Knebusch–Milnor Exact Sequence and Parity of Class Numbers

KAZIMIERZ SZYMICZEK

Abstract. We show that the Knebusch–Milnor exact sequence for the Witt group of quadratic forms over a number field K can be used to determine the parity of ideal class number of the field K. As an example we reprove the classic results on quadratic number fields with odd class numbers.

1991 Mathematics Subject Classification: Primary 11R29, Secondary 11E12

Introduction

The relationship between the integral theory of quadratic forms and class numbers of algebraic number fields is one of the fundamental features of algebraic number theory. It manifests most clearly in the Gauss' determination of the 2-rank of the (narrow) ideal class group of a quadratic field. On the other hand, the simpler theory of quadratic forms over number fields seems to have looser connection to the subtle questions of class numbers and class group structure.

In this note, however, we show that a general result on Witt groups of quadratic forms over number fields, the exactness of the Knebusch–Milnor sequence, supplies an effective criterion for the parity of class numbers. We try the strength of the criterion by showing that it provides a complete determination of quadratic number fields with odd class numbers. Thus these subtle arithmetic results follow rather easily from the simpler *rational* (as opposed to the more sophisticated *integral*) quadratic form theory.

The fact that Witt rings of number fields carry some data on the parity of class numbers was first noticed in [7], and then some further results in this direction were given in [4]. A deeper study of the relations between Witt equivalence of number fields and 2-ranks of ideal class groups will be presented in a forthcoming paper by P. E. Conner, R. Perlis and the author [2].

The notation is standard. We write $(a_1, \ldots, a_n)$ for the n–dimensional diagonal quadratic form $a_1X_1^2 + \cdots + a_nX_n^2$ over a field K, and $D_K(a_1, \ldots, a_n)$ for its value set. The Legendre symbol is written (a/p).

1 The Knebusch–Milnor sequence

Let K be a number field, $\mathcal{O}_K$ its ring of integers and $C(K)$ the ideal class group of K. We write $\Omega(K)$ for the set of all finite primes of K. For each $\mathbf{p} \in \Omega(K)$, let $K_\mathbf{p}$ be the $\mathbf{p}$–adic completion of K, and $\overline{K_\mathbf{p}}$ the residue class field of $K_\mathbf{p}$. Then, with $\mathbf{p}$ running over all finite primes of K we have the following *Knebusch–Milnor sequence* for the Witt groups $W(\mathcal{O}_K), W(K)$ and $W(\overline{K_\mathbf{p}})$:

$$0 \to W(\mathcal{O}_K) \xrightarrow{i} W(K) \xrightarrow{\partial_K} \coprod_{\mathbf{p}} W(\overline{K_\mathbf{p}}) \xrightarrow{\lambda} C(K)/C(K)^2 \to 0. \qquad (1)$$

Here i is the natural injection. In fact, without going into details of Witt groups of rings, it is best for us to define $W(\mathcal{O}_K)$ as the kernel of the homomorphism ∂_K.

We recall now the definition of ∂_K. For each finite prime $\mathbf{p}$ of K we consider the *second residue class homomorphism*

$$\partial_\mathbf{p} : W(K_\mathbf{p}) \longrightarrow W(\overline{K_\mathbf{p}}).$$

This can be defined only after fixing a prime element π in $K_\mathbf{p}$. Then every element $\phi \in W(K_\mathbf{p})$ can be written as

$$\phi = \langle a_1, \ldots, a_k, b_1\pi, \ldots, b_m\pi\rangle,$$

where a_i, b_j are units in $K_\mathbf{p}$. We set

$$\partial_\mathbf{p}(\phi) := \langle \bar{b}_1, \ldots, \bar{b}_m\rangle \in W(\overline{K_\mathbf{p}}),$$

where $\bar{b}$ is the canonical image of the $\mathbf{p}$–adic unit b in the residue class field $\overline{K_\mathbf{p}}$. Notice that this construction does not distinguish between dyadic and nondyadic primes.

Now we globalize. Given $\phi \in W(K)$ we write $\phi_\mathbf{p}$ for the image of ϕ under the natural homomorphism $W(K) \to W(K_\mathbf{p})$ and define $\partial_\mathbf{p}(\phi) := \partial_\mathbf{p}(\phi_\mathbf{p})$. Then, for each prime $\mathbf{p}$ we have the group homomorphism

$$\partial_\mathbf{p} : W(K) \to W(\overline{K_\mathbf{p}}).$$

For any fixed $\phi \in W(K)$ we have $\partial_\mathbf{p}(\phi) = 0$ for almost all primes $\mathbf{p}$. Hence we can aggregate these homomorphisms into one homomorphism

$$\partial_K : W(K) \longrightarrow \coprod_{\mathbf{p}} W(\overline{K_\mathbf{p}}), \quad \partial_K(\phi) = (\partial_\mathbf{p}(\phi)).$$

∂_K is said to be the *boundary* homomorphism. We will write ∂ instead of ∂_K, when there is no risk of ambiguity.

It remains to recall the definition of λ. Let $\eta = (\eta_\mathbf{p}) \in \coprod_\mathbf{p} W(\overline{K_\mathbf{p}})$. We set

$$\lambda(\eta) = [\prod_{\mathbf{p}} \mathbf{p}^{e(\eta_\mathbf{p})}]\, C(K)^2.$$

Here $e : W(\overline{K_{\mathbf{p}}}) \to \mathbb{Z}/2\mathbb{Z}$ is the ***dimension index*** homomorphism, and the square brackets are used to denote the ideal class in $C(K)$.

