ACTA ARITHMETICA
160.4 (2013)

The image of the natural homomorphism of Witt rings of orders in a global field

by

Beata Rothkegel (Katowice)

1. Introduction. Every homomorphism $\varphi\colon R \to P$ of commutative rings (with identity elements) induces a homomorphism $\varphi\colon WR \to WP$ between their Witt rings in the following way. If $\langle (M,\alpha)\rangle \in WR$ is the similarity class of an inner product space (M,α), i.e.

- M is a finitely generated projective R-module,
- $\alpha\colon M\times M \to R$ is a nonsingular bilinear form,

then

$$\varphi\langle (M,\alpha)\rangle = \langle (M',\alpha')\rangle,$$

where $M' = P\otimes_R M$ and $\alpha'\colon M'\times M' \to P$ is the nonsingular bilinear form defined by

$$\alpha'(x\otimes m, x'\otimes m') = xx'\varphi(\alpha(m,m')) \quad \text{for all } x,x'\in P,\ m,m'\in M. \tag{1.1}$$

The homomorphism $\varphi\colon WR\to WP$ is said to be *natural* if it is induced by an embedding $R\hookrightarrow P$. If R is a Dedekind domain and $P=K$ is its field of fractions, then the natural homomorphism $\phi\colon WR\to WK$ is injective (cf. [K, Satz 11.1.1]). This allows us to treat WR as a subring of WK.

Let K be a global field, R be a Dedekind domain and K be its field of fractions. Let $\mathcal{O} < R$ be an *order*, i.e.:

- $\mathcal{O}$ is a one-dimensional noetherian domain,
- R is the integral closure of $\mathcal{O}$ in the field K,
- R is a finitely generated $\mathcal{O}$-module.

We will examine the image of the natural homomorphism $\varphi\colon W\mathcal{O}\to WR$.

Since the homomorphism $\phi\colon WR\to WK$ is injective, it is easy to observe that it is enough to examine the image of the composition $\phi\circ\varphi\colon W\mathcal{O}\to WK$. In [C1, C2] that image is examined in the case of orders in the rings R_K

2010 *Mathematics Subject Classification*: Primary 11E81; Secondary 19G12.
Key words and phrases: order, natural homomorphism.

DOI: 10.4064/aa160-4-4

of algebraic integers of some quadratic number fields $K=\mathbb{Q}(\sqrt{D})$. Ciemała has proved that there are infinitely many orders $\mathcal{O} < R_K$ such that the natural homomorphism $\varphi\colon W\mathcal{O}\to WR_K$ is surjective. In Sections 3, 4, 7 we will formulate necessary and sufficient conditions for the surjectivity of the natural homomorphisms in the case of all nonreal quadratic number fields, all real quadratic number fields $K=\mathbb{Q}(\sqrt{D})$ such that -1 is a norm in the extension $K/\mathbb{Q}$, and all quadratic function fields.

If R is a commutative ring, then we write $U(R)$ for the group of invertible elements of R. If $a_1,\ldots,a_l\in U(R)$, then $\langle a_1,\ldots,a_l\rangle$ will denote both a diagonal quadratic form and its class in the Witt ring WR. We write $\langle\langle a_1,a_2\rangle\rangle$ for the 2-fold Pfister form $\langle 1,a_1\rangle\otimes\langle 1,a_2\rangle=\langle 1,a_1,a_2,a_1a_2\rangle$.

Let R be a Dedekind domain and K be its field of fractions. We define the group $E(R)$ of *singular elements* of R to be

$$E(R)=\{g\in\dot K:\operatorname{ord}_{\mathfrak{P}} g\equiv 0 \pmod 2 \text{ for every maximal ideal } \mathfrak{P}\lhd R\}.$$

Every maximal ideal $\mathfrak{P}$ of R determines a $\mathfrak{P}$-adic valuation on the field K with residue class field $\overline{K}_{\mathfrak{P}}$. According to [MH, (3.3) Corollary] we have the Knebusch–Milnor exact sequence

$$0\to WR\xrightarrow{\phi} WK\xrightarrow{\partial}\bigoplus_{\mathfrak{P}} W\overline{K}_{\mathfrak{P}},$$

where the direct sum extends over all maximal ideals $\mathfrak{P}$ of R. The additive group homomorphism ∂ is the direct sum of the second residue homomorphisms $\partial_{\mathfrak{P}}\colon WK\to W\overline{K}_{\mathfrak{P}}$. Directly from the sequence and the definition of $\partial_{\mathfrak{P}}$ we obtain

Proposition 1.1. *If $g\in\dot K$, then*

$$\langle g\rangle\in\phi(WR)\ \Leftrightarrow\ g\in E(R).$$

Let K be a global field of characteristic different from 2. Let $\mathcal{S}$ be a *Hasse set* on K (i.e. a finite nonempty set of primes of K containing the set of all infinite primes). Let $R=R_K(\mathcal{S})$ be the ring of $\mathcal{S}$-*integers* of the field K (the Hasse domain),

$$R_K(\mathcal{S})=\{g\in K:\operatorname{ord}_{\mathfrak{P}} g\ge 0 \text{ for all primes } \mathfrak{P}\notin\mathcal{S}\}.$$

From [Cz3, Theorem 4.2] it follows that if K is a nonreal field, then the group $\phi(WR_K(\mathcal{S}))$ is additively generated by some rank one forms $\langle g\rangle$, $g\in E(R_K(\mathcal{S}))$, and some 2-fold Pfister forms $\langle\langle f,d\rangle\rangle$. If K is formally real, then $\phi(WR_K(\mathcal{S}))$ is generated by forms $\langle g\rangle$, $g\in E(R_K(\mathcal{S}))$, 2-fold Pfister forms $\langle\langle f,d\rangle\rangle$ and some forms $\langle z,-ez\rangle$, $e\in E(R_K(\mathcal{S}))$ (cf. [Cz3, Theorem 4.7]). In Sections 2 and 6 we formulate necessary and sufficient conditions for

$$\langle g\rangle,\langle\langle f,d\rangle\rangle,\langle z,-ez\rangle\in\operatorname{im}(\phi\circ\varphi)$$

to hold in the case of any Dedekind domain R and its field of fractions K (a global field of characteristic not necessarily different from 2).

If $\langle a_1, \dots, a_l\rangle \in WK$ (i.e. $a_1, \dots, a_l \in \dot{K}$), then we often assume that $a_1, \dots, a_l \in \mathcal{O}$, thanks to the following observation. For every $i \in \{1, \dots, l\}$ there exist $x_i, y_i \in \mathcal{O} \setminus \{0\}$ such that $a_i = x_i/y_i$. Then $x_i y_i \in \mathcal{O}$. Moreover, $a_i\dot{K}^2 = x_i y_i \dot{K}^2$, so

$$\langle a_1, \dots, a_l\rangle = \langle x_1y_1, \dots, x_ly_l\rangle \quad \text{in } WK.$$

Throughout the paper, ϕ and φ will denote the natural homomorphisms $\phi\colon WR \to WK$ and $\varphi\colon W\mathcal{O} \to WR$ for a suitable Dedekind domain R, respectively. Whenever we write "$R < K$", we mean "R is a Dedekind domain and K is its field of fractions".

2. Forms of rank 1. Assume K is a global field, $R < K$ is a Dedekind domain and $\mathcal{O} < R$ is an order.

LEMMA 2.1. *Let $\langle (N, \beta)\rangle \in \phi(WR)$ and let $\det\beta$ be the determinant of the form β in a fixed basis of the space N over K. If $\langle (N, \beta)\rangle \in \operatorname{im}(\phi \circ \varphi)$, then there exists an ideal I of the order $\mathcal{O}$ and an element $k \in \dot{K}$ such that*

$$I^2 = (\det\beta \cdot k^2)\mathcal{O}.$$

Proof. Assume

$$\phi \circ \varphi\langle (M, \alpha)\rangle = \langle (N, \beta)\rangle,$$

where $M = I \oplus \mathcal{O}^{n-1}$, $n \ge 1$, and I is an ideal of $\mathcal{O}$ such that $I^2 = p\mathcal{O}$ for some $0 \ne p \in \mathcal{O}$ (cf. [W, Chapter I, Propositions 3.4, 3.5], [CS, Theorem 2.6]). Moreover, $\alpha\colon M \times M \to \mathcal{O}$ is a nonsingular $\mathcal{O}$-bilinear form defined by

$$\alpha((x, y_1, \dots, y_{n-1}), (x', y'_1, \dots, y'_{n-1})) = \frac{a}{p}xx' + \sum_{i=1}^{n-1} \frac{b_i}{p}(y_i x' + x y'_i) + \sum_{i,j=1}^{n-1} \frac{c_{ij}}{p} y_i y'_j$$

for all $(x, y_1, \dots, y_{n-1}), (x', y'_1, \dots, y'_{n-1}) \in M$, where $a \in R$, $b_i \in I$, $c_{ij} = c_{ji} \in I^2$ are uniquely determined (cf. [Ro, Proposition 2.8]). The determinant of

$$A = \begin{bmatrix} a & b_1 & b_2 & \cdots & b_{n-1} \\ b_1 & c_{11} & c_{12} & \cdots & c_{1\,n-1} \\ b_2 & c_{21} & c_{22} & \cdots & c_{2\,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & c_{n-1\,1} & c_{n-1\,2} & \cdots & c_{n-1\,n-1} \end{bmatrix}$$

is equal to $p^{n-1} \cdot u$ for some invertible $u \in \mathcal{O}$ (cf. [Ro, Theorem 2.9]).

Consider the basis

$$\mathcal{B} = (1 \otimes (p, 0, \ldots, 0), \ldots, 1 \otimes (0, \ldots, p, \ldots, 0), \ldots, 1 \otimes (0, \ldots, 0, p))$$

of the linear space $M' = K \otimes_{\mathcal{O}} M$ over K. Then the form $\alpha' \colon M' \times M' \to K$ (defined as in (1.1)) has matrix pA in the basis $\mathcal{B}$. Moreover,

$$\langle (M', \alpha') \rangle = \phi \circ \varphi \langle (M, \alpha) \rangle = \langle (N, \beta) \rangle,$$

so there exist metabolic spaces (M_1, α_1) and (N_1, β_1) over K such that

$$(M', \alpha') \perp (M_1, \alpha_1) \cong (N, \beta) \perp (N_1, \beta_1).$$

Therefore

$$\det(pA)\dot{K}^2 = \pm \det \beta \cdot \dot{K}^2, \quad \text{i.e.} \quad p^{2n-1} \cdot u\dot{K}^2 = \pm \det \beta \cdot \dot{K}^2.$$

There exists $k \in \dot{K}$ such that

$$pu = \pm \det \beta \cdot k^2,$$

so $I^2 = p\mathcal{O} = pu\mathcal{O} = (\det \beta \cdot k^2)\mathcal{O}$. ∎

We give a necessary and sufficient condition for $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$ for any $g \in E(R)$.

PROPOSITION 2.2. *Let $R < K$ be a Dedekind domain, $g \in E(R)$ and $\mathcal{O} < R$ be an order. Then $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$ if and only if there exists a fractional ideal I in the field K such that*

$$I^2 = g\mathcal{O}.$$

Proof. ($\Rightarrow$) From Lemma 2.1 it follows that there exists an ideal J of $\mathcal{O}$ and an element $k \in \dot{K}$ such that

$$J^2 = gk^2\mathcal{O}.$$

For the fractional ideal $I = J \cdot k^{-1}$ we have

$$I^2 = g\mathcal{O}.$$

($\Leftarrow$) The map $\alpha \colon I \times I \to \mathcal{O}$ defined by

$$\alpha(x, y) = \frac{1}{g} xy \quad \text{for all } x, y \in I$$

is a nonsingular bilinear form (cf. [CS, Theorem 3.1]). Hence $\langle (I, \alpha) \rangle \in W\mathcal{O}$. Consider the basis $\mathcal{B} = (1 \otimes g)$ of the space $M' = K \otimes_{\mathcal{O}} I$ over K. Then the form $\alpha' \colon M' \times M' \to K$ (defined as in (1.1)) has matrix $[g]$ in the basis $\mathcal{B}$, so

$$\phi \circ \varphi \langle (I, \alpha) \rangle = \langle g \rangle,$$

i.e. $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$. ∎

Now let $\mathfrak{f}$ be the *conductor* of the order $\mathcal{O}$, i.e.

$$\mathfrak{f} = \{x \in R : xR \subseteq \mathcal{O}\}$$

($\mathfrak{f}$ is the greatest ideal of R lying in $\mathcal{O}$). Denote by $\mathcal{J}_{\mathfrak{f}}(R)$ and $\mathcal{J}_{\mathfrak{f}}(\mathcal{O})$ the multiplicative monoids of all invertible ideals of R and $\mathcal{O}$, respectively, relatively prime to the conductor $\mathfrak{f}$, i.e.

$$\mathcal{J}_{\mathfrak{f}}(R) = \{I \lhd R : I \text{ is invertible, } I + \mathfrak{f} = R\},$$
$$\mathcal{J}_{\mathfrak{f}}(\mathcal{O}) = \{I \lhd \mathcal{O} : I \text{ is invertible, } I + \mathfrak{f} = \mathcal{O}\}.$$

We will use the following fact.

PROPOSITION 2.3 ([GHK, Lemma 3(i)]). *Let I be an invertible ideal of the order $\mathcal{O}$. Then I has a unique decomposition*

$$I = I_1 \cdot I_2,$$

where $I_1 \in \mathcal{J}_{\mathfrak{f}}(\mathcal{O})$ has a unique representation as a product of powers of pairwise distinct maximal ideals $\mathfrak{p} \lhd \mathcal{O}$ such that $\mathfrak{p} + \mathfrak{f} = \mathcal{O}$, while I_2 is a product of primary ideals $\mathfrak{q} \lhd \mathcal{O}$ such that $\mathfrak{q} + \mathfrak{f} \neq \mathcal{O}$.

From [GHK, proof of Proposition 4(ii)] it follows that an ideal $\mathfrak{p}$ of $\mathcal{O}$ is maximal if and only if there exists a maximal ideal $\mathfrak{P}$ of R such that

$$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}.$$

Let

$$\mathfrak{f} = \mathfrak{Q}_1^{r_1} \cdots \mathfrak{Q}_n^{r_n}, \qquad r_1, \ldots, r_n \in \mathbb{N},$$

where $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n$ are pairwise distinct maximal ideals of R. By [GHK, p. 93] an ideal $0 \neq I \lhd R$ is relatively prime to the conductor $\mathfrak{f}$ if and only if it has a unique representation as a product of powers of pairwise distinct maximal ideals $\mathfrak{P} \lhd R$, $\mathfrak{P} \notin \{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n\}$.

Also, by [GHK, proof of Proposition 4(ii)] an ideal $\mathfrak{p}$ of $\mathcal{O}$ is a maximal ideal relatively prime to $\mathfrak{f}$ if and only if there exists a unique maximal ideal $\mathfrak{P} \lhd R$ relatively prime to $\mathfrak{f}$ (i.e. $\mathfrak{P} \notin \{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n\}$) such that

$$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}.$$

Moreover, the map $F \colon \mathcal{J}_{\mathfrak{f}}(R) \to \mathcal{J}_{\mathfrak{f}}(\mathcal{O})$ defined by

$$F(I) = I \cap \mathcal{O} \qquad \text{for all } I \in \mathcal{J}_{\mathfrak{f}}(R)$$

is an isomorphism of monoids.

