Brauer-Kuroda relations for S-class numbers

Bart de Smit
Mathematisch Instituut
Universiteit Leiden
Postbus 9512, 2300 RA Leiden
Netherlands
E-mail: desmit@math.leidenuniv.nl

Abstract. Let L/K be a Galois extension of number fields. The class number relations of Brauer and Kuroda relate class numbers and regulators of the intermediate fields of L/K. For specific Galois groups G one often avoids regulators by considering the index of certain subgroups of unit groups, and since this index is a positive integer one obtains inequalities for class numbers. There seems to be no canonical way to do this in general. In this note, we give a general unit index formula that depends on a choice of a homomorphism φ of permutation modules over G. With an optimal choice of φ one can sometimes obtain sharp inequalities between expressions in class numbers. As an application we extend Kuroda's class number formula for elementary abelian extensions to S-class numbers, and we show that for the well-known number fields of the form $K=\mathbb{Q}(\sqrt[8]{a})$ and $K'=\mathbb{Q}(\sqrt[8]{16a})$, the class number quotient $h(K)/h(K')$ is equal to 1 or 2 or 1/2.

1991 Mathematics subject classification: 11R29

Acknowledgement. The author was supported by a fellowship from the Koninklijke Nederlandse Akademie van Wetenschappen.

1. Introduction

The subject of "class number relations" started with investigations of Dirichlet in 1842 into the class number h of quartic fields of the form $\mathbb{Q}(\sqrt{d}, \sqrt{-1})$ for a positive integer d which is not a square. Dirirchlet observed that either h or $2h$ is equal to the product of the class numbers h_d and h_{-d} of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$. A much more general result, valid for arbitrary Galois extensions of number fields, was given independently by Brauer [2] and Kuroda [9] in 1950. Their theorem is an easy consequence of Artin's formalism of L-functions and the formula for the residues at 1 of zeta functions of number fields. It says that for any relation between the permutation characters associated to the subgroups of the Galois group an expression of class numbers of intermediate fields, such as $h/(h_d h_{-d})$ in Dirichlet's case, will be equal to a certain expression involving only the regulators and numbers of root of unity of the intermediate fields. See (2.1) below for a precise statement.

For many specific types of Galois groups, this regulator expression can be written in terms of a unit index. In Dirichtlet's case, $2h/(h_d h_{-d})$ is the index in the unit group of $\mathbb{Q}(\sqrt{d}, \sqrt{-1})$ of the subgroup generated by the roots of unity and the unit group of $\mathbb{Q}(\sqrt{d})$. Such an index formula gives rise to divisibility relations between products of class numbers: $h_d h_{-d}$ divides $2h$. These explicit results get more complicated when the base field has non-trivial class group or postive unit rank. Even for the well-studied case of abelian extensions of type $(2, 2)$, a correct index formula only appeared in full generality in a paper of Lemmermeyer [11] in 1994. See Scholz [13], Walter [16, 15], Jehne [7] and Jaulent [6] for further examples and references.

In this paper we will show how to deduce index-formulas and divisibility results for class numbers from the result of Brauer and Kuroda in a systematic way. The method also works in the more general setting of S-class numbers. We will apply our result to arbitrary elementary abelian extensions and thus find Kuroda's class number formula for S-class numbers.

Both the index formula and the divisibility relation will depend on the choice of a homomorphism φ between permutation modules. The symbolic computations one needs to perform for specific small Galois groups in order to find those φ that give the strongest results on class numbers, can be carried out by computer. We refer to [1] for computational aspects, implementation issues, further examples, and an improvement in certain cases of the bound B in (2.2).

For the special case of number fields with identical zeta functions we get a more conceptual approach to techniques that have been used by Perlis in the seventies [12, 8]. A certain functoriality in φ now becomes clear. For the well-known fields $\mathbb{Q}(\sqrt[8]{a})$ and $\mathbb{Q}(\sqrt[8]{16a})$, that were considered by Perlis, this leads to sharp inequalities between the class numbers.

2. Main theorem

Let K be a number field and let G be a finite group that acts on K by field automorphisms. Let S be a finite G-stable set of primes of K that includes the infinite primes of K.

By a G-set we mean a finite set with a left-action of G. For a G-set X the set K_X of G-equivariant maps $X \to K$ is a finite étale algebra, i.e., a product of number fields. We call these number fields the components of K_X. The components of K_X correspond to G-orbits of X, and for $x \in X$ the component corresponding to the orbit Gx is isomorphic as a field to the field K^H of H-invariants in K, where H is the stabilizer of x in G.

All invariants for number fields can be extended to étale algebras: we write $h(K_X)$ and $R(K_X)$ for the product of the S-class numbers and S-regulators of the components of K_X. We write $\mu(K_X)$ for the torsion subgroup of K_X^*, and denote its order by $w(K_X)$. We let $U(K_X)$ be the product of the groups of S-units of the components of K_X.

For a G-set X the permutation character π_X of G is the map from $G \to \mathbb{Z}$ that sends $g \in G$ to the number of fix-points of g in X.

Let X and Y be two G-sets for which $\pi_X = \pi_Y$. Such G-sets are called linearly equivalent. Giving X and Y is our way to give what several authors call a "character relation", or "Brauer relation". If we let $\mathcal{H}$ be a set of representatives of the conjugacy classes of subgroups of G, and we define for $H \in \mathcal{H}$ the integer $a_H(X)$ to be the number of G-orbits of X containing a point whose stabilizer is equal to H, then the linear equivalence of X and Y can be expressed more traditonally by the character relation

$$\sum_{H \in \mathcal{H}} a_H(X) \cdot 1_H^G = \sum_{H \in \mathcal{H}} a_H(Y) \cdot 1_H^G.$$

