Journal of Algebra 423 (2015) 812–852

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On lattices over valuation rings of arbitrary rank ☆

Shaul Zemel

Fachbereich Mathematik, AG 5, Technische Universität Darmstadt, Schlossgartenstrasse 7, D-64289, Darmstadt, Germany

ARTICLE INFO

Article history:
Received 24 September 2013
Available online xxxx
Communicated by Eva Bayer-Fluckiger

Keywords:
Lattices
Bilinear forms
Valuation rings

ABSTRACT

We show how several results about p-adic lattices generalize easily to lattices over valuation ring of arbitrary rank having only the Henselian property for quadratic polynomials. If 2 is invertible we obtain the uniqueness of the Jordan decomposition and the Witt Cancellation Theorem. We show that the isomorphism classes of indecomposable rank 2 lattices over such a ring in which 2 is not invertible are characterized by two invariants, provided that the lattices contain a primitive norm divisible by 2 of maximal valuation.

Introduction

A well-known result states that for any odd prime p, the isomorphism classes of p-adic lattices correspond to the possible symbols of the form $\prod_{e=0}^{N}(p^e)^{\varepsilon_e n_e}$, where $\varepsilon_e \in \{\pm 1\}$ and $n_e \in \mathbb{N}$ for every e. Moreover, the Witt Cancellation Theorem holds for p-adic lattices, as is shown in [7]. The same assertions hold for lattices over the ring of integers $\mathcal{O}$ in a finite field extension of $\mathbb{Q}_p$. In all references known to the author (e.g., [7,9,4,13],

☆ This work was supported by the Minerva Fellowship (Max-Planck-Gesellschaft).
E-mail address: zemel@mathematik.tu-darmstadt.de.

http://dx.doi.org/10.1016/j.jalgebra.2014.10.022
0021-8693/

etc.) the proof is based on the p-adic valuation being *discrete*, or at least of rank 1 (see [5]). Recall that a valuation has rank 1 if the value group can be embedded in $(\mathbb{R}, +)$ as an ordered group. The first aim of this paper is to generalize these assertions to lattices over any 2-Henselian valuation ring with a finite residue field whose characteristic is not 2. Indeed, a very simple variation of the short argument appearing in Section 4 of Chapter 1 of [12] suffices to prove this result (see also Section 3 in Chapter 8 of [4] for the case of lattices over the ring $\mathbb{Z}_p$ of p-adic numbers).

We remark that several texts deal with non-unimodular lattices (also in the Hermitian setting) under various degrees of generality (see, e.g., [2] or [3]). However, these references use abstract tools such as quadratic forms over Hermitian categories. The book [11] also deals with related topics, but mostly in the quadratic setting, while we do not assume that our bilinear form comes from a quadratic form (in the sense of [1] in characteristic 2—see more details in Section 4). The book [10] considers bilinear forms over valuation rings, but treats them up to isomorphism over the quotient field rather than just over the valuation ring itself. It seems that our results are independent of the results appearing in [11] and [10]. In any case our proofs are very concrete and simple, and show how the desired assertions can be obtained solely from 2-Henselianity.

Next we consider unimodular rank 2 lattices, which contain the only non-trivial indecomposable lattices over valuation rings (up to multiplying the bilinear form by a scalar). We focus on the residue characteristic 2 case, where indeed such indecomposable lattices exist. We define an invariant for isomorphism classes of these lattices, which in some sense generalizes the Arf invariant defined in [1]. We then show how two invariants characterize the isomorphism classes of such lattices, in case they contain a primitive element whose norm is divisible by 2. We conclude by giving some relations between different Jordan decompositions (in residue characteristic 2) which yield isomorphic lattices, taking a Jordan decomposition of a lattice to a “more canonical” one.

In Section 1 we prove the existence of Jordan decompositions over any valuation ring, and show that an approximated isomorphism between lattices over a 2-Henselian valuation ring is a twist of a true isomorphism. Section 2 proves the “uniqueness of the symbol” result. In Section 3 we present the conventions for unimodular rank 2 lattices, with their *generalized Arf invariants*. Section 4 considers isomorphisms between unimodular rank 2 lattices containing a primitive vector of norm divisible by 2, and shows that the *fine Arf invariant* and the *class of minimal norms* characterize the isomorphism class of such lattices. Finally, in Section 5 we define when one Jordan decomposition in residue characteristic 2 is “more canonical” than another Jordan decomposition, and present certain transformations of Jordan decompositions which makes them “more canonical”.

I am thankful to U. First for reading this manuscript and providing several enlightening insights. Many thanks are due to the anonymous referee, whose suggestions have helped to greatly improve many aspects of this paper, as well as the clarity of several arguments.

1. Jordan decompositions

Let R be a commutative ring, and let M be a finite rank free R-module with a symmetric bilinear form. We denote the bilinear form by $(\cdot,\cdot) : M \times M \to R$, and for $x \in M$ we write x^2 for (x, x) (this element of R is called the *norm* of x). The bilinear form maps M to the dual module $M^* = Hom_R(M, R)$, and we call the bilinear form *non-degenerate* if this map $M \to M^*$ is injective. In this case we call M an *R-lattice*. Note that our non-degeneracy condition is weaker than the inner product condition considered in [12], where the map $M \to M^*$ is required to be bijective. In case this map is bijective we call the lattice M *unimodular*. We consider only the case where R is an integral domain, so we assume this from now on. In this case we can extend scalars to the field of fractions $\mathbb{K}$ of R, and obtain a $\mathbb{K}$-lattice, or equivalently an inner product space over $\mathbb{K}$. Then non-degeneracy is equivalent to requiring a non-zero determinant for the Gram matrix of the bilinear form using any basis for M.

Some authors (e.g., [12]) assume that a module underlying lattice is projective (and not necessarily free). However, our main interest here is the case where R is a valuation ring, hence a local ring, where these two conditions are equivalent.

Elements x and y of a lattice M are called *orthogonal* and denoted $x \perp y$ if $(x, y) = 0$. For a submodule N of M we denote $N^\perp$ its *orthogonal complement*, the submodule of M consisting of those $x \in M$ such that $x \perp y$ for all $y \in N$. Our non-degeneracy condition is equivalent to the assertion that $M^\perp = \{0\}$. A direct sum of lattices is *orthogonal* if every two elements from different lattices are orthogonal. Then an orthogonal direct sum of bilinear form modules is a lattice (i.e., non-degenerate) if and only if all the summands are lattices. Two lattices M and N are called *isomorphic*, denoted $M \cong N$, if there exists an R-module isomorphism between them which preserves the bilinear form. A non-degenerate lattice M has an orthogonal basis if and only if it is isomorphic to a direct sum of rank 1 lattices. For a lattice M and an element $0 \neq a \in R$, we denote $M(a)$ the lattice obtained from M by multiplying the bilinear form by a. This lattice is non-degenerate if and only if M has this property, and a basis for the module M is orthogonal for the lattice M if and only if it is orthogonal for $M(a)$.

We denote the group of invertible elements in the ring R by R^*, and the multiplicative group of $\mathbb{K}$ by $\mathbb{K}^*$. The determinant of a Gram matrix of a basis of M is independent of the choice of basis up to elements of $(R^*)^2$. Hence a statement of the form "the determinant of the bilinear form on M divides an element of R" is well-defined. We note that M is unimodular (hence non-degenerate in the sense of [12]) if and only if its determinant is in R^*.

An element x of a lattice M is called *primitive* if the module M/Rx is torsion-free. This condition is equivalent to x being an element of some basis of M, and it is preserved under multiplication from R^*. Note that this notion depends only on the structure of M as an R-module, and not on the bilinear form on M.

We call an R-lattice M *uni-valued* if it can be written as $L(\sigma)$ with L unimodular and $\sigma \in R$. This notion (at least over valuation rings) is closely related to the notion of

$\mathfrak{a}$-unimodularity considered, for example, in [13]. A *Jordan decomposition* of a lattice M is a presentation of M as $\bigoplus_{k=1}^{t} M_k$ with M_k uni-valued, such that if $M_k = L_k(\sigma_k)$ with L_k unimodular then $v(\sigma_k) \neq v(\sigma_l)$ wherever $k \neq l$. Note that if M and N are uni-valued with the same σ then so is $M \oplus N$. Hence the condition about the σ_k having different valuations can be easily achieved by successive combination of two uni-valued lattices with the same $v(\sigma)$ into one.

We now prove the existence of Jordan decompositions for lattices over arbitrary valuation rings. We follow closely the arguments in Chapter 1 of [12] (where bilinear forms over fields are considered) and [7] or Chapter 8 of [4] (which considers the p-adic numbers).

Let N be a (free) submodule of M which is non-degenerate of rank r. First we prove a simplified version of Lemma 1 of [7]:

Lemma 1.1. *Let e_i, $1 \leq i \leq r$ be a basis for N, and let $A \in M_r(R)$ be the matrix whose ij-entry is (e_i, e_j). For any $x \in M$ and $1 \leq i \leq r$, denote by $A_{i,x}$ the matrix whose ij-entry (with the same i) is (x, e_j) and all the other entries coincide with those of A. If* $\det A$ *divides* $\det A_{i,x}$ *in R for any i and x then M decomposes as $N \oplus N^{\perp}$ (as lattices).*

Proof. Since N is non-degenerate, we have $N \cap N^{\perp} = \{0\}$, hence $N \oplus N^{\perp}$ is a sub-lattice of M. We need to show equality. Given $x \in M$, we claim that there exists some $y = \sum_{i=1}^{r} a_i e_i \in N$ (with $a_i \in R$) such that $(x, e_j) = (y, e_j)$ for any $1 \leq j \leq r$. Indeed, these equalities (one for each $1 \leq j \leq r$) yield a system of linear equations for the coefficients a_i, which we can solve over $\mathbb{K}$ since the corresponding matrix is A (hence of non-zero determinant). But the solution is given using Cramer's formula, i.e., $a_i = \frac{\det A_{i,x}}{\det A} \in \mathbb{K}$, and our assumptions imply that these coefficients are in R. Now, since $y \in N$ and our assumption on y implies $x - y \in N^{\perp}$, we obtain that $x = y + (x - y) \in N \oplus N^{\perp}$, as desired. This proves the lemma. $\square$

Assume now that R is a *valuation ring*. This means that there is a totally ordered (additive) group Γ (the *value group*) and a surjective homomorphism $v : \mathbb{K}^* \to \Gamma$ (called the *valuation*) satisfying $v(x + y) \geq \min\{v(x), v(y)\}$ for every x and y in $\mathbb{K}$. Here and throughout, we extend v to a function on $\mathbb{K}$ by setting $v(0) = \infty$ and considering it larger than any element of Γ. The statement that R is the valuation ring of v means that R consists precisely of those elements $x \in \mathbb{K}$ such that $v(x) \geq 0$ (with 0 here is the trivial element of Γ). For any $\gamma \in \Gamma$ we define $I_\gamma = \{x \in \mathbb{K}^* \mid v(x) > \gamma\}$. It is a (proper) ideal in R if $\gamma \geq 0$. In particular, I_0 is the unique maximal ideal of R. We remark that an ideal of the sort $\{x \in \mathbb{K}^* \mid v(x) \geq \gamma\}$ is just the principal (perhaps fractional, if $\gamma < 0$) ideal σR with $v(\sigma) = \gamma$, hence requires no further notation.

In many references (e.g., [5]), the ordered group Γ is considered as a subgroup of the additive group of $\mathbb{R}$. Such valuations are called *of rank 1*. In particular, the *discrete* valuations, in which $\Gamma \cong \mathbb{Z}$ (covering the case of the p-adic numbers and their finite extensions) have rank 1. However, we pose no restrictions on v or Γ in this paper, hence the rank is arbitrary.

For any R-lattice M we define the *valuation of* M, denoted $v(M)$, to be $\min\{v(x, y) \mid x, y \in M\}$, where we use the shorthand $v(x, y)$ for $v((x, y))$. This value equals $\min_{i,j} v(e_i, e_j)$ wherever e_i, $1 \leq i \leq r$ is a basis for R, since (x, y) lies in the R-module generated by these elements for any x and y in R. In particular $v(M)$ is well-defined. If M is uni-valued, then by writing $M = L(\sigma)$ with L unimodular we have $v(M) = v(\sigma)$. In a Jordan decomposition $\bigoplus_{k=1}^{t} M_k$ of a lattice M the condition on the elements $\sigma_k \in R$ distinguishing the uni-valued components from being unimodular reduces to the assertion that these components have different valuations. We can thus assume, by changing the order if necessary, that $v(M_k) < v(M_{k+1})$ for every $1 \leq k < t$. Using these definitions, Lemma 1.1 yields

Proposition 1.2. *Any lattice M over a valuation ring R admits a Jordan decomposition.*

Proof. We apply induction on the rank of M. For rank 1 lattices the assertion is trivial. Let $v = v(M)$. Assume first that there is an element $x \in M$ such that $v(x^2) = v$. Then $N = Rx$ satisfies the condition of Lemma 1.1, so that we can write $M = N \oplus N^{\perp}$. On the other hand, if no such x exists, then we take x and y in M such that $v(x, y) = v$, and our assumption implies $v(x^2) > v$ and $v(y^2) > v$. We claim that x and y are linearly independent over R. Indeed, the equality $ax + by = 0$ implies $ax^2 + b(x, y) = 0$ and $a(x, y) + by^2 = 0$, hence $a \in bI_0$ and $b \in aI_0$, which is possible only if $a = b = 0$. Moreover, $N = Rx \oplus Ry$ satisfies the condition of Lemma 1.1. Indeed, the valuation of the determinant is $2v$, while the valuation of any other 2×2 determinant with entries in the image of the bilinear form has valuation at least $2v$. Thus also here $M = N \oplus N^{\perp}$. It remains to verify that in both cases N is uni-valued. To see this, observe that any rank 1 lattice is uni-valued, and in the second case dividing the bilinear form on N by (x, y) gives a unimodular lattice. The induction hypothesis allows us to decompose $N^{\perp}$ into uni-valued lattices, and adding N to the component of valuation v in $N^{\perp}$ (if it exists) completes the proof of the proposition. $\square$

The decomposition of Proposition 1.2 is called a *Jordan splitting* in [13]. From the proof of Proposition 1.2 we deduce

Corollary 1.3. *If $2 \in R^*$ then the components M_k have orthogonal bases. If $2 \notin R^*$ then either M_k has an orthogonal basis or it admits an orthogonal decomposition into lattices of rank 2 each having a basis $\{x, y\}$ such that $v(x^2)$ and $v(y^2)$ are both strictly larger than $v(x, y)$.*

Proof. First we show that if $2 \in R^*$ then there exists an element $x \in M$ with $v(x^2) = v(M)$. Indeed, if $v(x, y) = v$ and $v(2) = 0$ while $v(x^2) > v$ and $v(y^2) > v$ then $(x + y)^2 = x^2 + y^2 + 2(x, y)$ has valuation v. In view of the proof of Proposition 1.2, this proves the corollary in this case. Assume now $2 \notin R^*$. The proof of Proposition 1.2 shows that M_k can be written as an orthogonal direct sum of rank 1 lattices and rank 2 lattices of the sort described above. It remains to show that if a lattice of rank 1 appears in M_k then M_k has an orthogonal basis. It suffices (by induction) to prove that if N is the direct sum of one rank 1 lattice and one rank 2 lattice of this form having the same valuation then N has an orthogonal basis. Let now $N = Rx \oplus Ry \oplus Rz$ be a lattice in which $x \perp z$, $y \perp z$, and (x, y) and z^2 have common (finite) valuation v while $v(x^2) > v$ and $v(y^2) > v$. One checks directly that the three elements $tx + z$, $(z^2)y - t(x, y)z$, and $(y^2z^2 + t^2(x, y)^2)x - (x, y)(t^2x^2 + z^2)y - t(x^2y^2 - (x, y)^2)z$ form an orthogonal basis for N for any $t \in R^*$. This proves the corollary. □

Recall that a valuation ring R is called *Henselian* if Hensel's Lemma holds in R, namely if given three monic polynomials f, g_0, and h_0 in the polynomial ring $R[x]$ such that $f - g_0h_0$ lies in $I_0[X]$ (i.e., all the coefficients of that difference have positive valuation) and the resultant of g_0 and h_0 is in R^* then there exist monic polynomials g and h in $R[x]$ such that $f = gh$ and $g - g_0$ and $h - h_0$ are in $I_0[X]$. In particular, taking g to be of degree 1 renders this statement equivalent to the assertion that if $a \in R$ and monic $f \in R[x]$ satisfy $v(f(a)) > 0$ and $v(f'(a)) = 0$ then f has a root $b \in R$ with $b - a \in I_0$. We call a valuation ring R *2-Henselian* if the last assertion holds for any polynomial f of degree 2, and if $2 \neq 0$ in R. We note that a more general assertion holds in a Henselian ring, stating that for $f \in R[x]$ (not necessarily monic!) and an element $a \in R$ such that $v(f(a)) > 2v(f'(a))$ there exists a root b of f with $b - a \in I_{v(f'(a))}$. Indeed, following the proof of the equivalence of (e) and (f) in Theorem 18.1.2 of [6], we use the Taylor expansion to write $f(a - \frac{f(a)}{f'(a)}y)$ as $f(a)(1 - y + \frac{f(a)}{f'(a)^2}y^2g(y))$ for some polynomial g, and we present this expression as $f(a)y^dh(\frac{1}{y})$ where d is the degree of f and $h(x)$ has the form $x^d - x^{d-1} + \sum_{i=0}^{d-2} c_ix^i$ with $c_i \in I_0$. Since $v(h(1)) > 0$ and $v(h'(1)) = 0$ there exists a root $\lambda \in 1 + I_0 \subseteq R^*$ of h, so that the required root of f is $b = a - \frac{f(a)}{f'(a)} \cdot \frac{1}{\lambda}$. Since $\lambda \in R^*$ we know that $v(b-a) = v(\frac{f(a)}{f'(a)})$. In a 2-Henselian valuation ring this more general condition holds for any $f \in R[x]$ of degree 2. As Theorem 7 in Chapter 2 of [14] shows that every complete valuation ring is Henselian (and in particular 2-Henselian), our results hold for a variety of interesting valuation rings.

The following property of 2-Henselian rings will be used below.

Lemma 1.4. *An element of R of the form $1+y$ with $v(y) > 2v(2)$ lies in $(R^*)^2$, and has a unique square root $1 + z$ such that $v(z) > v(2)$. Moreover, the equality $v(y) = v(z)+v(2)$ holds in this case. Let A, B, and C be three elements of $\mathbb{K}$ such that $v(AC) > 2v(B)$ (hence $B \neq 0$). Then the equation $At^2+Bt+C = 0$ has one solution in $\mathbb{K}$ with valuation $v(\frac{C}{B})$ (so that this solution is in R if $v(C) \geq v(B)$). If $A \neq 0$ then the other solution has valuation $v(\frac{B}{A})$, which is strictly smaller.*

Proof. Consider the polynomial $f(t) = t^2 - 1 - y$ and the approximate root 1. The 2-Henselianity of R yields a root of this polynomial, which we write as $1 + z$, such that $z \in I_{v(2)}$ since $f'(1) = 2$. We also have $v(z) = v(\frac{f(1)}{f'(1)}) = v(y) - v(2)$. The second square root of $1 + y$ is $-1 - z$, and by subtracting 1 we obtain the element $-2 - z$ of R, which has valuation precisely $v(2)$ since $v(z) > v(2)$. Next, the equation $At^2 + Bt + C = 0$ has only one solution $t = -\frac{C}{B}$ if $A = 0$, and otherwise its two solutions are given by $\frac{-B\pm\sqrt{B^2-4AC}}{2A}$ (in an appropriate extension of $\mathbb{K}$ if necessary). Now, $B^2-4AC = B^2(1+y)$ for $y = -\frac{4AC}{B^2}$, and the inequality $v(y) > 2v(2)$ allows us to write $\sqrt{B^2 - 4AC}$ as $B(1+z)$ with $z \in R$ such that $v(z) = v(y) - v(2) = v(\frac{2AC}{B^2})$. The two solutions $\frac{B}{2A}(-1 \pm (1 + z))$ of the equation lie in $\mathbb{K}$. The solution with + is $\frac{Bz}{2A}$ and has the required valuation $v(\frac{C}{B})$ (like in the case $A = 0$), and the other solution has valuation $v(\frac{B}{A})$ since $v(2 - z) = v(2)$. As $v(AC) > v(B^2)$ implies $v(\frac{C}{B}) > v(\frac{B}{A})$, this proves the lemma. □

Note that the condition $2 \neq 0$ was implicitly used in Lemma 1.4, in assumptions in which some elements have valuations strictly larger than $v(2)$, as well as dividing by 2 in $\mathbb{K}$. All the assertions of Lemma 1.4 collapse if $2 = 0$ in R.