THEOREM 2.4. *Let K be a global field and $R < K$ be a Dedekind domain. Moreover, let $\mathcal{O} < R$ be an order, $\mathfrak{f}$ be the conductor of $\mathcal{O}$ and $g \in E(R) \cap \mathcal{O}$. If $g\mathcal{O} + \mathfrak{f} = \mathcal{O}$, then $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$.*

Proof. First we show that

$$gR \cap \mathcal{O} = g\mathcal{O}.$$

Since $g\mathcal{O} + \mathfrak{f} = \mathcal{O}$, we have

$$g\mathcal{O} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}, \qquad s_1, \ldots, s_m \in \mathbb{N}, \tag{2.1}$$

for some pairwise distinct maximal ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_m \lhd \mathcal{O}$ relatively prime to $\mathfrak{f}$. There exist maximal ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_m$ of R relatively prime to $\mathfrak{f}$ such that

$$\mathfrak{p}_1 = \mathfrak{P}_1 \cap \mathcal{O}, \quad \dots, \quad \mathfrak{p}_m = \mathfrak{P}_m \cap \mathcal{O}.$$

Fix $i \in \{1, \dots, m\}$ and observe that $\mathfrak{p}_i R = \mathfrak{P}_i$. Indeed, $\mathfrak{p}_i R \subseteq \mathfrak{P}_i$, so

$$\mathfrak{p}_i \subseteq \mathfrak{p}_i R \cap \mathcal{O} \subseteq \mathfrak{P}_i \cap \mathcal{O} = \mathfrak{p}_i, \quad \text{i.e.} \quad \mathfrak{p}_i R \cap \mathcal{O} = \mathfrak{P}_i \cap \mathcal{O}.$$

Since $\mathfrak{p}_i R, \mathfrak{P}_i \in \mathcal{J}_{\mathfrak{f}}(R)$ and

$$F\colon \mathcal{J}_{\mathfrak{f}}(R) \to \mathcal{J}_{\mathfrak{f}}(\mathcal{O}), \qquad F(I) = I \cap \mathcal{O},$$

is an isomorphism, $\mathfrak{p}_i R = \mathfrak{P}_i$. Therefore by (2.1),

$$gR = \mathfrak{P}_1^{s_1} \cdots \mathfrak{P}_m^{s_m}.$$

Using the map F we get

$$gR \cap \mathcal{O} = (\mathfrak{P}_1 \cap \mathcal{O})^{s_1} \cdots (\mathfrak{P}_m \cap \mathcal{O})^{s_m} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} = g\mathcal{O}.$$

From the assumption it follows that $g \in E(R) \cap R$, so $gR = J^2$ for some $J \lhd R$. It is easy to observe that J is relatively prime to $\mathfrak{f}$. Using again the isomorphism F we get

$$g\mathcal{O} = gR \cap \mathcal{O} = J^2 \cap \mathcal{O} = (J \cap \mathcal{O})^2,$$

so $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$ by Proposition 2.2. ∎

We will prove that the existence of $h \in \mathcal{O}$ such that

$$h\dot{K}^2 = g\dot{K}^2 \quad \text{and} \quad h\mathcal{O} + \mathfrak{f} = \mathcal{O}$$

is a necessary and sufficient condition for $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$.

Lemma 2.5. *Let $\mathfrak{q}$ be a primary ideal of the order $\mathcal{O}$ such that $\mathfrak{q} + \mathfrak{f} \neq \mathcal{O}$. Then the radical* $\operatorname{rad}\mathfrak{q}$ *of the ideal $\mathfrak{q}$ is a maximal ideal in $\mathcal{O}$ such that*

$$\operatorname{rad}\mathfrak{q} + \mathfrak{f} \neq \mathcal{O}.$$

Proof. Since $\mathfrak{q}$ is a primary ideal, $\operatorname{rad}\mathfrak{q}$ is a prime ideal. But $\mathcal{O}$ is a one-dimensional domain, so $\operatorname{rad}\mathfrak{q}$ is a maximal ideal.

Suppose $\operatorname{rad}\mathfrak{q} + \mathfrak{f} = \mathcal{O}$. We know that $\mathfrak{f} \subseteq \operatorname{rad}\mathfrak{f}$, so $\operatorname{rad}\mathfrak{q} + \operatorname{rad}\mathfrak{f} = \mathcal{O}$. Hence $\mathfrak{q} + \mathfrak{f} = \mathcal{O}$, a contradiction. ∎

Lemma 2.6. *Let $\mathfrak{f} = \mathfrak{Q}_1^{r_1} \cdots \mathfrak{Q}_n^{r_n}$, $r_1, \dots, r_n \in \mathbb{N}$, be the representation of the conductor $\mathfrak{f}$ of the order $\mathcal{O}$ as a product of powers of pairwise distinct maximal ideals of the Dedekind domain R. Moreover, let $\mathfrak{q}$ be a primary ideal in $\mathcal{O}$ such that $\mathfrak{q} + \mathfrak{f} \neq \mathcal{O}$. Then*

$$\mathfrak{q}R = \mathfrak{Q}_{i_1}^{s_1} \cdots \mathfrak{Q}_{i_m}^{s_m}$$

for some $s_1, \dots, s_m \in \mathbb{N}$ and pairwise distinct $i_1, \dots, i_m \in \{1, \dots, n\}$.

Proof. First observe that $\mathfrak{q}R \neq R$. Indeed, since $\mathfrak{q} \neq \mathcal{O}$, there exists a maximal ideal $\mathfrak{P} \cap \mathcal{O}$ of $\mathcal{O}$ such that

$$\mathfrak{q} \subseteq \mathfrak{P} \cap \mathcal{O}$$

($\mathfrak{P}$ is a maximal ideal of R). If $\mathfrak{q}R = R$, then

$$R = \mathfrak{q}R \subseteq (\mathfrak{P} \cap \mathcal{O})R \subseteq \mathfrak{P},$$

which is impossible.

Suppose that in the decomposition of the ideal $\mathfrak{q}R$ there is a maximal ideal $\mathfrak{P} \lhd R$ such that $\mathfrak{P} \notin \{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n\}$ (i.e. $\mathfrak{P} + \mathfrak{f} = R$). Then $\mathfrak{q}R \subseteq \mathfrak{P}$, so

$$\mathfrak{q} \subseteq \mathfrak{q}R \cap \mathcal{O} \subseteq \mathfrak{P} \cap \mathcal{O}.$$

The ideal $\mathfrak{P} \cap \mathcal{O}$ is a maximal ideal of $\mathcal{O}$ relatively prime to $\mathfrak{f}$. Moreover,

$$\operatorname{rad} \mathfrak{q} \subseteq \operatorname{rad}(\mathfrak{P} \cap \mathcal{O}) = \mathfrak{P} \cap \mathcal{O}. \tag{2.2}$$

From Lemma 2.5 it follows that $\operatorname{rad} \mathfrak{q}$ is a maximal ideal such that $\operatorname{rad} \mathfrak{q} + \mathfrak{f} \neq \mathcal{O}$. However, by (2.2), $\operatorname{rad} \mathfrak{q} = \mathfrak{P} \cap \mathcal{O}$, which leads to a contradiction. ∎

COROLLARY 2.7. *Let I be an invertible ideal of the order $\mathcal{O}$. Then*

$$I + \mathfrak{f} = \mathcal{O} \ \Leftrightarrow \ IR + \mathfrak{f} = R.$$

Proof. The implication "$\Rightarrow$" is obvious.

Assume $IR + \mathfrak{f} = R$. Suppose $I + \mathfrak{f} \neq \mathcal{O}$. From Proposition 2.3 it follows that in a representation of the ideal I there is a primary ideal $\mathfrak{q}$ of $\mathcal{O}$ such that $\mathfrak{q} + \mathfrak{f} \neq \mathcal{O}$. However, Lemma 2.6 shows that $\mathfrak{q}R \subseteq \mathfrak{Q}$ for some ideal $\mathfrak{Q} \lhd R$ in the decomposition of $\mathfrak{f}$. Hence $IR \subseteq \mathfrak{Q}$, i.e. $IR + \mathfrak{f} \neq R$, which is impossible. ∎

Now we prove a lemma which is true for any integral domain, not necessarily an order.

LEMMA 2.8. *Let P be an integral domain, I be an invertible ideal of P and $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \lhd P$ be pairwise distinct maximal ideals. Then*

$$I \neq I\mathfrak{p}_1 \cup \cdots \cup I\mathfrak{p}_m.$$

Proof. Of course $I\mathfrak{p}_1 \cup \cdots \cup I\mathfrak{p}_m \subseteq I$. We show by induction on m that

$$I \nsubseteq I\mathfrak{p}_1 \cup \cdots \cup I\mathfrak{p}_m.$$

For $m = 1$, if $I \subseteq I\mathfrak{p}_1$, then

$$I^{-1} \cdot I \subseteq I^{-1} \cdot I\mathfrak{p}_1,$$

i.e. $P \subseteq \mathfrak{p}_1$, a contradiction.

Suppose

$$I \subseteq I\mathfrak{p}_1 \cup \cdots \cup I\mathfrak{p}_{m-1} \cup I\mathfrak{p}_m.$$

By the induction assumption

$$I \nsubseteq I\mathfrak{p}_1 \cup \cdots \cup I\mathfrak{p}_{m-1}.$$

Choose an element

$$x \in I\mathfrak{p}_m \setminus (I\mathfrak{p}_1 \cup \cdots \cup I\mathfrak{p}_{m-1}). \tag{2.3}$$

We prove that

$$I\mathfrak{p}_1 \cap \cdots \cap I\mathfrak{p}_{m-1} \nsubseteq I\mathfrak{p}_m.$$

Indeed, if $I\mathfrak{p}_1 \cap \cdots \cap I\mathfrak{p}_{m-1} \subseteq I\mathfrak{p}_m$, then

$$I \cdot (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{m-1}) \subseteq I\mathfrak{p}_1 \cap \cdots \cap I\mathfrak{p}_{m-1} \subseteq I\mathfrak{p}_m,$$

i.e. $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{m-1} \subseteq \mathfrak{p}_m$. Since $\mathfrak{p}_1, \ldots, \mathfrak{p}_{m-1}$ are pairwise distinct (so relatively prime) maximal ideals,

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{m-1} \subseteq \mathfrak{p}_m.$$

Hence $\mathfrak{p}_i = \mathfrak{p}_m$ for some $i \in \{1, \ldots, m-1\}$, which is impossible.

Choose an element

$$y \in (I\mathfrak{p}_1 \cap \cdots \cap I\mathfrak{p}_{m-1}) \setminus I\mathfrak{p}_m.$$

Because I is an ideal, $x + y \in I$. There exists $i \in \{1, \ldots, m\}$ such that $x + y \in I\mathfrak{p}_i$.

If $i \in \{1, \ldots, m-1\}$, then $x \in I\mathfrak{p}_i$. This contradicts (2.3). If $i = m$, then $y \in I\mathfrak{p}_m$. This is also impossible. ∎

THEOREM 2.9. *Let K be a global field and $R < K$ be a Dedekind domain. Moreover, let $\mathcal{O} < R$ be an order, $\mathfrak{f}$ be the conductor of $\mathcal{O}$ and $g \in E(R) \cap \mathcal{O}$. Then $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$ if and only if there exists $h \in \mathcal{O}$ such that*

$$h\dot{K}^2 = g\dot{K}^2 \quad \textit{and} \quad hR + \mathfrak{f} = R.$$

Proof. ($\Rightarrow$) From Lemma 2.1 it follows that there exists an ideal J of $\mathcal{O}$ and an element $k \in \dot{K}$ such that

$$J^2 = gk^2\mathcal{O}.$$

Since $k = k_1/k_2$ for some $k_1, k_2 \in \mathcal{O} \setminus \{0\}$,

$$I^2 = gk_1^2\mathcal{O}, \tag{2.4}$$

where $I = Jk_2$ is an invertible ideal of $\mathcal{O}$.

From [GHK, proof of Proposition 4(ii)] it follows that there are only finitely many maximal ideals in $\mathcal{O}$ which are not relatively prime to $\mathfrak{f}$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be all the pairwise distinct maximal ideals of $\mathcal{O}$ such that

$$\mathfrak{p}_i + \mathfrak{f} \neq \mathcal{O} \quad \text{for each } i \in \{1, \ldots, m\}.$$

There exists an element

$$x \in I \setminus (I\mathfrak{p}_1 \cup \cdots \cup I\mathfrak{p}_m). \tag{2.5}$$

Obviously $x \neq 0$ and $x\mathcal{O} \subseteq I$. Moreover, $xI^{-1} \subseteq \mathcal{O}$ is an invertible ideal of $\mathcal{O}$.

Notice that $xI^{-1} + \mathfrak{f} = \mathcal{O}$. Indeed, otherwise by Proposition 2.3 there exists a primary ideal $\mathfrak{q} \lhd \mathcal{O}$ such that

$$\mathfrak{q} + \mathfrak{f} \neq \mathcal{O} \quad \text{and} \quad xI^{-1} \subseteq \mathfrak{q}.$$

But $\mathfrak{q} \subseteq \operatorname{rad}\mathfrak{q}$ and Lemma 2.5 shows that $\operatorname{rad}\mathfrak{q}$ is a maximal ideal in $\mathcal{O}$ such that $\operatorname{rad}\mathfrak{q} + \mathfrak{f} \neq \mathcal{O}$. Therefore

$$xI^{-1} \subseteq \mathfrak{q} \subseteq \operatorname{rad}\mathfrak{q} = \mathfrak{p}_i$$

for some $i \in \{1, \dots, m\}$. Hence $x\mathcal{O} \subseteq I\mathfrak{p}_i$, i.e. $x \in I\mathfrak{p}_i$. This contradicts (2.5).

Proposition 2.3 implies that the ideal xI^{-1} has a unique representation as a product of powers of maximal ideals of $\mathcal{O}$ relatively prime to $\mathfrak{f}$.

Since $x^2 \in I^2$, by (2.4) there exists a nonzero $h \in \mathcal{O}$ such that

$$x^2 = gk_1^2 h. \tag{2.6}$$

Of course $h\dot{K}^2 = g\dot{K}^2$. We show that $h\mathcal{O} + \mathfrak{f} = \mathcal{O}$. Indeed, otherwise by Proposition 2.3 there exists a primary ideal $\mathfrak{q}_1 \lhd \mathcal{O}$ such that

$$\mathfrak{q}_1 + \mathfrak{f} \neq \mathcal{O} \quad \text{and} \quad h\mathcal{O} \subseteq \mathfrak{q}_1.$$

Therefore by (2.6),

$$x^2\mathcal{O} = gk_1^2\mathcal{O} \cdot h\mathcal{O} \subseteq I^2\mathfrak{q}_1,$$

i.e. $(xI^{-1})^2 \subseteq \mathfrak{q}_1$. But the ideal $(xI^{-1})^2$ is a product of powers of maximal ideals of $\mathcal{O}$ relatively prime to $\mathfrak{f}$, so

$$(xI^{-1})^2 + \mathfrak{f} = \mathcal{O}.$$

Hence $\mathfrak{q}_1 + \mathfrak{f} = \mathcal{O}$, a contradiction.

Thus, $h\mathcal{O} + \mathfrak{f} = \mathcal{O}$, so $hR + \mathfrak{f} = R$.

($\Leftarrow$) By assumption, $h\dot{K}^2 = g\dot{K}^2$, so $h \in E(R) \cap \mathcal{O}$ and $\langle g \rangle = \langle h \rangle$ in the Witt ring WK. Corollary 2.7 yields $h\mathcal{O} + \mathfrak{f} = \mathcal{O}$, so $\langle g \rangle = \langle h \rangle \in \operatorname{im}(\phi \circ \varphi)$, by Theorem 2.4. ∎

COROLLARY 2.10. *Let $\mathfrak{f} = \mathfrak{Q}_1^{r_1} \cdots \mathfrak{Q}_n^{r_n}$, $r_1, \dots, r_n \in \mathbb{N}$, be the representation of the conductor $\mathfrak{f}$ of the order $\mathcal{O}$ as a product of powers of pairwise distinct maximal ideals of the Dedekind domain R. Moreover, let $g \in E(R) \cap \mathcal{O}$. Then $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$ if and only if there exists $h \in \mathcal{O}$ such that $h\dot{K}^2 = g\dot{K}^2$ and the ideal hR has a unique representation as a product of powers of pairwise distinct maximal ideals $\mathfrak{P} \notin \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_n\}$.*

3. Quadratic number fields. As an example we examine the surjectivity of the natural homomorphism $\varphi\colon W\mathcal{O} \to WR$ in the case when K is some quadratic number field and $R = R_K$ is the ring of algebraic integers of K.

Let $K = \mathbb{Q}(\sqrt{D})$, where D is a square-free integer. Assume $p_1, \dots, p_s$ are all the pairwise distinct prime divisors of the discriminant of the field K (if

$D \equiv 3 \pmod 4$, then we assume $p_1 = 2$). From [Cz1, pp. 110, 116–117] it follows that in the case when K is a nonreal field ($D < 0$) the set

$$\begin{aligned} \{\langle 1\rangle, \langle p_1\rangle, \dots, \langle p_{s-1}\rangle\} &\quad \text{when } D \neq -1, \\ \{\langle 1\rangle, \langle 2\rangle\} &\quad \text{when } D = -1, \end{aligned}$$

generates the group $\phi(WR_K)$.

