ACTA ARITHMETICA
LVIII.1 (1991)

On reciprocity equivalence of quadratic number fields

by

ALFRED CZOGAŁA (Katowice)

1. Introduction. Reciprocity equivalence of algebraic number fields has been introduced by Perlis and Szymiczek in [7] as a sufficient condition for the fields to be Witt equivalent.

Two algebraic number fields K and L are said to be *reciprocity equivalent* if there is a pair of maps (φ, Φ), where

$$\varphi\colon K^{\cdot}/K^{\cdot 2} \to L^{\cdot}/L^{\cdot 2}$$

is a group isomorphism and

$$\Phi\colon \Omega(K) \to \Omega(L)$$

is a bijection of the set of all primes of K (including infinite primes) onto the set of all primes of L and

$$(a,b)_P = (\varphi a, \varphi b)_{\Phi P}$$

for all $a, b \in K^{\cdot}/K^{\cdot 2}$ and $P \in \Omega(K)$.

Thus φ is a Hilbert symbol preserving isomorphism of groups of square classes of K and L.

The equivalence (φ, Φ) is said to be *tame* if

$$\operatorname{ord}_P a \equiv \operatorname{ord}_{\Phi P} \varphi a \pmod 2$$

for every finite prime P and every $a \in K^{\cdot}/K^{\cdot 2}$.

We quote, from [7], the following results.

If K and L are reciprocity equivalent, then K and L are Witt equivalent, i.e., the Witt rings $W(K)$ and $W(L)$ are isomorphic. Moreover, if there is a tame reciprocity equivalence between K and L, then Witt groups $W(O_K)$ and $W(O_L)$ are isomorphic, where O_K and O_L are rings of integers in K and L, and also the groups of ideal square classes $C(K)/C(K)^2$ and $C(L)/C(L)^2$ are isomorphic (here $C(K)$ is the ideal class group of K).

In this paper we obtain a complete classification of quadratic number fields with respect to tame reciprocity equivalence and also with respect to reciprocity equivalence.

For a number field K, we write $g(K)$ for the *number of dyadic primes* in K, $r(K)$ for the *number of real embeddings* of K, $N(K)$ for the *norm group* of the extension K/Q, $t(K)$ for the *number of distinct prime divisors of the discriminant* of K, and K_P for the *completion* of K at the prime P. If P is a finite prime of K and $x \in K^{\cdot}$, we say that x is *P-odd* iff $\operatorname{ord}_P x \equiv 1 \pmod 2$ and $\operatorname{ord}_R x \equiv 0 \pmod 2$ for every finite prime $R \neq P$ (i.e., x is P-odd iff the principal ideal (x) satisfies $(x) = P \cdot I^2$ for some fractional ideal I of K). If P is a finite prime of a number field K, then we write u_P for the *unique square class in K_P with the property that the extension $K_P(\sqrt{u_P})/K_P$ is quadratic unramified.*

The following two theorems are the main results of the paper.

THEOREM 1. *Let K and L be quadratic number fields and let P, Q be arbitrarily chosen dyadic prime ideals in K and L, respectively. K and L are tamely reciprocity equivalent if and only if the following eleven conditions are satisfied:*

(0) $-1 \in K^{\cdot 2} \Leftrightarrow -1 \in L^{\cdot 2}$.

(I) $r(K) = r(L)$.

(II) $g(K) = g(L)$.

(III) $-1 \in K_P^{\cdot 2} \Leftrightarrow -1 \in L_Q^{\cdot 2}$.

(IV) $t(K) = t(L)$.

(V) $-1 \in N(K) \Leftrightarrow -1 \in N(L)$.

(VI) *2 is prime in K or $2 \in |N(K)| \Leftrightarrow$ 2 is prime in L or $2 \in |N(L)|$.*

(VII) *If $-1 \notin N(K)$, then $-2 \in N(K) \Leftrightarrow -2 \in N(L)$.*

(VIII) *The extension $K_P(\sqrt{-1})/K_P$ is unramified $\Leftrightarrow$ $L_Q(\sqrt{-1})/L_Q$ is unramified (i.e., $u_P = -1 \Leftrightarrow u_Q = -1$).*

(IX) *If $g(K) = 2$ and $2 \in N(K)$, then $(2, x)_P = (2, y)_Q$, where x is P-odd and y is Q-odd.*

(X) *If $g(K) = 2$, $-1 \in N(K)$ and $2 \in N(K)$, then $(2, x)_P = (2, y)_Q$ and $(-1, x)_P = (-1, y)_Q$, where x, y are totally positive and x is P-odd, y is Q-odd.*

Moreover, the Hilbert symbols in (IX) *and* (X) *are independent of the choice of P and Q and of x and y.*

THEOREM 2. *Let K, L and also P, Q be as above. K and L are reciprocity equivalent if and only if the conditions* (0), (I), (II), (III) *are satisfied.*

The conditions (0), (I), ..., (VIII) can be checked for two quadratic fields K and L without any essential difficulties. In fact the arithmetic properties in those conditions can be easily rephrased in terms of discriminants of the fields in question. Thus it suffices to notice that for $K = \boldsymbol{Q}(\sqrt{d})$, where d is a square free integer $\neq 1$ and for P a dyadic prime in K, we have:

(1.1) $$-1 \in K^{\cdot 2} \Leftrightarrow d = -1.$$

(1.2) $$r(K) = 0 \text{ when } d < 0 \quad \text{and} \quad r(K) = 2 \text{ when } d > 0.$$

(1.3) $$g(K) = 2 \text{ when } d \equiv 1 \pmod 8 \quad \text{and} \quad g(K) = 1 \text{ otherwise.}$$

(1.4) $$-1 \in K_P^{\cdot 2} \Leftrightarrow d \equiv 7 \pmod 8.$$

(1.5) $$-1 \in N(K) \Leftrightarrow d > 0 \quad \text{and} \quad p \equiv 1, 2 \pmod 4 \text{ for every } p \mid d.$$

(1.6) $$2 \text{ is prime in } K \Leftrightarrow d \equiv 5 \pmod 8.$$

(1.7) $$2 \in N(K) \Leftrightarrow p \equiv 1, 2, 7 \pmod 8 \text{ for every prime } p \mid d.$$

(1.8) $$-2 \in N(K) \Leftrightarrow d > 0 \text{ and } p \equiv 1, 2, 3 \pmod 8 \text{ for every } p \mid d.$$

(1.9) $$u_P = -1 \Leftrightarrow d \equiv 3 \pmod 8.$$

However, checking (IX) and (X), whenever the conditions occur, requires first determining some appropriate elements x and y.

Theorem 2 implies that *there are exactly 7 classes of reciprocity equivalent quadratic number fields, represented by the fields $\boldsymbol{Q}(\sqrt{d})$, where $d = -1, \pm 2, \pm 7, \pm 17$.* As to Witt equivalence, Szymiczek proved in [8] that Witt equivalence and reciprocity equivalence of number fields actually coincide. Thus *there are exactly seven distinct Witt rings for the class of all quadratic number fields.*

On the other hand, *there are infinitely many classes of tamely reciprocity equivalent quadratic number fields*, since fields with distinct numbers of prime factors of discriminants are not tamely reciprocity equivalent. However, if we fix the number of prime factors of the discriminant, then there are at most 22 classes of tamely reciprocity equivalent quadratic fields with the given number of prime factors of the discriminant. For example, the following fields represent all the classes of tamely reciprocity equivalent quadratic number fields with exactly one prime factor of the discriminant: $\boldsymbol{Q}(\sqrt{d})$ where $d = -1, -2, -31, -7, 2, 17, 41, 73, 113$.

We prove Theorem 1 in Section 3. The proof is based on a necessary and sufficient condition for two number fields to be tamely reciprocity equivalent (Theorem 2.1 in Section 2).

Theorem 2 is proved in Section 4. We deduce the classification of quadratic number fields with respect to reciprocity equivalence from the more subtle classification result in Theorem 1.

These results were first found in the author's dissertation [3].

Reciprocity equivalence of number fields has been investigated lately in the dissertation [2] of J. Carpenter. As an application of her results, she found another proof of our Theorem 2.

2. Finiteness condition for tame reciprocity equivalence. A reciprocity equivalence (φ, Φ) between two number fields K and L is a pair of maps each defined on an infinite set. It has been shown in [7] how to produce a reciprocity equivalence starting from a finite set of data called "small equivalence".

According to [7], we say that a finite set S of primes of K is *sufficiently large* when S contains all infinite and dyadic primes, and when the class

number of the ring of *S-integers*

$$O_S = \{x \in K\colon \operatorname{ord}_P x \geqslant 0 \text{ for every } P \in \Omega(K)\backslash S\}$$

is odd. Let U_S be the group of *S-units* of K. Thus

$$U_S = \{x \in K\colon \operatorname{ord}_P x = 0 \text{ for every } P \in \Omega(K)\backslash S\}.$$

Dirichlet's Unit Theorem implies that the order of the unit square class group U_S/U_S^2 equals 2^s, where $s = \operatorname{card} S$. The group U_S/U_S^2 will be identified with its image under the natural embedding $U_S/U_S^2 \to K^\cdot/K^{\cdot 2}$. Thus $aK^{\cdot 2}$ lies in U_S/U_S^2 iff $\operatorname{ord}_P a \equiv 0 \pmod 2$ for every finite $P \in \Omega(K)\backslash S$.

