MINIMAL DISCRIMINANTS FOR FIELDS WITH SMALL FROBENIUS GROUPS AS GALOIS GROUPS

CLAUS FIEKER AND JÜRGEN KLÜNERS

Abstract. We apply class field theory to the computation of the minimal discriminants for certain solvable groups. In particular we apply our techniques to small Frobenius groups and all imprimitive degree 8 groups such that the corresponding fields have only a degree 2 and no degree 4 subfield.

1. Introduction

There is a long tradition in number theory to compile tables of number fields matching certain criteria. Commonly one computes tables of fields of a given degree or a specific Galois group that are complete with respect to some bound on the discriminant. So far, most of the tables were build with the help of geometric methods based on a theorem of Hunter [6, Thm 9.3.1] which states the existence of primitive elements that are not too large in comparison to the discriminant.
Recently the advent of constructive methods in class field theory [6, 9] made it feasible to build large tables with the help of class field theory rather than using the geometric methods. Of course, this applies mainly to the construction of fields with solvable Galois group. For example, in [5] class field theory is used to compute the minimal discriminants for all octic fields containing a quartic subfield.
In this paper we illustrate the use of class field theory to construct tables of fields where the Galois group is a small solvable group or a Frobenius group. In particular we prove the minimal discriminants for octic fields having only a degree 2 subfield and no degree 4 one. This is done by an analysis of the relative Galois group over the degree 2 field. Since the only possibilities here are $\mathfrak{A}_4$ and $\mathfrak{S}_4$ we are in the situation of solvable groups.
As a further application we construct the minimal fields with Galois group isomorphic to $C_p \rtimes C_l$ for $p \in \{7, 11, 13\}$ and all $1 < l \mid (p-1)$ and two primitive solvable groups in degree 8.

2. Notations

Let K/k be a finite field extension. By $d_{K/k}$ we denote the relative discriminant of the ring of integers $\mathbb{Z}_K$ of K as an ideal of k. In addition, d_K always denotes the absolute discriminant (so $d_{K/\mathbb{Q}} = d_K\mathbb{Z}$). We say that K/k has Galois group G, or short that K is a G-field, if the normal closure N of K/k has Galois group G over k. $\mathrm{N}_{K/k}$ denotes the norm function extended to ideals. Since the fractional ideals of the ring of integers of any number field form a group that is freely generated by the prime ideals, we write $\sqrt[r]{\mathfrak{a}}$ or $\mathfrak{a}^{1/r}$ to denote the unique ideal $\mathfrak{b}$ such that $\mathfrak{b}^r = \mathfrak{a}$ if such an ideal exists.

Part of this article was written during a visit by the second author to the Computational Algebra Group at the University of Sydney in September, 2001.

3. Discriminant Relations

Let N/k be a normal extension of number fields with Galois group G. We denote by $k \subseteq K_i \subseteq N$ intermediate fields of N/k which are fixed under $H_i \leq G$. The aim of this section is to determine relations between the discriminants of these fields. Using the notation of [19, VI.3] we denote by s_{G/H_i} the permutation character associated to the permutation representation of G acting on G/H_i. The following theorem is an immediate consequence of Proposition 6 and Corollary 1 in [19, VI.3].

Theorem 1. *For $a_i \in \mathbb{Z}$ let*

$$\sum_{i=1}^{r} a_i s_{G/H_i} = 0.$$

Then we get

$$\prod_{i=1}^{r} d_{K_i/k}^{a_i} = 1.$$

We remark that relations between the permutation characters give relations between the corresponding Dedekind zeta-functions [2, 14].

4. Frobenius groups

In this section we show that the so-called Frobenius groups have non-trivial relations as in Theorem 1. We denote by E the trivial group of size 1.

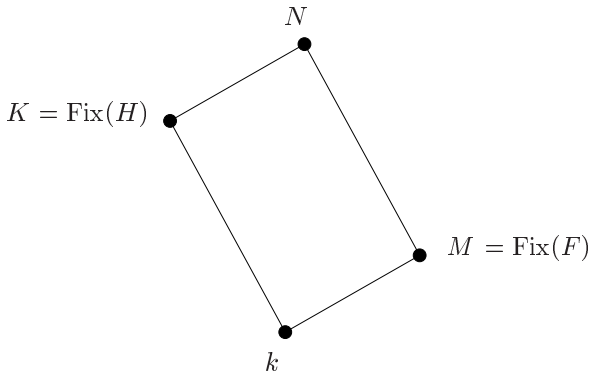
Definition 2. *Let $G = F \rtimes H$ be a finite group with $H \cap H^g = E$ for all $g \in G \setminus H$ and $|F|, |H| \neq 1$. Then G is called a Frobenius group with (Frobenius) kernel F and complement H. The permutation representation where G acts on G/H is called natural permutation representation.*

Example 3. *The dihedral groups D_n of size $2n$ with n odd, $\mathfrak{S}_3$, and $\mathfrak{A}_4$ are Frobenius groups.*

Theorem 4. *Let G be a Frobenius group with kernel F and complement H. Let N/k be a normal field extension with $\mathrm{Gal}(N/k) \cong G$. We denote by $K = \mathrm{Fix}(H)$ the fixed field of H and with $M = \mathrm{Fix}(F)$ the fixed field of F. Then*

$$d_{K/k} = d_{M/k}^{s} \mathrm{N}_{M/k}(d_{N/M})^{1/|H|},$$

where $s = \frac{|F|-1}{|H|}$.



Proof. We have the following relation of permutation characters, e.g. [10, p. 323]:

$$|H| s_{G/G} + s_{G/E} = |H| s_{G/H} + s_{G/F}.$$

The discriminant relation now follows using Theorem 1 and the fact that $d_{N/k} = d_{M/k}^{|F|} \mathrm{N}_{M/k}(d_{N/M})$. □

Let us describe how this theorem can be used to construct all extension fields K of k such that $\mathrm{N}_{k/\mathbb{Q}}(d_{K/k}) \leq B$ for some bound B, assuming that we are able to do the same for H-extensions of k and F-extensions of arbitrary number fields. For this application it is not necessary for G to be a Frobenius group. We only need to have a discriminant relation between the fields in the diagram. To make the method effective, F has to be Abelian.

Algorithm 5.

(1) *Compute all fields M/k with Galois group H such that* $\mathrm{N}_{k/\mathbb{Q}}(d^s_{M/k}) \leq B$.
(2) *For all these M do*
(3) *Compute all extensions N/M with Galois group F such that*
   (a) $\mathrm{N}_{k/\mathbb{Q}}(d^s_{M/k}\mathrm{N}_{M/k}(d_{N/M})^{1/|H|}) \leq B$,
   (b) $\mathrm{Gal}(N/k) = G$.
(4) *end for M*

In this approach we assume that we are able to construct fields M with Galois group H (which is smaller than G). In our applications the group F is an abelian group. Therefore we can apply class field theory in step 3 of this algorithm (see Sections 5 and 6).
In the following we derive some relations for Frobenius groups using Theorem 4. We use the notation nTm for the m-th transitive group of degree n in the ordering of [7]. This is the group we get by typing `TransitiveGroup(n,m)`; in Gap [18] or Magma [4].