Assume K is a real field ($D > 0$). Then K has two real infinite primes ∞_1, ∞_2. From [Cz1, pp. 114, 117–119] it follows that the set

$$\{\langle 1\rangle, \langle p_1\rangle, \dots, \langle p_{s-1}\rangle\}$$

is contained in the set of generators of the group $\phi(WR_K)$.

Let $N_{K/\mathbb{Q}}(\dot{K})$ denote the norm group of the extension $K/\mathbb{Q}$. If $-1 \in N_{K/\mathbb{Q}}(\dot{K})$, then there exists $b \in E(R_K)$ that is positive at ∞_1 and negative at ∞_2 (cf. [Cz2, proof of Proposition 3.2]). Moreover, the class $\langle b\rangle$ belongs to the set of generators of the group $\phi(WR_K)$. In particular, if $D \not\equiv 1 \pmod 8$, then the set

$$\{\langle 1\rangle, \langle p_1\rangle, \dots, \langle p_{s-1}\rangle, \langle b\rangle\}$$

generates $\phi(WR_K)$ (cf. [Cz1, pp. 114, 117]).

Let $K = \mathbb{Q}(\sqrt{D})$ be any quadratic number field. It is known that

$$R_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{when } D \not\equiv 1 \pmod 4, \\ \mathbb{Z}[(1+\sqrt{D})/2] & \text{when } D \equiv 1 \pmod 4. \end{cases}$$

Moreover, $\mathcal{O} < R_K$ is an order if and only if there exists $m \in \mathbb{N}$ such that

$$\mathcal{O} = \begin{cases} \mathbb{Z}[m\sqrt{D}] & \text{when } D \not\equiv 1 \pmod 4, \\ \mathbb{Z}[m(1+\sqrt{D})/2] & \text{when } D \equiv 1 \pmod 4 \end{cases}$$

(cf. [BC, p. 151]). The conductor $\mathfrak{f}$ of $\mathcal{O}$ is then the principal ideal generated by m, $\mathfrak{f} = mR_K$.

Proposition 3.1. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field, $\mathcal{O} < R_K$ be an order and $\mathfrak{f} = mR_K$ be its conductor. Let $p \in E(R_K)$ be a prime number satisfying one of the following two conditions:*

(i) $p \nmid m$,
(ii) $p \mid m$ *and* $p \mid D$.

Then $\langle p\rangle \in \operatorname{im}(\phi \circ \varphi)$.

Proof. (i) Since $\gcd(p, m) = 1$, there exist $x, y \in \mathbb{Z}$ such that

$$px + my = 1.$$

In particular $pR_K + \mathfrak{f} = R_K$, so $\langle p\rangle \in \operatorname{im}(\phi \circ \varphi)$.

(ii) Assume $m = p^r \cdot m'$ for some $r, m' \in \mathbb{N}$ and $p \nmid m'$. Consider the element

$$z := p^{r+1} \cdot m + m' \cdot m\sqrt{D} \in \mathcal{O}.$$

Then

$$z^2 = pm^2 \cdot \left[\left(p^{2r+1} + m'^2 \cdot \frac{D}{p}\right) + 2m\sqrt{D}\right] = pm^2 \cdot h.$$

Moreover, $h \in \mathcal{O}$ and $h\dot{K}^2 = p\dot{K}^2$. Since $p \nmid m'$ and D is a square-free integer, it is easy to observe that

$$\gcd\left(p^{2r+1}, m'^2 \cdot \frac{D}{p}\right) = 1.$$

Hence

$$p^{2r+1}R_K + m'^2 \cdot \frac{D}{p} R_K = R_K.$$

We show that $hR_K + \mathfrak{f} = R_K$. Indeed, otherwise there exists a maximal ideal $\mathfrak{Q}$ in the representation of the conductor $\mathfrak{f} = mR_K$ which is also in the representation of the ideal hR_K. Then $hR_K \subseteq \mathfrak{Q}$, i.e. $h \in \mathfrak{Q}$. But $2m\sqrt{D} \in \mathfrak{f} \subseteq \mathfrak{Q}$, so

$$p^{2r+1} + m'^2 \cdot \frac{D}{p} \in \mathfrak{Q}. \tag{3.1}$$

Because $p^r \cdot m' = m \in \mathfrak{Q}$, either $p \in \mathfrak{Q}$ or $m' \in \mathfrak{Q}$. In both cases, by (3.1),

$$p^{2r+1} \in \mathfrak{Q} \quad \text{and} \quad m'^2 \cdot \frac{D}{p} \in \mathfrak{Q}.$$

Therefore

$$R_K = p^{2r+1}R_K + m'^2 \cdot \frac{D}{p} R_K \subseteq \mathfrak{Q},$$

which is impossible.

Finally, from Theorem 2.9 it follows that $\langle p \rangle \in \operatorname{im}(\phi \circ \varphi)$. ∎

Observe that every prime divisor p_i, $i \in \{1, \ldots, s\}$, of the discriminant of the field $K = \mathbb{Q}(\sqrt{D})$ is a divisor of the integer D (except for $p_1 = 2$ in the case when $D \equiv 3 \pmod 4$).

Corollary 3.2. *Let $K = \mathbb{Q}(\sqrt{D})$ be a nonreal quadratic number field with $D \not\equiv 3 \pmod 4$. Moreover, let $\mathcal{O}$ be an order. Then the natural homomorphism $\varphi \colon W\mathcal{O} \to WR_K$ is surjective.*

Corollary 3.3. *Let $K = \mathbb{Q}(\sqrt{D})$ be a nonreal quadratic number field with $D \equiv 3 \pmod 4$. Moreover, let $\mathcal{O} = \mathbb{Z}[m\sqrt{D}]$ be an order such that $2 \nmid m$. Then the natural homomorphism $\varphi \colon W\mathcal{O} \to WR_K$ is surjective.*

Proposition 3.4. *Let $K = \mathbb{Q}(\sqrt{D})$ be any quadratic number field with $D \equiv 3 \pmod 4$. If $\mathcal{O} = \mathbb{Z}[m\sqrt{D}]$ is an order such that $2 \mid m$, then*

$$\langle p_1 \rangle = \langle 2 \rangle \notin \operatorname{im}(\phi \circ \varphi).$$

Proof. First assume $m = 2$. Denote $\mathcal{O}_1 := \mathbb{Z}[2\sqrt{D}]$ and suppose that $\langle 2 \rangle \in \operatorname{im}(\phi \circ \varphi_1)$, where $\varphi_1 \colon W\mathcal{O}_1 \to WR_K$ is the natural homomorphism.

In the same way as in (2.4), from Lemma 2.1 it follows that there exists an ideal I of $\mathcal{O}_1$ and an element $k_1 \in \mathcal{O}_1 \setminus \{0\}$ such that

$$I^2 = 2k_1^2\mathcal{O}_1.$$

Multiplying the above equality by the principal ideal of $\mathcal{O}_1$ generated by the element conjugate to k_1^2, we obtain

$$T^2 = 2n^2\mathcal{O}_1$$

for some ideal T of $\mathcal{O}_1$ and $n \in \mathbb{N}$. We will show that this is impossible.

Assume $2 \nmid n$. Then for every $x + 2y\sqrt{D} \in T$, where $x, y \in \mathbb{Z}$, we have

$$2 \mid (x + 2y\sqrt{D})^2.$$

Hence $2 \mid x$, so in particular the rational part of every element of the ideal T^2 is divisible by 4. But $2n^2 \in T^2 \cap \mathbb{N}$ and $2 \nmid n$, a contradiction.

Assume $n = 2^r \cdot n'$ for some $r, n' \in \mathbb{N}$ and $2 \nmid n'$. Then

$$T^2 = 2^{2r+1} \cdot n'^2\mathcal{O}_1. \tag{3.2}$$

Since $2r + 1 \geq 3$, for every $x + 2y\sqrt{D} \in T$ we have

$$2^3 \mid (x + 2y\sqrt{D})^2 \quad \text{in } \mathcal{O}_1 = \mathbb{Z}[2\sqrt{D}].$$

Hence

$$2^3 \mid (x^2 + 4y^2D) \quad \text{and} \quad 2^2 \mid xy.$$

By assumption, $D \equiv 3 \pmod 4$, so $2 \mid x$ and $2 \mid y$. Therefore

$$2 \mid (x + 2y\sqrt{D}) \quad \text{in } \mathcal{O}_1.$$

There exists an ideal T_1 of $\mathcal{O}_1$ such that

$$T = 2\mathcal{O}_1 \cdot T_1,$$

i.e. by (3.2),

$$T_1^2 = 2^{2r-1} \cdot n'^2\mathcal{O}_1,$$

where $2r - 1 \geq 1$.

Repeating this procedure until $2r - 1 = 1$, we prove that there exists an ideal T' of $\mathcal{O}_1$ such that

$$T'^2 = 2n'^2\mathcal{O}_1.$$

But $2 \nmid n'$, so this is impossible.

To sum up, we have shown that if $\mathcal{O}_1 = \mathbb{Z}[2\sqrt{D}]$, then $\langle 2\rangle \notin \operatorname{im}(\phi \circ \varphi_1)$.

Assume that $\mathcal{O} = \mathbb{Z}[m\sqrt{D}]$ is any order such that $2 \mid m$. Suppose that $\langle 2\rangle \in \operatorname{im}(\phi \circ \varphi)$. By Theorem 2.9 there exists $h \in \mathcal{O}$ such that

$$h\dot{K}^2 = 2\dot{K}^2 \quad \text{and} \quad hR_K + mR_K = R_K.$$

But

$$\mathbb{Z}[m\sqrt{D}] \subseteq \mathbb{Z}[2\sqrt{D}] = \mathcal{O}_1,$$

so $h \in \mathcal{O}_1$. Moreover,

$$R_K = hR_K + mR_K \subseteq hR_K + 2R_K, \quad \text{i.e.} \quad hR_K + 2R_K = R_K.$$

Using again Theorem 2.9 we get $\langle 2 \rangle \in \operatorname{im}(\phi \circ \varphi_1)$, a contradiction. Thus, $\langle 2 \rangle \notin \operatorname{im}(\phi \circ \varphi)$. ∎

COROLLARY 3.5. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \equiv 3 \pmod 4$. Moreover, let $\mathcal{O} = \mathbb{Z}[m\sqrt{D}]$ be an order such that $2 \mid m$. Then $\varphi\colon W\mathcal{O} \to WR_K$ is not surjective.*

Now assume $K = \mathbb{Q}(\sqrt{D})$ is a real field with $-1 \in N_{K/\mathbb{Q}}(\dot{K})$. If $p_1, \ldots, p_s$ are all the pairwise distinct prime divisors of the discriminant of K, then the condition $-1 \in N_{K/\mathbb{Q}}(\dot{K})$ can be replaced by $p_i \equiv 1, 2 \pmod 4$ for $i = 1, \ldots, s$.

We give a necessary and sufficient condition for $\langle b \rangle \in \operatorname{im}(\phi \circ \varphi)$, where $b \in E(R_K) \cap \mathcal{O}$ is positive at ∞_1 and negative at ∞_2.

In elementary number theory the following fact is known.

PROPOSITION 3.6. *Let $c = 2^r q_1 \cdots q_l$, where $r \in \mathbb{N} \cup \{0\}$ and $q_1, \ldots, q_l$ are odd prime numbers. Then the equation $X^2 + Y^2 = c$ has a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $\gcd(x, y, c) = 1$ if and only if $r \in \{0, 1\}$ and $q_i \equiv 1 \pmod 4$ for every $i \in \{1, \ldots, l\}$.*

PROPOSITION 3.7. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field with $D \equiv 1 \pmod 4$ and $-1 \in N_{K/\mathbb{Q}}(\dot{K})$. Let $\mathcal{O} = \mathbb{Z}[m(1 + \sqrt{D})/2]$ be an order with $m = 2^r q_1 \cdots q_l$, where $r \in \mathbb{N} \cup \{0\}$ and $q_1, \ldots, q_l$ are odd prime numbers. Moreover, let $b \in E(R_K) \cap \mathcal{O}$ be positive at ∞_1 and negative at ∞_2. Then $\langle b \rangle \in \operatorname{im}(\phi \circ \varphi)$ if and only if $r \in \{0, 1\}$ and $q_i \equiv 1 \pmod 4$ for every $i \in \{1, \ldots, l\}$.*

Proof. ($\Rightarrow$) By Theorem 2.9 there exists $h = x + ym(1 + \sqrt{D})/2 \in \mathcal{O}$ such that

$$h\dot{K}^2 = b\dot{K}^2 \quad \text{and} \quad hR_K + \mathfrak{f} = R_K.$$

Because $N_{K/\mathbb{Q}}(h) < 0$ and $h \in E(R_K) \cap \mathcal{O}$, we have

$$N_{K/\mathbb{Q}}(h) = -t^2 \quad \text{for some } t \in \mathbb{N}.$$

Observe that

$$-t^2 = N_{K/\mathbb{Q}}(h) = h\overline{h} = x^2 + m \cdot \left[xy + \frac{y^2}{4} m(1 - D) \right],$$

where $\overline{h}$ denotes the element conjugate to h. Since $D \equiv 1 \pmod 4$,

$$a := xy + \frac{y^2}{4} m(1 - D) \in \mathbb{Z}.$$

Hence

$$x^2 + t^2 = -ma, \quad \text{where } -ma \in \mathbb{N}. \tag{3.3}$$

We assume $\gcd(x^2,t^2,a)$ is a square-free integer (if $n^2 \mid \gcd(x^2,t^2,a)$ for some $n\in\mathbb{N}$, then we divide (3.3) by n^2).

Suppose either $r>1$, or $q_i \equiv 3 \pmod 4$ for some $i\in\{1,\dots,l\}$. By Proposition 3.6 there exists a prime number p such that $p\mid x$, $p\mid t$ and $p^2\mid ma$. Since $\gcd(x^2,t^2,a)$ is a square-free integer, $p\mid m$. Hence $p \mid (x+ym(1+\sqrt{D})/2)$ in the ring R_K, i.e.

$$hR_K+\mathfrak{f}=hR_K+mR_K\neq R_K,$$

a contradiction.

($\Leftarrow$) Let

$$m_1 := \begin{cases} m & \text{when } 2\nmid m,\\ m/2 & \text{when } 2\mid m.\end{cases}$$

Obviously $m_1\equiv 1 \pmod 2$.

Since $D\equiv 1 \pmod 4$ and $-1\in N_{K/\mathbb{Q}}(\dot{K})$, every prime divisor of D is congruent to 1 modulo 4. By Proposition 3.6 there exist $x,y\in\mathbb{Z}$ such that

$$x^2+y^2=m_1^2D \quad\text{and}\quad \gcd(x,y,m_1^2D)=1.$$

We assume $y\equiv 1 \pmod 2$.

Consider

$$g := x+m_1\sqrt{D} = \begin{cases} (x-m)+2m(1+\sqrt{D})/2 & \text{when } 2\nmid m,\\ (x-m_1)+m(1+\sqrt{D})/2 & \text{when } 2\mid m.\end{cases}$$

Observe that $g\in\mathcal{O}$ and

$$N_{K/\mathbb{Q}}(g)=g\overline{g}=x^2-m_1^2D=-y^2.$$

Moreover, $\gcd(N_{K/\mathbb{Q}}(g),m)=1$, so

$$gR_K+\mathfrak{f}=gR_K+mR_K=R_K.$$

We show that $g\in E(R_K)$.

If $g\in U(R_K)$, then $g\in E(R_K)$. Assume $g\notin U(R_K)$. Let $\mathfrak{P}$ be a maximal ideal in the decomposition of the ideal gR_K. The ideal $\mathfrak{P}$ lies over some prime number p.

(a) If p ramifies in K ($pR_K=\mathfrak{P}^2$), then $p\mid D$. Moreover, $p\mid N_{K/\mathbb{Q}}(g)$, so $\gcd(x,y,m_1^2D)>1$, a contradiction.

(b) If p remains prime in K ($pR_K=\mathfrak{P}$), then $p\mid g$ in R_K. It is easy to observe that $p\mid 2m$ and $p\mid N_{K/\mathbb{Q}}(g)$. If $p\mid m_1$, then $\gcd(x,y,m_1^2D)>1$, which is not the case. If $p=2$, then $2\mid y$, which is not the case either.