The S-zeta function of a subfield F of K is the meromorphic function on $\mathbb{C}$ which for $\mathrm{Re}(s) > 1$ is defined by

$$\zeta_{F,S}(s) = \sum_{\mathfrak{a}} (\mathrm{N}\mathfrak{a})^{-s},$$

where $\mathfrak{a}$ ranges over all integral ideals of F that are coprime to the finite primes in S, and $\mathrm{N}\mathfrak{a}$ is the norm of $\mathfrak{a}$. See Tate [14, Chap. I] for details. The S-zeta function of K_X is the product of the S-zeta functions of its components, which is also equal to the Artin L-series $L_S(s, \pi_X)$. Since $\pi_X = \pi_Y$ the algebras K_X and K_Y have the same S-zeta function. This is sometimes expressed by saying that K_X and K_Y are *arithmetically equivalent*. The absolute value of the leading coefficient Taylor expansion at 0 of the S-zeta function of K_X is equal to $h(K_X)R(K_X)/w(K_X)$; see [14, Chap. I, Cor. 2.2]. Thus, we have a version for S-class numbers and S-regulators of the theorem of Brauer and Kuroda [2, 9]:

$$\frac{h(K_X)R(K_X)}{w(K_X)} = \frac{h(K_Y)R(K_Y)}{w(K_Y)}. \tag{2.1}$$

For any ring R we denote the group ring of G over R by RG or $R[G]$, and for any G-set T we define the left RG-module $RT = R[T]$ as the free R-module on T with G permuting T. The fact that $\pi_X = \pi_Y$ implies that $\mathbb{Q}X$ is isomorphic to $\mathbb{Q}Y$ as a $\mathbb{Q}G$-module; see [10, Chap. XVIII, Th. 2.3]. This means that we can choose an injective $\mathbb{Z}G$-linear homomorphism

$$\varphi \colon \mathbb{Z}X \longrightarrow \mathbb{Z}Y$$

with a finite cokernel $\mathrm{Cok}\,\varphi$. It will be important later to choose φ in a particular way, but since there is no canonical way, we just formulate our results in terms of φ.

For two $\mathbb{Z}G$-modules P and M we write $(P, M) = \mathrm{Hom}_{\mathbb{Z}G}(P, M)$. Let U be the group of S-units of K. Then the group $U(K_X) = (\mathbb{Z}X, U)$ is the product of the groups of S-units of the components of K_X, and our map φ induces a group homomorphism

$$(\varphi, U)\colon\ U(K_Y) = (\mathbb{Z}Y, U) \longrightarrow (\mathbb{Z}X, U) = U(K_X).$$

When we tensor this map with $\mathbb{Q}$ we obtain the map $(\varphi, U \otimes_{\mathbb{Z}} \mathbb{Q})$, which is an isomorphism because φ induces an isomorphism $\mathbb{Q}X \to \mathbb{Q}Y$. Since $U(K_Y)$ and $U(K_X)$ are finitely generated abelian groups, it follows that the map (φ, U) has finite kernel and cokernel.

For a finite $\mathbb{Z}G$-module E we define

$$B(S, E) = \frac{\#(\mathbb{Z}S, E)}{\#(\mathbb{Z}, E)}.$$

Here we view $\mathbb{Z}$ as a $\mathbb{Z}G$-module by letting G act trivially, so $(\mathbb{Z}, E) \cong E^G$. Similarly, $(\mathbb{Z}S, E)$ is the product, over a set of G-orbit representatives $\mathfrak{p}$ of S, of $E^{D_\mathfrak{p}}$, where $D_\mathfrak{p}$ is the stabilizer of $\mathfrak{p}$ in G. Since S is non-empty, $B(S, E)$ is a positive integer. The main result of this paper is the following.

(2.2) Theorem. *Let $B = B(S, \operatorname{Cok}\varphi)$. Then we have*

$$\frac{h(K_Y)}{h(K_X)} = B \cdot \frac{\#\operatorname{Ker}(\varphi, U)}{\#\operatorname{Cok}(\varphi, U)} \ \mid\ B \cdot \frac{w(K_Y)}{w(K_X)}.$$

Here the symbol "|" means "divides", so for $x, y \in \mathbb{Q}^*$ we have $x \mid y$ if and only if $y/x \in \mathbb{Z}$. We prove this Theorem in Section 3.

It is a famous result of Brauer [2] that the left hand side in (2.2) only assumes finitely many values when G and the G-sets X and Y are fixed, and K ranges over the Galois extensions of $\mathbb{Q}$ with Galois group G. The Theorem gives an explicit upper bound for $h(K_X)/h(K_Y)$ depending on the choice of the map φ. To get a lower bound one switches the role of X and Y.

To get the best bound possible in (2.2) one has to choose φ is such a way that $B(S, \operatorname{Cok}\varphi)$ is minimal. For a specific Brauer relation the computational problem that this leads to is to minimize, for each prime p dividing the order of G, the number of factors p in the value of a certain multivariate polynomial with coefficients in $\mathbb{Z}$ outside the zero-set of some other multivariate polynomial. We refer to [1] for details and a better algorithm.

For specific G it is often helpful to use functoriality in φ rather than a single application of (2.2). We will illustrate this in Sections 4 and 5.

3. Proof of the theorem.

First, we define a norm-map in a general setting. Let P and M be left $\mathbb{Z}G$-modules. Then $\mathrm{Hom}_{\mathbb{Z}}(P,\mathbb{Z})$ is a right $\mathbb{Z}G$-module, and we write $\langle P,M\rangle = \mathrm{Hom}_{\mathbb{Z}}(P,\mathbb{Z})\otimes_{\mathbb{Z}G} M$. We now define the norm-homomorphism as the map

$$\langle P,M\rangle = \mathrm{Hom}_{\mathbb{Z}}(P,\mathbb{Z})\otimes_{\mathbb{Z}G} M \xrightarrow{N} \mathrm{Hom}_{\mathbb{Z}G}(P,M) = (P,M)$$

that sends $\varphi\otimes m$ to the homomorphism $x\mapsto \sum_{g\in G}\varphi(g^{-1}x)gm$. Note that this map is a natural transformation of functors in M and of contravariant functors in P. For $P = \mathbb{Z}[G/H]$ we recover the familiar norm map $N_H\colon M_H \to M^H$ from the H-coinvariants to the H-invariants of M. We first give a purely algebraic result.