An *S-equivalence* (or, a *small equivalence*) is a finite family of maps: Φ, φ_S, φ_P ($P \in S$), where

1. Φ maps bijectively S onto sufficiently large set ΦS of primes of L;
2. $\varphi_S\colon U_S/U_S^2 \to U_{\Phi S}/U_{\Phi S}^2$ is a group isomorphism;
3. $\varphi_P\colon K_P^\cdot/K_P^{\cdot 2} \to L_{\Phi P}^\cdot/L_{\Phi P}^{\cdot 2}$ is a group isomorphism, for each $P \in S$ and each φ_P preserves Hilbert symbols;
4. the maps combine into a commutative diagram:

$$(*) \qquad \begin{array}{ccc} U_S/U_S^2 & \longrightarrow & \prod\limits_{P\in S} K_P^\cdot/K_P^{\cdot 2} \\ \downarrow\varphi_S & & \downarrow\varphi_P \\ U_{\Phi S}/U_{\Phi S}^2 & \longrightarrow & \prod\limits_{P\in S} L_{\Phi P}^\cdot/L_{\Phi P}^{\cdot 2} \end{array}$$

An S-equivalence is said to be *tame* if φ_P is tame for every $P \in S$ (i.e., $\operatorname{ord}_P a \equiv \operatorname{ord}_{\Phi P}\varphi_P a \pmod 2$ for every $a \in K_P^\cdot$).

The main result in [7] asserts that *every S-equivalence of two number fields K and L can be extended to a reciprocity equivalence of K and L that is tame outside S. Thus there is a tame reciprocity equivalence between K and L iff there is a tame small equivalence between K and L.*

The following theorem is similar in nature to the above result.

Let $\Omega_0(K)$ be the *set of all infinite and of all dyadic primes* of K and let

$$K_0 = \{x \in K^\cdot\colon \operatorname{ord}_P x \equiv 0 \pmod 2 \text{ for every } P \in \Omega(K)\backslash\Omega_0(K)\}.$$

Clearly, K_0 is a subgroup of $K^\cdot$ and $K_0 \supseteq K^{\cdot 2}$.

In the theorem below and throughout the paper we use the same symbol for $x \in K^\cdot$ and for its canonical image in $K^\cdot/K^{\cdot 2}$. We will do the same with cosets of $K^\cdot$ modulo some other subgroups of $K^\cdot$.

THEOREM 2.1. *Two number fields K and L are tamely reciprocity equivalent if and only if there is a bijective map $\Phi\colon \Omega_0(K) \to \Omega_0(L)$ and a group isomorphism $\varphi\colon K_0/K^{\cdot 2} \to L_0/L^{\cdot 2}$ satisfying the following conditions:*

(1) *P is infinite real $\Leftrightarrow$ ΦP is infinite real.*

(2) *P is dyadic $\Leftrightarrow$ ΦP is dyadic; moreover $[K_P\colon \boldsymbol{Q}_2] = [L_{\Phi P}\colon \boldsymbol{Q}_2]$.*

(3) $\varphi(-1) = -1$.

(4) *x is positive at $P \Leftrightarrow \varphi x$ is positive at ΦP, for all $x \in K^\cdot$ and all infinite real primes P.*

(5) *For every dyadic prime P of K, φ induces a tame group isomorphism $\varphi_P\colon K_0K_P^{\cdot 2}/K_P^{\cdot 2} \to L_0L_{\Phi P}^{\cdot 2}/L_{\Phi P}^{\cdot 2}$ which preserves Hilbert symbols, and moreover $\varphi_P(u_P) = u_{\Phi P}$.*

We begin with the proof of the necessity part of Theorem 2.1.

For a number field K let K_+ denote the set of *totally positive* elements of K and let

$$K_{ev} = \{x \in K^\cdot\colon \operatorname{ord}_P x \equiv 0 \pmod 2 \text{ for every finite prime } P \text{ of } K\},$$

$$K_{sq} = \{x \in K_0\colon x \in K_P^{\cdot 2} \text{ for every prime } P \in \Omega_0(K)\}.$$

Each K_+, K_{ev}, K_{sq} is a subgroup of $K^\cdot$ and

$$K^{\cdot 2} \subseteq K_{sq} \subseteq K_+ \cap K_{ev} \subseteq K_{ev} \subseteq K_0.$$

PROPOSITION 2.2. *Let (φ, Φ) be a tame reciprocity equivalence between K and L.*

(a) *The map φ induces the following group isomorphisms:*
(i) $K_0/K^{\cdot 2} \simeq L_0/L^{\cdot 2}$,
(ii) $K_{sq}/K^{\cdot 2} \simeq L_{sq}/L^{\cdot 2}$,
(iii) $K_{ev} \cap K_+/K^{\cdot 2} \simeq L_{ev} \cap L_+/L^{\cdot 2}$,
(iv) $K_{ev}/K^{\cdot 2} \simeq L_{ev}/L^{\cdot 2}$.

(b) *The map Φ induces group isomorphism $C(K)/C(K)^2 \simeq C(L)/C(L)^2$.*

Proof. This follows easily from the tameness of φ.

LEMMA 2.3. *Let P and Q be finite primes in K and L, respectively, and let $\varphi_P\colon K_P^\cdot/K_P^{\cdot 2} \to L_Q^\cdot/L_Q^{\cdot 2}$ be a Hilbert symbol preserving group isomorphism. Then φ_P is tame if and only if $\varphi_P(u_P) = u_Q$.*

Proof. This follows from the fact that u_P is the unique square class in K_P with the property that $(u_P, x)_P = (-1)^{\operatorname{ord}_P x}$ for every $x \in K_P^\cdot$.

Proof of Theorem 2.1 (necessity). Let (φ, Φ) be a tame reciprocity equivalence between K and L. Then (φ, Φ) is a reciprocity equivalence and (1)–(4) are satisfied according to [7]. Further, restricting Φ to $\Omega_0(K)$ and φ to $K_0/K^{\cdot 2}$ and using Proposition 2.2 and Lemma 2.3, we get (5). This finishes the proof of the necessity part of Theorem 2.1.

For the proof of the sufficiency part of Theorem 2.1 we need several auxiliary results. First some notation.

For an ideal I in K we write $[I]$ for the *ideal class* of I in the ideal class group $C(K)$. We write $t' = t'(K)$ for the *2-rank of* $C(K)$; thus $t'(K) = \dim_{\boldsymbol{F}_2} C(K)/C(K)^2$. Further, $\delta = \delta(K)$ will denote the *dimension over $\boldsymbol{F}_2$ of the subspace of $C(K)/C(K)^2$ generated by the set $\{[P]\cdot C(K)^2\colon P \text{ dyadic}\}$.*

Finally, $c = c(K)$ is the *number of infinite complex primes* of K.

LEMMA 2.4. (a) $\dim_{F_2} K_{ev}/K^{\cdot 2} = r+c+t'$.
(b) $\dim_{F_2} K_0/K_{ev} = g-\delta$.

Proof. (a) Let $C_2(K)$ be the subgroup of $C(K)$ consisting of elements of order $\leqslant 2$ and let $U = U(K)$ be the group of units of K. The map $K_{ev} \to C_2(K)$, $x \mapsto [I]$, where $(x) = I^2$, is a surjective homomorphism with kernel $U \cdot K^{\cdot 2}$. Hence $K_{ev}/UK^{\cdot 2} \simeq C_2(K)$. Since $UK^{\cdot 2}/K^{\cdot 2} \simeq U/U^2$ we get

$$|K_{ev}/K^{\cdot 2}| = |U/U^2| \cdot |C_2(K)|.$$

Now $|U/U^2| = 2^{r+c}$ by Dirichlet's Unit Theorem, and the result follows.

(b) Assume $\delta < g$ and let $P_1, \ldots, P_\delta, P_{\delta+1}, \ldots, P_g$ be the dyadic primes of K, where $[P_1], \ldots, [P_\delta]$ are linearly independent in $C(K)/C(K)^2$. Then the map $K_0 \to F_2^{g-\delta}$, $a \mapsto (\mathrm{ord}_{P_{\delta+1}} a \pmod 2, \ldots, \mathrm{ord}_{P_g} a \pmod 2)$ is a surjective group homomorphism with kernel K_{ev}. Thus $K_0/K_{ev} \simeq F_2^{g-\delta}$ and (b) follows.

COROLLARY 2.5. $\dim_{F_2} K_0/K^{\cdot 2} = r+c+t'+g-\delta$.

LEMMA 2.6. *Suppose $b_1, \ldots, b_n \in K_{sq}$ are linearly independent in $K_{sq}/K^{\cdot 2}$ and let $R_1, \ldots, R_n$ be non-dyadic prime ideals in K satisfying:*

$$\left(\frac{b_i}{R_i}\right) = -1, \quad \left(\frac{b_j}{R_i}\right) = 1 \quad \text{for all } i, j \in \{1, \ldots, n\},\ i \neq j.$$

Then the ideal classes $[R_1], \ldots, [R_n]$ are linearly independent in $C(K)/C(K)^2$. Moreover, if $P_1, \ldots, P_\delta$ are dyadic primes with $[P_1], \ldots, [P_\delta]$ linearly independent in $C(K)/C(K)^2$, then the $\delta+n$ classes $[P_1], \ldots, [P_\delta], [R_1], \ldots, [R_n]$ are linearly independent in $C(K)/C(K)^2$.

Proof. The existence of $R_1, \ldots, R_n$ follows from Satz 169 in [4]. Linear dependence of the ideal classes would imply a relation $(x) = R_1 \cdot \ldots \cdot R_k \cdot I^2$, for some $x \in K^\cdot$ and $k \leqslant n$, after renumbering the ideals if necessary. Then $(b_1, x)_{R_1} = -1$ and $(b_1, x)_P = 1$ for every prime $P \neq R_1$, contradicting Hilbert reciprocity. The same argument proves the independence of the ideal classes of $P_1, \ldots, P_\delta, R_1, \ldots, R_n$.

COROLLARY 2.7. $\dim_{F_2} K_{sq}/K^{\cdot 2} \leqslant t'-\delta$.

LEMMA 2.8. (a) $\dim_{F_2} K_{sq}/K^{\cdot 2} = t'-\delta$.
(b) $\dim_{F_2} K_0/K_{sq} = r+c+g$.