The main result we will use in this paper states that (1) is an *exact* sequence. In fact, the sequence is exact independently of the particular choices of the involved second residue class homomorphisms. Proofs can be found in the books by J. Milnor and D. Husemoller [5], and W. Scharlau [6].

2 Knebusch–Milnor sequence class number parity criterion

The following criterion for parity of the class number of K follows immediately from the exactness of the sequence (1).

Class number parity criterion. *The class number h_K of a number field K is odd if and only if the boundary homomorphism ∂_K is surjective.*

PROOF: The class number h_K is odd if and only if the ideal class group $C(K)$ satisfies $C(K) = C(K)^2$ if and only if λ is a trivial homomorphism if and only if ∂_K is surjective. □

The surjectivity of $\partial = \partial_K$ will be established when we show that a set of generators of the target group lies in the image of ∂.

The group $\coprod_{\mathbf{p}} W(\overline{K_{\mathbf{p}}})$ is the direct sum of cyclic groups of orders 2 and 4, and we will choose the generators for these cyclic direct summands as our set of generators for the group. To explain this we first recall the structure of the Witt groups of residue class fields $\overline{K_{\mathbf{p}}}$. Here $\overline{K_{\mathbf{p}}}$ is a finite field and the structure of the Witt group $W(\overline{K_{\mathbf{p}}})$ depends on the number of elements $N(\mathbf{p}) := |\overline{K_{\mathbf{p}}}|$ of the residue class field (rather than on the characteristic).

If $N(\mathbf{p})$ is even (so that char $\overline{K_{\mathbf{p}}} = 2$), the Witt group $W(\overline{K_{\mathbf{p}}})$ is cyclic of order 2 generated by $\langle 1 \rangle$. If $N(\mathbf{p}) \equiv 3 \pmod 4$ the Witt group $W(\overline{K_{\mathbf{p}}})$ is cyclic of order 4 generated by $\langle 1 \rangle$. And for $N(\mathbf{p}) \equiv 1 \pmod 4$ the Witt group $W(\overline{K_{\mathbf{p}}})$ is the Klein four-group generated by $\langle 1 \rangle$ and $\langle \bar{u} \rangle$, where $\bar{u}$ is the residue $\pmod{\mathbf{p}}$ of a nonsquare unit u in $K_{\mathbf{p}}$. In the case $N(\mathbf{p}) \equiv 1 \pmod 4$ we choose and fix a nonsquare unit $u \in K_{\mathbf{p}}$ and denote it $u = u(\mathbf{p})$.

From this it follows that the group $\coprod_{\mathbf{p}} W(\overline{K_{\mathbf{p}}})$ is the direct sum of cyclic groups generated by the elements in the set

$$\{\eta^{\mathbf{p}} : \mathbf{p} \in \Omega(K)\} \quad \cup \quad \{\mu^{u(\mathbf{p})} : \mathbf{p} \in \Omega(K) \text{ with } N(\mathbf{p}) \equiv 1 \pmod 4\},$$

where

$$(\eta^{\mathbf{p}})_{\mathbf{q}} \quad = \quad \begin{cases} \langle 1 \rangle & \text{for } \mathbf{q} = \mathbf{p}, \\ \langle 0 \rangle & \text{for } \mathbf{q} \neq \mathbf{p}, \end{cases}$$

$$(\mu^{u(\mathbf{p})})_{\mathbf{q}} = \begin{cases} \langle \bar{u} \rangle & \text{for } \mathbf{q} = \mathbf{p}, \\ \langle 0 \rangle & \text{for } \mathbf{q} \neq \mathbf{p}. \end{cases}$$

Here the subscript $\mathbf{q}$ indicates the $\mathbf{q}$–th coordinate of the element.

The following lemma shows that trying to establish the surjectivity of ∂ we do not have to bother about locating the generators $\mu^{u(\mathbf{p})}$ in the image of ∂.

Lemma 1. *For a prime* $\mathbf{p} \in \Omega(K)$ *with* $N(\mathbf{p}) \equiv 1 \pmod 4$,

$$\eta^{\mathbf{p}} \in \operatorname{im} \partial \quad \textit{iff} \quad \mu^{u(\mathbf{p})} \in \operatorname{im} \partial.$$

Hence the boundary homomorphism ∂ *is surjective if and only if all the generators* $\eta^{\mathbf{p}}$, $\mathbf{p} \in \Omega(K)$, *lie in the image of* ∂.

PROOF: This is a simple consequence of the exactness of the sequence (1). For observe that the generators $\eta^{\mathbf{p}}$ and $\mu^{u(\mathbf{p})}$ have the same image under λ :

$$\lambda(\eta^{\mathbf{p}}) = [\mathbf{p}]\, C(K)^2 = \lambda(\mu^{u(\mathbf{p})}).$$

Hence, by the exactness of the sequence (1),

$$\eta^{\mathbf{p}} \in \operatorname{im} \partial \quad \text{iff} \quad \eta^{\mathbf{p}} \in \ker \lambda \quad \text{iff} \quad \mu^{u(\mathbf{p})} \in \ker \lambda \quad \text{iff} \quad \mu^{u(\mathbf{p})} \in \operatorname{im} \partial$$

which proves the Lemma. □

Lemma 2. *Let p be a rational prime and suppose p is inert in K, that is,* $p\mathcal{O}_K = \mathbf{p}$ *is a prime ideal. Then for the one-dimensional form* $\langle p \rangle \in W(K)$ *we have*

$$\partial \langle p \rangle = \eta^{\mathbf{p}}$$

for a suitable choice of the residue class homomorphism $\partial_{\mathbf{p}}$. *Hence* $\eta^{\mathbf{p}} \in \operatorname{im} \partial$ *for all inert primes* $\mathbf{p}$ *of* K.