(3.1) Lemma. *For any G-set T the cokernel of $\langle\varphi,\mathbb{Z}T\rangle$ is canonically isomorphic to the $\mathbb{Q}/\mathbb{Z}$-dual of $(\mathbb{Z}T,\mathrm{Cok}\,\varphi)$. In particular, $\#\,\mathrm{Cok}\langle\varphi,\mathbb{Z}T\rangle = \#(\mathbb{Z}T,\mathrm{Cok}\,\varphi)$.*

Proof. One obtains the map $\langle\varphi,\mathbb{Z}T\rangle$ out of φ in two steps: one first applies the functor $\mathrm{Hom}_{\mathbb{Z}}(-,\mathbb{Z})$ from the category of left $\mathbb{Z}G$-modules to the category of right $\mathbb{Z}G$-modules, and then the functor $-\otimes_{\mathbb{Z}G}\mathbb{Z}T$.

For $f\in\mathrm{Hom}(\mathbb{Z}X,\mathbb{Z})$ we consider the composite map

$$\mathbb{Z}Y \longrightarrow \mathbb{Z}Y\otimes\mathbb{Q} \xrightarrow{(\varphi\otimes 1)^{-1}} \mathbb{Z}X\otimes\mathbb{Q} \xrightarrow{f\otimes 1} \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Since this composition vanishes on $\varphi(\mathbb{Z}X)$, we obtain from f an induced homomorphism $\mathrm{Cok}\,\varphi\to\mathbb{Q}/\mathbb{Z}$. Writing $M = \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Cok}\,\varphi,\mathbb{Q}/\mathbb{Z})$ it is not hard to see that we thus get an exact sequence of right $\mathbb{Z}G$-modules

$$0\longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}Y,\mathbb{Z})\longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}X,\mathbb{Z})\longrightarrow M\longrightarrow 0.$$

By taking the tensor product over $\mathbb{Z}G$ with the left $\mathbb{Z}G$-module $\mathbb{Z}T$ we get a right exact sequence showing that $\mathrm{Cok}\langle\varphi,\mathbb{Z}T\rangle\cong M\otimes_{\mathbb{Z}G}\mathbb{Z}T$. The $\mathbb{Q}/\mathbb{Z}$-dual of this abelian group is

$$\mathrm{Hom}_{\mathbb{Z}}(M\otimes_{\mathbb{Z}G}\mathbb{Z}T,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}T,\mathrm{Hom}(M,\mathbb{Q}/\mathbb{Z}))$$

and by duality of finite abelian groups, this last group is $(\mathbb{Z}T,\mathrm{Cok}\,\varphi)$. This proves the Lemma.

We now prove (2.2). For $\mathfrak{p}\in S$ let $||\cdot||_{\mathfrak{p}}$ be the normalized valuation on K. This means that for a Haar measure on the completion $K_{\mathfrak{p}}$, an open set $O\subset K_{\mathfrak{p}}$ and any $x\in K^*$, we have $\mathrm{vol}(xO) = ||x||_{\mathfrak{p}}\,\mathrm{vol}(O)$. The product formula says that $\prod_{\mathfrak{p}\in S}||u||_{\mathfrak{p}} = 1$ for all $u\in U_S(K)$. For $\mathfrak{p}\in S$ let $n_{\mathfrak{p}}$ be the local degree of $\mathfrak{p}$, i.e., the degree of the completion of K at $\mathfrak{p}$ as an extension field of the completion of $\mathbb{Q}$. Now let $n = \sum_{\mathfrak{p}\in S} n_{\mathfrak{p}}$ and define the map $l = l(K)$ by

$$l\colon\ \mathbb{Z}\oplus U \longrightarrow \mathbb{R}S \qquad (a,u)\mapsto \sum_{\mathfrak{p}\in S}(a\frac{n_{\mathfrak{p}}}{n} + \log||u||_{\mathfrak{p}})\cdot\mathfrak{p}.$$

It follows from the Dirichlet unit theorem for S-units that the image of l is a cocompact lattice in $\mathbb{R}S$ and that the kernel of l is $\mu(K)$. If we write $S = \{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$ and we have a system of fundamental S-units $\{\epsilon_1,\dots,\epsilon_{r-1}\}$ for K, then the image of l is generated by the columns of the matrix

$$\begin{pmatrix} n_{\mathfrak{p}_1}/n & \log||\epsilon_1||_{\mathfrak{p}_1} & \cdots & \log||\epsilon_{r-1}||_{\mathfrak{p}_1} \\ \vdots & \vdots & & \vdots \\ n_{\mathfrak{p}_r}/n & \log||\epsilon_1||_{\mathfrak{p}_r} & \cdots & \log||\epsilon_{r-1}||_{\mathfrak{p}_r} \end{pmatrix}.$$

Recall that $R(K) = \det(\log||\epsilon_i||_{\mathfrak{p}_j})_{i,j=1}^{r-1}$ and that $\sum_{i=1}^{r} n_{\mathfrak{p}_i}/n = 1$. By adding rows 1 through $r-1$ to row r and using the product formula we see that

$$R(K) = \frac{\operatorname{covol}(\operatorname{Im} l(K))}{\operatorname{covol}(\mathbb{Z}S)} \tag{3.2}$$

for any Haar measure on the real vector space $\mathbb{R}S$. This interpretation of the S-regulator of K is based on comparing the images of two G-linear maps

$$\mathbb{Z}\oplus U \xrightarrow{\ l\ } \mathbb{R}S \xleftarrow{\ i\ } \mathbb{Z}S.$$

Applying the functor $(\mathbb{Z}[X], -)$ we get homomorphisms

$$(\mathbb{Z}X,\mathbb{Z})\oplus U(K_X) \longrightarrow (\mathbb{Z}X,\mathbb{R}S) \longleftarrow (\mathbb{Z}X,\mathbb{Z}S).$$

We now define the maps l_X and i_X by first composing with norm maps:

$$\langle\mathbb{Z}X,\mathbb{Z}\rangle\oplus U(K_X) \xrightarrow{\ l_X\ } (\mathbb{Z}X,\mathbb{R}S) \xleftarrow{\ i_X\ } \langle\mathbb{Z}X,\mathbb{Z}S\rangle.$$

The kernel of l_X is the torsion subgroup of $U(K_X)$, and i_X is injective.

