ACTA ARITHMETICA
LXVI.3 (1994)

Kuroda's class number formula

by

Franz Lemmermeyer (Heidelberg)

Introduction. Let k be a number field and K/k a V_4-extension, i.e. a normal extension with $\mathrm{Gal}(K/k) = V_4$, where V_4 is Klein's four-group. K/k has three intermediate fields, say k_1, k_2, and k_3. We will use the symbol N^i (resp. N_i) to denote the norm of K/k_i (resp. k_i/k), and by a widespread abuse of notation we will apply N^i and N_i not only to numbers but also to ideals and ideal classes. The unit groups (groups of roots of unity, class numbers) in these fields will be denoted by E_k, E_1, E_2, E_3, E_K $(W_k, W_1, \ldots, h_k, h_1, \ldots)$ respectively, and the (finite) index $q(K) = (E_K : E_1E_2E_3)$ is called the *unit index* of K/k.

For $k = \mathbb{Q}$, $k_1 = \mathbb{Q}(\sqrt{-1})$ and $k_2 = \mathbb{Q}(\sqrt{m})$ it was already known to Dirichlet [5] that $h_K = \frac{1}{2}q(K)h_2h_3$. Bachmann [2], Amberg [1] and Herglotz [12] generalized this class number formula gradually to arbitrary extensions $K/\mathbb{Q}$ whose Galois groups are elementary abelian 2-groups. A remark of Hasse [11, p. 3] seems to suggest that Varmon [30] proved a class number formula for extensions K/k with $\mathrm{Gal}(K/k)$ an elementary abelian p-group; unfortunately, his paper was not accessible to me. Kuroda [18] later gave a formula in case there is no ramification at the infinite primes. Wada [31] stated a formula for 2-extensions of $k = \mathbb{Q}$ without any restriction on the ramification (and without proof), and finally Walter [32] used Brauer's class number relations to deduce the most general Kuroda-type formula.

As we shall see below, Walter's formula for V_4-extensions does not always give correct results if K contains the 8th root of unity. This does not, however, seem to affect the validity of the work of Parry [22, 23] and Castela [4] who made use of Walter's formula.

The proofs mentioned above use analytic methods; for V_4-extensions $K/\mathbb{Q}$, however, there exist algebraic proofs given by Hilbert [14] (if $\sqrt{-1} \in K$), Kuroda [17] (if $\sqrt{-1} \in K$), Halter-Koch [9] (if K is imaginary), and Kubota [15, 16]. For base fields $k \neq \mathbb{Q}$, on the other hand, nothing seems to be known except the very recent work of Berger [3].

In this paper we will show how Kubota's proof can be generalized. In the first half of our proof, where we measure the extent to which $\mathrm{Cl}(K)$ is generated by the $\mathrm{Cl}(k_i)$, we will use class field theory in its ideal-theoretic formulation (cf. Hasse [10] or Garbanati [7]). The second half of the proof is a somewhat lengthy index computation.

1. Kuroda's formula. For any number field F, let $\mathrm{Cl}_u(F)$ be the odd part of the ideal class group of F, i.e. the direct product of the p-Sylow subgroups of $\mathrm{Cl}(F)$, $p \neq 2$. It has already been noticed by Hilbert that the odd part of $\mathrm{Cl}(F)$ behaves well in 2-extensions, and the following fact is a special case of a theorem of Nehrkorn [21] (it can also be found in Kuroda [18] or Reichardt [27]):

$$\text{(1.1)} \qquad \mathrm{Cl}_u(K) \cong \Big(\mathop{\times}_{i=1}^{3} \mathrm{Cl}_u(k_i)/\mathrm{Cl}_u(k) \Big) \times \mathrm{Cl}_u(k) \qquad \textit{for } V_4\textit{-extension } K/k\,.$$

Here $\times$ denotes the direct product. This simple formula allows us to compute the structure of $\mathrm{Cl}_u(K)$; of course we cannot expect a similar result to hold for $\mathrm{Cl}_2(K)$, mainly because of the following two reasons:

1. Ideal classes of k_i can become principal in K (capitulation), and this means that we cannot regard $\mathrm{Cl}_2(k_i)$ as a subgroup of $\mathrm{Cl}_2(K)$.

2. Even if they do not capitulate, ideal classes of subfields can coincide in K: consider a prime ideal $\mathfrak{p}$ which ramifies in k_1 and k_2; if the prime ideals above $\mathfrak{p}$ in k_1 and k_2 are not principal, they will generate the same non-trivial ideal class in K.

Nevertheless there is a homomorphism

$$j : \mathrm{Cl}(k_1) \times \mathrm{Cl}(k_2) \times \mathrm{Cl}(k_3) \to \mathrm{Cl}(K)$$

defined as follows: let $c_i = [\mathfrak{a}_i]$ be the ideal class in k_i generated by $\mathfrak{a}_i$; then $\mathfrak{a}_i\mathfrak{O}_K$ is the ideal in $\mathfrak{O}_K$ (= ring of integers in K) generated by $\mathfrak{a}_i$, and it is obvious that $j(c_1, c_2, c_3) = [\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3\mathfrak{O}_K]$ is well defined, and that moreover

$$h(K) = \frac{|\operatorname{cok} j|}{|\ker j|} \cdot h_1 h_2 h_3\,.$$

In order to compute $h(k)$ we have to determine the orders of the groups $\ker j$ and $\operatorname{cok} j = \mathrm{Cl}(K)/\operatorname{im} j$. This will be done as follows:

(1.2) *Let $\widehat{j}$ be the restriction of j to the subgroup*

$$\widehat{C} = \{(c_1, c_2, c_3) \mid N_1 c_1 N_2 c_2 N_3 c_3 = 1\}$$

of the direct product $\mathrm{Cl}(k_1) \times \mathrm{Cl}(k_2) \times \mathrm{Cl}(k_3)$. *Then*

$$h_k \cdot \frac{|\operatorname{cok} j|}{|\ker j|} = \frac{|\operatorname{cok} \widehat{j}|}{|\ker \widehat{j}|}\,.$$

Now the reciprocity law of Artin, combined with Galois theory, gives a correspondence $\stackrel{\text{Art}}{\longleftrightarrow}$ between subgroups of $\mathrm{Cl}(K)$ and subfields of the Hilbert class field K^1 of K. We will find that $\operatorname{im}\widehat{\jmath} \stackrel{\text{Art}}{\longleftrightarrow} K_{\text{gen}}$, the genus class field of K with respect to k, and then the well known formula of Furuta [6] shows

$$(1.3)\quad |\operatorname{cok}\widehat{\jmath}| = (\mathrm{Cl}(K) : \operatorname{im}\widehat{\jmath}) = (K_{\text{gen}} : k) = 2^{d-2}h_k\Big\{\prod e(\mathfrak{p})\Big\}\Big/(E_k : H)\,,$$

where

- d is the number of infinite places ramified in K/k;
- $e(\mathfrak{p})$ is the ramification index in K/k of a prime ideal $\mathfrak{p}$ in k;
- H is the group of units in E_k which are norm residues in K/k;
- $\prod$ is extended over all (finite) prime ideals of k.

The computation of $|\ker\widehat{\jmath}|$ is a bit tedious, but in the end we will find

$$(1.4)\qquad |\ker\widehat{\jmath}| = 2^{v-1}h_k^2\prod e(\mathfrak{p})\cdot(H : E_k^2)/q(K)\,,$$

where $v = 1$, if $K = k(\sqrt{\varepsilon}, \sqrt{\eta})$ with units $\varepsilon, \eta \in E_k$, and $v = 0$ otherwise.

