ON THE PRESENTATION OF THE GROTHENDIECK-WITT GROUP OF SYMMETRIC BILINEAR FORMS OVER LOCAL RINGS

ROBERT ROGERS AND MARCO SCHLICHTING

Abstract. We prove a Chain Lemma for inner product spaces over commutative local rings R with residue field other than $\mathbb{F}_2$ and use this to show that the usual presentation of the Grothendieck-Witt group of symmetric bilinear forms over R as the zero-th Milnor-Witt K-group holds provided the residue field of R is not $\mathbb{F}_2$.

Contents

1. Introduction

In [MH73, Lemma IV.1.1], Milnor proves that the Witt group $W(F)$ of inner product spaces, aka non-degenerate symmetric bilinear forms, of a field F is additively generated by elements $\langle a\rangle$, with $a \in F^*$, subject the following three relations.

(1) For all $a, b \in F^*$ we have $\langle a^2b\rangle = \langle b\rangle$.
(2) For all $a \in F^*$ we have $\langle a\rangle + \langle -a\rangle = 0$.
(3) For all $a, b, a+b \in F^*$ we have $\langle a\rangle + \langle b\rangle = \langle a+b\rangle + \langle (a+b)ab\rangle$.

From this, one readily obtains a presentation of the Grothendieck-Witt group $GW(F)$ of F with the same generators and relations (1), (2'), (3) where:

(2') For all $a \in F^*$ we have $\langle a\rangle + \langle -a\rangle = \langle 1\rangle + \langle -1\rangle$.

The goal of this paper is to generalise these presentations to commutative local rings (R, m, F). In fact, we will show in Theorem 1.3 and Corollary 1.5 below that the same presentation holds for $GW(R)$ and for $W(R)$ as long as the residue field F of the local ring R satisfies $F \neq \mathbb{F}_2$. If the residue field is $\mathbb{F}_2$, then there are counter-examples; see Proposition 4.1. It seems that our results are new when the residue field F has characteristic 2 or when $R \neq F = \mathbb{F}_3$.

Date: November 10, 2023.
1991 *Mathematics Subject Classification.* 11E81, 11E08, 19D45.
Key words and phrases. Symmetric bilinear form, Grothendieck-Witt group, Chain Lemma, Milnor-Witt K-theory.

Remark 1.1. The abelian group with generators $\langle a\rangle$, $a \in R^*$, and relations (1), (2'), (3) (and R in place of F) is also known as the zero-th Milnor-Witt K-group $K_0^{MW}(R)$ of R [Mor12], [GSZ16], [Sch17]. The presentation of $GW(R)$ as the zeroth Milnor-Witt K-group has become important in applications of $\mathbb{A}^1$-homotopy theory [Mor12], [AF22] and the homology of classical groups [Sch17] where the sheaf of Milnor-Witt K-groups plays a paramount role. To date, the lack of understanding of the relation between Milnor-Witt K-theory and Grothendieck-Witt groups when $\mathrm{char}(F) = 2$ is the reason that many results are only known away from characteristic 2. This paper therefore is part of the effort to establish these applications also in characteristic 2 and in mixed characteristic.

To state our results in detail, recall that an inner product space over a commutative ring R is a finitely generated projective R-module V equipped with a non-degenerate symmetric R-bilinear form $V \times V \to R : (x, y) \mapsto \langle x, y\rangle$; see [MH73]. When R is local, then V is free of some finite rank, say n. In that case, an orthogonal basis of V is a basis $v_1, ..., v_n \in V$ such that $\langle v_i, v_j\rangle = 0$ for $i \neq j$. Note that if the residue field of R has characteristic 2, an inner product space over R need not have an orthogonal basis. Nevertheless, we prove in Proposition 3.1 (3) that *stably* every inner product space over R has an orthogonal basis. Two orthogonal bases B, C of V are called *chain equivalent*, written $B \approx C$, or $B \approx_R C$ to emphasise the ring R, if there is a sequence $B_0, B_1, ..., B_r$ of orthogonal bases of V such that $B_0 = B$ and $B_r = C$, and $B_{i-1} \cap B_i$ has cardinality at least $n - 2$ for $i = 1, ..., r$. Our first result is the following.

Theorem 1.2 (Chain Lemma)**.** *Let (R, m, F) be a commutative local ring with residue field $F \neq \mathbb{F}_2$. Let V be an inner product space over R. Then any two orthogonal bases of V are chain equivalent.*

Of course, this is vacuous if V has no orthogonal basis. Theorem 1.2 was previously known when R is a field of characteristic not 2 [Wit37, Satz 7], [Lam05, Theorem I.5.2], and the local case easily reduces to the field case; see Lemma 2.4. The Theorem does not hold when $F = \mathbb{F}_2$; see Remark 2.11 and Lemma 2.4. The proof of Theorem 1.2 is given in Section 2.

We let $GW(R)$ be the Grothendieck-Witt ring of non-degenerate symmetric bilinear forms over R, that is, the Grothendieck group associated with the abelian monoid of isomorphism classes of inner product spaces over R with orthogonal sum as monoid operation [Kne77], [Sah72], [MH73], [Sch10]. The ring structure is induced by the tensor product of inner product spaces. For $a \in R^*$, we denote by $\langle a\rangle$ the basis element of the group ring $\mathbb{Z}[R^*]$ corresponding to $a \in R^*$, and also the rank 1 inner product space $\langle x, y\rangle = axy$, $x, y \in V = R$. In either case we let $\langle\langle a\rangle\rangle = 1 - \langle a\rangle$ and $h = \langle 1\rangle + \langle -1\rangle$. Note that we have a ring homomorphism.

$$\pi : \mathbb{Z}[R^*] \longrightarrow GW(R) : \langle a\rangle \mapsto \langle a\rangle. \tag{1.1}$$

Our main result is the following which asserts that this ring homomorphism is surjective with kernel the ideal generated by three types of relations.

Theorem 1.3 (Presentation of $GW(R)$)**.** *Let (R, m, F) be a commutative local ring with residue field $F \neq \mathbb{F}_2$. Then the Grothendieck-Witt ring $GW(R)$ of inner product spaces over R is the quotient ring of the integral group ring $\mathbb{Z}[R^*]$ of the group R^* of units of R modulo the following relations:*

(1) *For all* $a \in R^*$ *we have* $\langle\langle a^2 \rangle\rangle = 0$.
(2) *For all* $a \in R^*$ *we have* $\langle\langle a \rangle\rangle \cdot h = 0$.
(3) *(Steinberg relation) For all* $a, 1-a \in R^*$ *we have* $\langle\langle a \rangle\rangle \cdot \langle\langle 1-a \rangle\rangle = 0$.

In the context of Witt and Grothendieck-Witt groups, the Steinberg relation is also called Witt relation.

Remark 1.4. If the residue field F of R satisfies $F \neq \mathbb{F}_2, \mathbb{F}_3$ and we impose only the Steinberg relation (3) in Theorem 1.3, then imposing relation (1) is equivalent to imposing relation (2); see Lemma 3.6 (2) below. In particular, if the residue field is not $\mathbb{F}_2, \mathbb{F}_3$, then $GW(R)$ is the ring quotient of $\mathbb{Z}[R^*/R^{2*}]$ modulo the Steinberg relation (3). When $R = F$ is any field, including $F = \mathbb{F}_2, \mathbb{F}_3$, we can dispense with the relation (2) as well and obtain the presentation of $GW(F)$ as the quotient of the group ring $\mathbb{Z}[R^*/R^{2*}]$ modulo the Steinberg relations. Indeed, if $R = \mathbb{F}_3$, relations (1) and (2) are vacuous and if $R = \mathbb{F}_2$, all three relations (1), (2) and (3) are vacuous but the map $\pi : \mathbb{Z} = \mathbb{Z}[R^*] \to GW(R)$ is already an isomorphism.

