rho_1(s)\gamma^{-1} = \rho_2(s)$ for all $s \in R$. Hence we get that the two hermitian spaces constructed by using this two choices of embeddings are isomorphic. In other words, the hermitian form $h_{\mathcal{O}}$ is well defined, that is, it does not depend of the embedding of R into $\mathcal{O}$. Hence we have shown

Theorem 17. *If P is a local ring, then the map $h \mapsto \mathcal{O}_h$ gives a one-to-one correspondence between similarity classes of hermitian R-planes and isomorphism classes of R-primitive orders.*

Since being Bass is a local property, and we know that R-primitive orders are Bass orders, we get the following global result:

Corollary 18. *The orders $\mathcal{O}_h$ are Bass orders.*

Remark. It is easy to give a global example when the map $h \mapsto \mathcal{O}_h$ is not injective. Let $P = \mathbb{Z}$ and $R = \mathbb{Z}[i]$. We let h_1 be the hermitian form given by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 6 \end{smallmatrix}\right)$, and h_2 the form given by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$. We have that h_1 and h_2 do not belong to the same similarity class of hermitian forms over R. This can be seen by noting that there is no element v such that $(h_2(v, v)) = n(h_2) = (1)$, but such an element clearly exists for h_1. A straightforward calculation gives that $\mathcal{O}_{h_1} \cong \mathcal{O}_{h_2}$.

3 The quaternary lattice

Let A be a quaternion algebra over K with a maximal R-order Λ and a special involution τ. We will now construct a natural P-lattice L_τ in a certain F-subspace W_τ of A. The point of this lattice is that it parametrises optimally embedded suborders of Λ.

3.1 Construction

Define
$$W_\tau = \{\beta \in A \mid \tau(\beta)^* = \beta\},$$
which is a 4-dimensional vector space over F. Consider now the norm form $\mathrm{nr} : A \to K$. If $\beta \in W_\tau$, then $\mathrm{nr}(\beta) = \mathrm{nr}(\tau(\beta)^*) = \overline{\mathrm{nr}(\beta)}$. Hence nr restricts to a quadratic form on W_τ taking values in F:
$$\mathrm{nr}\,|_{W_\tau} : W_\tau \to F.$$
Let $A_0 = \{x \in A \mid \mathrm{nr}(x) \in F,\ \ \mathrm{nr}(x) \neq 0\}$. We define an action of A_0 on W_τ by
$$x \cdot \beta = \tau(x)\beta x^{-1}, \tag{10}$$
It is easy to check, that this induce a group homomorphism of A_0 into the orthogonal group $O(W_\tau, \mathrm{nr})$.

To define the lattice, we first need an auxiliary definition. Consider A as a right A-module. A map $\Phi : A \times A \to A$ is called an A-hermitian form if

i) $\Phi(x + y, z) = \Phi(x, z) + \Phi(y, z)$,

ii) $\Phi(xa, y) = \Phi(x, y)a$,

iii) $\Phi(x, y) = \tau(\Phi(y, x))^*$,

for all $a, x, y, z \in A$. Furthermore, we say that Φ is *integral* with respect to the order Λ, if

iv) $\Phi(x, y) \in \Lambda$ for all $x, y \in \Lambda$,

v) $\Phi(x, x) \in R + \mathcal{D}\Lambda$ for all $x \in \Lambda$.

Let τ be a special involution. For any β in W_τ, we define a hermitian form $\Phi_{\tau,\beta} : A \times A \to A$ by
$$\Phi_{\tau,\beta}(x, y) = \tau(y)^*\beta x.$$

We are interested in those elements β for which $\Phi_{\tau,\beta}$ satisfy the above integrality conditions, so we define a P-lattice L_τ of rank 4 by

$$L_\tau = \{\beta \in W_\tau \mid \Phi_{\tau,\beta} \text{ is integral}\}. \tag{11}$$

Let $\Lambda^1 = \{\lambda \in \Lambda \mid \mathrm{nr}(\lambda) = 1\}$. It is clear from the definitions, that if $\lambda \in \Lambda^1$ and $\beta \in L$, then $\tau(\lambda)\beta\lambda^* \in L$. Hence, the action (10) restricts to an action of Λ^1 on L. Now, we also define a dual lattice $L_\tau^\#$ to L_τ by

$$L_\tau^\# = \{l \in W_\tau \mid \mathrm{tr}(l^* L_\tau) \subseteq P\}.$$

In section 4.1, we will also define quadratic forms q_τ and $q_\tau^\#$ on these lattices.

3.2 Uniqueness

In this section we prove a somewhat technical result which relates the lattices we get if we use different involutions of the same local type. However, first we prove an elementary result: If $b \in A$ with $b \neq 0$, define the ideal

$$m_\Lambda(b) = \{x \in K \mid xb \in \Lambda\}. \tag{12}$$

Lemma 19. *Assume that K is a local field. If $\Lambda \cong M_2(R)$ and $a, b \in \Lambda$ with $m_\Lambda(b) = R$, then $\Lambda a \Lambda \subseteq b\Lambda$ if and only if $a \in \mathrm{nr}(b)\Lambda$.*

Proof. Let Π be a prime element of K. Assume that $m_\Lambda(b) = R$, i.e. $b \in \Lambda$ and $b \notin \Pi\Lambda$. The two-sided ideal $\Lambda a \Lambda$ satisfies $\Lambda a \Lambda = \Pi^n \Lambda$ for some integer n (see theorem 18.3 in [9]). We get $\Lambda a \Lambda \subseteq b\Lambda$ if and only if $\Pi^n \Lambda \subseteq b\Lambda$ if and only if $\Pi^n b^* \Lambda \subseteq \mathrm{nr}(b)\Lambda$ if and only if $b \in \Pi^{-n}\,\mathrm{nr}(b)\Lambda$. By the hypothesis on b, this is equivalent to $\Pi^n \in (\mathrm{nr}(b))$. The claim follows. ☐