PROOF: Choosing p as the prime element in the completion $K_{\mathbf{p}}$ it is immediate that $\partial \langle p \rangle = \eta^{\mathbf{p}}$. □

Lemma 3. *For an arbitrary prime ideal* $\mathbf{p}$ *in* $\mathcal{O}_K$ *the following are equivalent.*
(a) $\eta^{\mathbf{p}} \in \operatorname{im} \partial$.

(b) *There is a number* $\beta \in \mathcal{O}_K$ *and an ideal* $\mathbf{a}$ *in* $\mathcal{O}_K$ *such that*

$$\beta \mathcal{O}_K = \mathbf{p}\, \mathbf{a}^2. \tag{2}$$

(c) *There is a number* $\beta \in \mathcal{O}_K$ *such that with an appropriate choice of the prime element in the* $\mathbf{p}$–*adic completion of* K, *we have*

$$\eta^{\mathbf{p}} = \partial \langle \beta \rangle$$

for the one-dimensional form $\langle\beta\rangle$ in $W(K)$.

PROOF: If $\eta^{\mathbf{p}} \in \operatorname{im}\partial$, then, by the exactness of the sequence (1), we have $\eta^{\mathbf{p}} \in \ker\lambda$, that is,

$$C(K)^2 = \lambda(\eta^{\mathbf{p}}) = [\mathbf{p}]C(K)^2.$$

Thus there are a number $\beta \in \mathcal{O}_K$ and an ideal $\mathbf{a}$ of $\mathcal{O}_K$ such that (2) holds. This proves (a) $\Rightarrow$ (b).

Now assume (b) holds and consider the 1-dimensional form $\langle\beta\rangle \in W(K)$. By (2), we have $\partial_{\mathbf{q}}\langle\beta\rangle = 0$ for all prime ideals $\mathbf{q} \neq \mathbf{p}$. On the other hand, β has odd $\mathbf{p}$–order, hence $\beta = \pi x^2$ for some $\pi, x \in K_{\mathbf{p}}$ with $\operatorname{ord}_{\mathbf{p}} \pi = 1$. Choosing π as the prime element in $K_{\mathbf{p}}$ and adjusting the residue class homomorphism $\partial_{\mathbf{p}}$ to the new choice of the prime element, we get $\partial_{\mathbf{p}}\langle\beta\rangle = \langle 1\rangle$. This shows that the new boundary homomorphism ∂ (modified at the $\mathbf{p}$–th coordinate) satisfies $\partial\langle\beta\rangle = \eta^{\mathbf{p}}$. This proves (b) $\Rightarrow$ (c), and (c) $\Rightarrow$ (a) is trivial.

□

3 Quadratic fields with odd class numbers

The following is the complete list of quadratic fields with odd class numbers:

$$K = \mathbb{Q}(\sqrt{d}), \qquad d = -1, \pm 2, -q, r, 2q, qq_1, \tag{3}$$

where r is an arbitrary odd prime and q and q_1 are primes congruent to 3 $\pmod 4$ (see [1], Corollary (18.4)).

We now give a new proof of this result based on the class number parity criterion discussed in Section 2, and on the techniques of rational quadratic form theory.

Theorem. *For a quadratic number field K the following statements are equivalent.*

(A) *The class number h_K is odd.*

(B) *The boundary homomorphism ∂_K is surjective.*

(C) *Every rational prime number p which is split or ramified in K is represented, up to the sign, as the norm of a number in K.*

(D) *$K = \mathbb{Q}(\sqrt{d})$, where $d = -1, \pm 2, -q, r, 2q, qq_1$, with r an arbitrary odd prime number and q and q_1 prime numbers congruent to* 3 $\pmod 4$.

The proof will be given in a series of propositions showing that

(A) iff (B) $\Rightarrow$ (C) $\Rightarrow$ (D) $\Rightarrow$ (C) $\Rightarrow$ (B).

We will use the quadratic form theory over the p-adic fields and the local-global principle for quadratic forms over the rational number field $\mathbb{Q}$. Another often used argument is the theorem on the existence of prime numbers p with prescribed values of Legendre symbols $(a_1/p), \dots, (a_k/p)$ for any set $a_1, \dots, a_k$ of integers multiplicatively independent in the square class group $\mathbb{Q}^*/\mathbb{Q}^{*2}$ (see [3], Satz 147).

Proposition 1. (A) *iff* (B).

PROOF: This is our class number parity criterion from Section 2. □

Proposition 2. (B) $\Rightarrow$ (C).

