J. Symbolic Computation (2001) **31**, 97–112
doi:10.1006/jsco.1999.1016
Available online at http://www.idealibrary.com on IDEAL®

Class Number Relations from a Computational Point of View

WIEB BOSMA[†][§] AND BART DE SMIT[‡][¶][‖]

[†] *Mathematisch Instituut, Universiteit van Nijmegen, Postbus 9010,
6500 GL Nijmegen, The Netherlands*
[‡] *Mathematisch Instituut, Universiteit Leiden, Postbus 9512,
2300 RA Leiden, The Netherlands*

Brauer and Kuroda showed in the fifties how in a Galois extension of number fields, relations between permutation characters of subgroups provide relations between invariants, such as the discriminant, class number and regulator, of the corresponding intermediate fields. In this paper we investigate various computational aspects of these relations, we present examples, and we give a method to automatically produce class number formulas.

1. Introduction

The goal of this paper is to show how the discipline of finding "Brauer relations" and related formulas for class numbers of number fields can be automated. The two ingredients of this paper are a general approach to Brauer relations of class numbers (de Smit, 1999), and the capabilities of the computer algebra system Magma (Bosma *et al.*, 1997) in the area of group theory, algebraic number theory, matrix and polynomial arithmetic, and linear algebra. By applying the method one can recover and extend work of Jehne, Castela, Perlis and others. In particular, we give an algorithm to find bounds on the class number quotient for arithmetically equivalent number fields with given Galois group.

The use of Magma proved very beneficial for this project on the one hand, while on the other hand useful experience for the further development and integration of the system is gained from this type of application. Here is an indication of the range of tools that was used in our computations:

- permutation groups: the calculation of conjugacy classes, lattices of subgroups, the action on elements, cosets and double cosets;
- characters of finite groups: the computation of permutation characters;
- linear algebra: finding a basis for the kernel of mappings given by rectangular integral matrices, using Hermite normal form;

[§] E-mail: bosma@sci.kun.nl

[¶] The second author was supported by a fellowship from the Koninklijke Nederlandse Akademie van Wetenschappen.

[‖] E-mail: desmit@math.leidenuniv.nl

0747–7171/01/010097 + 16 $35.00/0

- polynomial algebra: manipulating matrices over a multivariate polynomial ring and computing determinants;
- algebraic number theory: computation of class numbers and unit groups for number fields, Galois groups, and lattices of subfields.

In Section 2 we will describe the number theoretic applications we are aiming for: obtaining bounds on class numbers and formulas relating class numbers to a unit index. In Section 3 we explain how to obtain character relations in the setting of permutation groups. We will see how to compute general bounds for class number quotients for a given character relation in Section 4. In Section 5 we show how in certain cases these bounds can be improved upon, and how optimal bounds are obtained. In Section 6 this leads to the recovery and extension of some classical class number formulas.

It is straightforward to generalize all results in this paper to S-class numbers.

2. Number Theoretic Results

Let us start with a detailed treatment of a very classical case of Brauer relations. We consider *biquadratic fields*, i.e. Galois extensions of the rational field $\mathbf{Q}$ with Galois group $V_4 = C_2 \times C_2$.

One reason for the interest in this case stems from the observation (Dirichlet, 1842) that the class number of $\mathbf{Q}(\sqrt{m}, \sqrt{-m})$ is either the product or half the product of the class numbers of $\mathbf{Q}(\sqrt{m})$ and $\mathbf{Q}(\sqrt{-m})$. Dirichlet also gave an easy criterion (in terms of the solvability of a Pell-like equation) to decide which is the case for given m.

More generally, it was proven in various ways (see Walter, 1979; Fröhlich and Taylor, 1991) that for the biquadratic field $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ with quadratic subfields $K_1 = \mathbf{Q}(\sqrt{m})$, $K_2 = \mathbf{Q}(\sqrt{n})$, and $K_3 = \mathbf{Q}(\sqrt{mn})$, we have

$$\frac{h(K)}{h(K_1)h(K_2)h(K_3)} = \frac{[U_K : U_{K_1}U_{K_2}U_{K_3}]}{B}, \qquad B = \begin{cases} 4, & \text{if } K \text{ is real,} \\ 2, & \text{if } K \text{ is complex.} \end{cases} \tag{2.1}$$

Here $h(F)$ and U_F denote the class number and the unit group of a number field F. The formula expresses the *class number quotient* on the left in terms of a *unit index* on the right. It follows at once that we have a lower bound on the class number quotient: it is an integral multiple of $1/B$. In fact we have

$$\frac{h(K)}{h(K_1)h(K_2)h(K_3)} = 2^{-i} \qquad \text{with} \qquad \begin{cases} 0 \le i \le 2, & \text{if } K \text{ is real,} \\ 0 \le i \le 1, & \text{if } K \text{ is complex.} \end{cases} \tag{2.2}$$

One cannot improve upon (2.2) without specifying the number fields further. To see this, we found examples using Magma: the following table lists some instances.

m	n	$h(K_1)$	$h(K_2)$	$h(K_3)$	$h(K)$	i
34	66	2	2	2	8	0
34	42	2	2	2	4	1
34	58	2	2	2	2	2
−6	−10	2	2	2	8	0
−6	−13	2	2	2	4	1

In this paper we describe an automatic procedure to produce formulas like (2.1) for other small Galois extensions of number fields, and to prove bounds on the class number quotients as in (2.2). It was indicated by Brauer (1951) and by Kuroda (1950) what the group-theoretic setting is for these results.

Let G be a finite group. For a subgroup H of G we let 1_H^G be the character of G induced by the trivial character of H. Suppose that for every subgroup H of G an integer a_H is given such that

$$\sum_{H<G} a_H 1_H^G = 0. \tag{2.3}$$

Such a relation is called a *character relation.* In Section 3 we will discuss how to find such character relations. As K ranges over the Galois extensions of $\mathbf{Q}$ with group G, the class number quotient

$$\prod_{H<G} h(K^H)^{a_H}$$

assumes only finitely many values (Brauer, 1951). Here K^H denotes the subfield of K that is invariant under H. Our main result will give effective bounds for this finite set of values. In Section 4 these bounds will be computed explicitly.

For $G = V_4$ with subgroups H_1, H_2, H_3 of order 2, we have the character relation

$$-1_{\{1\}}^G + 1_{H_1}^G + 1_{H_2}^G + 1_{H_3}^G - 2 \cdot 1_G = 0. \tag{2.4}$$

In this case, (2.2) describes the finite set of class number quotients.