Corollary 6. *Let G be one of the following Frobenius groups and N/k be a normal field extension with Galois group G. Using the notation of Theorem 4 we get the following relations:*

(1) $G = \mathfrak{A}_4 = V_4 \rtimes C_3$*:* $d_{K/k} = d_{M/k}\mathrm{N}_{M/k}(d_{N/M})^{1/3}$.
(2) *For $p \in \mathbb{P}$ and $1 \neq l \mid (p-1)$ let* $G := C_p \rtimes C_l$*:* $d_{K/k} = d_{M/k}^{\frac{p-1}{l}}\mathrm{N}_{M/k}(d_{N/M})^{1/l}$.
(3) $G = 8T25 = C_2^3 \rtimes C_7$*:* $d_{K/k} = d_{M/k}\mathrm{N}_{M/k}(d_{N/M})^{1/7}$.

5. Class Fields

In order to construct our fields we will make use of class field theory. We have to construct C_2, C_3 and V_4-extensions of number fields with restrictions on the absolute Galois group, the ramified primes and the absolute discriminant of the resulting field.
We recall some of the necessary notations from class field theory. For a complete account of the theoretical side see e.g. [15], for the practical side [6, 9]. We will restrict ourselves to the ideal theoretic approach to class field theory which is better suited for practical computations than the idèle-theoretic one.
For the remainder of this section we fix a base field M with its ring of integers $\mathbb{Z}_M$. Let $\mathfrak{m} := (\mathfrak{m}_0, \mathfrak{m}_\infty)$ be a module, i.e. $\mathfrak{m}_0$ an integral ideal of $\mathbb{Z}_M$ and $\mathfrak{m}_\infty$ a set of real places of M. An (fractional) ideal $\mathfrak{a}$ of $\mathbb{Z}_M$ is said to be coprime to $\mathfrak{m}$ iff it is coprime to $\mathfrak{m}_0$. For an algebraic number $\alpha \in M$ we define $\alpha \equiv 1 \mod {}^*\mathfrak{m}$ as $\alpha \equiv 1 \mod \mathfrak{m}_0$ and $v(\alpha) > 0$ for all $v \in \mathfrak{m}_\infty$. We say that $\mathfrak{m}$ divides some other module $\mathfrak{n}$ iff $\mathfrak{m}_0|\mathfrak{n}_0$ and $\mathfrak{m}_\infty \subseteq \mathfrak{n}_\infty$.
The ray class group $\mathrm{Cl}_\mathfrak{m}$ is the factor group $I^\mathfrak{m}$ of ideals coprime to $\mathfrak{m}$ by the subgroup $P_\mathfrak{m}$ of principal ideals generated by elements $\gamma \equiv 1 \mod {}^*\mathfrak{m}$. For $\mathfrak{m}|\mathfrak{n}$ we have a canonical epimorphism from $\mathrm{Cl}_\mathfrak{n}$ onto $\mathrm{Cl}_\mathfrak{m}$.
Let $P_\mathfrak{m} \leq U \leq I^\mathfrak{m}$ be arbitrary. The smallest module $\mathfrak{n}$ such that $I^\mathfrak{m}/U \to I^\mathfrak{n}/UP_\mathfrak{n}$ is injective is called the conductor $\mathfrak{f}_U$ of U. $P_\mathfrak{n} \leq U' \leq I^\mathfrak{n}$ is equivalent to U iff the preimages of $\mathrm{Cl}_{\mathfrak{m}\mathfrak{n}} \to I^\mathfrak{n}/U'$ and $\mathrm{Cl}_{\mathfrak{m}\mathfrak{n}} \to I^\mathfrak{m}/U$ coincide. In this case we write $U' \sim U$. The main results from class field theory we need are

Theorem 7. (1) *For any U there is exactly one abelian extension N/M such that $\mathrm{Gal}(N/M) \cong I^{\mathfrak{m}}/U$ where the isomorphism is given by the Artin-map: $\mathfrak{a}U \mapsto (\mathfrak{a}, N/M) \in \mathrm{Gal}(N/M)$ which maps prime ideals to their Frobenius automorphism.*

(2) *For any abelian extension N/M there is exactly one class of factor groups $I^{\mathfrak{m}}/U$ such that $\mathrm{Gal}(N/M) \cong I^{\mathfrak{m}}/U$.*

(3) *For any automorphism σ of M we have*

$$(\sigma\mathfrak{a}, N/M) = \sigma^{-1}(\mathfrak{a}, N/M)\sigma$$

(4) *Let $\mathfrak{f}$ be the conductor of $I^{\mathfrak{m}}/U$ and N/M the corresponding abelian extension. Then the ramified primes of N/M are exactly the divisors of $\mathfrak{f}$.*

Suppose now M/k normal with $\mathrm{Gal}(M/k) = H = \langle \sigma_1, \ldots, \sigma_r \rangle$.
In order for N/k to be normal it is necessary and sufficient that $\sigma_i(U) \sim U$ for $1 \leq i \leq r$, which in particular implies $\sigma_i(\mathfrak{f}_U) = \mathfrak{f}_U$. If $\sigma_i(\mathfrak{m}) = \mathfrak{m}$ then this simplifies to $\sigma_i(U) = U$. In this situation the Galois group of N/k is an extension of $\mathrm{Gal}(N/M)$ by $\mathrm{Gal}(M/k)$:

$$0 \to \mathrm{Gal}(N/M) \cong I^{\mathfrak{m}}/U \to \mathrm{Gal}(N/k) \to \mathrm{Gal}(M/k) \to 0$$

This extension is central iff $\mathfrak{a}U = \sigma_i(\mathfrak{a})U$ for all classes $\mathfrak{a}U$ of $I^{\mathfrak{m}}/U$ and all $1 \leq i \leq r$. If, in addition, H is cyclic, N/k is abelian.

6. p-EXTENSIONS

By the results of the last section, the computation of p-extensions of M that are normal (central, abelian) over k is reduced to the problem of finding suitable quotients of ray class groups.
To check $\sigma_i(U) \sim U$ we will assume that $\sigma_i(\mathfrak{m}) = \mathfrak{m}$ holds. In what follows $\mathfrak{m}_0$ is always generated by some ideal of k so this condition will always be fulfilled. $\mathfrak{m}_\infty$ will either be empty or contain all real places. Since we are free to choose U within its equivalence class, these choices are no restriction.
We want to compute a p-extension N of M such that

(1) $\mathrm{Gal}(N/M) \cong F = C_p^s$ for some prime p and some integer s,
(2) N/k is normal (possibly additional restrictions)
(3) and some conditions on the discriminant of N/M are met.