Proof. We view $V_0 = \prod_{P \in \Omega_0(K)} K_P^\cdot/K_P^{\cdot 2}$ as an inner product space over the field F_2 with the inner product defined as the product of Hilbert symbols:

$$B((x_P),(y_P)) = \prod_{P \in \Omega_0(K)} (x_P, y_P)_P, \quad \text{for } (x_P),(y_P) \in \prod K_P^\cdot/K_P^{\cdot 2}.$$

We have $\dim_{F_2} V_0 = 2 \cdot |\Omega_0(K)| = 2(r+c+g)$ (cf. [6], p. 178). Now K_0/K_{sq} with the inner product $\beta(x,y) = \prod_{P \in \Omega_0(K)} (x, y)_P$ for $x, y \in K_0$ can be viewed as a totally isotropic subspace of V_0. Indeed, for any non-dyadic finite prime P, any $x, y \in K_0$ are P-adic units, hence $(x, y)_P = 1$. Thus Hilbert reciprocity implies $\beta(x, y) = 1$. From [5], Lemma 1.2 (p. 57), it follows that

$$\dim_{F_2} K_0/K_{sq} \leqslant \tfrac{1}{2} \dim_{F_2} V_0 = r+c+g.$$

Now Corollaries 2.5 and 2.7 combined with the above inequality prove (a) and (b).

Proof of Theorem 2.1 (sufficiency). Given maps φ and Φ satisfying (1)–(5) we first observe that for any dyadic primes $P_1, \ldots, P_l$ of K, if $(x) = P_1 \cdot \ldots \cdot P_l \cdot I^2$ for some $x \in K^\cdot$ and an ideal I of K, then $(\varphi x) = \Phi P_1 \cdot \ldots \cdot \Phi P_l \cdot J^2$ for some ideal J of L. Thus Φ preserves linear independence of the square classes in $C(K)/C(K)^2$ generated by dyadic primes. It follows that $\delta(K) = \delta(L) = \delta$. Moreover, $\varphi(K_{sq}/K^{\cdot 2}) = L_{sq}/L^{\cdot 2}$, hence $t'(K) = t'(L) = t'$, by Lemma 2.8. Write $n = t'-\delta$ and $m = r+c+g$ (by hypothesis, r, c and g coincide for K and L). Let $\{a_1, \ldots, a_m\}$ be a basis for K_0/K_{sq} and $\{b_1, \ldots, b_n\}$ be a basis for $K_{sq}/K^{\cdot 2}$, where we choose $b_1 = -1$ whenever possible. Then $B_K = \{a_1, \ldots, a_m, b_1, \ldots, b_n\}$ is a basis for $K_0/K^{\cdot 2}$ and also $B_L = \{\varphi a_1, \ldots, \varphi a_m, \varphi b_1, \ldots, \varphi b_n\}$ is a basis for $L_0/L^{\cdot 2}$ such that $\{\varphi a_1, \ldots, \varphi a_m\}$ is a basis for L_0/L_{sq} and $\{\varphi b_1, \ldots, \varphi b_n\}$ is a basis for $L_{sq}/L^{\cdot 2}$, where $b_1 = -1$, whenever $-1 \in L_{sq} \setminus L^{\cdot 2}$.

We pick up non-dyadic prime ideals $R_1, \ldots, R_n$ in K and $T_1, \ldots, T_n$ in L such that

$$\left(\frac{b_i}{R_i}\right) = \left(\frac{\varphi b_i}{T_i}\right) = -1, \quad \left(\frac{x}{R_i}\right) = \left(\frac{\varphi x}{T_i}\right) = 1$$

for each $x \in B_K \setminus \{b_i\}$, $i = 1, 2, \ldots, n$.

If $P_1, \ldots, P_\delta$ are dyadic primes linearly independent in $C(K)/C(K)^2$, then

$$\{[P_1], \ldots, [P_\delta], [R_1], \ldots, [R_n]\} \text{ and } \{[\Phi P_1], \ldots, [\Phi P_\delta], [T_1], \ldots, [T_n]\}$$

form bases for $C(K)/C(K)^2$ and $C(L)/C(L)^2$, respectively (by Lemmas 2.6 and 2.8). The sets of primes

$$S = \Omega_0(K) \cup \{R_1, \ldots, R_n\} \quad \text{and} \quad S' = \Omega_0(L) \cup \{T_1, \ldots, T_n\}$$

are sufficiently large in K and L (in the sense of definition of a small equivalence) and $|S| = |S'| = r+c+t'+g-\delta$. Since $K_0/K^{\cdot 2}$ is a subgroup of U_S/U_S^2, we have $K_0/K^{\cdot 2} = U_S/U_S^2$ by Corollary 2.5, and similarly $L_0/L^{\cdot 2} = U_{S'}/U_{S'}^2$. We extend Φ to a map $\Phi: S \to S'$ by putting $\Phi(R_i) = T_i$, $i = 1, \ldots, n$. Then our choice of R_i, T_i implies that φ induces a tame group isomorphism

$$\varphi_P: K_0 K_P^{\cdot 2}/K_P^{\cdot 2} \to L_0 L_{\Phi P}^{\cdot 2}/L_{\Phi P}^{\cdot 2} \quad \text{for every } P \in \{R_1, \ldots, R_n\}.$$

From Lemma 2.9 below it follows that, for $P\in S$, the group isomorphism φ_P: $K_0K_P^{\cdot 2}/K_P^{\cdot 2} \to L_0L_{\Phi P}^{\cdot 2}/L_{\Phi P}^{\cdot 2}$ can be extended to a tame group isomorphism φ_P: $K_P^{\cdot}/K_P^{\cdot 2} \to L_{\Phi P}^{\cdot}/L_{\Phi P}^{\cdot 2}$ in a Hilbert symbol preserving way. Thus Φ, φ and φ_P, $P\in S$, determine an S-equivalence of K and L. Since this S-equivalence is tame, the main result in [7] guarantees the existence of an extension that is tame reciprocity equivalence between K and L. To complete the proof we must prove Lemma 2.9.

LEMMA 2.9. *Suppose P and Q are primes in K and L, respectively. Assume that $K_P^{\cdot}/K_P^{\cdot 2}$ and $L_Q^{\cdot}/L_Q^{\cdot 2}$ are isometric viewed as inner product spaces over F_2 (with Hilbert symbol as inner product). Let H and H' be subspaces of $K_P^{\cdot}/K_P^{\cdot 2}$ and $L_Q^{\cdot}/L_Q^{\cdot 2}$ and $-1\in H$, $-1\in H'$. Then every isometry f: $H \to H'$ such that $f(-1) = -1$, can be extended to an isometry of $K_P^{\cdot}/K_P^{\cdot 2}$ onto $L_Q^{\cdot}/L_Q^{\cdot 2}$. Moreover, if f is tame and $f(u_P) = u_Q$ (when $u_P\in H$), then there is a extension of f that is a tame group isomorphism.*

Proof. The non-degeneracy of Hilbert symbol implies that for every linearly independent elements $v_1, \ldots, v_k$ of $K_P^{\cdot}/K_P^{\cdot 2}$ and any $(e_i)\in\{1, -1\}^k$, there is an $x\in K_P^{\cdot}$ such that $(v_i, x)_P = e_i$, $i = 1, \ldots, k$.

Let $\{w_1, \ldots, w_k\}$ be a basis for H and $k < \dim_{F_2} K_P^{\cdot}/K_P^{\cdot 2}$. Then there are $x\in K_P^{\cdot}\backslash H$ and $y\in L_Q^{\cdot}\backslash H'$ such that $(w_i, x)_P = (fw_i, y)_Q$ for $i = 1, \ldots, k$. For if H is degenerate, there is $(e_i)\in\{1, -1\}^k$ such that $((w_i, z)_P) \neq (e_i)$ for every $z\in H$. Then also $((fw_i, z')_Q) \neq (e_i)$ for every $z'\in H'$. It suffices to choose $x\in K_P^{\cdot}$ and $y\in L_Q^{\cdot}$ such that $(w_i, x)_P = (fw_i, y)_Q = e_i$, $i = 1, \ldots, k$. If H is non-degenerate and x is an arbitrary element in $K_P^{\cdot}\backslash H$ then the system of equations $(fw_i, z)_Q = (w_i, x)_P$, $i = 1, \ldots, k$ has exactly 2^{n-k} solutions $z\in L_Q^{\cdot}/L_Q^{\cdot 2}$ (where $n = \dim_{F_2} L_Q^{\cdot}/L_Q^{\cdot 2}$) and exactly one of them belongs to H' (since H' is non-degenerate). It suffices to choose y to be a solution of the system not belonging to H'. With our choice of x and y, we have $(v, x)_P = (fv, y)_Q$ for every $v\in H$, in particular $(x, x)_P = (y, y)_Q$ ($-1\in H$ and $-1\in H'$ and $f(-1) = -1$). Putting $fx = y$ we thus extend f onto a $(k+1)$-dimensional subspace containing H.

To prove the second part observe that, if $u_P\in H$ and $u_Q\in H'$, then the result follows from the first part and from Lemma 2.3. If $u_P\notin H$ and $u_Q\notin H'$, then we first extend f to a tame isometry on the space generated by H and u_P and then again the result follows from Lemma 2.3.

We close this section with a sufficient condition for (not necessarily tame) reciprocity equivalence to be used in Section 4.