If we collect these results, define κ to be the $\mathbb{Z}$-rank of E_k, and recall the formula $(E_k : E_k^2) = 2^{\kappa+1}$, we obtain

(1.5) *Kuroda's class number formula for V_4-extensions K/k*:

$$h(K) = 2^{d-\kappa-2-v}q(K)h_1h_2h_3/h_k^2\,.$$

In particular,

$$h(K) = \begin{cases} \frac{1}{4}q(K)h_1h_2h_3 & \text{if } k = \mathbb{Q} \text{ and } K \text{ is real,}\\ \frac{1}{2}q(K)h_1h_2h_3 & \text{if } k = \mathbb{Q} \text{ and } K \text{ is imaginary,}\\ \frac{1}{4}q(K)h_1h_2h_3/h_k^2 & \text{if } k \text{ is an imaginary quadratic}\\ & \qquad \text{extension of } \mathbb{Q}. \end{cases}$$

2. The proofs. In order to prove (1.2) we define a homomorphism

$$\nu : C = \mathrm{Cl}(k_1)\times\mathrm{Cl}(k_2)\times\mathrm{Cl}(k_3) \to \mathrm{Cl}(k)\,,\qquad \nu(c_1, c_2, c_3) = N_1c_1N_2c_2N_3c_3\,.$$

If at least one of the extensions k_i/k is ramified, we know $N_i\,\mathrm{Cl}(k_i) = \mathrm{Cl}(k)$ by class field theory. If all the k_i/k are unramified, the groups $N_i\,\mathrm{Cl}(k_i)$ will have index $2 = (k_i : k)$ in $\mathrm{Cl}(k)$, and they will be different since

$$k_i/k \stackrel{\text{Art}}{\longleftrightarrow} N_i\,\mathrm{Cl}(k_i)$$

in this case. Therefore ν is onto, and if we put $\widehat{C} = \ker\nu$ we get an exact sequence $1 \to \widehat{C} \to C \to \mathrm{Cl}(k) \to 1$.

Let $\widehat{j}$ be the restriction of j to $\widehat{C}$; then the diagram

$$\begin{tikzcd}
1 \arrow[r] & \widehat{C} \arrow[r] \arrow[d, "\widehat{j}"] & C \arrow[r, "\nu"] \arrow[d, "j"] & \mathrm{Cl}(k) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{Cl}(L) \arrow[r] & \mathrm{Cl}(L) \arrow[r] & 1 \arrow[r] & 1
\end{tikzcd}$$

is exact and commutes. The "serpent lemma" gives us an exact sequence

$$1 \to \ker \widehat{j} \to \ker j \to \mathrm{Cl}(k) \to \mathrm{cok}\, \widehat{j} \to \mathrm{cok}\, j \to 1\,,$$

and this implies the index relation we wanted to prove:

$$h_k \cdot \frac{|\mathrm{cok}\, j|}{|\ker j|} = \frac{|\mathrm{cok}\, \widehat{j}|}{|\ker \widehat{j}|}\,.$$

Before we start to prove (1.3), we define $K^{(2)}$ to be the maximal field in K_{gen}/k such that $\mathrm{Gal}(K^{(2)}/k)$ is an elementary abelian 2-group. Moreover, we let J_K (resp. H_K) denote the group of (fractional) ideals (resp. principal ideals) of K.

(2.1) *To every subfield F of the Hilbert class field K^1 of K belongs exactly one ideal group $\mathfrak{h}_F$ with $H_K \subset \mathfrak{h}_F \subset J_K$. Under this correspondence*,

$$\mathrm{Gal}(K^1/F) \cong \mathrm{Cl}(K)/(J_K/\mathfrak{h}_F) \cong \mathfrak{h}_F/H_K\,,$$

and we find the following diagram of subfields F and corresponding Galois groups $\mathrm{Gal}(K^1/F)$:

$$\begin{tikzcd}
K^1 \arrow[r, leftrightarrow] \arrow[d, dash] & 1 \arrow[d, dash] \\
K_{\mathrm{gen}} \arrow[r, leftrightarrow] \arrow[d, dash] & \mathrm{im}\, \widehat{j} \arrow[d, dash] \\
K^{(2)} \arrow[r, leftrightarrow] \arrow[d, dash] & \mathrm{im}\, j \arrow[d, dash] \\
K \arrow[r, leftrightarrow] & \mathrm{Cl}(K).
\end{tikzcd}$$

P r o o f. The correspondence $K^{(2)} \leftrightarrow \mathrm{im}\, j$ will not be needed in the sequel and is included only for the sake of completeness; the main ingredients for a proof can be found in Kubota [16, Hilfssatz 13].

Before we start proving $K_{\mathrm{gen}} \leftrightarrow \mathrm{im}\, \widehat{j}$ we recall that K_{gen} is the class field of k for the ideal group $N_{K/k} H_K^{(\mathfrak{m})} \cdot H_{\mathfrak{m}}^{(1)}$ of the norm residues mod $\mathfrak{m}$ where the defining modulus $\mathfrak{m}$ is a multiple of the conductor $\mathfrak{f}(K/k)$ (the notation is explained in Hasse [10] or Garbanati [7], the result can be found in Scholz [29] or Gurak [8]). The assertion of Herz [13, Prop. 1] that $K_{\rm gen}$ is the class field for $N_{K/k}H_K^{(\mathfrak{m})}$ is faulty: one mistake in his proof lies in the erroneous assumption that every principal ideal of K is the norm of an ideal from K^1. Although this is true for prime ideals, it does not hold generally, as the following simple counterexample shows: the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$ is $K^1 = K(\sqrt{-1})$, and the principal ideal $(1+\sqrt{-5})$ cannot be a norm from K^1 since the prime ideals above $(2, 1+\sqrt{-5})$ and $(3, 1+\sqrt{-5})$ are inert in K^1/K. Moreover, contrary to Herz's claim, not every ideal in the Hilbert class field of K is principal: this is, of course, only true for ideals from K.

Our task now is to transfer the ideal group $N_{K/k}H_K^{(\mathfrak{m})} \cdot H_{\mathfrak{m}}^{(1)}$ in k, which is defined $\bmod\, \mathfrak{m}$, to an ideal group in K defined $\bmod\, 1$. To do this we need

(2.2) *For V_4-extensions K/k, the following assertions are equivalent*:

(i) $r \in k^\times$ *is a norm residue in K/k at every place of k*;
(ii) $r \in k^\times$ *is a* (*global*) *norm from k_1/k and k_2/k*;
(iii) *there exist $\alpha \in K^\times$ and $a \in k^\times$ such that $r = a^2 \cdot N_{K/k}\alpha$.*

The elements of $N_{K/k}H_K^{(\mathfrak{m})} \cdot H_{\mathfrak{m}}^{(1)}$ therefore have the form $(a^2 \cdot N_{K/k}\alpha)$, where $a \in k$, $\alpha \in K$, and $(\alpha) + \mathfrak{m} = (1)$. Using the Verschiebungssatz we find that $K_{\rm gen}/K$ belongs to the group

$$\mathfrak{h}_{\rm gen} = \{\mathfrak{a} \in J_K \mid \mathfrak{a} + \mathfrak{m} = (1)\,,\ N_{K/k}\mathfrak{a} \in N_{K/k}H_K^{(\mathfrak{m})} \cdot H_{\mathfrak{m}}^{(1)}\}\,.$$

Now $N_{K/k}\mathfrak{a} = (a \cdot N_{K/k}\alpha) \Leftrightarrow N_{K/k}(\mathfrak{a}/\alpha) = (a)$; we put $\mathfrak{b} = \mathfrak{a}/\alpha$ and claim that there are ideals $\mathfrak{a}_i$ in k_i such that $\mathfrak{b} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$. We assume without loss of generality that $\mathfrak{b}$ is an (entire) ideal in $\mathfrak{O}_K$. We may also assume that no ideal lying in a subfield k_i divides $\mathfrak{b}$. But then any $\mathfrak{P} \mid \mathfrak{b}$ necessarily has inertial degree 1, and no conjugate of $\mathfrak{P}$ divides $\mathfrak{b}$. Writing $\mathfrak{P}^m \| \mathfrak{b}$ we deduce

$$(N_{K/k}\mathfrak{P})^{\mathfrak{m}} \| N_{K/k}\mathfrak{b} = (a^2)\,,$$

and this implies $2 \mid m$.