The last properties just imposes some conditions on the module $\mathfrak{m}$ that we will ignore in this section. However these conditions will be important in the algorithms. Assume $\mathfrak{m}$ is given and we want to compute $P_{\mathfrak{m}} \leq U \leq I^{\mathfrak{m}}$ such that $I^{\mathfrak{m}}/U \cong F$ and N/k normal holds. Since p is the exponent of F, we obtain $(I^{\mathfrak{m}})^p \leq U \leq I^{\mathfrak{m}}$. By our choice of $\mathfrak{m}$, $\mathrm{Cl}_{\mathfrak{m}}[p] := I^{\mathfrak{m}}/(I^{\mathfrak{m}})^p$ is an $\mathbb{F}_p[H]$-module, and U corresponds to an $\mathbb{F}_p[H]$ submodule. The problem is now reduced to a purely module theoretic one and can be solved using the tools of module theory [11, 16].
In the special case of $H = \langle \sigma \rangle$ however, the situation is much easier, here the problem reduces to finding σ-invariant subspaces of the $\mathbb{F}_p$-vectorspace $\mathrm{Cl}_{\mathfrak{m}}[p]$.
Here we obtain the following:

Corollary 8. (1) *U exists iff there is a σ-invariant subspace of dimension s.*

(2) *For $s = 1$, N/k is abelian iff U is an eigenspace to the eigenvalue 1.*

An algorithmic solution for the special case $s = 1$ if we want all subgroups U giving central extensions is contained in

Algorithm 9. (1) *Set $\tilde{F} := \mathrm{Cl}_{\mathfrak{m}}[p]/(\mathrm{Id} - \sigma)\,\mathrm{Cl}_{\mathfrak{m}}[p]$.*

(2) *Using* [3] *or* [6, Thm 4.1.18] *find all subgroups U of index p.*

In order to find non-central extensions we use $(\lambda\,\mathrm{Id} - \sigma)$ for all $1 \neq \lambda \in \mathbb{F}_p^\times$ instead of $(\mathrm{Id} - \sigma)$ in step 1.

(Note that this procedure can also be applied to the problem of finding central extensions of cyclic fields of prime-power order.)
Now we want to give some necessary conditions for the module $\mathfrak{m}$. We can restrict ourselves to modules $\mathfrak{m}$ which are conductors. We know that exactly the prime ideals dividing $\mathfrak{m}_0$ are ramified in the corresponding abelian extension. Furthermore a prime ideal $\mathfrak{p}$ is wildly ramified if and only if $\mathfrak{p}^2 \mid \mathfrak{m}_0$. Therefore we get that all prime ideals but the ones dividing the degree have exponent 0 or 1. In the following lemma we give an estimate for the exponent of wildly ramified primes.

Lemma 10. *Let N/M be a cyclic extension of prime degree p and $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_k$ containing p which is ramified in N/M. Denote by e the ramification index (over M) of an ideal $\mathfrak{P}$ lying over $\mathfrak{p}$. Let $\mathfrak{m}$ be the conductor of this extension. Then we get that*

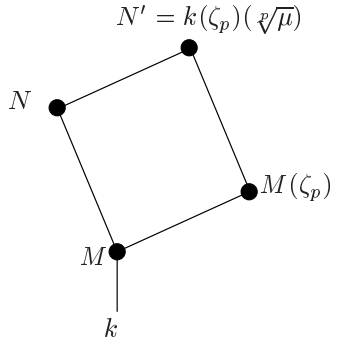
$$v_{\mathfrak{p}}(\mathfrak{m}_0) \leq \frac{e-1+ev_{\mathfrak{p}}(e)}{p-1},$$

where $v_{\mathfrak{p}}$ denotes the ordinary $\mathfrak{p}$ valuation of an ideal.

Proof. The lemma follows immediately by applying Remark 1 in [19, page 58]. □

7. Automorphisms

Having constructed suitable subgroups U, we can use the techniques described in [9] to compute defining equations for N/M. For our applications the explicit knowledge of the automorphism group of N/k is necessary, so we will explain how we can easily compute it, too.
During the class field computation for p-extensions, we construct the following system of fields:



In order to extend σ, a generator of $\mathrm{Gal}(M/k)$, to N, we first extend it to $M(\zeta_p)$. This is straightforward, since $M(\zeta_p)$ is the compositum of M/k and $k(\zeta_p)/k$ and for both fields we explicitly know all automorphisms.
Next, we extend σ to N'. Since N' is a Kummer-extension, the extension of σ must have the form

$$\sigma : \sqrt[p]{\mu} \mapsto \mu_0 \sqrt[p]{\mu}^r$$

where $\gcd(r,p) = 1$. From the action of σ on $\mathrm{Cl}_{\mathfrak{m}}[p]$ (7.3) we obtain linear equations for r. Having computed r we get μ_0 as any solution of $\mu_0^p = \sigma(\mu)\mu^{-r}$.
Finally, to restrict σ to N, we have several possibilities, none of which seems to be superior over the others, starting point for all of them is the knowledge of the primitive element of N/M as an element γ' of N'.
We applied linear algebra: solving the linear system $\sum_{i=0}^{p-1} \lambda_i {\gamma'}^i = \sigma(\gamma')$ we obtain the coefficients of $\sigma(\gamma)$ with respect to the M-basis $1, \gamma, \gamma^2, \ldots, \gamma^{p-1}$ of N.

8. Transitive groups of degree 8

We want to apply our methods to compute minima for some groups occuring in degree 8. There are 50 transitive groups of degree 8, seven of which are primitive. Consequently, we have 43 imprimitive groups of degree 8. All but seven of them have a block of size 2 (which corresponds to a subfield of degree 4). The minimal fields corresponding to these groups are determined in [5]. We compute the fields with minimal discriminants for all imprimitive groups which do not have a block of size 2. This means that the corresponding field extensions have a subfield of degree 2 and the relative Galois group is primitive on four points. Thus two cases arise.
In the first case, the relative Galois group is $\mathfrak{A}_4$ and we get the following absolute Galois groups:

(1) 8T33
(2) 8T34
(3) 8T42 $= \mathfrak{A}_4 \wr 2$.

In the second case, the relative Galois group is $\mathfrak{S}_4$, and the corresponding absolute groups are:

(1) 8T41
(2) 8T45
(3) 8T46
(4) 8T47 $= \mathfrak{S}_4 \wr 2$.