PROPOSITION 2.10. *Given two number fields K and L, let Φ: $\Omega_0(K) \to \Omega_0(L)$ be a bijective map and φ: $K_0/K_{sq} \to L_0/L_{sq}$ be a group isomorphism. If Φ and φ satisfy the conditions* (1) *through* (5) *of Theorem* 2.1, *then K and L are reciprocity equivalent.*

Proof. Assume $|K_{sq}/K^{\cdot 2}| = 2^n$ and $|L_{sq}/L^{\cdot 2}| = 2^{n+k}$, $k \geqslant 1$. We choose

a basis $B_K = \{a_1, \ldots, a_m, b_1, \ldots, b_n\}$ for $K_0/K^{\cdot 2}$ as in the proof of Theorem 2.1. Then $\{\varphi a_1, \ldots, \varphi a_m\}$ is a basis for L_0/L_{sq} and we adjoin appropriate elements $d_1, \ldots, d_{n+k}$ from L_{sq} to obtain a basis B_L for $L_0/L^{\cdot 2}$. We agree to take $d_1 = -1$ whenever $-1\in L_{sq}\backslash L^{\cdot 2}$. We choose non-dyadic primes $R_1, \ldots, R_n$ and dyadic primes $P_1, \ldots, P_\delta$ as in the proof of Theorem 2.1. Moreover, let $T_1, \ldots, T_{n+k}$ be non-dyadic prime ideals in L satisfying

$$\left(\frac{d_i}{T_i}\right) = -1, \quad \left(\frac{y}{T_i}\right) = 1 \quad \text{for every } y\in B_L\backslash\{d_i\},$$

$i = 1, \ldots, n+k$. According to Lemma 2.11 below there are pairwise distinct non-dyadic prime ideals $R_{n+1}, \ldots, R_{n+k}$ in K and $x_1, \ldots, x_k\in K^{\cdot}$ such that for every $i\in\{1, \ldots, k\}$ we have

1. $x_i = 1$ in $K_P^{\cdot}/K_P^{\cdot 2}$, for every $P\in\Omega_0(K)\cup\{R_1, \ldots, R_{n+k}\}$, $P \neq R_{n+i}$,

2. $\operatorname{ord}_{R_{n+i}} x_i = 1$ and $\operatorname{ord}_P x_i = 0$ for every P outside $\Omega_0(K) \cup\{R_1, \ldots, R_{n+k}\}$.

Hilbert reciprocity then implies that $(x, x_i)_P = 1$ for every $P\in\Omega(K)\backslash\{R_{n+i}\}$ and $x\in B_K$. In particular,

$$\left(\frac{-1}{R_{n+i}}\right) = 1 \quad \text{for every } i\in\{1, \ldots, k\}.$$

Thus we have

$$\left(\frac{-1}{R_i}\right) = \left(\frac{-1}{T_i}\right) \quad \text{for } i = 1, \ldots, n+k.$$

Similarly to the proof of Theorem 2.1 we show that the sets of primes $S = \Omega_0(K)\cup\{R_1, \ldots, R_{n+k}\}$ and $S' = \Omega_0(L)\cup\{T_1, \ldots, T_{n+k}\}$ are sufficiently large and $B_K\cup\{x_1, \ldots, x_k\}$ and B_L form bases for U_S/U_S^2 and $U_{S'}/U_{S'}^2$, respectively. We extend Φ onto S by putting $\Phi(R_i) = T_i$ ($i = 1, \ldots, k$) and we also extend φ onto U_S/U_S^2 by putting $\varphi(b_i) = d_i$ ($i = 1, \ldots, n$) and $\varphi(x_i) = d_{n+i}$ for $i = 1, \ldots, k$. Thus we get an S-equivalence and applying [7] we extend this small equivalence to a reciprocity equivalence between K and L.

LEMMA 2.11. *Let S be a finite set of primes of the number field K and let $v_P\in K_P^{\cdot}$ be given for each $P\in S$. Then there are infinitely many primes Q with the property that there is an $x\in K^{\cdot}$ satisfying*

1. $x = v_P$ *in* $K_P^{\cdot}/K_P^{\cdot 2}$, *for every* $P\in S$;

2. $\operatorname{ord}_Q x = 1$ *and* $\operatorname{ord}_P x = 0$ *for every prime* P *outside* $S\cup\{Q\}$.

This lemma is used and proved in the proof of Theorem 1 in [7].

3. Tame equivalence of quadratic number fields. In this section we prove Theorem 1. Thus from now on our number fields will be quadratic extensions

of the rationals. From Theorem 2.1 it follows that the field $Q(\sqrt{-1})$ constitutes a singleton class of reciprocity equivalence. Thus in this and next section we assume that K and L are quadratic number fields distinct from $Q(\sqrt{-1})$.

Assume that $K = Q(\sqrt{d})$, where d is a square-free integer, and let $p_1, \ldots, p_t$ be all pairwise distinct prime divisors of the discriminant of K. We agree that $p_1 = 2$ whenever $d \equiv 3 \pmod 4$. It is easy to see that the sets

$$\{-1, p_1, \ldots, p_{t-1}\}, \quad \text{when } d < 0,$$

$$\{p_1, \ldots, p_{t-1}\}, \quad \text{when } d > 0$$

are linearly independent in the group $K_{ev} \cap K_+/K^{\cdot 2}$. Since $K_{ev} \cap K_+/K^{\cdot 2}$ is a group of order 2^{c+t-1} (cf. [5], p. 99), we conclude that the sets form bases for the group in non-real and real case, respectively.

LEMMA 3.1. *For any fractional ideal I of K with norm $N(I) = 1$ there is a totally positive element q of K and a fractional ideal J of K satisfying $I = (q) \cdot J^2$.*

Proof. See [1], p. 275.

PROPOSITION 3.2. *The dimension of $K_{ev}/K_{ev} \cap K_+$ over $\mathbf{F}_2$ is equal to*

0 *when K is non-real,*
1 *when K is real and $-1 \notin N(K)$,*
2 *when $-1 \in N(K)$.*

Proof. If K is non-real, then $K_{ev} \cap K_+ = K_{ev}$. Assume that K is real. From $(a) = I^2$ it follows that $|N(a)| \in Q^{\cdot 2}$, hence $N(a) \in Q^{\cdot 2} \cup -Q^{\cdot 2}$. Moreover, $N(K_{ev}) \subseteq N(K)$. If $-1 \notin N(K)$, then for each $a \in K_{ev}$ we have either $a \in K_{ev} \cap K_+$ or $-a \in K_{ev} \cap K_+$. Now, assume that $-1 \in N(K)$. There exists an element a_0 in K_{ev} with negative norm. Namely, if $N(x) = -1$, then $(x) = (q) \cdot J^2$ for a fractional ideal J and totally positive element q, then $a_0 = (x/q) \in K_{ev}$ has negative norm. Elements $-1, a_0$ are linearly independent in $K_{ev}/K_{ev} \cap K_+$ and for each $a \in K_{ev}$, there are $m, n \in \{0, 1\}$ such that $(-1)^n a_0^m a \in K_{ev} \cap K_+$. The result follows.

PROPOSITION 3.3. *The norm of an ideal induces an injective homomorphism*

$$C(K)/C(K)^2 \to Q_+/|N(K)|.$$

Proof. Clearly, the map $I \mapsto N(I) \cdot |N(K)|$ is a well defined homomorphism on $C(K)$ and its kernel contains $C(K)^2$. If $N(I) = |N(x)|$ for a fractional ideal I and $x \in K^*$, then $N(I \cdot (x^{-1})) = 1$. Hence $I \cdot (x^{-1}) = (q) \cdot J^2$, according to Lemma 3.1, and so $[I] = [J]^2$.

Proof of Theorem 1 (necessity). As proved in [7], (0)–(III) are consequences of any reciprocity equivalence of K and L. Thus we concentrate on the remaining properties. So assume (φ, Φ) is a tame reciprocity equivalence between K and L, and P, Q are arbitrarily chosen dyadic prime ideals in K and L, respectively.

(V) The map φ induces a group isomorphism $K_{ev}/K_{ev} \cap K_+ \to L_{ev}/L_{ev} \cap L_+$, and condition (V) follows from Proposition 3.2.

(IV) Combine Proposition 2.2 (ii) and the remark preceding Lemma 3.1.

(VI) From Proposition 3.3 it follows that 2 is prime in K or $2 \in |N(K)|$ iff $[P] \in C(K)^2$. Since Φ sends dyadic primes to dyadic primes, (VI) follows by applying Proposition 2.2.

(VII) Suppose $-1 \notin N(K)$ and $-2 \in N(K)$. There is an $x \in K^*$ and a fractional ideal I such that $(x) = P \cdot I^2$, and $N(x) \in -2Q^{\cdot 2}$. Now let $\varphi x = y$. Then y is ΦP-odd, with negative norm. Here ΦP is a dyadic prime, hence 2 is not a prime in L and it follows that the norm of the ideal ΦP is equal to 2. Thus $N(y) \in -2Q^{\cdot 2}$, as desired.

(VIII) If the extension $K_P(\sqrt{-1})/K_P$ is quadratic unramified, then K has exactly one dyadic prime P, say, and also $Q = \Phi P$ is the unique dyadic prime in L. Now (VIII) follows from Lemma 2.3.

(IX) and (X). We choose x and y according to Proposition 3.3 and the additional requirement in (X) that x, say, be in K_+, can be satisfied by replacing x with $\pm ax$, where a is the element in K_{ev} with negative norm. We first show that the Hilbert symbols in question do not depend on the choice of x, y and the choice of dyadic primes P, Q.

So first fix P and take x and x' in K_0 satisfying the hypothesis. Then $xx' \in K_{ev}$ when $-1 \notin N(K)$ and $xx' \in K_{ev} \cap K_+$ when $-1 \in N(K)$. The assumptions in (IX) and (X) imply that for every prime factor p of the discriminant of K we have $p \equiv \pm 1 \pmod 8$ when $-1 \notin N(K)$ and $p \equiv 1 \pmod 8$ when $-1 \in N(K)$. Hence $x = \pm x'$ in K_P^*/K_P^{*2} when $-1 \notin N(K)$ and $x = x'$ in K_P^*/K_P^{*2} when $-1 \in N(K)$. This implies $(2, x)_P = (2, x')_P$ and also $(-1, x)_P = (-1, x')_P$ when $-1 \in N(K)$.