(c) Hence p splits in K, $pR_K=\mathfrak{P}\overline{\mathfrak{P}}$. Observe that the ideal $\overline{\mathfrak{P}}$ does not belong to the decomposition of the ideal gR_K. Otherwise, $p\mid g$ in R_K, which is a contradiction. The ideal $\overline{\mathfrak{P}}$ belongs only to the decomposition of the ideal $\overline{g}R_K$. Because

$$gR_K\cdot\overline{g}R_K=(yR_K)^2,$$

we have $\operatorname{ord}_{\mathfrak{P}} g=\operatorname{ord}_{\overline{\mathfrak{P}}}\overline{g}\equiv 0 \pmod 2$. Finally, $g\in E(R_K)\cap\mathcal{O}$.

Theorem 2.9 implies that

$$\langle g\rangle \in \operatorname{im}(\phi\circ\varphi). \tag{3.4}$$

Since $N_{K/\mathbb{Q}}(g) = -y^2$, from [Cz2, Proposition 3.2, p. 36] it follows that

$$b\dot{K}^2 = \pm g p_1^{r_1}\cdots p_{s-1}^{r_{s-1}}\dot{K}^2,$$

where $p_1\dots,p_{s-1}$ are pairwise distinct prime divisors of the discriminant of the field K and $r_i \in \{0,1\}$, $i = 1,\dots,s-1$. Hence

$$\langle b\rangle = \pm\langle g\rangle\langle p_1^{r_1}\rangle\cdots\langle p_{s-1}^{r_{s-1}}\rangle$$

in the Witt ring WK. By (3.4) and Proposition 3.1, $\langle b\rangle \in \operatorname{im}(\phi\circ\varphi)$. ∎

Corollary 3.8. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field with $D \equiv 5 \pmod 8$ and $-1 \in N_{K/\mathbb{Q}}(\dot{K})$. Moreover, let $\mathcal{O} = \mathbb{Z}[m(1+\sqrt{D})/2]$ be an order with $m = 2^r q_1\cdots q_l$, where $r \in \{0,1\}$ and $q_1,\dots,q_l$ are odd prime numbers such that $q_i \equiv 1 \pmod 4$ for every $i \in \{1,\dots,l\}$. Then $\varphi\colon W\mathcal{O} \to WR_K$ is surjective.*

Proof. This follows from statements on page 358 and Propositions 3.1 and 3.7. ∎

Corollary 3.9. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field with $D \equiv 1 \pmod 4$ and $-1 \in N_{K/\mathbb{Q}}(\dot{K})$. Moreover, let $\mathcal{O} = \mathbb{Z}[m(1+\sqrt{D})/2]$ be an order with $m = 2^r q_1\cdots q_l$, where $r \in \mathbb{N}\cup\{0\}$ and $q_1,\dots,q_l$ are odd prime numbers. If either $r > 1$, or $q_i \equiv 3 \pmod 4$ for some $i \in \{1,\dots,l\}$, then $\varphi\colon W\mathcal{O} \to WR_K$ is not surjective.*

Proposition 3.10. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field with $2\,|\,D$ and $-1 \in N_{K/\mathbb{Q}}(\dot{K})$. Let $\mathcal{O} = \mathbb{Z}[m\sqrt{D}]$ be an order with $m = 2^r q_1\cdots q_l$, where $r \in \mathbb{N}\cup\{0\}$ and $q_1,\dots,q_l$ are odd prime numbers. Moreover, let $b \in E(R_K)\cap\mathcal{O}$ be positive at ∞_1 and negative at ∞_2. Then $\langle b\rangle \in \operatorname{im}(\phi\circ\varphi)$ if and only if $r = 0$ and $q_i \equiv 1 \pmod 4$ for every $i \in \{1,\dots,l\}$.*

Proof. ($\Rightarrow$) Theorem 2.9 yields $h = x + ym\sqrt{D} \in \mathcal{O}$ such that

$$h\dot{K}^2 = b\dot{K}^2 \quad\text{and}\quad hR_K + \mathfrak{f} = R_K.$$

As in the proof of the implication "$\Rightarrow$" of Proposition 3.7 we notice that $N_{K/\mathbb{Q}}(h) = -t^2$ for some $t \in \mathbb{N}$. Hence

$$x^2 + t^2 = m^2y^2D.$$

We assume $\gcd(x,t,y) = 1$.

If either $r > 0$, or $q_i \equiv 3 \pmod 4$ for some $i \in \{1,\dots,l\}$, then by Proposition 3.6 there exists a prime number p such that $p\,|\,x$, $p\,|\,t$ and $p^2\,|\,m^2D$. Since D is a square-free integer, $p\,|\,m$. Then $p\,|\,h$ in R_K, so

$$hR_K + \mathfrak{f} = hR_K + mR_K \neq R_K,$$

a contradiction.

($\Leftarrow$) Since $-1 \in N_{K/\mathbb{Q}}(\dot{K})$, every odd prime divisor of D is congruent to 1 modulo 4. Proposition 3.6 gives $x, y \in \mathbb{Z}$ such that

$$x^2 + y^2 = m^2 D \quad \text{and} \quad \gcd(x, y, m^2 D) = 1.$$

Consider $g := x + m\sqrt{D} \in \mathcal{O}$. Obviously,

$$N_{K/\mathbb{Q}}(g) = x^2 - m^2 D = -y^2.$$

Moreover, $\gcd(N_{K/\mathbb{Q}}(g), m) = 1$, so

$$gR_K + \mathfrak{f} = gR_K + mR_K = R_K.$$

As in the proof of the implication "$\Leftarrow$" of Proposition 3.7, we show that $g \in E(R_K)$. Hence $\langle g \rangle \in \operatorname{im}(\phi \circ \varphi)$ and finally,

$$\langle b \rangle = \pm \langle g \rangle \langle p_1^{r_1} \rangle \cdots \langle p_{s-1}^{r_{s-1}} \rangle \in \operatorname{im}(\phi \circ \varphi). \ ■$$

Corollary 3.11. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field with $2 \mid D$ and $-1 \in N_{K/\mathbb{Q}}(\dot{K})$. Moreover, let $\mathcal{O} = \mathbb{Z}[m\sqrt{D}]$ be an order with $m = 2^r q_1 \cdots q_l$, where $r \in \mathbb{N} \cup \{0\}$ and $q_1, \ldots, q_l$ are odd prime numbers. Then $\varphi\colon W\mathcal{O} \to WR_K$ is surjective if and only if $r = 0$ and $q_i \equiv 1 \pmod 4$ for every $i \in \{1, \ldots, l\}$.*

Proof. This follows from page 358 and Propositions 3.1 and 3.10. ■

4. Quadratic function fields. Assume $\mathbb{F}$ is a finite field of characteristic $\neq 2$. Assume ϵ is a generator of the group $\dot{\mathbb{F}}$. Let $F = \mathbb{F}(X)$ be the rational function field over $\mathbb{F}$ and ∞_F be the prime of F with uniformizing parameter $1/X$.

Let $D \in \mathbb{F}[X]$ be a square-free polynomial of degree ≥ 1 and a_d be the leading coefficient of D. We assume a_d is either 1 or ϵ. Let $K = F(\sqrt{D})$.

Theorem 4.1 ([R, Proposition 14.6]).

(i) *If* $\deg D \equiv 1 \pmod 2$*, then ∞_F ramifies in K.*
(ii) *If* $\deg D \equiv 0 \pmod 2$ *and $a_d = 1$, then ∞_F splits in K.*
(iii) *If* $\deg D \equiv 0 \pmod 2$ *and $a_d = \epsilon$, then ∞_F is prime in K.*

The field K is said to be *real* if ∞_F splits in K, and *nonreal* otherwise.

Throughout this section we assume that $\mathcal{S}$ is the set of primes of K which lie over ∞_F. Let

$$D_K(\mathcal{S}) = \{g \in E(R_K(\mathcal{S})) : (-1, g)_{\mathfrak{P}} = 1 \text{ for every } \mathfrak{P} \in \mathcal{S}\},$$

where $(\cdot,\cdot)_{\mathfrak{P}}$ denotes the $\mathfrak{P}$-adic Hilbert symbol. Let $u_K(\mathcal{S})$ denote the 2-rank of the group $E(R_K(\mathcal{S}))/D_K(\mathcal{S})$ (cf. [Cz3, p. 607], [RC, p. 196]).

Assume $p_1, \ldots, p_s \in \mathbb{F}[X]$ are all the pairwise distinct monic irreducible polynomials which divide D. From [RC, Proposition 6.2] it follows that $\epsilon \in N_{K/F}(\dot{K})$ if and only if each p_i has even degree. If $\epsilon \in N_{K/F}(\dot{K})$, then there exists $b \in E(R_K(\mathcal{S}))$ such that $N_{K/F}(b) \in \epsilon\dot{F}^2$ (cf. [RC, Lemma 1.12]). By [RC, p. 208] and [Cz3, Theorem 4.2] the set of classes

$$(4.1)\qquad \begin{aligned} &\{\langle 1\rangle, \langle\epsilon\rangle, \langle p_1\rangle, \ldots, \langle p_{s-1}\rangle, \langle b\rangle\} &&\text{when } \epsilon \in N_{K/F}(\dot{K}),\\ &\{\langle 1\rangle, \langle\epsilon\rangle, \langle p_1\rangle, \ldots, \langle p_{s-1}\rangle\} &&\text{when } \epsilon \notin N_{K/F}(\dot{K}), \end{aligned}$$

is contained in the set of generators of the group $\phi(WR_K(\mathcal{S}))$. In particular, if K is either a nonreal field, or a real field and $u_K(\mathcal{S}) \neq 0$, then the set (4.1) generates $\phi(WR_K(\mathcal{S}))$.

It is known that

$$R_K(\mathcal{S}) = \mathbb{F}[X][\sqrt{D}].$$

Moreover, $\mathcal{O} < R_K(\mathcal{S})$ is an order if and only if there exists $0 \neq m \in \mathbb{F}[X]$ such that

$$\mathcal{O} = \mathbb{F}[X][m\sqrt{D}]$$

(cf. [R, p. 248, Proposition 17.6]). The conductor $\mathfrak{f}$ of $\mathcal{O}$ is the principal ideal generated by m, $\mathfrak{f} = mR_K(\mathcal{S})$.

PROPOSITION 4.2. *Let $K = F(\sqrt{D})$ be a quadratic function field, let $\mathcal{O} < R_K(\mathcal{S})$ be an order and let $\mathfrak{f} = mR_K(\mathcal{S})$ be its conductor. Suppose that $p \in E(R_K(\mathcal{S})) \cap \mathbb{F}[X]$ is an irreducible polynomial satisfying one of the following two conditions:*

(i) *$p \nmid m$,*
(ii) *$p \mid m$ and $p \mid D$.*

Then $\langle p\rangle \in \operatorname{im}(\phi \circ \varphi)$.

Proof. This is proved similarly to Proposition 3.1. ∎

The element ϵ is invertible in $\mathcal{O}$. Hence

$$(4.2)\qquad \langle\epsilon\rangle \in \operatorname{im}(\phi \circ \varphi).$$

COROLLARY 4.3. *Let $K = F(\sqrt{D})$ be a nonreal quadratic function field with $\epsilon \notin N_{K/F}(\dot{K})$. Moreover, let $\mathcal{O} < R_K(\mathcal{S})$ be an order. Then the natural homomorphism $\varphi\colon W\mathcal{O} \to WR_K(\mathcal{S})$ is surjective.*

COROLLARY 4.4. *Let $K = F(\sqrt{D})$ be a real quadratic function field with $\epsilon \notin N_{K/F}(\dot{K})$ and $u_K(\mathcal{S}) \neq 0$. Moreover, let $\mathcal{O} < R_K(\mathcal{S})$ be an order. Then $\varphi\colon W\mathcal{O} \to WR_K(\mathcal{S})$ is surjective.*

Assume $\epsilon \in N_{K/F}(\dot{K})$. We give a necessary and sufficient condition for $\langle b\rangle \in \operatorname{im}(\phi \circ \varphi)$.

LEMMA 4.5. *Let $c = q_1 \cdots q_l$, where $q_1, \ldots, q_l \in \mathbb{F}[X]$ are irreducible. Then the equation $X^2 - \epsilon Y^2 = c$ has a solution $(x, y) \in \mathbb{F}[X] \times \mathbb{F}[X]$ with $\gcd(x, y, c) \sim 1$ if and only if $\deg q_i \equiv 0 \pmod 2$ for every $i \in \{1, \ldots, l\}$.*

Proof. ($\Rightarrow$) Suppose $\deg q_i \equiv 1 \pmod 2$ for some $i \in \{1, \ldots, l\}$. Obviously, $x^2 - \epsilon y^2 \equiv 0 \pmod{q_i}$. Because $\gcd(x, y, c) \sim 1$, we have $y \not\equiv 0 \pmod{q_i}$. Then $(x/y)^2 \equiv \epsilon \pmod{q_i}$, i.e. ϵ is a square modulo q_i. This is impossible (cf. [R, Propositions 3.1 3), 3.2]).

($\Leftarrow$) We use induction on l. Fix $i \in \{1, \ldots, l\}$. Because $\deg q_i \equiv 0 \pmod 2$, we have

$$(\epsilon, q_i)_{q_i} = 1 \quad \text{and} \quad (\epsilon, q_i)_{\infty_F} = 1.$$

For every prime $\mathfrak{p} \notin \{q_i, \infty_F\}$ of the field F the elements ϵ, q_i are $\mathfrak{p}$-adic units, so $(\epsilon, q_i)_{\mathfrak{p}} = 1$. From the local-global principle it follows that the form $\langle \epsilon, q_i \rangle$ represents 1 over the field F. It is easy to observe that the form $\langle 1, -\epsilon \rangle$ represents q_i over F. By [P, 2.2 Theorem, Chapter 1] the form $\langle 1, -\epsilon \rangle$ represents q_i over the ring $\mathbb{F}[X]$. Hence there exist $z_i, t_i \in \mathbb{F}[X]$ such that $z_i^2 - \epsilon t_i^2 = q_i$. Obviously, $\gcd(z_i, t_i, q_i) \sim 1$.

Consider the equation $X^2 - \epsilon Y^2 = q_1 \cdots q_l q_{l+1}$. By the induction assumption there exist $x, y \in \mathbb{F}[X]$ such that

$$x^2 - \epsilon y^2 = q_1 \cdots q_l \quad \text{and} \quad \gcd(x, y, q_1 \cdots q_l) \sim 1.$$

Observe that

$$(z_{l+1}x + \epsilon t_{l+1}y)^2 - \epsilon(z_{l+1}y + t_{l+1}x)^2 = q_1 \cdots q_l q_{l+1},$$
$$(z_{l+1}x - \epsilon t_{l+1}y)^2 - \epsilon(z_{l+1}y - t_{l+1}x)^2 = q_1 \cdots q_l q_{l+1}.$$

Using elementary arguments we prove that either

$$\gcd(z_{l+1}x + \epsilon t_{l+1}y, z_{l+1}y + t_{l+1}x, q_1 \cdots q_l q_{l+1}) \sim 1, \quad \text{or}$$
$$\gcd(z_{l+1}x - \epsilon t_{l+1}y, z_{l+1}y - t_{l+1}x, q_1 \cdots q_l q_{l+1}) \sim 1. \ \blacksquare$$

PROPOSITION 4.6. *Let $K = F(\sqrt{D})$ be a quadratic function field with $\epsilon \in N_{K/F}(\dot{K})$. Let $\mathcal{O} = \mathbb{F}[X][m\sqrt{D}]$ be an order with $m = q_1 \cdots q_l$, where $q_1, \ldots, q_l \in \mathbb{F}[X]$ are irreducible polynomials. Moreover, let $b \in E(R_K(\mathcal{S})) \cap \mathcal{O}$ with $N_{K/F}(b) \in \epsilon \dot{F}^2$. Then $\langle b \rangle \in \operatorname{im}(\phi \circ \varphi)$ if and only if $\deg q_i \equiv 0 \pmod 2$ for every $i \in \{1, \ldots, l\}$.*

Proof. Using Lemma 4.5 we prove the implication "$\Rightarrow$" similarly to "$\Rightarrow$" of Proposition 3.10.