We remark that there are three further groups where the corresponding fields of degree 8 have a subfield of degree 2 such that the field of degree 8 is primitive over this subfield. In these cases there is a subfield of degree 4 and the field can be obtained as a quadratic extension. These groups are 8T13 $= \mathfrak{A}_4 \times C_2$, 8T14, and 8T24 $= \mathfrak{S}_4 \times C_2$. As mentioned above the minima for these groups are computed in [5]. As a byproduct of our computations we have been able to verify their results. Furthermore, our methods could be used to compute minima for some of the primitive groups as well. The group 8T25 $= C_2^3 \rtimes C_7$ is a Frobenius group and the discriminant relation is given in Corollary 6. A similar relation exists for the group 8T36 $= C_2^3 \rtimes (C_7 \rtimes C_3)$.
Now we want to describe how we proved the minima for above mentioned groups in degree 8. We noted above that all of them correspond to fields having a quadratic subfield k. We will demonstrate how, given a quadratic field, one can compute all of the degree 8 fields as extensions of k of (relative) degree 4 with a bound on the absolute discriminant. Since listing quadratic fields is equivalent to listing the corresponding discriminants which is essentially the same as listing square free integers, the necessary fields can be obtained easily.
Afterwards we have to describe a method to find $\mathfrak{A}_4$ or $\mathfrak{S}_4$ extensions of a given quadratic field. $\mathfrak{A}_4$ is a Frobenius group and we can apply the methods described before. Since $\mathfrak{S}_4$ is not a Frobenius group, we need a different approach. Let k be some number field and N/k be a normal extension with Galois group $\mathfrak{S}_4$. There are three subfields $k \subset K, L, M \subset N$ such that $[K : k] = 4$, $[L : k] = 6$ and $[M : k] = 3$, where L is the fixed field under a subgroup $C_2 \times C_2$ of $\mathfrak{S}_4$ which is not normal (see field diagram in Section 10). All of them are unique up to conjugation. The corresponding permutation representation of $\mathfrak{S}_4$ acting on the cosets of this $C_2 \times C_2$ is isomorphic to 6T7. Taking the right conjugate we can assume that $M \subset L$ holds. Using Theorem 1 we get $\mathrm{N}_{k/\mathbb{Q}}(d_{K/k}) = \mathrm{N}_{K/\mathbb{Q}}(d_{M/k}\mathrm{N}_{M/k}(d_{L/M}))$. Therefore we first have to produce $\mathfrak{S}_3$-extensions M/k of degree 3. Since M/k is not normal we first apply the methods described in Section 6 to produce a normal $\mathfrak{S}_3$-extension of k of degree 6. Afterwards we can get M as a subfield of this extension. Now we have to produce relative quadratic extensions L of M with the

right Galois group. Unfortunately the discriminant ideals does not carry enough information. Let $\omega_1, \ldots, \omega_n$ be a basis of a field extensions $L = M(\alpha)$. Then $d(\omega_1, \ldots, \omega_n) := \det(\sigma_i(\omega_j))^2$, where σ_i are the M-linear embeddings of L into $\mathbb{C}$ (cmp. [6, p. 78]). It is well known that the discriminants of (the minimal polynomial of) α and $d(\omega_1, \ldots, \omega_n)$ only differ by a square.

Lemma 11. *Let $L/M/k$ be extensions of number fields, where $L = M(\beta)$ is of degree n and $M = k(\alpha)$ is of degree m. Then $\{\alpha^i\beta^j \mid 0 \le i < m, 0 \le j < n\}$ is a basis of L/k and $d(1, \alpha, \ldots, \alpha^{i-1}\beta^{j-1}) = d(1, \beta, \ldots, \beta^{n-1})^m \mathrm{N}_{M/k}(d(1, \alpha, \ldots, \alpha^{m-1}))$.*

Proof. The first part of the lemma is trivial, it remains to prove the statement involving the discriminants.
Denote the conjugates (over k) of β by $\beta_1, \ldots, \beta_n$ and the conjugates of α by $\alpha_{i,j}$ $(1 \le i \le n, 1 \le j \le m)$, where $\alpha_{i,j}$ are lying above β_i.
We have $d(1, \alpha, \ldots, \alpha^{i-1}\beta^{j-1}) = (\det C)^2$, where C is a blockmatrix of the form

$$C = \begin{pmatrix} A_1 & \ldots & A_n \\ \beta_1 A_1 & \ldots & \beta_n A_n \\ \ldots & & \ldots \\ \beta_1^{n-1} A_1 & \ldots & \beta_n^{n-1} A_n \end{pmatrix}, \text{ where } A_i = \begin{pmatrix} 1 & \ldots & 1 \\ \alpha_{i,1} & \ldots & \alpha_{i,m} \\ \ldots & & \ldots \\ \alpha_{i,1}^{m-1} & \ldots & \alpha_{i,m}^{m-1} \end{pmatrix}.$$

Let B the corresponding matrix to $d(1, \beta, \ldots, \beta^{n-1})$. From the blockmatrix structure we get that $\det(C)^2 = (\det(A_1) \cdots \det(A_n) \det(B)^m)^2 =$
$\mathrm{N}_{M/k}(d(1, \alpha, \ldots, \alpha^{m-1}))d(1, \beta, \ldots, \beta^{n-1})^m$. □

The following Lemma can be found in [1, Lemmata 4,5] for the case $k = \mathbb{Q}$.

Lemma 12. *Let $L/M/k$ such that $[L : M] = 2$, $[M : k] = 3$ and suppose $L = M(\sqrt{\alpha})$.*

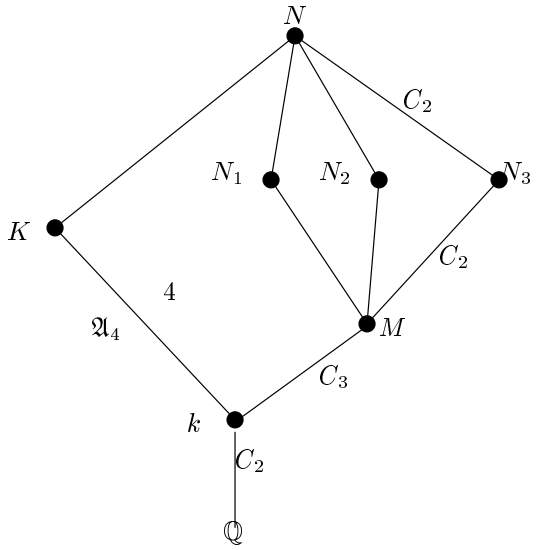
1. *Let $\mathrm{Gal}(M/k) = \mathfrak{S}_3$. Then L/k has Galois group 6T7 if and only if $\mathrm{N}_{M/k}(\alpha)$ is a square.*
2. *Let $\mathrm{Gal}(M/k) = C_3$. Then L/k has Galois group $6T4 = A_4(6)$ if and only if $\mathrm{N}_{M/k}(\alpha)$ is a square.*

Proof. Let 1, β, β^2 be a basis of M/k. The group 6T7 is a subgroup of $\mathfrak{A}_6$ and therefore $d(1, \alpha, \ldots, \alpha\beta^2)$ is a square. Using Lemma 11 we get $d(1, \alpha, \ldots, \alpha\beta^2) = d(1, \beta, \beta^2)^2 \mathrm{N}_{M/k}(d(1, \sqrt{\alpha}))$. It follows $\mathrm{N}_{M/k}(d(1, \sqrt{\alpha})) = 4\mathrm{N}_{M/k}(\alpha)$ is a square. On the other hand if $\mathrm{N}_{M/k}(\alpha)$ is a square we get that $d(1, \alpha, \ldots, \alpha\beta^2)$ is a square and therefore $\mathrm{Gal}(L/k) \le \mathfrak{A}_6 \cap C_2 \wr \mathfrak{S}_3$ using [13]. The group 6T7 is the only transitive subgroup which has all these properties. The proof for the A_4 case is analogous. □

We remark that $\mathrm{N}_{M/k}(\alpha)$ is a square implies that $\mathrm{N}_{M/k}(d_{L/M})$ is a square.

