On the Distribution of Galois Groups, II

Gunter Malle

CONTENTS

We propose a very precise conjecture on the asymptotics of the counting function for extensions of number fields with fixed Galois group and bounded norm of the discriminant. This sharpens a previous conjecture of the author. The conjecture is known to hold for abelian groups and a few nonabelian ones. We give a heuristic argument why the conjecture should be true. We also present some computational data for the nonsolvable groups of degree 5.

1. INTRODUCTION

We are interested in the distribution of number fields with a given Galois group. We propose a very precise conjecture on the density of fields having given Galois group and bounded discriminant.

Let G be a finite transitive permutation group on n points and let k be a number field. By abuse of notation, we will write $\mathrm{Gal}(K/k) = G$ if K/k is a field extension such that the Galois group of the Galois closure $\hat{K}/k$, viewed as a permutation group on the set of embeddings of K into $\hat{K}$, is permutation isomorphic to G. Our goal is the description of the asymptotic behaviour of

$$Z(k, G; x) := \left| \left\{ K/k \mid \mathrm{Gal}(K/k) = G,\ \mathcal{N}_{k/\mathbb{Q}}(d_{K/k}) \le x \right\} \right|,$$

the number of field extensions of k (inside a fixed algebraic closure $\bar{\mathbb{Q}}$) of degree n with Galois group isomorphic to G and with norm of the discriminant $d_{K/k}$ bounded above by x.

We propose the following conjecture on the growth of $Z(k, G; x)$ as x goes to infinity, that is, on the density of Galois groups:

Conjecture 1.1. *Let $G \neq 1$ be a transitive permutation group and let k be a number field. Then there exists a constant $c(k, G) > 0$ such that*

$$Z(k, G; x) \sim c(k, G)\, x^{a(G)} (\log x)^{b(k,G)-1},$$

2000 AMS Subject Classification: Primary 11R32, 11R29, 12-04

Keywords: Galois groups, density of extensions, distribution of discriminants

1058-6458/2004$0.50 per page

for certain explicit constants $a(G)$ and $b(k,G)$ (see (2–1) and (2–2)).

Here, for functions $f, g : \mathbb{R} \to \mathbb{R}_{>0}$ we write $f \sim g$ if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

The conjecture that $Z(k,G;x)$ has an asymptotic behaviour of the above form for some constants $a(k,G)$ and $b(k,G)$ has been stated before (see [Cohen et al. 00, Conjecture 1], for example). The point here is that we propose explicit expressions for $a(G)$ and $b(k,G)$: for a finite transitive permutation group $G \neq 1$ we let $a(G)$ be the inverse of the minimal index of nontrivial elements of G. We denote by $b(k,G)$ the number of k-rational conjugacy classes of G with minimal index. (These terms will be defined in the next section.)

Since we claim that $c(k,G) > 0$ for all k and G, the truth of our conjecture would imply in particular that any finite group occurs as a Galois group over any number field. At present, even this latter problem is still wide open.

Also, we will see in Corollary 2.3 that the validity of Conjecture 1.1 implies that the total number of field extensions of degree n and absolute value of the discriminant at most x should grow linearly with x. This last conjecture has been put forward by several authors, see for example Cohen [Cohen 00, Conjecture 9.3.5(1)].

The asymptotic behaviour of $Z(k,G;x)$ has been the object of several investigations and speculations. Notably, Wright proved that the conjecture is true for abelian groups G (see Section 3). Cohen and his collaborators have determined the asymptotics of $Z(k,G;x)$ for some small nonabelian groups. In collaboration with J. Klüners [Klüners and Malle], we investigated the asymptotics of $Z(k,G;x)$ for arbitrary nilpotent groups in regular representation, but the information obtained there is weaker than Conjecture 1.1.

The above conjecture would imply the author's conjecture stated in [Malle 02], where the value of $a(G)$ was already proposed.