By a G-set we mean a finite set with a left-action of G. Given a character relation as in (2.3) we let Y be the G-set obtained by taking a disjoint union of a_H copies of the G-set G/H, for the subgroups H of G with $a_H > 0$. Likewise, let X be the union over all H with $a_H < 0$ of $|a_H|$ copies of the G-set G/H. For example, for $G = V_4$, relation (2.4) gives G-sets X and Y with G-orbit lengths 4, 1, 1 and 2, 2, 2, respectively. The character relation (2.4) says that each $g \in G$ has the same number of fix-points on X and on Y. By character theory, this implies that the permutation module $\mathbf{Q}[X]$ is isomorphic to $\mathbf{Q}[Y]$ as a $\mathbf{Q}[G]$-module; see Lang (1993, Chapter XVIII, Theorem 2.3). This means that there is an injective $\mathbf{Z}[G]$-linear homomorphism φ: $\mathbf{Z}[X] \to \mathbf{Z}[Y]$ with a finite cokernel E. For any sequence $D_1, \ldots, D_r$ of subgroups of G we define

$$B(\varphi; D_1, \ldots, D_r) = \frac{1}{\#E^G} \prod_{i=1}^{r} \#E^{D_i}.$$

Now suppose that G acts by field automorphisms on a number field K. Let $D_1, \ldots, D_r$ be the stabilizers in G of G-orbit representatives of the infinite primes of K. Let $w(F)$ denote the number of roots of unity in a field F. For $x, y \in \mathbf{Q}^*$ we say that x divides y, and we write $x \mid y$ when $y/x \in \mathbf{Z}$. By de Smit (1999) we have

$$\prod_{H} \left(\frac{h(K^H)}{w(K^H)} \right)^{a_H} \ \mid \ B(\varphi; D_1, \ldots, D_r). \tag{2.5}$$

The expression on the left therefore also divides the greatest common divisor B of all $B(\varphi; D_1, \ldots, D_r)$ where φ ranges over the injective G-linear homomorphisms from $\mathbf{Z}[X]$ to $\mathbf{Z}[Y]$.

We will show in Section 4 how to compute for given G, X, Y, and $D_1, \ldots, D_r$ a divisor C of B such that (2.5) also holds with $B(\varphi; D_1, \ldots, D_r)$ replaced by C. We will give examples where C is a strict divisor of B.

The number $\prod_H w(K^H)^{a_H}$ is a power of 2, and it is equal to 1 when the roots of unity in K of order a power of 2 generate a cyclic extension of K^G; see Brauer (1951). Applying (2.5) to relation (2.4) and to the same relation with opposite signs, we find that the integer i in (2.2) satisfies $-1 \leq i \leq 2$ in the real case and $0 \leq i \leq 1$ in the complex case.

In Section 5 we will see how to improve the bound C in certain cases by using a property of functoriality in φ. For relation (2.4) this will give (2.2).

In Section 6 we will indicate how to compute unit index formulas like (2.1) for other Galois groups in a systematic way. We will use a more specific version of (2.5) for this, which we now formulate. Let U be the group of units of the ring of integers of K. Let $U(X)$ be the set of G-equivariant maps from X to U. For an abelian group A let $\bar{A}$ be the quotient of A by its torsion subgroup. Then φ induces a homomorphism $U(Y) \to U(X)$ which in turn induces a homomorphism

$$\prod_{H, a_H > 0} \left(\overline{U^H}\right)^{a_H} = \overline{U(Y)} \xrightarrow{\varphi^*} \overline{U(X)} = \prod_{H, a_H < 0} \left(\overline{U^H}\right)^{-a_H}.$$

Theorem 2.1. (de Smit, 1999) *We have*

$$\prod_H \left(\frac{h(K^H)}{w(K^H)}\right)^{a_H} = \frac{B(\varphi; D_1, \ldots, D_r)}{\#\mathrm{Cok}\, \varphi^*}.$$

3. Finding Character Relations

This section is entirely group theoretic: we describe how character relations as in (2.3) can be found for a given finite group G. The elementary theory of group characters we will employ can be found for example in Curtis and Reiner (1962) and James and Liebeck (1993); for computational issues see Dixon (1967) and Schneider (1990).

If H and H' are conjugate subgroups of G, then there is a "trivial" character relation $1_H^G - 1_{H'}^G = 0$. Therefore, we may as well consider the subgroups up to conjugation, i.e. we demand that $a_H = 0$ for all H outside a fixed set of representatives of the conjugacy classes of the subgroups of G. If there are s conjugacy classes of subgroups of G, then the character relations thus form a subgroup L of $\mathbf{Z}^s$. We will give a method to obtain a $\mathbf{Z}$-basis for L. By a theorem of Artin (Artin, 1931a,b; Curtis and Reiner, 1962), any rational character on a finite group G is a unique $\mathbf{Q}$-linear combination of permutation characters of *cyclic* subgroups. Thus, the rank of L is the number of conjugacy classes of non-cyclic subgroups of G. In particular: non-trivial character relations exist when G is not cyclic.

Let G be a finite group, given as a permutation group by explicit generators. The first step is to compute the conjugacy classes of G. For a given subgroup H the character 1_H^G, considered as a map from the conjugacy classes of G to $\mathbf{Z}$, is given by

$$1_H^G(C) = [G : H] \frac{\#(C \cap H)}{\#C}.$$

Thus, to find all relations between the permutation characters of a certain collection $\mathcal{S}$ of subgroups of G, one needs to compute a basis for the dependencies between the rows of the integer matrix $(1_H^G(C))_{H,C}$, where the row-index H runs over $\mathcal{S}$ and the column-index C runs over the conjugacy classes of G. This is a straightforward matrix kernel computation.

Example 3.1. Let us consider the alternating group A_4 on 4 elements. The matrix

$$\begin{pmatrix} 12 & 0 & 0 & 0 \\ 6 & 2 & 0 & 0 \\ 4 & 0 & 1 & 1 \\ 3 & 3 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

gives each permutation character 1_H^G as a row vector. The character value on the identity element of G is listed in the first column, so in the first column one reads off the index of the five representative subgroups H. Since A_4 contains V_4, the relation for V_4, induced up to G, gives the biquadratic relation $(-1, 3, 0, -2, 0)$ between the rows of the matrix. Other relations that one spots immediately are $(1, -1, -2, 0, 2)$ and $(0, 1, -1, -1, 1)$. For a Galois extension K of $\mathbf{Q}$ with Galois group A_4 we will denote by K_d a subfield of degree d, for $d = 3, 4, 6$. The relations $(0, 1, -1, -1, 1)$ and $(1, 0, -3, -1, 3)$ tell us, after omitting trivial factors $h(\mathbf{Q})$, that both quantities

$$\frac{h(K_6)}{h(K_3) \cdot h(K_4)} \qquad \text{and} \qquad \frac{h(K)}{h(K_3) \cdot h(K_4)^3} \tag{3.1}$$

assume only finitely many values as K ranges over all A_4-extensions of $\mathbf{Q}$.

Let us show how to find all character relations of the form $1_H^G = 1_{H'}^G$, when H and H' are non-conjugate subgroups of G of index at most 8, by a brute force method. Such (G, H, H') are called *Gassmann triples.* We list all transitive subgroups of degree $d \leq 8$, and then look for subgroups H of index d for which H induces the same permutation character as a point stabilizer.

A simple double loop in Magma over the subgroups of index n of the transitive subgroups of S_n, for $n \leq 8$ (see Cannon *et al.*, 2000, for the algorithm used), exhibits the pairs $(7, 168)$, $(8, 32)$, and $(8, 48)$ of degree and group order as the only ones where Gassmann triples exist. This also gives a computational alternative to the proof of Perlis (1977) of the fact that there are no Gassmann triples in degree less than 6.

If G is a Galois group of a field extension of $\mathbf{Q}$, then the condition $1_H^G = 1_{H'}^G$ is equivalent to the condition that the fields K^H and $K^{H'}$ have the same zeta function. If this condition holds, we say that the two fields are *arithmetically equivalent.* See Klingen (1998) for more examples and references.