Proposition 20. *If τ and ν are special involutions, which belong to the same local type, then there exists an element $\gamma \in W_\tau$ and an ideal $\mathfrak{i}$ in P such that $\nu(x) = \gamma^{-1}\tau(x)\gamma$ for all $x \in A$ and $L_\nu = \gamma^* \mathfrak{i} L_\tau$.*

Proof. By lemma 11, there exists an element $w \in W_\tau$ such that

$$\nu(x) = w^{-1}\tau(x)w$$

for all $x \in A$. If $x \in A$, then by a straightforward calculation, we get that $\nu(w^*x)^* = w^*x$ if and only if $\tau(x)^* = x$. Hence, we conclude that

$$W_\nu = w^* W_\tau,$$

so the two lattices L_ν and $w^* L_\tau$ span the same 4-dimensional F-vector space, i.e. they are commensurable.

We must show that for every prime $\mathfrak{p}$ there exists $r \in F_\mathfrak{p}$ such that

$$(L_\nu)_\mathfrak{p} = r w^* (L_\tau)_\mathfrak{p}. \tag{13}$$

Hence, we assume from now on that F is a local field. We examine the different cases:

We consider first the case $\pi \mid d(\Lambda)$. By lemma 12, we can make the identification $\Lambda = \Omega_F \times \Omega_F$ with $\tau(x, y) = (y, x)$. Consider now the involution ν given by $\nu(\lambda) = w^{-1}\tau(\lambda)w$, where $w = (c, c^*)$ with $c \in \Omega_F$. By the hypothesis that these two involutions are of the same local type, we have that $v_\pi(\mathrm{nr}(w)) = v_\pi(\mathrm{nr}(c))$ is even. This implies that c is of the form $s\epsilon$, for some $s \in F$ and $\epsilon \in \Omega_F^*$. We now get

$$L_\tau = \{(x, x^*) \mid x \in \Omega_F\}$$

and

$$L_\nu = \{(x, \epsilon x^* \epsilon^{-1}) \mid x \in \Omega_F\}.$$

Hence we get $L_\nu = s^{-1}w^* L_\tau$ and we are done in this case.

Assume now that $\pi \nmid d(\Lambda)$. We have that $\Lambda \cong M_2(R)$ and we let ι be the optimal involution on $M_2(R)$, which is given by element-wise conjugation, i.e.

$$\iota((a_{ij})) = (\overline{a}_{ij})$$

if $(a_{ij}) \in M_2(R)$. We now claim that it is sufficient to show the following:

Claim. *For any special involution σ on A, there exists $\gamma_\sigma \in W_\iota$ such that the following holds*

i) $\sigma(x) = \gamma_\sigma^{-1}\iota(x)\gamma_\sigma$ *for all* $x \in A$.

ii) $L_\sigma = \gamma_\sigma^* L_\iota$.

Assume namely that this claim is true. Then it is easy to check that the following holds: $\tau(\gamma_\tau^{-1}\gamma_\nu)^* = \gamma_\tau^{-1}\gamma_\nu$, $\nu(x) = (\gamma_\tau^{-1}\gamma_\nu)^{-1}\tau(x)\gamma_\tau^{-1}\gamma_\nu$ for every $x \in A$ and $L_\nu = (\gamma_\tau^{-1}\gamma_\nu)^* L_\tau$. By the uniqueness part of lemma 11, we have $\gamma_\tau^{-1}\gamma_\nu = rw$ for some $r \in F$, and hence we have shown that (13) holds if the claim holds. We will now prove the claim in the different cases.

Assume first that π is unramified in K. Let $\gamma_\sigma \in W_\iota$ be some element satisfying i) in the claim. Replacing, if necessary, γ_σ with $s\gamma_\sigma$ for some suitable $s \in F$, we may assume that $m_\Lambda(\gamma_\sigma) = (1)$ (see (12)). Now we have

$$L_\iota = \{y \in W_\iota \mid \Lambda y \Lambda \subseteq \Lambda\}$$

and

$$L_\sigma = \{\gamma_\sigma^* y \mid y \in W_\iota,\ \sigma(\Lambda)\gamma_\sigma^* y \Lambda \subseteq \Lambda\}.$$

But $\sigma(\Lambda)\gamma_\sigma^* y\Lambda \subseteq \Lambda$ if and only if $\gamma_\sigma^*\Lambda y \Lambda \subseteq \Lambda$, which, by lemma 19, is equivalent to $\Lambda y \Lambda \subseteq \Lambda$. Hence, we get $L_\sigma = \gamma_\sigma^* L_\iota$.