Theorem 1.3 was previously known for R a field (including $\mathbb{F}_2$) [MH73], and for local rings with residue field F of characteristic not two as long as $F \neq \mathbb{F}_3$ [Gil19, Theorem 2.2]. The theorem does not hold for local rings with residue field $\mathbb{F}_2$, in general; see Proposition 4.1. The proof of Theorem 1.3 is in Section 3, Corollary 3.5.

Since the Witt ring $W(R)$ is the quotient of the Grothendieck-Witt ring $GW(R)$ modulo the ideal generated by $h = 1 + \langle -1 \rangle$, we obtain the following from Theorem 1.3 generalising Milnor's presentation from fields to local rings.

Corollary 1.5. *Let* (R, m, F) *be a commutative local ring with residue field* $F \neq \mathbb{F}_2$. *Then the Witt group* $W(F)$ *of inner product spaces of* R *is additively generated by elements* $\langle a \rangle$, *with* $a \in R^*$, *subject the following three relations.*

(1) *For all* $a, b \in R^*$ *we have* $\langle a^2 b \rangle = \langle b \rangle$.
(2) *For all* $a \in R^*$ *we have* $\langle a \rangle + \langle -a \rangle = 0$.
(3) *For all* $a, b, a+b \in R^*$ *we have* $\langle a \rangle + \langle b \rangle = \langle a+b \rangle + \langle (a+b)ab \rangle$.

2. The Chain Lemma

For an inner product space V over R, we write $q : V \to R$ for the associated quadratic form defined by $q(x) = \langle x, x \rangle$ for $x \in V$. We call an element $v \in V$ *anisotropic* if $q(v) \in R^*$. Note that for an orthogonal basis $(u_1, ..., u_n)$ of V, every u_i is anisotropic, $i = 1, ..., n$. For units $a_1, ..., a_n \in R^*$, we denote by $\langle a_1, ..., a_n \rangle = \langle a_1 \rangle + \cdots + \langle a_n \rangle = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$ the inner product space which has orthogonal basis $u_1, ..., u_n$ with $q(u_i) = a_i$ for $i = 1, ..., n$.

Our first goal is to show in Lemma 2.4 below that the Chain Lemma (Theorem 1.2) for a local ring is equivalent to the Chain Lemma for its residue field.

Lemma 2.1. *Let* (R, m, F) *be a local ring,* $\varepsilon \in m$, *and let* V *be an inner product space over* R. *If* $B_1 = (u_1, ..., u_n)$ *is an orthogonal basis of* V, *then so is* $B_2 = (u_1 + \varepsilon u_2, u_2 - \varepsilon q(u_2) q(u_1)^{-1} u_1, u_3, ..., u_n)$. *Moreover, we have* $B_1 = B_2 \mod m$ *and* $B_1 \approx_R B_2$.

Proof. Since $\varepsilon \in m$, we have $B_1 = B_2 \mod m$, and B_2 is a basis since B_1 is. Orthogonality is checked directly. Since B_1 and B_2 differ in only two terms, they are chain equivalent, by definition. □

Lemma 2.2. *Let (R, m, F) be a local ring, and let V be an inner product space over R. If $B_1 = (u_1, ..., u_n)$ and $B_2 = (v_1, ..., v_n)$ are orthogonal bases of V such that $B_1 = B_2 \mod m$, then $B_1 \approx_R B_2$.*

Proof. The proof is by induction on $n \geqslant 1$. By the definition, for $n = 1$ and $n = 2$ any two orthogonal bases are chain equivalent. In particular, the claim is true for $n = 1, 2$. For $n > 2$, we claim that $(u_1, ..., u_n) \approx_R (v_1, u'_2, ..., u'_n)$ for some $u'_2, ..., u'_n \in V$ such that $u'_i = u_i \mod m$. Then the induction hypothesis applied to the two orthogonal bases $(u'_2, ..., u'_n)$ and $(v_2, ..., v_n)$ of the non-degenerate subspace $v_1^\perp$ of V yields $(u_1, ..., u_n) \approx_R (v_1, u'_2, ..., u'_n) \approx_R (v_1, v_2, ..., v_n)$. To prove the claim, note that $v_1 = u_1 + \varepsilon_1 u_1 + \varepsilon_2 u_2 + \cdots + \varepsilon_n u_n$ for some $\varepsilon_i \in m$ since $u_1 = v_1 \mod m$. For $i = 0, ..., n$, set $u_1^{(i)} = u_1 + \varepsilon_1 u_1 + \varepsilon_2 u_2 + \cdots + \varepsilon_i u_i$. Then $u_1^{(0)} = u_1$ and $u_1^{(n)} = v_1$. For $i = 2, ..., n$ we apply Lemma 2.1 recursively to the pair $(u_1^{(i-1)}, u_i)$ to find $u'_i \in V$ such that $u'_i = u_i \mod m$ and

$$(u_1, ..., u_n) \approx_R (u_1^{(1)}, u_2, ..., u_n) \approx_R (u_1^{(i)}, u'_2, ..., u'_i, u_{i+1}, ..., u_n)$$

where the first $\approx_R$ is the case $n = 1$. □

Lemma 2.3. *Let (R, m, F) be a local ring, and let V be an inner product space over R. Any orthogonal basis $\bar{u} = (\bar{u}_1, ..., \bar{u}_n)$ of $V_F = V \otimes_R F$ is the image mod m of an orthogonal basis $u = (u_1, ..., u_n)$ of V, called lift of $\bar{u}$. If two orthogonal bases $\bar{u}$, $\bar{v}$ of V_F differ by at most two places, then there are lifts u and v of $\bar{u}$ and $\bar{v}$ which differ in at most two places.*

Proof. Choose any lift u_1 of $\bar{u}_1$ inside V, then any lift u_2 of $\bar{u}_2$ inside $u_1^\perp \subset V$, then any lift u_3 of $\bar{u}_3$ inside $\{u_1, u_2\}^\perp \subset V$... This yields a lift u of $\bar{u}$. Assume $\bar{u} = (\bar{u}_1, \bar{u}_2, \bar{u}_3, ..., \bar{u}_n)$ and $\bar{v} = (\bar{v}_1, \bar{v}_2, \bar{u}_3, ..., \bar{u}_n)$. Let $u = (u_1, ..., u_n)$ be a lift of $\bar{u}$. Let (v_1, v_2) be a lift of $(\bar{v}_1, \bar{v}_2)$ inside $\{u_3, ..., u_n\}^\perp$. Then we can choose $v = (v_1, v_2, u_3, ..., u_n)$ as lift of $\bar{v}$. □

For two orthogonal bases B, C of an inner product space V over a local ring (R, m, F), we write $B \approx_F C$ if the images of B and C in $V_F = V \otimes_R F$ are chain equivalent over F. The following shows that the Chain Lemma (Theorem 1.2) for a local ring is equivalent to the Chain Lemma for its residue field.