(3.3) Lemma. *For any Haar measure on $(\mathbb{Z}X,\mathbb{R}S)$ we have*

$$\frac{\operatorname{covol}(\operatorname{Im} l_X)}{\operatorname{covol}(\operatorname{Im} i_X)} = R(K_X).$$

Proof. It suffices to consider transitive X, so take $X = G/H$ for some subgroup H of G. Then $K_X = K^H$ and the set of primes of K_X which extend to primes in S is

$T = H\backslash S$, the set of H-orbits of S. We therefore have $\mathbb{Z}T = (\mathbb{Z}S)_H$. For every $\mathfrak{q} \in S$ restricting to $\mathfrak{p} \in T$ we have $n_\mathfrak{q} = [K_\mathfrak{q} : (K^H)_\mathfrak{p}] \cdot n_\mathfrak{p}$, and for every $x \in K^H$ we have $||x||_\mathfrak{q} = ||x||_\mathfrak{p}^{n_\mathfrak{q}/n_\mathfrak{p}}$. One deduces from this that the diagram

$$\begin{array}{ccccc} \mathbb{Z} \oplus U^H & \xrightarrow{l(K^H)} & (\mathbb{R}S)_H & \longleftarrow & (\mathbb{Z}S)_H \\ \Big\downarrow{\scriptstyle (\#H, \mathrm{id})} & & \Big\downarrow{\scriptstyle N_H} & & \Big\downarrow{\scriptstyle N_H} \\ \mathbb{Z} \oplus U^H & \xrightarrow{l(K)} & (\mathbb{R}S)^H & \longleftarrow & (\mathbb{Z}S)^H \end{array}$$

commutes. Note that the induced maps from the upper corners to $(\mathbb{R}S)^H$ are the maps l_X and i_X. Lemma (3.3) now follows by applying (3.2) with K replaced by K^H.

We continue the proof of (2.2). By the functorial properties of N the homomorphism φ induces a commutative diagram

$$\begin{array}{ccccc} \langle \mathbb{Z}Y, \mathbb{Z}\rangle \oplus U(K_Y) & \xrightarrow{l_Y} & (\mathbb{Z}Y, \mathbb{R}S) & \xleftarrow{i_Y} & \langle \mathbb{Z}Y, \mathbb{Z}S\rangle \\ \Big\downarrow{\scriptstyle \langle\varphi,\mathbb{Z}\rangle\oplus(\varphi,U)} & & \Big\downarrow{\scriptstyle \varphi^*} & & \Big\downarrow{\scriptstyle \langle\varphi,\mathbb{Z}S\rangle} \\ \langle \mathbb{Z}X, \mathbb{Z}\rangle \oplus U(K_X) & \xrightarrow{l_X} & (\mathbb{Z}X, \mathbb{R}S) & \xleftarrow{i_X} & \langle \mathbb{Z}X, \mathbb{Z}S\rangle, \end{array}$$

where φ^* is an isomorphism of finite dimensional real vector spaces. Now choose a Haar measure on $(\mathbb{Z}X, \mathbb{R}S)$. Since i_X and i_Y are injective we have

$$\frac{\mathrm{covol}(\mathrm{Im}(\varphi^* \circ i_Y))}{\mathrm{covol}(\mathrm{Im}\, i_X)} = \#\,\mathrm{Cok}\langle\varphi, \mathbb{Z}S\rangle. \tag{3.4}$$

The kernels of l_X and l_Y are $\mu(K_X)$ and $\mu(K_Y)$. Let Q be the index of the subgroup of $U(K_X)$ generated by $\mu(K_X)$ and the image under (φ, U) of $U(K_Y)$. Then we have

$$\frac{\mathrm{covol}(\mathrm{Im}(\varphi^* \circ l_Y))}{\mathrm{covol}(\mathrm{Im}\, l_X)} = Q \cdot \#\,\mathrm{Cok}\langle\varphi, \mathbb{Z}\rangle.$$

Dividing this equation by (3.4) using Lemma (3.3) twice we find

$$\frac{R(K_Y)}{R(K_X)} = \frac{Q \cdot \#\,\mathrm{Cok}\langle\varphi, \mathbb{Z}\rangle}{\#\,\mathrm{Cok}\langle\varphi, \mathbb{Z}S\rangle}.$$

By (3.1) this is equal to Q/B. Using (2.1) we deduce that

$$\frac{h(K_Y)}{h(K_X)} = \frac{R(K_X)}{R(K_Y)} \cdot \frac{w(K_Y)}{w(K_X)} = \frac{B}{Q} \cdot \frac{w(K_Y)}{w(K_X)}.$$

Since Q is a positive integer this gives the divisibility relation in (2.2). In order to obtain the equality one considers the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu(K_Y) & \longrightarrow & U(K_Y) & \longrightarrow & U(K_Y)/\mu(K_Y) & \longrightarrow & 0 \\ & & \Big\downarrow & & \Big\downarrow{\scriptstyle (\varphi, U)} & & \Big\downarrow & & \\ 0 & \longrightarrow & \mu(K_X) & \longrightarrow & U(K_X) & \longrightarrow & U(K_X)/\mu(K_X) & \longrightarrow & 0. \end{array}$$

The rightmost vertical map is injective, and its cokernel has order Q, so by the snake lemma we have

$$\frac{w(K_Y)}{Q \cdot w(K_X)} = \frac{\#\,\mathrm{Ker}(\varphi, U)}{\#\,\mathrm{Cok}(\varphi, U)}.$$

This completes the proof of (2.2).