Assume now that π is ramified in K. By the hypothesis that σ is special, we have that $\Lambda_\sigma \cong M_2(P)$. We claim that this implies that, replacing γ_σ with $s\gamma_\sigma$ for some $s \in F$ if necessary, we can assume that γ_σ is of the form

$$\gamma_\sigma = \iota(\epsilon)^*\epsilon, \tag{14}$$

for some unit $\epsilon \in \Lambda$. To see this, fix an isomorphism $\Lambda_\iota \to \Lambda_\sigma$. Since $R\Lambda_\iota = R\Lambda_\sigma = \Lambda$, this map can be extended to an automorphism of Λ. By the Skolem-Noether theorem this automorphism is inner, and hence there exists an invertible element g in A such that $\Lambda_\sigma = g^{-1}\Lambda_\iota g$. Then we also get that g satisfies $g\Lambda = \Lambda g$, so $g\Lambda$ is a two-sided ideal. Hence $g\Lambda = a\Lambda$ for some $a \in K$, and therefore $g = a\epsilon$ for some $\epsilon \in \Lambda^*$. Thus, we get

$$\Lambda_\sigma = \epsilon^{-1}\Lambda_\iota\epsilon.$$

Now, for any $\lambda \in \Lambda_\iota$, we have $\sigma(\epsilon^{-1}\lambda\epsilon) = \epsilon^{-1}\lambda\epsilon$. Hence $\iota(\epsilon)\gamma_\sigma\epsilon^{-1} \in K$ and we get that γ_σ must be of the form

$$\gamma_\sigma = t\iota(\epsilon)^*\epsilon,$$

for some $t \in K$. But $\iota(\gamma_\sigma)^* = \gamma_\sigma$, so $\overline{t} = t$, and hence we have $t \in F$. Replacing γ_σ with $t^{-1}\gamma_\sigma$, we have demonstrated (14).

Now we get

$$L_\iota = \{x \in W_\iota \mid x \in R + \mathcal{D}\Lambda\}$$

and

$$L_\sigma = \{\gamma_\sigma^* y \mid y \in W_\iota,\ \gamma_\sigma^* x \in R + \mathcal{D}\Lambda\}.$$

With γ_σ as in (14), it is clear that for any $y \in \Lambda$, we have $y \in R + \mathcal{D}\Lambda$ if and only if $\gamma_\sigma^* y \in R + \mathcal{D}\Lambda$. It follows that $L_\sigma = \gamma_\sigma^* L_\iota$. We have now proved the claim in the case that K is a field.

Assume finally that π is split in K and that $\pi \nmid d(\Lambda)$. Then $R = P \times P$, and we identify Λ with $M_2(P) \times M_2(P)$, where $\iota(a, b) = (b, a)$. Hence

$$L_\iota = \{(x, x^*) \mid x \in M_2(P)\}.$$

Let $\gamma_\sigma = (b, b^*)$, where $b \in M_2(P)$ with $\det(b) \neq 0$. Without loss of generality, we can assume that b is primitive, i.e. $b \notin \pi M_2(P)$. We get

$$L_\sigma = \{\gamma_\sigma^* y \mid y \in W_\iota,\ \sigma(\Lambda)\gamma_\sigma^* y\Lambda \subseteq \Lambda\}.$$

If $y \in W_\iota$, so $y = (z, z^*)$, where $z \in M_2(F)$, then we have $\sigma(\Lambda)\gamma_\sigma^* y\Lambda \subseteq \Lambda$ if and only if $b^* M_2(P) z M_2(P) \subseteq M_2(P)$. According to lemma 19, this is equivalent to $z \in M_2(P)$. Hence we get $L_\sigma = \gamma_\sigma^* L_\iota$, so the claim holds in the split case too. $\square$

For future reference we now write down an explicit local description of the lattices for an optimal involution ι on Λ. If $\pi \mid d(\Lambda)$, then we have

$$L_\iota = \{\beta = (x, x^*) \mid x \in \Omega_F\} \tag{15a}$$

and

$$L_\iota^\# = \{l = (y, y^*) \mid y \in \Omega_F^\#\}. \tag{15b}$$

If $\pi \nmid d(\Lambda)$, then we have

$$L_\iota = \{\beta = \begin{pmatrix} \alpha & a\delta \\ b\delta & \overline{\alpha} \end{pmatrix} \mid \alpha \in R,\ a, b \in P\} \tag{16a}$$

and

$$L_\iota^\# = \{l = \begin{pmatrix} \alpha & a/\delta \\ b/\delta & \overline{\alpha} \end{pmatrix} \mid \alpha \in R^\#,\ a, b \in P\}. \tag{16b}$$

4 Optimally embedded orders

We use the notations of section 3. A P-suborder $\mathcal{O}$ of Λ is said to be *optimally embedded* if $\mathcal{O} = F\mathcal{O} \cap \Lambda$. If β is an invertible element in A, then we define a F-subalgebra of A:

$$A_{\tau,\beta} = \{a \in A \mid \beta a = \tau(a)\beta\},$$

and an order $\Lambda_{\tau,\beta}$ in $A_{\tau,\beta}$:

$$\Lambda_{\tau,\beta} = A_{\tau,\beta} \cap \Lambda.$$

Lemma 21. *Every F-subalgebra of A which is a quaternion algebra is of the form $A_{\tau,\beta}$ for some invertible element β in L.*

Proof. Since every F-subalgebra which is a quaternion algebra corresponds to an involution ν of type 2 having the given subalgebra as its fixed point set, the claim follows from lemma 11. □

In particular, lemma 21 implies that any optimally embedded order in Λ is of the form $\Lambda_{\tau,\beta}$ for some $\beta \in L$.

4.1 A Clifford algebra construction

In general the maximal order Λ is not isomorphic to an even Clifford algebra of a quaternary lattice. However, as we will see in this section, there is a natural large subring which is. For simplicity, we assume in this section that F is a local field.

