Counting Discriminants of Number Fields

Henri Cohen, Francisco Diaz y Diaz and Michel Olivier
Laboratoire A2X, U.M.R. 5465 du C.N.R.S.,
Université Bordeaux I,
351 Cours de la Libération,
33405 TALENCE Cedex, FRANCE

September 18, 2000

Abstract

This paper is intended as a summary of the conjectures and results obtained recently on the asymptotic and exact counting of relative and absolute extensions of number fields. No proofs are given.

Version of September 18, 2000

1 General Conjectures and Results

Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$. Let $K \subset \overline{\mathbb{Q}}$ be a number field, and let G be a transitive permutation group on n letters. We consider the set $\mathcal{F}_n(G)$ of all extensions L/K of degree n with $L \subset \overline{\mathbb{Q}}$ such that the Galois group of the Galois closure of L/K is isomorphic to G. We write

$$N_{K,n}(G,X) = |\{L \in \mathcal{F}_n(G),\ |\mathcal{N}(\mathfrak{d}(L/K))| \leq X\}\ ,$$

where $\mathfrak{d}(L/K)$ denotes the relative ideal discriminant, $\mathcal{N}$ the absolute norm (so that of course $|\mathcal{N}(\mathfrak{d}(L/K))| = |d(L)|$, the absolute value of the discriminant of L). The aim of this paper is to give results and conjectures on exact and asymptotic values of these quantities, without proof. It is very easy to generalize the results to the case where the behavior of a *finite* number of places of K in the extension L/K are specified, but we will not do this. It is also usually possible to give additional main terms and rather good error terms instead of asymptotic formulas, but we will not do this either.

A number of general conjectures on the subject has been made by several authors. In view of available data and theorems, it now seems reasonable to formulate the following precise conjectures (see for example [10] and [16]).

Conjecture 1.1 (1) *For each number field K and transitive group G on n letters as above, there exist three strictly positive constants $a_K(G)$, $b_K(G)$ and $c_K(G)$ such that*

$$N_{K,n}(G,X) \sim c_K(G)\, X^{a_K(G)} (\log X)^{b_K(G)}\ .$$

(2) *Furthermore, the constant* $a_K(G)$ *should not depend on* K *(so will be denoted by* $a(G)$*) and should be a rational number satisfying* $0 < a(G) \leq 1$*, and* $b_K(G)$ *should be a nonnegative integer, equal to* 0 *if* $a(G) = 1$*.*

(3) *If* G *is a primitive transitive group, we should have* $a(G) < 1$ *except when* $G \simeq S_n$*, in which case we should have* $a(S_n) = 1$*.*

(4) *On the contrary, if* n *is composite (so that there exist imprimitive groups* G*), there exists at least one imprimitive transitive group* G *such that* $a(G) = 1$*.*

(5) *The total number of extensions* L/K *in* $\overline{\mathbb{Q}}$ *of degree* n *and absolute discriminant bounded by* X *should be asymptotic to* $c_K X$ *for some positive constant* c_K*.*

An even more precise version of this conjecture concerning the value of $a(G)$ has been made by G. Malle [16] as follows.

Definition 1.2 *For any element* $g \in S_n$ *different from the identity, define the index* $\operatorname{ind}(g)$ *of* g *by the formula*

$$\operatorname{ind}(g) = n - |\textit{orbits of } g| \ .$$

We define the index $i(G)$ *of a transitive subgroup* G *of* S_n *by the formula*

$$i(G) = \min_{g \in G,\ g \neq 1} \operatorname{ind}(g) \ .$$

Examples:

(1) The index of a transposition is equal to 1, and this is the lowest possible index for a nonidentity element. It follows that $i(S_n) = 1$.

(2) If G is an Abelian group, and if ℓ is the smallest prime divisor of $|G|$, then it is easy to show that $i(G) = |G|(1 - 1/\ell)$.

Conjecture 1.3 *(Malle). For any transitive subgroup* G *of* S_n*, we should have* $a(G) = 1/i(G)$*.*

It can be shown that the statements (2), (3), and (4) about $a(G)$ in Conjecture 1.1 follow from Malle's conjecture.

The following results give support to the conjecture (see [19], [4], [5]).

Theorem 1.4 (1) *(Wright). Malle's conjecture is true for all Abelian groups* G*.*

(2) *(CDO). Malle's conjecture is true for* $n \leq 4$ *(we will give more precise results below) and for* $G = D_\ell$*, for* ℓ *prime.*

In addition, Malle gives partial results towards the statement that his conjecture is compatible with direct products and with wreath products.