4. Kuroda's formula for S-class numbers.

In this section we apply the theorem to a particular character relation for an abelian Galois group G of type $(p, p, \ldots, p)$ with p a prime number.

For ordinary class numbers (the case that S has only infinite primes), this class number formula has a long history. The case $p = 2$ with base field $\mathbb{Q}$ was analyzed by Herglotz [5] in 1921. In 1950 Kuroda [9] gave the formula for Galois extensions of type $(p, p, \ldots, p)$ without ramification at infinity. Walter [16] gave a version in 1979 that does allow ramification at infinity, but Lemmermeyer [11] pointed out that Walter's formula has a mistake for type $(2, 2)$, and he gave a correct formula for arbitrary extensions of type $(2, 2)$. We now give a general formula which also allows for more general S-class numbers.

Let p be a prime number and let $m \geq 2$. Let K/F be a Galois extension of number fields with Galois group $G \cong (\mathbb{Z}/p\mathbb{Z})^m$, and let S be a finite G-stable set of primes of K, containing the infinite primes. For $k \geq 0$ let $q(k) = (p^k - 1)/(p - 1)$. The group G has $g = q(m)$ subgroups $H_1, \ldots, H_g$ of index p. The fields $K_i = K^{H_i}$, with $i = 1, \ldots, g$ are the cyclic extensions of F within K of degree p. For $k = 0, \ldots, m$ let s_k be the number of G-orbits of S of length p^{m-k}, i.e., the number of primes of F extending to a prime of L in S with relative local degree p^k. Thus, $s_2 = \cdots = s_m = 0$ when S consists only of infinite primes.

(4.1) Proposition. *For $k \geq 2$ let t_k be given by*

$$t_k = -g + \frac{1}{2}\left((2m - k - 1)p^k + q(k) + 1\right).$$

Define $r \in \{0, \ldots, m\}$ by $p^r = [K \cap F(\sqrt[p]{U(F)}\,) : F]$ and A by

$$A = q(r) - r - t_0 + t_m s_0 + t_{m-1} s_1 + \cdots + t_0 s_m.$$

Then we have

$$\frac{h(K)h(F)^{g-1}}{h(K_1)\cdots h(K_g)} = p^{-A}\,[U(K) : U(K_1)\cdots U(K_g)].$$

(4.2) Remark. In the case of an extension of type $(2, 2)$ we have $g = 3$ and

$$A = \begin{cases} 2 + s_0 - s_2 & \text{if } K \subset F\left(\sqrt{U(F)}\,\right) \\ 1 + s_0 - s_2 & \text{otherwise.} \end{cases}$$

Proof. First let us specify a $\mathbb{Z}G$-linear homomorphism

$$\varphi\colon \mathbb{Z}G \oplus \mathbb{Z}^g \longrightarrow \mathbb{Z} \oplus \prod_{i=1}^{g} \mathbb{Z}[G/H_i]$$

by setting $\varphi(\sigma, 0) = (1, (\sigma H_i)_i)$ for $\sigma \in G$, and $\varphi(0, (n_i)_i) = (0, (n_i N_i)_i)$ where $N_i = \sum_{x \in G/H_i} x \in \mathbb{Z}[G/H_i]$.

We will first show that the $\mathbb{Z}G$-module $E = \operatorname{Cok} \varphi$ is finite, and compute $\# E$. For a cyclic group C of order p let $\mathbb{Z}(C) = \mathbb{Z}[C]/N_C \mathbb{Z}C$, where $N_C = \sum_{c \in C} c \in \mathbb{Z}C$. It is clear that φ is injective on $0 \oplus \mathbb{Z}^g$. By considering the map φ modulo the image of $0 \oplus \mathbb{Z}^g$, we see that φ has the same kernel and cokernel as the induced map

$$\psi \colon \mathbb{Z}G \longrightarrow \mathbb{Z} \times \prod_{i=1}^{g} \mathbb{Z}(G/H_i).$$

Note that $\psi \otimes \mathbb{Q}$ is the ring isomorphism giving the product decomposition of the étale algebra $\mathbb{Q}G$ into components. Thus, φ is injective, and $\# E = \# \operatorname{Cok} \psi$ is finite.

(4.3) Lemma. *For every $k \in \{0, \ldots, m\}$ and every subgroup D of G of index p^k we have $\# E^D = p^{t_k + g}$.*

Proof. Recall that for algebras $A_1 \subset A_2$ that are finitely generated and free as $\mathbb{Z}$-modules, we have an index formula for discriminants:

$$\Delta(A_1) = \Delta(A_2)[A_2 : A_1]^2.$$

We have $|\Delta(\mathbb{Z}G)| = p^{mp^m}$ and $|\Delta(\mathbb{Z}(C))| = p^{p-2}$ for a cyclic group C of order p. It follows that $\# E = p^{e(m)}$, where for $l \geq 0$ we let

$$e(l) = \frac{1}{2}\left(lp^l - q(l)(p-2)\right) = \frac{1}{2}\left((l-1)p^l + q(l) + 1\right).$$

Let $N_D \in \mathbb{Z}G$ be the formal sum of the elements of D. Then $(\mathbb{Z}G)^D = (\mathbb{Z}G) \cdot N_D$ and the sequence

$$0 \longrightarrow \mathbb{Z}G \cdot N_D \xrightarrow{\psi^D} \mathbb{Z} \times \prod_{\substack{i=1,\ldots,g \\ H_i \supset D}} \mathbb{Z}(G/H_i) \longrightarrow E^D \longrightarrow 0$$

is exact because $H^1(D, \mathbb{Z}G) = 0$. Applying what we have showed already with G replaced by G/D, we see that the canonical image R of the ring $\mathbb{Z}[G/D]$ in the middle group has index $p^{e(k)}$. The image of ψ^D is $(\# D)R = p^{m-k}R$ and R has $\mathbb{Z}$-rank p^k, so it follows that $\# E^D = (p^{m-k})^{p^k} p^{e(k)} = p^{t_k + g}$. This proves the Lemma.