We define quadratic forms

$$q_\tau : L_\tau \to P, \quad q_\tau(\beta) = x_\tau \operatorname{nr}(\beta),$$

and

$$q_\tau^\# : L_\tau^\# \to P, \quad q_\tau^\#(l) = y_\tau \operatorname{nr}(l),$$

where the factors x_τ and y_τ are elements of F chosen such that q_τ and $q_\tau^\#$ are primitive integral forms. These forms will hence only be defined up to a factor in P^*. It follows however from proposition 20 that the similarity classes of these quadratic forms do not depend on the choice of special involution τ (at least up to local type). We also remark that the quadratic forms q_τ and $q_\tau^\#$ also exists globally for instance in the case when P is a PID.

Consider now the quaternary quadratic lattice $(L_\tau^\#, q_\tau^\#)$ and the even Clifford algebra $C_0(L_\tau^\#, q_\tau^\#)$ associated to it. Define a function

$$\phi_\tau : L_\tau^\# \otimes_P L_\tau^\# \to A$$

by

$$\phi_\tau(l_1 \otimes l_2) = y_\tau l_1^* l_2.$$

We can extend ϕ_τ in a natural way to the even tensor algebra, so we get a map $\phi_\tau : \mathcal{T}_0(L_\tau^\#) \to A$. This map clearly vanishes on the ideal generated by the elements $l \otimes l - q_\tau^\#(l)$ giving an embedding of the ring $C_0(L_\tau^\#, q_\tau^\#)$ into the algebra A. Θ_τ will denote the image of the map

$$\phi_\tau : C_0(L_\tau^\#, q_\tau^\#) \to A$$

Θ_τ is a subring of A, but it should be noted that it is not in general an R-order. However, we have:

Lemma 22. *We have that $\Theta_\tau \subseteq \Lambda$ and $\Lambda/\Theta_\tau \cong R/d(\Lambda)$ (as abelian groups). More precisely, we have*

$$\Theta_\tau = \{\lambda \in \Lambda \mid \operatorname{nr}(\lambda - \tau(\lambda)) \in d(\Lambda)\}. \tag{17}$$

Proof. Let ν be another special involution of the same local type as τ. By proposition 20, there exists an element $\gamma \in L_\tau$ such that

$$L_\nu = \gamma^* L_\tau.$$

It immediately follows that

$$L_\tau^\# = \gamma L_\nu^\#,$$

and hence we get that $y_\nu = \eta \operatorname{nr}(\gamma) y_\tau$ for some $\eta \in P^*$.

Take arbitrary elements $\gamma l_1, \gamma l_2 \in \gamma L_\nu^\# = L_\tau^\#$. We get $\phi_\nu(l_1 \otimes l_2) = \eta \phi_\tau(\gamma l_1 \otimes \gamma l_2)$ and hence we have

$$\Theta_\nu = \Theta_\tau,$$

i.e. Θ_τ does not depend on the choice of involution (up to the local type).

Let now ι be an optimal involution on Λ of the same local type.

If $\pi \nmid d(\Lambda)$, then we need to show that $\Theta_\iota = \Lambda$. This is just a straightforward calculation given the description of $L_\iota^\#$ in (16).

Consider now the case $\pi \mid d(\Lambda)$. With notations as in (15) and in equation (1), we have that

$$(1,1),\ (E_1, -1-E_1),\ (\pi^{-1}E_2, -\pi^{-1}E_2),\ (\pi^{-1}E_3, -\pi^{-1}E_3)$$

is a basis of $L_\tau^\#$. A P-basis of Θ_τ is hence given by: $(1,1)$, $(\pi E_1, -\pi - \pi E_1)$, $(E_2, -E_2)$, $(E_3, -E_3)$, $(E_2 + E_3, E_3)$, $(\epsilon E_2, \epsilon E_2 + E_3)$, $(1 + E_1, 1 + E_1)$, $(\pi\epsilon - \pi - \pi E_1, -\pi\epsilon)$. Thus Θ_τ is a P-sublattice of Λ of index (π^2). We get

$$\Theta_\tau = \{(x,y) \in \Omega_F \times \Omega_F \mid \operatorname{nr}(x-y) \in (\pi)\},$$

which follows directly from the above description and equation (2). This equality is exactly (17). □

Note that Θ_τ is not an R-order if A is a skew field, but from equation (17), we immediately get

$$R\Theta_\tau = \Lambda. \tag{18}$$

4.2 Suborders and sublattices

For a primitive element $\beta \in L_\tau$, we define a ternary quadratic lattice $(L_{\tau,\beta}^\#, q_{\tau,\beta}^\#)$, where

$$L_{\tau,\beta}^\# = \{l \in L_\tau^\# \mid \operatorname{tr}(l^*\beta) = 0\}$$

and $q_{\tau,\beta}^\#$ denotes the restriction of $q_\tau^\#$ to $L_{\tau,\beta}^\#$. By restriction of ϕ_τ we get an embedding of the quaternion order $C_0(L_{\tau,\beta}^\#, q_{\tau,\beta}^\#)$ into A. The image is in fact a suborder of $A_{\tau,\beta}$.

Lemma 23. *The image of $C_0(L_{\tau,\beta}^\#, q_{\tau,\beta}^\#)$ under ϕ_τ is $\Theta_\tau \cap A_{\tau,\beta}$.*

Proof. If we take $l_1, l_2 \in L_{\tau,\beta}^\#$, then $\beta l_1^* l_2 = -l_1 \beta^* l_2 = l_1 l_2^* \beta = \tau(l_1^* l_2)\beta$, so $\phi_\tau(l_1 \otimes l_2) \in A_{\tau,\beta}$. We conclude that $C_0(L_{\tau,\beta}^\#, q_{\tau,\beta}^\#) \subseteq A_{\tau,\beta}$.