Remark 1.2. We note that all available evidence suggests that Conjecture 1.1 should remain true (with the same exponents $a(G)$ and $b(k,G)$) if we restrict ourselves to counting G-extensions with prescribed loval behaviour at a finite number of places of k, *provided that* there exists at least one G-extension with this local behaviour. (There are examples known for which this latter condition is not satisfied.)

2. THE CONSTANTS $a(G)$ AND $b(k,G)$

We now give precise definitions of the two exponents occurring in Conjecture 1.1. The first one is purely group theoretical. For a permutation σ on a finite set Ω, we define its *index* as

$$\mathrm{ind}(\sigma) := |\Omega| - |\Omega/\langle\sigma\rangle|,$$

the order of Ω minus the number of orbits of σ on Ω. Then, for a permutation group $G \neq 1$ we let

$$a(G) := \left(\min\{\mathrm{ind}(\sigma) \mid 1 \neq \sigma \in G\}\right)^{-1}, \qquad (2\text{–}1)$$

and we define $a(1) := 0$ for the trivial group. (More precisely we should have written $a(G \hookrightarrow \mathfrak{S}_n)$, since $a(G)$ also depends on the chosen permutation representation of G.)

The second constant not only depends on G but also on the number field k. Let $\Gamma := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$ and let $c : \Gamma \to \hat{\mathbb{Z}}^\times$ be the cyclotomic character, so that $\delta \in \Gamma$ acts on the primitive roots of unity by

$$\zeta_n^\delta = \zeta_n^{c(\delta)} \qquad \text{for } \zeta_n = \exp(2\pi i/n) \in \bar{\mathbb{Q}}.$$

Then, c factors through the commutator factor group $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$, the Galois group of the maximal abelian extension of $\mathbb{Q}$. Now, let G be a finite group and $\sigma \in G$. We define $\sigma^\delta := \sigma^{c(\delta)}$ for $\delta \in \Gamma$. This defines an action of Γ on the set of elements of G (factoring through $(\mathbb{Z}/|G|\mathbb{Z})^\times$) that commutes with inner automorphisms (conjugation). Thus, we get an induced action of Γ on the set $\mathrm{Cl}(G)$ of conjugacy classes of G. This action agrees with the action of Γ on the (entries of the) columns (indexed by $\mathrm{Cl}(G)$) of the complex character table of G.

Assume, moreover, that $G \leq \mathfrak{S}_n$. Since $c(\delta) \in \hat{\mathbb{Z}}$ is invertible, the elements σ and σ^δ are powers of one another and thus have the same index, $\mathrm{ind}(\sigma) = \mathrm{ind}(\sigma^\delta)$. So, the action of Γ respects indices.

For a number field $k \leq \bar{\mathbb{Q}}$, let $\Gamma_k := \mathrm{Gal}(\bar{\mathbb{Q}}/k)$ be its absolute Galois group. Let $1 \neq G \leq \mathfrak{S}_n$ be a transitive permutation group. Then, we define $b(k,G)$ to be the number of orbits of Γ_k on the set of those conjugacy classes of G with minimal index:

$$b(k,G) := |\{C \in \mathrm{Cl}(G) \mid \mathrm{ind}(C) = a(G)^{-1}\}/\Gamma_k|. \quad (2\text{–}2)$$

Observe that $a(G) \in (0,1]$ and $b(k,G) \in \mathbb{N}$ for all k and all $G \neq 1$.

Example 2.1. Let $G = C_p$, the cyclic group of prime order p in its regular permutation representation. Then, all

nontrivial elements have index $p-1$, which is hence the minimal index. We have $b(\mathbb{Q},G)=1$, since all nontrivial elements lie in the same $\hat{\mathbb{Z}}^\times$-orbit, and $b(\mathbb{Q}(\zeta_p),G)=p-1$, since now each element remains fixed under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_p))$. More generally, for a number field k denote by l, the degree of $k\cap\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, that is, the degree of the maximal subfield of k contained in the field of pth roots of unity. Then, the above definition shows that $b(k,G)=l$, which is just the same as $(p-1)/[k(\zeta_p):k]$ (see Section 3).

We determine possible values of $b(k,G)$ for small $a(G)^{-1}$.

