pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

On arithmetically equivalent number fields of small degree

Wieb Bosma[1] and Bart de Smit[2]

[1] Mathematisch Instituut, Universiteit Nijmegen
Postbus 9010, 6500 GL Nijmegen, the Netherlands
bosma@sci.kun.nl

[2] Mathematisch Instituut, Universiteit Leiden
P. O. Box 9512, 2300 RA Leiden, the Netherlands
desmit@math.leidenuniv.nl

Abstract. For each integer n, let $\mathcal{S}_n$ be the set of all class number quotients $h(K)/h(K')$ for number fields K and K' of degree n with the same zeta-function. In this note we will give some explicit results on the finite sets $\mathcal{S}_n$, for small n. For example, for every $x \in \mathcal{S}_n$ with $n \leq 15$, x or x^{-1} is an integer that is a prime power dividing $2^{14} \cdot 3^6 \cdot 5^3$.

1 Introduction

In broad terms the main question on number fields we address in this article is:

to what extent does the zeta-function determine the class number?

Number fields with the same zeta-function are said to be *arithmetically equivalent*. Arithmetically equivalent number fields have many invariants in common. For instance, they have the same degree, discriminant, signature, Galois closure, maximal normal subfield, and number of roots of unity. By considering the residue of the zeta-function we see that arithmetically equivalent K and K' also satisfy $h(K)R(K) = h(K')R(K')$, where h denotes the class number and R denotes the regulator of a number field. Our first result summarizes the possibilities for $h(K)/h(K')$ for fields of degree at most 15.

n \ r_2	0	1	2	3	4	5	6	7
7	2^3	–	2^2	–	–	–	–	–
8	$2^3 3^2$	–	2^2	$2^2 3$	2^2	–	–	–
11	3^5	–	–	–	3^3	–	–	–
12	$2^7 3^3 5^3$	–	2^3	2^3	$2^5 5^2$	$2^4 3^2$	$2^4 3^2 5$	–
13	3^6	–	–	–	3^4	–	–	–
14	2^{10}	–	2^5	–	2^4	2^6	2^5	2^3
15	2^{14}	–	–	–	2^{10}	–	2^8	–

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

Theorem 1. *Let K and K' be non-isomorphic arithmetically equivalent number fields of degree $n \leq 15$. Then n is equal to one of the integers in the first column of the above table, and if the number of complex infinite primes of K is denoted by r_2, the class number quotient $h(K)/h(K')$ is equal to p^k or p^{-k}, where p is a prime number, k is a non-negative integer, and p^k divides the number given in the table for the pair (n, r_2).*

A dash in the table means that this pair (n, r_2) does not occur.

The class number quotient bounds depend on the Galois configuration and the signature in a strong sense: the conjugacy class in the Galois group of complex conjugation. Therefore we first show in Section 2 that there are exactly 19 Galois configurations of degree at most 15 that contain a pair of arithmetically equivalent fields. To produce the list of the 19 possible Galois configurations we used the classification of transitive groups up to degree 15 by Butler, McKay and Royle [2], [3], [17], and a database of subgroup-lattices in the MAGMA-system. A relatively easy run on the MAGMA-system produces the list, and shows that it is complete.

The 19 Galois configurations can also be obtained from theoretical considerations; a better description of a particular configuration is useful for two purposes: it might give clues about how to realize number fields with these Galois groups, and it can also give a humanly readable proof that they contain non-isomorphic fields with the same zeta-function, which may inspire other constructions. We will give such descriptions in Section 2.

In Section 3 we employ methods of [6] to obtain bounds on class number quotients for each configuration. The required symbolic computations are performed in MAGMA using the ideas of [1].

LaMacchia [15] found a family of number fields, parametrized by two rational numbers, each of which is a member of a pair of arithmetically equivalent fields of degree 7. In Section 4 we construct the other member of the pair in terms of the two parameters.

By computing class numbers for pairs in this family and by using earlier results [5] about families in degree 8 constructed with 3-torsion points on elliptic curves, we give a computational proof of the following result in Section 5, showing that some of the bounds on the class number quotients are tight.

Theorem 2. *The set of values of the class number quotient $h(K)/h(K')$ as (K, K') ranges over all pairs of arithmetically equivalent number fields of degree at most 10 that are not totally real, is*

$$\{\frac{1}{4}, \frac{1}{3}, \frac{1}{2}, 1, 2, 3, 4\}.$$

The first known instances of pairs of arithmetically equivalent number fields with different class numbers were generated using a family of fields in degree 8; see [8], and also [1]. For that family, with pairs of fields of the form $\mathbb{Q}(\sqrt[8]{a})$ and $\mathbb{Q}(\sqrt[8]{16a})$, a factor 2^2 will never appear in the class number quotient; see [6].