For higher degrees one should use the classification of transitive groups of small degree for efficiency; see Bosma and de Smit (1999) for details. In a fixed group G one can simply scan for non-conjugate Gassmann equivalent subgroups. For instance, in the group $G = A_6$ of order 360 one finds that the two conjugacy classes of subgroups of order 4 give the same permutation character. In S_6 two of the seven conjugacy classes of subgroups of order 4 have identical permutation characters, thus leading to equivalent fields of degree 180. The latter example is the case Gassmann proposed originally as the very first instance of this phenomenon (Gassmann, 1926). One also finds arithmetically equivalent fields of degree $630, 210, 105, 15$ for which the normal closure has Galois group A_7. The cases of degree 210 and of degree 105 are particularly interesting since there we have three conjugacy classes of subgroups that all give the same permutation character.

4. Computing Bounds

Suppose we are given a finite group G and two G-sets X and Y. We wish to describe the G-linear homomorphisms φ: $\mathbf{Z}[X] \to \mathbf{Z}[Y]$. For $x \in X$ we have $\varphi(x) = \sum_{y \in Y} a_{x,y} y$ with $a_{x,y} \in \mathbf{Z}$. The condition that φ be G-equivariant means that $a_{gx,gy} = a_{x,y}$ for all $g \in G$. If we number the G-sets X and Y, and we number the G-orbits of $X \times Y$, then we can write down a generic matrix φ with entries taken from a set of variables $\{a_1, \ldots, a_t\}$ with $t = \#(G \backslash (X \times Y))$. This matrix, whose entries are in the polynomial ring $\mathbf{Z}[a_1, \ldots, a_t]$ is the *universal* homomorphism from $\mathbf{Z}[X]$ to $\mathbf{Z}[Y]$. Its rows are indexed by Y and its columns by X. For example, let us take $G = V_4$ again and let X and Y be the G-sets obtained from (2.4) with G-orbit lengths 4, 1, 1 and 2, 2, 2, respectively. Then

$$\varphi = \left(\begin{array}{cccc|c|c} a_1 & a_1 & a_2 & a_2 & a_7 & a_{10} \\ a_2 & a_2 & a_1 & a_1 & a_7 & a_{10} \\ \hline a_3 & a_4 & a_3 & a_4 & a_8 & a_{11} \\ a_4 & a_3 & a_4 & a_3 & a_8 & a_{11} \\ \hline a_5 & a_6 & a_6 & a_5 & a_9 & a_{12} \\ a_6 & a_5 & a_5 & a_6 & a_9 & a_{12} \end{array}\right) \tag{4.1}$$

is the universal matrix, and for every choice of values in $\mathbf{Z}$ for the variables $a_1, \ldots, a_t$, we obtain a G-linear homomorphism $\tilde{\varphi}$: $\mathbf{Z}[X] \to \mathbf{Z}[Y]$.

Let us construct for any subgroup H of G a matrix φ^H which is a generic description of the map $\mathbf{Z}[X]^H \to \mathbf{Z}[Y]^H$. Note that $\mathbf{Z}[X]^H$ has a $\mathbf{Z}$-basis consisting of the elements $\sum_{x \in O} x$ where O ranges over the H-orbits of X. Thus, one can construct φ^H out of φ by first replacing H-equivalent columns by their sum, and then selecting rows indexed by representatives in Y of $H \backslash Y$. For example, for the V_4-example we obtain

$$\varphi^G = \begin{pmatrix} 2a_1 + 2a_2 & a_7 & a_{10} \\ 2a_3 + 2a_4 & a_8 & a_{11} \\ 2a_5 + 2a_6 & a_9 & a_{12} \end{pmatrix}.$$

We also need a relative version of this construction, i.e. a matrix $\varphi^{H/G}$ describing the induced map $\mathbf{Z}[X]^H / \mathbf{Z}[X]^G \to \mathbf{Z}[Y]^H / \mathbf{Z}[Y]^G$. For every G-orbit of X we select an H-orbit contained in it, and we do the same for Y. In the matrix for φ^H, whose columns are indexed by $H \backslash X$ and whose rows are indexed by $H \backslash Y$, we now subtract from every row the unique selected row in the same G-orbit. Then we omit all selected rows (which are now zero) and all selected columns. For instance, to compute $\varphi^{1/G}$ in our V_4-example we subtract every even-numbered row from the one above it and omit the last three columns:

$$\varphi^{1/G} = \begin{pmatrix} a_1 - a_2 & a_1 - a_2 & a_2 - a_1 \\ a_3 - a_4 & a_4 - a_3 & a_3 - a_4 \\ a_5 - a_6 & a_6 - a_5 & a_6 - a_5 \end{pmatrix}.$$

If the a_i are specified to integers for which the integer matrix $\tilde{\varphi}$ that one obtains from the generic matrix φ has finite cokernel E, then we have

$$\#E^H = |\det(\tilde{\varphi}^H)|, \qquad \frac{\#E^H}{\#E^G} = |\det(\tilde{\varphi}^{H/G})|.$$

To see the first equality, note that $H^1(H, \mathbf{Z}[X]) = 0$ by Shapiro's lemma and the fact that $H^1(J, \mathbf{Z}) = 0$ for any finite group J acting trivially on $\mathbf{Z}$. To see the second equality one uses the first equality and the snake lemma. Given subgroups $D_1, \ldots, D_r$ of G with $r \geq 1$ we now define

$$B^{\mathrm{gen}} = \det(\varphi^G)^{r-1} \prod_{i=1}^{r} \det(\varphi^{D_i/G}) \in \mathbf{Z}[a_1, \ldots, a_t].$$

Note that B^{gen} is only defined up to sign since we had to specify an ordering of the rows and columns of the matrices whose determinant occurs in B^{gen}. The main property of this polynomial is that specifying the variables a_i to integers $\tilde{a}_i$, in such a way that the resulting homomorphism $\tilde{\varphi}$ is injective, will give

$$B(\tilde{\varphi}; D_1, \ldots, D_r) = |B^{\mathrm{gen}}(\tilde{a}_1, \ldots, \tilde{a}_t)|.$$

Now let G act on a number field K so that $D_1, \ldots, D_r$ are the stabilizers of G-orbit representatives of the infinite primes of K.

Theorem 4.1. *Let $C \in \mathbf{Z}_{\geq 1}$ be the content of the polynomial $B^{\mathrm{gen}} \in \mathbf{Z}[a_1, \ldots, a_t]$. Then we have*

$$\prod_H \left(\frac{h(K^H)}{w(K^H)} \right)^{a_H} \mid C.$$

Proof. For every prime p we need to show a divisibility relation of p-parts. Let p be a prime number. Write $B^{\mathrm{gen}} = p^n F$, where $F \in \mathbf{Z}[a_1, \ldots, a_t]$ has non-zero image $\bar{F}$ in $\mathbf{F}_p[a_1, \ldots, a_t]$. Then p^n is the p-part of C. The determinant of the generic matrix φ can be written as $p^a D$ with $D \in \mathbf{Z}[a_1, \ldots, a_t]$ and $\bar{D} \neq 0$ in $\mathbf{F}_p[a_1, \ldots, a_t]$.