Lemma 2.2. *Let $G\le\mathfrak{S}_n$ be a transitive permutation group with $a(G)=1$. Then $b(k,G)=1$ for all number fields k.*

Proof: First note that $a(G)=1$ implies that G contains transpositions. Moreover, these are the only permutations with index 1. Thus, we are done if we prove that all transpositions in G are conjugate. Let $\sigma,\tau\in G$ be two such transpositions. Since G acts transitively, we may choose a conjugate τ' of τ whose support has (at least) one point in common with the support of σ. If $\tau'\ne\sigma$, then τ' and σ generate a symmetric group of degree 3, but inside that all transpositions are conjugate. Hence, τ and σ are conjugate. □

Denote by

$$Z(k,n;x):=|\{K/k\mid (K:k)=n,\ \mathcal{N}_{k/\mathbb{Q}}(d_{K/k})\le x\}|$$

the total number of field extensions of k of degree n with bounded discriminant. Then we get the following:

Corollary 2.3. *Assume Conjecture 1.1. Then, for any $n>1$ there exists $c(k,n)>0$ with*

$$Z(k,n;x)\sim c(k,n)\,x.$$

Moreover, $c(k,n)=\sum_{a(G)=1}c(k,G)$, the sum running over the transitive subgroups G of $\mathfrak{S}_n$ with $a(G)=1$, up to conjugation.

Proof: Indeed, $Z(k,n;x)$ is the sum of $Z(k,G;x)$ over all classes of transitive subgroups G of $\mathfrak{S}_n$. Now, $a(G)\le 1$ for all G, and $a(G)=1$ implies $b(k,G)=1$ by Lemma 2.2. Since the symmetric group itself has $a(\mathfrak{S}_n)=1$, the statement follows from Conjecture 1.1. □

In particular, we conjecture that no proper subgroup $G<\mathfrak{S}_n$ of $\mathfrak{S}_n$ has a larger density than $\mathfrak{S}_n$ itself. Note, however, that for any composite n there exist proper subgroups $G<\mathfrak{S}_n$ with $a(G)=1$, and by [Malle 02, Proposition 6.1], for any composite n not relatively prime to six, there exist proper subgroups $G<\mathfrak{S}_n$ with $Z(k,G;x)\ge c\,x$ for an unbounded set of values x. The smallest such example is the dihedral group D_4, for which this statement was already shown by Baily, see [Cohen 00, page 449]. This should be compared to the Hilbert irreducibility theorem which states that the *polynomials* of degree n with Galois group different from $\mathfrak{S}_n$ are rare.

Now, let $G\le\mathfrak{S}_n$ be a transitive permutation group with $a(G)=1/2$. If G does not contain double transpositions, then $b(k,G)\le 2$. Indeed, in this case elements of minimal index are 3-cycles. Given two 3-cycles σ_1 and σ_2 in G, we may assume by transitivity that (up to conjugation) their supports have at least one point in common. Let $H:=\langle\sigma_1,\sigma_2\rangle\le G$ and let Ω be the union of the supports of σ_1 and σ_2. If the supports intersect in one point, then $|\Omega|=5$. Thus, H is a transitive subgroup of $\mathfrak{S}_5$ of order divisible by three, hence equal to $\mathfrak{A}_5$, so the two elements are conjugate. If the supports intersect in at least two points, H is equal to $\mathfrak{A}_{|\Omega|}$ on Ω, so σ_2 is conjugate to σ_1 or its inverse in H, so the same holds in G. In any case, G contains at most two classes of 3-cycles.

On the other hand, if G does contain double transpositions, there is no upper bound on $b(k,G)$:

Lemma 2.4. *For any number field k, the set*

$$\{b(k,G)\mid G\le\mathfrak{S}_n \text{ transitive},\ a(G)=1/2,\ n\ge 1\}$$

is unbounded.