To show the inverse inclusion, take $\lambda \in \Theta_\tau \cap A_{\tau,\beta}$. It follows from the definitions of the lattices and the fact that β is a primitive element of L_τ that $L_\tau^\# = L_{\tau,\beta}^\# \oplus P\omega$ for some $\omega \in L_\tau^\#$ with $\operatorname{tr}(\omega^*\beta) = 1$. Since λ belongs to Θ_τ, it can be written in the form $\lambda = \lambda_0 + y_\tau l_1^* \omega + y_\tau^2 l_2^* l_3 l_4^* \omega$, where λ_0 lies in the image of $C_0(L^{\#}_{\tau,\beta}, q^{\#}_{\tau,\beta})$ and $l_1, \ldots, l_4 \in L^{\#}_{\tau,\beta}$. A direct calculation gives now $0 = \beta\lambda - \tau(\lambda)\beta = -\tau(y_\tau l_1^* + y_\tau^2 l_2^* l_3 l_4^*)$. Hence $\lambda = \lambda_0 + (y_\tau l_1^* + y_\tau^2 l_2^* l_3 l_4^*)\omega = \lambda_0 \in \phi_\tau(C_0(L^{\#}_{\tau,\beta}, q^{\#}_\beta))$ and we are done. □

As a consequence of this result, we can now determine the factors x_τ and y_τ occurring in the definitions of q_τ and $q^{\#}_\tau$.

Proposition 24. *We have that x_τ is a generator of the P-ideal $d_P(\Lambda)d(\Lambda_\tau)^{-1}$, and y_τ is a generator of $Dd(\Lambda_\tau)$.*

Proof. We only have to show this locally, so assume that P is local.

If $\pi \mid d(\Lambda)$, then $(x_\tau) = (1)$ and $(y_\tau) = (\pi)$ by (15). We also have $d_P(\Lambda) = d(\Lambda_\tau) = (\pi)$, so we are done.

If $\pi \mid D$, then we have by hypothesis that $d_P(\Lambda) = d(\Lambda_\tau) = (1)$. The claim now follows by the explicit description in (16).

If finally $\pi \nmid d(\Lambda)$ and $\pi \nmid D$, then we have $L^{\#}_\iota = L_\iota$, that q_ι and $q^{\#}_\iota$ are unimodular and $\Lambda \cong C_0(L^{\#}_\iota, q^{\#}_\iota)$. Furthermore, we have $L_\tau = \gamma^* L_\iota$, where $\gamma \in L_\iota$ is primitive. Hence $x_\tau \in \mathrm{nr}(\gamma)^{-1}P^*$ and $y_\tau \in \mathrm{nr}(\gamma)P^*$. By lemma 23, we have $\Lambda_{\iota,\gamma} \cong C_0(L^{\#}_{\iota,\gamma}, q^{\#}_{\iota,\gamma})$. But $\Lambda_{\iota,\gamma} = \Lambda_\tau$, so we are done if we show that $d((L^{\#}_{\iota,\gamma}, q^{\#}_{\iota,\gamma})) = (\mathrm{nr}(\gamma))$.

We have $\gamma P + L^{\#}_{\iota,\gamma} \subseteq L^{\#}_\iota$. Using the fact that γ is a primitive element of L_ι, we get $\mathrm{tr}(\gamma^* L^{\#}_\iota) = P$. On the other hand, we get $\mathrm{tr}(\gamma^*(\gamma P + L^{\#}_{\iota,\gamma})) = \mathrm{tr}(\gamma^*\gamma)P = 2\,\mathrm{nr}(\gamma)P$, and so we see that $[L^{\#}_\iota : \gamma P + L^{\#}_{\iota,\gamma}] = (2\,\mathrm{nr}(\gamma))$. Using this, we get

$$d(\gamma P + L^{\#}_{\iota,\gamma}) = (2\,\mathrm{nr}(\gamma))^2 d(L^{\#}_\iota).$$

We can also compute $d(\gamma P + L^{\#}_{\iota,\gamma})$ by noting that $\gamma P + L^{\#}_{\iota,\gamma}$ is an orthogonal sum, and hence we have

$$d(\gamma P + L^{\#}_{\iota,\gamma}) = 2\,\mathrm{nr}(\gamma) 2 d(L^{\#}_{\iota,\gamma}).$$

We conclude that $d(L^{\#}_{\iota,\gamma}) = (\mathrm{nr}(\gamma))$, since $d(L^{\#}_\iota) = (1)$. □

Lemma 25. *The discriminant of the ternary quadratic lattice $(L^{\#}_{\tau,\beta}, q^{\#}_{\tau,\beta})$ is*

$$d(q^{\#}_{\tau,\beta}) = q_\tau(\beta) d_P(\Lambda).$$

Proof. If we consider the sublattice $P\beta + L^{\#}_{\tau,\beta} \subseteq L^{\#}_\tau$ and argue as in the end of the proof of proposition 24, we get the two equalities $d(P\beta + L^{\#}_{\tau,\beta}) = (2\,\mathrm{nr}(\beta))^2 d(L^{\#}_\tau)$ and $d(P\beta + L^{\#}_{\tau,\beta}) = 2q^{\#}_\tau(\beta)2d(L^{\#}_{\tau,\beta})$. Solving for $d(L^{\#}_{\tau,\beta})$ gives

$$d(L^{\#}_{\tau,\beta}) = \frac{(2\,\mathrm{nr}(\beta))^2 d(L^{\#}_\tau)}{4q^{\#}_\tau(\beta)}.$$

It follows by (15) and (16) that $d(L^{\#}_\tau) = d_P(\Lambda)^2 D$, and by proposition 24 we have $q^{\#}_\tau(\beta)P = d(\Lambda_\tau)D\,\mathrm{nr}(\beta)$, so

$$d(L^{\#}_{\tau,\beta}) = \frac{d_P(\Lambda)^2}{d(\Lambda_\tau)}\,\mathrm{nr}(\beta) = q_\tau(\beta) d_P(\Lambda).$$ □

Proposition 26. *In the local case, the discriminant of the P-order Λ_β is* $(q_\tau(\beta)) \cap d_P(\Lambda)$.