If there are values $\bar{a}_1, \ldots, \bar{a}_t \in \mathbf{F}_p$ so that $\bar{F}(\bar{a}_1, \ldots, \bar{a}_t) \neq 0$, then we can lift the $\bar{a}_i$ to $\tilde{a}_i \in \mathbf{Z}$, and if the resulting matrix $\tilde{\varphi}$ is invertible over $\mathbf{Q}$, then we obtain our result by (2.5). Of course such $\bar{a}_i$ might not exist in $\mathbf{F}_p$. We therefore consider the algebraic closure $\mathbf{F}_p^{\mathrm{alg}}$ of $\mathbf{F}_p$. The polynomial map $\bar{F}\bar{D}$ does not vanish as a function $(\mathbf{F}_p^{\mathrm{alg}})^t \to \mathbf{F}_p^{\mathrm{alg}}$. Therefore we can choose an integer $d \geq 1$ and elements $\bar{a}_1, \ldots, \bar{a}_t \in \mathbf{F}_{p^d}$ so that $\bar{F}(\bar{a}_1, \ldots, \bar{a}_t) \neq 0$ and $\bar{D}(\bar{a}_1, \ldots, \bar{a}_t) \neq 0$.

Now lift the irreducible polynomial of a generating element of $\mathbf{F}_{p^d}$ over $\mathbf{F}_p$ to a monic polynomial $P \in \mathbf{Z}[T]$ of degree d, and let R be the domain $\mathbf{Z}[T]/(P)$. Lifting the $\bar{a}_i \in \mathbf{F}_{p^d} = R/pR$ to elements $\tilde{a}_i \in R$, and substituting the values $\tilde{a}_i$ for the variables a_i in the generic matrix, we obtain an $R[G]$-linear map $\tilde{\varphi}$: $R[X] \to R[Y]$, and we denote its cokernel by E. Since $\det_R(\tilde{\varphi}) = p^a D(\tilde{a}_1, \ldots, \tilde{a}_n) \neq 0$, this map $\tilde{\varphi}$ is injective and E is finite.

The localization $R_{(p)}$ is a discrete valuation ring. By the theory of elementary divisors, the cardinality of the cokernel of a square matrix over $R_{(p)}$ is the index in $R_{(p)}$ of the ideal generated by its determinant. For each subgroup H of G we apply this to $E^H = \mathrm{Cok}\,(\tilde{\varphi}^H)$, and we see that

$$\mathrm{ord}_p(\# E^H) = \mathrm{ord}_p([R : \det_R(\tilde{\varphi}^H) \cdot R]).$$

It follows that

$$\mathrm{ord}_p(B(\tilde{\varphi}; D_1, \ldots, D_r)) = \mathrm{ord}_p([R : p^n F(\tilde{a}_1, \ldots, \tilde{a}_n) \cdot R]) = nd.$$

By forgetting the R-module structure of $R[X]$ and $R[Y]$, we can view $\tilde{\varphi}$ as a G-linear homomorphism $\mathbf{Z}[X]^d \to \mathbf{Z}[Y]^d$ with cokernel E. If we apply (2.5) to this map, and take the dth roots we obtain our result. This proves the theorem. □

Example 4.2. Let a be a positive integer that is not a square or twice a square. The fields K and K' generated by $\sqrt[8]{a}$ and $\sqrt[8]{16a}$ give rise to two transitive G-sets for the group $G = (\mathbf{Z}/8\mathbf{Z}) \rtimes (\mathbf{Z}/8\mathbf{Z})^*$, for which the permutation characters are equal. Perlis (1978) showed that their class numbers differ by a factor of at most 16, essentially by computing the optimal value of the polynomial B^{gen}, which is also equal to the number B in Section 2. However, in this case the content of B^{gen} is 8, so Theorem 4.1 gives a stronger result. Proposition 5.1 below gives an even better result.

Example 4.3. The group PSL$(2, 11)$ has two conjugacy classes of subgroups of index 11, and they are Gassman equivalent. Let G be the permutation group on $X = \{1, \ldots, 11\}$ generated by the elements $c = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)$, $d = (2, 3)(4, 11)(5, 6)(7, 10)$, and $e = (2, 6, 9)(3, 7, 4)(5, 10, 8)$. Then G is isomorphic to PSL$(2, 11)$, and $H = \langle d, e\rangle$ is the stabilizer in G of the element 1 of X.

Define Y as the G-set which as a $\langle c\rangle$-set coincides with X, but which has d-action given by $(1, 11)(3, 10)(4, 7)(8, 9)$ and e-action given by $(1, 11, 8)(2, 6, 9)(5, 10, 7)$. Then $H\backslash Y = \{\{1, 2, 6, 8, 9, 11\}, \{3, 4, 5, 7, 10\}\}$, so the generic map $\mathbf{Z}[X] \to \mathbf{Z}[Y]$ is given by permuting the column vector $(a_1\ a_1\ a_2\ a_2\ a_2\ a_1\ a_2\ a_1\ a_1\ a_2\ a_1)$ cyclically. The group $D = \langle d\rangle$ is the unique subgroup of G of order 2 up to conjugation. Writing $t = a_1 - a_2$ we compute $\varphi^{1/D}$ and $\varphi^{D/G}$ and verify that their determinants have contents 3^2 and 3^3:

$$\varphi^{1/D} = \begin{pmatrix} t & 0 & t & t \\ 0 & t & -t & t \\ -t & t & t & 0 \\ -t & -t & 0 & t \end{pmatrix} \qquad \varphi^{D/G} = \begin{pmatrix} 0 & t & t & -t & t & 0 \\ -t & t & 0 & 0 & 0 & t \\ -t & 0 & 0 & t & t & 0 \\ -t & -t & t & -t & t & t \\ 0 & -t & t & t & 0 & t \\ 0 & 0 & -t & 0 & t & t \end{pmatrix}.$$

It follows that two arithmetically equivalent number fields of degree 11 with Galois group PSL$(2, 11)$ have class numbers which differ by a factor of at most 3^5 in the totally real case, and a factor 3^3 if they are not totally real.

Remark 4.4. When the determinants in the definition of B^{gen} become awkwardly large, we should make sure that we use the smallest possible building blocks for the expression, and keep the expression in factored form. Recall that the content of a product of two polynomials is the product of their contents, so we can still compute C from this factored expression. Since we prefer many small factors to one large one, we make a filtration $D_i = D_{i,0} \subset D_{i,1} \subset \cdots \subset D_{i,k} = G$, for each i and we write

$$\det(\varphi^{D_i/G}) = \prod_{j=1}^{k} \det(\varphi^{D_{i,j-1}/D_{i,j}}).$$

Remark 4.5. There is one other approach, which avoids polynomial computations in many variables: one can simply pick random integer values $\tilde{a}_i$ for the a_i and do all computations with the integer matrix $\tilde{\varphi}$. By Theorem 4.1 we do not even have to check that $\tilde{\varphi}$ is invertible: if our $\tilde{\varphi}$ gives a non-zero bound B_0, then it is a multiple of C, so Theorem 4.1 holds with C replaced by B_0. Taking the greatest common divisor of such bounds B_0 for several choices of the integers $\tilde{a}_i$ will typically reveal the greatest common divisor B of all of them. However, Example 4.2 shows that B may be a strict multiple of C, and one will not know whether $B = C$ without doing the formal computations.