G. Dyer [10] found the first example of arithmetically equivalent fields in degree 12 with class number quotient 5, by using the method of [5].

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

2 Gassmann triples

The goal of this section is to determine for all $n \leq 15$ all possible Galois groups of arithmetically equivalent number fields of degree n.

Let $L/\mathbb{Q}$ be a Galois extension with Galois group G, and let H and H' be subgroups of G corresponding to intermediate fields $K = L^H$ and $K' = L^{H'}$. Recall that the fields K and K' are isomorphic if and only if the G-sets $X = G/H$ and $X' = G/H'$ are isomorphic, i.e., if there is a G-action preserving bijection between them. We say that the G-sets X and X' are *linearly equivalent* if every $g \in G$ has the same number of fix points on X and on X'. It is well-known that K and K' are arithmetically equivalent if and only if X and X' are linearly equivalent, which is also equivalent to H and H' giving rise to the same permutation character $1_H^G = 1_{H'}^G$ of G; see [4], Exercises 6.3, 6.4.

By a *Gassmann triple* (G, X, X') we mean a group G acting faithfully and transitively on two finite sets X and X', so that X and X' are linearly equivalent but not isomorphic as G-sets. The degree of (G, X, X') is the cardinality of X. The Galois configurations of non-isomorphic arithmetically equivalent fields of degree n are given by the Gassmann triples of degree n up to isomorphism, where we say $(G, X, X') \cong (H, Y, Y')$ if $G \cong H$ and, viewing Y and Y' as G-sets through this group isomorphism, we have $X \cong_G Y$ and $X' \cong_G Y'$.

The question whether for given positive integer n a Gassmann triple of degree n exists has been addressed in [11], [13], [14] with the help of the classification of finite simple groups. The degrees of the Gassmann triples with a *solvable* group have been determined in [7]. Combining these results, one finds that for $n \leq 100$ a Gassmann triple of degree n exists if and only if $n \geq 7$ and

$$n \neq 9,\ 10,\ 17,\ 19,\ 23,\ 25,\ 29,\ 34,\ 37,\ 38,\ 41,\ 43,\ 46,\ 47,\ 53,\ 58,\\ 59,\ 61,\ 67,\ 69,\ 71,\ 74,\ 79,\ 82,\ 83,\ 86,\ 87,\ 89,\ 94,\ 95,\ 97.$$

In particular we see from this list that the only Gassmann triples of degree at most 15 have degree 7, 8, 11, 12, 13, 14, or 15.

As we will see, all Gassmann triples of degree at most 15 can be directly constructed by, or at least derived from, one of the following three methods—see sections 2 and 5 of [7] for details.

(A) For a finite field $\mathbb{F}_q$ and $d \in \mathbb{Z}_{\geq 2}$ consider the vector space $V = {\mathbb{F}_q}^d$ and its $\mathbb{F}_q$-dual $V^* = \mathrm{Hom}(V, \mathbb{F}_q)$. Let S be a subgroup of ${\mathbb{F}_q}^*$ of index s, let $G = \mathrm{GL}_d(\mathbb{F}_q)/S$, and let $X = (V - \{0\})/S$ and $Y = (V^* - \{0\})/S$. If $d \geq 3$ or $s \geq 2$ then (G, X, Y) is a Gassmann triple of degree $s(q^d - 1)/(q - 1)$.

(B) Let $\mathbb{F}_q$ be a finite field of characteristic at least 7, and suppose that $q \equiv \pm 1$ modulo 5. Then $G = \mathrm{PSL}_2(\mathbb{F}_q)$ has two non-conjugate subgroups H and H' that are both isomorphic to A_5, and that are conjugate in $\mathrm{PGL}_2(\mathbb{F}_q)$. Then $(G, G/H, G/H')$ is a Gassmann triple of degree $q(q^2 - 1)/120$.

(C) Let p be a prime number, let $k > 1$ be an integer, and let $m > 1$ be a product of prime powers q that are 0 or 1 modulo p. Then there exist a Gassmann triple (G, X, X') of degree pmk with a 3-step abelian group $G = G_{p,m,k}$ of order $(pm)^k k$.