We continue the proof of (4.1). We will apply our main theorem not only to φ, but also to the the induced map φ_G on G-coinvariants. Note that we have a commutative diagram of $\mathbb{Z}G$-modules

$$\begin{array}{ccc} \mathbb{Z}G \oplus \mathbb{Z}^g & \longrightarrow & \mathbb{Z}^{g+1} \\ \Big\downarrow{\scriptstyle \varphi} & & \Big\downarrow{\scriptstyle \varphi_G} \\ \mathbb{Z} \oplus \prod_{i=1}^{g} \mathbb{Z}[G/H_i] & \longrightarrow & \mathbb{Z}^{g+1}, \end{array}$$

where the horizontal maps are given by the augmentation map on each summand. Note that $\operatorname{Cok}\varphi_G = E_G$ because taking coinvariants is right exact, and that $\operatorname{Cok}\varphi_G \cong (\mathbb{Z}/p\mathbb{Z})^g$. Applying the functor $(-, U(K))$ to the diagram we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U(F)^{g+1} & \longrightarrow & U(F) \oplus \prod_{i=1}^g U(K_i) & \longrightarrow & \prod_{i=1}^g U(K_i)/U(F) & \longrightarrow & 0 \\
 & & \big\downarrow{\scriptstyle (\varphi_G, U)} & & \big\downarrow{\scriptstyle (\varphi, U)} & & \big\downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & U(F)^{g+1} & \longrightarrow & U(K) \oplus U(F)^g & \longrightarrow & U(K)/U(F) & \longrightarrow & 0,
\end{array}$$

in which the rightmost vertical map f is the homomorphism induced by the inclusions $U(K_i)/U(F) \subset U(K)/U(F)$. Applying (2.2) to φ and to φ_G we see that

$$\begin{aligned}
\frac{h(K)h(F)^{g-1}}{h(K_1)\cdots h(K_g)} &= \left(\frac{B(S,E)\#\operatorname{Ker}(\varphi,U)}{\#\operatorname{Cok}(\varphi,U)}\right)^{-1}\left(\frac{B(S,E_G)\#\operatorname{Ker}(\varphi_G,U)}{\#\operatorname{Cok}(\varphi_G,U)}\right) \\
&= \frac{B(S,E_G)}{B(S,E)}\cdot\frac{\#\operatorname{Cok} f}{\#\operatorname{Ker} f}.
\end{aligned}$$

The last equality follows by applying the snake lemma to the diagram above.

In order to compute the B-factors, note first that $\#E_G = \#\operatorname{Cok}\varphi_G = p^g$. Let $S' \subset S$ be a set of representatives for the G-orbits of S and for $\mathfrak{p} \in S'$ let $D_\mathfrak{p}$ be the stabilizer of $\mathfrak{p}$ in G. Then we see with Lemma (4.3) that

$$\frac{B(S,E)}{B(S,E_G)} = \frac{\#E_G}{\#E^G}\prod_{\mathfrak{p}\in S'}\frac{\#E^{D_\mathfrak{p}}}{\#E_G} = p^{-t_0+t_m s_0+\cdots+t_0 s_m}.$$

It is clear that $\#\operatorname{Cok} f = [U(K) : U(K_1)\cdots U(K_g)]$, so it remains to show that we have $\#\operatorname{Ker} f = p^{q(r)-r}$. Suppose we have $u_i \in U(K_i)$ for $i = 1,\ldots,g$ with $u_1\cdots u_g \in U(F)$. For $j \neq i$ we have $\#(H_i \cap H_j) = p^{m-2}$, so the norm map N_{H_i} maps $U(K_j)$ within $U(F)^{p^{m-2}}$. Since $N_{H_i}(u_i) = u_i^{p^{m-1}}$ we can deduce that $u_i^{p^{m-1}} \in U(F)^{p^{m-2}}$ for all i. This means that for each i we can write $u_i^p = \zeta_i v_i$ with $\zeta_i \in K_i$, $v_i \in U(F)$ and $\zeta_i^{p^{m-2}} = 1$. Now let i be such that $\#\langle\zeta_i\rangle$ is maximal. Then we see that for $j \neq i$ we have $\zeta_j \in K_j \cap K_i = F$ and $u_j^p \in U(F)$. Since we have $\zeta_1\cdots\zeta_g \in F$, it follows that also $\zeta_i \in F$ and $u_i^p \in U(F)$. This proves that the kernel of f is annihilated by p. Kummer theory tells us that the p-torsion subgroups of the domain and codomain of f have ranks $q(r)$ and r respectively. Again by Kummer theory, f gives a surjection from the first to the second, so $\operatorname{Ker} f$ has rank $q(r) - r$. This proves (4.1).

5. An application to arithmetically equivalent fields

The best known examples of non-isomorphic number fields with the same zeta-function are the fields of the form $K = \mathbb{Q}(\sqrt[8]{a})$ and $K' = \mathbb{Q}(\sqrt[8]{16a})$, where a is an integer for which both $|a|$ and $2|a|$ are not squares.

(5.1) Proposition. *The class numbers h and h' of K and K' satisfy $h/h' \in \{\frac{1}{2}, 1, 2\}$.*

All three values $\frac{1}{2}, 1, 2$ actually occur for some a; see [3]. For instance, for $a = -15$ and for $a = 66$ we have $h/h' = 2$. Replacing a by $16a$ switches K and K'.

We first identify the Galois group. Let $\alpha = \sqrt[8]{a}$, and let ζ be a primitive 8-th root of unity. Then $L = \mathbb{Q}(\alpha, \zeta)$ is the Galois closure of K, and we have an embedding $K' \subset L$ that identifies $\sqrt[8]{16a}$ with $(\zeta + \zeta^{-1})\alpha$. The Galois group G of L over $\mathbb{Q}$ is the group of affine linear transformations of $\mathbb{Z}/8\mathbb{Z}$, i.e., the group of permutations T_a^b: $x \mapsto ax + b$ of $\mathbb{Z}/8\mathbb{Z}$ with $a \in (\mathbb{Z}/8\mathbb{Z})^*$ and $b \in \mathbb{Z}/8\mathbb{Z}$. The group G permutes the roots of $X^8 - a$ by $T_a^b(\zeta^i\alpha) = \zeta^{ai+b}\alpha$. Putting $H = \mathrm{Gal}(L/K)$ and $H' = \mathrm{Gal}(L/K')$, one checks that $H = \{T_a^b \in G : b = 0\}$, and $H' = \langle T_{-1}^0, T_3^4 \rangle$. Let S be the G-set of infinite primes of L.