PROOF: Suppose p is a rational prime split or ramified in K. Let $p\mathcal{O}_K = \mathbf{p}\bar{\mathbf{p}}$, where $\mathbf{p}$ is a prime ideal in $\mathcal{O}_K$ (here $\mathbf{p} = \bar{\mathbf{p}}$ when p ramifies in K). Since ∂_K is surjective, $\eta^{\mathbf{P}} \in \operatorname{im} \partial$. Hence, by Lemma 3, there is a $\beta \in \mathcal{O}_K$ and an ideal $\mathbf{a}$ in $\mathcal{O}_K$ satisfying

$$\beta\mathcal{O}_K = \mathbf{pa}^2 \qquad \text{and} \qquad \bar{\beta}\mathcal{O}_K = \bar{\mathbf{p}}\bar{\mathbf{a}}^2.$$

It follows that, for a positive rational integer a,

$$\beta\bar{\beta}\mathcal{O}_K = \mathbf{p}\bar{\mathbf{p}} \cdot (\mathbf{a}\bar{\mathbf{a}})^2 = p a^2 \mathcal{O}_{\mathbf{K}}.$$

Hence $N_{K/\mathbb{Q}}(\beta/a)\mathcal{O}_K = p\mathcal{O}_K$, and $p = \pm N_{K/\mathbb{Q}}(\beta/a)$, as required. □

Proposition 3. (C) $\Rightarrow$ (D).

PROOF: Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer and let K satisfy (C). We write $(1, -d)$ for the norm form $X^2 - dY^2$ in $K/\mathbb{Q}$. *Claim* 1. If d is divisible by at least two distinct primes, then all odd prime factors of d are congruent to 3 (mod 4). Suppose d is divisible by at least two distinct primes q and r and assume $q \equiv 1 \pmod 4$. Choose a prime p satisfying

$$(q/p) = (r/p) = -1 \quad \text{and} \quad (c/p) = 1,$$

where c satisfies $d = qrc$. Then we have $(d/p) = 1$ and so p splits in K. We will show that neither p nor $-p$ is a norm from K.

By reciprocity, $(p/q) = (q/p) = -1$. Hence p is a nonsquare unit in $\mathbb{Q}_q$. Then it follows that p is not represented by the form $(1, -d)$ over $\mathbb{Q}_q$, hence p is not represented by the norm form $(1, -d)$ over $\mathbb{Q}$.

On the other hand, -1 is a square in $\mathbb{Q}_q$, hence p and $-p$ are in the same square class in $\mathbb{Q}_q$. Since p is not represented by the form $(1, -d)$ over $\mathbb{Q}_q$, also $-p$ is not represented. Hence neither p nor $-p$ is a norm from K, contrary to the hypothesis (C). This proves Claim 1.

Claim 2. If $d > 0$, then d is divisible by at most two distinct primes. For suppose

q, q_1, q_2 are distinct prime factors of d and assume that q and q_1 are odd primes. Choose a prime p such that

$$(-1/p) = (q/p) = (q_2/p) = -1 \quad \text{and} \quad (r/p) = 1,$$

for all prime factors r of d distinct from q and q_2. Hence we have $p \equiv q \equiv q_1 \equiv 3 \pmod 4$, the latter by Claim 1. Moreover, $(d/p) = 1$ so that p splits in K. By quadratic reciprocity,

$$(-p/q) = -(p/q) = (q/p) = -1,$$

hence $-p$ is a nonsquare unit in $\mathbb{Q}_q$ and so is not represented by the form $(1, -d)$ over $\mathbb{Q}_q$. On the other hand, $(q_1/p) = 1$, hence $(p/q_1) = -1$ and so p is not represented by $(1, -d)$ over $\mathbb{Q}_{q_1}$.

It follows that neither $-p$ nor p is represented by the norm form $(1, -d)$ over $\mathbb{Q}$, contradicting (C). This proves Claim 2.

Claim 3. If $d < 0$, then either $d = -1, -2$, or $-d$ is a prime congruent to 3 (mod 4). Suppose $-d > 2$ and d has two distinct prime factors q and q_1. Suppose that q is odd. Write $d = -qq_1c$, where c is a positive integer. We choose an odd prime p satisfying

$$(q/p) = (q_1/p) = -1, \quad (-1/p) = 1 \quad \text{and} \quad (c/p) = 1.$$

Then $(d/p) = 1$ so that p splits in K. Moreover, $p \equiv 1 \pmod 4$ and $(q/p) = -1$ imply that $(p/q) = (q/p) = -1$. Thus p is a nonsquare unit in $\mathbb{Q}_q$ and so is not represented by $(1, -d)$ in $\mathbb{Q}_q$. It follows that p is not represented by the norm-form $(1, -d)$ over $\mathbb{Q}$. Since $d < 0$, the form $(1, -d)$ represents only positive rational numbers, hence $-p$ is not represented either, contradicting (C).

Thus we have proved that $-d = q$ is a prime number. It remains to show that $q \equiv 3 \pmod 4$. Suppose $q \equiv 1 \pmod 4$ and choose a prime number p satisfying

$$(-1/p) = (q/p) = -1.$$

Then $(d/p) = 1$ and $(p/q) = (q/p) = -1$. It follows that p splits in K and is not represented by the form $(1, -d)$ over $\mathbb{Q}_q$. Hence p is not the norm from K, and $-p$ is not either. This again contradicts (C) and proves our claim. Summarizing, if $d > 0$, then by Claim 2, d is of the form $r, 2q$ or qq_1, where r, q, q_1 are prime numbers. By Claim 1, q and q_1 are congruent to 3 (mod 4). On the other hand, when $d < 0$, then Claim 3 gives the desired result. □

Proposition 4. (D) ⇒ (C).