Lemma 2.4. *Let (R, m, F) be a local ring and V an inner product space over R. For two orthogonal bases B, C of V, if $B \approx_F C$, then $B \approx_R C$.*

Proof. Choose a sequence $\bar{B}_i$, $i = 0, ..., r$ of orthogonal bases of V_F such that $\bar{B}_0$ and $\bar{B}_r$ are the images of B and C in V_F and $\bar{B}_i$ differs from $\bar{B}_{i+1}$ in at most two places, $i = 0, ..., r-1$. By Lemma 2.3, for $i = 0, ..., r-1$ we can choose lifts B_i, C_{i+1} of $\bar{B}_i$ and $\bar{B}_{i+1}$ such that B_i and C_{i+1} differ in at most two places. By Lemma 2.2, we have $B \approx_R B_0$, $B_i \approx_R C_i$ for $i = 1, ..., r-1$ and $C_r \approx_R C$. Hence,

$$B \approx_R B_0 \approx_R C_1 \approx_R B_1 \approx_R C_2 \approx_R B_2 \approx_R C_3 \approx_R \cdots \approx_R C_r \approx_R C.$$

□

Our next goal is to prove in Theorem 2.6 the Chain Lemma (Theorem 1.2) for infinite fields of characteristic 2. We will make frequent use of the following.

Lemma 2.5. *Let $n \geqslant 2$ be an integer, and let $u = (u_1, ..., u_n)$ be an orthogonal basis of an inner product space V of rank n over a field F. Let $v_1 = a_1 u_1 + \cdots + a_n u_n$, where $a_1, ..., a_n \in F$. If for all $2 \leqslant r \leqslant n$, the partial linear combination $v_1^{(r)} =$*

$a_1u_1 + \cdots + a_ru_r$ is anisotropic, then $v_1 = v_1^{(n)}$ can be extended to an orthogonal basis $v = (v_1, ..., v_n)$ of V such that $u \approx_F v$.

Proof. Choose v_2 to be a generator of the orthogonal of $v_1^{(2)}$ inside $Fu_1 \perp Fu_2$. Then $u \approx (v_1^{(2)}, v_2, u_3, ..., u_n)$. For an integer r with $2 \leqslant r < n$, assume we have constructed elements $v_2, ..., v_r \in V$ such that $(v_1^{(r)}, v_2, ..., v_r, u_{r+1}, ..., u_n)$ is an orthogonal basis of V that is chain equivalent to u. Note that $v_1^{(r+1)}$ is an anisotropic vector in $Fv_1^{(r)} \perp Fu_{r+1}$. Choose v_{r+1} to be a generator of the orthogonal complement $(v_1^{(r+1)})^\perp$ of $Fv_1^{(r+1)}$ inside $Fv_1^{(r)} \perp Fu_{r+1}$. Then

$$u \approx (v_1^{(r)}, v_2, ..., v_r, u_{r+1}, ..., u_n) \approx (v_1^{(r+1)}, v_2, ..., v_{r+1}, u_{r+2}, ..., u_n).$$

By induction on r, we obtain the case $r = n$ which is the statement of the lemma. □

Theorem 2.6. *Let F be a field of characteristic 2, and let V be an inner product space over F. If F is finite, assume that $\dim_F V = 3$. Then any two orthogonal bases of V are chain equivalent.*

Proof. Assume first that $F \neq \mathbb{F}_2$. We proceed by induction on $n = \dim_F V \geqslant 0$. For $n = 0, 1, 2$, there is nothing to prove. If F is finite, assume $n = 3$, otherwise let $n \geqslant 3$. For an orthogonal basis $u = (u_1, u_2, ..., u_n)$ of V, let $C(u) \subset V$ be the set of all vectors $\alpha_1u_1 + \alpha_2u_2 + ... + \alpha_nu_n \in V$ such that

$$\alpha_1^2q(u_1) + \alpha_2^2q(u_2) + \cdots + \alpha_r^2q(u_r) \neq 0 \quad \text{for all} \quad r = 2, ..., n.$$

Let $v = (v_1, v_2, ..., v_n)$ be another orthogonal basis of V and consider the corresponding set $C(v)$. By Lemma 2.7 below, the intersection $C(u) \cap C(v)$ is non-empty. Thus, we can choose a vector $u_1' = v_1' \in C(u) \cap C(v)$. By Lemma 2.5 we can extend $u_1' = v_1'$ to orthogonal bases $u' = (u_1', u_2', ..., u_n')$ and $v' = (v_1', v_2', ..., v_n')$ of V such that $u \approx u'$ and $v \approx v'$. Now $(u_2', ..., u_n')$ and $(v_2', ..., v_n')$ are orthogonal bases of $(u_1')^\perp = (v_1')^\perp$ and thus $(u_2', ..., u_n') \approx (v_2', ..., v_n')$ by the induction hypothesis. In particular, $u' \approx v'$ since $u_1' = v_1'$, and we have proved $u \approx u' \approx v' \approx v$.

For $F = \mathbb{F}_2$ there is only one inner product space V of dimension 3, namely $\langle 1, 1, 1 \rangle$; see for instance Proposition 3.1 below. The only anisotropic vectors of V are e_1, e_2, e_3 and $e = e_1 + e_2 + e_3$. The vector e cannot be extended to an orthogonal basis since every vector in its orthogonal complement $e^\perp \subset V$ is isotropic. Thus, the only orthogonal basis of V is e_1, e_2, e_3 and the theorem trivially holds. □

Lemma 2.7. *Let $n, r \geqslant 1$ be integers, and let F be a field of characteristic 2. Let $V = F^n$ and let $q_1, ..., q_r$ be diagonalisable non-trivial homogeneous quadratic forms on V. If $|F| \geqslant r$, then there is $v \in V$ such that $q_i(v) \neq 0$ for $i = 1, ..., r$.*

Proof. We proceed by induction on $r \geqslant 1$. If $r = 1$ the quadratic form q_1 can be written as $\alpha_1x_1^2 + ... + \alpha_nx_n^2$ in a suitable basis of V. We can assume $\alpha_1 \neq 0$ since q_1 is non-trivial. Then $v = (1, 0, ..., 0)$ satisfies $q_1(v) = \alpha_1 \neq 0$. Assume $r \geqslant 2$. By induction hypothesis, we can pick $v_1 \in V$ such that $q_i(v_1) \neq 0$ for $i = 1, 2, ..., r-1$. If $q_r(v_1) \neq 0$ then we are done. Otherwise, pick $v_2 \in V$ such that $q_r(v_2) \neq 0$, and choose $\epsilon \in F$ such that ϵ^2 is not in the set

$$\left\{ \frac{q_i(v_2)}{q_i(v_1)} \mid 1 \leqslant i \leqslant r-1 \right\}$$

of cardinality at most $r-1$. Note that such an ϵ exists because the Frobenius morphism $F \to F, u \mapsto u^2$ is injective, and hence the set $\{\epsilon^2 \mid \epsilon \in F\}$ contains $|F| \geqslant r$ many elements. Then the vector $v = \varepsilon v_1 + v_2$ satisfies $q_i(v) \neq 0$ for $i = 1, ..., r$ since

$$q_i(\epsilon v_1 + v_2) = q_i(\epsilon v_1) + q_i(v_2) = \epsilon^2 q_i(v_1) + q_i(v_2) \neq 0 \quad \text{for} \quad i = 1, ..., r-1$$

and $q_r(\epsilon v_1 + v_2) = \epsilon^2 q_r(v_1) + q_r(v_2) = q_r(v_2) \neq 0$. □

In order to prove Theorem 1.2 for finite fields of characteristic 2 other than $\mathbb{F}_2$ we need the following lemma.