In the rest of this section we treat the first example of (3.1): let $K/\mathbf{Q}$ be a Galois extension whose Galois group is the alternating group A_4, and for each $d \in \{3, 4, 6\}$ we let K_d be a subfield of degree d.

Proposition 4.6. *We have*

$$\frac{h(K_6)}{h(K_3) \cdot h(K_4)} = 2^i \qquad \textit{with} \quad \begin{cases} -3 \leq i \leq 2, & \textit{if } K \textit{ is real} \\ -2 \leq i \leq 1, & \textit{if } K \textit{ is complex.} \end{cases}$$

Proof. Let $X = Y = \{1, 2, \ldots, 7\}$ as sets, let G be the subgroup of the permutation group on Y generated by $e_1 = (12)(34)$, $e_2 = (13)(24)$ and $c = (234)(567)$. Then $G = A_4$ and we let G act on X by letting e_1, e_2, c act as $(34)(56)$, $(12)(56)$ and $(135)(246)$ respectively. The G-orbits of X and Y have lengths 6, 1 and 4, 3. The generic G-linear homomorphisms φ: $\mathbf{Z}[X] \to \mathbf{Z}[Y]$ and ψ: $\mathbf{Z}[Y] \to \mathbf{Z}[X]$ are

$$\varphi = \left(\begin{array}{cccccc|c} a_1 & a_2 & a_1 & a_2 & a_1 & a_2 & a_6 \\ a_1 & a_2 & a_2 & a_1 & a_2 & a_1 & a_6 \\ a_2 & a_1 & a_1 & a_2 & a_2 & a_1 & a_6 \\ a_2 & a_1 & a_2 & a_1 & a_1 & a_2 & a_6 \\ \hline a_3 & a_3 & a_5 & a_5 & a_4 & a_4 & a_7 \\ a_4 & a_4 & a_3 & a_3 & a_5 & a_5 & a_7 \\ a_5 & a_5 & a_4 & a_4 & a_3 & a_3 & a_7 \end{array}\right) \qquad \psi = \left(\begin{array}{cccc|ccc} a_1 & a_1 & a_2 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_2 & a_1 & a_1 & a_3 & a_4 & a_5 \\ a_1 & a_2 & a_1 & a_2 & a_5 & a_3 & a_4 \\ a_2 & a_1 & a_2 & a_1 & a_5 & a_3 & a_4 \\ a_1 & a_2 & a_2 & a_1 & a_4 & a_5 & a_3 \\ a_2 & a_1 & a_1 & a_2 & a_4 & a_5 & a_3 \\ \hline a_6 & a_6 & a_6 & a_6 & a_7 & a_7 & a_7 \end{array}\right).$$

Let $D = \langle e_1 \rangle$ and $N = \langle e_1, e_2 \rangle$. The building blocks for the bound C in Theorem 4.1 can now easily be computed by hand. We give them in the table below, which for several superscripts "–" gives the generic matrix φ^- and ψ^- and the contents $C(\varphi^-)$ and $C(\psi^-)$ of their determinants:

–	matrix φ^-	$C(\varphi^-)$	matrix ψ^-	$C(\psi^-)$
G	$\begin{pmatrix} 3a_1 + 3a_2 & a_6 \\ 2a_3 + 2a_4 + 2a_5 & a_7 \end{pmatrix}$	1	$\begin{pmatrix} 2a_1 + 2a_2 & a_3 + a_4 + a_5 \\ 4a_6 & 3a_7 \end{pmatrix}$	2
N/G	$\begin{pmatrix} 2a_3 - 2a_5 & 2a_5 - 2a_4 \\ 2a_4 - 2a_5 & 2a_3 - 2a_4 \end{pmatrix}$	4	$\begin{pmatrix} a_3 - a_4 & a_4 - a_5 \\ a_5 - a_4 & a_3 - a_5 \end{pmatrix}$	1
D/N	$(a_1 - a_2)$	1	$(2a_1 - 2a_2)$	2
$1/D$	$\begin{pmatrix} a_1 - a_2 & a_1 - a_2 \\ a_1 - a_2 & a_2 - a_1 \end{pmatrix}$	2	$\begin{pmatrix} a_1 - a_2 & a_1 - a_2 \\ a_1 - a_2 & a_2 - a_1 \end{pmatrix}$	2

Since $K^{A_4} = \mathbf{Q}$, the infinite primes of K form a transitive G-set. If K is real then each element has trivial stabilizer in G, so that we obtain our bound by multiplying the contents in the last three rows. If K is complex, then D is a decomposition group at infinity so that we obtain the bound by multiplying the contents of only the middle two rows. □

5. Improved Bounds

In this section we will give a method which for certain character relations will give better results than in the last Section, even with less computational effort. This method is based on the fact that the "unit index" $\#\mathrm{Cok}\,\varphi^*$ in Theorem 2.1 is in some sense functorial in φ.

Let us assume that N is a normal subgroup of G for which the quotient G-sets $N\backslash X$ and $N\backslash Y$ are isomorphic. The quotient map $X \to N\backslash X$ induces a canonical isomorphism from the G-module $\mathbf{Z}[X]_N$ of N-coinvariants of $\mathbf{Z}[X]$ to $\mathbf{Z}[N\backslash X]$. For a given G-linear homomorphism φ: $\mathbf{Z}[X] \to \mathbf{Z}[Y]$ we obtain an induced G-linear homomorphism φ_N: $\mathbf{Z}[N\backslash X] \to \mathbf{Z}[N\backslash Y]$. Let $E = \mathrm{Cok}\,\varphi$. Since taking N-coinvariants is a right exact functor we have $\mathrm{Cok}\,\varphi_N = E_N$.

The projection map $X \to N\backslash X$ induces an injective map $U(N\backslash X) \longrightarrow U(X)$. Note that $U(X)$ is a product of unit groups $U(K^H)$ of subfields of K and that the image in $U(X)$ of $U(N\backslash X)$ is the product of the subgroups $U(K^{NH})$. Let us write i_X for the induced map $\overline{U(N\backslash X)} \longrightarrow \overline{U(X)}$. Then φ induces a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \overline{U(N\backslash Y)} \arrow[r, "i_Y"] \arrow[d, "{\varphi_N}^*"] & \overline{U(Y)} \arrow[r] \arrow[d, "\varphi^*"] & \mathrm{Cok}\,i_Y \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & \overline{U(N\backslash X)} \arrow[r, "i_X"] & \overline{U(X)} \arrow[r] & \mathrm{Cok}\,i_X \arrow[r] & 0.
\end{tikzcd} \tag{5.1}$$

Since the two leftmost vertical maps are injective, the snake lemma and Theorem 2.1 for φ and for φ_N now imply that

$$\prod_H \left(\frac{h(K^H)}{w(K^H)}\right)^{a_H} = \frac{\#\mathrm{Ker} f}{\#\mathrm{Cok}\, f} \cdot \frac{B(\varphi; D_1, \ldots, D_r)}{B(\varphi_N; D_1, \ldots, D_r)}. \tag{5.2}$$