Now suppose x and x' are chosen for dyadic primes P and P', respectively. Here $P' = \bar{P}$ is the conjugate ideal of P and $(x) = P \cdot I^2$ implies $(\bar{x}) = \bar{P} \cdot \bar{I}^2$ (here $\bar{x}$ is the conjugate of x). From the above it follows that without loss of generality we can assume $x' = \bar{x}$. Thus we get $(2, x)_P = (2, \bar{x})_{\bar{P}} = (2, x')_{P'}$ and in the case when $-1 \in N(K)$, $(-1, x)_P = (-1, \bar{x})_{\bar{P}} = (-1, x')_{P'}$.

To prove (IX) and (X) we can assume that $\Phi P = Q$ since, as we have already shown, the Hilbert symbols in question do not depend on the choice of dyadic primes. Suppose $\varphi(x) = y'$ and $\varphi(2) = c$. Then $(y') = Q \cdot J'^2$ and $(c) = Q \cdot \bar{Q} \cdot I'^2$ for certain fractional ideals I', J' in L. Also $(2, x)_P = (c, y')_Q$ and $(-1, x)_P = (-1, y')_Q$. Since $2c \in K_{ev} \cap K_+$, we have $c = \pm 2$ in L_Q^*/L_Q^{*2} and the equality $1 = (-1, 2)_P = (-1, c)_Q$ implies $c = 2$ in L_Q^*/L_Q^{*2}. Thus we get $(2, x)_P = (2, y')_Q$ and $(-1, x)_P = (-1, y')_Q$. Now as proved above, $(2, y)_Q = (2, y')_Q$ and moreover $(-1, y')_Q = (-1, y)_Q$ when $-1 \in N(K)$. This proves (IX) and (X).

Proof of Theorem 1 (sufficiency). We assume that K and L are

quadratic fields distinct from $Q(\sqrt{-1})$ and satisfy (I) through (X). Our task is to define two maps Φ and φ satisfying the hypotheses of Theorem 2.1.

We define Φ to be an arbitrary bijection on the set of infinite real primes of K onto the corresponding set of primes of L (we use (I)) and will define Φ on dyadic primes later on in the proof. We write P_∞ and $P_{\infty'}$ for the two infinite primes of K and Q_∞, $Q_{\infty'}$, for their images in L (when K and L are real fields).

The isomorphism φ: $K_0/K^{\cdot 2} \to L_0/L^{\cdot 2}$ will be defined on a suitably chosen basis of the group $K_0/K^{\cdot 2}$. The basis will be obtained from the following canonical group isomorphism:

$$K_0/K^{\cdot 2} \simeq K_0/K_{ev} \oplus K_{ev}/K_{ev} \cap K_+ \oplus K_{ev} \cap K_+/K_{sq} \oplus K_{sq}/K^{\cdot 2}.$$

The orders of the direct summands have been determined in Lemma 2.4 (b), Prop. 3.2 and Lemma 2.8. The conditions (I) through (VII) imply that the orders of the above direct summands are equal to the orders of the corresponding direct summands in the decomposition

$$L_0/L^{\cdot 2} \simeq L_0/L_{ev} \oplus L_{ev}/L_{ev} \cap L_+ \oplus L_{ev} \cap L_+/L_{sq} \oplus L_{sq}/L^{\cdot 2}.$$

As a first step in the proof, we define φ on $K_{sq}/K^{\cdot 2}$. Let $\{q_1, \ldots, q_n\}$ and $\{q_1', \ldots, q_n'\}$ be bases for $K_{sq}/K^{\cdot 2}$ and $L_{sq}/L^{\cdot 2}$, where $q_1 = -1$ and $q_1' = -1$ whenever $-1 \in K_{sq}$ and $-1 \in L_{sq}$. Then we put $\varphi q_i = q_i'$ for $i = 1, \ldots, n$.

Now the proof splits into two cases depending on the number of dyadic primes in K and L.

Part I. $g(K) = 1$. If P and Q are the unique dyadic primes in K and L, respectively, we put $\Phi P = Q$.

I.1. The group K_0/K_{ev} is non-trivial when $[P] \in C(K)^2$ and then it is generated by a P-odd element x. We can assume that x is totally positive when $-1 \in N(K)$ (since if not, one of $\pm ax$ is totally positive, where $a \in K_{ev}$, $N(a) < 0$). And if K is real and $-1 \notin N(K)$, we may assume that x is positive at P_∞ (if not, $-x$ is). Then x is also positive at $P_{\infty'}$ whenever 2 is a prime in K or $2 \in N(K)$ and x is negative at $P_{\infty'}$ when $-2 \in N(K)$. We choose $y \in L_0$ in a similar way (i.e. y is Q-odd and y is totally positive when $-1 \in N(L)$ and y is positive at Q_∞ when L is real and $-1 \notin N(L)$). Then we put $\varphi x = y$.

I.2. The group $K_{ev} \cap K_+/K_{sq}$ is canonically isomorphic to the group $(K_{ev} \cap K_+)K_P^{\cdot 2}/K_P^{\cdot 2}$ and, as a bilinear space, it is a totally isotropic subspace of the space of dyadic units modulo squares (after all, $(c, d)_P = 1$ for every $c, d \in K_{ev} \cap K_+$).

LEMMA 3.4. *If* $u_P \in (K_{ev} \cap K_+)K_P^{\cdot 2}$, *then* $[P] \notin C(K)^2$.

Proof. Suppose x is P-odd. Then $(x, u_P)_P = -1$ and for any prime $R \neq P$ we have $(x, u_P)_R = 1$ since x is an R-unit modulo squares. This contradicts Hilbert reciprocity.

I.3. Suppose K is non-real. Then $K_{ev} \cap K_+ = K_{ev}$. When $[P] \notin C(K)^2$, the group $K_{ev} \cap K_+/K_{sq}$ has order 4 with a basis $\{v, u\}$, where $u = u_P$ in $K_P^{\cdot}/K_P^{\cdot 2}$.

When $[P] \in C(K)^2$, the group $K_{ev} \cap K_+/K_{sq}$ has order 2 and its generator v is not equal to u_P in $K_P^{\cdot}/K_P^{\cdot 2}$ (Lemma 3.4). In either case we can assume that $v = -1$ whenever $-1 \notin K_P^{\cdot 2}$ and $K_P(\sqrt{-1})/K_P$ is ramified. We pick up a corresponding basis $\{v', u'\}$ or $\{v'\}$ for the other field and then we put $\varphi v = v'$ and $\varphi u = u'$ (when $[P] \notin C(K)^2$). This defines an isomorphism $K_{ev}K_P^{\cdot 2}/K_P^{\cdot 2} \to L_{ev}L_Q^{\cdot 2}/L_Q^{\cdot 2}$.

I.4. Now assume $-1 \in N(K)$. The group $K_{ev}/K_{ev} \cap K_+$ is generated by -1 and a, where $a \in K_{ev}$ and $N(a) < 0$. Choosing between a and $-a$ we can assume that a is positive at P_∞ and negative at $P_{\infty'}$. The group $L_{ev}/L_{ev} \cap L_+$ has a basis $\{-1, -a'\}$ with similar properties relative to Q_∞ and $Q_{\infty'}$. We put $\varphi(-1) = -1$ and $\varphi a = a'$. Hilbert reciprocity implies that $(-1, a)_P = (-1, -a)_P = -1$. Hence $-1, a$ are independent in $K_P^{\cdot}/K_P^{\cdot 2}$ and $u_P \notin -K_P^{\cdot 2} \cup \pm aK_P^{\cdot 2}$. The group $K_{ev} \cap K_+/K_{sq}$ is non-trivial only when $[P] \notin C(K)^2$. Let u be the generator of the group in the non-trivial case. Then $(-1, u)_P = (a, u)_P = 1$, hence $-1, a, u$ are independent in $K_P^{\cdot}/K_P^{\cdot 2}$ and $u = u_P$ in $K_P^{\cdot}/K_P^{\cdot 2}$. Choosing $u' \in L_{ev} \cap L_+$ to be u_Q in $L_Q^{\cdot}/L_Q^{\cdot 2}$, we define $\varphi u = u'$. This defines an induces group isomorphism φ_P: $K_{ev}K_P^{\cdot 2}/K_P^{\cdot 2} \to L_{ev}L_Q^{\cdot 2}/L_Q^{\cdot 2}$.

I.5. Consider now the case when K is real and $-1 \notin N(K)$. Then $K_{ev}/K_{ev} \cap K_+$ is generated by -1 and we set $\varphi(-1) = -1$. As in I.3 the group $K_{ev} \cap K_+/K_{sq}$ has a basis $\{w\}$ when $[P] \in C(K)^2$ and $\{w, u\}$ when $[P] \notin C(K)^2$. Here $w \notin K_P^{\cdot 2}$ and $w \neq u_P$ (in $K_P^{\cdot}/K_P^{\cdot 2}$) in the first case, and $\{w, u\}$ are independent in $K_P^{\cdot}/K_P^{\cdot 2}$ and $u = u_P$ (in $K_P^{\cdot}/K_P^{\cdot 2}$) in the second case.

If $-1 \notin K_P^{\cdot 2}$ and $u_P \neq -1$, then we may assume that $-w = u_P$ in $K_P^{\cdot}/K_P^{\cdot 2}$ when $-2 \in N(K)$, and $-w \in K_P^{\cdot 2}$ otherwise. Indeed, the subspace of U_P/U_P^2 generated by -1 and w is totally isotropic, hence either $-w \in K_P^{\cdot 2}$ or $-w = u_P$ in $K_P^{\cdot}/K_P^{\cdot 2}$. If $[P] \in C(K)^2$ and $-w \notin K_P^{\cdot 2}$, then $-w = u$ in $K_P^{\cdot}/K_P^{\cdot 2}$ and replacing w with wu we have $-w \in K_P^{\cdot}/K_P^{\cdot 2}$. When $[P] \in C(K)^2$ and x is the P-odd element found in I.1, Hilbert reciprocity gives $(-w, x)_P = -1$ when $-2 \in N(K)$, and then $-w = u_P$ in $K_P^{\cdot}/K_P^{\cdot 2}$, and $(-w, x)_P = 1$ in the remaining cases and then $-w \in K_P^{\cdot 2}$.