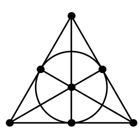
pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

Theorem 3. *There are exactly 19 Gassmann triples (G, X, X') of degree at most* 15*, up to isomorphism. The groups G, viewed as transitive groups acting on X, are given in the table below with Butler-McKay numbering.*

deg.	no.	$\#G$	description of G	construction
7	5	168	$\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{PGL}_3(\mathbb{F}_2)$	(A)
8	15	32	$G_{2,2,2} \cong C_8 \rtimes V_4$	(C)
	23	48	$\mathrm{GL}_2(\mathbb{F}_3)$	(A)
11	5	660	$\mathrm{PSL}_2(\mathbb{F}_{11})$	(B)
12	26	48	$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \cap A_{12}$	(A)
	38	72	$G_{2,3,2}$	(C)
	49	96	$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$	(A)
	57	96	$G_{2,2,3} \cap A_{12}$	(C)
	104	192	$G_{2,2,3}$	(C)
	124	240	$\mathrm{GL}_2(\mathbb{F}_5)/\pm 1$	(A)
13	7	5616	$\mathrm{PGL}_3(\mathbb{F}_3)$	(A)
14	10	168	$\mathrm{PGL}_3(\mathbb{F}_2)$	
	17	336	$\mathrm{PGL}_3(\mathbb{F}_2) \times C_2$	
	19	336	$\mathrm{PGL}_3(\mathbb{F}_2) \times C_2$	(A)
	52	56448	$\mathrm{PGL}_3(\mathbb{F}_2) \wr C_2$	(A)
15	15	180	$\mathrm{GL}_2(\mathbb{F}_4) \cong A_5 \times A_3$	
	21	360	$(S_5 \times S_3) \cap A_8$	
	47	2520	A_7	
	72	20160	$\mathrm{PGL}_4(\mathbb{F}_2) \cong A_8$	(A)

We explain the description of the group and the actions on the two sets X and X' degree by degree.

Degree 7 and degree 14. Taking a 3-dimensional vector space over $\mathbb{F}_2$, we get a Gassmann triple in degree 7 from construction (A). Here the group is $G = \mathrm{GL}_3(\mathbb{F}_2) = \mathrm{PGL}_3(\mathbb{F}_2)$, and the sets X and Y are the sets of points and lines in the projective plane $\mathbb{P}^2(\mathbb{F}_2)$.



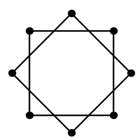
It was shown by Perlis [16] that this is the only Gassmann triple in degree 7.

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

In degree 14 the entries with number 19 and 52 have X equal to two copies of $\mathbb{P}^2(\mathbb{F}_2)$, where the groups are the direct product $\mathrm{PGL}_3(\mathbb{F}_2) \times C_2$ and the wreath product $\mathrm{PGL}_3(\mathbb{F}_2) \wr C_2$ respectively.

We obtain the other triples of degree 14 by adding "orientation" to the triple of degree 7. Let X be the set of points P of $\mathbb{P}^2(\mathbb{F}_2)$ together with a cyclic ordering of the three lines through P. Dually, Y is the set of lines L in $\mathbb{P}^2(\mathbb{F}_2)$ with a cyclic ordering of the three points on L. The group $\mathrm{PGL}_3(\mathbb{F}_2)$ acts naturally on X and Y, and we have a commuting action by C_2 which toggles the orientation of all points and lines. This gives the entries $(14, 10)$ and $(14, 17)$ in the table.

Degree 8. Construction (A) gives a Gassmann triple of degree 8 with group $G = \mathrm{GL}_2(\mathbb{F}_3)$. The other triple can be described with the following graph.



The plane symmetries of this graph form a dihedral subgroup D_8 of order 16 of the group of graph automorphisms. Define another graph automorphism σ by rotating one component over 180 degrees, and leaving the other component fixed. Then D_8 and σ generate a group G of graph automorphisms of order 32. The transitive actions of G on the set of vertices and on the set of edges now give a Gassmann triple of degree 8. We have $G \cong C_8 \rtimes V_4$, where the map $V_4 \to \mathrm{Aut}(C_8)$ is an isomorphism. This triple can also be obtained from construction (C) by taking $p = m = k = 2$. In fact, construction (C) was inspired by this graph theoretical example.

Degree 11. Construction (B) gives a triple of degree 11 with group $\mathrm{PSL}_2(\mathbb{F}_{11})$.

Degree 12. Construction (A) gives a triple with group $\mathrm{GL}_2(\mathbb{F}_5)/\pm 1$. We can also do construction (A) for a finite commutative local ring R rather than a finite field k. Then X is the set of elements in a free module V of rank d that are not annihilated by the maximal ideal of R, and Y is the same set in the R-linear dual of V, and $G = \mathrm{GL}_R(V)$. For $R = \mathbb{Z}/4\mathbb{Z}$ and $d = 2$ this gives entry $(12, 49)$, with $G = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ which is solvable of derived length 3, and entry $(12, 26)$ is a subgroup of index 2 acting on the same sets.