Proof. By lemma 23 and lemma 22, we know that the image of the order $C_0(L^{\#}_{\tau,\beta}, q^{\#}_{\tau,\beta})$ is $\Lambda_{\tau,\beta} \cap \Theta_\tau$. If $\pi \nmid d(\Lambda)$, then we have by lemma 22 that $\Lambda = \Theta_\tau$, and hence $\Lambda_{\tau,\beta} \cong C_0(L^{\#}_{\tau,\beta}, q^{\#}_{\tau,\beta})$. The claim therefore follows from lemma 25 and proposition 2. If $\pi \mid d(\Lambda)$, then we know that $\Lambda_{\tau,\beta} \cong \Omega_F$. Furthermore, q is isometric to $\mathrm{nr} : \Omega_F \to P$, by (15). Hence the claim follows, since we have that $\pi^2 \nmid q_\tau(\beta)$. □

Now we turn to the global case. The form q do not necessarily exist globally if P is not a PID, but we can reformulate our result using instead the norm form. Applying proposition 24, we get that following global version of proposition 26:

Theorem 27. *In the global case, the discriminant of the P-order Λ_β is the ideal* $(\mathrm{nr}(\beta)\mathfrak{r}) \cap d_P(\Lambda)$, *where* $\mathfrak{r} = d_P(\Lambda) d(\Lambda_\tau)^{-1}$.

Example. We work out a concrete example. Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{13})$, so $P = \mathbb{Z}$ and $R = \mathbb{Z}[r]$, where $r = (1+\sqrt{13})/2$. Consider the algebra $A = K[i,j]$, where $i^2 = 2$, $j^2 = -3$ and $ij + ji = 0$, and the involution τ on A which fixes the subalgebra $F[i,j]$. Let $e_1 = i$, $e_2 = i(j-1)/2$ and $e_3 = (j+1)/2$. A maximal order Λ in A is given by $\Lambda = R + Re_2 + Re_3 + R(e_1 - re_2)/2$. The discriminant is $d(\Lambda) = \mathfrak{p}_3\overline{\mathfrak{p}}_3 = (3)$. The order $\Lambda_\tau = \mathbb{Z}[i, (1+j)/2]$ is a maximal order over $\mathbb{Z}$ with discriminant 6. It is clear that no optimal involution exists on the algebra A.

We have the following $\mathbb{Z}$-basis $\beta_0, \ldots, \beta_3$ for L:

$$2,\ r - \sqrt{13}e_3,\ \sqrt{13}e_1,\ \sqrt{13}e_2.$$

The form q on L is given by $q(\beta) = 1/2\,\mathrm{nr}(\beta)$, and we get

$$q(t_0\beta_0 + \cdots + t_3\beta_3) = 2t_0 + t_0t_1 + 5t_1^2 - 13(t_2^2 - t_2t_3 + t_3^2).$$

One checks that a given integer is primitively represented by q if and only if it is not divisible by 9 and its class modulo 13 is not a non-zero square. So, since $\left(\frac{3}{13}\right) = \left(\frac{-1}{13}\right) = 1$, there exists an optimally embedded order Λ_β with discriminant N (with $N = |q(\beta)|$ or $N = 3|q(\beta)|$) if and only if $v_3(N) = 1$ and $\left(\frac{N}{13}\right) \neq -1$. We will see in the next section that the orders Λ_β can be completely described up to genus.

5 Genera of optimally embedded orders

As an application of our results, we are now going to determine the local isomorphism classes of optimally embedded orders in Λ, i.e. determine the genera of the orders Λ_β. Since, as we have seen, the choice of special involution τ is not essential, from now on we will fix the choice of one involution τ and we will drop it from our notations. Take a primitive element $\beta \in L$ and consider the order Λ_β. Let $\mathfrak{p}$ be a prime ideal in P. We want to determine $(\Lambda_\beta)_\mathfrak{p}$.

If $\mathfrak{p} \mid d(\Lambda)$, then we already know that $(\Lambda_\beta)_\mathfrak{p} \cong \Omega_\mathfrak{p}$ by lemma 12 so nothing more needs to be done in this case.

Assume now that $\mathfrak{p} \nmid d(\Lambda)$. First we will show that there is a non-degenerate hermitian form compatible with the involution. We have $A_\mathfrak{p} \cong M_2(K_\mathfrak{p})$ by lemma 9. Consider the 2-dimensional $K_\mathfrak{p}$-module $V_\mathfrak{p} = K_\mathfrak{p} \oplus K_\mathfrak{p}$, and the $R_\mathfrak{p}$-module $M_\mathfrak{p} = R_\mathfrak{p} \oplus R_\mathfrak{p} \subset V_\mathfrak{p}$. We identify $A_\mathfrak{p}$ with $\mathrm{End}_{K_\mathfrak{p}}(V_\mathfrak{p})$, and $\Lambda_\mathfrak{p}$ with $\mathrm{End}_{R_\mathfrak{p}}(M_\mathfrak{p})$.