9. $\mathfrak{A}_4$

In order to construct tables of $\mathfrak{A}_4$-extensions K of quadratic fields subject to $|d_{K/\mathbb{Q}}| \le B$, we will work with the following field diagram:
From $d_{K/\mathbb{Q}} = d_k^4 N(d_{K/k})$ we immediately get $|d_k| \le \sqrt[4]{B}$ and $N(d_{K/k}) \le B/d_k^4$. Furthermore, from Corollary 6 we conclude $N(d_{M/k}) \le N(d_{K/k}) \le B/d_k^4$. Since $\mathrm{Gal}(M/k) \cong C_3$, this implies $N(\mathfrak{f}_{M/k}) \le \sqrt{B/d_k^4} = \sqrt{B}/d_k^2$ (because $d_{M/k} = \mathfrak{f}_{M/k}^2$).
In the last step we need to compute V_4-extensions N of M such that N/k is normal, but N_i/k is not normal for $1 \le i \le 3$.
In our actual computations, we started by computing a table of all C_3-extensions M of quadratic fields with absolute discriminant $|d_{M/\mathbb{Q}}| \le B_M$ using:



Algorithm 13. *Computation of C_3-extensions M of real quadratic fields of absolute discriminant $|d_{M/\mathbb{Q}}| \leq B_M$.*

(1) $d_k := 5$
(2) *while* $d_k \leq \sqrt[3]{B_M}$ *do*
(3) *let k be the quadratic field of discriminant d_k*
(4) *let $b = 2$, if 3 is unramified in k, and $b = 4$ otherwise (Lemma 10).*
(5) *compute a list l of ideals $\mathfrak{a} \subseteq \mathbb{Z}_k$ such that $\mathfrak{a}$ apart from the 3 part is square free, the exponents of the 3 parts are bounded by b, and $N(\mathfrak{a}) \leq \sqrt{B_M/d_k^3}$.*
(6) *for each $\mathfrak{a}$ in l do*
(7) *if the conductor of $\mathrm{Cl}_\mathfrak{a}$ is different from $\mathfrak{a}$, try next $\mathfrak{a}$.*
(8) *for all $P_\mathfrak{a} \leq U \leq I^\mathfrak{a}$ with $[I^\mathfrak{a} : U] = 3$ do*
(9) *check if $\mathfrak{f}_U$ equals $\mathfrak{a}$. If not, try next U.*
(10) *compute M as the class field corresponding to U.*
(11) *end do U*
(12) *end do $\mathfrak{a}$*
(13) *find the next quadratic discriminant.*
(14) *end do*

(and a corresponding algorithm for imaginary quadratic base fields).
A total of 7121 C_3-extensions of imaginary quadratic fields with $B_M = 10^{10}$ and 10601 extensions of real quadratic fields with $B_M = 10^{12}$ have been computed.
In the next stage, we compute V_4-extensions of those sextic fields:

Algorithm 14. *Computation of V_4-extensions.*

(1) *For each M in the list computed before do*
(2) *Compute k as a subfield of M*
(3) *Compute a non trivial automorphism σ of M/k*
(4) *Let $b = 2e + 1$, where e denotes the maximal ramification index of a prime ideal in $\mathbb{Z}_M$ lying over 2.*
(5) *Compute a list l of ideals $\mathfrak{a} \subseteq \mathbb{Z}_M$ that are square free (apart from the 2 part, which is bounded by b) and invariant under σ. For each $\mathfrak{a}$ do:*
(6) *Let V be the $\mathbb{F}_2[\sigma]$ module $I^\mathfrak{a}/(I^\mathfrak{a})^2$. Compute all irreducible 2-dimensional quotients U of V*
(7) *if $\mathfrak{f}_U = \mathfrak{a}$, compute N as the corresponding class field.*
(8) *extend σ to N (this still has order 3)*
(9) *compute K as the field fixed by σ*

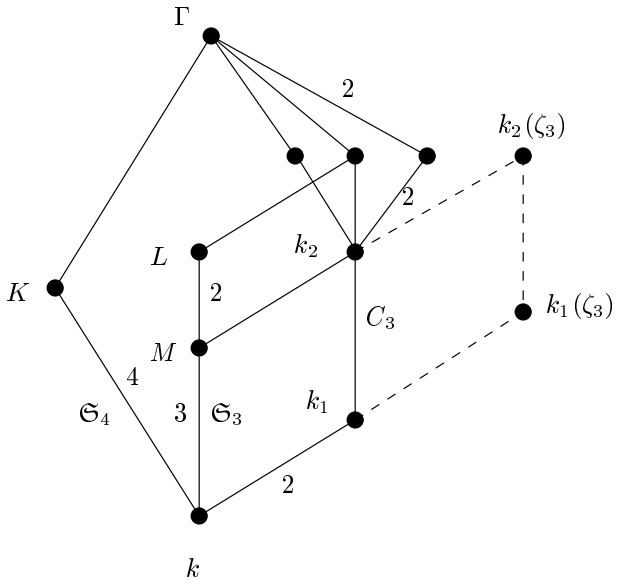
(10) *end do U*
(11) *end do*

A total of 60 fields with group 8T33, 36 fields with 8T34 and 1437 field with 8T42 have been computed. Therefore we proved:

Theorem 15. *The minimal discriminants for imprimitive degree 8 fields with relative Galois group $\mathfrak{A}_4$ are as given in Table 2.*

10. $\mathfrak{S}_4$

The computation of $\mathfrak{S}_4$-extensions follows the following diagram of fields. In our situation k is a quadratic extension of $\mathbb{Q}$.



As one can see, the first step is the compilation of tables of $\mathfrak{S}_3$ extensions of quadratic fields. This task is addressed here: To compute the relative $\mathfrak{S}_3$-extensions we use the dotted part of the diagram. We decided to use a two pass approach: we first computed imprimitive quartic fields $k_1/\mathbb{Q}$ and, in a second pass, extend these fields by C_3-extensions and get the S_3 subfield using Galois theory.
The task of compiling tables of quartic fields was further split up by Galois groups and signatures.

$\mathrm{Gal}(K/\mathbb{Q})$	$\mathrm{Gal}(k_1/\mathbb{Q})$	$r_1 \in$
8T41	V_4	$\{0,4,8\}$
8T45	V_4	$\{0,4,8\}$
8T46	C_4	$\{0,4,8\}$
8T47	D_4	$\{0,2,4,6,8\}$

We have used different bounds for the discriminant for each group and signature. The tables of D_4 and C_4-extensions were computed using class field theory, for the V_4-extensions a more direct approach was used.