Proof: Let $n=2^r\ge 4$, and consider the elementary abelian 2-subgroup N of $\mathfrak{S}_n$ generated by the double transpositions $(2i-1,2i)(2j-1,2j)$ for $1\le i<j\le n/2$. This contains $\binom{2^{r-1}}{2}$ double transpositions. Let H be any group of order 2^{r-1} embedded into $\mathfrak{S}_n$ via its regular permutation representation on the set of 2^{r-1} pairs $(2i-1,2i)$ with $1\le i\le 2^{r-1}$. The semidirect product $G:=\langle N,H\rangle$ is an even transitive 2-group of order $2^{2^{r-1}-1}\cdot 2^{r-1}=2^{2^{r-1}+r-2}$ containing double transpositions, so $a(G)=1/2$. Under the action of H, the double transpositions in N fall into at least 2^{r-2} classes. Thus, $b(k,G)\ge 2^{r-2}$. □

For $n=4$ the construction in the proof of Lemma 2.4 gives the Klein four group, for $n=8$ we get the two transitive groups $8T_{20}$ and $8T_{22}$, with $b(k,G)=2$ and $b(k,G)=3$, respectively; and for $n=16$ the construction

leads to five groups, corresponding to the five groups of order 8, with $4 \le b(k,G) \le 7$. It is clear that similar arguments apply for smaller values of $a(G)$ as well.

If two transitive subgroups G_1 and G_2 of $\mathfrak{S}_n$ have $a(G_1) = a(G_2)$ and $b(\mathbb{Q}, G_1) = b(\mathbb{Q}, G_2)$, then Conjecture 1.1 predicts that the asymptotics of their counting functions should differ by a constant. The smallest degree for which such a pair of nonisomorphic groups exists is four, with the groups $G_1 = D_4$ and $G_2 = \mathfrak{S}_4$. The results of Cohen et al. and Bhargava cited in the next section show that

$$c(\mathbb{Q}, \mathfrak{S}_4)/c(\mathbb{Q}, D_4) = 9.68838\ldots .$$

The next smallest cases are $G_1 = D_5$ and $G_2 = F_{20}$ in degree 5. For neither of these groups the asymptotics are known, but computational results seem to indicate that $c(\mathbb{Q}, D_5)/c(\mathbb{Q}, F_{20}) \sim 1.5$ for totally real extensions with these groups.

In degree 6, there are six groups with $a(G) = 1/2$ and $b(\mathbb{Q}, G) = 1$, four with $a(G) = 1/2$ and $b(\mathbb{Q}, G) = 2$, four with $a(G) = 1$ and $b(\mathbb{Q}, G) = 1$, and two with $a(G) = 1/3$ and $b(\mathbb{Q}, G) = 1$.

3. KNOWN RESULTS

In the case of abelian groups G, the asymptotic behavior of $Z(k, G; x)$ was completely determined by Wright [Wright 89] using class field theory. He showed that, in this case,

$$Z(k, G; x) \sim c(k, G)\, x^{a(G)} (\log x)^{\nu(k,G)-1}$$

for some constant $c(k, G) > 0$, where $\nu(k, G)$ is defined as follows: let p denote the smallest prime dividing the order of G and let n_p denote the number of elements of order p in G. Thus, n_p is of the form $p^r - 1$ for some $r \ge 1$. Then $\nu(k, G) := n_p/(k(\zeta_p) : k)$, where ζ_p denotes a primitive pth root of unity. By Example 2.1 it is clear that we have $\nu(k, G) = b(k, G)$. Thus we have the following theorem:

Theorem 3.1. [Wright 89] *Conjecture 1.1 holds for abelian groups.*

Example 3.2. Let $G = \mathfrak{A}_4$ in its natural permutation representation of degree 4. Then $a(G) = 1/2$ and $b(k, G) = 3$ if $\zeta_3 := \exp(2\pi i/3) \in k$; otherwise, $b(k, G) = 2$. Cohen et al. [Cohen et al. 02a, Section 2.7] conjecture on the basis of extensive data and heuristical arguments that

$$Z(k, \mathfrak{A}_4; x) \sim \begin{cases} c(k, \mathfrak{A}_4)\sqrt{x}\, \log x & \text{if } \zeta_3 \notin k \\ c(k, \mathfrak{A}_4)\sqrt{x}\, \log^2 x & \text{if } \zeta_3 \in k \end{cases}$$

for constants $c(k, \mathfrak{A}_4) > 0$, in agreement with Conjecture 1.1.