Lemma 2.8. *Let $F \neq \mathbb{F}_2$ be finite field of characteristic 2, and let $n \geqslant 4$ be an even integer. Assume that any two orthogonal bases of an inner product space over F of dimension smaller than n are chain equivalent. Then the two bases e and $\hat{e}$ of $\langle 1, 1, ..., 1\rangle = \langle 1\rangle^{\oplus n}$ below are chain equivalent:*

$$e = (e_1, e_2, ..., e_n) \approx \hat{e} = (\hat{e}_1, \hat{e}_2, ..., \hat{e}_n)$$

where $\hat{e}_r = \sum_{1 \leqslant i \neq r \leqslant n} e_i$.

Proof. The orthogonal basis $e = (e_1, e_2, ..., e_n)$ is chain equivalent to an orthogonal basis $u = (u_1, ..., u_n)$ with $u_1 = a_1 e_1 + \cdots + a_n e_n$ if for $r = 1, ..., n$ we have $\sum_{1 \leqslant i \leqslant r} a_i \neq 0$. See Lemma 2.5. Similarly, $\hat{e} = (\hat{e}_1, \hat{e}_2, ..., \hat{e}_n)$ is chain equivalent to an orthogonal basis $v = (v_1, ..., v_n)$ with $v_1 = b_1 \hat{e}_1 + \cdots + b_n \hat{e}_n$ if for $r = 1, ..., n$ we have $\sum_{1 \leqslant i \leqslant r} b_i \neq 0$. Note that

$$v_1 = b_1 \hat{e}_1 + \cdots b_n \hat{e}_n = \hat{b}_1 e_1 + \cdots + \hat{b}_n e_n$$

where $\hat{b}_r = \sum_{1 \leqslant i \neq r \leqslant n} b_i$. Choose elements $b_1, b_n \in F$ such that $b_1, b_n, b_1 + b_n \neq 0$. This is possible since F has more than 2 elements. Set $b_i = 0$ for $1 < i < n$ and $a_i = \hat{b}_i$. Then

$$\hat{b}_i = \begin{cases} b_n & i = 1 \\ b_1 + b_n & 1 < i < n \\ b_1 & i = n \end{cases}$$

and therefore, for $r = 1, ..., n$ we have

$$\sum_{1 \leqslant i \leqslant r} a_i = \sum_{1 \leqslant i \leqslant r} \hat{b}_i = \begin{cases} b_n & 1 \leqslant r < n,\ r \text{ odd} \\ b_1 & 1 \leqslant r < n,\ r \text{ even} \\ b_1 + b_n & r = n \end{cases}$$

and

$$\sum_{1 \leqslant i \leqslant r} b_i = \begin{cases} b_1 & 1 \leqslant r < n \\ b_1 + b_n & r = n \end{cases}$$

In particular, the last two sums are non-zero for $r = 1, ..., n$. Hence, there are orthogonal bases u and v as above with $e \approx u$, $\hat{e} \approx v$ and $u_1 = v_1$. By assumption applied to the inner product space $u_1^\perp = v_1^\perp$ of dimension $n-1$, we have $(u_2, ..., u_n) \approx (v_2, ..., v_n)$. Therefore,

$$e \approx u \approx v \approx \hat{e}.$$

□

Example 2.9. As an illustration of Lemma 2.8, the following explicitly shows that $(e_1, e_2, e_3, e_4) \approx (\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{e}_4)$ over $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$ where we set $\beta = 1 + \alpha$ and note that $\alpha\beta = 1$, $\alpha + \beta = 1$, $\alpha^2 = \beta$, $\beta^2 = \alpha$:

$$\begin{array}{clccr}
 & (e_1, & e_2, & e_3, & e_4) \\
\approx & (\alpha e_1 + \beta e_2, & \beta e_1 + \alpha e_2, & e_3, & e_4) \\
\approx & (e_1 + \alpha e_2 + \alpha e_3, & \beta e_1 + \alpha e_2, & \beta e_1 + e_2 + \beta e_3, & e_4) \\
\approx & (\beta e_1 + e_2 + e_3 + \alpha e_4, & \beta e_1 + \alpha e_2, & \beta e_1 + e_2 + \beta e_3, & \alpha e_1 + \beta e_2 + \beta e_3 + \beta e_4) \\
\approx & (\beta e_1 + e_2 + e_3 + \alpha e_4, & \beta e_1 + \alpha e_2, & e_1 + \alpha e_2 + \beta e_3 + e_4, & \beta e_3 + \alpha e_4) \\
\approx & (\beta e_1 + e_2 + e_3 + \alpha e_4, & e_1 + \beta e_2 + \alpha e_3 + e_4, & e_1 + \alpha e_2 + \beta e_3 + e_4, & \alpha e_1 + e_2 + e_3 + \beta e_4) \\
\approx & (\beta e_1 + e_2 + e_3 + \alpha e_4, & e_1 + e_3 + e_4, & e_1 + e_2 + e_4, & \alpha e_1 + e_2 + e_3 + \beta e_4) \\
\approx & (e_2 + e_3 + e_4, & e_1 + e_3 + e_4, & e_1 + e_2 + e_4, & e_1 + e_2 + e_3) \\
= & (\hat{e}_1, & \hat{e}_2, & \hat{e}_3, & \hat{e}_4)
\end{array}$$

In contrast, over $\mathbb{F}_2$ we have $(e_1, e_2, e_3, e_4) \not\approx (\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{e}_4)$; see Remark 2.11.

Theorem 2.10. *Let F be a finite field of characteristic 2 such that $F \neq \mathbb{F}_2$. Let V be an inner product space over F. Then any two orthogonal bases of V are chain equivalent.*