Our argument splits into two cases depending on the number of ramified primes in the field K. Hence it will be convenient to separate the fields with one ramified prime from those with two ramified primes. We defme the following two classes of quadratic fields:

$$A \ := \ \{Q(V5), \quad c\check{r}=-1,\pm 2,-g,r, \quad g \ EE \ 3 \quad (\mathrm{mod}\ 4), \quad r = 1 \quad (\mathrm{mod}\ 4)\},$$

$$B \ := \ \{Q(VS), \quad d=q,2q,qq_u \quad q = q_t = 3 \quad (\mathrm{mod}\ 4)\},$$

where always g, gi and r are rational prime numbers.

Thus *AUB* covers all fields in the list (3), and in each field of the class *A* there is just one ramified prime, while in fields of the class *B* there are two ramified primes.

The following two lemmas provide a more detailed version of Proposition 4.

Lemma 4. *Let K — Q(vd) be a quadratic number field listed in* (3). (a) *// K belongs to the class A, then every rational prime split in K is the norm of a number in K.* (b) *If K belongs to the class B and p is a rational prime split in K, then either p or —p is the norm of a number in K.*

PROOF: We want to show that for every split rational prime *p* the norm form (1, *—d)* represents one of dbp over Q. For this we use the local-global principle. It suffices to show that

$$pEDq_p\{l,-dy \qquad \text{for} \qquad P\backslash 2pd \tag{4a}$$

in the čase (a), and

$$p£Dq_p\{l_)-d) \quad \text{for} \quad P\backslash 2pd \qquad \text{or} \qquad -p \ £ \ DQ_P(1,-d) \quad \text{for} \quad P\backslash 2pd \tag{4b}$$

in the čase (b). Here *P* denotes a rational prime. Consider hrst the prime *P* = *p*. If *p* ^ 2 is split in Ji, then we háve *(d/p)* = 1, and, by HensePs lemma, *d* is a square in Q_p. If *p* — 2 splits in /i, we must háve *d* = 1 (mod 8). But then *d* is a square in the dyadic field Q2. Hence if any prime *p* splits in *K,* then oř is a square in Q_p. It follows that (1, — *d)* ~ (1,-1) over Q_p, and so the form (1, *—d)* is universal over Q_p, hence represents *p* as well as — *p* over Q_p. Thus when *P* — *p* the statements (4a) and (4b) hold in the stronger form asserting that both *p* and *—p* are represented by (1, —oř) over Q_p. Now we proceed to the statement (a). The prime *P* = *p* has already been dealt with and so to prove (4a) it suffices to show that for any split prime p,

$$PG\%(1,-(I) \qquad \text{for} \qquad P\backslash 2d. \tag{5}$$

Consider the prime *P* = *q* = 3 (mod 4). First assume that *p* ^ 2. If *q* \ d, we must háve oř = — g, and since *p* is split in *K,* the field discriminant — g is a quadratic residue modp. Hence, in terms of Legendre symbols, *(q/p)* = (— *l/p)* = $(-1)(P^{-1})/^{2}$. On the other hand, by quadratic reciprocity,

$$(p/q) = (q/p) \cdot (-1)^{\wedge ' v} = (q/p) \cdot (-1)^{\wedge} = 1.$$

Hence each split rational prime $p \neq 2$ is a quadratic residue mod$q$. By Hensel's lemma, p is a square in $\mathbb{Q}_q$ and so p is certainly represented by the form $(1, -d)$ over $\mathbb{Q}_q$.

Now let $p = 2$. So 2 is split in $K = \mathbb{Q}(\sqrt{d})$, with $d = -q$. This forces $-q \equiv 1 \pmod 8$, hence $(2/q) = 1$, and so 2 is a square in $\mathbb{Q}_q$. Thus $p = 2$ is represented by the form $(1, -d)$ over $\mathbb{Q}_q$. This establishes (5) in the case $P = q$. Next we consider $P = r$. Now $d = r \equiv 1 \pmod 4$. Again we first assume that $p \neq 2$. Then $(r/p) = 1$, and by reciprocity, $(p/r) = 1$. Hence p is a square in $\mathbb{Q}_r$ and so p is represented by the form $(1, -d)$ over $\mathbb{Q}_r$.

When $p = 2$ is the split prime, we have $d = r \equiv 1 \pmod 8$, and it follows that 2 is a square in $\mathbb{Q}_r$. Then $p = 2$ is represented by the form $(1, -d)$ over $\mathbb{Q}_r$. Thus for all d considered in case (a) we have verified (5) for all primes $P \mid 2d$ except for $P = 2$. In other words, the Hilbert symbol $(p, d)_P$ assumes the value 1 for all primes P (including the infinite primes) except possibly for $P = 2$. By Hilbert reciprocity, $(p, d)_2 = 1$, as well. It follows that p is represented by the form $(1, -d)$ everywhere locally, hence, by the Hasse-Minkowski Principle, p is represented by $(1, -d)$ over $\mathbb{Q}$, as desired. Now we prove (b).

Let p be a rational prime split in K. Since (4b) has already been verified for the prime $P = p$ with *or* replaced by *and*, it suffices to show that

$$p \in D_{\mathbb{Q}_P}(1, -d) \text{ for } P \mid 2d \qquad \text{or} \qquad -p \in D_{\mathbb{Q}_P}(1, -q) \text{ for } P \mid 2d. \tag{6}$$

Consider the prime $P = q$. We have

$$(-p/q) = (-1)^{\frac{q-1}{2}}(p/q) = -(p/q),$$

hence either p or $-p$ is a square in $\mathbb{Q}_q$. It follows that one of the numbers $\pm p$ is represented by the form $(1, -d)$ in the field $\mathbb{Q}_q$.