Malle does not give a conjecture for the value of the exponent of the logarithm $b_K(G)$ (in fact he does not even conjecture such a precise form). However, in the Abelian case, the same paper of Wright proves the following theorem:

Theorem 1.5 *(Wright). Let G be an Abelian group, and let ℓ be the smallest prime divisor of $|G|$ (so that $a(G) = (|G|(1-1/\ell))^{-1}$). Denote by $B_\ell(G)$ the number of elements of G of order ℓ, which will be of the form $\ell^k - 1$ for some positive k. Then we have*

$$b_K(G) = \frac{B_\ell(G)}{[K(\zeta_\ell) : K]} - 1 \, .$$

The paper of Wright also claims an explicit expression for the constant $c_K(G)$, but although it is a finite product of adelic integrals, as far as the authors are aware, it has not been computed explicitly by this method apart from the case where G is of order 2. We have computed it by other means in more general situations.

Finally, concerning statement (4) of the general conjecture, Malle proves the following theorem:

Theorem 1.6 *If n is a composite number divisible by either 2 or 3, there exists an imprimitive transitive subgroup G of S_n such that $a(G) = 1$.*

He of course conjectures that this remains true for any composite n, not only those divisible by 2 and 3. In particular, if the main conjecture is true, this shows that, for composite n, the proportion of S_n-extensions among all extensions of degree n is strictly less than 1. Thanks to our results, this is now a theorem for $n = 4$.

This is in complete opposition with the situation for *polynomials*, where Hilbert's irreducibility theorem shows that "almost all" polynomials of degree n have Galois group S_n.

2 Results in Small Degrees

2.1 $G = C_2$

$$N_{K,2}(C_2, X) \sim c_K(C_2)\, X \quad \text{with}$$

$$c_K(C_2) = \frac{1}{2^{r_2}} \frac{\zeta_K(1)}{\zeta_K(2)} \, .$$

Here $r_2 = r_2(K)$ is the number of complex places of K, and $\zeta_K(1)$ is a useful abuse of notation for the residue of $\zeta_K(s)$ at $s = 1$.

This very simple result deserves to be better known, but its proof is not simple (a few pages). It is due (using Shintani's theory of zeta functions of prehomogeneous vector spaces, see [17], [18], [20]) to Datskowsky and Wright

[13], and was recently reproved by the authors using Kummer theory. Of course, in particular

$$c_{\mathbb{Q}}(C_2)=\frac{1}{\zeta(2)}=\frac{6}{\pi^2}\;.$$

Using some nontrivial series manipulation [11], one can for example compute exactly (3 weeks CPU time)

$$N_{\mathbb{Q},2}(C_2,10^{25})=6079271018540266286517795\,.$$

2.2 $G = C_3$

$$N_{K,3}(C_3,X)\sim\begin{cases}c_K(C_3)\,X^{1/2} & \text{if } \zeta_3\notin K\\ c_K(C_3)\,X^{1/2}\log X & \text{if } \zeta_3\in K\;.\end{cases}$$

Here, when $\zeta_3\notin K$, setting $K_z=K(\zeta_3)=K(\sqrt{-3})$, we have

$$c_K(C_3)=\frac{1}{2\cdot 3^{r_1+r_2-1}}\frac{\zeta_{K_z}(1)}{\zeta_K(2)}\prod_{\left(\frac{K_z}{\mathfrak{p}}\right)=1}\left(1-\frac{2}{\mathcal{N}\mathfrak{p}(\mathcal{N}\mathfrak{p}+1)}\right)$$
$$\prod_{\left(\frac{K_z}{\mathfrak{p}}\right)=0}\left(1+\frac{1}{\mathcal{N}\mathfrak{p}+1}-\frac{1}{\mathcal{N}\mathfrak{p}^{(e(\mathfrak{p})+1)/2}}\right)\prod_{\substack{\left(\frac{K_z}{\mathfrak{p}}\right)=-1\\ \mathfrak{p}\mid 3}}\left(1+\frac{2}{\mathcal{N}\mathfrak{p}}-\frac{2}{\mathcal{N}\mathfrak{p}^{e(\mathfrak{p})/2}}\right)\;.$$

In the above, $\left(\frac{K_z}{\mathfrak{p}}\right)=-1,0$ or 1 means that $\mathfrak{p}$ is inert, ramified or split in the quadratic extension K_z/K, and $e(\mathfrak{p})=e(\mathfrak{p}/3)$ is the absolute ramification index of a prime ideal dividing 3. Note that, of course, in the second product the condition $\left(\frac{K_z}{\mathfrak{p}}\right)=0$ implies that $\mathfrak{p}\mid 3$ (it is in fact equivalent to $e(\mathfrak{p})$ being odd).