Proof. We proceed by induction on the dimension $n = \dim_F V$ of V. For $n = 0, 1, 2$, there is nothing to prove, and the case $n = 3$ was treated in Theorem 2.6. Thus, we can assume $n \geqslant 4$. Let $v = (v_1, v_2, ..., v_n)$ and $w = (w_1, w_2, w_3, ..., w_n)$ be two orthogonal bases of V. Among all orthogonal bases of V that are chain equivalent to v choose one, say $u = (u_1, u_2, u_3, ..., u_n)$, such that for the linear combination $w_1 = a_1u_1 + \cdots + a_nu_n$ the number r of non-zero coefficients $a_i \neq 0$ is minimal. Reordering, we can assume $a_1, ..., a_r \neq 0$ and $a_{r+1} = \cdots = a_n = 0$. Clearly $1 \leqslant r \leqslant n$. If $r = 1$ then $v \approx u \approx (w_1, u_2, u_3, ..., u_n) \approx (w_1, w_2, ..., w_n)$ since $(u_2, u_3, ...u_n) \approx (w_2, ..., w_n)$, by induction hypothesis applied to the orthogonal complement $w_1^\perp$ of w_1 inside V. If $r = 2$ then $v \approx u \approx (w_1, u_2', u_3, ..., u_n)$ where u_2' is a non-zero vector of the orthogonal complement of w_1 inside of $Fu_1 \perp Fu_2$. Then $v \approx (w_1, u_2', u_3, ..., u_n) \approx (w_1, w_2, ..., w_n)$ since $(u_2', u_3, ...u_n) \approx (w_2, ..., w_n)$, by induction hypothesis applied to the orthogonal complement $w_1^\perp$ of w_1 inside V. Assume $r \geqslant 3$. Since every element in F is a square, we can rescale and assume $q(u_i) = q(w_i) = 1$, $i = 1, ..., n$ as rescaling yields chain equivalent bases. Assume that there is a pair $1 \leqslant i \neq j \leqslant r$ such that $a_iu_i + a_ju_j$ is anisotropic. After reordering, we can assume $i = 1$, $j = 2$. Set $u_1' = a_1u_1 + a_2u_2$ and let u_2' be a non-zero vector in the orthogonal complement of u_1' inside $Fu_1 \perp Fu_2$. Then $u \approx (u_1', u_2', u_3, ...u_n)$ and $w_1 = u_1' + a_3u_3 + \cdots + a_ru_r$ contradicting minimality of r. Thus, for all pairs $1 \leqslant i, j \leqslant r$ the vector $a_iu_i + a_ju_j$ is isotropic, that is, $0 = q(a_iu_i + a_ju_j) = a_i^2q(u_i) + a_j^2q(u_j) = a_i^2 + a_j^2 = (a_i + a_j)^2$, so $a_i + a_j = 0$, for $1 \leqslant i \leqslant r$, that is, $a = a_1 = a_2 = a_3 = \cdots = a_r \neq 0$. Then $w_1 = a(u_1 + \cdots + u_r)$. Since $1 = q(w_1) = a^2(q(u_1) + \cdots q(u_r)) = ra^2$, the positive integer r is odd. Therefore, $1 = ra^2 = a^2$ implies $a = 1$, and we have $w_1 = u_1 + \cdots + u_r$. If $r < n$, we can use Lemma 2.8 to find an orthogonal basis $u_2', ..., u_{r+1}'$ of $Fu_2 \perp ... \perp Fu_{r+1}$ such that $(u_1, ..., u_{r+1}) \approx (w_1, u_2', ..., u_{r+1}')$. Then

$$v \approx (u_1, u_2, u_3, ..., u_n) \approx (w_1, u_2', u_3, ..., u_{r+1}', u_{r+2}, ..., u_n) \approx w$$

since $(u_2', u_3, ..., u_{r+1}', u_{r+2}, ..., u_n) \approx (w_2, w_3, ..., w_n)$, by the induction hypothesis applied to $w_1^\perp$ inside V. Finally, the case $r = n$ is impossible. Indeed, if $r = n$, then every vector in $w_1^\perp \subset V$ is isotropic contradicting the the assumption that $(w_2, ..., w_n)$ is an orthogonal basis of $w_1^\perp$. $\square$

Proof of Theorem 1.2. The analog of Theorem 2.6 for fields F of characteristic not 2 is classical and holds without restriction on the size of F; see for instance [Lam05, Theorem I.5.2]. Together with Theorems 2.6 and 2.10, this implies Theorem 1.2 in view of Lemma 2.4. □

Remark 2.11. The Chain Lemma does not hold for $R = F = \mathbb{F}_2$ and $V = \mathbb{F}_2^4$ equipped with the form $\langle 1\rangle^{\perp 4}$. The orthogonal basis $e = \{e_1, e_2, e_3, e_4\}$ is only chain equivalent to itself since $\langle 1\rangle \perp \langle 1\rangle$ has unique orthogonal basis $\{e_1, e_2\}$. But V has also orthogonal basis $\hat{e} = \{\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{e}_4\}$ where $\hat{e}_i = e_1 + e_2 + e_3 + e_4 - e_i$ for $i = 1, ..., 4$. In particular, the two orthogonal basis e and $\hat{e}$ of V are not chain equivalent.

3. Presentation of $GW(R)$

For an invertible symmetric matrix $A \in M_n(R)$, we denote by $\langle A\rangle$ the inner product space R^n equipped with the form $\langle x, y\rangle = {}^t x A y$, $x, y \in R^n$ where ${}^t x$ denotes the transpose of the column vector x. The following shows that every inner product space stably admits an orthogonal basis. In particular, the ring homomorphism (1.1) is surjective.

Proposition 3.1. *Let (R, m, F) be a commutative local ring.*

(1) *For any inner product space M over R there is an isometry*
$$M \cong \langle u_1\rangle \perp \cdots \perp \langle u_l\rangle \perp N_1 \perp \cdots \perp N_r$$
for some $u_i \in R^*$ and $N_i = \left\langle \left(\begin{smallmatrix} a_i & 1 \\ 1 & b_i \end{smallmatrix}\right)\right\rangle$ with $a_i, b_i \in m$.

(2) *For any $a, b \in m$ there is an isometry of inner product spaces*
$$\left\langle \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix} \right\rangle + \langle -1\rangle \cong \left\langle \frac{1 - ab}{(-1 + a)(-1 + b)} \right\rangle + \langle -1 + a\rangle + \langle -1 + b\rangle.$$

(3) *For any inner product space V over R, there is an inner product space W with orthogonal basis such that $V \perp W$ has an orthogonal basis. In particular, the Grothendieck-Witt group $GW(R)$ of symmetric inner product spaces is additively generated by one-dimensional spaces $\langle u\rangle$, $u \in R^*$.*

Proof. For part (1), if $q(x) = \langle x, x\rangle = u \in R^*$ is a unit for some $x \in M$ then $M = Rx \perp (Rx)^\perp$ is a decomposition into non-degenerate subspaces, and $Rx = \langle u\rangle$. Hence, repeatedly splitting off one-dimensional inner product spaces, we can write $M = \langle u_1\rangle \perp \cdots \perp \langle u_l\rangle \perp N$ where $u_i \in R^*$ and $q(x) \in m$ for all $x \in N$. If $N \neq 0$ then the rank of N is at least 2, and we can find $x, y \in N$ such that $\langle x, y\rangle = 1$. The subspace N_1 spanned by x and y is non-degenerate with Gram matrix $\left(\begin{smallmatrix} a & 1 \\ 1 & b \end{smallmatrix}\right)$ where $a = q(x)$ and $b = q(y)$. In paricular, $N = N_1 \perp N_1^\perp$ is decomposition into non-degenerate subspaces, and $N_1 = \langle \left(\begin{smallmatrix} a & 1 \\ 1 & b \end{smallmatrix}\right)\rangle$. Now we keep splitting off rank 2 spaces N_i to obtain the desired form.