Our first result states that the existence of an approximate isomorphism between lattices over 2-Henselian valuation rings implies that the lattices are indeed isomorphic. See Theorem 2 of [5] for the special case of complete valuation rings of rank 1, and Corollary 36a of [9] or Lemma 5.1 of [4] for the case $R = \mathbb{Z}_p$.

Theorem 1.5. *Let M and N be R-lattices. Decompose M as in Proposition 1.2, and assume that M and N are isomorphic when we reduce modulo $I_{v(M_t)+2v(2)}$. Then $M \cong N$ as R-lattices.*

Proof. Denote $I_{v(M_t)+2v(2)}$ by I. An isomorphism over R/I can be lifted to an R-module homomorphism $\varphi : M \to N$ (since M is a free module). Moreover, φ must be bijective: Observe that M and N must have the same rank, and by choosing bases for both modules the determinant of φ is a unit modulo I hence lies in R^*. φ preserves the bilinear form up to I, and we now show how to alter φ to a lattice isomorphism from M to N. We apply induction on the (common) rank of M and N.

Assume first that M_1 has an orthogonal basis, and let x be an element of the basis of M_1. Then $v(x^2)$ is minimal in M, and the fact that $x^2 \notin I$ implies the equality $v(\varphi(x)^2) = v(x^2)$. This valuation is also minimal in N. Moreover, the inequality $v(\frac{x^2}{\varphi(x)^2} - 1) > 2v(2)$ holds, so that by Lemma 1.4 there is $c \in R^*$ with $v(c-1) > v(2)$ such that $c^2 = \frac{x^2}{\varphi(x)^2}$. Lemma 1.1 implies that $M = Rx \oplus (Rx)^\perp$, and we define $\psi : M \to N$ by taking x to $c\varphi(x)$ and $u \in (Rx)^\perp$ to $\varphi(u) - \frac{(\varphi(u),\varphi(x))}{\varphi(x)^2}\varphi(x)$. Since $(\varphi(u), \varphi(x)) \in I$ (as $(u, x) = 0$), we have $\frac{(\varphi(u),\varphi(x))}{\varphi(x)^2} \in I_{2v(2)} \subseteq R$. Now, $\psi(x)^2 = x^2$, and if $u \perp x$ then we have $\psi(u) \perp \psi(x)$. If $w \in M$ is another vector such that $w \perp x$ as well, then we have

$$(\psi(u), \psi(w)) = (\varphi(u), \varphi(w)) - \frac{(\varphi(u), \varphi(x))(\varphi(w), \varphi(x))}{\varphi(x)^2}.$$

The congruence $(\varphi(u), \varphi(w)) \equiv (u, w)(\mathrm{mod}\ I)$ and the relations $\frac{(\varphi(u),\varphi(x))}{\varphi(x)^2} \in R$ and $(\varphi(w), \varphi(x)) \in I$ now imply $(\psi(u), \psi(w)) \equiv (u, w)(\mathrm{mod}\ I)$ for any u and w in $(Rx)^\perp$.

On the other hand, if M_1 has no orthogonal basis, then we take some x and y in M_1 such that $v(x,y)$ is minimal in M, and then $v(\varphi(x),\varphi(y)) = v(x,y)$ is minimal in N. Moreover, $v(\varphi(x)^2)$ and $v(\varphi(y)^2)$ are both larger than $v(x,y)$. We need to modify $\varphi(x)$ and $\varphi(y)$ in order to obtain elements spanning a rank 2 sublattice of N which is isomorphic to $Rx \oplus Ry$. We claim that there exist elements s and t in $I_{v(2)}$ and $c \equiv 1 (\mathrm{mod}\ I_{v(2)})$ such that

$$\big(c\varphi(x) + cs\varphi(y)\big)^2 = x^2, \qquad \big(\varphi(y) + t\varphi(x)\big)^2 = y^2,$$

and

$$\big(c\varphi(x) + cs\varphi(y), \varphi(y) + t\varphi(x)\big) = (x,y).$$

First we apply Lemma 1.4 with the numbers $A = \varphi(x)^2$, $B = 2(\varphi(x),\varphi(y))$, and $C = \varphi(y)^2 - y^2 \in I$ (these numbers satisfy the assumptions of that lemma). The corresponding solution t, of valuation $v(\frac{C}{B}) > v(2)$, satisfies $(\varphi(y) + t\varphi(x))^2 = y^2$ as required.

Further, denote $x^2y^2 - (x,y)^2$ by Δ and $\varphi(x)^2\varphi(y)^2 - (\varphi(x),\varphi(y))^2$ by Δ_φ, so that $v(\Delta) = v(\Delta_\varphi) = 2v(x,y)$ (see Corollary 1.3). Observe that

$$\big(\varphi(x),\varphi(y)\big)^2 - (x,y)^2 = \big(\big(\varphi(x),\varphi(y)\big) - (x,y)\big)\big(\big(\varphi(x),\varphi(y)\big) + (x,y)\big)$$

and

$$\varphi(x)^2\varphi(y)^2 - x^2y^2 = \varphi(x)^2\big(\varphi(y)^2 - y^2\big) + y^2\big(\varphi(x)^2 - x^2\big)$$

are elements of $(x,y)I$, so that $\Delta_\varphi - \Delta$ lies in the same ideal and $x^2(\frac{\Delta_\varphi}{\Delta} - 1) \in I$. Hence $C = \varphi(x)^2 - x^2\frac{\Delta_\varphi}{\Delta} \in I$, while $B = 2(\varphi(x),\varphi(y)) + 2tx^2\frac{\Delta_\varphi}{\Delta}$ has valuation $v(x,y) + v(2)$ and $A = \varphi(y)^2 - t^2x^2\frac{\Delta_\varphi}{\Delta}$ has valuation $v(x^2) \geq v(x,y)$. Thus, we can use Lemma 1.4 again and obtain a solution s, of valuation $v(\frac{C}{B}) > v(2)$, to $As^2 + Bs + C = 0$. Furthermore, since s and t are in $I_{v(2)}$, the number $\frac{(1+st)(\varphi(x),\varphi(y)) + s\varphi(y)^2 + t\varphi(x)^2}{(x,y)}$ is congruent to 1 modulo $I_{v(2)}$ (hence lies in R^*). We denote by c the inverse of this number, hence $v(c-1) > v(2)$ as well. The two elements $c\varphi(x) + cs\varphi(y)$ and $\varphi(y) + t\varphi(x)$ span $R\varphi(x) \oplus R\varphi(y)$ since the determinant $c(1 - st)$ of the transition matrix is in R^*, and the choice of c implies $(c\varphi(x) + cs\varphi(y), \varphi(y) + t\varphi(x)) = (x,y)$.

In order to evaluate $(c\varphi(x) + cs\varphi(y))^2$ we write the square of the denominator of c as

$$\begin{aligned}
&\big[s^2\big(\varphi(x),\varphi(y)\big)^2 + 2s\varphi(x)^2\big(\varphi(x),\varphi(y)\big) + \big(\varphi(x)^2\big)^2\big]t^2 \\
&\quad + 2\big[s^2\varphi(y)^2\big(\varphi(x),\varphi(y)\big) + s\varphi(x)^2\varphi(y)^2 + s\big(\varphi(x),\varphi(y)\big)^2 + \varphi(x)^2\big(\varphi(x),\varphi(y)\big)\big]t \\
&\quad + \big[s^2\big(\varphi(y)^2\big)^2 + 2s\varphi(y)^2\big(\varphi(x),\varphi(y)\big) + \big(\varphi(x),\varphi(y)\big)^2\big].
\end{aligned}$$

Substituting the quadratic equation for t in each of the coefficients of s^2, s, and 1 takes the latter expression to the form

$$\left[y^2\varphi(y)^2 - \Delta_\varphi t^2\right]s^2 + 2\left[y^2\left(\varphi(x), \varphi(y)\right) + \Delta_\varphi t\right]s + \left[y^2\varphi(x)^2 - \Delta_\varphi\right].$$

Multiplying $(c\varphi(x) + cs\varphi(y))^2 - x^2$ by the latter expression yields (recall the numerator (x, y) of c)

$$\begin{aligned}&\left[(x,y)^2\varphi(y)^2 - x^2y^2\varphi(y)^2 + x^2\Delta_\varphi t^2\right]s^2\\ &\quad + 2\left[(x,y)^2\left(\varphi(x), \varphi(y)\right) - x^2y^2\left(\varphi(x), \varphi(y)\right) - x^2\Delta_\varphi t\right]s\\ &\quad + \left[(x,y)^2\varphi(x)^2 - x^2y^2\varphi(x)^2 + x^2\Delta_\varphi\right].\end{aligned}$$

The coefficients of s^2, s, and 1 are $t^2x^2\Delta_\varphi - \varphi(y)^2\Delta$, $-2tx^2\Delta_\varphi - 2(\varphi(x), \varphi(y))\Delta$, and $x^2\Delta_\varphi - \varphi(x)^2\Delta$ respectively, so the quadratic equation for s shows that the latter expression vanishes. This shows that $(c\varphi(x) + cs\varphi(y))^2 = x^2$ as desired.

Let $u \in (Rx \oplus Ry)^\perp$ be given. As in the proof of Lemma 1.1, we can find, using Cramer's rule, the coefficients of $\varphi(x)$ and $\varphi(y)$ which should be subtracted from $\varphi(u)$ in order to obtain a vector perpendicular to $\varphi(x)$ and $\varphi(y)$. These coefficients are of the form $\frac{\det A_{i,u}}{\Delta}$, hence lie in R, and in fact in $I_{2v(2)}$. We define a map $\psi : M \to N$ by sending x to $c\varphi(x) + cs\varphi(y)$, y to $\varphi(y) + t\varphi(x)$, and $u \in (Rx \oplus Ry)^\perp$ to $\varphi(u)$ modified by the appropriate multiples of $\varphi(x)$ and $\varphi(y)$. The map ψ is an isomorphism of $Rx \oplus Ry$ onto its image $R\varphi(x) \oplus R\varphi(y)$ and it takes $(Rx \oplus Ry)^\perp$ onto the orthogonal complement of the latter space. In addition, $(\psi(u), \psi(w)) \equiv (u, w) (\mathrm{mod}\ I)$ for every u and w in $(Rx \oplus Ry)^\perp$ by arguments similar to the previous case, using the orthogonality of $\psi(u)$ and $\psi(w)$ to $\varphi(x)$ and to $\varphi(y)$.

In both cases M decomposes as $K \oplus K^\perp$ and we have altered φ to a map ψ which is an isomorphism on K and preserves the orthogonality between K and $K^\perp$. Since the restriction of ψ to $K^\perp$ (denoted $\psi|_{K^\perp}$) becomes an isomorphism when reducing modulo I, the induction hypothesis allows us to alter $\psi|_{K^\perp}$ to an isomorphism $\eta : K^\perp \to \psi(K^\perp)$. The map which takes $x \in K$ to $\psi(x)$ and $u \in K^\perp$ to $\eta(u)$ is the desired isomorphism from M to N. $\square$

We note that in each induction step in Theorem 1.5 the element $c - 1$ of R, as well as s and t in the second case, lie in $I_{v(2)}$. Moreover, the coefficients we use when changing the map on the orthogonal complement in each step lie in $I_{2v(2)}$. This proves the stronger statement, that reducing any "isomorphism-up-to-I" modulo the (larger) ideal $I_{v(2)}$ yields the image (modulo $I_{v(2)}$) of a true isomorphism from M to N.

2. Uniqueness of the decomposition if $2 \in R^*$

We recall that for odd p there are two isomorphism classes of unimodular p-adic lattices of rank n, and the isomorphism classes correspond to the possible values of the Legendre symbol of the discriminant of the lattice over the prime p (see, for example, Section 3 of [17]). Then the decomposition of a general p-adic lattice as described in Section 1 allows us to define the *symbol* of the p-adic lattice, which is an expression of the form $\prod_{k=0}^{m}(p^k)^{\varepsilon_k n_k}$ with $n_k \in \mathbb{N}$ being the rank of the uni-valued component of valuation k and $\varepsilon_k \in \{\pm 1\}$ is the appropriate Legendre symbol. Moreover, the possible symbols are in one-to-one correspondence with isomorphism classes of p-adic lattices. We now use a simple argument to show that a similar assertion holds over any 2-Henselian valuation ring (of arbitrary rank) with a finite residue field in which 2 is invertible.

Following Section 4 of [12], we define, for a decomposition of M as an orthogonal direct sum $K \oplus L$, the *reflection* corresponding to this decomposition to be the map $r : M \to M$ which takes $x \in K$ to x and $y \in L$ to $-y$. This map is an involution, which preserves the bilinear form on M. First we prove

Lemma 2.1. *Let R be a valuation ring in which $2 \in R^*$, let M be an R-lattice, and let x and y be elements in M having the same norm. Let v be the valuation of this common norm, and assume further that the norm of any $z \in M$ is at least v. Then there is a reflection on M taking x to y.*

Proof. Write $x = u+w$ and $y = u-w$ for $u = \frac{x+y}{2}$ and $w = \frac{x-y}{2}$. The norm equality $x^2 = y^2$ implies $u \perp w$, hence this common norm equals u^2+w^2. Under our assumption on v we have $v(u^2) \geq v$, $v(w^2) \geq v$, and $v(u^2+w^2) = v$, whence at least one of the two inequalities is an equality. Since $2 \in R^*$, the proof of Corollary 1.3 shows that the 1-dimensional sublattice generated by the corresponding element (u or w) satisfies the conditions of Lemma 1.2, giving a decomposition of M. Observing again that $u \perp w$, we find that if $v(u^2) = v$ then the reflection with respect to the decomposition $M = Ru \oplus (Ru)^{\perp}$ gives the desired outcome, while if $v(w^2) = v$ we can use the one corresponding to the decomposition $M = (Rw)^{\perp} \oplus Rw$. This proves the lemma. □

As an application of Lemma 2.1 we deduce

Corollary 2.2. *Every automorphism of a rank n lattice M over a valuation ring R such that $2 \in R^*$ is the composition of at most n reflections.*

Proof. We apply induction on n, the case $n = 1$ being trivial (since $Aut(M)$ is just $\{\pm 1\}$ in this case). Corollary 1.3 yields an orthogonal basis for M, and let x be an element of this basis whose norm has minimal valuation. Given an automorphism f of M, the elements x and $f(x)$ of M satisfy the conditions of Lemma 2.1, hence there exists a reflection r on M taking $f(x)$ to x. Lemma 1.1 implies $M = Rx \oplus (Rx)^{\perp}$, and the composition $r \circ f$ fixes x, hence restricts to an automorphism of $(Rx)^{\perp}$. By the induction hypothesis, the latter automorphism is a composition of at most $n-1$ reflections on $(Rx)^{\perp}$, and by extending each such reflection to M by leaving x invariant we obtain that $r \circ f$ is the composition of at most $n-1$ reflections on M. Composing with $r^{-1} = r$ completes the proof of the corollary. □

Next we prove a special case of the Witt Cancellation Theorem, which holds for lattices over any valuation ring in which 2 is invertible.

Proposition 2.3. *Let M and N be lattices over a valuation ring R in which $v(2) = 0$, and define $v = \min\{v(M), v(N)\}$. Let L be a rank 1 lattice spanned by an element x whose norm has valuation not exceeding v, and assume that $M \oplus L$ and $N \oplus L$ are isomorphic. Then the lattices M and N are isomorphic.*

Proof. Let $f : M \oplus L \to N \oplus L$ be an isomorphism. The elements $0_N + x$ and $f(0_M + x)$ of $N \oplus L$ satisfy the conditions of Lemma 2.1, yielding a reflection r on $N \oplus L$ taking the latter element to the former. Writing $g = r \circ f$, we obtain an isomorphism from $M \oplus L$ to $N \oplus L$ which takes the direct summand L of the first lattice onto the direct summand L in the second one. This isomorphism must therefore take M isomorphically onto N, which proves the proposition. □

Proposition 2.3 generalizes a special case of Theorem 1 of [7], with a simpler proof. We can now prove the main result for the case $v(2) = 0$:

Theorem 2.4. *Let M and N be lattices over a 2-Henselian valuation ring R such that $2 \in R^*$. Decompose M and N, using Proposition 1.2, as $\bigoplus_{k=1}^{t} M_k$ and $\bigoplus_{k=1}^{s} N_k$ respectively. If $M \cong N$ then $t = s$ and for any k we have $M_k \cong N_k$ (and in particular $v(M_k) = v(N_k)$).*

Proof. The ranks of M and N must be equal, and we apply induction on this common rank. The case of rank 1 is immediate. Let $y \in M_1$ be a basis element as in Corollary 1.3. Then $v(y^2)$ is minimal in M, and let $w \in N$ be an element having the same norm as y (such w exists since $M \cong N$). $v(w^2)$ is also minimal in N, hence $v(N_1) = v(M_1)$. Write $w = \sum_{k=1}^{s} w_k$ with $w_k \in N_k$ for any $1 \leq k \leq s$. The minimality of $v(w^2)$ implies $v(w_k^2) > v(w^2)$ for any $k \geq 2$. Thus, the image of $\frac{w^2}{w_1^2}$ modulo I_0 is 1. Since $v(2) = 0$, Lemma 1.4 yields the existence of $c \in R^*$ such that $w^2 = c^2 w_1^2$, so that $z = cw_1 \in N_1$ has the same norm as y. Lemma 1.1 allows us to write M as $Ry \oplus (Ry)^\perp$ and N as $Rz \oplus (Rz)^\perp$. Let L be a rank 1 lattice generated by an element x having the same norm as y and z. The sublattices $(Ry)^\perp$ of M and $(Rz)^\perp$ of N, together with this element x, satisfy the conditions of Proposition 2.3 (indeed, $M \cong L \oplus (Ry)^\perp$ and $N \cong L \oplus (Rz)^\perp$ are isomorphic, and the valuation condition holds by our choice of y and z), so that $(Ry)^\perp \cong (Rz)^\perp$ by that proposition. Applying Lemma 1.1 to M_1 with y and to N_1 with z yields the decompositions $M_1 = Ry \oplus (Ry)^\perp_{M_1}$ and $N_1 = Rz \oplus (Rz)^\perp_{N_1}$, where the orthogonal complements $(Ry)^\perp_{M_1}$ and $(Ry)^\perp_{N_1}$ are uni-valued with valuation $v(M_1) = v(N_1)$. Therefore we can write $(Ry)^\perp = (Ry)^\perp_{M_1} \oplus \bigoplus_{k=2}^{t} M_k$ and $(Rz)^\perp = (Rz)^\perp_{N_1} \oplus \bigoplus_{k=2}^{s} N_k$ as uni-valued decompositions with increasing valuations, and the induction hypothesis implies $t = s$, $M_k \cong N_k$ for $k \geq 2$, and $(Ry)^\perp_{M_1} \cong (Rz)^\perp_{N_1}$. As $Ry \cong Rz$ as well, we deduce also $M_1 \cong N_1$, which completes the proof of the theorem. □

The Witt Cancellation Theorem for 2-Henselian valuation rings in which 2 is invertible follows as

Corollary 2.5. *Let M, N, and L be three lattices over such a ring R. If $M \oplus L \cong N \oplus L$ then $M \cong N$.*

Proof. Write $M = \bigoplus_{k=1}^{t} M_k$, $N = \bigoplus_{k=1}^{t} N_k$, and $L = \bigoplus_{k=1}^{t} L_k$ as in Proposition 1.2, where we assume that $v(M_k) = v(N_k) = v(L_k)$ for any $1 \leq k \leq t$ (allowing empty components if necessary for such a unified notation). Then we can write $M \oplus L$ and $N \oplus L$ as $\bigoplus_{k=1}^{t}(M_k \oplus L_k)$ and $\bigoplus_{k=1}^{t}(N_k \oplus L_k)$, both being decompositions to uni-valued lattices of increasing valuations. Theorem 2.4 yields $M_k \oplus L_k \cong N_k \oplus L_k$ for any $1 \leq k \leq t$, and we claim that $M_k \cong N_k$ for every such k. One way to establish this assertion is by dividing the bilinear forms on M_k, N_k, and L_k by a suitable element of R to make them unimodular, and then use the Witt Cancellation Theorem for unimodular lattices proved in Theorem 4.4 of [12]. Alternatively, L_k has an orthogonal basis by Corollary 1.3, and we can "cancel" these basis elements iteratively using Proposition 2.3 since the valuation condition is satisfied. In any case, this assertion implies $M = \bigoplus_{k=1}^{t} M_k \cong \bigoplus_{k=1}^{t} N_k = N$ as desired. □

Theorem 2.4 generalizes Theorem 4 of [5] to (2-Henselian) valuation rings of arbitrary rank, and Corollary 2.5 generalizes Theorem 2 of [7] and Theorem 5 of [5] to this case, again with simplified proofs.