Assume for the moment that we have an injective G-linear homomorphism

$$\varphi\colon \mathbb{Z}[G/H] \longrightarrow \mathbb{Z}[G/H'].$$

We will explicitly give such a φ below.

By (2.2) we then have $h' \mid B(S, E)h$, where $E = \mathrm{Cok}\,\varphi$. One can now minimize $B(S, E)$ over all choices of φ. This rephrases Perlis' method [12], and it gives $h' \mid 16h$ if $a > 0$ and $h' \mid 4h$ if $a < 0$. It turns out that with double modules, i.e., a map $\mathbb{Z}[G/H]^2 \to \mathbb{Z}[G/H']^2$, one can improve the result for $a > 0$ to $h' \mid 8h$. Rather than such a direct application of (2.2) we will use a relative version of this argument, which uses the fact that K and K' both contain the field $F = \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt[4]{a})$.

Let $N = \mathrm{Gal}(L/F) \subset G$. The center of G is $Z = \langle T_1^4 \rangle$, and we have $N = ZH = ZH'$. Taking Z-coinvariants we obtain a commutative diagram of $\mathbb{Z}G$-modules

(5.2)
$$\begin{array}{ccccccc} & & \mathbb{Z}[G/H] & \xrightarrow{\varphi} & \mathbb{Z}[G/H'] & & \\ & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi'} & & \\ \mathbb{Z}[G/H]_Z & = & \mathbb{Z}[G/N] & \xrightarrow{\varphi_Z} & \mathbb{Z}[G/N] & = & \mathbb{Z}[G/H']_Z, \end{array}$$

where π and π' are the canonical projection maps. Put $E = \mathrm{Cok}\,\varphi$. Then we have $E_Z = \mathrm{Cok}\,\varphi_Z$. We now apply the functor $\mathrm{Hom}_{\mathbb{Z}G}(-, U)$, where U is the group of units of L, and we obtain an induced diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U(F) & \longrightarrow & U(K') & \longrightarrow & U(K')/U(F) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle(\varphi_Z, U)} & & \downarrow{\scriptstyle(\varphi, U)} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & U(F) & \longrightarrow & U(K) & \longrightarrow & U(K)/U(F) & \longrightarrow & 0. \end{array}$$

We claim that $U(K')/U(F)$ is torsion free. To see this, suppose that the image of $u \in U(K')$ in $U(K')/U(F)$ is a non-trivial p-torsion element for a prime number p. Writing $v = u^p \in F$ we see that $v^2 = N_{K'/F}(u)^p \in F^p$. If p is odd then it follows that $v \in F^p$ so that $u^p = w^p$ for some $w \in F$. But then $u/w \in \mu(K') \subset \mu(F)$ so that $u \in F$. So we have $p = 2$, and $K' = F(\sqrt{v})$, which implies that K'/F is only ramified at primes of F that lie over 2. But our assumption on a is that it $\mathrm{ord}_l(a)$ is odd for some odd prime number l, and this l is then totally ramified in $K'/\mathbb{Q}$. Thus, $U(K')/U(F)$ is torsion free. Since $(\varphi, U) \otimes \mathbb{Q}$ is an isomorphism, it follows that f is injective.

Just as in the previous section we apply (2.2) twice, and we see with the snake lemma that

$$\frac{h'}{h} = \frac{B(S,E)}{B(S,E_Z)} \cdot \frac{1}{\#\operatorname{Cok} f}.$$

It remains to show that there exits an injective G-linear homomorphism φ: $\mathbb{Z}[G/H] \to \mathbb{Z}[G/H']$ such that $B(S,E)/B(S,E_Z) = 2$ for $E = \operatorname{Cok}\varphi$. We would then have $h' \mid 2h$, and replacing a by $16a$ we also see that $h \mid 2h'$, so that the Proposition follows.

The element $t = T_1^1$ of G generates a group C of order 8, and $\mathbb{Z}[G/H]$ and $\mathbb{Z}[G/H']$ are free $\mathbb{Z}C$-modules of rank 1. The H-orbits of G/H' are $\{H', t^4H'\}$ and $\{t^iH', t^{-i}H'\}$ for $i = 1, 2, 3$. It follows that we have $\varphi(H) = x \cdot H'$ with $x \in \mathbb{Z}C$ of the form

$$x = a_1(1+t^4) + a_2(t+t^7) + a_3(t^2+t^6) + a_4(t^3+t^5) \tag{5.3}$$

for certain $a_i \in \mathbb{Z}$. Conversely, such an element x gives rise to a G-linear homomorphisms $\mathbb{Z}[G/H] \to \mathbb{Z}[G/H']$ given by $gH \mapsto g \cdot xH'$ for $g \in G$. Let E be its cokernel.