If σ, τ, and $\sigma\tau$ are the automorphism of K/k fixing k_1, k_2 and k_3 respectively, the identity

$$2 = 1 + \sigma + 1 + \tau - (1 + \sigma\tau)\sigma$$

in $\mathbb{Z}[\mathrm{Gal}(K/k)]$ shows $\mathfrak{P}^2 = N^1\mathfrak{P} \cdot N^2\mathfrak{P} \cdot (N^3\mathfrak{P})^{-\sigma}$, and we are done.

Now $(a^2) = N_{K/k}\mathfrak{b} = N_{K/k}(\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3) = (N_1\mathfrak{a}_1 N_2\mathfrak{a}_2 N_3\mathfrak{a}_3)^2$, and extracting the square root we obtain $(a) = N_1\mathfrak{a}_1 N_2\mathfrak{a}_2 N_3\mathfrak{a}_3$.

Conversely, all ideals $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$ with $\mathfrak{a} + \mathfrak{m} = (1)$ and $(a) = N_1\mathfrak{a}_1 N_2\mathfrak{a}_2 N_3\mathfrak{a}_3$ lie in $\mathfrak{h}_{\rm gen}$, and the same is true of all principal ideals prime to $\mathfrak{m}$ since the class field $K_{\mathfrak{h}}$ corresponding to $\mathfrak{h}$ is unramified if and only if

$H_K^{(\mathfrak{m})} \subset \mathfrak{h}$. Therefore

$$\mathfrak{h}_{\mathrm{gen}} = \{\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \mid \mathfrak{a} + \mathfrak{m} = (1),\ N_1\mathfrak{a}_1N_2\mathfrak{a}_2N_3\mathfrak{a}_3 = (a) \text{ for some } a \in k\} \cdot H_K^{(\mathfrak{m})}$$

and by removing the condition $\mathfrak{a}+\mathfrak{m} = (1)$, which amounts to replacing $\mathfrak{h}_{\mathrm{gen}}$ by an equivalent ideal group, we finally see

$$\mathfrak{h}_{\mathrm{gen}} = \{\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \mid N_1\mathfrak{a}_1N_2\mathfrak{a}_2N_3\mathfrak{a}_3 = (a) \text{ for some } a \in k\} \cdot H_K\,.$$

The corresponding class group is $J_K/\mathfrak{h}_{\mathrm{gen}}$, and this gives

$$\mathrm{Gal}(K_{\mathrm{gen}}/K) \cong \mathfrak{h}_{\mathrm{gen}}/H_K = \{c = c_1c_2c_3 \mid N_1c_1N_2c_2N_3c_3 = 1\} = \widehat{C}\,.$$

Now (1.3) follows from Furuta's formula for the genus class number.

It remains to prove (2.2); this result is due to Pitti [24–26], and similar observations have been made by Leep and Wadsworth [19, 20]. Our proof of (ii)⇒(iii) goes back to Kubota [15, Hilfssatz 14], while (iii)⇒(i) has already been noticed by Scholz [28, p. 102].

(i)⇒(ii) is just an application of Hasse's norm residue theorem for cyclic extensions;

(ii)⇒(iii). Choose $\alpha_1 \in k_1$ and $\alpha_2 \in k_2$ with $N_1\alpha_1 = N_2\alpha_2 = r$. Since $\sigma\tau$ acts non-trivially on k_1 and k_2, this implies $(\alpha_1/\alpha_2)^{1+\sigma\tau} = 1$. Hilbert's theorem 90 shows the existence of $\alpha \in K^\times$ such that $\alpha_1/\alpha_2 = \alpha^{1-\sigma\tau}$. Now

$$\alpha^{1-\sigma\tau} = \alpha^{1+\sigma}(\alpha^{1+\tau})^{-\sigma} \quad \text{and} \quad \alpha^{1+\sigma}/\alpha_1 = (\alpha^{1+\tau})^{\sigma}/\alpha_2 \in k_1 \cap k_2 = k\,.$$

Put $a = \alpha^{1+\sigma}/\alpha_1$ and verify $N_{K/k}\alpha = (\alpha^{1+\sigma})^{1+\tau} = ra^2$.

(iii)⇒(i) is a consequence of formula (9) in §6 of part II of Hasse's "Zahlbericht" [10] which says

$$\left(\frac{\beta, k_1k_2}{\mathfrak{p}}\right) = \left(\frac{\beta, k_1}{\mathfrak{p}}\right)\left(\frac{\beta, k_2}{\mathfrak{p}}\right).$$

Since $r = N_i((N^i\alpha)/a),\ i = 1, 2$, we see that r is a norm from k_1 and k_2, and Hasse's formula just tells us that r is a norm residue in $k_1k_2 = K$.

Before we proceed with the computation of $|\ker\widehat{j}|$, we will pause for a moment to look at (2.1) with more care. The fact that K_{gen} is the class field of k for the ideal group $N_{K/k}H_K^{(\mathfrak{m})} \cdot H_{\mathfrak{m}}^{(1)}$ is well known for abelian K/k. Moreover, the principal genus theorem of class field theory says that K_{gen} is the class field of K for the class group $\{c^{\sigma-1} \mid c \in \mathrm{Cl}(K)\}$, if $\mathrm{Gal}(K/k) = \langle\sigma\rangle$ is cyclic. If K/k is abelian (and not necessarily cyclic), the class field K_{cen} for the class group $\langle c^{\sigma-1} \mid c \in \mathrm{Cl}(K),\ \sigma \in \mathrm{Gal}(K/k)\rangle$ is called the *central class field*, and in general K_{cen} is strictly bigger than K_{gen}. A description of K_{gen} in terms of the ideal class group of K is unknown for non-cyclic K/k, and (2.1) answers this open question for the simplest non-cyclic group, the four-group $V_4 \cong (\mathbb{Z}/2\mathbb{Z})^2$. For other non-cyclic groups, this is very much an open problem.

In the V_4-case, the fact that $\langle c^{\sigma-1} \mid c \in \mathrm{Cl}(K),\ \sigma \in \mathrm{Gal}(K/k)\rangle \subset \mathrm{im}\,\widehat{j}$ can be verified directly by noting that $c^{\sigma-1} = (c^\sigma)^{\sigma\tau+1} \cdot (c^{-1})^{\tau+1} \in C_2 \times C_3$ is annihilated by ν.