There are classical examples showing that without the condition $2 \in R^*$, both Theorem 2.4 and Corollary 2.5 no longer hold. Over $\mathbb{Z}_2$ the lattice M generated by two orthogonal elements of norms 1 and 2 is isomorphic to the lattice N having an orthogonal basis consisting of vectors of norms 3 and 6. Since $v(1) = v(3) = 0$ and $v(2) = v(6) = 1$ but $\frac{3}{1} = \frac{6}{2} = 3 \notin (\mathbb{Z}_2^*)^2$, this example demonstrates that Theorem 2.4 fails for $R = \mathbb{Z}_2$ (for the analysis of $\mathbb{Z}_2$-lattices, see [8]). Still over $\mathbb{Z}_2$, taking $x^2 = y^2 = 0$ and $(x, y) = z^2 = t = 1$ in the proof of Corollary 1.3 shows that adding an orthogonal norm 1 vector to the hyperbolic plane generated by two norm 0 vectors x and y with $(x, y) = 1$ (denoted $M_{0,0}$ in the notation of Sections 3 and 4) one obtains a lattice admitting an orthonormal basis consisting of three elements with norms 1, 1, and -1 respectively, which gives a counter-example to Corollary 2.5 over $\mathbb{Z}_2$. The 2-Henselianity is also important: Consider the ring $\mathbb{Z}_{p\mathbb{Z}}$ obtained from $\mathbb{Z}$ by localizing in the prime ideal $p\mathbb{Z}$ for some odd prime p. It is a discrete valuation ring with quotient field $\mathbb{F}_p$ of odd characteristic, which is not complete. As in the first example over $\mathbb{Z}_2$, the lattice generated by two orthonormal vectors of norms 1 and p also admits an orthogonal basis whose norms are $1+p$ and $p+p^2$, and unless $1+p$ is a square in $\mathbb{Z}$, this shows that Theorem 2.4 does not hold over $\mathbb{Z}_{p\mathbb{Z}}$ (in case $1 + p$ is a square, one may use a similar argument with $1 + t^2p$ for other $t \in \mathbb{Z}$ fur this purpose). As for the general Witt Cancellation Theorem for valuation rings which are not 2-Henselian but with $2 \in R^*$, finding counter-examples seems complicated, in view of Proposition 2.3 and the fact that the Witt Cancellation Theorem holds in general when M, N, and L all have rank 1. We leave this question for further research.

Theorem 2.4 shows that the classification of general R-lattices (for R a 2-Henselian valuation ring with $2 \in R^*$) reduces to the classification of unimodular R-lattices in the following sense. For every $v \geq 0$ fix some element $\sigma_v \in R$ with valuation v, with $\sigma_0 = 1$. By Theorem 2.4 every R-lattice M can be written *uniquely* up to an isomorphism as $\bigoplus_v M_v(\sigma_v)$ with M_v unimodular such that $M_v = 0$ for all but finitely many v. Moreover, in this case the unimodular lattices are determined up to isomorphism by their (non-degenerate) restriction to the residue field $\mathbb{F}$ of R (see, for example, Theorem 1.5—note that $v(2) = 0$ by our assumption on R and $v(M_t) = 0$ by unimodularity). Hence, the classification of R-lattices simplifies to the classification of lattices over the field $\mathbb{F}$, whose characteristic differs from 2, for which many methods have been developed. For general fields this problem is not at all simple: For example, for $\mathbb{F}$ a global field the isomorphism classes depend on all the completions of $\mathbb{F}$. However, if $\mathbb{F}$ is *finite* then the isomorphism class of an $\mathbb{F}$-lattice M is determined by its rank and sign (i.e., the image of the determinant of a Gram matrix of a basis of M in the order 2 group $\mathbb{F}^*/(\mathbb{F}^*)^2$)—see, for example, Proposition 5 in Chapter IV of [15]. Let $1^{\varepsilon n}$ denote a unimodular R-lattice (R as above, with a finite residue field $\mathbb{F}$) whose restriction modulo I_0 has rank n and sign $\varepsilon \in \mathbb{F}^*/(\mathbb{F}^*)^2 \cong \{\pm 1\}$. Using the shorthand $\sigma_v^{\varepsilon n}$ for $1^{\varepsilon n}(\sigma_v)$, we have thus proved

Proposition 2.6. *Any isomorphism class of lattices over a 2-Henselian valuation ring R with finite residue $\mathbb{F}$ of odd characteristic contains a unique representative of the form $\bigoplus_v \sigma_v^{\varepsilon_v n_v}$ (where the direct sum is finite).*

Proof. The existence of such a representative follows from Proposition 1.2 and the fact that every uni-valued R-lattice is (up to isomorphism) of the form $\sigma_v^{\varepsilon_v n_v}$ for unique v, n_v, and ε_v (see the previous paragraph). The uniqueness follows from Theorem 2.4. This proves the proposition. □

In the case where R is a *discrete* valuation ring we can take σ_v for $v \in \mathbb{N}$ to by the vth power of a uniformizer π of R. In particular, Proposition 2.6 yields the known symbols for lattices over p-adic rings (for odd p), but it holds in much greater generality.

3. Unimodular rank 2 lattices

Corollary 1.3 implies that there are only two types of lattices over a valuation ring R which are *indecomposable* (namely, cannot be written as the orthogonal direct sum of two proper sublattices). Such a lattice is either generated by one element, or is spanned by two elements x and y such that $v(x, y)$ is strictly smaller than the valuations of the norms of both x and y. Both such lattices are uni-valued, hence (after fixing a_v for each possible valuation v) it suffices for the description of the isomorphism classes of such lattices to consider just unimodular lattices. For rank 1 lattices the task is easy: Each isomorphism class of unimodular rank 1 lattices corresponds to an element of $R^*/(R^*)^2$, which is the norm of a generator of a lattice in this isomorphism class. We consider classes modulo $(R^*)^2$ since multiplying the generator by $c \in R^*$ yields a generator for the same module, with norm multiplied by c^2. In fact, if the unimodularity assumption is relaxed, the isomorphism classes of non-degenerate rank 1 lattices correspond to classes in $(R \setminus \{0\})/(R^*)^2$, and these assertions hold over any integral domain R.

We now consider unimodular rank 2 lattices, in which the basis elements x and y satisfy $(x, y) \in R^*$. In fact, every unimodular rank 2 lattice L over a valuation ring admits such a basis: If for a given basis x and y of L we have $(x, y) \notin R^*$ (i.e., $(x, y) \in I_0$) then without loss of generality unimodularity implies $v(x^2) = 0$. Thus, x and $x + y$ form a basis for L such that $(x, x + y) \in R^*$. Multiplying x or y by an element of R^*, we may assume $(x, y) = 1$.

Given α and β in R, we denote the rank 2 lattice spanned by elements x and y with $x^2 = \alpha$, $(x, y) = 1$, and $y^2 = \beta$ by $M_{\alpha,\beta}$. Without loss of generality, we always assume $v(\alpha) \leq v(\beta)$. An interesting question, which will be answered under some assumptions in Section 4 below, is finding necessary and sufficient conditions on α, β, γ and δ such that $M_{\alpha,\beta} \cong M_{\gamma,\delta}$. The present section is devoted to the description of the lattices $M_{\alpha,\beta}$, and is divided into three subsections. In Subsection 3.1 we classify the lattices $M_{\alpha,0}$ and prove a technical lemma which will later have various applications. Subsection 3.2 considers conditions for existence of a primitive element with norm of maximal valuation in $M_{\alpha,\beta}$. Finally, Subsection 3.3 defines the generalized Arf invariant of such a lattice (under this maximality assumption on β) and proves that it is an invariant of the isomorphism class of the lattice. Unless stated otherwise, R is a 2-Henselian valuation ring.

3.1. Isotropic lattices and general technicalities

Recall that a non-zero norm 0 vector is called *isotropic*, and a lattice is called *isotropic* if it contains an isotropic vector. Our first observation is

Lemma 3.1. *If $v(\alpha) + v(\beta) > 2v(2)$ then $M_{\alpha,\beta}$ is isotropic.*

Proof. Write $(y + tx)^2 = \alpha t^2 + 2t + \beta$. Then the coefficients $A = \alpha$, $B = 2$, and $C = \beta$ satisfy the condition of Lemma 1.4. Hence there exists some $t \in \mathbb{K}$ which annihilates this expression, and the inequality $v(C) > v(B)$ (which follows from $v(\alpha) \leq v(\beta)$ and $v(\alpha) + v(\beta) > 2v(2)$) implies that we can take $t \in R$ (and even $t \in I_0$). The vector $y + tx$ of $M_{\alpha,\beta}$ is then isotropic, which proves the lemma. □

We now prove another assertion about the possible values of norms of elements of $M_{\alpha,\beta}$ having minimal valuation under certain conditions. In the case $v(2) > 0$ the *Artin–Schreier map* $\rho : \mathbb{F} \to \mathbb{F}$ is defined by $\rho(x) = x^2 - x$. It is an additive homomorphism on $\mathbb{F}$, whose kernel is the prime subfield $\mathbb{F}_2 \subseteq \mathbb{F}$, and its image is denoted $\mathbb{F}_{AS}$. By some abuse of notation, the map from R to R defined by the same formula $x \mapsto x^2 - x$ will be also denoted ρ, though it is no longer a homomorphism of additive groups. We denote $\rho(R)$ by R_{AS}. First we need

Lemma 3.2. *If $y \in R$ then $y \in R_{AS}$ holds if and only if $y + I_0 \in \mathbb{F}_{AS}$.*

Proof. If $y = \rho(x)$ then $y + I_0 = \rho(x + I_0)$. Conversely, if $y + I_0 = \rho(x + I_0)$ for some $x \in R$ then substitute $t = s + x$ in the polynomial $f(t) = t^2 - t - y$ in order to obtain $g(s) = s^2 - (1-2x)s + (x^2 - x - y)$. The coefficients $A = 1$, $B = 2x - 1$, and $C = x^2 - x - y$ satisfy $v(AC) > v(B^2)$ since $v(C) > 0$ and $v(A) = v(B) = 0$ (recall that $2 \in I_0$). Hence Lemma 1.4 yields a root $s \in I_0 \subseteq R$ of this polynomial. The element $x + s$ of R (with the same $\mathbb{F}$-image as x) satisfies $\rho(x + s) = y$, which completes the proof of the lemma. □

We now prove an important technical result which will be needed later.

Lemma 3.3. *Let α and β be two elements of R such that $v(\beta) \geq v(2)$ and $v(\beta) \geq v(\alpha)$. We define the set T to be $(R^*)^2 \cdot (\alpha + 2R)$ in case $v(\beta) > v(2)$ and as $(R^*)^2 \cdot (\alpha + \frac{4}{\beta}R_{AS})$ if $v(\beta) = v(2)$. (i) If $v(\alpha) \geq v(2)$ and $v(\beta) > v(2)$ then $T = 2R$, and this is the set of all norms of elements in $M_{\alpha,\beta}$. (ii) In the case $v(2) > v(\alpha)$ the set T consists of all the norms of elements of $M_{\alpha,\beta}$ having minimal valuation, which then equals $v(\alpha)$. (iii) In the boundary case $v(\beta) = v(2) = v(\alpha)$ an element lies in T precisely when it is the norm of a primitive element of $M_{\alpha,\beta}$.*

Proof. First we show that an element of R lies in T if and only if it is the norm of some element $z \in M_{\alpha,\beta}$ of the form $z = cx + dy$ with $c \in R^*$. Indeed, such an element of $M_{\alpha,\beta}$ can be written as $c(x + sy)$ with $s \in R$, and its norm $c^2(\alpha + 2s + s^2\beta)$ is of the form $c^2(\alpha + 2r)$ since $2|\beta$. Moreover, if $v(\beta) = v(2)$ then by writing $s = -\frac{2}{\beta}x$ we find that $r = \frac{2}{\beta}\rho(x) \in \frac{2}{\beta}R_{AS}$. Conversely, given r and c we need to show that $c^2(\alpha + 2r)$ can be obtained as the norm of such $z \in M_{\alpha,\beta}$. By writing $z = c(x + sy)$ again this assertion reduces to finding $s \in R$ such that $r = s + s^2\frac{\beta}{2}$. Consider the polynomial $f(s) = \frac{\beta}{2}s^2 + s - r$. If $v(\beta) > v(2)$ and r is arbitrary, then the coefficients $A = \frac{\beta}{2} \in I_0$, $B = 1 \in R^*$, and $C = -r \in R$ satisfy the conditions of Lemma 1.4, yielding a solution $s \in R$ (of valuation $v(\frac{C}{B}) = v(r) \geq 0$). On the other hand, if $v(\beta) = v(2)$ and $r \in \frac{2}{\beta}R_{AS}$ then the substitution $s = -\frac{2}{\beta}t$ takes $f(s)$ to the form $\frac{2}{\beta}(t^2 - t + \frac{\beta}{2}r)$, which has a root t by our assumption on r.

Now, if $v(\beta) > v(2)$ and $v(\alpha) \geq v(2)$ then $T = 2R$, and since for every element $z = ax + by \in M_{\alpha,\beta}$ the three terms $a^2\alpha$, $2ab$, and $b^2\beta$ of z^2 are divisible by 2, we obtain $T = \{z^2 \mid z \in M_{\alpha,\beta}\}$. This proves (i). On the other hand, assume $v(\alpha) < v(2)$, and let $z \in M_{\alpha,\beta}$ be an element whose norm has the same valuation as α. We write $z = cx + dy$, and if $c \in I_0$ then the three terms $c^2\alpha$, $2cd$, and $d^2\beta$ of $(cx + dy)^2$ lie in $I_{v(\alpha)}$. Since this contradicts the assumption $v(z^2) = v(\alpha)$ we deduce $c \in R^*$, and we have already seen that $z^2 \in T$ for such z. This proves (ii). It remains to consider the case $v(\beta) = v(2) = v(\alpha)$. In this case a primitive element of $M_{\alpha,\beta}$ not considered in the above paragraph takes the form $z = h(y + tx)$ with $h \in R^*$ and $t \in I_0$, and satisfies $z^2 = h^2(\beta + 2t + t^2\alpha)$. But the element $w = h[(\frac{2}{\alpha} + t)x - y]$ has the same norm as z and the coefficient of x in w is in R^* (since $\frac{2}{\alpha} \in R^*$ and $t \in I_0$), so that the norm of z lies in T for such z as well. This proves (iii) and completes the proof of the lemma. □

We remark that the element $w \in M_{\alpha,\beta}$ defined at the end of the proof of Lemma 3.3 is the image of z under the reflection with respect to x, taking $u \in M_{\alpha,\beta}$ to $u - \frac{2(u,x)}{\alpha}x$. This element is well-defined as an automorphism of $M_{\alpha,\beta}$ since $\frac{2}{\alpha} \in R$, though it is not a reflection with respect to a decomposition since $M_{\alpha,\beta}$ does not decompose as $Rx \oplus (Rx)^{\perp}$ if $v(\alpha) > 0$.

The proof of parts (i) and (ii) of Lemma 3.3 allows us to classify isotropic rank 2 unimodular lattices over any valuation ring (not necessarily 2-Henselian):

Proposition 3.4. *Let R be any valuation ring. The lattices $M_{\alpha,0}$ and $M_{\gamma,0}$ are isomorphic if and only if $\gamma = c^2(\alpha + 2r)$ for some $c \in R^*$ and $r \in R$. Therefore the isomorphism classes of isotropic unimodular rank 2 lattices are in one-to-one correspondence with the set $(R/2R)/(R^*)^2$.*

Proof. The only place where we used the 2-Henselian property of R in the proof of Lemma 3.3 was in our search for a solution to the equation $\frac{\beta}{2}s^2 + s = r$ for $r \in R$. But if $\beta = 0$ then $s = r$ is a solution, so that Lemma 3.3 with $\beta = 0$ holds over any valuation ring R. Thus, if x and y form the basis for $M_{\alpha,0}$ as above then $c(x + ry)$ and $\frac{y}{c}$ span the same lattice and define an isomorphism with $M_{\gamma,0}$ for $\gamma = c^2(\alpha + 2r)$. It remains to show that if $M_{\alpha,0} \cong M_{\gamma,0}$ then $\gamma = c^2(\alpha + 2r)$ for some $r \in R$ and $c \in R^*$. If $2|\alpha$ then γ, as the norm of some element of $M_{\alpha,0}$, is divisible by 2 (the proof of Lemma 3.3 again), which completes the proof for this case. Assume now $v(\alpha) < v(2)$. The isomorphism from $M_{\gamma,0}$ to $M_{\alpha,0}$ takes the isotropic generator of $M_{\gamma,0}$ to a primitive isotropic vector $w \in M_{\alpha,0}$, which can be either $\frac{y}{c}$ or $\frac{1}{c}(y - \frac{2}{\alpha}x)$ for $c \in R^*$. The other basis vector of $M_{\gamma,0}$ must be taken to some $z \in M_{\alpha,0}$ with $(z, w) = 1$. In the first case we have $z = c(x + ry)$ for some $r \in R$, and the norm of z is $c^2(\alpha + 2r)$ as shown above. Otherwise $w = \frac{1}{c}(y - \frac{2}{\alpha}x)$, and writing $z = ax + by$ with a and b in R, the equality $(z, w) = 1$ implies $a = -c - \frac{2}{\alpha}b$. It follows that z takes the form $-cx + b(y - \frac{2}{\alpha}x)$ for some $b \in R$, and its norm $c^2\alpha - 2bc$ also has the asserted form. This proves the proposition. □

The reflection with respect to x appears implicitly also in the proof of Proposition 3.4, since it takes the element $\frac{y}{c}$ of $M_{\alpha,0}$ to $\frac{1}{c}(y - \frac{2}{\alpha}x)$.