Thus in the cases $d = q$ and $d = 2q$ we have proved that one of the numbers $\pm p$ is represented by the form $(1, -d)$ in all the fields $\mathbb{Q}_P$, except possibly in $\mathbb{Q}_2$.

Now we consider the case $d = qq_1$. The same argument as for $P = q$ above applies when $P = q_1$. We show that one of $\pm p$ is *simultaneously* represented by $(1, -d)$ over $\mathbb{Q}_q$ and over $\mathbb{Q}_{q_1}$. We again consider separately the cases $p \neq 2$ and $p = 2$.

If $p \neq 2$, then p split in K implies that $(qq_1/p) = 1$, hence $(q/p) = (q_1/p)$. On the other hand,

$$(p/q) = (q/p) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = (q_1/p) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q_1-1}{2}} = (p/q_1),$$

and also $(-p/q) = -(p/q) = -(p/q_1) = (-p/q_1)$. Hence either p is a square in $\mathbb{Q}_q$ and in $\mathbb{Q}_{q_1}$ or $-p$ is a square in $\mathbb{Q}_q$ and in $\mathbb{Q}_{q_1}$. It follows that when $p \neq 2$, one of the numbers $\pm p$ is represented by the form $(1, -d)$ in $\mathbb{Q}_q$ and in $\mathbb{Q}_{q_1}$. Now let $p = 2$ be the split prime. Then we have $d = qq_1 \equiv 1 \pmod 8$, and so $q \equiv q_1 \pmod 8$.

If $q \equiv q_1 \equiv 3 \pmod 8$, then $(-2/q) = (-2/q_1) = 1$, hence -2 is a square in both $\mathbb{Q}_q$ and $\mathbb{Q}_{q_1}$.

The other possibility is $q \equiv q_1 \equiv 7 \pmod 8$, and then $(2/q) = (2/q_1) = 1$, hence 2 is a square in both $\mathbb{Q}_q$ and $\mathbb{Q}_{q_1}$.

In each case either $p = 2$ or $-p = -2$ is represented by the form $(1, -d)$ over $\mathbb{Q}_q$ and over $\mathbb{Q}_{q_1}$. Summarizing, we have shown that (6) holds for all prime divisors P of $2d$ except possibly for $P = 2$. By Hilbert reciprocity, (6) holds for $P = 2$, as well.

Thus with a proper choice of the sign, $\pm p$ is represented by the form $(1, -d)$ everywhere locally, hence, by the Hasse-Minkowski Principle, $\pm p$ is represented by $(1, -d)$ over $\mathbb{Q}$, as desired. □

Lemma 5. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field listed in (3). Let p be a rational prime ramified in K. Then either p or $-p$ is the norm of a number in K.*

Proof: When $K \in \mathcal{A}$, then we have $N_{K/\mathbb{Q}}(\sqrt{d}) = -d$ for $d = \pm 2, -q, r$ and $N_{K/\mathbb{Q}}(1 + i) = 2$ for $d = -1$. This proves the Lemma for fields in $\mathcal{A}$. Now we assume that $K \in \mathcal{B}$. Consider first the case when $d = q$. Then the ramified primes are $p = 2$ and $p = q$. If $q \equiv 3 \pmod 8$, then $(-2/q) = 1$, hence, by the local-global principle, -2 is represented by the form $(1, -q)$ over $\mathbb{Q}$. If $q \equiv 7 \pmod 8$, then $(2/q) = 1$, hence 2 is represented by the form $(1, -q)$ over $\mathbb{Q}$. Thus either 2 or -2 is the norm of a number in K. As to the ramified prime $p = q$, we have $-q = N_{K/\mathbb{Q}}(\sqrt{q})$. Now let $d = 2q$. The ramified primes are $p = 2$ and $p = q$. If $q \equiv 3 \pmod 8$, then $(-2/q) = 1$, hence -2 is a square in $\mathbb{Q}_q$. It follows that the quadratic form $(1, -2q)$ represents both -2 and q over $\mathbb{Q}_q$, and by the local-global principle, the form represents -2 and q over $\mathbb{Q}$.

If $q \equiv 7 \pmod 8$, then $(2/q) = 1$, hence 2 is a square in $\mathbb{Q}_q$. It follows that the quadratic form $(1, -2q)$ represents both 2 and $-q$ over $\mathbb{Q}_q$, and by the local-global principle, the form represents 2 and $-q$ over $\mathbb{Q}$. Finally let $d = qq_1$ so that the ramified primes are $p = q$ and $p = q_1$. First suppose that $(q/q_1) = 1$. Then q is a square in $\mathbb{Q}_{q_1}$, hence is represented by the form $(1, -qq_1)$ over $\mathbb{Q}_{q_1}$. Moreover, $(-q_1/q) = -(q_1/q) = (q/q_1) = 1$, hence $-q_1$ is a square in $\mathbb{Q}_q$. It follows that $(1, -qq_1) \cong (1, q)$ over $\mathbb{Q}_q$, and so q is represented by the form $(1, -qq_1)$ over $\mathbb{Q}_q$ as well. By the local-global principle, q is represented by the norm form $(1, -qq_1)$ over $\mathbb{Q}$.

Now consider the other ramified prime $p = q_1$. We know that q is a square in $\mathbb{Q}_{q_1}$, hence $(1, -qq_1) \cong (1, -q_1)$ over $\mathbb{Q}_{q_1}$ so that $-q_1$ is represented by $(1, -qq_1)$ over $\mathbb{Q}_{q_1}$. On the other hand, $-q_1$ is a square in $\mathbb{Q}_q$ and so $-q_1$ is represented by the form $(1, -qq_1)$ over $\mathbb{Q}_q$. By the local-global principle, $-q_1$ is represented by the norm form $(1, -qq_1)$ over $\mathbb{Q}$.