($\Leftarrow$) Since $\epsilon \in N_{K/F}(\dot{K})$, every monic irreducible polynomial which divides D has even degree. Lemma 4.5 yields $x, y \in \mathbb{F}[X]$ such that

$$x^2 - \epsilon y^2 = m^2 D \quad \text{and} \quad \gcd(x, y, m^2 D) \sim 1.$$

Consider $g := x + m\sqrt{D} \in \mathcal{O}$. Similarly to the proofs of "$\Leftarrow$" of Propositions 3.7 and 3.10 we show that

$$\langle g \rangle \in \operatorname{im}(\phi \circ \varphi). \tag{4.3}$$

Since $N_{K/F}(g) = \epsilon y^2$, from [RC, p. 208] it follows that

$$b\dot{K}^2 = g\epsilon^r p_1^{r_1} \cdots p_{s-1}^{r_{s-1}} \dot{K}^2,$$

where $p_1, \dots, p_{s-1} \in \mathbb{F}[X]$ are pairwise distinct monic irreducible polynomials which divide D, and $r, r_i \in \{0,1\}$, $i = 1, \dots, s-1$. Hence

$$\langle b\rangle = \langle g\rangle\langle \epsilon^r\rangle\langle p_1^{r_1}\rangle \cdots \langle p_{s-1}^{r_{s-1}}\rangle$$

in WK. By (4.2), (4.3) and Proposition 4.2, $\langle b\rangle \in \operatorname{im}(\phi \circ \varphi)$. ∎

COROLLARY 4.7. *Let $K = F(\sqrt{D})$ be a nonreal quadratic function field with $\epsilon \in N_{K/F}(\dot{K})$. Moreover, let $\mathcal{O} = \mathbb{F}[X][m\sqrt{D}]$ be an order with $m = q_1 \cdots q_l$, where $q_1, \dots, q_l \in \mathbb{F}[X]$ are irreducible polynomials such that* $\deg q_i \equiv 0 \pmod 2$ *for every $i \in \{1, \dots, l\}$. Then the natural homomorphism $\varphi\colon W\mathcal{O} \to WR_K(\mathcal{S})$ is surjective.*

COROLLARY 4.8. *Let $K = F(\sqrt{D})$ be a real quadratic function field with $\epsilon \in N_{K/F}(\dot{K})$ and $u_K(\mathcal{S}) \neq 0$. Moreover, let $\mathcal{O} = \mathbb{F}[X][m\sqrt{D}]$ be an order with $m = q_1 \cdots q_l$, where $q_1, \dots, q_l \in \mathbb{F}[X]$ are irreducible polynomials such that* $\deg q_i \equiv 0 \pmod 2$ *for every $i \in \{1, \dots, l\}$. Then $\varphi\colon W\mathcal{O} \to WR_K(\mathcal{S})$ is surjective.*

Corollaries 4.7 and 4.8 follow from statements on page 365, (4.2) and Propositions 4.2 and 4.6.

COROLLARY 4.9. *Let $K = F(\sqrt{D})$ with $\epsilon \in N_{K/F}(\dot{K})$. Moreover, let $\mathcal{O} = \mathbb{F}[X][m\sqrt{D}]$ be an order with $m = q_1 \cdots q_l$, where $q_1, \dots, q_l \in \mathbb{F}[X]$ are irreducible polynomials. If* $\deg q_i \equiv 1 \pmod 2$ *for some $i \in \{1, \dots, l\}$, then $\varphi\colon W\mathcal{O} \to WR_K(\mathcal{S})$ is not surjective.*

5. Forms of rank ≥ 1. Let K be a global field and $R < K$ be a Dedekind domain. Now we generalize Theorem 2.4.

LEMMA 5.1. *Let $\mathcal{O} < R$ be an order, $\mathfrak{f}$ be its conductor and $\mathfrak{P}$ be a maximal ideal of R such that $\mathfrak{P} + \mathfrak{f} = R$. Then the localisation of the ring R at the ideal $\mathfrak{P}$ is equal to the localisation of $\mathcal{O}$ at the maximal ideal $\mathfrak{P} \cap \mathcal{O}$,*

$$R_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}\cap\mathcal{O}}.$$

Proof. "$\supseteq$" This inclusion is obvious.

"$\subseteq$" Let $x/y \in R_{\mathfrak{P}}$. Then $x, y \in R$ and $y \notin \mathfrak{P}$. Because $\mathfrak{P} + \mathfrak{f} = R$, we have $\mathfrak{f} \not\subseteq \mathfrak{P}$. Choose an element $z \in \mathfrak{f} \setminus \mathfrak{P}$. Then $zx, zy \in \mathcal{O}$ and

$$\frac{x}{y} = \frac{zx}{zy} \in \mathcal{O}_{\mathfrak{P}\cap\mathcal{O}}.$$

Indeed, if $zy \in \mathfrak{P} \cap \mathcal{O}$, then $zy \in \mathfrak{P}$, i.e. either $z \in \mathfrak{P}$ or $y \in \mathfrak{P}$, which is not the case. ∎

COROLLARY 5.2. *Let M be an R-module and $\mathfrak{P}$ be a maximal ideal of R such that $\mathfrak{P} + \mathfrak{f} = R$. Then the localisation of the module M at the ideal $\mathfrak{P}$ is equal to the localisation of M over the order $\mathcal{O}$ at the maximal ideal*

$\mathfrak{P} \cap \mathcal{O} \lhd \mathcal{O}$:

$$M_{\mathfrak{P}} = M_{\mathfrak{P} \cap \mathcal{O}}.$$

LEMMA 5.3. *Let $\mathcal{O} < R$ be an order and $M_1, \ldots, M_s \subseteq K^l$ be $\mathcal{O}$-modules, $l \in \mathbb{N}$. Moreover, let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$. Then*

$$(M_1)_{\mathfrak{p}} \cap \cdots \cap (M_s)_{\mathfrak{p}} = (M_1 \cap \cdots \cap M_s)_{\mathfrak{p}}.$$

Proof. The inclusion $\supseteq$ is obvious.

"$\subseteq$" Let $x \in (M_1)_{\mathfrak{p}} \cap \cdots \cap (M_s)_{\mathfrak{p}}$. Then

$$x = \frac{m_1}{y_1} = \cdots = \frac{m_s}{y_s}$$

for some $m_1 \in M_1, \ldots, m_s \in M_s$ and $y_1, \ldots, y_s \in \mathcal{O} \setminus \mathfrak{p}$. Multiplying the above equalities of vectors by $y_1 \cdots y_s$ we get the existence of elements $z_1, \ldots, z_s \in \mathcal{O} \setminus \mathfrak{p}$ such that

$$z_1 m_1 = \cdots = z_s m_s \in M_1 \cap \cdots \cap M_s.$$

Hence

$$x = \frac{m_1}{y_1} = \frac{z_1 m_1}{z_1 y_1} \in (M_1 \cap \cdots \cap M_s)_{\mathfrak{p}}. \blacksquare$$

Let $\alpha\colon K^l \times K^l \to K$ be a bilinear form. Assume that α has a nonsingular diagonal matrix

$$A = \begin{bmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_l \end{bmatrix}$$

in the canonical basis of K^l, i.e. $\langle a_1, \ldots, a_l \rangle \in WK$. Moreover, assume that $\langle a_1, \ldots, a_l \rangle \in \phi(WR)$, $a_i \in \mathcal{O}$ and $a_i R + \mathfrak{f} = R$ for every $i \in \{1, \ldots, l\}$. We will generalize Theorem 2.4 to the form $\langle a_1, \ldots, a_l \rangle$.

Observe that

$$\operatorname{ord}_{\mathfrak{P}} a_i = 0 \quad \text{for every } i \in \{1, \ldots, l\}$$

for all but a finite number of maximal ideals $\mathfrak{P} \lhd R$.

(I) Fix such an $\mathfrak{P} \lhd R$. Consider the free module $\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \subseteq K^l$ over the ring $R_{\mathfrak{P}}$, where

$$w_1^{\mathfrak{P}} = (1, 0, \ldots, 0), \quad \ldots, \quad w_l^{\mathfrak{P}} = (0, \ldots, 0, 1).$$

Consider the restriction of α to $\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \times \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}$. Then the form $\alpha\colon \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \times \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \to R_{\mathfrak{P}}$ has matrix A in the basis $(w_1^{\mathfrak{P}}, \ldots, w_l^{\mathfrak{P}})$. Since $\operatorname{ord}_{\mathfrak{P}} a_i = 0$ for every $i \in \{1, \ldots, l\}$,

$$\det A = a_1 \cdots a_l \in U(R_{\mathfrak{P}}).$$

Thus α is nonsingular over the ring $R_{\mathfrak{P}}$.

(II) Let $\mathfrak{P} \lhd R$ be a maximal ideal R such that

$$\operatorname{ord}_{\mathfrak{P}} a_i > 0 \quad \text{for some } i \in \{1, \dots, l\}.$$

The localisation $R_{\mathfrak{P}}$ is a $\mathfrak{P}$-adic valuation ring. If $\overline{K}_{\mathfrak{P}}$ denotes the residue class field, then from [MH, (3.3) Corollary] it follows that $\langle a_1, \dots, a_l \rangle$ belongs to the kernel of the second residue homomorphism of Witt groups $\partial_{\mathfrak{P}}\colon WK \to W\overline{K}_{\mathfrak{P}}$. By [MH, proof of (3.1) Theorem] there exists a free module ($R_{\mathfrak{P}}$-lattice) $\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \subseteq K^l$ over $R_{\mathfrak{P}}$ such that the form $\alpha\colon \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \times \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \to R_{\mathfrak{P}}$ is nonsingular.

Denote by $\mathcal{P}_{\mathfrak{f}}$ the set of all maximal ideals $\mathfrak{P}$ of R such that $\mathfrak{P} + \mathfrak{f} = R$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be all the pairwise distinct maximal ideals of $\mathcal{O}$ such that

$$\mathfrak{p}_j + \mathfrak{f} \neq \mathcal{O} \quad \text{for every } j \in \{1, \dots, m\}.$$

Let

$$M := \bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \Big) \cap \bigcap_{j=1}^{m} \mathcal{O}_{\mathfrak{p}_j}^{l},$$

where for every $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$ the vectors $w_1^{\mathfrak{P}}, \dots, w_l^{\mathfrak{P}}$ are as in (I) and (II). It is easy to observe that M is an $\mathcal{O}$-module.

Proposition 5.4. *Let $a_1, \dots, a_l \in \mathcal{O}$ and suppose $a_i R + \mathfrak{f} = R$ for every $i \in \{1, \dots, l\}$. Under the assumptions and notation of pages* 368 *and* 369*,*

(i) $M_{\mathfrak{P} \cap \mathcal{O}} = \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}$ *for every* $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$*,*
(ii) $M_{\mathfrak{p}_j} = \mathcal{O}_{\mathfrak{p}_j}^{l}$ *for every* $j \in \{1, \dots, m\}$*.*

Proof. (i) Fix $\mathfrak{P}_0 \in \mathcal{P}_{\mathfrak{f}}$. It is easy to observe that

$$M \subseteq \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0}.$$

From Lemma 5.1 it follows that $R_{\mathfrak{P}_0} = \mathcal{O}_{\mathfrak{P}_0 \cap \mathcal{O}}$. Therefore

$$M_{\mathfrak{P}_0 \cap \mathcal{O}} \subseteq \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0}. \tag{5.1}$$

To show the opposite inclusion, let $\mathfrak{Q}_1, \dots, \mathfrak{Q}_n$ be all the pairwise distinct maximal ideals of R such that

$$\mathfrak{Q}_i + \mathfrak{f} \neq R \quad \text{for every } i \in \{1, \dots, n\}$$

(these are all the maximal ideals in the decomposition of $\mathfrak{f}$). Consider the module

$$N := \bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \Big) \cap \bigcap_{i=1}^{n} R_{\mathfrak{Q}_i}^{l}$$

over the ring R. Since

$$w_1^{\mathfrak{P}} = (1,0,\dots,0),\ \dots,\ w_l^{\mathfrak{P}} = (0,\dots,0,1)$$

for all but a finite number of $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$, from [O, 81:14], [MH, (3.2) Lemma] it follows that

$$N_{\mathfrak{P}_0} = \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0}.$$

Hence in particular

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq \Big[\bigcap_{\mathfrak{P}\in\mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}\Big)\Big]_{\mathfrak{P}_0}.$$

Because by assumption $\mathfrak{P}_0 + \mathfrak{f} = R$, Corollary 5.2 yields

$$\Big[\bigcap_{\mathfrak{P}\in\mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}\Big)\Big]_{\mathfrak{P}_0} = \Big[\bigcap_{\mathfrak{P}\in\mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}\Big)\Big]_{\mathfrak{P}_0\cap\mathcal{O}},$$

i.e.

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq \Big[\bigcap_{\mathfrak{P}\in\mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}\Big)\Big]_{\mathfrak{P}_0\cap\mathcal{O}}. \tag{5.2}$$

We will show that also

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq \bigcap_{j=1}^{m} (\mathcal{O}_{\mathfrak{p}_j}^l)_{\mathfrak{P}_0\cap\mathcal{O}}.$$

Fix an ideal $\mathfrak{p}_j$.

(I) Assume that $\mathfrak{P}_0$ is an ideal such that

$$\operatorname{ord}_{\mathfrak{P}_0} a_i = 0 \quad \text{for every } i \in \{1,\dots,l\}.$$

Then

$$w_1^{\mathfrak{P}_0} = (1,0,\dots,0),\ \dots,\ w_l^{\mathfrak{P}_0} = (0,\dots,0,1),$$

so $w_1^{\mathfrak{P}_0},\dots,w_l^{\mathfrak{P}_0} \in \mathcal{O}_{\mathfrak{p}_j}^l$. Hence

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} = \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} \mathcal{O}_{\mathfrak{P}_0\cap\mathcal{O}} \subseteq (\mathcal{O}_{\mathfrak{p}_j}^l)_{\mathfrak{P}_0\cap\mathcal{O}},$$

and finally

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq \bigcap_{j=1}^{m} (\mathcal{O}_{\mathfrak{p}_j}^l)_{\mathfrak{P}_0\cap\mathcal{O}}.$$

(II) Assume that

$$\operatorname{ord}_{\mathfrak{P}_0} a_i > 0 \quad \text{for some } i \in \{1,\dots,l\}.$$

Fix such an element a_{i_0}, $i_0 \in \{1,\dots,l\}$.

Since by assumption $a_{i_0}R + \mathfrak{f} = R$, observe that $a_{i_0} \in U(\mathcal{O}_{\mathfrak{p}_j})$. Indeed, it is enough to prove that $a_{i_0} \notin \mathfrak{p}_j$. From Corollary 2.7 it follows that $a_{i_0}\mathcal{O} + \mathfrak{f} = \mathcal{O}$. Therefore if $a_{i_0} \in \mathfrak{p}_j$, then

$$\mathcal{O} = a_{i_0}\mathcal{O} + \mathfrak{f} \subseteq \mathfrak{p}_j + \mathfrak{f} \neq \mathcal{O},$$

which is impossible.

Let $\pi \in R_{\mathfrak{P}_0}$ with $\operatorname{ord}_{\mathfrak{P}_0} \pi = 1$. Then $a_{i_0} = \pi^k \cdot u$ for some $k \in \mathbb{N}$ and $u \in U(R_{\mathfrak{P}_0})$.

Observe that

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} K = K^l = (1,0,\dots,0)K \oplus \cdots \oplus (0,\dots,0,1)K. \tag{5.3}$$

For every vector $w_i^{\mathfrak{P}_0}$ there exist $x_1,\dots,x_l \in K$ such that

$$w_i^{\mathfrak{P}_0} = (1,0,\dots,0)x_1 + \cdots + (0,\dots,0,1)x_l.$$

Fix x_s, $s \in \{1,\dots,l\}$. Assume $x_s \neq 0$. Then $x_s = \pi^r \cdot v$ for some $r \in \mathbb{Z}$ and $v \in U(R_{\mathfrak{P}_0})$.