We remark that if $\alpha \in R^*$ then $M_{\alpha,0}$ is decomposable, since the elements x and $t = x - \alpha y$ are orthogonal and have the norms α and $-\alpha$ respectively. Conversely, a direct sum of two unimodular rank 1 lattices which is isotropic must be of this form: If z and w are perpendicular and have norms in R^* then for some combination $az + bw$ to have be isotropic we must have $a^2z^2 = -b^2w^2$. Hence $v(a) = v(b)$, and by replacing w by $u = \frac{b}{a}w$ we obtain a generator u for Rw such that $u^2 = -z^2$. Therefore Proposition 3.4 implies the following

Corollary 3.5. *For $\alpha \in R^*$ (R being any valuation ring) denote $H_{\alpha,0}$ the lattice generated by two orthogonal elements of norms α and $-\alpha$. Given α and γ in R^*, the relation $H_{\alpha,0} \cong H_{\gamma,0}$ holds if and only if $\gamma = c^2\alpha + 2r$ for $c \in R^*$ and $r \in R$.*

Proof. The previous paragraph shows that for any $\alpha \in R^*$ the lattices $H_{\alpha,0}$ and $M_{\alpha,0}$ are isomorphic. Hence the assertion follows from Proposition 3.4. □

In particular, if $v(2) = 0$ then $R/2R$ is trivial, and Proposition 3.4 implies that every isotropic unimodular rank 2 lattice over R is a hyperbolic plane (namely, a lattice isomorphic to $M_{0,0}$ in the notation of Proposition 3.4). This statement is in correspondence with the results at the end of Section 2, since the same assertion holds over $\mathbb{F}$ if the characteristic of $\mathbb{F}$ is not 2. Corollary 3.5 implies in this case that all the lattices of the form $H_{\alpha,0}$ with $\alpha \in R^*$ are isomorphic. On the other hand, if $v(2) > 0$ then the elements of $(I_0/2R)/(R^*)^2$ correspond to *indecomposable* isotropic unimodular lattices of rank 2. If $v(2) = 0$ then $I_0/2R$ is not well-defined and can be considered as the empty set (since I_0 is the complement of R^* and the image of R^* in $R/2R$ is the entire set $R/2R$), which corresponds to the fact that there exist no indecomposable rank 2 lattices in this case (Corollary 1.3 again).

3.2. Primitive vectors with norms of maximal valuation

The anisotropic case is more delicate. Lemma 3.1 allows us to restrict attention to the case $v(\alpha)+v(\beta) \leq 2v(2)$ when we consider anisotropic lattices. The following lemma will turn out useful in what follows.

Lemma 3.6. *If $v(\alpha)+v(\beta) \leq 2v(2)$ then the valuation of the norm of a non-zero element of $M_{\alpha,\beta}$ of the form $tx+sy$ with t and s in R can be evaluated as $\min\{v(t^2\alpha), v(s^2\beta)\}$, provided that the two terms $t^2\alpha$ and $s^2\beta$ have different valuations. In case $v(t^2\alpha) = v(s^2\beta)$ and $v(\alpha)+v(\beta) < 2v(2)$, the valuation of $(tx+sy)^2$ is larger than the common valuation of $t^2\alpha$ and $s^2\beta$ if and only if $v(t^2\alpha+s^2\beta) \geq v(t^2\alpha) = v(s^2\beta)$.*

Proof. The element in question has norm $t^2\alpha + 2st + s^2\beta$, and we claim that $v(2st) > \min\{v(t^2\alpha), v(s^2\beta)\}$ under our assumptions. If $s = 0$ this is clear, so assume $s \neq 0$. Now, assuming by contradiction that $v(2st) \leq v(s^2\beta)$ and $v(2st) \leq v(t^2\alpha)$, we obtain the inequalities $v(\frac{t}{s}) \leq v(\frac{\beta}{2})$ and $v(\frac{t}{s}) \geq v(\frac{2}{\alpha})$, the combination of which yields $v(\frac{\beta}{2}) \geq v(\frac{2}{\alpha})$. But the latter inequality implies $v(\alpha)+v(\beta) \geq 2v(2)$, and this may occur with $v(\alpha)+v(\beta) \leq 2v(2)$ only if $v(\alpha)+v(\beta) = 2v(2)$ and $v(t^2\alpha) = v(s^2\beta)$, a case which we have excluded in our assumptions. This establishes the claim. It follows that comparing $v((sx+ty)^2)$ with $\min\{v(t^2\alpha), v(s^2\beta)\}$ is the same as comparing $v(t^2\alpha+s^2\beta)$ with that minimum, which completes the proof of the lemma. □

If $v(\alpha) \leq v(2)$ (and $v(\alpha) \leq v(\beta)$, as always), then x is a primitive element of $M_{\alpha,\beta}$ whose norm has minimal valuation. This is obvious, since the three terms appearing in the expansion of the norm of any element $ax+by$ of M have valuations of at least $v(\alpha)$. Maximal valuation is a more complicated property, whose existence is guaranteed only under some conditions on R in Proposition 3.10 below. We shall restrict attention, from now on, only to those lattices $M_{\alpha,\beta}$ which do contain such elements. Henceforth, *we assume in our notation* $M_{\alpha,\beta}$ *that* β*, as a norm of a primitive element of* $M_{\alpha,\beta}$*, has maximal valuation.* For the characterization of such lattices, we need a parity notion for elements of the value group Γ. We call an element of Γ *even* if it is divisible by 2 in Γ (namely, if it is the valuation of an element of $(\mathbb{K}^*)^2$), and *odd* otherwise. A distinguished class of elements of even valuation is given in the following

Definition 3.7. An element a of even valuation is called an *approximate square* if $a \equiv b^2 (\mathrm{mod}\ I_{v(a)})$ for some $b \in R$. If $v(a) = 0$ we call a a *residual square*. Given an even valuation u, we let J_u be the union of the ideal I_u with the set of approximate squares of valuation u.

The condition that $v(a)$ is even in Definition 3.7 is in fact redundant, since no element of odd valuation can satisfy the required property for being an approximate square. We claim that if $v(2) > 0$ then the sets J_u for even u are additive subgroups of R. Indeed, J_0 is just the inverse image of $\mathbb{F}^2$ (including 0) under the projection from R to $\mathbb{F}$; It is a group since $x \mapsto x^2$ is additive on a field of characteristic 2 and $\mathbb{F}^2$ is just the image of this map. In the general case we observe that if $a \in R$ has even valuation u then a is an approximate square if and only if $\frac{a}{\sigma^2}$ is a residual square for some (hence any) $\sigma \in R$ with $2v(\sigma) = u$. Hence $J_u = \sigma^2 J_0$ for any such σ, showing that it is also a group. As $I_u \subseteq J_u$, we may allow ourselves the slight abuse of notation by referring as approximate squares also to images in R/I_u of approximate squares of valuation u, and this remains well-defined. We remark that the natural definition of J_u for an odd valuation u is just I_u, since there are no approximate squares of valuation u.

In our examination of lattices $M_{\alpha,\beta}$ with primitive vectors of norms with maximal valuation we shall distinguish among the cases $v(\alpha) + v(\beta) < 2v(2)$ and $v(\alpha) + v(\beta) = 2v(2)$.

Proposition 3.8. *The case* $v(\alpha)+v(\beta) < 2v(2)$ *and* $v(\beta)$ *is maximal occurs precisely when the element* $\frac{\beta}{\alpha}$ *of* R *is not an approximate square. More explicitly, if* $v(\alpha)+v(\beta) < 2v(2)$ *then* $v(\beta)$ *is maximal either when* $v(\frac{\beta}{\alpha})$ *is odd, or when* $v(\frac{\beta}{\alpha})$ *is even but* $\frac{\beta}{\alpha\sigma^2} + I_0$ *is not in* $(\mathbb{F}^*)^2$ *for some (hence any)* $\sigma \in R$ *with* $2v(\sigma) = v(\frac{\beta}{\alpha})$*, but in no other case.*

Proof. A primitive element $z \in M_{\alpha,\beta}$ takes either the form $c(y + tx)$ with $t \in R$ and $c \in R^*$ or the form $c(x + sy)$ with $s \in I_0$ and $c \in R^*$. For the valuation of the norm of z, we can assume $c = 1$. For the norm of an element of the form $x + sy$, the fact that $v(\beta) \geq v(\alpha)$ and $s \in I_0$ allows us to apply Lemma 3.6, which yields that the valuation of this norm is just $v(\alpha)$. As for $z = y + tx$, Lemma 3.6 shows that the valuation of z^2 is $\min\{v(\beta), v(t^2\alpha)\}$ unless $v(\beta) = v(t^2\alpha)$ and the sum $\beta + t^2\alpha$ has larger valuation. If $v(\frac{\beta}{\alpha})$ is odd then the equality $v(\beta) = v(t^2\alpha)$ cannot be achieved, hence any primitive z has norm of valuation at most $v(\beta)$. Otherwise we take $t = \sigma r$ for σ as above and $r \in R^*$, and $\beta + t^2\alpha$ has valuation larger than $v(\beta)$ if and only if $1 + r^2 \cdot \frac{\alpha\sigma^2}{\beta} \in I_0$. The maximality of $v(\beta)$ is thus equivalent to $1 + r^2 \cdot \frac{\alpha\sigma^2}{\beta}$ being in R^* for every such r, and since 2 must be in I_0 to allow $v(\alpha)+v(\beta) < 2v(2)$, the latter condition forbids the image of $\frac{\beta}{\alpha\sigma^2}$ modulo I_0 to belong to $(\mathbb{F}^*)^2$. This proves the proposition. □

It is clear that Proposition 3.8 can be stated in terms of properties of the product $\alpha\beta$ rather than the quotient $\frac{\beta}{\alpha}$.

Corollary 3.9. *If the residue field $\mathbb{F}$ of R is perfect then the situation described in Proposition 3.8 occurs only if $v(\frac{\beta}{\alpha})$ is odd.*

Proof. $\mathbb{F}$ is of characteristic 2, and it is perfect if and only if $(\mathbb{F}^*)^2 = \mathbb{F}^*$. Hence the second setting in Proposition 3.8 cannot occur in this case. □

Using Proposition 3.8, we derive a condition on R assuring the existence of a primitive element whose norm has maximal valuation in every R-lattice $M_{\alpha,\beta}$. We recall that an extension $\mathbb{L}$ of $\mathbb{K}$ with a valuation w on $\mathbb{L}$ such that $w|_{\mathbb{K}} = v$ is called *immediate* if $w(\mathbb{L}) = \Gamma$ and the quotient field S/J_0, with S the valuation ring of $(\mathbb{L}, w)$ and J_0 the maximal ideal in S, is isomorphic to $\mathbb{F}$.

Proposition 3.10. *Assume that $\mathbb{K}$ admits no quadratic immediate extensions. Then every lattice $M_{\alpha,\beta}$ contains a primitive element whose norm has maximal valuation.*

Proof. Let $M_{\alpha,\beta}$ be a lattice without such an element. First we observe that $v(\alpha)+v(\beta) < 2v(2)$. For if $v(\alpha) + v(\beta) > 2v(2)$ then $M_{\alpha,\beta}$ is isotropic by Lemma 3.1, and the norm of an isotropic vector has maximal valuation ∞. Moreover, if $v(\alpha) + v(\beta) = 2v(2)$ then the fact the β is not maximal allows us to find a primitive element of norm δ with $v(\delta) > v(\beta)$. This implies $M_{\alpha,\beta} \cong M_{\gamma,\delta}$ for some γ with $v(\gamma) \geq v(\alpha)$, and we are again in the isotropic case.

Now, a primitive element of $M_{\alpha,\beta}$ whose norm has valuation larger than $v(\alpha)$ must be of the form $z = c(y + tx)$ for some $c \in R^*$ (see the second paragraph of the proof of Lemma 3.3), and again we can take $c = 1$ since we are interested only in $v(z^2)$. We now construct a sequence of elements $z_\sigma = y + t_\sigma x$, for σ in some maximal well-ordered set Σ, whose norms $\beta_\sigma = z_\sigma^2$ satisfy $v(\beta_\tau) > v(\beta_\sigma)$ for $\tau > \sigma$. We do this using transfinite induction, starting with $t_0 = 0$, $z_0 = y$, and $\beta_0 = \beta$. Assume that we constructed z_σ for $\sigma \in \Sigma$. If Σ has a maximal element τ, then we can find some $t_{\tau+1}$ such that $z_{\tau+1}$ has norm $\beta_{\tau+1}$ with valuation bigger than $v(\beta_\tau)$ (since β_τ is not maximal). Then the index $\tau + 1$ increases Σ. If Σ does not contain any maximal element, but there exists some primitive element of $M_{\alpha,\beta}$ having norm with valuation exceeding $v(\beta_\sigma)$ for every $\sigma \in \Sigma$, then we saw that this element can be written as $z_\tau = y + t_\tau x$, and we increase Σ by adding τ as a new maximal element. We stop when it is impossible to add further elements to Σ. The fact that we take elements from a fixed lattice implies that this transfinite process must terminate. We thus obtain a well-ordered set Σ, having no last element, and t_σ for each $\sigma \in \Sigma$ such that $v(\beta_\tau) > v(\beta_\sigma)$ for every $\tau > \sigma$ in Σ, and such that no primitive element of $M_{\alpha,\beta}$ has norm with valuation exceeding $v(\beta_\sigma)$ for every $\sigma \in \Sigma$.

We claim that $\{t_\sigma\}_{\sigma\in\Sigma}$ is an algebraic pseudo-convergent sequence in R, with no pseudo-limit in R (see Definitions 10, 12, and 15 in Section 2 of [14]). Indeed, let σ and τ be elements of Σ with $\sigma < \tau$, and write $z_\tau = z_\sigma + (t_\tau - t_\sigma)x$. As $v(\alpha) + v(\beta_\sigma) < 2v(2)$, Lemma 3.6 implies that $v(\beta_\sigma) = v((t_\tau - t_\sigma)^2\alpha)$, for otherwise the condition $v(\beta_\tau) > v(\beta_\sigma)$ cannot be satisfied (the fact that (x, z_σ) equals $1 + t_\sigma\alpha$ rather than 1 does not affect the validity of Lemma 3.6). As in the proof of Proposition 3.8 we obtain that $v(\frac{\beta_\sigma}{\alpha})$ is even and equals $2v(t_\tau - t_\sigma)$ for each $\sigma \in \Sigma$. Hence $v(t_\tau - t_\sigma) = \eta_\sigma$ with $\eta_\sigma \in \Gamma$ strictly increasing with σ (as $2\eta_\sigma = v(\frac{\beta_\sigma}{\alpha})$), which shows that $\{t_\sigma\}_{\sigma\in\Sigma}$ is pseudo-convergent. Moreover, $\beta_\sigma = f(t_\sigma)$ for $f(t) = \beta + 2t + \alpha t^2$, and since $v(\beta_\sigma)$ strictly increases with σ, the algebraicity of $\{t_\sigma\}_{\sigma\in\Sigma}$ follows. Had this pseudo-convergent sequence a pseudo-limit $s \in R$, a similar argument would show that $y + sx$ has norm δ with $v(\delta) \geq v(\beta_\sigma)$ for every $\sigma \in \Sigma$, contrary to our assumption on Σ. Then Lemmas 12 and 19 of Section 2 of [14] yield a quadratic immediate extension $\mathbb{L}$ of $\mathbb{K}$ generated by adding a pseudo-limit to this sequence, in contradiction to our assumption on $\mathbb{K}$. This contradiction shows that $M_{\alpha,\beta}$ must contain a primitive element with maximal valuation. □

In particular, Proposition 3.10 shows that if $\mathbb{K}$ is *maximally complete* (i.e., admits no immediate extensions at all) then every lattice $M_{\alpha,\beta}$ contains a primitive element of norm with maximal valuation. The proof of Proposition 3.10 also shows that any lattice $M_{\alpha,\beta}$ contains such a primitive element in case the set of positive $\gamma \in \Gamma$ which are smaller than $2v(2)$ is *finite* (e.g., when $\Gamma = \mathbb{Z}$), a fact which is also easily verified directly.

The conditions for $v(\alpha) + v(\beta) = 2v(2) > 0$ are somewhat different.

Proposition 3.11. *If $v(\alpha) + v(\beta) = 2v(2)$ then $v(\beta)$ is maximal if and only if $\frac{\alpha\beta}{4} \in R^* \setminus R_{AS}$.*

Proof. The condition $v(\alpha) + v(\beta) = 2v(2)$ implies that $\varepsilon = -\frac{\alpha\beta}{4} \in R^*$. As in the proof of Proposition 3.8, we may restrict attention to norms of elements of the form $z = y + tx \in M_{\alpha,\beta}$, and the norm of such an element has valuation either $v(t^2\alpha)$ or $v(\beta)$ unless $v(t) = v(\frac{2}{\alpha})$ (which is equivalent here to $2v(t) = v(\frac{\beta}{\alpha})$). We therefore write $t = -\frac{2}{\alpha}s$ (with $s \in R^*$), and then $z^2 = \frac{4}{\alpha}(s^2 - s - \varepsilon)$. As $v(\frac{4}{\alpha}) = v(\beta)$, the valuation of z^2 exceeds $v(\beta)$ if and only if $\varepsilon + I_0 = \rho(s + I_0)$. Since z is primitive and $s \in R$ is arbitrary, we find that $v(\beta)$ is maximal if and only if $-\varepsilon + I_0 = \varepsilon + I_0 \notin \mathbb{F}_{AS}$, which is equivalent, by Lemma 3.2, to the desired condition $-\varepsilon \notin R_{AS}$. This proves the proposition. □

Corollary 3.12. *If ρ is surjective (in particular if $\mathbb{F}$ is algebraically closed) then any lattice $M_{\alpha,\beta}$ with $v(\alpha) + v(\beta) = 2v(2)$ is isotropic.*

Proof. The proof of Proposition 3.11 shows that $v(\beta)$ cannot be maximal, since we can take $s \in R$ such that $v(s^2 - s - \varepsilon) > 0$. But this shows that $M_{\alpha,\beta} \cong M_{\alpha,\delta}$ with $v(\delta) > v(\beta)$

(take the basis x and $\frac{y+tx}{1-2s}$ with $t=-\frac{2}{\alpha}s$ as in the latter proof). Since $v(\alpha)+v(\delta)>2v(2)$, Lemma 3.1 shows that this lattice is isotropic. This proves the corollary. $\square$

3.3. Generalized Arf invariants

Following Lemma 3.1 and Propositions 3.8 and 3.11, we define, under the assumption that $v(2)>0$, the following invariant of a unimodular rank 2 lattice containing a primitive element with norm of maximal valuation.

Definition 3.13. Let $M_{\alpha,\beta}$ be a unimodular rank 2 lattice over R such that β has maximal valuation. We define the *generalized Arf invariant* of $M_{\alpha,\beta}$ as follows:

1. If $M_{\alpha,\beta}$ is isotropic (i.e., $\beta=0$), define the generalized Arf invariant to be 0. This is called a *vanishing* generalized Arf invariant.
2. If $v(\alpha)+v(\beta)<2v(2)$ and is odd, then we define the generalized Arf invariant of $M_{\alpha,\beta}$ to be the class $\alpha\beta+I_{v(\alpha\beta)}$. These generalized Arf invariants are called *odd*.
3. In the case where $0<v(\alpha)+v(\beta)<2v(2)$ and is even, the generalized Arf invariant of $M_{\alpha,\beta}$ is defined to be the (non-zero) class $\alpha\beta+J_{v(\alpha\beta)}$ (modulo the group of approximate squares of valuation $v(\alpha\beta)$). This type of generalized Arf invariants is called *even*.
4. In case $v(\alpha)+v(\beta)=2v(2)$ we take the generalized Arf invariant of $M_{\alpha,\beta}$ to be the image of $\alpha\beta$ in $4R/4R_{AS}$. These are called *exact* generalized Arf invariants.

We remark that the odd and even cases in Definition 3.13 may be unified, since we saw that for odd u the natural definition is $J_u=I_u$. For the exact case, the group $4R/4R_{AS}$ in question is the image of $\mathbb{F}/\mathbb{F}_{AS}$ (depending only on $\mathbb{F}$) arising from multiplication by 4 on R and projecting onto the appropriate quotient.