The computation of $|\ker \widehat{j}|$ will be done in several steps. We call an ideal $\mathfrak{a}_1$ in k_1 *ambiguous* if $\mathfrak{a}_1^\tau = \mathfrak{a}_1$. An ideal class $c \in \mathrm{Cl}(k_1)$ is called *ambiguous* if $c^\tau = c$, and *strongly ambiguous* if $c = [\mathfrak{a}_1]$ for an ambiguous ideal $\mathfrak{a}_1$. Let A_i denote the group of strongly ambiguous ideal classes in k_i $(i = 1, 2, 3)$. Then $A = A_1 \times A_2 \times A_3$ is a subgroup of C, and $\widehat{A} = \widehat{C} \cap A_1 \times A_2 \times A_3$ is a subgroup of $\widehat{C}$. The idea of the proof is to restrict $\widehat{j}$ (once more) from $\widehat{C}$ to $\widehat{A}$ and to compute the kernel of this restricted map by using the formula for the number of ambiguous ideal classes.

In (1.3) we defined H as the group of units in E_k which are norm residues in K/k at every place of k. Using (2.2) we see that

$$H = \{\eta \in E_k : \eta = N_i \alpha_i \text{ for some } \alpha_i \in k_i,\ i = 1, 2, 3\}\,.$$

Let $H_0 = E_1^N \cap E_2^N \cap E_3^N$ be the subgroup of H consisting of those units that are relative norms of units for every k_i/k. The computation of $|\ker \widehat{j}|$ starts with the following observation:

(2.3) If j^* is the restriction of $\widehat{j}$ to $\widehat{A}$, then $|\ker \widehat{j}| = (H : H_0) \cdot |\ker j^*|$.

Let $R = \{\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \mid \mathfrak{a}_i \in I_i \text{ is ambiguous in } k_i/k\}$ and $R_\pi = R \cap H_K$; then

$$|\ker j^*| = |A|/(R : R_\pi)\,. \tag{2.4}$$

Now the computation of $|\ker \widehat{j}|$ is reduced to the determination of $(H : H_0)$ and $(R : R_\pi)$; let $t = |\mathrm{Ram}(K/k)|$ be the number of (finite) prime ideals of k ramified in K, and λ denote the $\mathbb{Z}$-rank of E_K. We will prove

$$(R : R_\pi) = 2^{t+\kappa-\lambda-2-v} h_k q(K) \prod (E_i^N : E_k^2)/(H_0 : E_k^2)\,. \tag{2.5}$$

The number $|A_i|$ of strongly ambiguous ideal classes in k_i/k is given by the well known formula (cf. Hasse's Zahlbericht [10], Teil Ia, §13).

(2.6) $|A_i| = 2^{\delta_i-\kappa-2} h_k \cdot (E_i^N : E_k^2)$, where δ_i denotes the number of (finite and infinite) places in k which are ramified in k_i/k.

Once we know how the δ_i are related to t, κ, λ etc., we will be able to deduce (1.4) from (2.3)–(2.6). To this end, let t_i be the "finite part" of δ_i, i.e. the number $|\mathrm{Ram}(k_i/k)|$ of prime ideals in k ramified in k_i/k, and let d_i denote the infinite part. Then $\delta_i = d_i + t_i$, and

$$2^{t_1+t_2+t_3} = 2^t \cdot \prod e(\mathfrak{p})\,, \quad 2d = d_1+d_2+d_3\,, \quad \text{and} \quad \lambda - 4\kappa = 3 - 2d\,. \tag{2.7}$$

Since $|A| = \prod |A_i|$, we obtain from (2.4) and (2.6)

$$|A| = 2^{\delta_1+\delta_2+\delta_3-3\kappa-6} h_k^3 \cdot \prod (E_i^N : E_k^2)\,;$$

dividing by (2.5) yields

$$|\ker j^*| = 2^{t_1+t_2+t_3-t+d_1+d_2+d_3+\lambda-4\kappa-4+v} h_k^2 \cdot (H_0 : E_k^2)/q(K)\,,$$

and using (2.7) we find

$$|\ker j^*| = 2^{v-1} h_k^2 \prod e(\mathfrak{p}) \cdot (H_0 : E_k^2)/q(K)\,.$$

Substituting this formula into equation (2.3) we finally obtain (1.4).

In order to prove (2.3) let $([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) \in \ker \widehat{j}$; then $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 = (\alpha)$ for some $\alpha \in K^\times$. Since $(N_{K/k}\alpha) = (N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3)^2$ (equality of ideals in $\mathfrak{O}_k$) and because $([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) \in \widehat{C}$, there exists $a \in k$ such that $(N_{K/k}\alpha) = (a)^2$. This shows that $\eta = (N_{K/k}\alpha)/a^2$ is a unit in E_k, which is unique mod $NE_K \cdot E_k^2$. Moreover, $\eta \in H$ since $\eta = N_i((N^i\alpha)/a)$. Therefore

$$\vartheta_0 : \ker \widehat{j} \to H/NE_K \cdot E_k^2\,, \qquad ([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) \to \eta NE_K \cdot E_k^2\,,$$

is a well defined homomorphism. We want to show that ϑ_0 is onto: to this end, let $\eta \in H$; using (2.2) we can find an $a \in k$ such that $N_{K/k}\alpha = \eta a^2$. In the proof of (2.1) we have seen that an equation $N_{K/k}\mathfrak{a} = (a)^2$ implies the existence of ideals $\mathfrak{a}_i$ in k_i such that $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$. This gives $(\alpha) = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$.

Now $(N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3)^2 = (N_{K/k}\alpha) = (a)^2$ yields $(a) = N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3$, and we have shown $\eta \in \operatorname{im}\vartheta_0$.

Since $\vartheta_0 : \ker \widehat{j} H/NE_K \cdot E_k^2$ is onto, the same is true for any homomorphism $\ker \widehat{j} H/H_0$ which is induced by an inclusion $NE_K \cdot E_k^2 \subset H_0 \subset H$. Obviously, the group $H_0 = E_1^N \cap E_2^N \cap E_3^N$ defined above is such a group, and so $\vartheta : \ker \widehat{j} H/H_0$ is onto. An element $([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) \in \ker \widehat{j}$ belongs to $\ker \vartheta$ if and only if

$$\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 = (\alpha)\,, \qquad (a) = N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3\,, \qquad (N_{L/k}\alpha)/a^2 = \eta \in H_0\,.$$

Let $\varrho_i = N^i\alpha/a$; then $\mathfrak{a}_1^{1-\tau} = (\varrho_1)$, $\mathfrak{a}_2^{1-\sigma\tau} = (\varrho_2)$, $\mathfrak{a}_3^{1-\sigma} = (\varrho_3)$ and $N_i\varrho_i = \eta \in H_0$. Writing $\eta = N_i\varepsilon_i$, where $\varepsilon_i \in E_i$, and replacing ϱ_i by ϱ_i/ε_i, we may assume that $N_i\varrho_i = 1$. Hilbert's theorem 90 shows $\varrho_1 = \beta_1^{1-\tau}$, $\varrho_2 = \beta_2^{1-\sigma\tau}$, and $\varrho_3 = \beta_3^{1-\sigma}$ for some $\beta_i \in k_i$. The ideals $\mathfrak{b}_i = \mathfrak{a}_i\beta_i^{-1}$ are ambiguous, and we have $[\mathfrak{b}_i] = [\mathfrak{a}_i]$. This means that the ideal classes $[\mathfrak{a}_i]$ are strongly ambiguous, and we conclude

$$\ker \vartheta \subset \ker \widehat{j} \cap A_1 \times A_2 \times A_3 = \ker j^*\,.$$

If, on the other hand, $([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) \in \ker \widehat{j}$ and the ideals $\mathfrak{a}_i$ are ambiguous, then the $\varrho_i = N^i\alpha/a$ are units, and

$$\eta = \vartheta([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) = N_i\varrho_i \in E_1^N \cap E_2^N \cap E_3^N = H_0\,.$$

We have seen that $\ker\vartheta = \ker j^*$, which shows that the sequence

$$1 \to \ker j^* \to \ker\widehat{j} \xrightarrow{\vartheta} H/H_0 \to 1$$

is exact; (2.3) follows at once.