Lemma 28. *There exists a non-degenerate hermitian form $h : V_\mathfrak{p} \times V_\mathfrak{p} \to K_\mathfrak{p}$ such that*

$$h(av, u) = h(v, \tau(a)^* u) \text{ for all } a \in A_\mathfrak{p},\ u, v \in V_\mathfrak{p}.$$

In other words, the hermitian form h has the map $a \mapsto \tau(a)^*$ as its adjoint involution. Furthermore, h is uniquely determined up to a non-zero factor in $F_\mathfrak{p}$.

Proof. Let g be a non-degenerate hermitian form on $V_\mathfrak{p}$. Then $g(au, v) = g(u, \nu(a)^* v)$ for all $u, v \in V_\mathfrak{p}$, where ν is some involution of type 2 on $A_\mathfrak{p}$. Now, by lemma 11, there exists an invertible element $\gamma \in A_\mathfrak{p}$ such that $\nu(\gamma)^* = \gamma$ and $\tau(a) = \gamma^{-1}\nu(a)\gamma$ for all $a \in A_\mathfrak{p}$. Let $h(u, v) = g(\gamma u, v)$. We have $h(u, v) = g(\gamma u, v) = g(u, \gamma v) = \tau(g(\gamma v, u)) = \tau(h(v, u))$, so h is a hermitian form. Furthermore, we get $h(au, v) = h(u, \gamma^{-1}\nu(a)^*\gamma v) = h(u, \tau(a)^* v)$ and hence h has the required properties. The uniqueness is clear. ☐

Choose now one form h as in lemma 28. Given an element $\beta \in A$ with $\tau(\beta)^* = \beta$, we define

$$h_\beta(v, u) = h(\beta v, u),$$

for $v, u \in V_\mathfrak{p}$. It is readily verified that h_β is a hermitian form on $V_\mathfrak{p}$.

Lemma 29. *$\beta a = \tau(a)\beta$ if and only if $h_\beta(av, u) = h_\beta(v, a^* u)$ for all $u, v \in V_\mathfrak{p}$.*

Proof. $h_\beta(av, u) = h_\beta(v, a^* u)$ if and only if $h(\beta a v, u) = h(\beta v, a^* u)$ if and only if $h(\beta a v, u) = h(\tau(a)\beta v, u)$. The claim follows. ☐

We have thus shown

Proposition 30. *$(\Lambda_\beta)_\mathfrak{p}$ is isomorphic to the order constructed from the hermitian $R_\mathfrak{p}$-plane $(M_\mathfrak{p}, h_\beta)$ by (4).*

If we combine this with theorem 17, we get:

Proposition 31. *If $\mathfrak{p} \nmid d(\Lambda)$, then $(\Lambda_\beta)_\mathfrak{p}$ is $R_\mathfrak{p}$-primitive.*

We remark that the global orders Λ_β are in general not R-primitive. If $\mathfrak{p} \mid d(\Lambda)$, then it is impossible to embed $R_\mathfrak{p} \cong P_\mathfrak{p} \times P_\mathfrak{p}$ in $(\Lambda_\beta)_\mathfrak{p} \cong \Omega_{F_\mathfrak{p}}$.

If we apply proposition 5, we get the following corollary of proposition 31:

Corollary 32. *The Eichler number of the order $(\Lambda_\beta)_\mathfrak{p}$ is given by*

i) $e((\Lambda_\beta)_\mathfrak{p}) = 1$ *if $\mathfrak{p}$ is split and $\mathfrak{p} \nmid d(\Lambda)$,*

ii) $e((\Lambda_\beta)_\mathfrak{p}) = -1$ *if $\mathfrak{p}$ is unramified and $\mathfrak{p} \mid d(\Lambda_\beta)$,*

iii) $e((\Lambda_\beta)_\mathfrak{p}) = 0$ *if $\mathfrak{p}$ is ramified and $\mathfrak{p}^2 \mid d(\Lambda_\beta)$.*

Now we want to determine whether $(A_\beta)_\mathfrak{p}$ splits or not. If $\mathfrak{p}$ splits in K (and $\mathfrak{p} \nmid d(\Lambda)$), then we know from lemma 9 that $(A_\beta)_\mathfrak{p}$ splits.

Assume that $\mathfrak{p}$ is unramified in K. Then, by proposition 3, we have that $(A_\beta)_\mathfrak{p}$ splits if and only if $v_\mathfrak{p}(d(\Lambda_\beta)) = v_\mathfrak{p}(q(\beta))$ is even.

Assume that $\mathfrak{p}$ is ramified in K. According to proposition 14, we have that $(A_\beta)_\mathfrak{p}$ is a split algebra if and only if

$$-\det(h_\beta) = -\det(h)\,\mathrm{nr}(\beta)$$

defines a trivial class in $F_\mathfrak{p}^*/\,\mathrm{nr}_{K_\mathfrak{p}/F_\mathfrak{p}}(K_\mathfrak{p}^*)$. If $\beta = 1$, then $A_\beta = B$, so A_β splits since the involution τ is assumed to be special. We conclude that $-\det(h) \in \mathrm{nr}_{K_\mathfrak{p}/F_\mathfrak{p}}(K_\mathfrak{p}^*)$. We summarise:

Proposition 33. *Let $\mathfrak{p}$ be a prime. If $\mathfrak{p}$ is split in K, then $(A_\beta)_\mathfrak{p}$ is split if and only if $\mathfrak{p} \nmid d(\Lambda)$. If $\mathfrak{p}$ is unramified in K, then $(A_\beta)_\mathfrak{p}$ is split if and only if $v_\mathfrak{p}(q(\beta))$ is even. If $\mathfrak{p}$ is ramified in K, then $(A_\beta)_\mathfrak{p}$ is split if and only if $\mathrm{nr}(\beta) \in \mathrm{nr}_{K_\mathfrak{p}/\mathbb{Q}_\mathfrak{p}}(K_\mathfrak{p}^*)$.*

By theorem 8, we have now completely determined the genus of the order Λ_β.