Construction (C) gives the other entries. The group $G_{2,3,2}$ has derived length 2, and the group $G_{2,2,3}$ and its subgroup $G_{2,2,3} \cap A_{12}$ have derived length 3.

Degree 13. The points in the projective plane over $\mathbb{F}_3$ together with the points in the dual projective plane form a Gassmann triple with group $\mathrm{PGL}_3(\mathbb{F}_3)$ and degree 13 by construction (A).

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

Degree 15. Construction (A) gives a Gassmann triple of degree 15 with group $G = \mathrm{GL}_4(\mathbb{F}_2)$. By one of the exceptional isomorphisms of simple groups [9] we have $G \cong A_8$. It turns out that we obtain other Gassmann triples by keeping the same sets, but restricting the group to the subgroup A_7, or $A_5 \times A_3$, or $(S_5 \times S_3) \cap A_8$ of A_8.

This completes the description of the 19 Gassmann triples. The second part of the proof of Theorem 3 is to show that the table is complete. The proof is based on the database of transitive groups of degree d up to 15 due to Butler, McKay and Royle [2], [3], [17]. For each transitive group G from their classification we need to determine all conjugacy classes of subgroups of index d which give rise to the same permutation character of G as a point stabilizer.

A brute force way to do this, is to find all classes of subgroups of index d and test their permutation characters. On a 1100 Mhz Athlon with 256K cache and 512 MB main memory, one can check Theorem 3 in this way with a run of Magma 2.8 of 208 seconds.

While we have no better method than brute force in general, one can often decide that a transitive group is not part of a Gassmann triple by group theoretic means. For instance, it follows from the lemmas below that neither the symmetric nor the alternating group on d letters is part of a Gassmann triple, for any d. From 1997, when the list of 19 triples was first presented at the Journées Arithmétiques in Limoges, up until the summer of 2001 when Magma 2.8 was released, these additional methods were indispensable because the routines for finding subgroups would fail on groups with a large radical index such as the alternating group on 10 letters.

Lemma 1. *Let A be the symmetric or alternating group on a finite set X. For each finite set T with trivial A-action and each A-set Y which is linearly equivalent to $X \cup T$ we have $Y \cong_A X \cup T$.*

Proof. If A is cyclic, then this is clear, so assume that the cardinality n of X is at least 3. In order to prove the lemma we first prove a weaker statement. We claim that on both $X \cup T$ and Y the group A has only one non-trivial orbit and that it has length n. To see this, note that A contains a cyclic subgroup C of order n or $n-1$, and that Y is isomorphic to $X \cup T$ as a C-set. Thus Y has an A-orbit of length n or $n-1$. Since the number of A-orbits of $X \cup T$ and Y is the same, the only case where the claim might fail is the case where Y consists of a trivial G-set, one orbit of length 2 and one orbit of length $n-1$. But then A embeds into $C_2 \times S_{n-1}$ because A acts faithfully on Y. By comparing cardinalities, and using the fact that $A_4 \not\cong C_2 \times S_3$ one sees that this is impossible. This proves the claim. The lemma now follows by applying the claim to A and to a point stabilizer in A of a point in X.

Lemma 2. *Let G be a finite group and X a transitive G-set and let k be a positive integer. Suppose that $X = X_1 \cup \cdots \cup X_k$ is a decomposition of X into blocks and let A be the subgroup of G of elements that fix $X_2 \cup \cdots \cup X_k$ pointwise. If A is the symmetric or alternating group on X_1 and A is non-abelian, then every G-set which is linearly equivalent to X, is G-isomorphic to X.*

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

Proof. We may assume that G acts faithfully on X. Let Y be a G-set which is linearly equivalent to X. For $i \in \{1, \ldots, k\}$ let A_i be the subgroup of G of elements which fix $X \setminus X_i$ pointwise. Then the A_i are the distinct conjugates of $A = A_1$. By the previous lemma, each A_i has exactly one non-trivial orbit Y_i on Y, and we have $X_i \cong_{A_i} Y_i$. It follows that the collection of all Y_i is G-stable, so that $Y_1 \cup \cdots \cup Y_k$ is a sub-G-set of Y. But since G has the same number of orbits on X and Y we have $Y = Y_1 \cup \cdots \cup Y_k$, and by counting elements we see that the Y_i are disjoint. It follows that X and Y are isomorphic over the normal subgroup $N = A_1 \times \cdots \times A_k$ of G. This means that the G-set B of bijections from X to Y contains an N-invariant element. Since A is non-abelian, the action of A on X_1 is two-transitive and $\mathrm{Aut}_A(X_1) = \{1\}$. It follows that $\#B^N = 1$. Since N is normal in G, the set B^N is a G-stable subset of B, and its unique element is a G-isomorphism from X to Y. This proves the lemma.