By a result of Davenport and Heilbronn (see [Cohen 00, page 449]), Conjecture 1.1 holds for the symmetric group $\mathfrak{S}_3$, and by Cohen et al. [Cohen et al. 02b, Section 2.6] it also holds for the dihedral group D_4 of order 8 in its degree 4 permutation representation.

Bhargava [Bhargava 01, Theorem 5.1] has shown that the number of totally real quartic $\mathfrak{S}_4$-fields over $\mathbb{Q}$ grows asymptotically like cx, with an explicit constant $c > 0$.

4. A HEURISTIC ARGUMENT

Let $K/\mathbb{Q}$ be a number field of degree n. This induces a transitive permutation representation $G \le \mathfrak{S}_n$ of the Galois group G of its Galois closure on the embeddings of K into $\bar{\mathbb{Q}}$. Let p be a prime dividing the discriminant $d_{K/\mathbb{Q}}$ but not dividing $|G|$. Thus, p is tamely ramified in $K/\mathbb{Q}$. If p^k is the precise power of p dividing $d_{K/\mathbb{Q}}$, then the inertia group at p is generated by a permutation $g \in G$ with $\mathrm{ind}(g) = k$ (see, for example, [Koch 00]). Hence, we have in particular $a(G) \ge 1/k$. Moreover, $k = a(G)^{-1}$ does occur if the relevant inertia group is generated by a nontrivial element of G with minimal possible index. Thus, if $a(G) = 1/k$, then the possible discriminants of G-extensions of $\mathbb{Q}$ are of the form

$$\pm \prod_{i=1}^{r} p_i^{a_i} \qquad \text{with } p_i \in \mathbb{P},\ a_i \ge k, \text{ and } r \ge 1.$$

In [Malle 02] we proposed a heuristic explanation for the exponent $a(G)$ in our conjecture based on the assumption that all integers of this type are 'equally likely' to occur as discriminants of a G-extension of $\mathbb{Q}$. Here, we present a refinement which also takes into account the number of conjugacy classes with minimal index and then also explains the exponent $b(\mathbb{Q}, G)$.

The density of the integers of the above form is clearly dominated by the density of those with $a_i = k$, $1 \le i \le r$. Now, assume that $d = d_{K/\mathbb{Q}}$ is an integer of this form. Then, for each of the r ramified primes, the inertia group generator could lie in one of the $b := b(\mathbb{Q}, G)$ classes with minimal index. If all these cases arise (just once), then we get b^r extensions with discriminant d. Then, the asymptotic behaviour of $Z(\mathbb{Q}, G; x)$ would be approximated by

$$\sum_{n=1}^{x^{a(G)}} b^{\omega(n)},$$

where $\omega(n)$ denotes the number of different prime divisors of n. The asymptotic behaviour of the latter function is well-known:

Lemma 4.1. *We have*

$$\sum_{n=1}^{x^{a(G)}} b^{\omega(n)} \sim c\, x^{a(G)} (\log x)^{b-1}$$

for some constant $c = c(G,b) > 0$.

Proof: Let's consider the Dirichlet series

$$f(s) := \sum_{n \geq 1} \frac{b^{\omega(n)}}{n^s}.$$

For s with large enough real part $\Re(s)$ this can be written as an Euler product over all primes p as follows:

$$\begin{aligned} f(s) &= \prod_p (1 + bp^{-s} + bp^{-2s} + \ldots) \\ &= \prod_p \left(1 + (b-1)p^{-s}\right)\left(1 + p^{-s} + p^{-2s} + \ldots\right) \\ &= \prod_p \left(1 + (b-1)p^{-s}\right)\left(1 - p^{-s}\right)^{-1}. \end{aligned}$$