In order to analyse the factors on the right we introduce a combinatorial parameter: if H is a subgroup of G containing N, then we let $j_H(X)$ be the product over the H-orbits O of X of the integers $\#O/\#(O/N)$. Note that the canonical map $\mathbf{Z}[X]^H \to \mathbf{Z}[N\backslash X]^H$ is an injection with a cokernel of order $j_H(X)$. By also applying this statement for Y instead of X, one deduces with the snake lemma that

$$\frac{\#(E_N)^H}{\#E^H} = \frac{j_H(Y)}{j_H(X)}.$$

Put $J(H) = j_H(Y)/j_H(X)$ and let

$$B_{\mathrm{rel}}(\varphi; D_1, \ldots, D_r) = \frac{B(\varphi; D_1, \ldots, D_r)}{B(\varphi_N; D_1, \ldots, D_r)} = \frac{\#(E_N)^G}{\#E^G} \prod_{i=1}^{r} \frac{\#E^{D_i}}{\#(E_N)^{D_i}}.$$

For each $i \in \{1, \ldots, r\}$ we have

$$\frac{\#E^{D_i}}{\#(E_N)^{D_i}} = \frac{\#E^{D_i}}{\#E^{ND_i}} \frac{\#E^{ND_i}}{\#(E_N)^{ND_i}} = \frac{|\det(\varphi^{D_i/ND_i})|}{J(ND_i)}.$$

It follows that

$$\pm B_{\mathrm{rel}}(\varphi; D_1, \ldots, D_r) = J(G) \prod_i \frac{\det(\varphi^{D_i/ND_i})}{J(ND_i)}.$$

The expression on the right, which is only defined up to sign, can be computed for the generic homomorphism φ as in Section 4. This gives a polynomial $B_{\mathrm{rel}}^{\mathrm{gen}} \in \mathbf{Q}[a_1, \ldots, a_t]$.

Let $C_{\mathrm{rel}} \in \mathbf{Q}_{>0}$ be the content of this polynomial, i.e. C_{rel} is the positive generator of the fractional $\mathbf{Z}$-ideal generated by the coefficients of $B^{\mathrm{gen}}_{\mathrm{rel}}$.

Proposition 5.1. *Let $t(X)$ and $t(Y)$ be the orders of the torsion subgroups of* $\operatorname{Cok} i_X$ *and* $\operatorname{Cok} i_Y$*. Then we have divisibility relations*

$$\prod_H \left(\frac{h(K^H)}{w(K^H)}\right)^{a_H} \mid C_{\mathrm{rel}} \cdot \frac{t(Y)}{t(X)} \mid C_{\mathrm{rel}} \cdot j_G(Y).$$

Let us sketch the proof. In the setting above we have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & (\operatorname{Cok} i_Y)_{\mathrm{tors}} \arrow[r] \arrow[d] & \operatorname{Cok} i_Y \arrow[r] \arrow[d, "f"] & \overline{\operatorname{Cok} i_Y} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (\operatorname{Cok} i_X)_{\mathrm{tors}} \arrow[r] & \operatorname{Cok} i_X \arrow[r] & \overline{\operatorname{Cok} i_X} \arrow[r] & 0.
\end{tikzcd}$$

The rightmost vertical map is injective, so by the snake lemma we have $\frac{\#\mathrm{Ker} f}{\#\operatorname{Cok} f} \mid \frac{t(Y)}{t(X)}$. By (5.2) we now see that

$$\prod_H \left(\frac{h(K^H)}{w(K^H)}\right)^{a_H} \mid B^{\mathrm{gen}}_{\mathrm{rel}}(\tilde{a}_1, \ldots, \tilde{a}_t) \cdot \frac{t(Y)}{t(X)}$$

for any $\tilde{a}_1, \ldots, \tilde{a}_t \in \mathbf{Z}$ for which the resulting map $\tilde{\varphi}\colon \mathbf{Z}[X] \to \mathbf{Z}[Y]$ is injective. Note that for every positive integer d and every G-set Z, the disjoint union Z_d of d copies of Z satisfies $t(Z_d) = t(Z)^d$. With this one extra ingredient the first divisibility in Proposition 5.1 now follows by the argument given in the proof of Theorem 4.1.

For the second divisibility we use a theorem of van Tieghem (1975): for any extension of number fields $F \subset E$, the torsion subgroup of $E^*/(F^*\mu(E))$ is a finite group whose order divides $[E : F]$. Here $\mu(E)$ denotes the group of roots of unity in E. See May (1980, Proposition 1) or Stevenhagen (1990, Theorem 4.4) for a short proof. It follows from van Tieghem's result that $t(Y)$ divides $j_G(Y)$. This proves Proposition 5.1.

We refer to de Smit (1999) for a worked-out example of this method which shows that the class numbers of the fields from Example 4.2 generated by $\sqrt[8]{a}$ and $\sqrt[8]{16a}$ can only differ by a factor of 2. We can now also strengthen Proposition 4.6.

Proposition 5.2. *For $K/\mathbf{Q}$ Galois with group A_4 let K_d be a subfield of degree d for $d \in \{3, 4, 6\}$. Then:*

$$\left\{\frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1\right\} \subset \left\{\frac{h(K_6)}{h(K_3) \cdot h(K_4)} : \quad \mathrm{Gal}(K, \mathbf{Q}) = A_4,\ K \textit{ real}\right\} \subset \left\{\frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2\right\};$$

$$\left\{\frac{h(K_6)}{h(K_3) \cdot h(K_4)} : \quad \mathrm{Gal}(K, \mathbf{Q}) = A_4,\ K \textit{ complex}\right\} = \left\{\frac{1}{4}, \frac{1}{2}, 1\right\}.$$

Proof. Let N be the normal subgroup of order 4 of the group $G = A_4$. We use the notation from the proof of Proposition 4.6, so X and Y will be G-sets with G-orbits of lengths 6, 1, and 3, 4, respectively. We will apply Theorem 5.1, so that only the matrices in the last two rows of the table at the end of Section 4 are relevant. First note that $j_G(X) = 2$, $j_G(Y) = 4$, $j_N(X) = 8$ and $j_N(Y) = 4$. We have $t(Y) = 1$, because $\operatorname{Cok} i_Y = \overline{U(K_4)}$ is torsion free. By Proposition 5.1 we obtain

$$\frac{h(K_3)h(K_4)}{h(K_6)} \mid \frac{j_G(Y)j_N(X)}{j_G(X)j_N(Y)} c = 4c,$$

where $c = 1$ if K is complex and $c = 2$ if K is real. For an equality the other way around we note that $t(X) \mid j_G(X) = 2$, and we obtain a divisibility relation

$$\frac{h(K_6)}{h(K_3)h(K_4)} \mid \frac{j_G(X)j_N(Y)}{j_G(Y)j_N(X)} t(X)c' = \frac{t(X)c'}{4} \mid \frac{c'}{2}, \tag{5.3}$$

where $c' = 2$ if K is complex and $c' = 4$ if K is real. Note that equalities in (5.3) can only hold if $t(X) = 2$, i.e. if we obtain K_6 out of K_3 by adjoining the square root of a fundamental unit of K_3.