The importance of the generalized Arf invariant from Definition 3.13 is revealed in the following

Proposition 3.14. *The generalized Arf invariant is an invariant of the isomorphism class of $M_{\alpha,\beta}$.*

Proof. The valuations of α and β are well-defined by the minimality and maximality assumptions. Denote $v(\alpha)+v(\beta)$ by u. Recall that the discriminant of $M_{\alpha,\beta}$ is $-1+\alpha\beta$, and we consider its class modulo $(R^*)^2$. If $M_{\gamma,\delta}\cong M_{\alpha,\beta}$ then $1-\alpha\beta=c^2(1-\gamma\delta)$, and since β and δ lie in I_0, it follows that $c^2\in 1+I_0$ hence $c\in 1+I_0$. If $u>2v(2)$ then Lemma 3.1 implies $u=\infty$, $\beta=\delta=0$, both discriminants are -1, and both generalized Arf invariants are 0. Hence the assertion is immediate in this case. Assume now that $u\leq 2v(2)$, and write $c=1-h$ with $h\in I_0$. By taking the images on both sides modulo I_u and noting that $c^2\gamma\delta\equiv\gamma\delta(\mathrm{mod}\ I_u)$ we obtain

$$\gamma\delta\equiv h^2-2h+\alpha\beta(\mathrm{mod}\ I_u).$$

We shall consider the cases $v(h) \geq v(2)$ and $v(h) < v(2)$ separately. Recall that $I_u \subseteq J_u$ for even u and $I_{2v(2)} \subseteq 4R_{AS}$, so that the condition $\gamma\delta \equiv \alpha\beta (\mathrm{mod}\ I_u)$ yields the asserted conclusion for any (non-vanishing) generalized Arf invariant.

Now, as $u \leq 2v(2)$, if $v(h) > v(2)$ then $h^2 - 2h \in I_u$ and $\gamma\delta \equiv \alpha\beta (\mathrm{mod}\ I_u)$. The same argument holds if $v(h) = v(2)$ and $u < 2v(2)$. The remaining case in which $v(h) \geq v(2)$ is where $v(h) = v(2)$ and $u = 2v(2)$. We write $h = 2t$ with $t \in R$, and the congruence shows that the difference between $\gamma\delta$ and $\alpha\beta$ is $4\rho(t)$ modulo $I_{2v(2)}$. Proposition 3.11 shows that $\alpha\beta + 4\rho(t)$ is not in $I_{2v(2)}$ for any $t \in R$, so that the corresponding class is non-zero, and Lemma 3.2 completes the proof of this case. Hence the assertion holds wherever $v(h) \geq v(2)$.

We now consider the case where $v(h) < v(2)$, which implies $v(2h) > 2v(h)$. It follows that if $2v(h) < u$ then the congruence cannot hold. This establishes the inequality $2v(h) \geq u$, which in particular completes the proof for exact generalized Arf invariants. We also have $2h \in I_u$, and we may omit it from the congruence. Thus, if $2v(h) > u$ then we again have $\gamma\delta \equiv \alpha\beta (\mathrm{mod}\ I_u)$, which in particular completes the proof for the case of odd u since $2v(h) \geq u$ implies $2v(h) > u$ in this case. It remains to consider the case where $u < 2v(2)$ and is even, and $2v(h) = u$. But our congruence shows that the difference $\gamma\delta - \alpha\beta$ is h^2 modulo I_u, and as $2v(h) = u$ this difference belongs to J_u. As Proposition 3.8 implies that the class of $\alpha\beta + J_u$ is non-zero, this completes the proof of the proposition. □

The case $u = 2v(2)$ in Proposition 3.14 generalizes the Arf invariant defined in [1] for such lattices, whence the name. For more on this relation, see Subsection 4.3. Note that this case (the exact generalized Arf invariants) arises from *non-zero* classes in $4R/4R_{AS}$; this is, in some sense, complemented by the vanishing generalized Arf invariant, representing the remaining, trivial class in $4R/4R_{AS}$. In any case, our generalized Arf invariant carries also the additional information about the valuation v. In Section 4 we shall present a refinement of the generalized Arf invariant in some cases, and use it to classify lattices $M_{\alpha,\beta}$ satisfying some additional conditions.

We remark that we have defined the generalized Arf invariant only for rank 2 lattices, while the classical Arf invariant is defined for quadratic modules of arbitrary even rank. As the generalized Arf invariant depends on some maximality conditions, defining it for higher rank lattices requires much more care, together with results of the same type as those appearing in Section 5 below.

We remark that many results from this section remain valid when the 2-Henselian assumption is relaxed. E.g., Lemma 3.2 holds over R also if we relax the hypothesis $2 \neq 0$ in 2-Henselianity: The polynomial f from the proof of that lemma satisfies $f(x) \in I_0$ and $f'(x) = 2x - 1$ lies in R^*, so that the usual Henselian property can be used to prove it. In this case, ρ is a homomorphism of additive groups also as a map on R. For Proposition 3.4 in the case where $2 = 0$ in R, we note that the only isotropic vectors in $M_{\alpha,0}$ are multiples of y (and there are no reflections involved). Hence the set $(R/2R)/(R^*)^2$ appearing in the classification there becomes just the set $R/(R^*)^2$, whose non-zero elements appeared in the classification of rank 1 lattices. The remaining assertions do not use the 2-Henselian property, and we just remark that if $2 = 0$ in R then a lattice $M_{\alpha,\beta}$ with β maximal is either isotropic or satisfies the conditions of Proposition 3.8. However, since 2-Henselianity is used in Lemma 3.1, and the rest of this section uses the inequality $v(\alpha) + v(\beta) \leq 2v(2)$ for anisotropic lattices, we prefer to stay in the 2-Henselian setting.

4. Invariants of lattices with primitive norms in $2R$

In this section we define a refinement of the generalized Arf invariant from Definition 3.13 in case the valuation is larger than $v(2)$. We then present an additional invariant of lattices $M_{\alpha,\beta}$ containing primitive elements with norms divisible by 2, and show that these two invariants characterize isomorphism classes of such lattices. In the end of this section we reproduce the results for lattices over the 2-adic ring $\mathbb{Z}_2$, and give also the example of lattices over $\mathbb{Z}_2[\sqrt{2}]$.

4.1. A criterion for isomorphism and fine Arf invariants

We first present the main criterion for isomorphism between lattices of the form $M_{\alpha,\beta}$ with $v(\beta) \geq v(2)$.

Lemma 4.1. *Assume $v(\alpha) \leq v(2) \leq v(\beta) \leq v(\frac{4}{\alpha})$. A lattice $M_{\gamma,\delta}$, where δ is a norm of primitive element with maximal valuation, is isomorphic to $M_{\alpha,\beta}$ if and only if $\gamma = c^2(\alpha + 2r)$ for some $r \in R$ (with the restriction $r \in \frac{2}{\beta}R_{AS}$ if $v(\beta) = v(2)$) and $c \in R^*$, and $\delta = \frac{\beta+2a-\frac{\alpha+2r}{1-\alpha\beta}a^2}{c^2(1+2\beta r)}$ for some $a \in R$ with $2v(a) \geq v(\frac{\beta}{\alpha})$. In particular, if γ is as above and $\delta - \frac{\beta}{c^2} \in I_{2v(2)-v(\alpha)}$ then $M_{\gamma,\delta} \cong M_{\alpha,\beta}$. In the limit case $v(\delta - \frac{\beta}{c^2}) = v(\frac{4}{\alpha})$, we obtain $M_{\gamma,\delta} \cong M_{\alpha,\beta}$ if and only if the element $\frac{\gamma}{4c^2}(c^2\delta - \beta)$ of R^* lies in R_{AS}. If $v(\alpha) < v(2)$ this is equivalent to $\frac{\alpha}{4}(\beta - c^2\delta) \in R_{AS}$.*

Proof. Since we assume $v(\alpha) \leq v(\beta)$ and $v(\gamma) \leq v(\delta)$, we find that γ is the norm of an element $z \in M_{\alpha,\beta}$ of the form $z = c(x+sy)$ with $c \in R^*$ and $s \in R$. Indeed, if $v(\alpha) < v(\beta)$ this is clear, and if $v(\alpha) = v(2) = v(\beta)$ then the assertion follows by using the reflection with respect to x (the one mentioned after Lemma 3.3) if necessary. Lemma 3.3 now implies that γ has the form $c^2(\alpha + 2r)$ with $c \in R^*$ and $r = s + \frac{\beta}{2}s^2 \in R$, and $r \in \frac{2}{\beta}R_{AS}$ if $v(\beta) = v(2)$. The second basis element w of $M_{\gamma,\delta}$ satisfies $(z, w) = 1$, which implies

$$c(1 + s\beta)w = y + \frac{a}{1 - \alpha\beta}\big((1 + s\beta)x - (\alpha + s)y\big)$$

for some $a \in R$. This is because $(y, z) = c(1+s\beta)$ and $(1+s\beta)x-(\alpha+s)y$ spans the space $(Rz)^{\perp}$. Therefore $\delta = \frac{[c(1+s\beta)w]^2}{c^2(1+s\beta)^2} = \frac{\beta+2a-\frac{\alpha+2r}{1-\alpha\beta}a^2}{c^2(1+2\beta r)}$ as asserted, and the inequality $2v(a) \geq v(\frac{\beta}{\alpha})$ follows from the maximality of δ (and implies $v(\delta) = v(\beta)$—see Propositions 3.8

and 3.11). Conversely, the map taking the two basis elements of $M_{\gamma,\delta}$ with such γ and δ to $z = c(x + sy)$ and the asserted w defines an isomorphism to $M_{\alpha,\beta}$ (the surjectivity of this map follows either by evaluating the determinant of this change of basis or just from unimodularity). This establishes the first assertion. Now, given γ (hence c^2), it remains to show that if $\delta - \frac{\beta}{c^2} \in I_{2v(2)-v(\alpha)}$, or if $v(\delta - \frac{\beta}{c^2}) = v(\frac{4}{\alpha})$ and $\frac{\gamma}{4c^2}(c^2\delta - \beta)$ lies in R_{AS}, then we can find an appropriate value of a. Write $\frac{\alpha+2r}{1-\alpha\beta}$ as $\eta\alpha$ for some η (which belongs to R^* since $\eta = \frac{\gamma}{c^2\alpha(1-\alpha\beta)}$ and $v(\gamma) = v(\alpha)$), and we need to find $a \in R$ such that $c^2(1 + 2\beta r)\delta = \beta + 2a - \eta\alpha a^2$. Denoting the left hand side by λ, we find $v(\eta - \frac{\gamma}{c^2\alpha}) = v(\alpha\beta) > 0$ and $v(\lambda - c^2\delta) \geq v(2\beta\delta) > v(\frac{4}{\alpha})$. Next, we write $a = \frac{\lambda-\beta}{2}b$, and look for a solution for

$$0 = -\eta\alpha a^2 + 2a + (\beta - \lambda) = (\beta - \lambda)\left[\eta\alpha\frac{(\lambda - \beta)}{4}b^2 - b + 1\right].$$

If $\delta - \frac{\beta}{c^2} \in I_{2v(2)-v(\alpha)}$ then $A = \eta\alpha\frac{(\lambda-\beta)}{4} \in I_0$, and Lemma 1.4 with $B = -1$ and $C = 1$ yields a solution $b \in R$. If $v(\delta - \frac{\beta}{c^2}) = v(\frac{4}{\alpha})$ then $\frac{4}{\alpha}(\lambda - \beta) \in R^*$, so that we write $b = \frac{4}{\eta\alpha(\lambda-\beta)}h$ and the equation becomes $0 = \frac{4}{\eta\alpha(\lambda-\beta)}[h^2 - h + \eta\alpha\frac{(\lambda-\beta)}{4}]$. The approximations for λ and η above show that $\eta\alpha\frac{(\lambda-\beta)}{4}$ has the same $\mathbb{F}$-image as the element $\frac{\gamma}{4c^2}(c^2\delta - \beta)$ of R_{AS}, so that Lemma 3.2 implies the existence of a solution to the latter equation. Finally, if $v(\alpha) < v(2)$ then η, hence also $\frac{\gamma}{c^2\alpha}$, are in $1 + I_0$, so that $\frac{\gamma}{4c^2}(\beta - c^2\delta) \in R_{AS}$ if and only if $\frac{\alpha}{4}(c^2\delta - \beta) \in R_{AS}$. This proves the lemma. $\square$

Lemma 4.1 is the main tool for investigating whether two lattices of the form $M_{\alpha,\beta}$ and $M_{\gamma,\delta}$, with β and δ maximal with valuations at least $v(2)$, are isomorphic. We begin by showing that isomorphism classes of lattices with generalized Arf invariant in $I_{v(2)}$ can be described using yet another invariant, which is finer than the generalized Arf invariant.

Proposition 4.2. *(i) The set $S = \{t^2 - 2t \mid t \in R, 2v(t) > v(2)\}$ is a subgroup of $I_{v(2)}$ which contains $I_{2v(2)}$. (ii) If $M_{\alpha,\beta} \cong M_{\gamma,\delta}$ with β and δ maximal and the (common) generalized Arf invariant is contained in $I_{v(2)}$, then $\alpha\beta$ and $\gamma\delta$ coincide modulo S. (iii) There exists a well-defined map from elements of the quotient $I_{v(2)}/S$ containing a representative of maximal valuation onto the set of generalized Arf invariants with valuation larger than $v(2)$.*

Proof. (*i*) The inclusion $S \subseteq I_{v(2)}$ is clear. For $y \in I_{2v(2)}$ we have $\frac{y}{4} \in I_0 \subseteq R_{AS}$, and if $\frac{y}{4} = \rho(x)$ then y is obtained as $t^2 - 2t$ for $t = 2x$. In order to show that S is a subgroup, we show that the difference between two elements $t^2 - 2t$ and $s^2 - 2s$ of S also lies in S, since it is of the form $(t - s + h)^2 - 2(t - s + h)$ for some h such that $2v(h) > v(2)$. Indeed, comparing terms yields the equation $h^2 + 2(t - s - 1)h + 2s^2 - 2ts = 0$ for h, where the coefficients $A = 1$, $B = 2(t - s - 1)$, and $C = 2s^2 - 2ts$ satisfy $v(A) = 0$, $v(B) = v(2)$, and $v(C) > 2v(2)$. To see the inequality concerning $v(C)$, observe that

$v(s^2) > v(2)$ and $v(ts) > v(2)$ because $2v(t) + 2v(s) > 2v(2)$ by our assumptions on s and t. Lemma 1.4 thus yields a solution h of valuation $v(\frac{C}{B})$, which is the same valuation as $v(ts - s^2) > v(2)$. Hence $2v(t - s + h) > v(2)$ and the difference is indeed an element of S.

(*ii*) Let now $M_{\alpha,\beta}$ and $M_{\gamma,\delta}$ be isomorphic lattices such that the common valuation u of $\alpha\beta$ and $\gamma\delta$ satisfies $u > v(2)$. Then $1 - \gamma\delta = c^2(1 - \alpha\beta)$ for some $c \in R^*$, and an argument similar to the proof of Proposition 3.14 shows that c must be of the form $1-h$ with $2v(h) \geq u$. But then $\alpha\beta(h^2 - 2h) \in I_{2v(2)} \subseteq S$ and $h^2 - 2h \in S$, so that $\gamma\delta - \alpha\beta \in S$ as asserted.

(*iii*) Let ω be a representative of a class of $I_{v(2)}/S$ of maximal valuation, i.e., $v(\omega + t^2 - 2t) \leq v(\omega)$ for every t with $2v(t) > v(2)$. If $v(\omega) > 2v(2)$ then $\omega \in S$ hence $\omega = 0$. Otherwise, the set of such representatives of the class $\omega + S$ is just $\omega + (S \cap \omega R)$, and it contains no element of $I_{v(\omega)}$. Considerations similar to those presented in the proof of Proposition 3.14 yield the following conclusions: If $v(\omega) < 2v(2)$ and is odd then $S \cap \omega R \subseteq I_{v(\omega)}$. If $v(\omega) < 2v(2)$ but is even, then the image of $S \cap \omega R$ modulo $I_{v(\omega)}$ coincides with that of $J_{v(\omega)}$. Finally, if $v(t^2 - 2t) \geq 2v(2)$ then $t \in 2R$, and if $t = 2r$ then $t^2 - 2t = 4\rho(r)$. The latter observation implies the equality $S \cap 4R = 4R_{AS}$ (and in particular we see that $I_{2v(2)} \subseteq S$ again). The maximality of $v(\omega)$ in its class implies that ω must satisfy the conditions for $\alpha\beta$ in Propositions 3.8 and 3.11 (i.e., either $v(\omega) < 2v(2)$ is odd, or $v(\omega) < 2v(2)$ is even and ω is not an approximate square, or $v(\omega) = 2v(2)$ and ω not lying in $4R_{AS}$). In particular every such ω defines a generalized Arf invariant. Moreover, our arguments show that this generalized Arf invariant is the image of ω in the quotient of ω modulo the group $(S \cap \omega R) + I_{v(\omega)}$, which is coarser than the quotient modulo $(S \cap \omega R)$ and coincides with it if $v(\omega) = 2v(2)$. Hence the map taking a class in $I_{v(2)}/S$ containing an element ω of maximal valuation to the generalized Arf invariant represented by ω is well-defined, as it just takes the image of ω in one quotient to the image of ω in a coarser quotient. This proves the proposition. □

On the basis of these arguments, we make the following

Definition 4.3. A *fine Arf invariant* is defined to be the set of representatives of maximal valuation in a class in $I_{v(2)}/S$ containing such representatives. The *valuation of a fine Arf invariant* is the valuation of any such representative. A fine Arf invariant is said to be

1. *vanishing* if it comes from the trivial class with the representative 0;
2. *odd* if its valuation is smaller than $2v(2)$ and odd;
3. *even* in case its valuation is smaller than $2v(2)$ and even; and
4. *exact* in case its valuation equals precisely $2v(2)$.

Given a lattice $M_{\alpha,\beta}$ with β of maximal valuation as the norm of a primitive element in this lattice and with generalized Arf invariant of valuation larger than $v(2)$, we define the *fine Arf invariant of* $M_{\alpha,\beta}$ to be the set of elements of valuation $v(\alpha\beta)$ in the class $\alpha\beta$ modulo S.

Part (*ii*) of Proposition 4.2 shows that the fine Arf invariant of a lattice $M_{\alpha,\beta}$ whose generalized Arf invariant has valuation larger than $v(2)$ is an invariant of the isomorphism class of $M_{\alpha,\beta}$. The type (vanishing, odd, even, or exact) of a fine Arf invariant from Definition 4.3 coincides with the type of the generalized Arf invariant to which is it taken by the map from part (*iii*) of Proposition 4.2. This map also preserves the valuations of fine and generalized Arf invariants, and its restriction to vanishing and exact fine Arf invariants (i.e., to valuations at least $2v(2)$) gives a natural bijection between these fine and generalized Arf invariants. It is clear that this map takes the fine Arf invariant of a lattice $M_{\alpha,\beta}$ (for which the fine Arf invariant is defined) to the generalized Arf invariant of this lattice.