Part (2) follows from the equation
$$\begin{pmatrix} -\frac{1}{-1+a} & -\frac{1}{-1+b} & \frac{-1+ab}{(-1+a)(-1+b)} \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} a & 1 & 0 \\ 1 & b & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} -\frac{1}{-1+a} & -1 & 0 \\ -\frac{1}{-1+b} & 0 & -1 \\ \frac{-1+ab}{(-1+a)(-1+b)} & 1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \frac{1-ab}{(-1+a)(-1+b)} & 0 & 0 \\ 0 & -1 + a & 0 \\ 0 & 0 & -1 + b \end{pmatrix}.$$

Finally, (3) follows from (1) and (2). □

Lemma 3.2. *Let (R, m, F) be a commutative local ring with residue field $F \neq \mathbb{F}_2$. Then the kernel $ker(\pi)$ of the ring homomorphism (1.1) is generated as abelian subgroup of $\mathbb{Z}[R^*]$ by the following elements:*

$$\langle\alpha\rangle - \langle\beta\rangle \text{ with } \alpha, \beta \in R^* \text{ and } \langle\alpha\rangle \cong \langle\beta\rangle$$
$$\langle\alpha\rangle + \langle\beta\rangle - \langle\gamma\rangle - \langle\delta\rangle \text{ with } \alpha, \beta, \gamma, \delta \in R^* \text{ and } \langle\alpha, \beta\rangle \cong \langle\gamma, \delta\rangle.$$

Proof. By definition, an element $\sum_{i=1}^{n}\langle a_i\rangle - \sum_{j=1}^{m}\langle b_j\rangle$ of $\mathbb{Z}[R^*]$ with $a_i, b_j \in R^*$ is in $\ker(\pi) \subset \mathbb{Z}[R^*]$ if and only if there is an inner product space K and an isometry

$$K \oplus \bigoplus_{i=1}^{n}\langle a_i\rangle \cong K \oplus \bigoplus_{j=1}^{m}\langle b_j\rangle. \tag{3.1}$$

In particular, $n = m$. By Proposition 3.1 (2), there exists an inner product space W over R such that $K \oplus W$ admits an orthogonal basis. Replacing K with $K \oplus W$, we can assume that K in (3.1) has an orthogonal basis, say $\{z_1, ..., z_l\}$. The inner product space $(M, \beta) := \langle a_1, ..., a_n\rangle \oplus K \cong \langle b_1, ..., b_n\rangle \oplus K$ has the following two orthogonal bases:

$$A = \{x_1, ..., x_n, z_1, .., z_l\}, \text{with } \beta(x_i, x_i) = a_i, \text{ and } \beta(z_i, z_i) = c_i, \text{ and}$$

$$B = \{y_1, ..., y_n, z_1, .., z_l\}, \text{with } \beta(y_i, y_i) = b_i, \text{ and } \beta(z_i, z_i) = c_i.$$

By Theorem 1.2, we can choose a chain of orthogonal bases, $C_0, C_1, ..., C_{N-1}, C_N$ such that C_i and C_{i+1} differ in at most 2 elements, $i = 0, ..., N-1$, and $C_0 = A$, $C_N = B$. Let $\langle c_1^{(i)}, ..., c_{n+l}^{(i)}\rangle$ be the diagonal form corresponding to C_i. As C_i and C_{i+1} differ in at most two vectors,

$$(c_1^{(i)} + ... + c_{n+l}^{(i)}) - (c_1^{(i+1)} + ... + c_{n+l}^{(i+1)})$$

is of the form

$$a - b \text{ with } \langle a\rangle \cong \langle b\rangle$$
$$\text{or}$$
$$a + b - a' - b' \text{ with } \langle a, b\rangle \cong \langle a', b'\rangle.$$

Since

$$\begin{aligned}
\textstyle\sum_{i=1}^{n} a_i - \sum_{j=1}^{n} b_j &= (\textstyle\sum_{i=1}^{n} a_i + \sum_{i=1}^{l} c_i) - (\sum_{j=1}^{n} b_j + \sum_{i=1}^{l} c_i) \\
&= \textstyle\sum_{i=1}^{n+l} c_i^{(0)} - \sum_{j=1}^{n+l} c_j^{(N)} \\
&= \textstyle\sum_{k=0}^{N-1}(\sum_{i=0}^{n+l} c_i^{(k)} - \sum_{i=0}^{n+l} c_i^{(k+1)}),
\end{aligned}$$

we are done. □

Lemma 3.3. *Let R be a commutative ring. Assume we have an isometry of inner product spaces $\langle a, b\rangle \cong \langle c, d\rangle$ over R where $a, b, c, d \in R^*$ with $d = abc$ and $c = ax^2 + by^2$, $x, y \in R$. If $f = as^2 + bt^2$, then*

$$f = c\left(\frac{asx + bty}{c}\right)^2 + d\left(\frac{tx - sy}{c}\right)^2.$$

Proof. Direct verification. □

For a commutative local ring R, let $K_0^{MW}(R)$ be the quotient ring of $\mathbb{Z}[R^*]$ modulo the ideal generated by the relations (1), (2) and (3) of Theorem 1.3 where $\langle\langle a\rangle\rangle = 1 - \langle a\rangle$ and $\langle a\rangle \in \mathbb{Z}[R^*]$ is the element corresponding to $a \in R^*$.

Lemma 3.4. *Let (R, m, F) be a commutative local ring with residue field $F \neq \mathbb{F}_2$, and let $a, b, c, d \in R^*$ with $\langle a, b\rangle \cong \langle c, d\rangle$ as inner product spaces over R. Then the following equality holds in $K_0^{MW}(R)$:*

$$\langle a\rangle + \langle b\rangle = \langle c\rangle + \langle d\rangle.$$

Proof. The isometry $\langle a, b\rangle \cong \langle c, d\rangle$ implies $c = ax^2 + by^2 \in R$ for some $x, y \in R$ and $d = abc \in R^*/R^{2*}$. Since $\langle r^2 d\rangle = \langle d\rangle \in K_0^{MW}(R)$, we can assume $d = abc \in R^*$. If $x, y \in R^*$, we say that c is *regularly represented* by $\langle a, b\rangle$. In this case

$$\begin{aligned}
\langle a\rangle + \langle b\rangle &= \langle ax^2\rangle + \langle by^2\rangle \\
&= \langle c\rangle\left(\langle ac^{-1}x^2\rangle + \langle bc^{-1}y^2\rangle\right) \\
&= \langle c\rangle\left(\langle 1\rangle + \langle abc^{-2}x^2y^2\rangle\right) \\
&= \langle c\rangle + \langle d\rangle
\end{aligned}$$

in $K_0^{MW}(R)$ where we used the Steinberg relation for the third equality.

Assume now that one of x or y is in the maximal ideal m of R, then the other is a unit since c is a unit. Without loss of generality, we can assume $x \in R^*$ and $y \in m$. We claim that if there is $z \in R^*$ such that $ax^2 + bz^2 \in R^*$, then $\langle a\rangle + \langle b\rangle = \langle c\rangle + \langle d\rangle \in K_0^{MW}(R)$. Indeed, given $z \in R^*$ such that $\gamma = ax^2 + bz^2 \in R^*$ we set $\delta = ab\gamma$. Then $\langle a, b\rangle \cong \langle \gamma, \delta\rangle$, and γ is regularly represented by $\langle a, b\rangle$. In particular, $\langle\gamma\rangle + \langle\delta\rangle = \langle a\rangle + \langle b\rangle \in K_0^{MW}(R)$. Since $c = ax^2 + by^2$, Lemma 3.3 yields

$$c = \gamma\left(\frac{ax^2 + byz}{\gamma}\right)^2 + \delta\left(\frac{xy - xz}{\gamma}\right)^2.$$

Note that $(ax^2 + byz)\gamma^{-1}$ and $(xy - xz)\gamma^{-1}$ are units in R since $x, z, a, b, \gamma \in R^*$ and $y \in m$. In particular, c is regularly represented by $\langle\gamma, \delta\rangle$ and thus $\langle c\rangle + \langle d\rangle = \langle\gamma\rangle + \langle\delta\rangle \in K_0^{MW}(R)$. Hence,

$$\langle c\rangle + \langle d\rangle = \langle\gamma\rangle + \langle\delta\rangle = \langle a\rangle + \langle b\rangle \quad \in \quad K_0^{MW}(R).$$