Algorithm 16. *Computation of D_4-extensions of $\mathbb{Q}$ up to discriminant $|d_{k_1}| \leq B_{k_1}$.*

(1) $d_k := 5$
(2) *while* $d_k \leq \sqrt[2]{B_{k_1}}$ *do*
  (3) *Let k be the quadratic field of discriminant d_k,* $\mathrm{Gal}(k/\mathbb{Q}) = \langle\sigma\rangle$.
  (4) *Let $b = 2e+1$, where e denotes the ramification index of a prime ideal in $\mathbb{Z}_k$ lying over 2.*

(5) *compute a list l of ideals $\mathfrak{a} \subseteq \mathbb{Z}_k$ such that $\mathfrak{a}$ apart from the 2 part is square free, the exponents of the 2 parts are bounded by b, and $N(\mathfrak{a}) \leq B_{k_1}/d_k^2$.*
(6) *for each $\mathfrak{a}$ in l do*
(7) *if the finite part of the conductor of $\mathrm{Cl}_{\mathfrak{a}\infty_1\infty_2}$ is different from $\mathfrak{a}$, try next $\mathfrak{a}$.*
(8) *for all $P_\mathfrak{a} < U < I^\mathfrak{a}$ with $[I^\mathfrak{a} : U] = 2$ do*
(9) *check if the finite part of $\mathfrak{f}_U$ equals $\mathfrak{a}$. If not, try next U.*
(10) *if $\sigma(U) = U$, try next U.*
(11) *compute k_1 as class field corresponding to U.*
(12) *end do U*
(13) *end do $\mathfrak{a}$*
(14) *find the next quadratic discriminant.*
(15) *end do*

In order to compute C_4-extensions of $\mathbb{Q}$ stronger criteria were used. First of all a C_2-extension embeds into a C_4-extension if and only if it is totally real and all odd ramified primes are congruent 1 mod 4. It is necessary that all primes which are ramified in k must ramify in k_1. This reduces the number of ideals in the list l dramatically. Furthermore, we only enumerate subgroups U invariant under the action of σ.
The V_4-extensions were obtained directly as the product of two quadratics.
We computed 582 totally complex C_4 fields of discriminant $< 10^8$, 13360 totally real fields of discriminant $< 5 \cdot 10^{10}$, 13076 complex V_4 fields ($< 10^8$), 32262 totally real V_4 fields ($< 4 \cdot 10^{10}$), and 426788 D_4 fields of all signatures.
To finally get the $\mathfrak{S}_3$-extensions of k, a similar procedure was used. A total of 64432 $\mathfrak{S}_3$-extension was obtained.
The last step is to compute the $\mathfrak{S}_4$-extensions. Suppose that we have computed a list of $\mathfrak{S}_3$-extensions of k up to a suitable bound (the field M in the diagram). We want to compute relative quadratic extensions as explained in Section 8.

Algorithm 17. *Computation of $\mathfrak{S}_4$-extensions of a quadratic field k up to discriminant $|d_K| \leq B$.*

(1) *Compute all $\mathfrak{S}_3$-extensions M/k such that $|d_M d_k| \leq B$.*
(2) *For all M do*
(3) *Compute b according to Lemma 10.*
(4) *Compute a list l of ideals $\mathfrak{a} \subseteq \mathbb{Z}_M$ of absolute norm smaller or equal to $\frac{B}{d_M d_k}$ that are square free (apart from the 2 part, which is bounded by exponent b) such that the norm is a square (see Lemma 12).*
(5) *for each $\mathfrak{a}$ do*
(6) *Compute all quotients U of size 2 such that $f_H = \mathfrak{a}$.*
(7) *For all of these U compute the class field $L = M(\sqrt{\alpha})$.*
(8) *For all of these L with $\mathrm{N}_{M/k}(\alpha)$ is a square in k use Algorithm 3.5 in* [12] *to compute the field K.*
(9) *end do $\mathfrak{a}$*
(10) *end do M*

Using the above algorithm we proved:

Theorem 18. *The minimal discriminants for imprimitive degree 8 fields with relative Galois group $\mathfrak{S}_4$ are as given in Table 3.*

11. Minimal discriminants for some Frobenius groups

In Corollary 6 we gave discriminant relations for the Frobenius groups $G := C_p \rtimes C_l$, where p is prime and $1 \neq l \mid (p-1)$. The construction of fields with these Galois groups over a given number field k is as follows. First construct a cyclic extension

M/k with Galois group $C_l = \langle\sigma\rangle$. Now we have to find cyclic extensions N/M with Galois group C_p such that $\mathrm{Gal}(N/k) \cong C_p \rtimes C_l$. Using Corollary 8 we have to find σ-invariant subspaces of dimension 1 which are not an eigenspace to the eigenvalue 1 (to avoid the direct product $C_p \times C_l$). We computed the minimal discriminants for these groups for $p = 7, 11, 13$. Since all non trivial elements in Frobenius groups in its natural permutation representation on p points have at most one fix point, the corresponding fields are totally real or have exactly one real embedding. Using similar algorithms as in Sections 9 and 10 we proved:

Theorem 19. *The minimal discriminants for fields of prime degree $7 \leq p \leq 13$ with Galois group $C_p \rtimes C_l$ are as given in Table 1.*

In Corollary 6 we noted a relation for the Frobenius group 8T25 $= C_2^3 \rtimes C_7$. To produce such extensions we have to find extensions M/k with Galois group $C_7 = \langle\sigma\rangle$. Afterwards we have to find extensions N/M such that $\mathrm{Gal}(N/M) = C_2^3$ and $\mathrm{Gal}(N/k) = C_2^3 \rtimes C_7$. Using Corollary 8 we have to find all irreducible σ-invariant eigenspaces of dimension 3. Analogously we proved:

Theorem 20. *The minimal discriminants for fields of degree 8 with Galois group $C_2^3 \rtimes C_7$ are as given in Table 4.*

As noted above we can find a similar discriminant relation for the group 8T36=$C_2^3 \rtimes (C_7 \rtimes C_3)$. This is a primitive group which is no Frobenius group. In order to construct fields with group 8T36 we proceed as follows: Let N/k be a normal extension with Galois group 8T36. Denote by K, M, and L subfields of degree 8,7, and 14, respectively. We suppose that $M \subset L$. Using Theorem 1 we get $\mathrm{N}_{k/\mathbb{Q}}(d_{K/k}) = \mathrm{N}_{K/\mathbb{Q}}(d_{M/k}\mathrm{N}_{M/k}(d_{L/M}))$. Therefore we have to find degree 7 extensions M such that the Galois group of the splitting field is isomorphic to $C_7 \rtimes C_3$. We have described in Section 11 how to construct such fields. For each of theses M's we have to compute quadratic extensions L/M such that the splitting field of L/k has Galois group 8T36. Similar to the $\mathfrak{S}_4$-case we can prove that the norm of the finite part of the conductor of L/M must be a square. The Galois group of L/k is 14T11 which is a subgroup of $\mathfrak{A}_1 4$ and therefore $d_{L/k}$ is a square. From $d_{L/k} = d_{M/k}^2 \mathrm{N}_{M/k}(d_{L/M})$ we get the desired result. For the coprime 2-part we can do better by looking at the possible conjugacy classes of that group. Denote by $\tilde{\mathfrak{f}}$ the part of $\mathfrak{f}$ which is prime to 2. Then $\mathrm{N}_{M/k}(\tilde{f})$ has to be a fourth power. Using these restrictions we produce all quadratic fields (up to the given bound) and check if we get the desired Galois group. After the computation of L/k we can compute K/k using the algorithms described in [12]. We remark that the norm of the 2-part is not necessarily a fourth power. We proved:

Theorem 21. *The minimal discriminants for fields of degree 8 with Galois group $C_2^3 \rtimes (C_7 \rtimes C_3)$ are as given in Table 4.*

12. Tables

The following tables contain the minimal discriminants of fields with prescribed Galois groups and r_1 real zeros. The notation "Hilbert class field or ray class field of a polynomial" means that our field is contained in the corresponding class field of the field generated by a zero of that polynomial. In these cases we have proved the minimum, but were not able to compute a generating polynomial.