These lemmas tell us that the 28 largest transitive groups of degree less than 16, with orders ranging from 648000 to 1307674368000 = 15!, are not part of any Gassmann triple. The biggest group on which we use the brute force method is the 57th transitive group of degree 14, which has order 645120. The largest radical index where we apply brute force is 95040, which is the order of the simple group M_{12}, the Mathieu group in degree 12.

In all 19 Gassmann triples of degree less than 16 we found exactly two conjugacy classes of subgroups inducing the same permutation character, and they are conjugate by an outer automorphism. In other words, for these 19 triples we have $(G, X, X') \cong (G, X', X)$. This completes the proof of the Theorem.

The list of Gassmann triples of degree less than 24, based on the classification of transitive groups of degree up to 23 of A. Hulpke, was presented by the second author at a meeting in Durham in the summer of 2000. It was computed in a similar way by improving the lemmas above. A brute force run on Magma 2.8 seems to get stuck in degree 16.

3 Bounds on the class number quotient

In the previous section we computed the possible Galois groups associated to a pair of non-isomorphic arithmetically equivalent fields. In this section we compute a bound on the class number quotient in each of the cases we found. To do this, we use the method explained in [6] and [1].

Let $L/\mathbb{Q}$ be a Galois extension with Galois group G, and suppose we have subgroups H, H' so that the fields $K = L^H$ and $K' = L^{H'}$ are arithmetically equivalent. Then there is an injective $\mathbb{Z}[G]$-linear map $\phi : \mathbb{Z}[G/H] \to \mathbb{Z}[G/H']$. For each subgroup J of G one has an induced map $\phi_J : \mathbb{Z}[J\backslash G/H] \to \mathbb{Z}[J\backslash G/H']$. Now let $D \subset G$ be a decomposition group at infinity. In other words, choose an embedding $L \subset \mathbb{C}$ and let D be the subgroup of order 1 or 2 of G generated by complex conjugation. For $x, y \in \mathbb{Q}$ we say that x divides y if $y \in \mathbb{Z}x$.

Proposition 1. *The class number quotient* $\dfrac{h(K)}{h(K')}$ *divides* $\dfrac{\#Cok(\phi_D)}{\#Cok(\phi_G)}$.

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

One gets a bound on the left hand side by computing the smallest possible value of the right hand side if one lets ϕ vary. There are some improvements on this bound, which are explained in [1]. Using these improvements we get the following table of bounds for the 19 Gassmann triples.

deg.	class number bound for given r_2								$\#G$	no.
	0	1	2	3	4	5	6	7		
7	2^3	–	2^2	–	–	–	–	–	168	5
8	2^3	–	2^2	2^2	2^2	–	–	–	32	15
	3^2	–	–	3	1	–	–	–	48	23
11	3^5	–	–	–	3^3	–	–	–	660	5
12	2^7	–	–	–	2^4	–	2^3	–	48	26
	3^3	–	–	–	–	3^2	3^2	–	72	38
	2^7	–	–	–	2^5	2^4	2^4	–	96	49
	2^4	–	2^3	–	2^2	–	2	–	96	57
	2^4	–	2^3	2^3	2^2	2^2	2	–	192	104
	5^3	–	–	–	5^2	–	5	–	240	124
13	3^6	–	–	–	3^4	–	–	–	5616	7
14	2^{10}	–	–	–	–	–	2^5	–	168	10
	2^{10}	–	–	–	–	2^6	2^5	2^3	336	17
	2^6	–	–	–	2^4	–	–	2^3	336	19
	2^6	–	2^5	–	2^4	–	–	2^3	56448	52
15	2^{10}	–	–	–	–	–	2^6	–	180	15
	2^{10}	–	–	–	–	–	2^6	–	360	21
	2^{14}	–	–	–	–	–	2^8	–	2520	47
	2^{14}	–	–	–	2^{10}	–	2^8	–	20160	72

We list the bounds by degree $[K : \mathbb{Q}] = \#X$, the number of the group in the classification, and the number r_2 of complex infinite primes of K, which is equal to the number of orbits of length 2 of the D on X. Combining the lines for a fixed degree we obtain a proof of Theorem 1.