4.2. Classes of minimal norms

Lemma 4.1 shows that if $v(\beta) \geq v(2)$ and $M_{\alpha,\beta} \cong M_{\gamma,\delta}$ then γ differs from some element in $(R^*)^2\alpha$ by an element in $2R$ (and even in $\frac{4}{\beta}R_{AS}$ if $v(\beta) = v(2)$). Lemma 3.2 implies that the set $\frac{4}{\beta}R_{AS}$ depends only on the image of β modulo $I_{v(\beta)}$, so that we can write it (at least heuristically at this point) as $\frac{4\alpha}{\eta}R_{AS}$ using the generalized Arf invariant η of $M_{\alpha,\beta}$. Thus, if $v(\beta) = v(2)$ then γ and α can be described as related through the action of the multiplicative group $(R^*)^2(1 + \frac{4}{\eta}R_{AS})$. In order to put the relation for $v(\beta) > v(2)$ on the same basis, we remark that (at least for the non-zero classes with $v(\alpha) < v(2)$) the relation $\gamma \in (R^*)^2(\alpha + 2R)$ can also be phrased using the action of the group $(R^*)^2(1 + \frac{2}{\xi}R)$ where $\xi \in R$ is any element of R with $v(\xi) = v(\alpha)$. We therefore introduce the following

Definition 4.4. A *coarse class of minimal norms* is an element of the set $(R/2R)/(R^*)^2$. Given a lattice $M_{\alpha,\beta}$ such that $v(\beta)$ is maximal and satisfies $v(\beta) > v(2)$, we define the *class of minimal norms of* $M_{\alpha,\beta}$ to be the image of α in the set of coarse classes of minimal norms. Given a generalized Arf invariant η with $v(\eta) \leq 2v(2)$ (i.e., non-vanishing) we define a *fine class of minimal norms arising from* η to be the orbit of an element of R, of valuation u satisfying $2u \leq v(\eta)$, under the action of the multiplicative group $(R^*)^2(1 + \frac{4}{\tau}R_{AS})$, where τ is some element of R whose class in the appropriate quotient is η. Let $M_{\alpha,\beta}$ be a lattice with generalized Arf invariant η, and assume that $v(\beta)$ is maximal and equals $v(2)$ (so that $v(\eta) \geq v(2)$). In this case we define the *class of minimal norms of* $M_{\alpha,\beta}$ to be the image of α in the set of fine classes of minimal norms arising from η.

Note that the condition on $v(\beta)$ implies that if the generalized (or fine) Arf invariant η of $M_{\alpha,\beta}$ is not of vanishing type then the class of minimal norms of $M_{\alpha,\beta}$ has valuation strictly smaller than $v(\eta) - v(2)$ if $v(\beta) > v(2)$, and its valuation equals precisely $v(\eta) - v(2)$ in case $v(\beta) = v(2)$.

The fact that the objects appearing in Definition 4.4 are well-defined, and the main classification result of this paper, are as follows:

Theorem 4.5. *The set of fine classes of minimal norms arising from each generalized Arf invariant η with $v(\eta) \leq 2v(2)$ is well-defined. Given a generalized Arf invariant η with $v(\eta) > v(2)$, the isomorphism classes of lattices $M_{\alpha,\beta}$ with generalized Arf invariant η and with primitive elements with norm in $2R$ (of maximal valuation) are characterized precisely by their fine Arf invariant and their classes of minimal norms.*

Proof. The set in question is defined as orbits under the action of the group $(R^*)^2(1 + \frac{4}{\tau}R_{AS})$, where τ represents the generalized Arf invariant η. We must thus show that taking another representative for η yields the same group. Now, η can be either odd, even, or exact, so that we have to consider the effect of adding to τ an element from $I_{v(\eta)}$, $J_{v(\eta)}$, or $4R_{AS}$ respectively.

Now, adding an element from $I_{v(\eta)}$ to τ is the same as dividing it by something from $1 + I_0$. The effect on $\frac{4}{\tau}R_{AS}$ is multiplication of R_{AS} by $1 + I_0$, which leaves it invariant by Lemma 3.2. In particular, the assertion for odd η follows. For even η it remains to consider the effect of adding λ^2 to τ, where $2v(\lambda) = v(\eta)$. The group $1 + \frac{4}{\tau+\lambda^2}R_{AS}$ will in general be different from $1 + \frac{4}{\tau}R_{AS}$, but we claim that it is contained in $(R^*)^2(1 + \frac{4}{\tau}R_{AS})$. Indeed, Proposition 3.8 shows that $\frac{\lambda^2}{\tau} \notin 1 + I_0$, so that $1 + \frac{\lambda^2}{\tau} \in R^*$ and every element of $1 + \frac{4}{\tau+\lambda^2}R_{AS}$ may be written as $1 + \frac{4}{\tau+\lambda^2}\rho[(1 + \frac{\lambda^2}{\tau})r]$ for some $r \in R$. But we may expand

$$\rho\left[\left(1 + \frac{\lambda^2}{\tau}\right)r\right] = \left(1 + \frac{\lambda^2}{\tau}\right)\rho(r) + \frac{\lambda^2}{\tau}\left(1 + \frac{\lambda^2}{\tau}\right)r^2$$

(a direct calculation using the definition of ρ), so that our element becomes $1 + \frac{4}{\tau}\rho(r) + \frac{4\lambda^2 r^2}{\tau^2}$. As $2v(\lambda) = v(\tau) = v(\eta) < 2v(2)$, we find that $\frac{2\lambda r}{\tau} \in I_0$ and $v(\frac{4\lambda r}{\tau}) > v(\frac{4\lambda^2 r^2}{\tau^2})$, so that dividing this element by $(1 + \frac{2\lambda r}{\tau})^2$ yields an element of $1 + \frac{4}{\tau}\rho(r) + I_{2v(2)-v(\tau)}$. But Lemma 3.2 implies that the latter expression takes the form $1 + \frac{4}{\tau}\rho(s)$ for some $s \in R$, so that our original expression equals $(1 + \frac{2\lambda r}{\tau})^2(1 + \frac{4}{\tau}\rho(s))$ and lies in $(R^*)^2(1 + \frac{4}{\tau}R_{AS})$ as desired. Interchanging the roles of τ and $\tau + \lambda^2$ now show that the groups arising from both numbers coincide, which proves that sets of fine classes of minimal norms arising from even η are also well-defined.

When the generalized Arf invariant η is exact, we need to verify that adding an element from $4R_{AS}$ to τ leaves the group $(R^*)^2(1 + \frac{4}{\tau}R_{AS})$ invariant. Hence we consider an element of the group $1 + \frac{4}{\tau+4\rho(h)}R_{AS}$ for some $h \in R$. Note that we may always replace h by $1 - h$, since they have the same ρ-image. The number $\frac{4\rho(h)}{\tau}$ cannot be in $1 + I_0$ by Proposition 3.11, so that $1 + \frac{4\rho(h)}{\tau} \in R^*$ and we write an element of our group as $1+\frac{4}{\tau+4\rho(h)}\rho[(1+\frac{4\rho(h)}{\tau})r]$. Using a similar expansion, the latter expression equals $1+\frac{4}{\tau}\rho(r)+\frac{16\rho(h)r^2}{\tau^2}$. Writing the two ρ-images explicitly, we get

$$1+\frac{4}{\tau}\big(r^2-r\big)+\frac{16r^2}{\tau^2}\big(h^2-h\big)=1+\frac{16r^2h^2}{\tau^2}+\frac{4r^2}{\tau}-\frac{4r}{\tau}\left(1+\frac{4rh}{\tau}\right).$$

We may assume, by replacing h by $1-h$ if necessary, that $1+\frac{4rh}{\tau}\in R^*$. When we divide this expression by $(1+\frac{4rh}{\tau})^2$, the sum of the first two terms gives an element of $1+I_0$ (which equals $1+\frac{4}{\tau}I_0$ since $\frac{4}{\tau}\in R^*$), and the remaining three terms become just $\frac{4}{\tau}\rho(\frac{r}{1+4rh/\tau})$. Invoking Lemma 3.2 again yields an element $s\in R$ such that the whole sum is just $1+\frac{4}{\tau}\rho(s)$, so that our original element equals $(1+\frac{4rh}{\tau})^2(1+\frac{4}{\tau}\rho(s))$ and lies in $(R^*)^2(1+\frac{4}{\tau}R_{AS})$. The symmetry between τ and $\tau+4\rho(h)$ now establishes the invariance of the group $(R^*)^2(1+\frac{4}{\tau}R_{AS})$ under this operation, so that the sets of fine classes of minimal norms are well-defined also for exact η. This proves the first assertion.

Now, Lemma 4.1 shows that isomorphic lattices of the form $M_{\alpha,\beta}$ with $v(\beta)\geq v(2)$ and $v(\alpha\beta)>v(2)$ have the same class of minimal norms, and that no finer invariant for the minimal norm exists. Moreover, part (*ii*) of Proposition 4.2 shows that the fine Arf invariant is also an invariant of isomorphism classes of such lattices. Conversely, assume that $M_{\alpha,\beta}$ and $M_{\gamma,\delta}$ have the same fine Arf invariant and the same class of minimal norms. In particular, the difference between the valuation of the (common) generalized Arf invariant η of these two lattices and $v(\alpha)$ coincides with its difference from $v(\gamma)$, so that we consider either the coarse classes of minimal norms in both lattices or the fine classes of minimal norms arising from η. Since the (appropriate) classes of α and γ coincide, Lemma 4.1 shows that $M_{\gamma,\delta}$ is isomorphic to $M_{\alpha,\mu}$ for some $\mu\in R$. Moreover, by part (*ii*) of Proposition 4.2 the lattice $M_{\alpha,\mu}$ has the same fine Arf invariant as $M_{\gamma,\delta}$ and $M_{\alpha,\beta}$, meaning that $\alpha\beta-\alpha\mu\in S$. If the fine (or generalized) Arf invariant vanishes then $\mu=\beta=0$ and we are done. Otherwise $v(\eta)\leq 2v(2)$, and we write the difference $\alpha\beta-\alpha\mu$ as t^2-2t. We claim that $2v(t)\geq v(\eta)$. Indeed, otherwise $v(t)<v(2)$ and all the elements $\alpha\mu$, $\alpha\beta$, and $2t$ have valuations larger than $v(t^2)$, so that the equality $\alpha\beta-\alpha\mu=t^2-2t$ cannot hold. Now, since $v(\eta)=v(\alpha\beta)\geq 2v(\alpha)$ we can write $t=\alpha b$ for $b\in R$ with $2v(b)\geq v(\frac{\beta}{\alpha})$ and obtain the equality $\mu=\beta+2b-\alpha b^2$. We claim that this equality implies an equality of the form $\mu=\beta+2a-\frac{\alpha a^2}{1-\alpha\beta}$ for some $a\in R$ with $2v(a)\geq v(\frac{\beta}{\alpha})$. Indeed, write $a=b+h$ in the desired equality, and using the given relation between μ, β, and b we obtain the equation $Ah^2+Bh+C=0$ with $A=-\frac{\alpha}{1-\alpha\beta}$ (of valuation $v(\alpha)$), $B=2(1-\frac{\alpha b}{1-\alpha\beta})$ (of valuation $v(2)$—recall that $t=\alpha b$ and $\alpha\beta$ are both in I_0), and $C=-\frac{\alpha^2b^2\beta}{1-\alpha\beta}$ (of valuation at least $v(\alpha)+2v(\beta)$ by the condition on b). The inequalities $v(\alpha\beta)=v(\eta)>v(2)$ and $v(\beta)\geq v(2)$ allow us to apply Lemma 1.4, and show that the valuation $v(\frac{C}{B})$ of the solution h is larger than $v(2)$. This proves the existence of an appropriate a, and Lemma 4.1 completes the proof of the theorem. $\square$

Since the proof of part (*iii*) of Proposition 4.2 shows that over an exact or vanishing generalized Arf invariant there exists only one fine Arf invariant, the result of Theorem 4.5 in these cases can be phrased as in the following

Corollary 4.6. (*i*) *Assume that $v(\beta) > v(2)$ and $v(\alpha) + v(\beta) \geq 2v(2)$. Then the class of α in $(R/2R)/(R^*)^2$ and the generalized Arf invariant η (the image of $\alpha\beta$ modulo $4R_{AS}$) characterize the isomorphism class of $M_{\alpha,\beta}$, where the vanishing of the former invariant implies the vanishing of the latter.* (*ii*) *If $v(\alpha) = v(\beta) = v(2)$ then the isomorphism classes of such lattices are characterized by the generalized Arf invariant η, and in case $\eta \neq 0$ (i.e., η is exact), also by the class of elements of $2R/(R^*)^2(1 + \frac{4}{\tau}R_{AS})$ (of valuation 2), where $\tau \in 4R$ is such that $\eta = \tau + 4R_{AS}$, containing all the norms of primitive elements in a lattice in this isomorphism class.*

Proof. Part (*i*) follows directly from Theorem 4.5. Part (*ii*) is obtained by combining Theorem 4.5 and Lemma 3.3. □

The case of a vanishing generalized Arf invariant (namely, isotropic lattices) of Theorem 4.5 and Corollary 4.6 reproduces the result of Proposition 3.4, though the latter holds over any valuation ring while Theorem 4.5 and Corollary 4.6 require the 2-Henselian property.

Once again, the lattices with classes of minimal norms of valuation 0 are decomposable. Such a lattice $M_{\alpha,\beta}$, with $\tau \in R$ representing the fine Arf invariant of $M_{\alpha,\beta}$, is isomorphic to the lattice $H_{\alpha,\tau}$ spanned by two orthogonal elements u and w of norms α and $\alpha(\tau-1)$: Indeed, by taking $\tau = \alpha\beta$ we find that $x = u$ and $y = \frac{u+w}{\alpha}$ form a basis for $H_{\alpha,\tau}$ as an isomorphic image of $M_{\alpha,\beta}$. Therefore Theorem 4.5 implies also the following

Corollary 4.7. *Let α and γ be elements in R^* and let τ and λ be elements in $I_{v(2)}$ representing generalized Arf invariants. The lattices $H_{\alpha,\tau}$ and $H_{\gamma,\lambda}$ are isomorphic if and only if $\tau - \lambda \in S$ and α and γ are in the same coarse class of minimal norms in $(R/2R)/(R^*)^2$.*

As above, the case $\tau = \lambda = 0$ in Corollary 4.7 yields Corollary 3.5 (under the 2-Henselianity assumption).

Note that Theorem 4.5 and Corollary 4.7 deal only with lattices whose generalized Arf invariants come from $I_{v(2)}$. Next we show that these results extend to generalized Arf invariants with valuation precisely $v(2)$ under some conditions on the 2-Henselian valuation ring R.

Proposition 4.8. *Assume that R satisfies either* (*i*) *$v(2)$ is odd,* (*ii*) *$\mathbb{F}$ is perfect, or* (*iii*) *ρ is surjective. Then all the lattices $M_{\alpha,\beta}$ with $\beta \in 2R$ having maximal valuation are classified by their fine Arf invariant and the appropriate class of minimal norms.*

Proof. Define $S^+ = \{t^2 - 2t \mid t \in R,\ 2v(t) \geq v(2)\}$. If we can show that S^+ is a subgroup of $2R$, then Definition 4.3 may be extended to introduce fine Arf invariants with valuation precisely $v(2)$, using classes in $2R/S^+$. Apart from this extension, there are two additional places in the proofs of Proposition 4.2 and Theorem 4.5 where we have used strict inequalities for our arguments. One is where for a generalized Arf invariant coming from $\alpha\beta \in I_{v(2)}$ and an element h with $2v(h) > v(2)$, the expression $\alpha\beta(h^2 - 2h)$ lies in $I_{2v(2)} \subseteq S$ (part (ii) of Proposition 4.2). The second place appears at the end of the proof of Theorem 4.5, where we concluded that if α and β are as above and b satisfies $2v(b) \geq v(\frac{\beta}{\alpha})$, then the sum of the valuations of $A = -\frac{\alpha}{1-\alpha\beta}$ and of $C = -\frac{\alpha^2b^2\beta}{1-\alpha\beta}$ is larger than $2v(2)$, so that a solution to the equation for a exists by Lemma 1.4. Note that the latter sum $v(AC)$ is just $v(\alpha^3b^2\beta)$.

Now, in case (i) the conditions $2v(t) \geq v(2)$ and $2v(h) \geq v(2)$ become strict inequalities since they compare the odd valuation $v(2)$ with an even valuation. Hence $S^+ = S$ is a group, and classes from $2R/S$ define fine Arf invariants which are invariants of isomorphism classes of lattices (and map to generalized Arf invariants as before). As for $v(\alpha^3b^2\beta)$, it is at least $v(\alpha^2\beta^2)$ since $2v(b) \geq v(\frac{\beta}{\alpha})$, hence $AC \in 4R$. But if $v(\alpha\beta) > v(2)$ then we already have $AC \in I_{2v(2)}$, while in the case of equality $v(\frac{\beta}{\alpha})$ is odd, the equality with $v(b)$ is strict, and again $AC \in I_{2v(2)}$. This proves for case (i). Hence we consider cases (ii) and (iii) under the additional assumption that $v(2)$ is even.

Case (ii) with even $v(2)$ is simple: As there are no generalized Arf invariants of even valuation $v(2)$ by Corollary 3.9, there is no need for any extension of the definitions, and all inequalities involving $v(\alpha\beta)$ remain strict. In case (iii) we consider again the equation $h^2+2(t-s-1)h+2s^2-2ts = 0$ for h in the proof of part (i) of Proposition 4.2, where now s and t give rise to elements from S^+. By writing $h = 2(1-t+s)g$ this equation becomes $g^2 - g + \frac{s^2-st}{2(1-t+s)^2} = 0$ (recall that s^2 and st are in $2R$ as above), and this Artin–Schreier equation has a solution by our assumption on ρ and Lemma 3.2. Moreover, as $S \cap 4R = 4R_{AS}$ is the full ideal $4R$ in this case, the conditions $v(\alpha\beta) \geq v(2)$ and $2v(h) \geq v(2)$ are sufficient for $\alpha\beta(h^2 - 2h)$ to be in $4R \subseteq S$. Hence S^+ is a group, fine Arf invariants of valuation $v(2)$ are well-defined, and they are preserved under isomorphism of lattices. Finally, the equation for a can be transformed by similar means to an Artin–Schreier equation looking for a pre-image of $\frac{\alpha^3b^2\beta}{4(1-\alpha\beta-\alpha b)}$, which again exists under our assumption. This completes the proof of the proposition. □

We remark that extending Corollary 4.7 to the cases (i) or (iii) in Proposition 4.8 requires using the fine classes of minimal norms arising from the common generalized Arf invariant arising from τ and λ in case $v(\lambda) = v(\tau) = v(2)$, rather than the coarse classes of minimal norms appearing in that corollary. The fact that there are no even generalized Arf invariants in case (ii) of Proposition 4.8 agrees, for the case of R is a (complete) discrete valuation ring, with the parity condition on the weight and norm ideals in Section 93 of [13].

On the other hand, if none of the conditions of Proposition 4.8 is satisfied, then S^+ is no longer a group, but generalized Arf invariants of valuation $v(2)$ exist. Therefore, an appropriate definition of fine Arf invariants of valuation $v(2)$, which will be preserved under isomorphisms, requires much more care and will probably be more involved. Attempts to extend to generalized Arf invariants of valuation smaller than $v(2)$ encounter more severe difficulties (as no group structure is expected there), and will be left for future research. However, we point out one fact that arises from the proof of Lemma 4.1 in this more general case: If $\delta - \beta$ lies in $I_{2v(2)-v(\alpha)}$ then $M_{\alpha,\beta} \cong M_{\alpha,\delta}$. Indeed, putting $s = 0$ and $c = 1$ there (i.e., $z = x$) shows that the vector w has norm $\beta + 2a - \frac{\alpha a^2}{1-\alpha\beta}$ (note that the maximality of β shows that $1 - \alpha\beta$ cannot be in I_0, by Proposition 3.8). As comparing this value to δ yields a quadratic equation in which the sum of the valuations of $A = -\frac{\alpha}{1-\alpha\beta}$ and $C = \beta - \delta$ is larger than twice the valuation of $B = 2$, Lemma 1.4 yields a solution a to this equation, which proves the assertion. Moreover, the assumption that $v(\beta) \geq v(\alpha)$ was not used in this argument, so that we also deduce $M_{\alpha,\beta} \cong M_{\gamma,\beta}$ if $\gamma - \alpha \in I_{2v(2)-v(\beta)}$. This fact will be useful in completing the classification for lattices over $\mathbb{Z}_2[\sqrt{2}]$ in Subsection 4.3 below.