The proof of (2.4) will be done in two steps. First we notice that $\operatorname{im} j^*$ consists of those ideal classes in $j(\widehat{C})$ that are generated by ambiguous ideals in k_i/k. Define

$$R = \{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3, \mathfrak{a}_i \in J_i \text{ ambiguous}\},$$

$$\widehat{R} = \{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3, \mathfrak{a}_i \in J_i \text{ ambiguous}, \ \nu([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) = 1\},$$

and let π be the homomorphism $J_K \supset \widehat{R} \ni \mathfrak{A} \to [\mathfrak{A}] \in \mathrm{Cl}(K)$. Then $\pi : \widehat{R} \to \operatorname{im} j^*$ is obviously onto, and $\ker\pi = \widehat{R} \cap H_K$. But if $\varrho \in K$ and $(\varrho) = \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 \in \widehat{R}$,

$$(\varrho)^2 = (\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3)^2 = (N_1\mathfrak{a}_1 \cdot N_2\mathfrak{a}_2 \cdot N_3\mathfrak{a}_3) = (r)$$

for some $r \in k$. This shows

$$\ker\pi = \{(\varrho) \mid \varrho \in K, \ (\varrho)^2 = (r) \text{ for some } r \in k\} = R_\pi,$$

therefore

$$(\widehat{R} : R_\pi) = |\operatorname{im}\pi| = |\operatorname{im} j^*| = (\widehat{A} : \ker j^*),$$

which is equivalent to

$$|\ker j^*| = |\widehat{A}|/(\widehat{R} : R_\pi). \tag{2.8}$$

The homomorphism $\nu : C \to \mathrm{Cl}(k)$ defined at the beginning of Section 2 sends $([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) \in A = A_1 \times A_2 \times A_3 \subset C$ to $[\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3]^2 \in \mathrm{Cl}(k)$ (remember that the square of an ambiguous ideal of k_i/k is an ideal in $\mathfrak{O}_k$), and we see that

$$1 \to \widehat{A} \to A \xrightarrow{\nu} A_1^2A_2^2A_3^2 \to 1$$

is a short exact sequence. Now

$$1 \to \widehat{R} \to R \xrightarrow{\overline{\nu}} A_1^2A_2^2A_3^2 \to 1$$

where $\overline{\nu}(\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3) = \nu([\mathfrak{a}_1],[\mathfrak{a}_2],[\mathfrak{a}_3]) = [\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3]^2$, is also exact. From these facts we conclude $(A : \widehat{A}) = (R : \widehat{R})$, and this allows us to transform (2.8):

$$|\ker j^*| = |\widehat{A}|/(\widehat{R} : R_\pi) = (A : \widehat{A})|\widehat{A}|/(R : \widehat{R})(\widehat{R} : R_\pi) = |A|/(R : R_\pi).$$

This is just (2.4).

Next we determine $(R : R_\pi)$. To this end, let $(\varrho) \in R_\pi$. Then $(\varrho)^2 = (r)$ for some $r \in k^\times$, and $\eta = \varrho^2/r$ is a unit in $\mathfrak{O}_K$. Since the ideal (ϱ) is fixed by $\mathrm{Gal}(K/k)$, $\eta_i = (N_{K/k_i}\varrho)/r$ is a unit in E_i. If $\sigma \in \mathrm{Gal}(K/k)$ is an automorphism that acts non-trivially on k_3/k, we find that $\eta = \eta_1\eta_2\eta_3^{-\sigma} \in E_1E_2E_3$, where

$$N_1\eta_1 = N_2\eta_2 = N_3(\eta_3^{-\sigma}) = (N_{K/k}\varrho)/r^2.$$

The unit η we have found is determined up to a factor $\in E_kE^2$ (from now on, the unit group E_K will appear quite often, so we will write E instead of E_K), and so we can define a homomorphism $\varphi : R_\pi \to E/E_kE^2$ by assigning the class of the unit $\eta = \varrho^2/r$ to an ideal $(\varrho) \in R_\pi$ that satisfies $(\varrho)^2 = (r)$, $r \in k^\times$. We cannot expect φ to be onto because only such units $\eta_1\eta_2\eta_3 \in E_1E_2E_3$ can lie in the image of φ whose relative norms $N_i\eta_i$ coincide. Therefore we define

$$E^* = \{e_1e_2e_3 \mid e_i \in E_i,\ N_1e_1 \equiv N_2e_2 \equiv N_3e_3 \bmod E_k^2\}$$

and observe that $\operatorname{im}\varphi \subset E^*/E_kE^2$. Moreover,

(2.9) *Let $\eta = e_1e_2e_3 \in E^*$; then $K(\sqrt{\eta})/k$ is a normal extension, $\mathrm{Gal}(K(\sqrt{\eta})/k)$ is elementary abelian, and there are $\varrho \in K^\times$ and $r \in k^\times$ such that $\eta = \varrho^2/r$.*

Proof. $K(\sqrt{\eta})/k$ is normal if and only if for every $\sigma \in \mathrm{Gal}(K/k)$ there exists an $\alpha_\sigma \in K^\times$ such that $\eta^{1-\sigma} = \alpha_\sigma^2$. Let $\mathrm{Gal}(K/k) = \{1, \sigma, \tau, \sigma\tau\}$ and suppose that σ fixes k_1; then

$$\eta^{1-\sigma} = (e_1e_2e_3)^{1-\sigma} = (e_2e_3)^{1-\sigma} = (e_2e_3)^2/(N_2e_2 \cdot N_3e_3)\,,$$

and this is a square in $K^\times$ since $N_2e_2 \equiv N_3e_3 \bmod E_k^2$.

It is an easy exercise to show that $\mathrm{Gal}(K/k)$ is elementary abelian if and only if $\alpha_\sigma^{1+\sigma} = \alpha_\tau^{1+\tau} = \alpha_{\sigma\tau}^{1+\sigma\tau} = +1$. In our case, these equations are easily verified (for example $\alpha_\sigma = e_2e_3/e$ for some $e \in E_k$ such that $e^2 = N_2e_2 \cdot N_3e_3$, and therefore $\alpha_\sigma^{1+\sigma} = (N_2e_2N_3e_3)/e^2 = +1$).

Now $K(\sqrt{\eta})/k$ is elementary abelian, and so $k(\sqrt{\eta}) = k(\sqrt{r})$ for some $r \in k^\times$. This implies the existence of $\varrho \in k^\times$ such that $\varrho^2 = \eta r$.