Table 1: Minimal discriminants of Frobenius groups $C_p \rtimes C_l$

group	r_1	
$C_7 \rtimes C_2$	7	$192\ 100\ 033 = 577^3$ $x^7 - 2x^6 - 7x^5 + 10x^4 + 13x^3 - 10x^2 - x + 1$
	1	$-357\ 911 = -71^3$ $x^7 - 2x^6 + 2x^5 + x^3 - 3x^2 + x - 1$
$C_7 \rtimes C_3$	7	$1\ 817\ 487\ 424 = 2^6 73^4$ $x^7 - 8x^5 - 2x^4 + 16x^3 + 6x^2 - 6x - 2$
$C_7 \rtimes C_6$	7	$12\ 431\ 698\ 517 = 7^4 173^3$ $x^7 - x^6 - 12x^5 + 9x^4 + 37x^3 - 26x^2 - 21x + 5$
	1	$-38\ 014\ 691 = -11^3 13^4$ $x^7 - 3x^6 + 9x^5 - 13x^4 + 17x^3 - 10x^2 + 4x + 1$
$C_{11} \rtimes C_2$	11	$3\ 670\ 285\ 774\ 226\ 257 = 1297^5$ $x^{11} - 5x^{10} - 4x^9 + 54x^8 - 53x^7$ $-127x^6 + 208x^5 + 69x^4 - 222x^3 + 29x^2 + 56x - 5$
	1	$-129\ 891\ 985\ 607 = -167^5$ $x^{11} - x^{10} + 5x^9 - 4x^8 + 10x^7 - 6x^6 + 11x^5 - 7x^4 + 9x^3 - 4x^2 + 2x + 1$
$C_{11} \rtimes C_5$	11	$1\ 771\ 197\ 285\ 652\ 216\ 321 = 191^8$ Hilbert class field of $x^5 + x^4 - 76x^3 - 359x^2 - 437x - 155$
$C_{11} \rtimes C_{10}$	11	$3\ 483\ 293\ 138\ 903\ 825\ 541 = 3^5 7^5 31^8$ Hilbert class field of $x^{10} - 7x^9 - 29x^8 + 272x^7 - 78x^6$ $-1948x^5 + 1274x^4 + 4243x^3 - 1393x^2 - 2035x + 625$
	1	$-34\ 522\ 712\ 143\ 931 = -11^{13}$ $x^{11} - 11x^9 + 55x^7 + 11x^6 - 143x^5 - 66x^4 + 165x^3 + 121x^2 + 11$
$C_{13} \rtimes C_2$	13	$282\ 638\ 808\ 125\ 771\ 304\ 198\ 601 = 8101^6$ $x^{13} - x^{12} - 50x^{11} - 6x^{10} + 857x^9 + 943x^8 - 5045x^7 - 9319x^6$ $+3890x^5 + 13442x^4 + 1835x^3 - 2759x^2 + 304x + 4$
	1	$48\ 551\ 226\ 272\ 641 = 191^6$ $x^{13} - 6x^{12} + 10x^{11} - 16x^{10} + 22x^9 - 19x^8$ $+11x^7 - 5x^6 - x^5 + 5x^4 - 4x^3 + 2x - 1$
$C_{13} \rtimes C_3$	13	$353\ 629\ 668\ 200\ 918\ 277\ 880\ 881 = 3^{12} 13^{16}$ $x^{13} - 39x^{11} + 468x^9 - 1989x^7 - 507x^6$ $+2886x^5 + 1443x^4 - 624x^3 - 234x^2 + 3$
$C_{13} \rtimes C_4$	13	$4\ 832\ 905\ 768\ 528\ 976\ 580\ 078\ 125 = 5^9 1163^6$ Hilbert class field of $x^4 + 3x^3 - 1456x^2 - 4368x + 416141$
	1	$51\ 185\ 893\ 014\ 090\ 757 = 13^{15}$ $x^{13} + 13x^{10} - 26x^8 + 13x^7 + 52x^6 - 39x^4 + 26x^2 + 13x + 2$
$C_{13} \rtimes C_6$	13	$157\ 840\ 477\ 768\ 256\ 032\ 709\ 001 = 3^{12} 7^8 61^6$ Ray class field of (3) of $x^6 + 3x^5 - 56x^4 - 131x^3 + 637x^2 + 164x - 1079$
	1	$38\ 376\ 770\ 428\ 210\ 201 = 13^8 19^6$ Hilbert class field of $x^6 - x^5 + 6x^4 + x^3 + 85x^2 - 118x + 415$
$C_{13} \rtimes C_{12}$	13	$145\ 952\ 577\ 189\ 773\ 202\ 214\ 912 = 2^{12} 7^6 13^{13}$ Ray class field of (26) of $x^{12} - x^{11} - 25x^{10} + 25x^9 + 235x^8 - 235x^7 - 1013x^6$ $+1013x^5 + 1899x^4 - 1899x^3 - 1013x^2 + 1013x - 181$
	1	$33\ 171\ 021\ 564\ 453\ 125 = 5^9 19^8$ Hilbert class field of $x^{12} + 2x^{11} + 9x^{10} + 29x^9 + 105x^8 - 163x^7$ $+228x^6 - 254x^5 + 469x^4 - 104x^3 + 23x^2 - 5x + 1$

Table 2: Minimal discriminants of imprimitive degree 8 extensions with relative Galois group $\mathfrak{A}_4$

group	r_1	
8T33	8	$94\,540\,875\,625=5^4 7^4 251^2$ $x^8-2x^7-14x^6+32x^5+44x^4-121x^3-19x^2+126x-36$
	4	$2\,522\,550\,625=5^4 7^4 41^2$ $x^8+3x^7-2x^6-13x^5+2x^4+34x^3+4x^2-30x+5$
	0	$1\,262\,025\,625=5^4 7^4 29^2$ $x^8+2x^7+4x^5+12x^4-2x^3-14x^2+5x+11$
8T34	8	$3\,747\,708\,810\,000=2^4 3^8 5^4 239^2$ $x^8-2x^7-29x^6+34x^5+223x^4-62x^3-151x^2-46x-4$
	4	$20\,880\,250\,000=2^4 5^6 17^4$ $x^8+x^7-6x^6-13x^5-6x^4-x^3-14x^2-7x+1$
	0	$1\,614\,110\,976=2^8 3^8 31^2$ $x^8-2x^7-2x^6+8x^5+14x^4-40x^3+40x^2-20x+4$
8T42	8	$22\,982\,560\,000=2^8 5^4 379^2$ $x^8-2x^7-18x^6-2x^5+63x^4+44x^3-22x^2-4x+1$
	4	$618\,765\,625=5^6 199^2$ $x^8-3x^7-5x^6+17x^5+9x^4-27x^3-10x^2+13x+1$
	0	$12\,075\,625=5^4 139^2$ $x^8+4x^5+2x^4+4x^2-x+1$