Thus if $(q/q_1) = 1$, the numbers q and $-q_1$ are represented by the norm form of

K, hence are norms of some numbers in K. It remains to consider the case when $(q/q_1) = -1$. But then we have $(q_1/q) = -(q/q_1) = 1$, and by symmetry, $-q$ and q_1 are the norms of some numbers in K. □

PROOF OF PROPOSITION 4: Combine Lemmas 4 and 5. □

In the final part of the proof we will use the following auxiliary result.

Lemma 6. *Let K be a quadratic number field. Suppose p is a rational prime and*

$$\pm\, pa^2 = \beta\bar{\beta}, \tag{7}$$

where $a \in \mathbb{N}$, $\beta \in \mathcal{O}_K$ and the rational positive integer a assumes the smallest possible value.

(a) *If p is split in K, then β and $\bar{\beta}$ do not have any common prime ideal factors.*

(b) *If p is ramified in K, $p\mathcal{O}_K = \mathbf{q}^2$, where $\mathbf{q}$ is a prime ideal, then the only common prime ideal factor of β and $\bar{\beta}$ is $\mathbf{q}$ and*

$$\operatorname{ord}_{\mathbf{q}} \beta = \operatorname{ord}_{\mathbf{q}} \bar{\beta} = 1.$$

PROOF: Let p be a rational prime which is either split or ramified in K, and let $\mathbf{p}$ be a prime ideal in $\mathcal{O}_K$ and

$$\mathbf{p}|\beta \quad \text{and} \quad \mathbf{p}|\bar{\beta}, \tag{8}$$

where β and $\bar{\beta}$ satisfy (7). There are three cases to consider. First assume that the prime ideal $\mathbf{p}$ is a factor of a split rational prime r. Since $\mathbf{p}|\bar{\beta}$ implies $\bar{\mathbf{p}}|\beta$, we have $r\mathcal{O}_K = \mathbf{p}\bar{\mathbf{p}}|\beta$. It follows that $r|\beta$ and so also $r|\bar{\beta}$. This forces $r|a$ and so, with $\beta_1 = \beta/r$ and $a_1 = a/r$, we have

$$\pm pa_1^2 = \beta_1\bar{\beta}_1,$$

where $a_1 < a$ and $\beta_1 \in \mathcal{O}_K$, contrary to the choice of a and β. The second case is when $\mathbf{p}$ is an inert prime. Hence $\mathbf{p} = r\mathcal{O}_K$, where r is a rational prime. Then (8) implies that $r|\beta$ and $r|\bar{\beta}$, hence $r|a$, and we argue as in the first case to reach a contradiction. Thus far we have proved that in both cases (a) and (b) the numbers β and $\bar{\beta}$ do not have any split or inert common prime ideal factors.

Now we consider the case when $\mathbf{p}$ is the factor of a ramified prime q, that is, $\mathbf{p}^2 = q\mathcal{O}_K$. Then (8) implies that $q|pa^2$. Here we have to distinguish between the cases (a) and (b).

If p is split, then we must have $q \mid a^2$ (since q is ramified and so $p \neq q$).

If p is ramified in K, $p\mathcal{O}_K = \mathbf{q}^2$, where $\mathbf{q}$ is a prime ideal, and $\mathbf{p} \neq \mathbf{q}$, then $q|pa^2$ implies again that $q|a^2$. In both cases it follows that $q|a$, hence $\mathbf{p}^4|\beta\bar{\beta}$. Since $\mathbf{p} = \bar{\mathbf{p}}$, it follows that $\mathbf{p}^2|\beta$ and $\mathbf{p}^2|\bar{\beta}$, hence $q|a$, $q|\beta$, $q|\bar{\beta}$, and once again we reach a contradiction. This finishes the proof of (a) and shows that, in the case (b), the only common prime ideal factor of β and $\bar{\beta}$ is the ideal $\mathbf{q}$. Suppose $\mathbf{q}^2|\beta$. Since $p\mathcal{O}_K = \mathbf{q}^2$ and $\mathbf{q} = \bar{\mathbf{q}}$, we also have $\mathbf{q}^2|\bar{\beta}$. Hence $p|\beta$, $p|\bar{\beta}$ and $p^2|\beta\bar{\beta} = \pm pa^2$. It follows that $p|a$, and, as above, this contradicts the choice of a and β. Hence $\operatorname{ord}_{\mathbf{q}}\beta = 1$, and since $\mathbf{q} = \bar{\mathbf{q}}$, we have also $\operatorname{ord}_{\mathbf{q}}\bar{\beta} = 1$.

□

Proposition 5. (C) $\Rightarrow$ (B).

Proof: In view of Lemmas 1 and 2 it suffices to show that for all split and all ramified primes $\mathbf{p}$ of the field K, the generators $\eta^{\mathbf{p}}$ are in the image of ∂. So let $\mathbf{p}$ be a factor of a rational prime p which splits or ramifies in K. By (C), we can assume that there is a positive rational integer a and a number $\beta \in \mathcal{O}_K$ such that

$$\pm pa^2 = \beta\bar{\beta}.$$

Of all equations of this type we choose one in which a assumes the least value.