Similarly, we construct corresponding basis $\{w', u'\}$ or $\{w'\}$ for the group $L_{ev} \cap L_+/L_{sq}$ and we set $\varphi w = w'$ and $\varphi u = u'$.

I.6. In all cases (I.3, I.4 and I.5), it follows that φ is a tame isomorphism on $K_0/K^{\cdot 2}$ and induces an isomorphism

$$\varphi_P\colon\ K_0K_P^{\cdot 2}/K_P^{\cdot 2} \to L_0L_Q^{\cdot 2}/L_Q^{\cdot 2}$$

(here $\varphi_P(x) = y$ when $[P] \in C(K)^2$), and also $\varphi_P(u_P) = u_Q$. Moreover, φ satisfies conditions (3) and (4) from Theorem 2.1. Hence for any infinite real prime R and $c, d \in L_0$ we have $(c, d)_R = (\varphi c, \varphi d)_{\Phi R}$. By Hilbert reciprocity,

$$\prod_{R \in \Omega_0(K)} (c, d)_R = 1 = \prod_{R \in \Omega_0(K)} (\varphi c, \varphi d)_{\Phi R}$$

hence $(c,d)_P = (\varphi c, \varphi d)_Q$ and φ preserves dyadic Hilbert symbols. Thus Theorem 2.1 applies and settles the case when $g(K) = 1$.

Part II. $g(K) = 2$.

II.1. Let P, P' and Q, Q' be the dyadic primes in K and L, respectively. When $-1 \in N(K)$ or $-2 \in N(K)$ we will specify the choice of P and Q later on. Anyway, we intend to put $\Phi P = Q$ and $\Phi P' = Q'$.

II.2. Since $[P] = [P']^{-1}$, we have $|K_0/K_{ev}| = 1$ or 2 depending on whether $2 \notin |N(K)|$ or not. In either case we choose 2 to be a basis element for the group, and the other basis element x will be P-odd. A similar construction of the basis applies to L_0/L_{ev}.

II.3. The group $K_{ev} \cap K_+/K_{sq}$ is generated by the prime divisors of the field discriminant (see the remark preceding Lemma 3.1). Modifying this set of generators if necessary, we will find a convenient basis for the group.

II.4. Assume K is non-real. When $2 \notin N(K)$, there is a prime divisor p of the field discriminant of K such that $p \equiv 3, 5 \pmod 8$. Take $p_1 = \pm p \equiv 5 \pmod 8$; then $\{-1, 2, p_1\}$ is a basis for K_0/K_{sq}. Choosing similarly $\{-1, 2, p_1'\}$, a basis for L_0/L_{sq}, we define φ sending $-1 \mapsto -1$, $2 \mapsto 2$, $p_1 \mapsto p_1'$. When $2 \in N(K)$, then K_0/K_{sq} has basis $\{-1, 2, x\}$, where x is P-odd. Choosing between x and $-x$ we may assume that $x = 2$ or $x = 10$ in $K_P^\cdot/K_P^{\cdot 2}$. The first happens when $(2,x)_P = 1$ and the second when $(2,x)_P = -1$. Since $\bar{x} = 2x \bmod K^{\cdot 2}$ we have $x = 1$ or $x = 5$ in $K_{P'}^\cdot/K_{P'}^{\cdot 2}$, in the two cases, respectively. An analogous choice of $y \in L_0$ is made so that y is Q-odd and $y = 2$ in $L_Q^\cdot/L_Q^{\cdot 2}$, when $(2,y)_Q = 1$ (then $y = 1$ in $L_{Q'}^\cdot/L_{Q'}^{\cdot 2}$) and $y = 10$ in $L_Q^\cdot/L_Q^{\cdot 2}$, when $(2,y)_Q = -1$ (then $y = 5$ in $L_{Q'}^\cdot/L_{Q'}^{\cdot 2}$). Now φ will send $-1, 2, x$ to $-1, 2, y$, respectively.

II.5. Now let $-1 \in N(K)$. Let $a \in K_{ev}$ and $N(a) < 0$. As in I.4 we can assume that a is positive at P_∞ and negative at $P_{\infty'}$. Then $(-1,a)_P = -(-1,a)_{P'}$. We fix P to be the dyadic prime for which $(-1,a)_P = 1$. It follows that $a = 1$ or 5 in $K_P^\cdot/K_P^{\cdot 2}$. A similar choice is made in the field L.

If $2 \notin N(K)$, then there is a prime divisor p of the discriminant of K such that $p \equiv 5 \pmod 8$. Replacing a with pa if necessary, we have $a = 1$ in $K_P^\cdot/K_P^{\cdot 2}$ (then $a = -1$ in $K_{P'}^\cdot/K_{P'}^{\cdot 2}$). The set $\{-1, a, 2, p\}$ is a basis for K_0/K_{sq}. A similar basis $\{-1, a', 2, p'\}$ is found for L_0/L_{sq}, where $p' \equiv 5 \pmod 8$ and $a' = 1$ in $L_Q^\cdot/L_Q^{\cdot 2}$. We define φ to send $-1 \mapsto -1$, $2 \mapsto 2$, $a \mapsto a'$ and $p \mapsto p'$.

If $2 \in N(K)$ and x is P-odd and totally positive, then by Hilbert reciprocity, $(a,x)_P = (a,x)_{P'}$. On the other hand, $\bar{a} = -a \bmod K^{\cdot 2}$ and $\bar{x} = 2x \bmod K^{\cdot 2}$, hence

$$(a,x)_{P'} = (\bar{a},\bar{x})_P = (a,2)_P \cdot (-1,x)_P \cdot (a,x)_P.$$

Thus $(a,2)_P = (-1,x)_P$. It follows that $a = 1$ or 5 in $K_P^\cdot/K_P^{\cdot 2}$ when $(-1,x)_P = 1$ or -1, respectively. And similarly $a' = 1$ or 5 in $L_Q^\cdot/L_Q^{\cdot 2}$ depending on whether

$(-1,y)_Q = 1$ or -1. From $(-1,x)_P = (-1,y)_Q$ and $(2,x)_P = (2,y)_Q$ it follows that x and y can be represented in $K_P^\cdot/K_P^{\cdot 2}$ and $L_Q^\cdot/L_Q^{\cdot 2}$ by the same number l from the set $\{2, -2, 10, -10\}$. Then in $K_{P'}^\cdot/K_{P'}^{\cdot 2}$ and $L_{Q'}^\cdot/L_{Q'}^{\cdot 2}$, x and y are represented by $2l$. Similarly, if a and a' are represented modulo squares in K_P and L_Q by $k \in \{1, 5\}$, then they are represented by $-k$ in $K_{P'}$ and $L_{Q'}$ modulo squares. The groups K_0/K_{sq} and L_0/L_{sq} have bases $\{-1, a, 2, x\}$ and $\{-1, a', 2, y\}$ and φ is defined to send $-1 \mapsto -1$, etc.

II.6. Assume K is real and $-1 \notin N(K)$. When $2 \notin |N(K)|$, there are prime factors p, q of the discriminant of K such that $p \equiv 3, 7 \pmod 8$ and $q \equiv 5 \pmod 8$. We choose $p_1 = p$ or pq, whichever satisfies $p_1 \equiv 7 \pmod 8$, and then $\{-1, 2, p_1, q\}$ is a basis for K_0/K_{sq}. A similar basis is found for L_0/L_{sq} leading to a corresponding group isomorphism.

When $2 \in N(K)$, we find a basis $\{-1, 2, p, x\}$ for K_0/K_{sq}, where p is a prime, $p \equiv 7 \pmod 8$ and x is P-odd and totally positive. Then we can assume that $x = 2$ or 10 in $K_P^\cdot/K_P^{\cdot 2}$ (change x to px if necessary), depending on whether $(2,x)_P = 1$ or -1 (in $K_{P'}^\cdot/K_{P'}^{\cdot 2}$ we have $x = 1$ or 5, resp., since $\bar{x} = 2x \bmod K^{\cdot 2}$). Again, the same construction is possible in L_0/L_{sq} leading to a group isomorphism.

It remains to consider the case when $-2 \in N(K)$. Here there is a prime factor $p \equiv 3 \pmod 8$ of the discriminant of K. Let $x, x' \in K_0$ and let x be P-odd, x' be P'-odd and x, x' be positive at P_∞ and negative at $P_{\infty'}$. Multiplying by p if necessary, we can assume that $x = 1$ or 5 in $K_{P'}^\cdot/K_{P'}^{\cdot 2}$ and $x' = 1$ or 5 in $K_P^\cdot/K_P^{\cdot 2}$. By Hilbert reciprocity, $(x,x')_P = -(x,x')_{P'}$. Of the two dyadic primes we write P for the one satisfying $(x,x')_P = 1$. Then $(x,x')_{P'} = -1$, hence $x = 5$ in $K_{P'}^\cdot/K_{P'}^{\cdot 2}$ and so $x = -10$ in $K_P^\cdot/K_P^{\cdot 2}$ (since $\bar{x} = -2x \bmod K^{\cdot 2}$). Similarly, we can assume $y = 5$ in $L_{Q'}^\cdot/L_{Q'}^{\cdot 2}$ and $y = -10$ in $L_Q^\cdot/L_Q^{\cdot 2}$, where y is Q-odd and positive at Q_∞ and negative at $Q_{\infty'}$. Now φ is defined to map the basis $\{-1, 2, p, x\}$ of K_0/K_{sq} onto a corresponding basis $\{-1, 2, p', y\}$ of L_0/L_{sq}.

II.7. From the very definition of φ it is clear that φ satisfies conditions (3), (4), (5) of Theorem 2.1. Thus applying Theorem 2.1 we conclude that K and L are tamely reciprocity equivalent. This completes the proof of Theorem 1.