Because of (2.9), $\varphi : R_\pi \to E^*/E_kE^2$ is onto. Moreover,

$$\begin{aligned}\ker\varphi &= \{(\varrho) \in R_\pi \mid \varrho^2/r = ue^2,\ u \in E_k,\ e \in E\}\\ &= \{(\varrho) \in R_\pi \mid \exists r \in k^\times,\ e \in E : (\varrho/e)^2 = r\}\\ &= \{(\varrho) \in R_\pi \mid \varrho^2 = r \text{ for } r \in k^\times\}\,.\end{aligned}$$

Let $R_0 = \ker\varphi$; the group of principal ideals H_k is a subgroup of R_0, and it has index $(R_0 : H_k) = 2^{2-u}$, where $2^u = (E^{(2)} : E_k)$ and $E^{(2)} = \{e \in E : e^2 \in E_k\}$. The proof is very easy: let $\Lambda = \{\varrho \in K^\times \mid \varrho^2 \in k^\times\}$ and map $\Lambda/k^\times$ onto R_0/H_k by sending $\varrho k^\times$ to $(\varrho)H_k$. The sequence

$$1 \to E^{(2)}k^\times/k^\times \to \Lambda/k^\times \to R_0/H_k \to 1$$

is exact, and since $\Lambda/k^\times$ has order 4 ($\Lambda/k^\times = \{k^\times, \sqrt{a}k^\times, \sqrt{b}k^\times, \sqrt{ab}k^\times\}$, where $K = k(\sqrt{a}, \sqrt{b})$) and $E^{(2)}k^\times/k^\times \cong E^{(2)}/E_k$, the claim is proven. We see

$$(R_0 : H_k) = \begin{cases} 1 & \text{if we can choose } a, b \in E_k, \\ 2 & \text{if we can choose } a \in E_k \text{ or } b \in E_k, \text{ but not both,} \\ 4 & \text{otherwise.} \end{cases}$$

Now we find $(R : H_k) = (R : J_k)(J_k : H_k) = 2^t h_k$, where $t = |\mathrm{Ram}(K/k)|$, and

$$\begin{aligned}(R : R_\pi) &= (R : H_k)/\{(R_\pi : R_0)(R_0 : H_k)\} \\ &= 2^{t-2} h_k (E^{(2)} : E_k)/(E^* : E_k E^2)\,.\end{aligned}$$

Since

$$(E : E_k E^2) = (E : E^2)/(E_k E^2 : E^2)\,,$$

$$(E_k E^2 : E^2) = (E_k : E^2 \cap E_k) = \frac{(E_k : E_k^2)}{(E^2 \cap E_k : E_k^2)}$$

and

$$(E^2 \cap E_k : E_k^2) = (E^{(2)} : E_k)\,,$$

we get $(E : E_k E^2) = 2^{\lambda-\kappa}(E^{(2)} : E_k)$, where λ and κ denote the $\mathbb{Z}$-rank of E and E_k, respectively. Collecting everything, we find

$$\begin{aligned}(R : R_\pi) &= 2^t h_k/\{(E^* : E_k E^2)(R_0 : H_k)\} \\ &= 2^t h_k (E : E^*)(E^{(2)} : E_k)/4(E : E_k E^2) = 2^{t+\kappa-\lambda-2} h_k (E : E^*)\,.\end{aligned}$$

But $(E : E^*) = (E : E_1E_2E_3) \cdot (E_1E_2E_3 : E^*)$, and the first factor is the unit index $q(K)$; this shows

$$(R : R_\pi) = 2^{t+\kappa-\lambda-2} h_k \cdot q(K) \cdot (E_1E_2E_3 : E^*)\,. \tag{2.10}$$

In order to study the group $E_1E_2E_3/E^*$, we define $E_i^* = \{e_i \in E_i : N_i e_i \in E_k^2\}$ and notice $E_1^*E_2^*E_3^* \subset E^* \subset E_1E_2E_3 \subset E$. The group $E^*/E_1^*E_2^*E_3^*$ is actually one we have encountered before:

$$E^*/E_1^*E_2^*E_3^* \cong H_0/E_k^2\,. \tag{2.11}$$

P r o o f. Map $e_1e_2e_3 \in E^*$ onto the coset $N_1e_1E_k^2 = N_2e_2E_k^2 = N_3e_3E_k^2$.

It is therefore sufficient to compute the index $(E_1E_2E_3 : E_1^*E_2^*E_3^*)$; to this end we introduce the natural homomorphism

$$\xi : E_1/E_1^* \times E_2/E_2^* \times E_3/E_3^* \to E_1E_2E_3/E_1^*E_2^*E_3^*\,,$$

which, of course, is onto. Letting $\overline{e}_i$ denote the coset $e_iE_i^*$ we find

$$\ker \xi = \{(\overline{e}_1, \overline{e}_2, \overline{e}_3) : e_1e_2e_3 = u_1u_2u_3 \text{ for some } u_i \in E_i^*\}\,.$$

We need to characterize $\ker\xi$. Assume that $(e_1E_1^*, e_2E_2^*, e_3E_3^*) \in \ker\xi$; then $e_1e_2e_3 = u_1u_2u_3$ for some $u_i \in E_i^*$. Replacing the $e_iE_i^*$ by $e_iu_i^{-1}E_i^*$ if necessary, we may assume that $e_1e_2e_3 = 1$. Applying $1+\sigma$ to this equation (where σ fixes k_1) yields $e_1^2N_2e_2N_3e_3 = 1$, and this implies $e_1^2 \in E_k$; in a similar way we find $e_2^2 \in E_k$ and $e_3^2 \in E_k$. If $N_2 e_2$ were a square in E_k, so were $N_3 e_3$, and e_1 would have to lie in E_k: but then $e_i \in E_i^*$ for $i = 1, 2, 3$, and $(\overline{e}_1, \overline{e}_2, \overline{e}_3)$ is trivial. So if $\ker \xi \neq 1$, we must have $e_i \in E_i \setminus E_k$ for $i = 2, 3$; but we have seen $e_i^2 =: \varepsilon_i \in E_k$, so we get $k_i = k(\sqrt{\varepsilon_i})$ for $i = 2, 3$ and, therefore, $k_1 = k(\sqrt{\varepsilon_2 \varepsilon_3})$. Moreover,

$$\ker \xi = \{1, (\sqrt{\varepsilon_1} E_1^*, \sqrt{\varepsilon_2} E_2^*, \sqrt{\varepsilon_3} E_3^*)\}\,.$$

Thus we have shown that $\ker \xi \neq 1$ implies $u = 2$ and $|\ker \xi| = 2$, where the index $2^u = (E^{(2)} : E_k)$ was introduced above. If, on the other hand, $u = 2$, then $k_i = k(\sqrt{\varepsilon_i})$ for units $\varepsilon_i \in E_k$, and $(\sqrt{\varepsilon_1} E_1^*, \sqrt{\varepsilon_2} E_2^*, \sqrt{\varepsilon_3} E_3^*)$ is a non-trivial element of $\ker \xi$. Therefore $|\ker \xi| = 2^v$ with $v = 2^u - u - 1$, and

$$(2.12) \qquad (E_1 E_2 E_3 : E_1^* E_2^* E_3^*) = 2^{-v} \Big\{ \prod (E_i : E_i^*) \Big\}\,.$$

To determine $(E_i : E_i^*)$, we make use of a well known group-theoretical lemma:

(2.13) *Let G be a group and assume that H is a subgroup of finite index in G. If f is a homomorphism from G to another group, then*

$$(G : H) = (G^f : H^f)(G_f H : H),$$

where $G^f = \operatorname{im} f$, $G_f = \ker f$, *and H^f is the image of the restriction of f to H.*

We apply this lemma to $G = E_i$, $H = E_i^*$, $f = N_i$. Then $G_f = \{\varepsilon \in E_i : N_i \varepsilon = 1\} \subset E_i^* = H$, $G^f = E_i^N = \{N_i \varepsilon : \varepsilon \in E_i\}$, and $H^f = E_k^2$, and (2.13) gives

$$(E_i : E_i^*) = (G : H) = (G^f : H^f) = (E_i^N : E_k^2)\,.$$

Putting (2.10)–(2.12) together, we find

$$\begin{aligned}(R : R_\pi) &= 2^{t+\kappa-\lambda-2} h_k \cdot q(K) \cdot (E_1 E_2 E_3 : E^*) \\ &= 2^{t+\kappa-\lambda-2} h_k \cdot q(K) \cdot (E_1 E_2 E_3 : E_1^* E_2^* E_3^*)/(E^* : E_1^* E_2^* E_3^*) \\ &= 2^{t+\kappa-\lambda-2-v} h_k \cdot q(K) \cdot \prod (E_i^N : E_k^2)/(H_0 : E_k^2)\,,\end{aligned}$$

which is (2.5).