If $F \neq \mathbb{F}_3$ (and $F \neq \mathbb{F}_2$, by assumption) then we can find an element $z \in R^*$ with $ax^2 + bz^2 \in R^*$ as in this case F has at least 3 units and we only need to make sure that its class $\bar{z}$ in $F = R/m$ satisfies $\bar{z}^2 \notin \{-ab^{-1}x^2\} \subset F$. If there is no $z \in R^*$ such that $ax^2 + bz^2 \in R^*$, then $F = \mathbb{F}_3$ and $a + b, a - c \in m$ as in this case square units in R are 1 modulo m. Then $\langle c, -b\rangle \cong \langle a, -d\rangle$ since $a = c(1/x)^2 - b(y/x)^2$ and $d = abc$. Note that there is $z \in R^*$ such that $\gamma = c(1/x)^2 - bz^2 \in R^*$. For instance, $z = 1/x \in R^*$ will do since $c - b = 2c - (a + b) + (a - c) \in R^*$. As proved above, this implies $\langle c\rangle + \langle -b\rangle = \langle a\rangle + \langle -d\rangle$ in $K_0^{MW}(R)$. Using relation (2) of Theorem (1.3) which holds in $K_0^{MW}(R)$, we have

$$\langle a\rangle + \langle b\rangle = \langle a\rangle - \langle -b\rangle + h = \langle c\rangle - \langle -d\rangle + h = \langle c\rangle + \langle d\rangle \quad \in \quad K_0^{MW}(R).$$

□

Corollary 3.5. *Let (R, m, F) be a commutative local ring with residue field $F \neq \mathbb{F}_2$. Then the surjection (1.1) induces an isomorphism*

$$K_0^{MW}(R) \xrightarrow{\cong} GW(R).$$

Proof. Let $J \subset \mathbb{Z}[R^*]$ be the ideal generated by the relations (1), (2) and (3) of Theorem 1.3, that is, J is the kernel of the ring homomorphism $\mathbb{Z}[R^*] \to K_0^{MW}(R)$. As before, let $\pi : \mathbb{Z}[R^*] \to GW(R)$, $\langle a\rangle \mapsto \langle a\rangle$ be the canonical ring homomorphism (1.1). It is well known that $J \subset \ker\pi$. Indeed, the first relation is the isometry $\langle u\rangle \cong \langle a^2u\rangle$ given by the multiplication with $a \in R^*$, the second relation follows from

$$\begin{pmatrix} 0 & 1 \\ u & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & u \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & u \\ u & 0 \end{pmatrix},$$

that is, $\langle\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\rangle \cong \langle u\rangle \cdot \langle\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\rangle$ and the equality $\langle\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\rangle = h \in GW(R)$ in view of Proposition 3.1 (2) with $a = b = 0$. The last relation is a consequence of the equality

$$\begin{pmatrix} 1 & -1 \\ 1-a & a \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1-a \end{pmatrix}\begin{pmatrix} 1 & 1-a \\ -1 & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & a(1-a) \end{pmatrix}.$$

Lemma 3.2 gives us additive generators of $\ker(\pi)$. By definition of $K_0^{MW}(R)$ and Lemma 3.4, these generators are in J, and so, $J = \ker(\pi)$. □

We finish the section with a proof of Remark 1.4. Let $\tilde{K}_0^{MW}(R)$ be the ring quotient of $\mathbb{Z}[R^*]$ modulo the Steinberg relations (3) in Theorem 1.3.

Lemma 3.6. *Let (R, m, F) be a commutative local ring with residue field $F \neq \mathbb{F}_2, \mathbb{F}_3$. Then for all $a \in R^*$, the following holds in $\tilde{K}_0^{MW}(R)$:*

1. $\langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle = 0$,
2. $\langle\langle a^2\rangle\rangle = \langle\langle a\rangle\rangle \cdot h$.

Proof. Part (1) was implicitly proved in [Sch17, Lemma 4.4]. The analogous arguments for Milnor K-theory are due to [Mil70]. We give the relevant details here. First assume $\bar{a} \neq 1$ where $\bar{a}$ means reduction modulo the maximal ideal $m \subset R$. Then $1 - a, 1 - a^{-1} \in R^*$. Therefore, in $K_0^{MW}(R)$, we have

$$\begin{aligned} \langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle &= \langle\langle a\rangle\rangle \left(\langle\langle 1-a\rangle\rangle - \langle -a\rangle\langle\langle 1-a^{-1}\rangle\rangle\right) \\ &= -\langle -a\rangle\langle\langle a\rangle\rangle\langle\langle 1-a^{-1}\rangle\rangle = \langle -a\rangle\langle a\rangle\langle\langle a^{-1}\rangle\rangle\langle\langle 1-a^{-1}\rangle\rangle \\ &= 0. \end{aligned}$$

If $\bar{a} = 1$, choose $b \in R^*$ with $\bar{b} \neq 1$. This is possible since $F \neq \mathbb{F}_2$. Then $\bar{a}\bar{b} \neq 1$. Therefore, in $K_0^{MW}(R)$, we have

$$\begin{aligned} 0 &= \langle\langle ab\rangle\rangle\langle\langle -ab\rangle\rangle = \langle\langle a\rangle\rangle\left(\langle\langle -a\rangle\rangle + \langle -a\rangle\langle\langle b\rangle\rangle\right) + \langle a\rangle\langle\langle b\rangle\rangle\left(\langle\langle a\rangle\rangle + \langle a\rangle\langle\langle -b\rangle\rangle\right) \\ &= \langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle + h\langle a\rangle\langle\langle a\rangle\rangle\langle\langle b\rangle\rangle. \end{aligned}$$

Hence, for all $\bar{b} \neq 1$ we have $\langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle = -h\langle a\rangle\langle\langle a\rangle\rangle\langle\langle b\rangle\rangle$. Now, choose $b_1, b_2 \in A^*$ such that $\bar{b}_1, \bar{b}_2, \bar{b}_1\bar{b}_2 \neq 1$. This is possible since $|F| \geqslant 4$. Then

$$\begin{aligned} \langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle &= -h\langle a\rangle\langle\langle a\rangle\rangle\langle\langle b_1b_2\rangle\rangle \\ &= -h\langle a\rangle\langle\langle a\rangle\rangle(\langle\langle b_1\rangle\rangle + \langle b_1\rangle\langle\langle b_2\rangle\rangle) \\ &= \langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle + \langle b_1\rangle\langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle. \end{aligned}$$

Hence, $\langle b_1\rangle\langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle = 0$. Multiplying with $\langle b_1^{-1}\rangle$ yields the result.

In $\mathbb{Z}[R^*]$ we have $\langle\langle a\rangle\rangle\langle\langle -a\rangle\rangle \cdot \langle -1\rangle + \langle\langle a^2\rangle\rangle = \langle\langle a\rangle\rangle \cdot h$ which implies part (2). □

4. An example of $GW(R) \not\cong K_0^{MW}(R)$

In this section, R will be the local ring $R = \mathbb{F}_2[x]/(x^4)$. The goal is to prove the following.