4. Reciprocity equivalence of quadratic number fields. Here we prove Theorem 2. It remains to show that the conditions (0)–(III) imply the existence of a reciprocity equivalence between K and L. As in Section 3 we assume that our quadratic fields are distinct from $Q(\sqrt{-1})$.

The strategy of our proof of Theorem 2 is as follows. Suppose K and L (distinct from $Q(\sqrt{-1})$) satisfy (I), (II) and (III). From Section 3 we know that if K and L satisfy additionally (IV), ..., (X), then they are tamely reciprocity equivalent, which is clearly more than we need. Our first step is to show that even if we drop condition (IV) from the above list, then we still can prove that K and L are reciprocity equivalent. And then we will eliminate the

other conditions from the set (V), ..., (X) showing that what remains is sufficient for reciprocity equivalence of K and L. In the end we will be left with (I)–(III) only, and that is what the Theorem asserts. So suppose K and L, distinct from $Q(\sqrt{-1})$, satisfy (I)–(III).

LEMMA 4.1. *If K and L satisfy* (V)–(X) *(in addition to* (I)–(III)*), then K and L are reciprocity equivalent.*

Proof. The conditions (I)–(III) and (V)–(X) allow us to construct a bijection Φ: $\Omega_0(K) \to \Omega_0(L)$ and a group isomorphism φ: $K_0/K_{sq} \to L_0/L_{sq}$ exactly in the same way we did in the proof of Theorem 1. Then we apply Proposition 2.10 to get the result.

We observe that for any quadratic field K there is a quadratic field L such that

(i) K and L satisfy the conditions (I)–(III) and (V)–(X) (so that, in view of Lemma 4.3, K and L are reciprocity equivalent),

(ii) $|L_{sq}/\dot{L}^2| = 2$, when L is non-real and -1 is a local square at a dyadic prime, $L_{sq} = \dot{L}^2$ otherwise.

Indeed, when $g(K) = 1$ or $2 \notin N(K)$, then it is easy to find L by choosing appropriately the prime factors of the discriminant (using (1.1)–(1.9)) to satisfy (i) and (ii). And if $g(K) = 2$ and $2 \in N(K)$ we can take L as follows:

1) $L = Q(\sqrt{-31})$ or $Q(\sqrt{-7})$, when K is non-real depending on whether $(2,x)_P$ equals 1 or -1.

2) $L = Q(\sqrt{161})$ or $Q(\sqrt{217})$, when K is real depending on whether $(2,x)_P$ equals 1 or -1.

3) $L = Q(\sqrt{113})$ or $Q(\sqrt{41})$ or $Q(\sqrt{17})$ or $Q(\sqrt{73})$ when $-1 \in N(K)$ and the pair of Hilbert symbols $((-1,x)_P, (2,x)_P)$ equals $(1,1)$, $(1,-1)$, $(-1,1)$, $(-1,-1)$, respectively.

Thus from now we will assume that K and L satisfy the condition (ii) above.

LEMMA 4.2. *If K and L are non-real and -1 is a local square at a dyadic prime in K, then K and L are reciprocity equivalent.*

Proof. It is sufficient to consider the case $2 \notin N(K)$ and $2 \in N(L)$. Let P and Q be the unique dyadic primes in K and L, resp. As in the proof of Theorem 1 we construct a basis $\{-1, v, u\}$ for $K_0/\dot{K}^2$ and $\{-1, v', y\}$ for $L_0/\dot{L}^2$, where the quadratic extensions $K_P(\sqrt{v})/K_P$ and $L_Q(\sqrt{v'})/L_Q$ are ramified, $K_P(\sqrt{u})/K_P$ is quadratic unramified and y is Q-odd. Choose non-dyadic primes R and T in K and L, resp., to satisfy

$$\left(\frac{-1}{R}\right) = \left(\frac{-1}{T}\right) = -1 \quad \text{and} \quad \left(\frac{a}{R}\right) = \left(\frac{b}{T}\right) = 1$$

for every $a \in \{v, u\}$ and $b \in \{v', y\}$. As in the proof of Theorem 2.1 we conclude

that the sets $S = \Omega_0(K) \cup \{R\}$ and $S' = \Omega_0(L) \cup \{T\}$ are sufficiently large and the bases considered are, in fact, bases for the groups of S-units and S'-units, respectively, modulo squares. And again as in the proof of Theorem 2.1 we check that putting $\Phi P = Q$, $\Phi R = T$ and $\varphi(-1) = -1$, $\varphi(v) = v'$, $\varphi(u) = y$ defines an S-equivalence between K and L. Thus, by [7], K and L are reciprocity equivalent.

Continuing the proof of Theorem 2 we will assume that K and L are real fields or -1 is not a dyadic square in K and L. Then the sets $S = \Omega_0(K)$ and $S' = \Omega_0(L)$ are sufficiently large in K and L, resp., and the groups of S-units and S'-units modulo squares are $K_0/\dot{K}^2$ and $L_0/\dot{L}^2$, respectively. Put $V_S = \prod_{R \in S} \dot{K}_R/\dot{K}_R^2$. Then V_S can be viewed as inner product space of dimension $2s$ (where $s = |\Omega_0(K)|$) with the bilinear form β_S defined by $\beta_S(x,y) = \prod_{R \in S}(x,y)_R$. And similarly for $V_{S'} = \prod_{R \in S} \dot{L}_{\Phi R}/\dot{L}_{\Phi R}^2$ we define $\beta_{S'}(x,y) = \prod_{R \in S}(x,y)_{\Phi R}$. We will identify U_S/U_S^2 (and $U_{S'}/U_{S'}^2$) with its image in V_S (in $V_{S'}$) under the natural embedding.

The local isomorphisms φ_{P_∞} and $\varphi_{P_\infty'}$ are defined naturally. When $g(K) = 2$, we require that the isomorphisms φ_P and $\varphi_{P'}$ send $-1, 2, 5$ to $-1, 2, 5$, respectively, where P and P' are the dyadic primes in K. When $g(K) = 1$, Lemma 2.9 implies that there is an isomorphism φ_P: $\dot{K}_P/\dot{K}_P^2 \to \dot{L}_Q/\dot{L}_Q^2$ with $\varphi(-1) = -1$ and moreover, φ_P preserves Hilbert symbols (where P, Q are dyadic primes in K and L).

The bijection Φ is chosen arbitrarily (on $\Omega_0(K)$) subject only to the requirement that infinite real primes go to infinite real primes and dyadic primes go to dyadic primes.

Put $F = \prod_{R \in S} \varphi_R$. Enlarging the set S if necessary (by adjoining at most two more primes) we will define an isomorphism φ_S making the diagram (*) in Section 2 commutative (i.e., $\varphi_S x = Fx$ for every $x \in U_S$).

Consider first the case where K and L are real fields. As in the proof of Theorem 1, we show that there is a basis B_K for the group U_S/U_S^2 $(= K_0/\dot{K}^2)$, where $B_K = \{-1, v, w\}$ or $\{-1, 2, v, w\}$ depending on whether $g(K) = 1$ or 2, where $v, w \in K_0$.

(a) If $Fv = v'$ and $Fw = w'$ for some $v', w' \in U_{S'}$, then we define φ_S on B_K by sending $-1, v, w$ to $-1, v', w'$, respectively, and moreover, 2 to 2, if $g_2(K) = 2$. Thus we get an S-equivalence for K and L.

(b) If $Fv = v' \in U_{S'}/U_{S'}^2$ and $Fw \notin U_{S'}/U_{S'}^2$ we find a $w' \in U_{S'}$, which adjoined to $\{-1, v'\}$ (or to $\{-1, 2, v'\}$ when $g(K) = 2$) makes the set into a basis B_L for the group $U_{S'}/U_{S'}^2$. Then

$$\beta_{S'}(Fw, w') = -1.$$

Indeed, Hilbert reciprocity gives $\beta_S(x, w) = 1$ for $x \in \{-1, v\}$ and for $x = 2$ when $g(K) = 2$. Thus for every $x' \in \{-1, v'\}$ and for $x' = 2$ when $g(K) = 2$, we have $\beta_{S'}(x', Fw) = 1$. Again from Hilbert reciprocity we have $\beta_{S'}(y', z') = 1$ for $y', z' \in U_{S'}$. Hence $\beta_{S'}(Fw, w') = 1$ would imply that $U_{S'} \cup \{Fw\}$ spans an

$s+1$-dimensional totally isotropic subspace in $2s$-dimensional non-degenerate space $V_{S'}$, a contradiction.

Let $Fw = (w_{\Phi R})_{R\in S}$ and $F^{-1}w' = (w'_R)_{R\in S}$. By Lemma 2.11, there are non-dyadic primes P_1, Q_1 in K and L, resp., and $x_1 \in K^\cdot$, $y_1 \in L^\cdot$ such that

$$x_1 = w'_R \text{ in } K^\cdot_R/K^{\cdot 2}_R, \quad y_1 = w_{\Phi R} \text{ in } L^\cdot_{\Phi R}/L^{\cdot 2}_{\Phi R} \quad \text{for } R\in S,$$

$$x_1 \in U_{S_1}, \quad y_1 \in U_{S'_1} \quad \text{and} \quad \operatorname{ord}_{P_1} x_1 = \operatorname{ord}_{Q_1} y_1 = 1,$$

where $S_1 = S\cup\{P_1\}$, $S'_1 = S'\cup\{Q_1\}$.