Now

$$(1 + (b-1)p^{-s})(1-p^{-s})^{b-1} = 1 - \binom{b}{2} p^{-2s} + \ldots - (b-1)(-p)^{-bs}.$$

Hence, $f(s)$ equals

$$\prod_p \left(1 - p^{-s}\right)^{-b} \left(1 - \binom{b}{2} p^{-2s} + \ldots - (b-1)(-p)^{-bs}\right) = \zeta(s)^b\, g(s)$$

for all s with $\Re(s) > 1$, where ζ is the Riemann ζ-function and $g(s)$ is a function holomorphic in $\Re(s) \geq 1$ with $g(1) \neq 0$. For example, if $b = 2$ then $f(s) = \zeta(s)^2/\zeta(2s)$. Thus, $f(s)$ is holomorphic in $\Re(s) \geq 1$, except for a pole of order b at $s = 1$, so by a Tauberian theorem we deduce that

$$\sum_{n=1}^{x^{a(G)}} b^{\omega(n)} \sim c'\, x^{a(G)} (\log x^{a(G)})^{b-1} = c\, x^{a(G)} (\log x)^{b-1}$$

with constants $c, c' > 0$, as claimed. □

5. EXPERIMENTAL DATA

In this section, we present the results of computational enumerations of totally real $\mathfrak{A}_5$- and $\mathfrak{S}_5$-extensions of $\mathbb{Q}$ of bounded discriminant.

5.1 The Alternating Group $\mathfrak{A}_5$

We have written a program in the number theory package KANT [Daberkow et al. 97] to enumerate totally real extensions of $\mathbb{Q}$ of degree 5 with Galois group $\mathfrak{A}_5$. By the theorem of Hunter [Cohen 00, Theorem 9.3.1], any such extension $K/\mathbb{Q}$ with discriminant $d_{K/\mathbb{Q}} \leq D$ can be generated by a root of a (totally real) polynomial of the form

$$f(X) = X^5 + a_4 X^4 - a_3 X^3 + a_2 X^2 + a_1 X + a_0,$$

where $a_4 \in \{0,1,2\}$ and

$$0 \leq a_3 \leq \sqrt[4]{\frac{D}{20}} - \frac{2a_4^2}{5}.$$

We have used the following procedure to enumerate all such polynomials. First, note that all of the derivatives of f, $f^{(i)}$ for $i = 1, 2, \ldots$, also have to be totally real. To obtain bounds for the coefficient a_2, we use the fact that the second derivative f'' of f is totally real. Thus, its discriminant, which is a quadratic polynomial in a_2, has to be positive. This yields bounds for a_2, when a_3 and a_4 have been chosen:

$$\left|25a_2 + a_4(15a_3 + 4a_4^2)\right| \leq \sqrt{2(5a_3 + 2a_4^2)^3}.$$

To bound a_1 note that f' has to be totally real; thus, its constant coefficient a_1 has to be such that f' has four real zeros. This happens precisely for values of a_1 in a (possibly empty) interval with bounds described by the values of $f' - a_1$ at zeros of f'' (the maxima and minima of f').

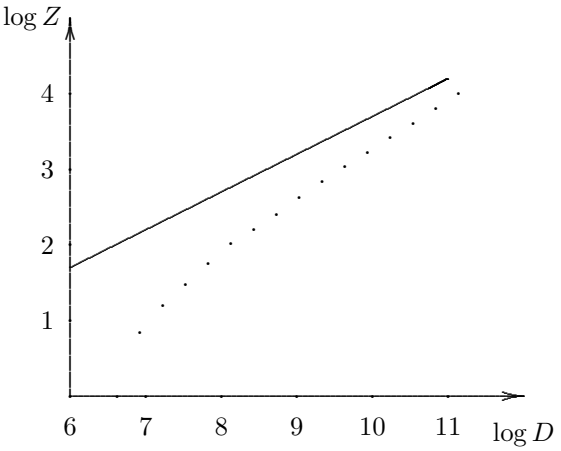
Now the discriminant of f is a polynomial $d(X) \in \mathbb{Q}[a_1, \ldots, a_4]$ of degree 4 where the coefficients are formal expressions in $a_1, \ldots, a_4$. These coefficients can be computed explicitly at this stage already. We now make use of the desired Galois group of the polynomial: for $a \in \{0, \ldots, m\}$ we compute a table T indicating whether the value $d(a)$ is a square modulo m, for $m \in \{11, 63, 64, 65\}$. (This is inspired by the square detection algorithm described in Cohen [Cohen 93, 1.7.2].) If there is no such a, then the present value of a_1 can be discarded. Otherwise, the values a_0 such that f is totally real lie in a finite (possibly empty) interval I. By guessing (using information from a previous value for a_1), or by