4.3. Relations to quadratic forms and examples

A notion closely related to (symmetric) bilinear forms, which has not appeared in this paper yet, is the notion of quadratic forms. Recall that a *quadratic form* on an R-module M is a map $q : M \to R$ which satisfies $q(rx) = r^2x^2$ for all $r \in R$ and $x \in M$, and such that the map taking x and y in M to $q(x + y) - q(x) - q(y)$ is a bilinear form on M (this is the *bilinear form coming from* q). We denote this bilinear form $\varphi(q)$, so that we have a map $\varphi = \varphi_M$ from the set of quadratic forms on M to the set of bilinear forms on M. In case $2 \in R^*$, every bilinear form comes from a unique quadratic form, namely $q(x) = \frac{x^2}{2}$. Hence φ is a canonical bijection. If $2 \notin R^*$ but is not a zero-divisor in R (e.g., $2 \neq 0$ and R is an integral domain), then φ is injective, but may not be surjective. This is so, since we can localize by 2 (making φ bijective again), but some bilinear forms which are R-valued will require the quadratic form to take values in the localization. Those lattices in which the bilinear form comes from a quadratic form via φ are the lattices called *even* in the terminology of [17] and others. But other lattices exist: E.g., $M_{\alpha,\beta}$ is even precisely when α and β are both in $2R$, i.e., the generalized (or equivalently fine) Arf invariant is exact or vanishing and the class of minimal norms comes from $2R$. In case $2 = 0$, however, this map φ is in general neither injective nor surjective (this is the map considered in [1] for R a field of characteristic 2). Hence a quadratic form on a module over an integral domain yields more information than the one obtained using the bilinear form arising as its φ-image alone only if the integral domain in question has a fraction field of characteristic 2.

The last assertion of Corollary 4.6 shows the relation of exact and vanishing generalized Arf invariants to the classical Arf invariants: Any field $\mathbb{F}$ of characteristic 2 is the quotient field of a 2-Henselian valuation ring R whose fraction field $\mathbb{K}$ has characteristic 0 (for an example of such a ring in which the valuation is complete and discrete, take R to be the ring $W(\mathbb{F})$ of Witt vectors over $\mathbb{F}$—see, e.g., Section II.6 of [16] for more details on this construction). Any non-degenerate (or *fully regular* in the terminology of [1]) quadratic form of dimension 2 over $\mathbb{F}$ is isomorphic to a form $q : (r, s) \mapsto \lambda r^2 + rs + \mu s^2$ for some λ and μ in $\mathbb{F}$ (see Theorem 2 of [1]—note that by normalizing one of the basis elements we can make the product 1, i.e., we can take $b_i = 1$ for all i). Let α and β be elements of $2R$ such that $\frac{\alpha}{2} + I_0 = \lambda$ and $\frac{\beta}{2} + I_0 = \mu$. Then the quadratic form q can be seen as the reduction modulo I_0 of the map $z \mapsto \frac{z^2}{2}$ for $z = rx + by \in M_{\alpha,\beta}$. If $M_{\alpha,\beta} \cong M_{\gamma,\delta}$ for some γ and δ in $2R$ then q is isomorphic over $\mathbb{F}$ to the quadratic form $Q : (r, s) \mapsto \varphi r^2 + rs + \psi s^2$ for $\varphi = \frac{\gamma}{2} + I_0$ and $\psi = \frac{\delta}{2} + I_0$ (by reducing the isomorphism modulo I_0). On the other hand, Corollary 4.6 implies that the isomorphism class of $M_{\alpha,\beta}$ is independent of the choice of $\alpha \in 2\lambda + I_{v(2)}$ and $\beta \in 2\mu + I_{v(2)}$. This implies that if q and Q above are isomorphic over $\mathbb{F}$ then $M_{\alpha,\beta} \cong M_{\gamma,\delta}$: Indeed, lifting the isomorphism over $\mathbb{F}$ to any map over R yields an isomorphism between $M_{\alpha,\beta}$ and $M_{\kappa,\nu}$ for $\kappa \in 2\varphi + I_{v(2)}$ and $\nu \in 2\psi + I_{v(2)}$, and the previous assertion implies $M_{\kappa,\nu} \cong M_{\gamma,\delta}$. Thus, isomorphism classes of fully regular quadratic forms of rank 2 over $\mathbb{F}$ correspond to isomorphism classes of lattices $M_{\alpha,\beta}$ over R, where α and β are in $2R$ (i.e., of even lattices $M_{\alpha,\beta}$). Now, exact or vanishing generalized Arf invariants are "4 times" the Arf invariant Δ defined in [1] (this means $4\Delta \in 4R/4R_{AS}$ for $\Delta \in \mathbb{F}/\mathbb{F}_{AS}$), and the set of numbers $\frac{z^2}{2} + I_0$ obtained from primitive $z \in M_{\alpha,\beta}$ is precisely the set of squares of non-zero elements of the odd part of the Clifford algebra of q over $\mathbb{F}$. Since Lemma 3.3 implies that this set is either $\mathbb{F}$ or an orbit in $\mathbb{F}/(\mathbb{F}^*)^2(1 + \frac{4}{\tau}\mathbb{F}_{AS})$ (after division by 2 and dividing modulo I_0), and the remainder of the structure of the Clifford algebra is determined by the condition that the two basis elements x and y are chosen such that $(x, y) = 1$, Corollary 4.6 implies Theorem 3 of [1] (in fact, this normalization shows that applying ρ to the element xy of the Clifford algebra yields the Arf invariant Δ, the condition about Δ in that theorem is redundant).

The results of Section 3 as well as this section thus generalize the classical assertions from [1] to many lattices in which the bilinear form does not necessarily come from a quadratic form. It seems likely that a similar argument can treat binary quadratic forms over some valuation rings in which $2 = 0$ and which are not fields—note that the results of this section are contained in Proposition 3.4 in case $2 = 0$ since we assume here $\beta \in 2R$ throughout. We leave this question for future research.

We now use our results in order to classify the unimodular rank 2 lattices over two rings. Recall that every such lattice is isomorphic to some lattice $M_{\alpha,\beta}$ with $v(\beta) \geq v(\alpha)$, and this lattice is decomposable if and only if α is invertible, a case in which the lattice is isomorphic to some lattice $H_{\alpha,\tau}$ (see the paragraph preceding Corollary 4.7). We start with $R = \mathbb{Z}_2$, the ring of 2-adic integers. As $\rho(\mathbb{F}_2) = 0$, we have $R_{AS} = I_0 = 2R$. All the lattices of the form $M_{\alpha,\beta}$ admit primitive vectors with norms of maximal valuations, by Proposition 3.10 or the finiteness of valuations smaller than $v(2)$. There are three possible generalized Arf invariants: 0 (vanishing), $4+8R$ (exact), and $2+4R$ (odd). Moreover, the set $(R/2R)/(R^*)^2$ of coarse classes of minimal norms consists of two elements, represented by 0 and 1, the latter having valuation 0. The condition $2v(t) > v(2)$ in the definition of S implies $2|t$ hence $S = 8R$. Moreover, both conditions (i) and (ii) of Proposition 4.8 are satisfied, so that we can classify all the $\mathbb{Z}_2$-lattices $M_{\alpha,\beta}$ using our method. The isotropic lattices are $M_{0,0}$ (the hyperbolic plane) and $M_{1,0}$ (which is isomorphic to $H_{1,0}$, hence generated by 2 orthogonal vectors having opposite norms). Over the exact generalized Arf invariant lies the fine Arf invariant $4+8R$. A lattice having this fine Arf invariant with $v(\beta)>v(2)$ must have 1 in its coarse class of minimal norms. Such a lattice must therefore be isomorphic to $M_{1,4}$, which can be generated by orthogonal elements of norms 1 and 3 as its isomorph $H_{1,4}$. The multiplicative group corresponding to this generalized Arf invariant is just $1+\frac{4}{4}R_{AS}=1+2R=\mathbb{Z}_2^*$. There is thus only one fine class of minimal norms of valuation 1 arising from this generalized Arf invariant, yielding the lattice $M_{2,2}$. The remaining fine Arf invariants are $2+8R$ and $-2+8R$, lying over the odd generalized Arf invariant $2+4R$. Both have valuation $v(2)=1$, so that we have to consider the fine classes of minimal norms of valuation 0 corresponding to $2+4R$. The group by which we divide is $1+\frac{4}{2}R_{AS}=1+4R$, so that there are two such classes, represented by 1 and -1. The invariants 1 and $2+8R$ yield a lattice isomorphic to $M_{1,2}$, which is generated by two orthogonal elements of norm 1 like $H_{1,2}$. With the invariants -1 and $2+8R$ comes the lattice $M_{-1,-2}$, an orthogonal basis of which can be taken with both norms -1 (consider $H_{-1,-2}$). Taking now the class with 1 and fine Arf invariant $-2+8R$ yields the lattice $M_{1,-2}$, a basis of its isomorph $H_{1,-2}$ has norms 1 and -3. The last lattice, with invariants -1 and $-2+8R$, must be isomorphic to $M_{-1,2}$, which, being isomorphic to $H_{-1,2}$, has an orthogonal basis with elements of norms -1 and 3. One can easily verify that these results reproduce the results of [8] for rank 2 unimodular 2-adic lattices, since $-3\equiv 5(\mathrm{mod}\ 8)$, $-1\equiv 7(\mathrm{mod}\ 8)$, and the lattice $M_{-1,-2}$ can be written as $M_{3,-2}$ (since $-1\equiv 3(\mathrm{mod}\ 4)$) and the isomorphic lattice $H_{3,-2}$ has an orthonormal basis consisting of two norm 3 vectors.

We now turn to present the explicit picture our results yield for the ring $R=\mathbb{Z}_2[\sqrt{2}]$. The fine Arf invariants we obtain have valuation larger than $v(2)$ (Corollary 3.9 or condition (*ii*) of Proposition 4.8), and once again $R_{AS}=I_0$, which here equals $\sqrt{2}R$. Proposition 3.10 (or the fact that only finitely many positive elements of Γ are smaller than $v(2)=2$) shows again that in every lattice $M_{\alpha,\beta}$ we can take β to have maximal valuation. The elements in $1+4\sqrt{2}R$ are squares, and $(R^*)^2/(1+4\sqrt{2}R)$ consists of one additional non-trivial class, which is represented by $(1+\sqrt{2})^2=3+2\sqrt{2}$. A generalized Arf invariant of a lattice can be 0 (vanishing), $4+4\sqrt{2}R$ (exact), $2\sqrt{2}+4R$ (odd), or $\sqrt{2}+2R$ (odd). Fine Arf invariants are defined only above the first three generalized Arf invariants. The group S is based on elements satisfying $2v(t)>v(2)$, which means $2|t$ hence $S=4\sqrt{2}R$. As the action of $(R^*)^2\subseteq 1+2R$ on $R/2R$ is trivial, there are 4 coarse classes of minimal norms, represented by 0, $\sqrt{2}$, 1, and $1+\sqrt{2}$, with valuations ∞, 1, 0, and 0 respectively. Hence there are 4 isomorphism classes of isotropic R-lattices, in which the generalized and fine Arf invariants are vanishing, namely $M_{0,0}$, $M_{\sqrt{2},0}$, $M_{1,0}$, and $M_{1+\sqrt{2},0}$. Considering the exact generalized and fine Arf invariant $4+4\sqrt{2}R$, as all the non-zero coarse classes of minimal norms have valuation smaller than $v(2)=2$, we obtain 3 isomorphism classes of non-even lattices having this fine Arf invariant, which are represented by $M_{\sqrt{2},2\sqrt{2}}$, $M_{1,4}$, and $M_{1+\sqrt{2},4}$ (recall that $\frac{4}{1+\sqrt{2}}=4\sqrt{2}-4$ is congruent to 4 modulo $4\sqrt{2}R$). When considering fine classes of minimal norms arising from this generalized Arf invariant, the acting group is just $1+\sqrt{2}R=R^*$, so that there is only one element of valuation 2 in this set, giving rise to the lattice $M_{2,2}$. The generalized Arf invariant $2\sqrt{2}+4R$ appears as the image of two fine Arf invariants, one being $2\sqrt{2}+4\sqrt{2}R$, and the other one is $2\sqrt{2}+4+4\sqrt{2}R$. The isomorphism classes of lattices $M_{\alpha,\beta}$ with $v(\beta)\geq 3$ having these fine Arf invariants are represented by the coarse classes of minimal norms 1 and $1+\sqrt{2}$. The corresponding lattices are (up to isomorphism) $M_{1,2\sqrt{2}}$ and $M_{1+\sqrt{2},2\sqrt{2}+4}$ with the fine Arf invariant $2\sqrt{2}+4\sqrt{2}R$, while $M_{1,2\sqrt{2}+4}$ and $M_{1+\sqrt{2},2\sqrt{2}}$ have the fine Arf invariant $2\sqrt{2}+4+4\sqrt{2}R$. The fine classes of minimal norms arising from the generalized Arf invariant $2\sqrt{2}+4R$ are obtained modulo the action of the group $1+2R$ (which already contains $(R^*)^2$). As the classes of valuation 1 are represented by $\sqrt{2}$ and $2+\sqrt{2}$, we obtain the two additional lattices $M_{\sqrt{2},2}$ and $M_{2+\sqrt{2},2+2\sqrt{2}}$ with the fine Arf invariant $2\sqrt{2}+4\sqrt{2}R$, together with the lattices $M_{\sqrt{2},2+2\sqrt{2}}$ and $M_{2+\sqrt{2},2}$ having the fine Arf invariant $2\sqrt{2}+4+4\sqrt{2}R$. Theorem 4.5 shows that these 16 isomorphism classes of R-lattices are distinct, and every unimodular R-lattice of rank 2 admitting a primitive vector of norm in $2R$ belongs to one of these isomorphism classes.

We end this section by completing the classification of those unimodular rank 2 lattices over $R=\mathbb{Z}_2[\sqrt{2}]$ to which Theorem 4.5 does not apply. These lattices all have generalized Arf invariant $\sqrt{2}+2R$, and they are all decomposable. By the remark at the end of Subsection 4.2 they take the form $M_{\alpha,\beta}$ where α can be taken from any set of representatives for $R^*/(1+4R)$ (there are 8 such classes) and for β one may use any set of representatives for the classes in $\sqrt{2}R/4\sqrt{2}R$ having valuation 1 (again 8 such classes). We identify, for the moment, these sets of representatives with the corresponding classes, so that the two operations we introduce below on these classes may be considered to be normalized to always take representatives to representatives. There are 64 pairs in $R^*/(1+4R)\times\sqrt{2}R^*/(1+4R)$, and there are three operations on these pairs such that two pairs are connected through these operations if and only if they yield isomorphic lattices. The first operation takes α and β to $r^2\alpha$ and $\frac{\beta}{r^2}$ for $r\in R^*$. This operation has exponent 2 here since $(R^*)^2/(1+4R)$ has order 2. In addition, we may replace α by $\alpha+2s+\beta s^2$ for $s\in R$, and β by $\frac{\beta}{(1+\beta s)^2}$. The valuations of α and β and the fact that we consider elements modulo multiplication from $1+4R$ show that this operation depends only on the class of s in $\mathbb{F}=\mathbb{F}_2$, yielding another operation of order 2. In addition, we can take β to $\beta+2t+\alpha t^2$ and α to $\frac{\alpha}{(1+\alpha t)^2}$ for $t\in R$ with $v(t)>0$. By letting γ^2 represent the non-trivial class in $(R^*)^2/(1+4R)$ and choosing $s=-\alpha$ and $t=-\beta$ to represent the non-trivial choices of the two latter operations, we find that our operations, which we denote ζ, σ, and τ, send the pair (α,β) to $(\alpha\gamma^2,\beta\gamma^2)$, $(\alpha(\alpha\beta-1),\beta\gamma^2)$, and $(\alpha\gamma^2,\beta(\alpha\beta-1))$ respectively. Working modulo $1+4R$ one sees that ζ is central, all three have order 2, and the commutator of σ and τ is ζ. Hence these three operations generate a dihedral group of order 8, which operates on our set of 64 pairs without fixed points. It follows that there are 8 orbits, and representatives for these orbits can be taken to be $M_{1,\sqrt{2}}$, $M_{1,\sqrt{2}+4}$, $M_{1,-\sqrt{2}}$, $M_{1,-\sqrt{2}+4}$, $M_{-1,\sqrt{2}}$, $M_{-1,\sqrt{2}+4}$, $M_{-1,-\sqrt{2}}$, and $M_{-1,-\sqrt{2}+4}$ (i.e., an R-lattice with generalized Arf invariant $\sqrt{2}+2R$ is isomorphic to precisely one of these 8 lattices). One can find ad-hoc invariants: The closest analogue of the fine Arf invariant would be elements in $\sqrt{2}+2\sqrt{2}R$ modulo $4\sqrt{2}R$, but not for every lattice $M_{\alpha,\beta}$ the product $\alpha\beta$ lies in this set (sometimes one has to switch to an isomorphic lattice), and the choice of the elements $\sqrt{2}+2\sqrt{2}R$ rather than $\sqrt{2}+2+2\sqrt{2}R$ does not have an immediate extension to the general case. As for classes of minimal norms (which depend on $\alpha\beta$), 1 and $1+\alpha\beta$ (and their images after multiplying by squares) lie in one class while -1 and $-1+\alpha\beta$ (times squares) lie in another class, and this situation does not seem to have a clear description of the sort of Definition 4.4. This illustrates how the existence of norms in $2R$ simplifies our method substantially.

5. Towards canonical forms in residue characteristic 2

In this section we derive some relations between lattices of 2-Henselian valuation rings in which $v(2)>0$. The idea is to give canonical representatives for isomorphism classes of such lattices. This goal remains far out of reach, but we give some results toward it.

The Jordan decomposition of a lattice M, given in Proposition 1.2, is, in this case, not unique. However, the different Jordan decompositions yielding isomorphic lattices do have some properties in common:

Proposition 5.1. *Let $M=\bigoplus_{k=1}^{t}M_k$ and $M=\bigoplus_{k=1}^{t}N_k$ be two Jordan decompositions of the same lattice M, with $v(M_k)=v(N_k)$ for every k (allowing empty components if necessary). Then the uni-valued lattices N_k and M_k have the same rank (in particular, no empty components are needed in two such presentations), and one of them has a diagonal basis if and only if the other one has such a basis.*

Proof. We use the same method as in Section 93 of [13]. Take some $0\leq v\in\Gamma$, and consider the subset M_v of all elements $x\in M$ such that $v(x,y)\geq v$ for every $y\in M$. We claim that this is a sub-lattice of M. Note that since R is not necessarily Noetherian (because the valuation is not discrete), the assertion does not follow from the fact that M^v is a submodule of M: Indeed, the condition $v(x,y)\geq v$ can be interpreted as (x,y) being in the principal ideal J of elements with valuation at least v, and if we apply this condition for a non-principal ideal J then the resulting subset is not a finitely generated submodule of M. Now, if M decomposes as $L\oplus N$ then M_v decomposes as $L_v\oplus N_v$, so that in particular M_v decomposes either as $\bigoplus_{k=1}^{t}M_{k,v}$ or as $\bigoplus_{k=1}^{t}N_{k,v}$. Let $a\in R$ with $v(a)=v$. If N is uni-valued, say $N=L(\sigma)$ with L unimodular and $v(\sigma)=v(N)$, then $N_v=N$ if $v(N)\geq v$ and $N_v=\frac{a}{\sigma}N$ if $v(N)\leq v$: The first assertion is obvious, and the second assertion holds because any primitive element $x\in N$ satisfies $\{(x,y)\mid y\in N\}=\sigma R$ since N is uni-valued. It follows that $M_{k,v}$ (or $N_{k,v}$) are lattices for every k, and M_v is a sub-lattice of M.

The lattice M_v has valuation at least v. Moreover, its decompositions as $\bigoplus_{k=1}^{t}M_{k,v}$ or $\bigoplus_{k=1}^{t}N_{k,v}$ are decompositions to uni-valued lattices (but not necessarily in increasing valuation orders). To see this, we examine N_v for the uni-valued lattice $N=L(\sigma)$ again.