On the other hand, if $\zeta_3\in K$ we have the much simpler formula

$$c_K(C_3)=\frac{1}{4\cdot 3^{r_2}}\zeta_K(1)^2\prod_{\mathfrak{p}}\left(1+\frac{2}{\mathcal{N}\mathfrak{p}}\right)\left(1-\frac{1}{\mathcal{N}\mathfrak{p}}\right)^2\;.$$

In particular,

$$c_{\mathbb{Q}}(C_3)=\frac{11\sqrt{3}}{36\pi}\prod_{p\equiv 1\pmod 6}\left(1-\frac{2}{p(p+1)}\right)\;.$$

The general result is apparently new, but the result for $K=\mathbb{Q}$ is due to H. Cohn [12].

Using some nontrivial series manipulation [11], one can for example compute exactly

$$N_{\mathbb{Q},3}(C_3,10^{37})=501310370031289126\,.$$

2.3 $G = S_3$

$$N_{K,3}(S_3,X) \sim c_K(S_3)\,X \quad \text{with}$$

$$c_K(S_3) = \left(\frac{2}{3}\right)^{r_1-1}\left(\frac{1}{6}\right)^{r_2}\frac{\zeta_K(1)}{\zeta_K(3)} = \frac{2^{r_1-r_2-1}}{3^{r_1+r_2-1}}\frac{\zeta_K(1)}{\zeta_K(3)}\ .$$

In particular

$$c_{\mathbb{Q}}(S_3) = \frac{1}{\zeta(3)}\ .$$

This last result is the beautiful and difficult result of Davenport–Heilbronn [14], [15], but the general result is much deeper and is due to Datskowsky and Wright [13]. Our methods enable us to find the correct power of X and $\log X$ (1 and 0 respectively), but give a dreadful expression for the constant $c_K(S_3)$.

Using the algorithmic methods of K. Belabas [2], based on the Heilbronn–Davenport theory, one can for example compute exactly

$$N_{\mathbb{Q},3}(S_3, 10^{11}) = 81414013239\,.$$

2.4 $G = C_4$

$$N_{K,4}(C_4,X) \sim c_K(C_4)\,X^{1/2}\ .$$

We have not had time to compute the constant $c_K(C_4)$ in the general case. For $K = \mathbb{Q}$, we have

$$c_{\mathbb{Q}}(C_4) = \frac{3}{\pi^2}\left(\left(1+\frac{\sqrt{2}}{24}\right)\prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^{1/2}(p+1)}\right)-1\right)\ .$$

This result is due in principle to A. Baily [1], but there are computational mistakes in his paper.

Using some nontrivial series manipulation [11], one can for example compute exactly

$$N_{\mathbb{Q},4}(C_4, 10^{30}) = 122051516492357\,.$$

2.5 $G = V_4 = C_2 \times C_2$

$$N_{K,4}(V_4,X) \sim c_K(V_4)\,X^{1/2}\log^2 X \quad \text{with}$$

$$c_K(V_4) = \frac{1}{3\cdot 4^{r_2+2}}\zeta_K(1)^3\prod_{\mathfrak{p}\nmid 2}\left(1+\frac{3}{\mathcal{N}\mathfrak{p}}\right)\left(1-\frac{1}{\mathcal{N}\mathfrak{p}}\right)^3$$
$$\prod_{\mathfrak{p}\mid 2}\left(1+\frac{4}{\mathcal{N}\mathfrak{p}}+\frac{1}{\mathcal{N}\mathfrak{p}^2}-\frac{1}{\mathcal{N}\mathfrak{p}^{e(\mathfrak{p})+1}}-\frac{1}{\mathcal{N}\mathfrak{p}^{e(\mathfrak{p})+2}}\right)\left(1-\frac{1}{\mathcal{N}\mathfrak{p}}\right)^3\ ,$$

where here $e(\mathfrak{p}) = e(\mathfrak{p}/2)$ is the absolute ramification index of a prime ideal $\mathfrak{p}$ over 2. In particular,

$$c_{\mathbb{Q}}(V_4) = \frac{23}{960} \prod_p \left(1 + \frac{3}{p}\right)\left(1 - \frac{1}{p}\right)^3 .$$

This last result is due in principle to A. Baily [1], but once again there are computational mistakes in his paper.