computing a suitable zero of $d(X)'$ (that is, the position of the maximum of $d(X)$), we find one integer b in this interval I (if it is nonempty). Then, all possible a_0 can be reached successively by increasing (and decreasing) b. For each value we first check whether the discriminant can be a square by table-lookup in table T for $a_0 \bmod m$, $m \in \{11, 63, 64, 65\}$. (This dramatically reduces the number of evaluations of $d(X)$ and of integer-square-tests, and thus reduces the running time.) If a_0 passes these tests, we check whether $d(a_0)$ is indeed the square of an integer and whether f is irreducible; in the latter case we output the polynomial f.

The polynomials obtained this way are then filtered according to their Galois group (which at this point can be one of $\mathfrak{A}_5$, D_5, or C_5). Then, the $\mathfrak{A}_5$-fields are tested for isomorphism. (To speed up this step, it is sensible to first find a reduced generating polynomial for each $\mathfrak{A}_5$-field, using the `polredabs` command in Pari, for example, and to discard doubles.) Note that fields with the solvable groups D_5 and C_5 can be enumerated much more efficiently using methods from class field theory, see for example [Cohen 00, Section 9] or [Cohen et al. 00].

We give the results of these computations in the form of a diagram in doubly logarithmic scale, showing numbers of field extensions with group $\mathfrak{A}_5$. We also print a line with slope $a(\mathfrak{A}_5) = 1/2$. Since $b(\mathbb{Q}, \mathfrak{A}_5) = 2$, our conjecture predicts that the number of extensions should grow proportionally to $\sqrt{x} \log x$.

Table 1 gives the distribution of all totally real $\mathfrak{A}_5$-fields of discriminant $d_K \le 2^{37} = 1.37..10^{11}$.



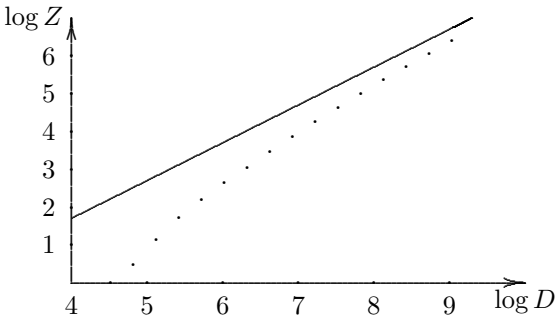
D	$Z(\mathbb{Q}, \mathfrak{A}_5; D)$
2^{22}	1
2^{23}	7
2^{24}	16
2^{25}	30
2^{26}	57
2^{27}	104
2^{28}	159
2^{29}	251
2^{30}	421
2^{31}	681
2^{32}	1095
2^{33}	1685
2^{34}	2612
2^{35}	4094
2^{36}	6371
2^{37}	9933

TABLE 1. First 9,933 totally real $\mathfrak{A}_5$-extensions.

5.2 The Symmetric Group $\mathfrak{S}_5$

For the symmetric group $\mathfrak{S}_5$, a KANT-program was used to compute all totally real degree 5 extensions of $\mathbb{Q}$ with symmetric Galois group up to discriminant 10^9. The results are displayed in Table 2. Here, Conjecture 1.1 predicts a linear growth of $Z(\mathbb{Q}, \mathfrak{S}_5; x)$ with x.