In the table we combined results for the different subgroups D of G which give rise to the same r_2. So for specific D one can sometimes give a better bound than the one given in the table. For some of the bounds we know they can only be attained under certain strong conditions. We refer to [1], Proposition 5.2, for details.

4 A family of arithmetically equivalent fields of degree 7

In order to test to what extent the bound in the previous section are sharp, we computed class groups for particular instances. For a good supply of arithmetically equivalent fields of degree 7 we use a family of LaMacchia [15]:

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

$$f_{s,t}(X) = X^7 + (-6t+2)X^6 + (8t^2+4t-3)X^5 + (-s-14t^2+6t-2)X^4 + (s+6t^2-8t^3-4t+2)X^3 + (8t^3+16t^2)X^2 + (8t^3-12t^2)X - 8t^3.$$

LaMacchia proved that over the function field $\mathbb{Q}(s,t)$ this polynomial is irreducible, and that its Galois group is isomorphic $G = \mathrm{GL}_3(\mathbb{F}_2)$. If we specify s and t to particular values in $\mathbb{Q}$, then the resulting polynomial in $\mathbb{Q}[X]$ might be reducible, and even if it is irreducible, then its Galois group is a subgroup of G which might not be the whole of G. But Hilbert's irreducibility theorem guarantees that there are infinitely many pairs $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ for which the resulting polynomial $f_{a,b}$ in $\mathbb{Q}[X]$ is irreducible with Galois group G.

Proposition 2. *Let $a, b \in \mathbb{Q}$; if $f_{a,b}$ is irreducible in $\mathbb{Q}[X]$ then $f_{-a,b}$ is also irreducible, and the number fields of degree 7 defined by $f_{a,b}$ and $f_{-a,b}$ are arithmetically equivalent. If, moreover, $f_{a,b}$ has full Galois group $GL_3(\mathbb{F}_2)$ then these fields are not isomorphic.*

Let us consider the action of G on the 7 points of the projective plane over $\mathbb{F}_2$. The induced action on the 35 unordered triples of distinct points has two orbits: the orbit of length 7 of collinear triples, and the orbit of length 28 of non-collinear triples. The idea is that if G is the Galois group of a polynomial f over $\mathbb{Q}$ of degree 7, we can compute the polynomial P of degree 35 whose roots are all sums of three distinct roots of f. If P is a product of two irreducible polynomials P_7 and P_{28} of degree 7 and degree 28, then the field defined by P_7 is the field which is arithmetically equivalent but not isomorphic to the field defined by f.

Let us first address the issue of computing P given f. If f is monic with integer coefficients, then we could find approximations of the roots of f in $\mathbb{C}$, and then compute approximations of P. Since $P \in \mathbb{Z}[X]$ we can round off the coefficients to integers and if there is no unfortunate error blow-up then this gives the correct P.

An alternative approach uses resultants. Let us write

$$f(X) = \prod_{i=1}^{7}(X - \alpha_i).$$

For $k \in \mathbb{Q}$ with $k \neq 0$ we put

$$f_k(X) = \prod_i (X - k\alpha_i) = k^7 f(X/k).$$

Denote by R the resultant with respect to the variable T. Then we have

$$R(f_{-1}(T-X), f(T)) = \prod_{i,j}^{7}(X - \alpha_i - \alpha_j) = Q_1(X)^2 \cdot f_2(X),$$

where

$$Q_1(X) = \prod_{i<j}(X - \alpha_i - \alpha_j).$$

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

By computing the resultant, dividing by $f_2(X)$ and taking the square root we can thus compute $Q_1(X)$ without working in any larger fields than $\mathbb{Q}$. Similarly, we can find an expression for our polynomial P:

$$R(f_{-1}(T-X), Q_1) = \prod_{i<j}\prod_{k}(X - \alpha_i - \alpha_j - \alpha_k) = P(X)^3 Q_2(X),$$

with

$$Q_2 = \prod_{i}\prod_{j\neq i}(X - \alpha_i - 2\alpha_j).$$

We can find Q_2 by computing one more resultant:

$$R(f_{-1}(T-X), f_2(T)) = Q_2(X) f_3(X).$$

The three resultant equations allow one to successively compute Q_1, Q_2 and P by taking resultants, computing quotients and take a square and a cube root.

Note that the largest resultant has degree 147, but it turns out that one can do this computation for any given $f \in \mathbb{Q}[X]$ quite easily on a computer. We then find the degree 7 factor P_7 of P by a rational polynomial factorization algorithm.