If $r \geq 0$, then $x_s \in R_{\mathfrak{P}_0} = \mathcal{O}_{\mathfrak{P}_0 \cap \mathcal{O}}$, so

$$(0,\dots,\underset{s}{1},\dots,0)x_s \in (\mathcal{O}^l_{\mathfrak{p}_j})_{\mathfrak{P}_0 \cap \mathcal{O}}.$$

If $r < 0$, then choose $c \in \mathbb{N}$ such that $r \geq -ck$. Then

$$x_s = \pi^r \cdot v = a_{i_0}^{-c} \cdot \pi^{r+ck} \cdot u^c \cdot v,$$

where $a_{i_0}^{-c} \in \mathcal{O}_{\mathfrak{p}_j}$, $\pi^{r+ck} \cdot u^c \cdot v \in R_{\mathfrak{P}_0} = \mathcal{O}_{\mathfrak{P}_0 \cap \mathcal{O}}$, so again

$$(0,\dots,\underset{s}{1},\dots,0)x_s \in (\mathcal{O}^l_{\mathfrak{p}_j})_{\mathfrak{P}_0 \cap \mathcal{O}}.$$

We get

$$w_i^{\mathfrak{P}_0} \in (\mathcal{O}^l_{\mathfrak{p}_j})_{\mathfrak{P}_0 \cap \mathcal{O}}. \tag{5.4}$$

Hence

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq (\mathcal{O}^l_{\mathfrak{p}_j})_{\mathfrak{P}_0 \cap \mathcal{O}},$$

and finally

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq \bigcap_{j=1}^{m} (\mathcal{O}^l_{\mathfrak{p}_j})_{\mathfrak{P}_0 \cap \mathcal{O}}.$$

From (I), (II) and (5.2) it follows that

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq \Big[\bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}\Big)\Big]_{\mathfrak{P}_0 \cap \mathcal{O}} \cap \bigcap_{j=1}^{m} (\mathcal{O}^l_{\mathfrak{p}_j})_{\mathfrak{P}_0 \cap \mathcal{O}}.$$

By Lemma 5.3,

$$\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}_0} R_{\mathfrak{P}_0} \subseteq M_{\mathfrak{P}_0 \cap \mathcal{O}}.$$

(ii) Fix $j_0 \in \{1, \ldots, m\}$. The inclusion $M_{\mathfrak{p}_{j_0}} \subseteq \mathcal{O}^l_{\mathfrak{p}_{j_0}}$ is obvious. Observe that

$$(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1) \in \bigcap_{j=1}^{m} \mathcal{O}^l_{\mathfrak{p}_j}.$$

Hence

$$\mathcal{O}^l_{\mathfrak{p}_{j_0}} \subseteq \Big(\bigcap_{j=1}^{m} \mathcal{O}^l_{\mathfrak{p}_j} \Big)_{\mathfrak{p}_{j_0}}. \tag{5.5}$$

Denote by $\mathcal{P}_{\mathfrak{f}_1}$ and $\mathcal{P}_{\mathfrak{f}_2}$ the sets of maximal ideals $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$ such that

$$\operatorname{ord}_{\mathfrak{P}} a_i = 0 \quad \text{for every } i \in \{1, \ldots, l\}$$

and of maximal ideals $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$ such that

$$\operatorname{ord}_{\mathfrak{P}} a_i > 0 \quad \text{for some } i \in \{1, \ldots, l\},$$

respectively. Obviously $\mathcal{P}_{\mathfrak{f}_2}$ is a finite set.

Because for every $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}_1}$ we have

$$w_1^{\mathfrak{P}} = (1, 0, \ldots, 0), \ \ldots, \ w_l^{\mathfrak{P}} = (0, \ldots, 0, 1),$$

as in (5.5) we obtain

$$\mathcal{O}^l_{\mathfrak{p}_{j_0}} \subseteq \Big(\bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}_1}} \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \Big)_{\mathfrak{p}_{j_0}}. \tag{5.6}$$

However, using (5.3) for $\mathfrak{P}_0 = \mathfrak{P}$ and applying similar arguments to those for (5.4) we prove that

$$(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1) \in \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \Big)_{\mathfrak{p}_{j_0}}$$

for every $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}_2}$, i.e.

$$\mathcal{O}^l_{\mathfrak{p}_{j_0}} \subseteq \bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}_2}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \Big)_{\mathfrak{p}_{j_0}}. \tag{5.7}$$

From (5.5)–(5.7) and Lemma 5.3 it follows that $\mathcal{O}^l_{\mathfrak{p}_{j_0}} \subseteq M_{\mathfrak{p}_{j_0}}$. ∎

PROPOSITION 5.5. *Let $a_1, \ldots, a_l \in \mathcal{O}$ and suppose that $a_i R + \mathfrak{f} = R$ for every $i \in \{1, \ldots, l\}$. Moreover, let*

$$M = \bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}} \Big) \cap \bigcap_{j=1}^{m} \mathcal{O}_{\mathfrak{p}_j}^{l}$$

under the assumptions and notation of pages 368 *and* 369. *Then the $\mathcal{O}$-module M is finitely generated and projective of rank l.*

Proof. Fix a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$. Assume $\mathfrak{p} + \mathfrak{f} = \mathcal{O}$. There exists a unique maximal ideal $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$ such that $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$. Therefore from Proposition 5.4 it follows that

$$M_{\mathfrak{p}} = M_{\mathfrak{P} \cap \mathcal{O}} = \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}.$$

Hence $M_{\mathfrak{p}}$ is a free $\mathcal{O}_{\mathfrak{p}}$ $(= R_{\mathfrak{P}})$-module of rank l.

Let $\mathfrak{p} + \mathfrak{f} \neq \mathcal{O}$ (i.e. $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$). Again Proposition 5.4 yields $M_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^{l}$, so $M_{\mathfrak{p}}$ is a free $\mathcal{O}_{\mathfrak{p}}$-module of rank l.

To sum up, the localisation of the module M at every maximal ideal of the order $\mathcal{O}$ is a free module of rank l. Therefore it suffices to prove that M is finitely generated over $\mathcal{O}$.

Observe that we have at most finitely many vectors $w_i^{\mathfrak{P}}$ such that $w_i^{\mathfrak{P}} \notin \mathcal{O}^l$. Every coordinate of a vector $w_i^{\mathfrak{P}}$ has the form

$$x_i^{\mathfrak{P}} / y_i^{\mathfrak{P}} \quad \text{for some } x_i^{\mathfrak{P}} \in \mathcal{O},\ y_i^{\mathfrak{P}} \in \mathcal{O} \setminus \{0\}.$$

Consider the following element z of the order $\mathcal{O}$. If there does not exist a vector $w_i^{\mathfrak{P}}$ such that $w_i^{\mathfrak{P}} \notin \mathcal{O}^l$, then we take $z = 1$. Otherwise, let z be the product of the denominators $y_i^{\mathfrak{P}}$ of all vectors $w_i^{\mathfrak{P}}$ such that $w_i^{\mathfrak{P}} \notin \mathcal{O}^l$. Then $z w_i^{\mathfrak{P}} \in \mathcal{O}^l$ for every $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$. Moreover,

$$zM = \bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} \Big(\bigoplus_{i=1}^{l} z w_i^{\mathfrak{P}} R_{\mathfrak{P}} \Big) \cap \bigcap_{j=1}^{m} z\mathcal{O}_{\mathfrak{p}_j}^{l} \subseteq \bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} R_{\mathfrak{P}}^{l} \cap \bigcap_{j=1}^{m} \mathcal{O}_{\mathfrak{p}_j}^{l}.$$

But $R_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P} \cap \mathcal{O}}$ for every $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$, so

$$zM \subseteq \bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} \mathcal{O}_{\mathfrak{P} \cap \mathcal{O}}^{l} \cap \bigcap_{j=1}^{m} \mathcal{O}_{\mathfrak{p}_j}^{l}.$$

Since $\{\mathfrak{P} \cap \mathcal{O} : \mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}\}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are all the pairwise distinct maximal ideals of $\mathcal{O}$ (cf. [GHK, proof of Proposition 4(ii)]), it is easy to observe that

$$\bigcap_{\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}} \mathcal{O}_{\mathfrak{P} \cap \mathcal{O}}^{l} \cap \bigcap_{j=1}^{m} \mathcal{O}_{\mathfrak{p}_j}^{l} = \mathcal{O}^l.$$

Hence $zM \subseteq \mathcal{O}^l$ is a submodule of the finitely generated $\mathcal{O}$-module $\mathcal{O}^l$. But $\mathcal{O}$ is a noetherian domain, so zM is a finitely generated $\mathcal{O}$-module. It suffices to notice that $M \cong zM$, i.e. M is finitely generated over $\mathcal{O}$. ∎

THEOREM 5.6. *Let K be a global field and $R < K$ be a Dedekind domain. Moreover, let $\mathcal{O} < R$ be an order, $\mathfrak{f}$ be the conductor of $\mathcal{O}$ and suppose that $\langle a_1, \dots, a_l\rangle \in \phi(WR)$ with $a_1, \dots, a_l \in \mathcal{O}$. If*

$$a_i R + \mathfrak{f} = R \quad \textit{for every } i \in \{1, \dots, l\},$$

then $\langle a_1, \dots, a_l\rangle \in \operatorname{im}(\phi \circ \varphi)$.

Proof. Let $\alpha\colon K^l \times K^l \to K$ be a nonsingular bilinear form with matrix

$$A = \begin{bmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_l \end{bmatrix}$$

in the basis

$$\mathcal{B} = ((1, 0, \dots, 0), \dots, (0, \dots, 0, 1))$$

of K^l. Consider the finitely generated projective $\mathcal{O}$-module M from Proposition 5.5 and the restriction of α to $M \times M$, and fix a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$.

Assume $\mathfrak{p} + \mathfrak{f} = \mathcal{O}$. Then there exists a unique maximal ideal $\mathfrak{P} \in \mathcal{P}_{\mathfrak{f}}$ of R such that $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$. We have

$$M_{\mathfrak{p}} = M_{\mathfrak{P}\cap\mathcal{O}} = \bigoplus_{i=1}^{l} w_i^{\mathfrak{P}} R_{\mathfrak{P}}.$$

Moreover, $R_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{p}}$. From (I) and (II) on pages 368 and 369 it follows that the localisation $\alpha_{\mathfrak{p}}\colon M_{\mathfrak{p}} \times M_{\mathfrak{p}} \to \mathcal{O}_{\mathfrak{p}}$ is nonsingular over $\mathcal{O}_{\mathfrak{p}}$.

Let $\mathfrak{p} + \mathfrak{f} \neq \mathcal{O}$. Then $M_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^l$. Since $a_i R + \mathfrak{f} = R$, we have $a_i \in U(\mathcal{O}_{\mathfrak{p}})$ for every $i \in \{1, \dots, l\}$ (see proof of Proposition 5.4(i)). The localisation $\alpha_{\mathfrak{p}}\colon M_{\mathfrak{p}} \times M_{\mathfrak{p}} \to \mathcal{O}_{\mathfrak{p}}$ has matrix A in the basis $\mathcal{B}$ of the free module $M_{\mathfrak{p}}$. Hence $\alpha_{\mathfrak{p}}$ is nonsingular over $\mathcal{O}_{\mathfrak{p}}$.

To sum up, the localisation of the form α at every maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ is nonsingular. Hence by [B, (1.4) Proposition] the form $\alpha\colon M \times M \to \mathcal{O}$ is nonsingular over $\mathcal{O}$, so in particular $\langle (M, \alpha)\rangle \in W\mathcal{O}$.

It is easy to observe that

$$\phi \circ \varphi\langle (M, \alpha)\rangle = \langle a_1, \dots, a_l\rangle,$$

i.e. $\langle a_1, \dots, a_l\rangle \in \operatorname{im}(\phi \circ \varphi)$. ∎

6. Forms $\langle\langle f, d\rangle\rangle$, $\langle z, -ez\rangle$. Now we formulate some facts for integral semilocal domains.

PROPOSITION 6.1. *If P is an integral semilocal domain, then every element of the Witt ring WP can be written in the form $\langle a_1, \dots, a_l \rangle$ for some $a_1, \dots, a_l \in U(P)$.*

Proof. Since P is an integral domain, every finitely generated projective P-module is free (cf. [M, p. 26]). It suffices to use [M, 2.7 Corollary, p. 32]. ■

Let P be an integral semilocal domain and K be its field of fractions. Denote by $I(K)$ the fundamental ideal of WK consisting of the Witt classes of even dimensional forms over K. Denote by $I^2(P)$ the subgroup of the second power $I^2(K)$ of the ideal $I(K)$ additively generated by the set

$$\{\langle\langle a, b\rangle\rangle \in WK : a, b \in U(P)\}.$$

We will write

$$\langle a_1, \dots, a_l \rangle \equiv \langle b_1, \dots, b_k \rangle \bmod I^2(P)$$

if $\langle a_1, \dots, a_l \rangle - \langle b_1, \dots, b_k \rangle \in I^2(P)$.

PROPOSITION 6.2. *Let $\langle a_1, \dots, a_l \rangle \in WP$ with $a_1, \dots, a_l \in U(P)$ and l odd. Moreover, let*

$$a_1 \cdots a_l \dot{K}^2 = \begin{cases} \dot{K}^2 & \text{when } l \equiv 3 \pmod 4, \\ -\dot{K}^2 & \text{when } l \equiv 1 \pmod 4. \end{cases}$$

Then $\langle 1, a_1, \dots, a_l \rangle \in I^2(P)$.

Proof. We use induction on l. If $l = 1$, then $a_1 \dot{K}^2 = -\dot{K}^2$, so $\langle a_1 \rangle = \langle -1 \rangle$ in WK. Therefore

$$\langle 1, a_1 \rangle = \langle 1, -1 \rangle = \langle 1, -1, 1, -1 \rangle \in I^2(P).$$

Assume $l = 3$. Then $a_1 a_2 a_3 \dot{K}^2 = \dot{K}^2$, i.e. $a_3 \dot{K}^2 = a_1 a_2 \dot{K}^2$. Hence

$$\langle 1, a_1, a_2, a_3 \rangle = \langle 1, a_1, a_2, a_1 a_2 \rangle \in I^2(P). \tag{6.1}$$

Let $l = 5$. Observe that

$$\begin{aligned} \langle a_1, a_2, a_3, a_4 \rangle = \langle 1, a_1, a_2, a_1 a_2 \rangle + \langle 1, a_3, a_4, a_3 a_4 \rangle \\ - \langle 1, 1, a_1 a_2, a_1 a_2 \rangle + \langle a_1 a_2, -a_3 a_4 \rangle \end{aligned} \tag{6.2}$$

in WK, so

$$\langle 1, a_1, a_2, a_3, a_4, a_5 \rangle \equiv \langle 1, a_1 a_2, -a_3 a_4, a_5 \rangle \bmod I^2(P).$$

Since $\langle a_1 a_2, -a_3 a_4, a_5 \rangle \in WP$ and $-a_1 a_2 a_3 a_4 a_5 \dot{K}^2 = \dot{K}^2$, analogously to (6.1) we get

$$\langle 1, a_1 a_2, -a_3 a_4, a_5 \rangle \in I^2(P).$$

Hence $\langle 1, a_1, a_2, a_3, a_4, a_5 \rangle \in I^2(P)$.

Assume $l = 4k + 3$ for some $k \in \mathbb{N}$. Using (6.2) we obtain

$$\langle a_1, \dots, a_{4k} \rangle \equiv \langle b_1, \dots, b_{2k} \rangle \bmod I^2(P)$$

for some $b_1, \dots, b_{2k} \in U(P)$. Therefore

$$\begin{aligned}\langle 1, a_1, \dots, a_l\rangle &= \langle 1, a_1, \dots, a_{4k}, a_{4k+1}, a_{4k+2}, a_{4k+3}\rangle \\ &\equiv \langle 1, b_1, \dots, b_{2k}, a_{4k+1}, a_{4k+2}, a_{4k+3}\rangle \bmod I^2(P).\end{aligned}$$

Observe that

$$b_1 \cdots b_{2k}\dot{K}^2 = \begin{cases} a_1 \cdots a_{4k}\dot{K}^2 & \text{when } k \equiv 0 \pmod 2, \\ -a_1 \cdots a_{4k}\dot{K}^2 & \text{when } k \equiv 1 \pmod 2). \end{cases}$$

Assume $k = 2s$ for some $s \in \mathbb{N}$. The form

$$\langle b_1, \dots, b_{2k}, a_{4k+1}, a_{4k+2}, a_{4k+3}\rangle \in WP$$

has rank $4s + 3 < l$. Its determinant over K is equal to $a_1 \cdots a_l\dot{K}^2 = \dot{K}^2$. By the induction assumption,

$$\langle 1, b_1, \dots, b_{2k}, a_{4k+1}, a_{4k+2}, a_{4k+3}\rangle \in I^2(P),$$

i.e. $\langle 1, a_1, \dots, a_l\rangle \in I^2(P)$.

Assume $k = 2s + 1$ for some $s \in \mathbb{N} \cup \{0\}$. The form

$$\langle b_1, \dots, b_{2k}, a_{4k+1}, a_{4k+2}, a_{4k+3}\rangle \in WP$$

has rank $4(s + 1) + 1 < l$. Its determinant over K is $-a_1 \cdots a_l\dot{K}^2 = -\dot{K}^2$. By the induction assumption,

$$\langle 1, b_1, \dots, b_{2k}, a_{4k+1}, a_{4k+2}, a_{4k+3}\rangle \in I^2(P),$$

i.e. $\langle 1, a_1, \dots, a_l\rangle \in I^2(P)$.