The proof of Proposition 5.2 is then finished by furnishing examples; see the table below, and the comments in Example 5.3.

f	$\operatorname{sig}(K_4)$	$h(K_6)$	$h(K_4)$	$h(K_3)$	i
$x^4 - 2x^3 + 2x^2 + 2$	$(0,2)$	1	1	1	0
$x^4 - x^3 - 3x + 4$	$(0,2)$	1	2	1	-1
$x^4 - 16x^3 + 72x^2 + 81$	$(0,2)$	12	16	3	-2
$x^4 - 7x^2 - 3x + 1$	$(4,0)$	1	1	1	0
$x^4 - x^3 - 7x^2 + 2x + 9$	$(4,0)$	2	1	4	-1
$x^4 - 6753x^2 - 39936x + 9110416$	$(4,0)$	48	4	48	-2
$x^4 - 579x^2 + 426x + 74440$	$(4,0)$	648	4	1296	-3

□

Example 5.3. The table lists one example for each of the seven class number quotients of Proposition 5.2; an irreducible polynomial generating K_4 is given, with its signature. The normal closure K of K_4 has Galois group A_4, and the class numbers for the fields K_d are listed.

We consulted several sources for families of polynomials generating number fields for which the normal closure has Galois group A_4. All quartic fields of discriminant up to 10^6 in absolute value are publicly available, see Buchmann *et al.* (1995). Both in the real and in the complex case, examples with class number quotients 1 and 1/2 can be found among these. Seidelmann (1918) gives a univariate polynomial with three parameters which by rational specialization of the parameters usually yields a quartic A_4-field, and which produces them all this way. In various places in the literature, polynomials with a single parameter t can be found that realize A_4 as a Galois group over $\mathbf{Q}(t)$. For almost all specializations of t in $\mathbf{Q}$ they realize A_4 over $\mathbf{Q}$. Explicitly, Matzat (1987) gives the polynomial

$$F_t(x) = x^4 - \frac{1}{1+3t^2}(4x - 3).$$

This produces complex fields and for the first 77 integral values of t this alternately yields the class number quotients 1 and 1/2. With Hilbert's polynomial (Hilbert, 1892; Serre, 1992)

$$G_t = x^4 - \frac{16}{3}x^3 + 8x^2 + t^2$$

several complex fields with class number quotient 1/4 were generated.

These polynomials tend to produce very few fields of small discriminant. To produce more examples of totally real fields, we used the polynomial

$$H_t(x) = x(x+396)^2(x+11) + (x+4)^2(x+256)t^2,$$

(communicated to us by Jürgen Klüners). It enabled us to find examples with class number quotients 1/4 and 1/8.

We did not find any examples with class number quotient 2.

6. Unit Index Formulas

In certain cases one can make a more or less canonical choice for the map φ. This can have two advantages. First of all, the computation of the bound becomes much faster than for generic matrices φ. Secondly, the "unit index" $\#\mathrm{Cok}\,\varphi^*$ can often be interpreted in a nice way. This way one recovers "class number formulas" such as (2.1), and one has an algorithm to produce them for other groups as well.

Let us first describe the building blocks of such "canonical" maps. If $H \le H' \le G$, then there is a canonical projection π: $\mathbf{Z}[G/H] \to \mathbf{Z}[G/H']$, and a "norm map" n: $\mathbf{Z}[G/H'] \to \mathbf{Z}[G/H]$ sending $x \in G/H'$ to the formal sum of the $y \in G/H$ with $\pi(y) = x$. For a $\mathbf{Z}[G]$-module M, the map $\mathrm{Hom}_{\mathbf{Z}[G]}(\pi, M)$ is the inclusion map $M^{H'} \to M^H$ on invariants, and $\mathrm{Hom}_{\mathbf{Z}[G]}(n, M)$ is the map $M^H \to M^{H'}$ that sends $m \in M^H$ to $\sum_h hm$ where h runs over a set of representatives in H' of H'/H. For transitive G-sets X and Y we say that a map $\mathbf{Z}[X] \to \mathbf{Z}[Y]$ is a projection (or a norm map) if there are G-set isomorphisms $X \cong G/H$ and $Y \cong G/H'$, with $H \subset H'$ (or $H' \subset H$), so that the induced map $\mathbf{Z}[G/H] \to \mathbf{Z}[G/H']$ is a projection (or norm map).

Example 6.1. For example, to deduce (2.1) from Theorem 2.1 one takes φ in such a way that the summand $\mathbf{Z}[G]$ of $\mathbf{Z}[X]$ is mapped to each of the summands $\mathbf{Z}[G/H_i]$ by the projection map. In the notation of (4.1) we take φ of the form

$$\varphi = \begin{pmatrix} \pi & n & 0 \\ \pi & 0 & n \\ \pi & 0 & 0 \end{pmatrix} = \left(\begin{array}{cccc|c|c} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right).$$

One finds that $B(\varphi; D) = 4$ if $\#D = 1$ (the real case) and $B(\varphi; D) = 2$ if $\#D = 2$ (the complex case). By Theorem 2.1 we have

$$\frac{h(K)}{h(K_1)h(K_2)h(K_3)} = \frac{[U_K : \mu(K)U_{K_1}U_{K_2}U_{K_3}]}{B} W,$$

where $W = w(K)w(\mathbf{Q})^2 w(K_1)^{-1} w(K_2)^{-1} w(K_3)^{-1}$. In Section 2 we addressed roots of unity after (2.5), and in this case it follows that

$$W \ne 1 \iff \#\mu(K) = 8 \iff \mu(K) \not\subset U_{K_1}U_{K_2}U_{K_3},$$

and one checks that we always have

$$W[U_K : \mu(K)U_{K_1}U_{K_2}U_{K_3}] = [U : U_{K_1}U_{K_2}U_{K_3}].$$

Thus, (2.1) follows from Theorem 2.1.

One obtains a "dual" formula by considering the transpose of φ, which is a map $\mathbf{Z}[Y] \to \mathbf{Z}[X]$. We then obtain

$$\frac{h(K)}{h(K_1)h(K_2)h(K_3)} = \frac{B'}{Q}W,$$

where $B' = \#D$, and Q is the index in $U_{K_1} \times U_{K_2} \times U_{K_3}$ of the subgroup generated by $\mu(K_1) \times \mu(K_2) \times \mu(K_3)$ and the image of the map $U_K \to U_{K_1} \times U_{K_2} \times U_{K_3}$ which sends u to $(N_{K/K_i}(u))_{i=1}^3$.