If $v(N) \geq v$ then $N_v = N = L(\sigma)$ is uni-valued with valuation $v(N) = v(\sigma)$, while if $v(N) \leq v$ then $N_v = \frac{a}{\sigma}N$ is isomorphic to $L(\frac{a^2}{\sigma})$ and has valuation $2v - v(N)$. In particular, $v(N_v) > v$ unless $v(N) = v$. Consider now $M_v(\frac{1}{a})$. The inequality $v(M_v) \geq v = v(a)$ shows that it is still a lattice, and we take the tensor product of this lattice with $\mathbb{F}$. The images of all the components $M_{k,v}$ or $N_{k,v}$ with $v(M_k) = v(N_k) \neq v$ become degenerate in this $\mathbb{F}$-valued bilinear form, and a maximal non-degenerate subspace of this $\mathbb{F}$-vector space arises from M_k or N_k in case $v(M_k) = v(N_k) = v$. In particular the ranks of M_k and N_k coincide for each k, and Corollary 1.3 shows that each of them has an orthogonal basis if and only if some element of $M_v(\frac{1}{a})$ has a norm not in I_0. This proves the proposition. □

A more detailed examination of the proof of Proposition 5.1 allows one to derive a stronger assertion. Define, for each $2 \leq k < t$, the element u_k of Γ to be $\min\{v(M_k) - v(M_{k-1}), v(M_{k+1}) - v(M_k)\} > 0$, and for the extremal values $k = 1$ and $k = t$ let $u_1 = v(M_2) - v(M_1)$ and $u_t = v(M_t) - v(M_{t-1})$. Replacing $\mathbb{F} = R/I_0$ by R/b_kR with $b_k \in I_0$ having valuation u_k shows that the images of $M_k(\frac{1}{a})$ and $N_k(\frac{1}{a})$ modulo b_kR are isomorphic. This implies

Corollary 5.2. *(i) The two sets $\{x^2 + ab_kR \mid x \in M_k\}$ and $\{y^2 + ab_kR \mid y \in N_k\}$ are the same subset of R/ab_kR. (ii) If $u_k > 2v(2)$ then $M_k \cong N_k$.*

Proof. Part (i) follows directly from the isomorphism $M_k(\frac{1}{a}) \cong N_k(\frac{1}{a})$ modulo b_kR (alternatively, this set is just the images of all norms from M_v modulo ab_kR, and it is contained in aR/ab_kR). Part (ii) is a consequence of this isomorphism and Theorem 1.5. □

In fact, if $2 \in R^*$ then the condition $u_k > 2v(2)$ is satisfied for any k. Thus, Corollary 5.2 yields another proof of Theorem 2.4.

We shall define an order on the set of Jordan decompositions of lattices, together with explicit forms of the components, in which one such Jordan decomposition (with additional data) is larger than another one if it is more canonical in the sense explained below. The idea is to define certain unimodular components to be more canonical than others, and certain forms of such a component as more canonical than other forms of the same component. After fixing σ_v for every v, the more canonical uni-valued components of valuation v are the more canonical unimodular ones with the bilinear form multiplied by σ_v. For a general lattice M, we say that the Jordan decomposition $\bigoplus_{k=1}^t M_k$ of M is more canonical than $\bigoplus_{k=1}^t N_k$ if there exists some $1 \leq l \leq t$ such that $M_k = N_k$ for all $k < l$ and M_l is more canonical than N_l. A canonical form of a lattice M would be a Jordan decomposition of M, with the components given in a specific form, which is more canonical than any other Jordan decomposition of M or any other expression for the components.

Before we give the details, we present the case $R = \mathbb{Z}_2$ considered in [8]. In this case the unimodular components have symbols resembling those arising from lattices over $\mathbb{Z}_p$ for odd p. The symbols take the form $1_t^{\varepsilon n}$ or $1_{II}^{\varepsilon n}$, where n is again the rank and ε is a Legendre symbol related to the discriminant of the lattice. The additional index t denotes an *odd* (or *properly primitive* in the terminology of [8] and others) component, admitting an orthonormal basis in which $t \in \mathbb{Z}/8\mathbb{Z}$ is the image of the sum of the norms of the elements of such a basis. On the other hand, an index II means that the component is *even* (or *improperly primitive*), i.e., admitting no orthonormal basis (see Corollary 1.3). The parameter λ of [8] equals $\varepsilon \cdot (-1)^{\frac{(n-t-4)(n-t-6)}{8}}$ in this notation. Uni-valued lattices have symbols $(2^k)_t^{\varepsilon n}$ or $(2^k)_{II}^{\varepsilon n}$ (standing for the unimodular lattice $1_t^{\varepsilon n}$ or $1_{II}^{\varepsilon n}$ with the bilinear form multiplied by 2^k), and a Jordan decomposition of a general 2-adic lattice is a product of such expressions (like for p-adic lattices for odd p), yielding again a symbol for the lattice (with the chosen Jordan decomposition). However, in this case different symbols can give rise to isomorphic lattices (or equivalently, two different Jordan decompositions of the same lattice may yield different symbols for the same lattice). Now, [8] considers a rank 1 lattice over $R = \mathbb{Z}_2$ representing $(R^*)^2 = 1 + 8\mathbb{Z}_2$ to be more canonical than the other unimodular rank 1 lattices, and $M_{0,0}$ (whose generalized Arf invariant is 0 hence is vanishing) to be more canonical than $M_{2,2}$ (with exact generalized Arf invariant $4 + 8\mathbb{Z}_2$). Moreover, here $\Gamma = \mathbb{Z}$, and for $0 \leq v \in \Gamma$ we take $\sigma_v = 2^v$. [8] shows how to define the order of being more canonical on all possible Jordan decompositions, and the canonical form of a lattice M appearing in Theorem 1 of [8] is the Jordan decomposition of M which is the most canonical one in this order. We remark that the order depends on the (arbitrary) choice, which of $3 + 8\mathbb{Z}_2$ and $7 + 8\mathbb{Z}_2$ is more canonical, a choice which is harder to generalize in the arguments below (a choice of similar type appears also in the classification of unimodular rank 2 lattices over $R = \mathbb{Z}_2[\sqrt{2}]$ having generalized Arf invariant $\sqrt{2} + 2R$ at the end of Subsection 4.3).

We now define when one form of a unimodular lattice is more canonical than another form, for lattices over a 2-Henselian valuation ring R in which $v(2) > 0$. First, a canonical form is based either on an orthogonal basis (if it exists) or of a direct sum of lattices of the form $M_{\alpha,\beta}$ with α and β in I_0 (the proof of Corollary 1.3 shows that such a form always exists for a unimodular lattice). In order to define the further relations in the order, we say that an element $f \in R^*$ is *closer to 1* than $g \in R^*$ if $v(f - 1) > v(g - 1)$. Now, one form of a lattice is more canonical than another form of the same lattice (or from a form of a different lattice) if it has discriminant closer to 1. If the lattice admits an orthogonal basis, then one orthogonal basis is more canonical than another if it contains more elements of norms in $1 + I_0$. If two bases have the same number of elements with norms in $1+I_0$, we order the base such that the elements whose norms are closer to 1 come first. Then the basis x_j, $1 \leq j \leq n$ is more canonical than y_j, $1 \leq j \leq n$ if there exists some $1 \leq k \leq n$ such that x_k^2 is closer to 1 than y_k^2 and $v(x_j^2 - 1) = v(y_j^2 - 1)$ for all $j < k$. In particular, an orthogonal basis containing a maximal set of elements of norm precisely 1 will be more canonical than a basis not having this property. For a lattice of the form $\bigoplus_j M_{\alpha_j,\beta_j}$, we choose the order such that the valuations of generalized Arf invariants are decreasing. Then one form is more canonical than another using a condition similar to the orthogonal base case, with "x^2 being closer to 1" replaced by "the generalized Arf invariant having higher valuation". For two unimodular lattices given in a certain form, we call one of them more canonical than the other according to the same rules.

Let L be a unimodular lattice over R (a 2-Henselian valuation ring with $v(2)>0$) having an orthogonal basis. Using the argument of Section 1, we find that the reduction of L modulo I_0 decomposes as the orthogonal direct sum of elements of norms $1+I_0$, and an $\mathbb{F}$-lattice in which no norm equals $1+I_0$. Lifting this basis to a basis of L and altering by elements of I_0, we obtain an orthogonal basis x_j, $1\leq j\leq n$ for M in which $x_j^2\in 1+I_0$ for $j\leq l$, and no combination of x_j with $l+1<j\leq n$ has a norm in $1+I_0$. If $\mathbb{F}$ is perfect then any non-zero norm is a square times an element of $1+I_0$, so that the reduction can always be taken orthogonal and $l=n$. If M is a lattice with Jordan decomposition $M=\bigoplus_{k=1}^t M_k$ such that $M_1=L$, then mixing with the components M_k of higher valuation cannot yield norms from $\bigoplus_{j=l+1}^n Rx_j\oplus\bigoplus_{k>1} M_k$ which are in $1+I_0$, hence cannot render our form of $L=M_1$ more canonical.

We now turn to unimodular rank one components generated by an element with a norm in $1+I_0$. Recall that a more canonical form for such a lattice will be based on a generator x whose norm is such that $v(x^2-1)$ is large. Now, if we can have a most canonical form for such a lattice (i.e., $x^2=1+r$ with the maximal possible $v(r)$, which is thus positive) then either $r=0$, $v(r)<2v(2)$ and is odd, $v(r)<2v(2)$ is even and r is not in $\sigma^2R^2+I_{v(r)}$ for $\sigma\in R$ with $2v(\sigma)=v(r)$, or $v(r)=2v(2)$ and r is not in $4R_{AS}$. Indeed, if $v(r)>2v(2)$ then x^2 is a square by Lemma 1.4. Otherwise, we compare $1+r$ to $c^2(1+r)$, c has to be $1+h$ for $h\in I_0$ with $2v(h)\geq v(r)$, and considerations like those presented in Section 3 prove the assertion.

The first step towards a canonical form is provided by the following

Proposition 5.3. *Let M be a unimodular lattice generated by two orthogonal elements x and y, whose norms are $1+r$ and $1+s$ respectively. Assume that $v(s)\geq v(r)>0$, $v(s)$ is maximal, and r is such that $v(r)$ is maximal among the norms of primitive generators of $(Ry)^\perp$. If $v(r)$ is smaller than both $v(s)$ and $v(2)$ then the generalized Arf invariant which r represents is an invariant of the lattice. If $v(r)+v(s)>2v(2)$ then M is isomorphic to a lattice spanned by two orthogonal elements of norms 1 and $(1+r)(1+s)$ respectively, hence $s=0$ by maximality. If $s\neq 0$ but $v(s)$ is maximal (and $v(s)>0$) then r and s satisfy the conditions of Proposition 3.8 or 3.11 with $\alpha=r$ and $\beta=s$.*

Proof. For any $t\in R$, the elements $x+(1+r)ty$ and $y-(1+s)tx$ are orthogonal and have norms $(1+r)[1+t^2(1+r)(1+s)]$ and $(1+s)[1+t^2(1+r)(1+s)]$ respectively. We take only t which is not in $1+I_0$, so that these vectors are primitive and generate M. We can thus divide these elements by $1+t$, and obtain generators of M having norms $1+u$ and $1+w$ with

$$u=\frac{t^2(1+s)(r^2+2r)+r-2t+st^2}{(1+t)^2},\qquad w=\frac{t^2(1+r)(s^2+2s)+s-2t+rt^2}{(1+t)^2}.$$

Every presentation of M with an orthogonal basis is obtained in this way, up to multiplying $1+u$ and $1+w$ by elements from $(R^*)^2$: This follows directly from primitivity and orthogonality. We are looking for isomorphic presentations of M with $v(w) \geq v(s)$. Hence if $v(r) < v(s)$ we take t either with $2v(t) \geq v(\frac{s}{r}) > 0$ or $v(t) \geq v(\frac{2}{r}) > 0$. It follows that u represents the same generalized Arf invariant as r, and by the usual maximality argument this generalized Arf invariant is an invariant of the isomorphism class of this lattice. If $v(r) + v(s) > 2v(2)$ (hence $v(s) > v(2)$) then the equation $w = 0$ is quadratic in t, with A of valuation at least $v(r)$ and with $B = -2$ and $C = s$. Lemma 1.4 gives a solution t of valuation $v(\frac{s}{2}) > 0$ to this equation, so that $w = 0$ can indeed be obtained. The evaluation of $1+u$ as $(1+r)(1+s)$ is carried out either using the equation for t or using discriminant considerations. Now assume that $s \neq 0$ and $v(s)$ is maximal (so that no element of M has norm precisely 1). The maximality of s implies that $v(s - 2t + rt^2) \leq v(s)$ for every $t \in R \setminus (1 + I_0)$, since the denominator in the expression for w is in R^* and the other term in the numerator has valuation larger than $v(s)$. Arguments similar to those of Section 3 now complete the proof of the proposition. $\square$

A slight modification of the proof of Proposition 5.3 shows that if a lattice L admits an orthonormal basis with norms in $1 + I_0$ such that one norm is $1 + r$ with $v(r) < v(2)$ and all the other norms are closer to 1 than $1 + r$ then r defines a generalized Arf invariant which is an invariant of L.

The effect of combining a lattice $M_{\alpha,\beta}$ (with α and β in I_0) with a unimodular rank 1 lattice spanned by a vector z with $z^2 = u \in R^*$ is already considered in the proof of Corollary 1.3. The norms of the three basis elements given there in this case are $u + \alpha t^2$, $t^2 u + u^2 \beta$, and $-(u + \alpha t^2)(t^2 + u\beta)(1 - \alpha\beta)$ respectively. Modulo I_0, these norms are $u + I_0$, $t^2 u + I_0$, and $-t^2 u + I_0$, which are all equivalent to $u + I_0$ modulo $(R^*)^2$ since $\mathbb{F}$ has characteristic 2.

We now examine the effect of adding a lattice of positive valuation to a unimodular lattice.

Proposition 5.4. *Let M be a unimodular lattice whose discriminant in a given basis is in $1 + I_0$, and let L be a lattice with $v(L) > 0$. Write the discriminant of M in this basis as $1 + r$, and assume that there exist primitive elements $x \in M$ and $y \in L$, with norms a and b respectively, such that $t^2 ab \in r + I_{v(r)}$ for some $t \in R$. Then, the lattice $M \oplus L$ is isomorphic to $N \oplus K$ with N having the same reduction modulo I_0 as M and has discriminant $1 + s$ with $v(s) > v(r)$, and K is a lattice with the same valuation as L and whose discriminant is the discriminant of L multiplied by $1 + t^2 ab$.*

Proof. Let x_i, $1 \leq i \leq n$ be a basis for M giving the discriminant $1 + r$ and in which $x_n^2 = a$, and let y_j, $1 \leq j \leq m$ be a basis for L with $y_m^2 = b$. Consider the elements $z_i = x_i + t(x_i, x_n)y_m$ and $w_j = y_j - t(y_j, y_m)x_n$ of $M \oplus L$. One verifies that $z_i \perp w_j$ for all i and j, and $(z_i, z_j) \equiv (x_i, x_j) (\mathrm{mod}\ I_0)$ since $y_m^2 = b \in I_0$ as $v(L) > 0$. We take N to be the lattice spanned by z_i, $1 \leq i \leq n$ and K to be the lattice generated by w_j,

$1 \leq j \leq m$. If D is the matrix defined by $d_{ij} = (x_i, x_j)$ (with determinant $1 + r$ by assumption) then the matrix giving the discriminant of N is $D + t^2 b d_n d_n^t$, where d_n is the last column of D. By the Matrix Determinant Lemma, the determinant of this matrix is $(1 + t^2 b \cdot d_n^t D^{-1} d_n) \det D$, and since $D^{-1} d_n$ is the nth standard basis vector and $d_{nn} = x_n^2 = a$, this expression reduces to $(1 + t^2 ab)(1 + r)$. Writing the latter expression as $1 + s$ with $s = r + t^2 ab + rt^2 ab$ and observing that r and $t^2 ab$ are in I_0, $t^2 ab \in r + I_{v(r)}$, and $\mathbb{F}$ has characteristic 2, we find that $v(s) > v(r)$. For elements of the lattice K the expression (w_j, w_k) differs from (y_j, y_k) by $at(y_j, y_m)(y_k, y_m)$ of valuation at least $2v(L)$. Evaluating the discriminant of K can be carried out in the same way as the discriminant of N (since L is non-degenerate, the corresponding matrix has non-zero determinant hence can be inverted over $\mathbb{K}$). This completes the proof of the proposition. $\square$

Proposition 5.4 can be used in various manners in order to convert a component in a Jordan decomposition of a lattice into a more canonical one, while affecting only the Jordan components with higher valuations. As two possible examples, consider the following: A lattice element with norm $1 + r$ (contained in a unimodular component) with $v(r)$ maximal can be taken to an element of norm $1 + s$ with $v(s) > v(r)$, and a lattice $M_{\alpha,\beta}$ can be altered in this way to a lattice $M_{\gamma,\delta}$ with generalized Arf invariant of higher valuation. In some cases, the class of minimal norms can also change to a class with larger valuation. All the transformations presented in [8] over $R = \mathbb{Z}_2$ are special cases of Propositions 5.3 and 5.4.

References

[1] C. Arf, Untersuchungen über Quadratische Formen in Körpern der Charakteristik 2, J. Reine Angew. Math. 183 (1941) 148–167.

[2] E. Bayer-Fluckiger, L. Fainsilber, Non unimodular Hermitian forms, Invent. Math. 123 (1996) 233–240.

[3] E. Bayer-Fluckiger, U. First, D.A. Moldovan, Hermitian categories, extension of scalars and systems of sesquilinear forms, Pacific J. Math. 270 (1) (2014) 1–26, http://dx.doi.org/10.2140/pjm.2014.270.1.

[4] J.W.S. Cassels, Rational Quadratic Forms, London Math. Soc. Monogr. Ser., vol. 13, Academic Press, London, New York, San Francisco, 1978, xvi+413 pp.

[5] W.H. Durfee, Congruence of quadratic forms over valuation rings, Duke Math. J. 11 (1944) 687–697.

[6] I. Efrat, Valuations, Orderings, and Milnor K-Theory, Math. Surveys Monogr., vol. 124, 2006, 288 pp.

[7] B.W. Jones, An extension of a theorem of Witt, Bull. Amer. Math. Soc. (N.S.) 48 (1942) 133–142.

[8] B.W. Jones, A canonical quadratic form for the ring of 2-adic integers, Duke Math. J. 11 (1944) 715–727.

[9] B.W. Jones, The Arithmetic Theory of Quadratic Forms, Carus Math. Monogr., vol. 10, The Mathematical Association of America, 1950, x+212 pp.

[10] M. Knebusch, Specialization of Quadratic and Symmetric Bilinear Forms, Algebra Appl., vol. 11, Springer-Verlag, London, 2010, ix+192 pp.

[11] M.-A. Knus, Quadratic and Hermitian Forms over Rings, Grundlehren Math. Wiss., vol. 294, Springer-Verlag, Berlin, Heidelberg, 1991, xi+526 pp.

[12] J. Milnor, D. Husemoller, Symmetric Bilinear Forms, Ergeb. Math. Grenzgeb., vol. 73, Springer-Verlag, 1973, 146 pp.

[13] O.T. O'Meara, Introduction to Quadratic Forms, Grundlehren Math. Wiss., vol. 117, Springer-Verlag, Berlin, Göttingen, Heidelberg, 1963, xi+342 pp.

[14] O.F.G. Schilling, The Theory of Valuations, Math. Surveys Monogr., vol. IV, Amer. Math. Soc., Providence, RI, 1950, vii+255 pp.

[15] J.P. Serre, A Course in Arithmetic, Grad. Texts in Math., vol. 7, Springer-Verlag, New York, 1973, viii+115 pp.

[16] J.P. Serre, Local Fields, Grad. Texts in Math., vol. 67, Springer-Verlag, Berlin, New York, 1979, viii+241 pp.

[17] S. Zemel, A p-adic approach to the Weil representation of discriminant forms arising from even lattices, submitted for publication.