Analogously to the case $l = 4k + 3$ we prove that $\langle 1, a_1, \dots, a_l\rangle \in I^2(P)$ for $l = 4k + 1$, $k \in \mathbb{N}$. ∎

Let K be a global field and $R < K$ be a Dedekind domain. Moreover, let $\mathcal{O} < R$ be an order and $\mathfrak{f}$ be its conductor. Let $\mathcal{P} = \bigcup_{i=1}^{m} \mathfrak{p}_i$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ are all the pairwise distinct maximal ideals of $\mathcal{O}$ such that

$$\mathfrak{p}_i + \mathfrak{f} \neq \mathcal{O} \quad \text{for every } i \in \{1, \dots, m\}.$$

Denote by $\mathcal{O}_{\mathcal{P}}$ the localisation of the order $\mathcal{O}$ at the set $\mathcal{O} \setminus \mathcal{P}$. The ring $\mathcal{O}_{\mathcal{P}}$ is an integral semilocal domain.

LEMMA 6.3. *If $a \in \mathcal{O}$ is nonzero, then*

$$a \in U(\mathcal{O}_{\mathcal{P}}) \iff aR + \mathfrak{f} = R.$$

Proof. ($\Leftarrow$) It suffices to observe that $a \notin \mathfrak{p}_i$ for every $i \in \{1, \dots, m\}$ (see proof of Proposition 5.4(i)).

($\Rightarrow$) Suppose $aR + \mathfrak{f} \neq R$. Then there exists a maximal ideal $\mathfrak{Q}$ in the decomposition of $\mathfrak{f}$ such that $aR \subseteq \mathfrak{Q}$ (cf. [GHK, p. 93]). Hence

$$a \in \mathfrak{Q} \cap \mathcal{O} = \mathfrak{p}_i \quad \text{for some } i \in \{1, \dots, m\}$$

(cf. [GHK, proof of Proposition 4(ii)]). This is impossible. ∎

COROLLARY 6.4. *The group $I^2(\mathcal{O}_\mathcal{P})$ is additively generated by the Pfister forms $\langle\langle a,b\rangle\rangle \in WK$ such that $a,b \in \mathcal{O}$ and $aR+\mathfrak{f}=R$, $bR+\mathfrak{f}=R$.*

Proof. Let $\langle\langle c,d\rangle\rangle \in WK$ and $c,d \in U(\mathcal{O}_\mathcal{P})$. Then $c=x_1/y_1$, $d=x_2/y_2$ for some $x_1,x_2,y_1,y_2 \in \mathcal{O}\setminus\mathcal{P}$. Moreover, we have $a:=x_1y_1 \in \mathcal{O}\cap U(\mathcal{O}_\mathcal{P})$, $b:=x_2y_2 \in \mathcal{O}\cap U(\mathcal{O}_\mathcal{P})$ and $\langle\langle c,d\rangle\rangle = \langle\langle a,b\rangle\rangle$ in WK. ∎

THEOREM 6.5. *Let K be a global field, $R<K$ be a Dedekind domain and $\mathcal{O}<R$ be an order. Moreover, let $\langle a_1,\dots,a_l\rangle \in \phi(WR)$ with l odd and*

$$a_1\cdots a_l\dot{K}^2 = \begin{cases} \dot{K}^2 & \text{when } l\equiv 3 \pmod 4,\\ -\dot{K}^2 & \text{when } l\equiv 1 \pmod 4.\end{cases}$$

Then

$$\langle a_1,\dots,a_l\rangle \in \operatorname{im}(\phi\circ\varphi) \;\Leftrightarrow\; \langle 1,a_1,\dots,a_l\rangle \in I^2(\mathcal{O}_\mathcal{P}).$$

Proof. ($\Leftarrow$) From Corollary 6.4 it follows that

$$\langle 1,a_1,\dots,a_l\rangle = \langle 1,b_1,c_1,b_1c_1\rangle + \dots + \langle 1,b_k,c_k,b_kc_k\rangle \in \phi(WR)$$

for some $b_1,c_1,\dots,b_k,c_k \in \mathcal{O}$ such that

$$b_iR+\mathfrak{f}=R,\qquad c_iR+\mathfrak{f}=R\qquad \text{for every } i\in\{1,\dots,k\}.$$

Since none of the maximal ideals in the decomposition of $\mathfrak{f}$ belongs to the decompositions of the ideals b_iR, c_iR, none of them belongs to the decomposition of b_ic_iR. Therefore

$$b_ic_iR+\mathfrak{f}=R\quad \text{for every } i\in\{1,\dots,k\}.$$

By Theorem 5.6,

$$\langle 1,a_1,\dots,a_l\rangle = \langle 1,b_1,c_1,b_1c_1\rangle + \dots + \langle 1,b_k,c_k,b_kc_k\rangle \in \operatorname{im}(\phi\circ\varphi),\ \text{i.e.}$$
$$\langle a_1,\dots,a_l\rangle = -\langle 1\rangle + \langle 1,a_1,\dots,a_l\rangle \in \operatorname{im}(\phi\circ\varphi).$$

($\Rightarrow$) Let $\varphi_1\colon W\mathcal{O}_\mathcal{P}\to WK$ be the natural homomorphism. Because $\langle a_1,\dots,a_l\rangle \in \operatorname{im}(\phi\circ\varphi)$, also $\langle a_1,\dots,a_l\rangle \in \operatorname{im}\varphi_1$. By Proposition 6.1 there exist $b_1,\dots,b_k \in U(\mathcal{O}_\mathcal{P})$ such that

$$\varphi_1(\langle b_1,\dots,b_k\rangle) = \langle a_1,\dots,a_l\rangle.$$

Then $\langle b_1,\dots,b_k\rangle = \langle a_1,\dots,a_l\rangle$ in WK. Moreover, $k\equiv l \pmod 2$, i.e. k is odd. Comparing the discriminants of these forms we get

$$(-1)^{\frac12 k(k-1)}b_1\cdots b_k\dot{K}^2 = (-1)^{\frac12 l(l-1)}a_1\cdots a_l\dot{K}^2.$$

Therefore

$$b_1\cdots b_k\dot{K}^2 = \begin{cases} \dot{K}^2 & \text{when } k\equiv 3 \pmod 4,\\ -\dot{K}^2 & \text{when } k\equiv 1 \pmod 4.\end{cases}$$

By Proposition 6.2,

$$\langle 1,a_1,\dots,a_l\rangle = \langle 1,b_1,\dots,b_k\rangle \in I^2(\mathcal{O}_\mathcal{P}).\ ∎$$

Corollary 6.6. *Let* $\langle\langle f,d\rangle\rangle \in \phi(WR)$. *Then*

$$\langle\langle f,d\rangle\rangle \in \operatorname{im}(\phi\circ\varphi) \ \Leftrightarrow\ \langle\langle f,d\rangle\rangle \in I^2(\mathcal{O}_{\mathcal{P}}).$$

Proof. Notice that $\langle\langle f,d\rangle\rangle \in \operatorname{im}(\phi\circ\varphi) \Leftrightarrow \langle f,d,fd\rangle \in \operatorname{im}(\phi\circ\varphi)$. ∎

Let $\mathcal{P}_2$ denote the set of all dyadic primes of the field K.

Corollary 6.7. *Let* K *be a global field with* $\operatorname{char} K \neq 2$, $\mathcal{S}$ *be a Hasse set on* K *and* $\mathcal{O} < R_K(\mathcal{S})$ *be an order. Moreover, let* $\mathfrak{f}$ *be the conductor of* $\mathcal{O}$ *and* $\langle\langle f,d\rangle\rangle \in \phi(WR_K(\mathcal{S}))$. *If there exist* $f',d' \in \mathcal{O}$ *with the properties that* $f'R_K(\mathcal{S}) + \mathfrak{f} = R_K(\mathcal{S})$, $d'R_K(\mathcal{S}) + \mathfrak{f} = R_K(\mathcal{S})$ *and*

(i) $(-f',-d')_{\mathfrak{P}} = (-f,-d)_{\mathfrak{P}}$ *for every* $\mathfrak{P} \in \mathcal{P}_2 \cup \mathcal{S}$,
(ii) $(-f',-d')_{\mathfrak{P}} = 1$ *for every* $\mathfrak{P} \notin \mathcal{P}_2 \cup \mathcal{S}$,

then $\langle\langle f,d\rangle\rangle \in \operatorname{im}(\phi\circ\varphi)$.

Proof. Let $\mathfrak{P} \in \mathcal{S}$ be a real prime of K. Denote by $\operatorname{sign}_{\mathfrak{P}}$ the signature determined by $\mathfrak{P}$. From (i) it follows that

$$\operatorname{sign}_{\mathfrak{P}}\langle\langle f',d'\rangle\rangle = \operatorname{sign}_{\mathfrak{P}}\langle\langle f,d\rangle\rangle.$$

Assume $\mathfrak{P} \in \mathcal{P}_2 \cup \mathcal{S}$ is a finite prime. Denote by $h_{\mathfrak{P}}$ the $\mathfrak{P}$-adic Hasse–Witt invariant. Also from (i) it follows that

$$h_{\mathfrak{P}}\langle\langle f',d'\rangle\rangle = (-f',-d')_{\mathfrak{P}} = (-f,-d)_{\mathfrak{P}} = h_{\mathfrak{P}}\langle\langle f,d\rangle\rangle.$$

If $\mathfrak{P} \notin \mathcal{P}_2 \cup \mathcal{S}$, then $(-f,-d)_{\mathfrak{P}} = 1$ (cf. [Cz3, Lemma 3.4]), so by (ii),

$$h_{\mathfrak{P}}\langle\langle f',d'\rangle\rangle = h_{\mathfrak{P}}\langle\langle f,d\rangle\rangle.$$

Finally, $\langle\langle f',d'\rangle\rangle \cong \langle\langle f,d\rangle\rangle$ over the $\mathfrak{P}$-adic completion $K_{\mathfrak{P}}$ of the field K for every prime $\mathfrak{P}$ of K. By the local-global principle, $\langle\langle f',d'\rangle\rangle \cong \langle\langle f,d\rangle\rangle$ over K. Hence $\langle\langle f',d'\rangle\rangle = \langle\langle f,d\rangle\rangle$ in WK.

From Corollary 6.4 it follows that $\langle\langle f',d'\rangle\rangle \in I^2(\mathcal{O}_{\mathcal{P}})$. By Corollary 6.6,

$$\langle\langle f,d\rangle\rangle = \langle\langle f',d'\rangle\rangle \in \operatorname{im}(\phi\circ\varphi). \ ∎$$

Theorem 6.5 also has the following corollaries for the form $\langle z,-ez\rangle$, $e \in E(R) \cap \mathcal{O}$.

Corollary 6.8. *Let* K *be any global field,* $R < K$ *be a Dedekind domain and* $\mathcal{O} < R$ *be an order. Moreover, let* $\mathfrak{f}$ *be the conductor of* $\mathcal{O}$ *and* $\langle z,-ez\rangle \in \phi(WR)$ *with* $e \in E(R)\cap\mathcal{O}$. *Then* $\langle z,-ez\rangle \in \operatorname{im}(\phi\circ\varphi)$ *if and only if* $\langle\langle -e,z\rangle\rangle \in I^2(\mathcal{O}_{\mathcal{P}})$ *and there exists* $e' \in \mathcal{O}$ *such that*

$$e'\dot{K}^2 = e\dot{K}^2 \quad \textit{and} \quad e'R + \mathfrak{f} = R.$$

Proof. By assumption, $e \in E(R)$, so $\langle e\rangle \in \phi(WR)$. Hence

$$\langle -e,z,-ez\rangle = -\langle e\rangle + \langle z,-ez\rangle \in \phi(WR).$$

($\Leftarrow$) Since $\langle 1, -e, z, -ez\rangle \in I^2(\mathcal{O}_{\mathcal{P}})$, from Theorem 6.5 it follows that $\langle -e, z, -ez\rangle \in \operatorname{im}(\phi\circ\varphi)$. But $\langle e\rangle \in \operatorname{im}(\phi\circ\varphi)$ (see Theorem 2.9), so

$$\langle z, -ez\rangle = \langle e\rangle + \langle -e, z, -ez\rangle \in \operatorname{im}(\phi\circ\varphi).$$

($\Rightarrow$) Since $\langle z, -ez\rangle \in \operatorname{im}(\phi\circ\varphi)$, by Lemma 2.1 there exists an ideal J of $\mathcal{O}$ and an element $k \in \dot{K}$ such that

$$J^2 = ek^2\mathcal{O}.$$

For the fractional ideal $I = Jk^{-1}$ we have

$$I^2 = e\mathcal{O}.$$

By Proposition 2.2,

$$\langle e\rangle \in \operatorname{im}(\phi\circ\varphi). \tag{6.3}$$

Hence

$$\langle -e, z, -ez\rangle = -\langle e\rangle + \langle z, -ez\rangle \in \operatorname{im}(\phi\circ\varphi).$$

By Theorem 6.5,

$$\langle\langle -e, z\rangle\rangle \in I^2(\mathcal{O}_{\mathcal{P}}).$$

The second part of the conclusion follows from (6.3) and Theorem 2.9. ■

Corollary 6.9. *Let K be a global field with* $\operatorname{char} K \neq 2$, *$\mathcal{S}$ be a Hasse set on K and $\mathcal{O} < R_K(\mathcal{S})$ be an order. Moreover, let $\mathfrak{f}$ be the conductor of $\mathcal{O}$ and $\langle z, -ez\rangle \in \phi(WR_K(\mathcal{S}))$ with $e \in E(R_K(\mathcal{S}))\cap\mathcal{O}$. If there exist $e', z' \in \mathcal{O}$ such that $e'\dot{K}^2 = e\dot{K}^2$, $e'R_K(\mathcal{S}) + \mathfrak{f} = R_K(\mathcal{S})$, $z'R_K(\mathcal{S}) + \mathfrak{f} = R_K(\mathcal{S})$ and*

(i) *$(e, -z')_{\mathfrak{P}} = (e, -z)_{\mathfrak{P}}$ for every $\mathfrak{P} \in \mathcal{P}_2 \cup \mathcal{S}$,*
(ii) *$(e, -z')_{\mathfrak{P}} = 1$ for every $\mathfrak{P} \notin \mathcal{P}_2 \cup \mathcal{S}$,*

then $\langle z, -ez\rangle \in \operatorname{im}(\phi\circ\varphi)$.

Proof. Analogously to the proof of Corollary 6.7 we show that

$$\langle\langle -e, z\rangle\rangle = \langle\langle -e, z'\rangle\rangle$$

in WK. Because $e'\dot{K}^2 = e\dot{K}^2$,

$$\langle\langle -e, z\rangle\rangle = \langle\langle -e, z'\rangle\rangle = \langle\langle -e', z'\rangle\rangle.$$

From Corollary 6.4 it follows that

$$\langle\langle -e, z\rangle\rangle = \langle\langle -e', z'\rangle\rangle \in I^2(\mathcal{O}_{\mathcal{P}}).$$

By Corollary 6.8, $\langle z, -ez\rangle \in \operatorname{im}(\phi\circ\varphi)$. ■

Example 6.10. Let $K = \mathbb{Q}(\sqrt{3})$. There is one dyadic prime $\mathfrak{P}_0$ in K, so $\mathcal{P}_2 = \{\mathfrak{P}_0\}$. The ring R_K of algebraic integers of K is the ring $R_K(\mathcal{S})$ of $\mathcal{S}$-integers of K, where $\mathcal{S}$ consists of the two infinite primes ∞_1, ∞_2 of K. Assume $\sqrt{3}$ is positive at ∞_1 and negative at ∞_2. Since $-1 \notin N_{K/\mathbb{Q}}(\dot{K})$, from [Cz1, p. 114, 118] it follows that the set

$$\{\langle 1\rangle, \langle 2\rangle, \langle z, -ez\rangle\}$$

generates the group $\phi(WR_K)$, where $e=-1$ and $z\in K$ is such that
$$(-1,z)_{\mathfrak{P}_0}=-1,\quad (-1,z)_{\infty_1}=-1,\quad (-1,z)_{\infty_2}=1$$
(cf. [Cz1, p. 113]). Observe that
$$\begin{aligned}(-1,-z)_{\mathfrak{P}_0}&=(-1,-1)_{\mathfrak{P}_0}(-1,z)_{\mathfrak{P}_0}=-1,\\(-1,-z)_{\infty_1}&=(-1,-1)_{\infty_1}(-1,z)_{\infty_1}=1,\\(-1,-z)_{\infty_2}&=(-1,-1)_{\infty_2}(-1,z)_{\infty_2}=-1.\end{aligned}$$
Consider the element $a:=1-\sqrt{3}\in R_K=\mathbb{Z}[\sqrt{3}]$. For $n\in\mathbb{N}$ let
$$a^n=x_n+y_n\sqrt{3},\quad x_n,y_n\in\mathbb{Z}.$$
Analogously to [C2, Lemma 2] one can prove that there are infinitely many prime numbers dividing the sequence $(y_{2n+1})_{n=1}^{\infty}$. Hence there are infinitely many natural odd numbers m such that m divides (y_{2n+1}). Choose such an m and a number $2n+1$ such that $m\,|\,y_{2n+1}$.