Example 6.2. Let G be the dihedral group of order 8. Let H and H' be non-conjugate non-normal subgroups of order 2 and let C be the cyclic subgroup of order 4. Then we have a character relation

$$1_{\{1\}}^G + 2 \cdot 1_G = 1_H^G + 1_{H'}^G + 1_C^G.$$

Let X and Y be corresponding G-sets with G-orbits of lengths $8, 1, 1$ and $4, 4, 2$, respectively. If we insist that the map φ: $\mathbf{Z}[X] \to \mathbf{Z}[Y]$ is such that the component of rank 8 of $\mathbf{Z}[X]$ maps to the components of rank 4, 4 and 2 by projection maps, then φ is of the form

$$\varphi = \begin{pmatrix} \pi & * & * \\ \pi & * & * \\ \pi & * & * \end{pmatrix} = \left(\begin{array}{cccccccc|c|c} 1&0&0&1&0&0&0&0&a_1&a_4 \\ 0&1&0&0&0&0&1&0&a_1&a_4 \\ 0&0&1&0&0&1&0&0&a_1&a_4 \\ 0&0&0&0&1&0&0&1&a_1&a_4 \\ \hline 1&1&0&0&0&0&0&0&a_2&a_5 \\ 0&0&1&1&0&0&0&0&a_2&a_5 \\ 0&0&0&0&1&1&0&0&a_2&a_5 \\ 0&0&0&0&0&0&1&1&a_2&a_5 \\ \hline 1&0&1&0&1&0&1&0&a_3&a_6 \\ 0&1&0&1&0&1&0&1&a_3&a_6 \end{array}\right).$$

Let $D \subset G$ be a subgroup of G of order 1 or 2. It turns out that $B(\varphi; D)$ does not depend upon the choices of $a_1, \ldots, a_6$. In fact:

$$B(\varphi; D) = \begin{cases} 16, & \text{if } D = \{1\}, \\ 8, & \text{if } D = Z(G), \\ 4, & \text{if } D \ntriangleleft G. \end{cases}$$

If G is the Galois group of a normal extension K of $\mathbf{Q}$ with unit group U, and D is the decomposition group of an infinite prime, then Theorem 2.1 gives

$$\frac{h(K)}{h(K^H)h(K^{H'})h(K^C)} = \frac{[U : \mu(K)U^H U^{H'} U^C]}{B}W,$$

where $W = w(K)w(\mathbf{Q})^2 w(K^H)^{-1} w(K^{H'})^{-1} w(K^C)^{-1}$. By the same argument as in the previous example one can erase W and $\mu(K)$. Thus we recover the formula of Castela

(1978):

$$\frac{h(K)}{h(K^H)h(K^{H'})h(K^C)} = \frac{[U : U^H U^{H'} U^C]}{B} \text{ with } B = \begin{cases} 16, & \text{if } D = \{1\}, \\ 8, & \text{if } D = Z(G), \\ 4, & \text{if } D \ntriangleleft G. \end{cases}$$

Example 6.3. Finally, let us look at the second class number quotient in (3.1). Let $G = A_4$ and for $i \in \{1, 3, 4, 12\}$ let X_i be a transitive G-set of order i. Then the G-set $X = X_1 \cup X_1 \cup X_1 \cup X_{12}$ is linearly equivalent to $Y = X_4 \cup X_4 \cup X_4 \cup X_3$. We can select a homomorphism φ: $\mathbf{Z}[X] \to \mathbf{Z}[Y]$ so that the component map from $\mathbf{Z}[X_{12}]$ to $\mathbf{Z}[Z]$ is a projection for each G-orbit Z of Y. One then finds that

$$\frac{h(K)}{h(K_3) \cdot h(K_4)^3} = 2^r Q,$$

where $r = -10$ if K is real, and $r = -6$ if K is complex, and Q is the index in U_K of the subgroup generated by all elements of degree at most 4 over $\mathbf{Q}$. The formula for the real case was already given by Jehne (1977).

References

Artin, E. (1931a). Die Gruppentheoretischen Struktur der Diskriminanten algebraischer Zahlkörper. *J. reine angew. Math.*, **164**, 1–11.

Artin, E. (1931b). Zur Theorie der L-Reihen mit allgemeinen Gruppencharaktere. *Abh. Math. Sem. Univ. Hamburg*, **8**, 292–306.

Bosma, W., Cannon, J., Playoust, C. (1997). The Magma algebra system I: the user language. *J. Symb. Comput.*, **24**, 235–265.

Bosma, W., de Smit, B. (2000). On arithmetically equivalent fields of small degree (in preparation).

Brauer, R. (1951). Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. *Math. Nachr.*, **4**, 158–174.

Buchmann, J., Ford, D., Pohst, M. (1995). FTP site for number fields of degree 4, Institut de Mathématiques de Bordeaux, available online at `ftp://megrez.math.u-bordeaux.fr/pub/numberfields/degree4/`.

Cannon, J., Cox, B., Holt, D. (2000). Computing the subgroups lattice of a permutation group. *J. Symb. Comput.*, **31**, 149–162, doi: 10.1006/jsco.1999.1016.

Castela, C. (1978). Nombre de classes d'idéaux d'une extension diédrale de degré 8 de **Q**. *Séminaire de Théorie des Nombres de Bordeaux 1977–1978*, Exp. No. 5.

Curtis, C. W., Reiner, I. (1962). *Representation Theory of Finite Groups and Associative Algebras.* New York, John Wiley and Sons.

de Smit, B. (1999). Brauer-Kuroda relations for S-class numbers. Report MI 1999-26, Mathematisch Instituut, Universiteit Leiden.

Dirichlet, P. G., Lejeune, (1842). Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. *J. Reine Angew. Math.*, **24**, 291–371.

Dixon, J. D. (1967). High speed computation of group characters. *Numer. Math.*, **10**, 446–450.

Fröhlich, A., Taylor, M. J. (1991). *Algebraic Number Theory.* Cambridge, Cambridge University Press.

Gassmann, F. (1926). Bemerkungen zu der vorstehenden Arbeit von Hurwitz ('Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe'). *Math. Z.*, **25**, 124–143.

Hilbert, D. (1892). Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. *J. Reine Angew. Math.*, **110**, 204–219.

James, G., Liebeck, M. (1993). *Representations and Characters of Groups.* Cambridge, Cambridge University Press.

Jehne, W. (1977). Über die Einheiten- und Divisorenklassengruppe von reellen Frobeniuskörpern von Maximaltyp. *Math. Z.*, **152**, 223–252.

Klingen, N. (1998). *Arithmetical Similarities.* Oxford, Oxford University Press.

Kuroda, S. (1950). Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.*, **1**, 1–10.

Lang, S. (1993). *Algebra*, 3rd edn. Reading, MA, U.S.A., Addison Wesley.

Matzat, B. H. (1987). *Konstruktive Galoistheorie.* Berlin-New York, Springer-Verlag.

May, W. (1980). Fields with free multiplicity groups modulo torsion. *Rocky Mountain J. Math.*, **10**, 599–604.

Perlis, R. (1977). On the equation $\zeta_K(s) = \zeta_{K'}(s)$. *J. Number Theory*, **9**, 342–360.

Perlis, R. (1978). On the class numbers of arithmetically equivalent fields. *J. Number Theory*, **10**, 458–509.

Schneider, G. J. A. (1990). Dixon's character table algorithm revisited. *J. Symb. Comput.*, **9**, 601–606.

Seidelmann, F. (1918). Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich. *Math. Ann.*, **18**, 230–233.

Serre, J.-P. (1992). *Topics in Galois Theory.* Boston, Jones and Bartlett.

Stevenhagen, P. (1990). Ray class groups and governing fields. *Publ. Math. Fac. Sci. Besançon 1989/90*, 1–94.

van Tieghem, E. (1975). Radikalen van multiplikatieve groepen in de algebraïsche getaltheorie. Thesis, Katholieke Universiteit Leuven.

Walter, C. D. (1979). Kuroda's class number relation. *Acta Arith.*, **35**, 41–51.

Originally Received 25 July 1996
Accepted 14 October 1999