The sets $B'_K = B_K\cup\{x_1\}$ and $B'_L = B_L\cup\{y_1\}$ form bases for $U_{S_1}/U^2_{S_1}$ and $U_{S'_1}/U^2_{S'_1}$, respectively. We extend Φ by putting $\Phi P_1 = Q_1$ and we define φ_{S_1} on B'_K by sending $-1, v, w, x_1$ to $-1, v', y_1, w'$, respectively, and 2 to 2 when $g(K) = 2$. Then we have

$$(w, x_1)_{P_1} = \beta_S(w, F^{-1}w') = \beta_{S'}(Fw, w') = -1,$$

$$(w', y_1)_{Q_1} = \beta_{S'}(Fw, w') = -1.$$

Moreover, for $x\in\{-1, v\}$, and $x = 2$ when $g(K) = 2$, we have $Fx\in U_{S'}/U^2_{S'}$ and so

$$(x, x_1)_{P_1} = \beta_S(x, F^{-1}w') = \beta_{S'}(Fx, w') = 1.$$

Analogously, for $x'\in\{-1, v'\}$, and $x' = 2$ when $g(K) = 2$ we have

$$(x', y_1)_{Q_1} = \beta_{S'}(x', Fw) = \beta_S(F^{-1}x', w) = 1.$$

Hence φ_{S_1} induces an isomorphism $\varphi_{P_1}\colon K^\cdot_{P_1}/K^{\cdot 2}_{P_1} \to L^\cdot_{Q_1}/L^{\cdot 2}_{Q_1}$ which preserves Hilbert symbols. Thus we get an S_1-equivalence of K and L, as required.

(c) Now assume that $Fv\notin U_{S'}/U^2_{S'}$ and $Fw\notin U_{S'}/U^2_{S'}$. Then there are v', $w'\in U_{S'}$ such that

$$\beta_{S'}(Fv, v') = -1, \quad \beta_{S'}(Fv, w') = 1,$$

$$\beta_{S'}(Fw, v') = 1, \quad \beta_{S'}(Fw, w') = -1.$$

Indeed, as in case (b) we find w' satisfying $\beta_{S'}(Fvw, w') = -1$, that is, $\beta_{S'}(Fv, w') = -\beta_{S'}(Fw, w')$. We can assume that $\beta_{S'}(Fv, w') = 1$. Similarly, as in (b), we show that there is v' such that $\beta_{S'}(Fv, v') = -1$. The elements we need are v', w' or $v'w', w'$ depending on whether $\beta_{S'}(Fw, v')$ is 1 or -1.

Now $B_L = \{-1, v', w'\}$ (or $B_L = \{-1, 2, v', w'\}$ when $g(K) = 2$) is a basis for $U_{S'}/U^2_{S'}$.

Let $Fw = (w_{\Phi R})_{R\in S}$, $Fv = (v_{\Phi R})_{R\in S}$, $F^{-1}w' = (w'_R)_{R\in S}$, $F^{-1}v' = (v'_R)_{R\in S}$. There are non-dyadic, distinct primes P_1, P_2 in K and Q_1, Q_2 in L, and $x_i\in K^\cdot$, $y_i\in L^\cdot$ $(i = 1, 2)$, such that

$$x_1 = v'_R \quad \text{and} \quad x_2 = w'_R, \quad \text{in } K^\cdot_R/K^{\cdot 2}_R \quad \text{for } R\in S,$$

$$y_1 = v_{\Phi R} \quad \text{and} \quad y_2 = w_{\Phi R}, \quad \text{in } L^\cdot_{\Phi R}/L^{\cdot 2}_{\Phi R} \quad \text{for } R\in S,$$

$$x_2 = 1 \quad \text{in } K^\cdot_{P_1}/K^{\cdot 2}_{P_1}, \quad y_2 = 1 \quad \text{in } L^\cdot_{Q_1}/L^{\cdot 2}_{Q_1},$$

$$x_i\in U_{S_1}, \quad y_i\in U_{S'_1}, \quad \operatorname{ord}_{P_i} x_i = \operatorname{ord}_{Q_i} y_i = 1 \ (i = 1, 2)$$

where $S_1 = S\cup\{P_1, P_2\}$, $S'_1 = S'\cup\{Q_1, Q_2\}$.

The sets $B_K\cup\{x_1, x_2\}$ and $B_L\cup\{y_1, y_2\}$ form bases for $U_{S_1}/U^2_{S_1}$ and $U_{S'_1}/U^2_{S'_1}$, respectively. We extend Φ onto S_1 by putting $\Phi P_i = Q_i$ $(i = 1, 2)$. The isomorphism φ_{S_1} is defined by sending $-1, v, w, x_1, x_2$ to $-1, y_1, y_2, v', w'$, respectively, and also $\varphi_{S_1}(2) = 2$ when $g(K) = 2$. As in the previous case we check that

$$(-1, x_i)_{P_i} = (-1, y_i)_{Q_i} = 1 \quad (i = 1, 2),$$

$$(v, x_1)_{P_1} = (v', y_1)_{Q_1} = -1, \quad (w, x_2)_{P_2} = (w', y_2)_{Q_2} = -1.$$

Moreover,

$$(v, x_2)_{P_2} = \beta_S(v, F^{-1}w') = \beta_{S'}(Fv, w') = 1$$

and similarly $(w, x_1)_{P_1} = 1$. Further,

$$(v', y_2)_{Q_2} = \beta_{S'}(v', Fw) = 1$$

and similarly $(w', y_1)_{Q_1} = 1$. We also have

$$\prod_{R\in S}(x_1, x_2)_R = \prod_{R\in S}(Fw, Fv)_{\Phi R} = 1$$

by Hilbert reciprocity. Hence our choice of x_2 gives $(x_1, x_2)_{P_2} = 1$, i.e., $x_1\in K^{\cdot 2}_{P_2}$. Similarly we get $y_1\in L^{\cdot 2}_{Q_2}$. Summing up, φ_{S_1} induces local isomorphisms $\varphi_{P_i}\colon K^\cdot_{P_i}/K^{\cdot 2}_{P_i} \to L^\cdot_{Q_i}/L^{\cdot 2}_{Q_i}$ $(i = 1, 2)$, and these preserve Hilbert symbols.

Thus we have constructed an S_1-equivalence between K and L. This finishes the proof of Theorem 2 for real fields. When K and L are non-real, $B_K = \{-1, v\}$ when $g(K) = 1$, and $B_K = \{-1, 2, v\}$ when $g(K) = 2$, for a certain $v\in K_0$. As in the case when K and L are real fields (cases (a) and (b) above) we enlarge S if necessary by adjoing a prime, and construct a small equivalence between K and L. This completes the proof of Theorem 2.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Theory of Numbers* (in Russian), Moskva 1985.

[2] J. Carpenter, *Finiteness Theorems for Forms over Number Fields*, Dissertation, LSU Baton Rouge, La. 1989.

[3] A. Czogała, *Witt rings of algebraic number fields* (in Polish), Dissertation, Silesian University, Katowice, 1987.

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

[5] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer, Berlin–Heidelberg–New York 1974.
[6] O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin–Göttingen–Heidelberg 1963.
[7] R. Perlis and K. Szymiczek, *Matching Witts with number fields*, Preprint, 1988.
[8] K. Szymiczek, *Matching Witts locally and globally*, Math. Slovaca (to appear).

INSTITUTE OF MATHEMATICS
SILESIAN UNIVERSITY
Bankowa 14, PL-40-007 Katowice, Poland

Received on 30.3.1989
and in revised form on 29.12.1989 (1920)

ACTA ARITHMETICA
LVIII.1 (1991)

Generalization of a theorem of Siegel

by

JONATHAN W. SANDS (Burlington, Vt.)

I. Introduction. The arithmetic of non-maximal orders in number fields has gained importance with the rise of computational number theory. Indeed it is a subtle problem to determine an integral basis for the maximal order and at times one would prefer to compute in a non-maximal order for which an integral basis is available. Yet references on the arithmetic of non-maximal orders in number fields are few. Dedekind's work [5] is still perhaps the most complete. We will present a modern formulation of some basic results as background, and then focus our interest on regulators. Our main result may then be viewed as an appendix (after Siegel) to Dedekind's monograph.

If $\mathcal{O}$ is an order contained in the maximal order $\mathcal{O}_K$ of a number field K, the regulator $R_{\mathcal{O}}$ is defined for $\mathcal{O}$ just as it is for $\mathcal{O}_K$, after replacing the unit group $\mathcal{O}_K^*$ by the smaller group $\mathcal{O}^*$. The primary goal of this paper is to obtain an effective upper bound on $R_{\mathcal{O}}$. Siegel [12] did this in the case of $\mathcal{O} = \mathcal{O}_K$ by proving an effective version of a result of Landau [7]. Our result builds on Siegel's by using a formula of Dedekind [5] to relate $R_{\mathcal{O}}$ to $R_K = R_{\mathcal{O}_K}$ and then applying a result of Robin [10] based on the method of Rosser–Schoenfeld [11].

The results of Siegel and Dedekind involve class numbers as well. Define the class group $Cl_{\mathcal{O}}$ of $\mathcal{O}$ to be the group of invertible fractional ideals of $\mathcal{O}$ modulo the group of nonzero principal fractional ideals of $\mathcal{O}$: $Cl_{\mathcal{O}} = I_{\mathcal{O}}/P_{\mathcal{O}}$. This group is finite [2], [5] of order $h_{\mathcal{O}}$, the class number of $\mathcal{O}$. Siegel [12] defines $g_K = 2^{r_1}h_K R_K/w_K$, where r_1 is the number of real embeddings of K and w_K is the order of the torsion subgroup of $\mathcal{O}_K^*$. Put $w_{\mathcal{O}}$ equal to the order of the torsion subgroup of $\mathcal{O}^*$, and furthermore put $t_{\mathcal{O}}$ equal to the order of the torsion subgroup of $I_{\mathcal{O}}$. Of course $t_{\mathcal{O}_K}$ equals 1, but in general we will see that $t_{\mathcal{O}}$ must only be finite. We generalize Siegel's definition by setting $g_{\mathcal{O}} = 2^{r_1}h_{\mathcal{O}}R_{\mathcal{O}}/w_{\mathcal{O}}t_{\mathcal{O}}$. This allows us to devise a new statement of Dedekind's formula.

THEOREM (Dedekind). $g_{\mathcal{O}} = g_{\mathcal{O}_K}$.

Research supported by NSF EPSCoR Grant R11-810679.