We know from Lemma 6 how to determine the common prime ideal factors of β and $\bar{\beta}$. Hence we can compute easily the images of the quadratic form $\langle\beta\rangle \in W(K)$ under all residue class homomorphisms. First assume that p splits in K. Let $p\mathcal{O}_K = \mathbf{p}\bar{\mathbf{p}}$ be the prime ideal decomposition of the prime p and let the notation be chosen so that $\mathbf{p} \mid \beta$. Then, by Lemma 6, we have

$$\operatorname{ord}_{\mathbf{p}}\beta = \operatorname{ord}_{\mathbf{p}}\beta\bar{\beta} = \operatorname{ord}_{\mathbf{p}} pa^2 \equiv 1 \pmod 2.$$

Thus $\beta = \pi x^2$, where π is a prime element in $K_{\mathbf{p}}$ and $x \in K_{\mathbf{p}}$. We choose π to be the prime element determining the action of the second residue class homomorphism $\partial_{\mathbf{p}}$. Then we have $\partial_{\mathbf{p}}\langle\beta\rangle = \langle 1\rangle$.

On the other hand, $\operatorname{ord}_{\bar{\mathbf{p}}}\beta = 0$, hence $\partial_{\bar{\mathbf{p}}}\langle\beta\rangle = 0$. Now we compute $\partial_{\mathbf{q}}\langle\beta\rangle$, when $\mathbf{q}$ is any prime ideal in $\mathcal{O}_K$ distinct from the prime factors $\mathbf{p}$ and $\bar{\mathbf{p}}$ of p. Suppose $\mathbf{q}|\beta$. Then, by Lemma 6, we have

$$\operatorname{ord}_{\mathbf{q}}\beta = \operatorname{ord}_{\mathbf{q}}\beta\bar{\beta} = \operatorname{ord}_{\mathbf{q}} pa^2 = \operatorname{ord}_{\mathbf{q}} a^2 \equiv 0 \pmod 2.$$

Clearly, if $\mathbf{q}$ does not divide β, then we also have $\operatorname{ord}_{\mathbf{q}}\beta \equiv 0 \pmod 2$. Thus we have $\partial_{\mathbf{q}}\langle\beta\rangle = 0$ for all $\mathbf{q} \neq \mathbf{p}$. Hence $\partial\langle\beta\rangle = (\partial_{\mathbf{q}}\langle\beta\rangle) = \eta^{\mathbf{p}}$. It remains to consider the ramified primes. Let $p\mathcal{O}_K = \mathbf{q}^2$ be the prime ideal decomposition of the prime p. Then, by Lemma 6, we have

$$\operatorname{ord}_{\mathbf{q}}\beta = \operatorname{ord}_{\mathbf{q}}\bar{\beta} = 1.$$

Thus β is a prime element in $K_{\mathbf{q}}$ and so it determines the action of the second residue class homomorphism $\partial_{\mathbf{q}}$. With this choice of the prime element we have $\partial_{\mathbf{q}}\langle\beta\rangle = \langle 1\rangle$. Now we compute $\partial_{\mathbf{p}}\langle\beta\rangle$, when $\mathbf{p}$ is any prime ideal in $\mathcal{O}_K$ distinct from the prime factor $\mathbf{q}$ of p. Suppose $\mathbf{p}|\beta$. Then, by Lemma 6, we have

$$\operatorname{ord}_{\mathbf{p}} \beta = \operatorname{ord}_{\mathbf{p}} \beta\bar{\beta} = \operatorname{ord}_{\mathbf{p}} pa^2 = \operatorname{ord}_{\mathbf{p}} a^2 \equiv 0 \pmod 2.$$

Clearly, if $\mathbf{p}$ does not divide β, then we also have $\operatorname{ord}_{\mathbf{p}} \beta \equiv 0 \pmod 2$. Thus we have $\partial_{\mathbf{p}}\langle\beta\rangle = 0$ for all $\mathbf{p} \neq \mathbf{q}$. Hence $\partial\langle\beta\rangle = (\partial_{\mathbf{p}}\langle\beta\rangle) = \eta^{\mathbf{q}}$.

This proves that the boundary homomorphism ∂ is surjective. □

References

[1] Conner, P. E., Hurrelbrink, J., *Class number parity*, World Scientific Publishing Co., Singapore, 1988.

[2] Conner, P. E., Perlis, R., Szymiczek, K., *Wild sets and 2-ranks of class groups*, Acta Arith., to appear.

[3] Hecke, E., *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlagsgesellschaft, Leipzig, 1923.

[4] Jakubec, S., Marko, F., Szymiczek, K., *Parity of class numbers and Witt equivalence of quartic fields*, Math. Comput. **64** (1995), 1711–11715. Corrigendum, ibid. (to appear).

[5] Milnor, J., Husemoller, D., *Symmetric Bilinear Forms*, Springer–Verlag, Berlin–Heidelberg–New York, 1973.

[6] Scharlau, W., *Quadratic and Hermitian Forms*, Springer–Verlag, Berlin–Heidelberg–New York, 1985.

[7] Szymiczek, K., *Witt equivalence of global fields*, Commun. Alg. **19** (1991), 1125–1149.

Address: Instytut Matematyki, Uniwersytet Śląski, Bankowa 14,
40 007 Katowice, Poland, e-mail: szymiczekgate.math.us.edu.pl

Talk at the First Czech–Polish Conference on Number Theory, University of Ostrava, Ostrava, Czech Republic, May 30, 1996.