Theorem 34. *If $\mathfrak{p}$ is split in K and $\mathfrak{p} \mid d(\Lambda)$, then $(\Lambda_\beta)_\mathfrak{p} \cong \Omega_{F_\mathfrak{p}}$. Otherwise $(\Lambda_\beta)_\mathfrak{p}$ is the unique Bass order, which allows an embedding of $R_\mathfrak{p}$, has discriminant given by theorem* 27 (*or proposition* 26) *and splitting behaviour as described in proposition* 33.

6 Spinorial kernel groups

In [7] James showed, in some situations, that the group Λ^1 maps surjectively onto the spinorial kernel group $O'(L)$ for a an explicitly given lattice L. As a second application of our previous work we now prove an extension of those results to the general setting, in particular we have no dyadic restrictions.

Consider the quadratic space (W, nr). If $\gamma \in A$ with $\mathrm{nr}(\gamma) \in F^*$, then the map ϕ_γ given by (cf. (10))

$$\phi_\gamma(w) = \tau(\gamma) w \gamma^{-1},$$

is an element of the orthogonal group $O(W, \mathrm{nr})$. The so called spinor norm of ϕ_γ is $\mathrm{nr}(\gamma)F^{*2} \in F^*/F^{*2}$. Hence we get a map

$$\Phi : A^1 \to O'(W),$$

given by $\Phi(\gamma) = \phi_\gamma$, where $O'(W)$ denotes the subgroup of the special orthogonal group of (W, nr) consisting of elements with spinor norm 1. It is known (see e.g. [7]), that the sequence

$$1 \to \{\pm 1\} \to A^1 \xrightarrow{\Phi} O'(W) \to 1 \tag{19}$$

is exact.

For a lattice L in W, we let $O'(L)$ denote the subgroup of $O'(W)$ of elements preserving L. In [7], James constructed in some cases an explicit lattice L such that the sequence (19) induces an exact sequence

$$1 \to \{\pm 1\} \to \Lambda^1 \xrightarrow{\Phi} O'(L) \to 1. \tag{20}$$

It turns out that our previously constructed lattice L always has this property.

Theorem 35. *With L defined as in* (11)*, the sequence* (20) *is exact.*

Proof. Take an element $\gamma \in A^1$ such that $\Phi(\gamma) \in O'(L)$. We need to show that $\gamma \in \Lambda$. This only has to be shown locally so we assume from now on that we are in the local case, and use the notations from section 4. It is clear that the subgroups $O'(L)$ and $O'(L^{\#})$ of $O'(W)$ are equal, so $\Phi(\gamma) \in O'(L^{\#})$, i.e. $\tau(\gamma)L^{\#}\gamma^* = L^{\#}$. But applying this to our Clifford algebra construction, we get that $\gamma\Theta\gamma^* = \Theta$, which in turn implies that $\gamma\Lambda = \Lambda\gamma$ by (18). Hence $\gamma\Lambda$ is a two-sided Λ-ideal, and we get $\gamma\Lambda = x\Lambda$ for some $x \in K$. We conclude that $x^{-1}\gamma = \epsilon$ for some $\epsilon \in \Lambda^*$. Using that $\mathrm{nr}(\gamma) = 1$ we get $x^2 = \mathrm{nr}(\epsilon^{-1}) \in R^*$, so $x \in R^*$. Hence we get $\gamma \in \Lambda^*$, and we are done. $\square$

References

[1] J. Brzezinski, *On orders in quaternion algebras,* Communications in algebra, 11(5), 501–522 (1983)

[2] J. Brzezinski, *On automorphisms of quaternion orders,* J. Reine Angew. Math. 403, 166–186 (1990)

[3] J. Brzezinski, *On embedding numbers into quaternion orders,* Comment. Math. Helvetici 66, 302–318 (1991)

[4] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren,* J. Reine Angew. Math. 195, 127–151 (1955)

[5] H. Granath, *On Quaternionic Shimura Surfaces,* Thesis, 2002 (available at http://www.math.chalmers.se/Math/Research/Preprints/)

[6] R. Jacobowitz, *Hermitian Forms over Local Fields,* Amer. J. Math. 84, p. 441–465 (1962)

[7] D. G. James, *Quaternion Algebras, Arithmetic Kleinian Groups and $\mathbb{Z}$-lattices,* Pacific J. Math, Vol. 203, (2002) no. 2, p. 395–412

[8] M. Peters, *Ternäre und quaternäre quadratische Formen und Quaternionenalgebren,* Acta Arithmetica 15, p. 329–365 (1969)

[9] I. Reiner, *Maximal Orders,* Academic Press, 1975

[10] W. Scharlau, *Quadratic and Hermitian Forms,* Springer-Verlag, 1985

[11] G. Shimura, *Euler Products and Eisenstein Series,* American Mathematical Society, 1997

[12] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions,* Springer-Verlag, 1980

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, Germany
granath@mpim-bonn.mpg.de