Proposition 4.1. *For $R = \mathbb{F}_2[x]/(x^4)$, the natural surjection $K_0^{MW}(R) \to GW(R) : \langle a\rangle \mapsto \langle a\rangle$ has kernel $\mathbb{Z}/2$. In fact, we have isomorphisms of abelian groups*

$$GW(R) \cong \mathbb{Z} \oplus (\mathbb{Z}/2)^2 \quad \textit{and} \quad K_0^{MW}(R) \cong \mathbb{Z} \oplus (\mathbb{Z}/2)^3.$$

Proof. It is clear that the three defining relations for $K_0^{MW}(R)$ hold in $GW(R)$. This is true for any commutative local ring R; see the proof of Corollary 3.5. In particular, the map $K_0^{MW}(R) \to GW(R)$ is well-defined. It is surjective for any local ring R, by Proposition 3.1. Let $I \subset GW(R)$, $\tilde{I} \subset K_0^{MW}(R)$ and $J \subset \mathbb{Z}[R^*/R^{2*}]$ be the kernel of the surjective ring homomorphisms to $\mathbb{Z}$ sending $\langle a\rangle$ to $1 \in \mathbb{Z}$ for $a \in R^*$. We have natural surjections $J \twoheadrightarrow \tilde{I} \twoheadrightarrow I$ sending $\langle\langle a\rangle\rangle$ to $\langle\langle a\rangle\rangle$. The first part of the proposition is the statement that the surjection $\tilde{I} \twoheadrightarrow I$ has kernel $\mathbb{Z}/2$.

For $R = \mathbb{F}_2[x]/(x^4)$, the group R^* has 8 elements. The group homomorphism $R^* \to R^* : a \mapsto a^2$ has image $\{1, 1+x^2\}$. In particular, the cokernel R^*/R^{2*} is a group of order 4 in which $a^2 = 1$ for all its elements. Hence, that group is not cyclic and thus $R^*/R^{2*} \cong K_4 = C_2 \times C_2$ is the Klein 4-group. A set of coset representatives for R^*/R^{2*} is given by the elements 1, $1+x$, $1+x+x^2$, $1+x^2+x^3 \in R^*$ since $(1+x)(1+x^2+x^3) = 1+x+x^2+2x^3+x^4 = 1+x+x^2$ is not a square. From the matrix equation

$$\begin{pmatrix} x & 1 \\ 1 & x+x^2+x^3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1+x \end{pmatrix} \begin{pmatrix} x & 1 \\ 1 & x+x^2+x^3 \end{pmatrix} = \begin{pmatrix} 1+x+x^2 & 0 \\ 0 & 1+x^2+x^3 \end{pmatrix}$$

we see that $\langle 1\rangle + \langle 1+x\rangle = \langle 1+x+x^2\rangle + \langle 1+x^2+x^3\rangle \in GW(R)$. For any $\mathbb{F}_2$-algebra, we have $2I = 0$ as $h = \langle 1\rangle + \langle -1\rangle = 2$ and thus $0 = \langle\langle u\rangle\rangle h = 2\langle\langle u\rangle\rangle$ for all $u \in R^*$. In particular, we obtain

$$0 = \langle\langle 1+x\rangle\rangle + \langle\langle 1+x+x^2\rangle\rangle + \langle\langle 1+x^2+x^3\rangle\rangle = \sum_{u \in R^*/R^{2*}} \langle\langle u\rangle\rangle \in GW(R)$$

from which we see that $I^2 = 0$. Indeed, for $u \in R^*/R^{2*}$ we have $\langle\langle u\rangle\rangle^2 = 2\langle\langle u\rangle\rangle = 0$, and for $v \neq u \in R^*/R^{2*}$, $u, v \neq 1 \in R^*/R^{2*}$, we have

$$\langle\langle u\rangle\rangle\langle\langle v\rangle\rangle = \langle\langle u\rangle\rangle + \langle\langle v\rangle\rangle + \langle\langle uv\rangle\rangle = \sum_{w \in R^*/R^{2*}} \langle\langle w\rangle\rangle = 0 \in GW(R).$$

For every local ring, we have an isomorphism $R^*/R^{2*} \cong I/I^2 : a \mapsto \langle\langle a\rangle\rangle$. So, in our case we have $I = I/I^2 = R^*/R^{2*} \cong (\mathbb{Z}/2)^2$.

To compute $\tilde{I}$ for $R = \mathbb{F}_2[x]/(x^4)$, we note that if $a \in R$ is a unit then $1-a$ is not a unit and the Steinberg relation is vacuous. Moreover, $\langle\langle u\rangle\rangle h = 2\langle\langle u\rangle\rangle$ as $h = 2$, and thus, $K_0^{MW}(R)$ is the quotient of $\mathbb{Z}[R^*/R^{2*}]$ by the relation $2\langle\langle u\rangle\rangle = 0$ for $u \in R^*/R^{2*}$. It follows that $\tilde{I} = J/2J = (\mathbb{Z}/2)^3$ since J has $\mathbb{Z}$ basis the elements $\langle\langle u\rangle\rangle$, $1 \neq u \in R^*/R^{2*}$. Hence, the surjection $\tilde{I} \twoheadrightarrow I$ which is $(\mathbb{Z}/2)^3 \twoheadrightarrow (\mathbb{Z}/2)^2$ has kernel $\mathbb{Z}/2$.

As abelian groups, we have $GW(R) \cong \mathbb{Z} \oplus I$ and $K_0^{MW}(R) \cong \mathbb{Z} \oplus \tilde{I}$. In particular, the computations above show that $GW(R) \cong \mathbb{Z} \oplus (\mathbb{Z}/2)^2$ and $K_0^{MW}(R) \cong \mathbb{Z} \oplus (\mathbb{Z}/2)^3$. □

References

[AF22] Aravind Asok and Jean Fasel. Vector bundles on algebraic varieties. *ICM 2022 Proceedings, arXiv:2111.03107*, 2022.

[Gil19] Stefan Gille. On quadratic forms over semilocal rings. *Trans. Amer. Math. Soc.*, 371(2):1063–1082, 2019.

[GSZ16] Stefan Gille, Stephen Scully, and Changlong Zhong. Milnor-Witt K-groups of local rings. *Adv. Math.*, 286:729–753, 2016.

[Kne77] Manfred Knebusch. Symmetric bilinear forms over algebraic varieties. In *Conference on Quadratic Forms—1976 (Proc. Conf., Queen's Univ., Kingston, Ont., 1976)*, Queen's Papers in Pure and Appl. Math., No. 46, pages 103–283. Queen's Univ., Kingston, ON, 1977.

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[MH73] John Milnor and Dale Husemoller. *Symmetric bilinear forms*. Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas], Band 73. Springer-Verlag, New York-Heidelberg, 1973.

[Mil70] John Milnor. Algebraic K-theory and quadratic forms. *Invent. Math.*, 9:318–344, 1969/70.

[Mor12] Fabien Morel. $\mathbb{A}^1$*-algebraic topology over a field*, volume 2052 of *Lecture Notes in Mathematics*. Springer, Heidelberg, 2012.

[Sah72] Chih Han Sah. Symmetric bilinear forms and quadratic forms. *J. Algebra*, 20:144–160, 1972.

[Sch10] Marco Schlichting. Hermitian K-theory of exact categories. *J. K-Theory*, 5(1):105–165, 2010.

[Sch17] Marco Schlichting. Euler class groups and the homology of elementary and special linear groups. *Adv. Math.*, 320:1–81, 2017.

[Wit37] Ernst Witt. Theorie der quadratischen Formen in beliebigen Körpern. *J. Reine Angew. Math.*, 176:31–44, 1937.

Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, UK

Email address: `m.schlichting@warwick.ac.uk, Robert.Rogers@warwick.ac.uk`