(5.4) Lemma. *If E is finite, then*

$$\frac{B(S,E)}{B(S,E_Z)} = 2(a_2 - a_4)^2.$$

Proof. Let $V = \operatorname{Ker}\pi$ and $V' = \operatorname{Ker}\pi'$ in diagram (5.2). Then both V and V' are free modules of rank 1 over the ring $\mathbb{Z}[t]/(t^4+1) \cong \mathbb{Z}[\zeta]$, with generators $H - t^4H$ and $H' - t^4H'$. On this basis, the map $V \xrightarrow{\varphi} V'$ is multiplication by the image of x in $\mathbb{Z}[\zeta]$, which is $(a_2 - a_4)(\zeta - \zeta^3)$. It follows that

$$[V' : \varphi(V)] = |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}((a_2 - a_4)(\zeta - \zeta^3))| = 4(a_2 - a_4)^4.$$

Let $D = \langle\delta\rangle$ be the decomposition group of an infinite prime of L. The image of δ in $G/C = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^*$ is -1, so DZ is abelian of type $(2,2)$. The DZ-sets G/H and G/H' are linearly equivalent, and they do not have orbits of length 1. The characters $\pi_{DZ/J}$ with $J \subsetneqq DZ$ are linearly independent, so it follow that the DZ-sets G/H and G/H' are isomorphic. This implies that V and V' are isomorphic as $\mathbb{Z}D$-modules. Let $V^+ = V^D = \{v \in V\colon\ \delta(v) = v\}$ and $V^- = \{v \in V\colon\ \delta(v) = -v\}$. Then we have $[V : V^+ \oplus V^-] = [V' : V'^+ \oplus V'^-] < \infty$, so that

$$4(a_2 - a_4)^4 = [V' : \varphi(V)] = [V'^+ : \varphi(V^+)][V'^- : \varphi(V^-)].$$

Without having to distinguish the different possibilities for δ we can exploit a symmetry between V^+ and V^-: we have an isomorphism $V^+ \to V^-$ given by $v \mapsto t^2 v$ because $\delta t^2 = t^{-2}\delta = -t^2\delta$ in $\mathrm{Aut}(V)$. The same holds for V', and since φ commutes with t^2 it follows that

$$[V'^+ : \varphi(V^+)] = [V'^- : \varphi(V^-)] = 2(a_2 - a_4)^2.$$

One checks that the kernel of the canonical map $V \to \mathbb{Z}[G/H]_D$ is V^-. Doing the same for V' one sees that we have a commutative diagram of free $\mathbb{Z}$-modules with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & V^- & \longrightarrow & V & \longrightarrow & \mathbb{Z}[G/H]_D & \xrightarrow{\pi_D} & \mathbb{Z}[G/H]_{DZ} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \varphi_D} & & \downarrow{\scriptstyle \varphi_{DZ}} & & \\
0 & \longrightarrow & V'^- & \longrightarrow & V' & \longrightarrow & \mathbb{Z}[G/H']_D & \xrightarrow{\pi'_D} & \mathbb{Z}[G/H']_{DZ} & \longrightarrow & 0.
\end{array}$$

The vertical maps are injective, and the cokernels have orders $2(a_2 - a_4)^2$, $4(a_2 - a_4)^4$, $\#E_D$, and $\#E_{DZ}$, respectively. It follows that $\#E_D/\#E_{DZ} = 2(a_2 - a_4)^2$. Since D is cyclic we have $\#E_D = \#E^D$ and $\#E_{DZ} = \#(E_Z)_D = \#(E_Z)^D$. By taking G-invariants in the diagram (5.2) we get a diagram of cyclic groups and one sees that $\#E^G = \#(E_Z)^G$. Thus, we obtain

$$\frac{B(S,E)}{B(S,E_Z)} = \frac{\#E^D/\#E^G}{\#(E_Z)^D/\#(E_Z)^G} = \frac{\#E_D}{\#E_{DZ}} = 2(a_2 - a_4)^2$$

and the Lemma follows.

Let us take $a_2 = 1$ and $a_4 = 0$ in the Lemma. The element x in (5.3) gives rise an *injective* homomorphism φ if x is not a zero-divisor in the ring $\mathbb{Z}C = \mathbb{Z}[t]/(t^8 - 1)$. This means that we should choose $a_1, a_3 \in \mathbb{Z}$ such that $a_1(1+t^4) + (t+t^7) + a_3(t^2+t^6)$ does not vanish when plugging in *any* 8-th root of unity for t. If, for instance, $a_1 = 2$ and $a_3 = 0$ then this is the case, so we have produced an injective homomorphism φ with $B(S,E)/B(S,E_Z) = 2$. This completes the proof of Proposition (5.1).

References

1. W. Bosma, B. de Smit, *Class number relations from a computational point of view*, Report MI 1999-27, Mathematisch Instituut, Universiteit Leiden. To appear in: J. Symbolic Comput.
2. R. Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. **4** (1951), 158–174.
3. B. de Smit, R. Perlis, *Zeta functions do not determine class numbers,* Bull. Amer. Math. Soc. (N.S.) **31** (1994), 213–216.
4. G. Lejeune Dirichlet, *Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes*, J. Reine Angew. Math. **24** (1842), 291–371.
5. G. Herglotz, *Über einen Dirichlet'schen Satz*, Math. Nachr. **12** (1922), 255–261.
6. J.-F. Jaulent, *Unités et classes dans les extensions métabéliennes de degré nl^s sur un corps de nombres algébriques*, Ann. Inst. Fourier (Grenoble) **31**, 1 (1981), 39–62.
7. W. Jehne, *Über die Einheiten- und Divisorenklassengruppe von reellen Frobeniuskörpern von Maximaltyp*, Math. Z. **152** (1977), 223–252.
8. N. Klingen, *Arithmetical similarities*, Oxford University Press, Oxford, 1998.
9. S. Kuroda, *Über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. **1** (1950), 1–10.
10. S. Lang, *Algebra*, third edition, Addison Wesley, Reading Mass., 1993.
11. F. Lemmermeyer, *Kuroda's class number formula*, Acta Arith. **66** (1994), 245–260.
12. R. Perlis, *On the class numbers of arithmetically equivalent fields*, J. Number Theory **10** (1978), 489–509.
13. A. Scholz, *Idealklassen und einheiten in kubischen Körpern*, Monathsh. Math. Phys. **40** (1933), 211–222.
14. J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Progr. Math. **47**, Birkhäuser, Boston, 1984.
15. C. D. Walter, *A class number relation in Frobenius extensions of number fields*, Mathematika **24** (1977), 216-225.
16. C. D. Walter, *Kuroda's class number relation*, Acta Arith. **35** (1979), 41–51.