The only claim left to prove is (2.7). If $\mathfrak{p}$ is a place in k which ramifies in K/k, then $e(\mathfrak{p}) = 2$ if $\mathfrak{p}$ ramifies in two of the three intermediate fields, and $e(\mathfrak{p}) = 4$ if $\mathfrak{p}$ is ramified in k_i/k for $i = 1, 2, 3$ (this can only happen for $\mathfrak{p} \mid 2$). This observation yields the first and the second equation in (2.7).

Now $n = (k : \mathbb{Q}) = r_k + 2s_k$ and $4n = (K : \mathbb{Q}) = r_K + 2s_K$, where r_* (resp. s_*) denotes the number of real (resp. complex) infinite places in a field. Suppose that exactly d infinite places of k ramify in K/k; then $r_K = 4(r_k - d)$, $s_K = 4s_k + 2d$, and Dirichlet's unit theorem gives $\kappa = r_k + s_k - 1$

and

$$\lambda = r_K + s_K - 1 = 4(r_k - d) + 4s_k + 2d - 1 = 4\kappa - 2d + 3\,.$$

3. Walter's formula. Assume that K/k is a normal extension, $\mathrm{Gal}(K/k) = (\mathbb{Z}/l\mathbb{Z})^m$ (l prime), and suppose moreover that there is no ramification above the infinite primes of k. The formula given by Kuroda [18] is

$$\frac{H}{h} = l^{-A}(E : E_\Omega) \cdot \prod h_i/h\,.$$

Here

- h is the class number of k,
- H is the class number of K,
- h_i is the class number of the intermediate field k_i; there are exactly $t = (l^m - 1)/(l - 1)$ such k_i,
- E is the unit group of $\mathfrak{O}_K$,
- $E_\Omega = \prod E_i$ is the group generated by the units of the subfields k_i,
- $A = \dfrac{l^u - 1}{l - 1} - u + \dfrac{\kappa + 1}{2}\left((m-1)(l^m-1) + \dfrac{l^m - 1}{l - 1} - m\right) - \kappa\left(\dfrac{l^m - 1}{l - 1} - m\right)$;
- u is the number of independent extensions of type $k_i = k(\sqrt[l]{e})$, where e is a unit in $\mathfrak{O}_k$.

Using these notations, the formula given by Walter [32] reads as follows:

$$\frac{H}{h} = l^{-A}(E : WE_\Omega) \cdot \prod h_i/h\,,$$

where W is the group of roots of unity in K and

$$A = \frac{l^u - 1}{l - 1} - u + \frac{1}{2}(m - 1)(\lambda - 1) - \frac{\kappa - 1}{2}\left(\frac{l^m - 1}{l - 1} - 1\right) - w\,.$$

In order to define w, we have to distinguish two cases:

(A) None of the k_i has the form $k_i = k(\sqrt{-1})$: then $w = 0$;

(B) $l = 2$ and $k_1 = k(\sqrt{-1})$, say; then $2^w = (W^{(2)} : W_1^{(2)})$, where $W^{(2)}$ (resp. $W_1^{(2)}$) is the 2-Sylow group of W (resp. W_1), and W_1 is the group of roots of unity in k_1.

It is easily seen that $2^w = (W : \prod W_i)$ (just remember that the field of p^nth roots of unity has cyclic Galois group over $\mathbb{Q}$ for $p > 2$). If we recall the fact that Kuroda's formula applies only if no infinite places ramify (which implies that $\lambda + 1 = l^m(\kappa + 1)$), the two formulae give the same result if and only if $\gamma := (E : E_\Omega)/2^w(E : WE_\Omega) = 1$. Obviously $\gamma = 1$ if $l > 2$; for $l = 2$ we obtain

$$(E : E_\Omega) = (E : WE_\Omega)(WE_\Omega : E_\Omega) = (E : WE_\Omega)(W : E_\Omega \cap W)\,.$$

Now $\prod W_i \subset E_\Omega \cap W$, therefore

$$(W : E_\Omega \cap W) = \Big(W : \prod W_i\Big) \Big/ \Big(E_\Omega \cap W : \prod W_i\Big)$$

and

$$\gamma = (E : E_\Omega)/2^w (E : WE_\Omega) = \Big(E_\Omega \cap W : \prod W_i\Big).$$

As can be seen, $\gamma = 1$ if and only if $W \cap \prod E_i = \prod W_i$, i.e. if and only if every root of unity that can be written as a product of units from the subfields, is actually a product of roots of unity lying in the subfields. If K does not contain the 8th roots of unity, this is certainly true; the following example shows that it does not hold in general. Take $k = \mathbb{Q}(\sqrt{3})$, $K = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}) = \mathbb{Q}(\zeta_{24})$; Walter's formula yields $h(K) = 2$; but $\mathbb{Z}[\zeta_{24}]$ is known to be Euclidean with respect to the norm, and therefore has class number 1.

Let $k_1 = k(i)$, $k_2 = k(\sqrt{2})$, $k_3 = k(\sqrt{-2})$; we define

$$\begin{gathered}
\varepsilon_2 = 1 + \sqrt{2}, \quad \varepsilon_3 = 2 + \sqrt{3}, \quad \varepsilon_6 = 5 + 2\sqrt{6}, \\
\sqrt{\varepsilon_3} = (1 + \sqrt{3})/\sqrt{2}, \quad \sqrt{\varepsilon_6} = \sqrt{2} + \sqrt{3}, \\
\sqrt{-\varepsilon_3} = (1 + \sqrt{3})/\sqrt{2}i, \quad \sqrt{i\varepsilon_3} = (1 + \sqrt{3})/(1 - i), \\
\sqrt{\zeta_8 \varepsilon_2 \sqrt{\varepsilon_3 \varepsilon_6}} = \frac{1}{4}(4 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6} + 2i + \sqrt{-2} + \sqrt{-6}).
\end{gathered}$$

Then $\kappa = 1$, $\lambda = 3$, $t_1 = 2$, $t_2 = 3$, $d = 2$, $u = 2$ since $k_1 = k(\sqrt{-1})$, $k_2 = k(\sqrt{\varepsilon_3})$, and $k_3 = k(\sqrt{-\varepsilon_3})$, $w = 1$ since $W = \langle \zeta_{24} \rangle$ and $W_1 = \langle \zeta_{12} \rangle$, and $q(K) = 2$ (in this example, the unit indices $(E : E_\Omega)$ and $(E : WE_\Omega)$ coincide, and in Wada [31] it is shown that $(E : E_\Omega) = 2$). Walter's formula gives

$$h(K) = \frac{1}{2} q(K) \cdot \prod h_i = \frac{1}{2} \cdot 2 \cdot 2 = 2.$$

We have also computed the groups that occur in our proof of Kuroda's formula:

- $E_k = \langle -1, \varepsilon_3 \rangle$;
- $E_1 = \langle \zeta_{12}, \sqrt{i\varepsilon_3} \rangle$, $E_1^* = \langle \zeta_{12}, \varepsilon_3 \rangle$, $E_1^N = \langle \varepsilon_3 \rangle$;
- $E_2 = \langle -1, \varepsilon_2, \sqrt{\varepsilon_3}, \sqrt{\varepsilon_6} \rangle$, $E_2^* = \langle -1, \varepsilon_2^2, \varepsilon_3, \sqrt{\varepsilon_6} \rangle$, $E_2^N = \langle -1, \varepsilon_3 \rangle$;
- $E_3 = \langle -1, \sqrt{-\varepsilon_3} \rangle$, $E_3^* = \langle -1, \varepsilon_3 \rangle$, $E_3^N = \langle \varepsilon_3 \rangle$;
- $\prod (E_i : E_i^*) = 2 \cdot 4 \cdot 2 = 16$;
- $H_0 = \langle \varepsilon_3 \rangle$; $H = H_0$, since -1 certainly is no norm residue mod ∞;
- $E = \langle \zeta_{24}, \varepsilon_2, \sqrt{\varepsilon_3}, \sqrt{\zeta_8 \varepsilon_2 \sqrt{\varepsilon_3 \varepsilon_6}} \rangle$ (cf. Wada [31]);
- $E_1 E_2 E_3 = \langle \zeta_{24}, \varepsilon_2, \sqrt{\varepsilon_3}, \sqrt{\varepsilon_6} \rangle$ ($\zeta_8 = \sqrt{i\varepsilon_3}/\sqrt{\varepsilon_3}$), $q(K) = 2$;
- $E^* = \langle \zeta_{12}, \varepsilon_2^2, \sqrt{i\varepsilon_3}, \sqrt{\varepsilon_6} \rangle$, $(E : E^*) = 8$, $(E_1 E_2 E_3 : E^*) = 4$;
- $E_1^* E_2^* E_3^* = \langle \zeta_{12}, \varepsilon_2^2, \varepsilon_3, \sqrt{\varepsilon_6} \rangle$, $(E^* : E_1^* E_2^* E_3^*) = 2$;
- $E^{(2)} = \langle i, \sqrt{\varepsilon_3} \rangle$;

- $\ker\psi = \{(\bar{1},\bar{1},\bar{1}),\ (iE_1^*, \sqrt{\varepsilon_3}E_2^*, \sqrt{-\varepsilon_3}E_3^*)\}$, because $i\cdot\sqrt{\varepsilon_3}\sqrt{-\varepsilon_3} = \varepsilon_3$ can be written in the form $\varepsilon_3 = \varepsilon_3\cdot 1\cdot 1 \in E_1^*E_2^*E_3^*$, while $\sqrt{\varepsilon_3} \notin E_2^*$.

The prime ideal $\mathbf{2}$ in k_3 above 2 generates an ideal class of order 2 in $\mathrm{Cl}(k_3)$: $\mathbf{2}$ is not principal, because its relative norm to $\mathbb{Q}(\sqrt{-6})$ is not, and its order divides 2 because $\mathbf{2}^2 = (1+\sqrt{3})$. This implies

$$|A_1| = |A_2| = 1, \qquad A_3 = \langle[\mathbf{2}]\rangle, \qquad \ker j = \ker j^* = 1\times 1\times A_3 \cong A_3\,.$$

References

[1] E. J. Amberg, *Über den Körper, dessen Zahlen sich rational aus zwei Quadratwurzeln zusammensetzen*, Diss., Zürich, 1897.

[2] P. Bachmann, *Zur Theorie der complexen Zahlen*, J. Reine Angew. Math. 67 (1867), 200–204.

[3] R. I. Berger, *Hasse's class number product formula for generalized Dirichlet fields and other types of number fields*, Manuscripta Math. 76 (1992), 397–406.

[4] C. Castela, *Nombre de classes d'idéaux d'une extension diédrale d'un corps de nombres*, C. R. Acad. Sci. Paris Sér. A 287 (1978), 483–486.

[5] G. L. Dirichlet, *Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes*, J. Reine Angew. Math. 24 (1842), 291–371.

[6] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. 29 (1967), 281–285.

[7] D. Garbanati, *Class field theory summarized*, Rocky Mountain J. Math. 11 (1980), 195–225.

[8] S. J. Gurak, *Ideal-theoretic characterization of the relative genus field*, J. Reine Angew. Math. 296 (1977), 119–124.

[9] F. Halter-Koch, *Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Anwendung auf biquadratisch-bizyklische Zahlkörper*, J. Number Theory 4 (1972), 144–156.

[10] H. Hasse, *Zahlbericht*, 3 Aufl., Physica, 1970.

[11] —, *Über die Klassenzahl abelscher Zahlkörper*, Springer, 1985.

[12] G. Herglotz, *Über einen Dirichletschen Satz*, Math. Z. 12 (1922), 255–261.

[13] C. S. Herz, *Construction of class fields*, in: Seminar on Complex Multiplication, Lecture Notes in Math. 21, Springer, 1957, VIII, 1–21.

[14] D. Hilbert, *Über den Dirichletschen biquadratischen Zahlkörper*, Math. Ann. 45 (1894), 309–340; see also: Gesammelte Abhandlungen I, Springer, 1970, 24–52.

[15] T. Kubota, *Über die Beziehung der Klassenzahlen der Unterkörper des bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. 6 (1953), 119–127.

[16] —, *Über den bizyklischen biquadratischen Zahlkörper*, ibid. 10 (1956), 65–85.

[17] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sec. I 4 (5) (1943), 383–406.

[18] —, *Über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. 1 (1950), 1–10.

[19] D. B. Leep and A. R. Wadsworth, *The transfer ideal of quadratic forms and a Hasse norm theorem mod squares*, Trans. Amer. Math. Soc. 315 (1989), 415–431.

[20] —, —, *The Hasse norm theorem mod squares*, J. Number Theory 42 (1992), 337–348.

[21] H. Nehrkorn, *Über absolute Idealklassengruppen und Einheiten in algebraischen Zahlkörpern*, Abh. Math. Sem. Univ. Hamburg 9 (1933), 318–334.
[22] Ch. J. Parry, *Real quadratic fields with class numbers divisible by five*, Math. Comp. 31 (1977), 1019–1029.
[23] —, *On the class number of relative quadratic fields*, ibid. 32 (1978), 1261–1270.
[24] Ch. Pitti, *Étude des normes dans les extensions à groupe de Klein*, C. R. Acad. Sci. Paris Sér. A 274 (1972), 1433–1435.
[25] —, *Étude des normes dans les extensions à groupe de Klein*, Séminaire Delange–Pisot–Poitou 14 (1972/73), no. 7.
[26] —, *Éléments de norme* 1 *dans les extensions à groupe de Klein*, C. R. Acad. Sci. Paris Sér. A 277 (1973), 273–275.
[27] H. Reichardt, *Über die Idealklassengruppe des Dirichletschen biquadratischen Zahlenkörpers*, Acta Arith. 21 (1972), 323–327.
[28] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen I*, J. Reine Angew. Math. 175 (1936), 100–107.
[29] —, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen II*, ibid. 182 (1940), 217–234.
[30] J. Varmon, *Über abelsche Körper, deren alle Gruppeninvarianten aus einer Primzahl l bestehen, und über abelsche Körper als Kreiskörper*, Akad. Abhandl., Lund, 1925.
[31] H. Wada, *On the class number and the unit group of certain algebraic number fields*, J. Fac. Sci. Univ. Tokyo 13 (1966), 201–209.
[32] C. D. Walter, *Kuroda's class number relation*, Acta Arith. 35 (1979), 41–51.

ERWIN-ROHDE-STR. 19
69120 HEIDELBERG, GERMANY

Received on 12.7.1993 (2461)