If we take $f = f_{s,t}$ it would be nice to obtain P_7 as a polynomial with coefficients in $\mathbb{Q}(s,t)$, so that we do not have to go through the resultant computation for each pair of rational numbers a, b. One could try to do this with the resultant-method given above, with base-field $\mathbb{Q}(s,t)$ rather than $\mathbb{Q}$. This symbolic computation turns out not to be feasible. Instead, we compute P_7 for many values of a and b in $\mathbb{Z}$ and then interpolate. To see how this works, let us consider the polynomial P. The coefficients of P can be expressed in terms of the symmetric functions $\sigma_1, \ldots, \sigma_7$ in $\alpha_1, \ldots, \alpha_7$, where $f = X^7 - \sigma_1 X^6 + \sigma_2 X^5 - \ldots + \sigma_7$. Giving each σ_i degree i we see that all coefficients of P have degree at most 35. It follows that the coefficients have at most degree 35 in s and t. In fact, since s occurs only in σ_3 and σ_4, the degree in s is at most 11. The factor P_7 of P therefore also has coefficients $c_i(s,t)$ which are polynomials of degree at most 11 and 35 in s and t. With these bounds on the degree we can now find these polynomials by interpolating. For fixed t_0 we need at least 12 values of s to determine the polynomial $c_i(t_0, s)$, and if we do this for at least 36 values of t_0 then we know $c_i(t,s)$ by interpolation. We thus computed that P_7 is equal to the polynomial

$$\begin{aligned} g_{s,t} = {} & X^7 + (-18t+6)X^6 + (124t^2 - 64t + 6)X^5 + (-408t^3 + 208t^2 - 4t - 16)X^4 \\ & + (6(t-1)s + 640t^4 - 156t^3 - 116t^2 + 84t - 27)X^3 \\ & + ((-36t^2 + 36t - 12)s - 384t^5 - 152t^4 + 120t^3 + 88t^2 - 34t - 6)X^2 \\ & + (-s^2 + (48t^3 - 20t^2 - 2t - 2)s - 64t^5 - 84t^4 + 52t^3 - 8t^2 - 12t)X \\ & + (-8t^3 - 4t^2)s + 384t^6 + 80t^5 - 88t^4 - 24t^3. \end{aligned}$$

To finish the proof of the proposition one notices that $f_{-s,t}(X)$ divides the polynomial $X^7 g_{s,t}((X-1)(1+2t/X))$, which means that the field defined by $g_{s,t}$ is contained in the field defined by $f_{-s,t}$. Thus, the polynomials $f_{s,t}$ and $f_{-s,t}$ give the Galois configuration of the desired Gassmann triple (G, X, X') over the field $\mathbb{Q}(s,t)$.

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

If we specify s and t to rational numbers a, b, and $f_{a,b} \in \mathbb{Q}[X]$ is irreducible, then the Galois group of $f_{a,b}$ is a subgroup G_0 of G which is transitive on X. Then G_0 contains an element of order 7, so it is also transitive on X', so $f_{-a,b}$ is also irreducible. Since X is linearly equivalent to X' over G_0, the two fields are arithmetically equivalent. Since there is only one Gassmann triple for degree 7 the two fields are isomorphic if and only if $G_0 \neq G$.

5 Class number computations

In this section we prove Theorem 2.

The first three lines in the table of Theorem 1 show that for arithmetically equivalent fields K and K' of degree at most 10 that are not totally real, the class number quotient $h(K)/h(K')$ or its reciprocal lies in $\{1, 2, 3, 4\}$. It remains to exhibit examples to prove that all possibilities occur. In [5] examples are given of arithmetically equivalent fields K, K' of degree 8 with $h(K)/h(K') = 3$.

We use the family of polynomials $f_{s,t}$ and $f_{-s,t}$ from the previous section to generate examples for the remaining cases. Using MAGMA we selected the subset of 1091 pairs of integers (a, b) with $0 \leq a, |b| \leq 100$, for which the field discriminant of the number field generated by $f_{a,b}$ has less than 25 decimal digits. In 276 of these cases the fields are totally real and in all other cases there are 2 pairs of complex embeddings.

We have used h and h' to denote the class numbers of the number fields generated by the polynomials $f_{s,t}$ and $f_{-s,t}$. The table below summarizes the class number quotients found.

r_2 \ h/h'	1	1/2	2/1	1/4	4/1	$\sum$
2	607	104	98	2	4	815
0	210	38	25	2	1	276

The last row, representing the 276 totally real fields found, is given here for comparison, and to show that no factor 8 was found in the class number quotients.

The table below lists, of the 815 pairs that are not totally real, those with class number quotients 4 and 1/4, and the smallest (in terms of discriminant) with class number quotients 1, 2 and 1/2.