Table 3: Minimal discriminants of imprimitive degree 8 extensions with relative Galois group $\mathfrak{S}_4$

8T41	8	$47\,461\,236\,736=2^{16} 23^2 37^2$ $x^8-24x^6+44x^5+20x^4-64x^3-4x^2+24x+4$
	4	$258\,405\,625=5^4 643^2$ $x^8-4x^7+2x^6+18x^5-19x^4-10x^3+21x^2-9x+1$
	0	$24\,255\,625=5^4 197^2$ $x^8+3x^7+4x^6+4x^5+6x^4+6x^3+4x^2+2x+1$
8T45	8	$43\,816\,955\,625=3^2 5^4 2791^2$ $x^8+x^7-11x^6-8x^5+40x^4+17x^3-54x^2-6x+19$
	4	$118\,810\,000=2^4 5^4 109^2$ $x^8-3x^7-3x^6+17x^5-12x^4-9x^3+13x^2-6x+1$
	0	$55\,115\,776=2^{16} 29^2$ $x^8-2x^6+x^4+4x^2+4x+1$
8T46	8	$210\,791\,778\,125=5^5 43^2 191^2$ $x^8+x^7-31x^6-20x^5+130x^4-10x^3-170x^2+125x-25$
	4	$402\,753\,125=5^5 359^2$ $x^8-x^7+x^5-4x^4+5x^3+6x^2-2x-1$
	0	$275\,653\,125=3^6 5^5 11^2$ $x^8+2x^7+7x^6+11x^5+19x^4+20x^3+20x^2+10x+5$
8T47	8	$661\,518\,125=5^4 439^1 2411^1$ $x^8+x^7-9x^6-13x^5+11x^4+17x^3-4x^2-4x+1$
	6	$-74\,906\,875=-5^4 119851^1$ $x^8-3x^6+3x^5+3x^4-7x^3-2x^2+3x+1$
	4	$16\,643\,125=5^4 31^1 859^1$ $x^8-x^7-2x^6+2x^5-x^3+x+1$
	2	$-5\,756\,875=-5^4 61^1 151^1$ $x^8-2x^6+3x^5-3x^3+2x^2+x-1$
	0	$1\,342\,413=3^4 16573^1$ $x^8+3x^7+6x^6+7x^5+7x^4+6x^3+4x^2+2x+1$

Table 4: Minimal discriminants of some primitive groups of degree 8

group	r_1	
8T25=	8	$9\ 745\ 585\ 291\ 264=2^{14}29^6$ $x^8-2x^7-20x^6+10x^5+102x^4+26x^3-112x^2-50x+7$
$C_2^3 \rtimes C_7$	0	$594\ 823\ 321=29^6$ $x^8-4x^7+8x^6-6x^5+2x^4+6x^3-3x^2+x+3$
8T36=	8	$6\ 423\ 507\ 767\ 296=2^{12}199^4$ $x^8-40x^6-16x^5+272x^4+144x^3-320x^2-40x+44$
$C_2^3 \rtimes (C_7 \rtimes C_3)$	0	$1\ 817\ 487\ 424=2^6 73^4$ $x^8+3x^7+20x^4+18x^3-18x^2-8x+14$

All of the above computations were done using Kash 2.2 ([8, 17]). For a large part of the tables (all of the degree 4 and 6 fields) we used a network of 30 IBM-PPC running under AIX. The final step was done on some PC running under Linux. We used a total of about 2 weeks on the network plus 1 more week on the PC. The fields can be obtained from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/tables`.

References

[1] A. M. Baily. On the density of discriminants of quartic fields. *J. reine angew. Math.*, 315:190–210, 1980.

[2] R. Brauer. Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. *Math.Nachr.*, 4:158–174, 1950.

[3] Lynne M. Butler. Subgroup lattices and symmetric functions. *Mem. Am. Math. Soc.*, 539, 1994.

[4] J. J. Cannon. MAGMA. http://www.maths.usyd.edu.au:8000/u/magma/, 2000.

[5] H. Cohen, F. Diaz y Diaz, and M. Olivier. Tables of octic fields with a quartic subfield. *Math.Comput.*, 68:1701–1716, 1999.

[6] Henri Cohen. *Advanced Topics in Computational Number Theory*. Springer, 2000.

[7] J.H. Conway, A. Hulpke, and J. McKay. On transitive permutation groups. *London Math. Soc. J. of Comp. and Math.*, 1:1–8, 1998.

[8] Mario Daberkow, Claus Fieker, Jürgen Klüners, Michael Pohst, Katherine Roegner, and Klaus Wildanger. KANT V4. *J. Symb. Comput.*, 24(3):267–283, 1997.

[9] Claus Fieker. Computing class fields via the artin map. *Math. Comput.*, 70(235):1293–1303, 2001.

[10] A. Fröhlich and M.J. Taylor. *Algebraic Number Theory*. Cambridge University Press, 1991.

[11] Derek F. Holt and Sarah Rees. Testing modules for irreducibility. *J. Aust. Math. Soc., Ser. A*, 57(1):1–16, 1994.

[12] Jürgen Klüners and Gunter Malle. Explicit Galois realization of transitive groups of degree up to 15. *J.Symb.Comput.*, 30:675–716, 2000.

[13] M. Krasner and L.A. Kaloujnine. Produit complet des groupes de permutation et problème d'extension de groupes II. *Acta Sci. Math. (Szeged)*, 14:39–66, 1951.

[14] S. Kuroda. Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.*, 1:1–10, 1950.

[15] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer, 2nd edition, 1994.

[16] Richard A. Parker. The computer calculation of modular characters. (the meat-axe). In *Computational group theory, Proc. Symp.*, pages 267–274, Durham/Engl., 1982.

[17] M. Pohst. KASH. http://www.math.tu-berlin.de/algebra/, 2001.

[18] M. Schönert et al. GAP 3.4, patchlevel 4. School of Mathematical and Computational Sciences, University of St.Andrews, Scotland, 1997.

[19] J.-P. Serre. *Local Fields*. Springer, New York, 1995.

School of Mathematics and Statistics F07, University of Sydney NSW 2006, Australia
E-mail address: `claus@maths.usyd.edu.au`

Universität Heidelberg, IWR, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany.
E-mail address: `klueners@iwr.uni-heidelberg.de`