Consider the order $\mathcal{O}=\mathbb{Z}[m\sqrt{3}]$. Obviously,
$$a^{2n+1}=x_{2n+1}+y_{2n+1}\sqrt{3}\in\mathcal{O}.$$
Because
$$N_{K/\mathbb{Q}}(a^{2n+1})=N_{K/\mathbb{Q}}(1-\sqrt{3})^{2n+1}=-2^{2n+1},$$
we have $\gcd(N_{K/\mathbb{Q}}(a^{2n+1}),m)=1$. Hence
$$a^{2n+1}R_K+\mathfrak{f}=a^{2n+1}R_K+mR_K=R_K.$$
Moreover,
$$\begin{aligned}(-1,-a^{2n+1})_{\mathfrak{P}_0}&=(-1,N_{K/\mathbb{Q}}(1-\sqrt{3}))_2=(-1,-2)_2=-1,\\(-1,-a^{2n+1})_{\infty_1}&=(-1,-1+\sqrt{3})_{\infty_1}=1,\\(-1,-a^{2n+1})_{\infty_2}&=(-1,-1+\sqrt{3})_{\infty_2}=-1.\end{aligned}$$
For every $\mathfrak{P}\notin\mathcal{P}_2\cup\mathcal{S}$ the elements -1, $-a^{2n+1}$ are $\mathfrak{P}$-adic units, so $(-1,-a^{2n+1})_{\mathfrak{P}}=1$. By Corollary 6.9, $\langle z,-ez\rangle\in\operatorname{im}(\phi\circ\varphi)$. Hence and from Proposition 3.1 it follows that $\varphi\colon W\mathcal{O}\to WR_K$ is surjective.

We have obtained the following observation.

There are infinitely many natural odd numbers m such that the natural homomorphism $\varphi\colon W\mathbb{Z}[m\sqrt{3}]\to WR_K$ is surjective.

7. Real quadratic global fields. Let $K=\mathbb{Q}(\sqrt{D})$ be a quadratic number field, where $D\equiv 1 \pmod 8$ is a square-free positive integer. There are two dyadic primes $\mathfrak{P}_1$, $\mathfrak{P}_2$ in K, so $\mathcal{P}_2=\{\mathfrak{P}_1,\mathfrak{P}_2\}$. Analogously to Example 6.10 the ring R_K of algebraic integers of K is the ring $R_K(\mathcal{S})$ of $\mathcal{S}$-integers of K, where $\mathcal{S}$ consists of the two infinite primes ∞_1, ∞_2 of K.

Assume $-1\in N_{K/\mathbb{Q}}(\dot{K})$ and choose $b\in E(R_K)$ positive at ∞_1 and negative at ∞_2. Let $p_1,\dots,p_s$ be all the pairwise distinct prime divisors of D. From [Cz1, pp. 114, 118] it follows that the set

$$\{\langle 1\rangle, \langle p_1\rangle, \ldots, \langle p_{s-1}\rangle, \langle b\rangle, \langle\langle f, d\rangle\rangle\}$$

generates the group $\phi(WR_K)$, where $f, d \in K$ are such that $-f$ is totally positive and

$$(-f, -d)_{\mathfrak{P}_1} = (-f, -d)_{\mathfrak{P}_2} = -1$$

(cf. [Cz1, p. 109]).

Proposition 7.1. *Let $\mathcal{O} = \mathbb{Z}[m(1+\sqrt{D})/2]$ be an order such that every odd prime divisor of $m \in \mathbb{N}$ is congruent to* 1 *modulo* 4. *Then*

$$\langle\langle f, d\rangle\rangle \in \operatorname{im}(\phi \circ \varphi).$$

Proof. For an odd prime number p denote by $\left(\frac{\cdot}{p}\right)$ the Legendre symbol.

By [O, 65:17] there are infinitely many prime numbers p such that

$$\left(\frac{D}{p}\right) = -1 \quad \text{and} \quad \left(\frac{-1}{p}\right) = -1.$$

Fix such a p. From $\left(\frac{D}{p}\right) = -1$ it follows that p does not split in K. From $\left(\frac{-1}{p}\right) = -1$ it follows that $p \equiv 3 \pmod 4$. Hence $p \nmid m$, so

$$pR_K + \mathfrak{f} = pR_K + mR_K = R_K.$$

Let $\mathfrak{P}$ be the prime of K which lies over p. Then $(-1, p)_{\mathfrak{P}} = 1$. Because $p \equiv 3 \pmod 4$, we have $(-1, p)_2 = -1$, i.e.

$$(-1, p)_{\mathfrak{P}_1} = (-1, p)_{\mathfrak{P}_2} = (-1, p)_2 = -1.$$

Moreover,

$$(-1, p)_{\infty_1} = (-f, -d)_{\infty_1} = 1 \quad \text{and} \quad (-1, p)_{\infty_2} = (-f, -d)_{\infty_2} = 1.$$

For every prime $\mathfrak{r} \notin \{\mathfrak{P}\} \cup \mathcal{P}_2 \cup \mathcal{S}$ of K the elements -1, p are $\mathfrak{r}$-adic units, so $(-1, p)_{\mathfrak{r}} = 1$. By Corollary 6.7, $\langle\langle f, d\rangle\rangle \in \operatorname{im}(\phi \circ \varphi)$. ■

Corollary 7.2. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field with $D \equiv 1 \pmod 4$ and $-1 \in N_{K/\mathbb{Q}}(\dot{K})$. Moreover, let $\mathcal{O} = \mathbb{Z}[m(1+\sqrt{D})/2]$ be an order with $m = 2^r q_1 \cdots q_l$, where $r \in \mathbb{N} \cup \{0\}$ and $q_1, \ldots, q_l$ are odd prime numbers. Then the natural homomorphism $\varphi\colon W\mathcal{O} \to WR_K$ is surjective if and only if $r \in \{0, 1\}$ and $q_i \equiv 1 \pmod 4$ for every $i \in \{1, \ldots, l\}$.*

Proof. This follows from Propositions 3.1, 3.7 and 7.1 and Corollaries 3.8 and 3.9. ■

Now assume $K = F(\sqrt{D})$ is a real quadratic function field as in Section 4. The set $\mathcal{S}$ consists of two primes ∞_1, ∞_2 of K which lie over the prime ∞_F of $F = \mathbb{F}(X)$ with uniformizing parameter $1/X$. Assume $u_K(\mathcal{S}) = 0$.

Let ϵ be a generator of the group $\dot{\mathbb{F}}$. If $\epsilon \in N_{K/F}(\dot{K})$, then choose $b \in E(R_K(\mathcal{S}))$ such that $N_{K/F}(b) \in \epsilon \dot{F}^2$. Let $p_1, \ldots, p_s \in \mathbb{F}[X]$ be all the pairwise distinct monic irreducible polynomials which divide D. By [RC, p. 208] and [Cz3, Theorem 4.2] the set

$$\{\langle 1\rangle, \langle\epsilon\rangle, \langle p_1\rangle, \ldots, \langle p_{s-1}\rangle, \langle b\rangle, \langle\langle f,d\rangle\rangle\} \quad \text{when } \epsilon \in N_{K/F}(\dot{K}),$$
$$\{\langle 1\rangle, \langle\epsilon\rangle, \langle p_1\rangle, \ldots, \langle p_{s-1}\rangle, \langle\langle f,d\rangle\rangle\} \quad \text{when } \epsilon \notin N_{K/F}(\dot{K}),$$

generates the group $\phi(WR_K(\mathcal{S}))$, where $f, d \in K$ are such that

$$(-f,-d)_{\infty_1} = (-f,-d)_{\infty_2} = -1$$

(cf. [Cz3, p. 611]).

Proposition 7.3. *Assume $\epsilon \in N_{K/F}(\dot{K})$. Let $\mathcal{O} = \mathbb{F}[X][m\sqrt{D}]$ be an order with $m = q_1 \cdots q_l$, where $q_1, \ldots, q_l \in \mathbb{F}[X]$ are irreducible polynomials with $\deg q_i \equiv 0 \pmod 2$ for every $i \in \{1, \ldots, l\}$. Then $\langle\langle f,d\rangle\rangle \in \operatorname{im}(\phi \circ \varphi)$.*

Proof. For an irreducible polynomial $p \in \mathbb{F}[X]$ denote by $\left(\frac{\cdot}{p}\right)$ the quadratic residue symbol (cf. [R, p. 24]).

By [O, 65:17] there are infinitely many irreducible polynomials $p \in \mathbb{F}[X]$ such that

$$\left(\frac{D}{p}\right) \neq 1 \quad \text{and} \quad \left(\frac{\epsilon}{p}\right) \neq 1.$$

Fix such a p. From $\left(\frac{D}{p}\right) \neq 1$ it follows that p does not split in K (cf. [R, Proposition 10.5]. From $\left(\frac{\epsilon}{p}\right) \neq 1$ it follows that $\deg p \equiv 1 \pmod 2$ (cf. [R, Proposition 3.2]). Hence $p \nmid m$, so

$$pR_K(\mathcal{S}) + \mathfrak{f} = pR_K(\mathcal{S}) + mR_K(\mathcal{S}) = R_K(\mathcal{S}).$$

Let $\mathfrak{P}$ be the prime of K which lies over p. Then $(\epsilon, p)_{\mathfrak{P}} = 1$. Because $\deg p \equiv 1 \pmod 2$, we have $(\epsilon, p)_{\infty_F} = -1$, i.e.

$$(\epsilon, p)_{\infty_1} = (\epsilon, p)_{\infty_2} = (\epsilon, p)_{\infty_F} = -1.$$

For every prime $\mathfrak{r} \notin \{\mathfrak{P}\} \cup \mathcal{S}$ of K the elements ϵ, p are $\mathfrak{r}$-adic units, so $(\epsilon, p)_{\mathfrak{r}} = 1$. By Corollary 6.7, $\langle\langle f,d\rangle\rangle \in \operatorname{im}(\phi \circ \varphi)$. ∎

Corollary 7.4. *Let $K = F(\sqrt{D})$ be a real quadratic function field with $\epsilon \in N_{K/F}(\dot{K})$. Moreover, let $\mathcal{O} = \mathbb{F}[X][m\sqrt{D}]$ be an order such that $m = q_1 \cdots q_l$, where $q_1, \ldots, q_l \in \mathbb{F}[X]$ are irreducible polynomials. Then the homomorphism $\varphi\colon W\mathcal{O} \to WR_K(\mathcal{S})$ is surjective if and only if $\deg q_i \equiv 0 \pmod 2$ for every $i \in \{1, \ldots, l\}$.*

Proof. This follows from (4.2), Propositions 4.2, 4.6 and 7.3, and Corollaries 4.8 and 4.9. ∎

Proposition 7.5. *Let $K = F(\sqrt{D})$ be a real quadratic function field with $\epsilon \notin N_{K/F}(\dot{K})$ and $u_K(\mathcal{S}) = 0$. Moreover, let $\mathcal{O} < R_K(\mathcal{S})$ be an order. Then $\langle\langle f,d\rangle\rangle \in \operatorname{im}(\phi \circ \varphi)$.*

Proof. From [RC, Proposition 6.2] it follows that there is an irreducible divisor p_i of the polynomial D such that $\deg p_i \equiv 1 \pmod 2$. It is easy to observe that p_i ramifies in K.

Analogously to the proof of Proposition 7.3 we show that

$$(\epsilon, p_i)_{\infty_1} = (\epsilon, p_i)_{\infty_2} = -1$$

and $(\epsilon, p_i)_{\mathfrak{r}} = 1$ for every prime $\mathfrak{r} \notin \mathcal{S}$ of K.

Proposition 4.2 implies that $\langle p_i \rangle \in \operatorname{im}(\phi \circ \varphi)$. By Theorem 2.9 there exists $h \in \mathcal{O}$ such that

$$h\dot{K}^2 = p_i \dot{K}^2 \quad \text{and} \quad hR_K(\mathcal{S}) + \mathfrak{f} = R_K(\mathcal{S}).$$

Obviously,

$$(\epsilon, h)_{\infty_1} = (\epsilon, h)_{\infty_2} = -1$$

and $(\epsilon, h)_{\mathfrak{r}} = 1$ for every prime $\mathfrak{r} \notin \mathcal{S}$ of K. Now Corollary 6.7 implies that $\langle\langle f, d \rangle\rangle \in \operatorname{im}(\phi \circ \varphi)$. ∎

COROLLARY 7.6. *Let $K = F(\sqrt{D})$ be a real quadratic function field with $\epsilon \notin N_{K/F}(\dot{K})$. Moreover, let $\mathcal{O} < R_K(\mathcal{S})$ be an order. Then the homomorphism $\varphi\colon W\mathcal{O} \to WR_K(\mathcal{S})$ is surjective.*

Proof. This follows from (4.2), Propositions 4.2 and 7.5, and Corollary 4.4. ∎

References

[B] R. Baeza, *Quadratic Forms over Semilocal Rings*, Lecture Notes in Math. 655, Springer, Berlin, 1978.

[BC] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Nauka, Moscow, 1985 (in Russian).

[C1] M. Ciemała, *Natural homomorphisms of Witt rings of orders in algebraic number fields*, Math. Slovaca 54 (2004), 473–477.

[C2] M. Ciemała, *Natural homomorphisms of Witt rings of orders in algebraic number fields, II*, Acta Math. Univ. Ostrav. 14 (2006), 13–16.

[CS] M. Ciemała and K. Szymiczek, *On the existence of nonsingular bilinear forms on projective modules*, Tatra Mt. Math. Publ. 32 (2005), 1–13.

[Cz1] A. Czogała, *Generators of the Witt groups of algebraic integers*, in: Number Theory (Cieszyn, 1998), Ann. Math. Sil. 12 (1998), 105–121.

[Cz2] A. Czogała, *On reciprocity equivalence of quadratic number fields*, Acta Arith. 58 (1991), 27–46.

[Cz3] A. Czogała, *Witt rings of Hasse domains of global fields*, J. Algebra 244 (2001), 604–630.

[GHK] A. Geroldinger, F. Halter-Koch and J. Kaczorowski, *Non-unique factorizations in orders of global fields*, J. Reine Angew. Math. 459 (1995), 89–118.

[K] M. Knebusch, *Grothendieck und Wittringe von nichtausgearteten symmetrischen Bilinearformen*, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. 1969/1970, 93–157.

[M] M. A. Marshall, *Bilinear Forms and Orderings on Commutative Rings*, Queen's Papers in Pure Appl. Math. 71, Queen's Univ., Kingston, ON, 1985.

[MH] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Ergeb. Math. Grenzgeb. 73, Springer, New York, 1973.

[O] O. T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren Math. Wiss. 117, Academic Press, New York, and Springer, Berlin, 1963.

[P] A. Pfister, *Quadratic Forms with Applications to Algebraic Geometry and Topology*, London Math. Soc. Lecture Note Ser. 217, Cambridge Univ. Press, 1995.

[R] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, New York, 2002.

[Ro] B. Rothkegel, *Nonsingular bilinear forms on direct sums of ideals*, Math. Slovaca 63 (2013), 707–724.

[RC] B. Rothkegel and A. Czogała, *Singular elements and the Witt equivalence of rings of algebraic integers*, Ramanujan J. 17 (2008), 185–217.

[W] Ch. Weibel, *An introduction to algebraic K-theory*, http://www.math.uiuc.edu/K-theory/0105/.

Beata Rothkegel
Institute of Mathematics
University of Silesia
Bankowa 14
40-007 Katowice, Poland
E-mail: brothkegel@math.us.edu.pl

Received on 20.7.2012
and in revised form on 25.2.2013 (7134)