In [Malle 02, Section 7], we gave a heuristical explanation of the exponent $a(G)$ in the conjecture. For that, we postulated that the set of integers, which occur as discriminants of field extensions with a given group G with $a(G) = 1$, has positive density among all integers. In particular, one might expect that the multiplicative



D	$Z(\mathbb{Q}, \mathfrak{S}_5; D)$
2^{22}	3 035
2^{23}	7 488
2^{24}	18 211
2^{25}	43 112
2^{26}	100 077
2^{27}	229 657
2^{28}	518 546
2^{29}	1 153 555
2^{30}	2 537 415

TABLE 2. First 2,537,415 totally real $\mathfrak{S}_5$-extensions.

structure of discriminants (in a range) resembles that of all integers (in a range).

We used the data of the first 10^6 totally real $\mathfrak{S}_5$-extensions to test this assumption. More precisely, we checked the divisibility of the discriminants by the first 100 primes. A proportion of $1/p$ of all integers (in a range) is divisible by a prime p. It turns out that, in our range for all relatively small primes except 2, the actual proportion is less than the expected one, slightly increasing with p. But, the deviation is at most by 17% (for the prime $p = 17$) and quite a bit smaller for most other primes.

5.3 Regular Groups in Degree 8

There are two nonabelian regular permutation groups of degree 8: the dihedral group and the quaternion group of order 8. Both of them have $a(G) = 1/4$, and elements with minimal index are precisely the involutions. But, while the quaternion group Q_8 has just one involution, the central one, the dihedral group D_4 has three conjugacy classes of involutions. Thus, $b(k, Q_8) = 1$ and $b(k, D_4) = 3$ for any number field k. Computations in KANT by J. Klüners indicate that indeed the number of Q_8-extensions grows linearly with $x^{1/4}$, while the number of D_4-extensions of degree 8 grows proportionally to $x^{1/4}(\log x)^2$, as would be expected by Conjecture 1.1.

ACKNOWLEDGMENTS

I would like to thank Jürgen Klüners for computing large tables of number fields of degree 8 with groups Q_8 and D_4.

REFERENCES

[Bhargava 01] M. Bhargava. "Higher Composition Laws." PhD. diss., Princeton University, 2001.

[Cohen 93] H. Cohen. *A Course in Computational Algebraic Number Theory*. Berlin-Heidelberg-New York: Springer, 1993.

[Cohen 00] H. Cohen. *Advanced Topics in Computational Number Theory*. Berlin-Heidelberg-New York: Springer, 2000.

[Cohen et al. 00] H. Cohen, F. Diaz y Diaz, and M. Olivier. *Counting Discriminants of Number Fields*. MSRI preprint 2000-026, 2000.

[Cohen et al. 02a] H. Cohen, F. Diaz y Diaz, and M. Olivier. "A Survey of Discriminant Counting." In *Algorithmic Number Theory*, LNCS 2369, edited by C. Fieker, D. R. Kohel, pp. 80–94. Berlin-Heidelberg-New York: Springer, 2002.

[Cohen et al. 02b] H. Cohen, F. Diaz y Diaz, and M. Olivier. "Enumerating Quartic Dihedral Extensions." *Compositio Math* 133 (2002), 65–93.

[Daberkow et al. 97] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. "KANT V4." *J. Symb. Comput* 24 (1997), 267–283.

[Klüners and Malle] J. Klüners and G. Malle. "Counting Nilpotent Galois Extensions." To appear in *Journal reine angew. Math.*

[Koch 00] H. Koch. *Number Theory—Algebraic Numbers and Functions*, Providence, RI: American Mathematical Society, 2000.

[Malle 02] G. Malle. "On the Distribution of Galois Groups." *J. Number Theory* 92 (2002), 315–329.

[Wright 89] D. Wright. "Distribution of Discriminants of Abelian Extensions." *Proc. London Math. Soc* 58 (1989), 17–50.

Gunter Malle, FB Mathematik/Informatik, Universität Kassel, Heinrich-Plett-Str. 40, D–34132 Kassel, Germany.
(malle@mathematik.uni-kassel.de)

Received November 3, 2002; accepted October 16, 2003.