Class groups (and unit groups) in MAGMA are computed by a method that generates relations between prime ideals of bounded norm. This is guaranteed to give the correct class number if all primes up to the Minkowski bound are taken into consideration. For fields of small discriminant, including the first example with class number quotient 4 listed in the table, the method can be used to certify the class number. It took around 7 minutes of CPU time to find the class number pair for $(62, -1)$ with MAGMA this way.

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

(a, b)	D	factorization of D	h/h'
$(8, 1)$	232745536	$2^6 \cdot 1907^2$	$1/1$
$(7, -1)$	24497571289	$281^2 \cdot 557^2$	$1/2$
$(5, 1)$	31811219449	$59^2 \cdot 3023^2$	$2/1$
$(62, -1)$	3770079362544784	$2^4 \cdot 15350243^2$	$4/1$
$(22, -6)$	2429680593739514347584	$2^6 \cdot 3^6 \cdot 11^4 \cdot 71^2 \cdot 101^2 \cdot 263^2$	$1/4$
$(83, 4)$	3174516214584075350089	56342845283^2	$6/24$
$(81, -6)$	10630565571038999396281	$19^2 \cdot 557^2 \cdot 1697^2 \cdot 5741^2$	$8/2$
$(53, -6)$	10726579028522017397529	$3^4 \cdot 13^2 \cdot 1453^2 \cdot 609227^2$	$8/2$
$(2, -6)$	155678051656088618455296	$2^8 \cdot 3^6 \cdot 37^2 \cdot 24684721^2$	$4/1$

For large discriminants this computation is no longer feasible. In that case the Minkowski bound can be replaced by the (usually much smaller) Bach bound, at the cost of correctness only being guaranteed under assumption of the generalized Riemann hypothesis. This was used to compute the other class number pairs, each taking less than a minute.

Alternatively, some local computations with independent units together with bounds on the regulator may provide fairly fast provably correct results; cf. [8]. For this Magma has a built in function `pFundamentalUnits`, which we also used to verify the above class number quotients.

References

1. Wieb Bosma, Bart de Smit, *Class number relations from a computational point of view*, J. Symbolic Computation **31** (2001), 97–112.
2. G. Butler, *The transitive groups of degree fourteen and fifteen*, J. Symbolic Computation **16** (1993), 413–422.
3. G. Butler, J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911.
4. J. W. S. Cassels, A. Fröhlich (eds), *Algebraic Number Theory*, Academic Press (1986) (reprint).
5. B. de Smit, *Generating arithmetically equivalent number fields with elliptic curves*, in: J. P. Buhler (Ed.), Algorithmic Number Theory (Proceedings ANTS III), Lecture Notes in Computer Science, Vol. 1423. Springer-Verlag, Berlin (1998), 392–399.
6. B. de Smit, *Brauer-Kuroda relations for S-class numbers*, Acta Arithmetica **98** (2001), 133–146.
7. B. de Smit, H. W. Lenstra, Jr., *Linearly equivalent actions of solvable groups*, J. Algebra **228** (2000), 270–285.
8. B. de Smit and R. Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. **31** (1994), 213–215.
9. L. E. Dickson, *Linear groups with an exposition of the Galois Field Theory*, Dover (1958), reprint of 1901 original.

pp. 67–79 in: *ANTS Proceedings 2002*, Fieker, Kohel (eds.), LNCS 2369, Springer-Verlag 2002.

10. G. Dyer, *Two arithmetically equivalent number fields with class number quotient five*, preprint, 1999, Mathematical Research Experiences for Undergraduates at Louisiana State University, LEQS.
11. W. Feit, *Some consequences of the classification of finite simple groups*, in: B. Cooperstein and G. Mason (eds.), *The Santa Cruz conference on finite groups 1979* Proc. Sympos. Pure Math. Vol. 37, Amer. Math. Soc., Providence (1980), 175–181.
12. F. Gassmann, *Bemerkungen zu der vorstehnden Arbeit von Hurwitz*, (*'Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe'*), Math. Z. **25** (1926), 124–143.
13. R. M. Guralnick, *Subgroups inducing the same permutation representation*, J. Algebra **81** (1983), 312–319.
14. R. M. Guralnick and D. B. Wales, *Subgroups inducing the same permutation representation, II*, J. Algebra **96** (1985), 94–113.
15. S. E. LaMacchia, *Polynomials with Galois group PSL*$(2,7)$, Comm. Algebra **8** (1980), 983–992.
16. R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), 342–360.
17. G. F. Royle, *The transitive groups of degree twelve*, J. Symbolic Computation **4** (1987), 255–268.