Using some nontrivial series manipulation [11], one can for example compute exactly

$$N_{\mathbb{Q},4}(V_4, 10^{35}) = 6894524058812256194 .$$

2.6 $G = D_4$

$$N_{K,4}(D_4, X) \sim c_K(D_4)\, X \quad \text{with}$$

$$c_K(D_4) = \sum_{[k:K]=2} \frac{1}{2^{r_2(k)}\, \mathcal{N}(\mathfrak{d}(k/K))^2} \frac{\zeta_k(1)}{\zeta_k(2)} .$$

In particular,

$$c_{\mathbb{Q}}(D_4) = \frac{6}{\pi^2} \sum_D \frac{2^{-r_2(D)}}{D^2} \frac{L_D(1)}{L_D(2)} ,$$

where the sum runs over all (positive or negative) discriminants of quadratic fields, $r_2(D) = r_2(\mathbb{Q}(\sqrt{D}))$, and $L_D(s)$ is the Dirichlet L-series attached to the character $\left(\frac{D}{n}\right)$. Note that we do not know how to compute this sum in any other way than the naive method, hence we know only about 7 or 8 decimals.

Using genus theory in a suitable way, combined with series manipulation, one can for example compute exactly

$$N_{\mathbb{Q},4}(D_4, 10^{17}) = 10465196820067560 .$$

All the above results are due to the authors (see [6]). Since D_4 quartic extensions of $\mathbb{Q}$ form a positive proportion of all quartic number fields, it is remarkable that one is able to compute $N_{\mathbb{Q},4}(D_4, X)$ for $X = 10^{17}$: the published tables only go up to 10^6. It should be emphasized at this point that all our methods for counting exactly are algorithmic, and that if the number of fields is reasonable, we can just as easily construct *tables* of extensions, see for example [4].

2.7 $G = A_4$

$$N_{K,4}(A_4, X) \sim \begin{cases} c_K(A_4)\, X^{1/2} \log X & \text{if } \zeta_3 \notin K \\ c_K(A_4)\, X^{1/2} \log^2 X & \text{if } \zeta_3 \in K . \end{cases}$$

Here $c_K(A_4)$ is a complicated explicit constant. To give an example of the complexity, we have in particular

$$c_{\mathbb{Q}}(A_4) = \lim_{N \to \infty} \frac{1}{3 \log 2\zeta(3)} \sum_{\substack{K_3 \\ N < f(K_3) \le 2N}} \frac{h(K_3) R(K_3) c_2(K_3) c_r(K_3)}{f(K_3)^2} P(K_3)$$

with

$$P(K_3) = \prod_{p \text{ split in } K_3} \frac{(1+3/p)(1-1/p)^2}{1+1/p+1/p^2} ,$$

where K_3 ranges over all cyclic cubic extensions of $\mathbb{Q}$ up to isomorphism (which can easily be described explicitly), $f(K_3)$, $h(K_3)$, $R(K_3)$ denote the conductor, class number and regulator of K_3,

$$c_r(K_3) = \prod_{p \mid f(K_3)} \frac{1}{1+1/p+1/p^2}$$

and $c_2(K_3) = 11/2$ if 2 is inert in K_3, while $c_2(K_3) = 23/5$ if 2 is totally split in K_3.

Using this method, we can also compute exactly (in 3 weeks of CPU time)

$$N_{\mathbb{Q},4}(A_4, 10^{13}) = 5278424 .$$

The reason that it takes so long to compute is the computation of the class number and regulator for all the necessary cyclic cubic fields K_3.

These results are due to the authors [5].

2.8 $G = S_4$

$$N_{K,4}(S_4, X) \sim c_K(S_4)\, X ,$$

where $c_K(S_4)$ is an even more complicated explicit constant similar to the one above (except that the sum will be over all noncyclic cubic extensions of K instead of cyclic cubic extensions, and there will be no limit). We do not even give the expression for $c_{\mathbb{Q}}(S_4)$, although it is quite similar to $c_{\mathbb{Q}}(A_4)$.

Using an extension of Shintani's method requiring a huge amount of work and computations, it seems that A. Yukie will soon be able to prove the same result for S_4-extensions, but with a much nicer expression for the constant $c_K(S_4)$ (exactly as Datskowsky and Wright's result gave a nice expression for $c_K(S_3)$), see [21]. The expression that he finds (which is not quite proved yet) is

$$c_{K,4}(S_4) = 2\left(\frac{37}{96}\right)^{r_1}\left(\frac{1}{24}\right)^{r_2}\prod_{\mathfrak{p}}\left(1+\frac{1}{\mathcal{N}\mathfrak{p}^2}-\frac{1}{\mathcal{N}\mathfrak{p}^3}-\frac{1}{\mathcal{N}\mathfrak{p}^4}\right) ,$$

so that in particular

$$c_{\mathbb{Q}}(S_4) = \frac{37}{48}\prod_{p}\left(1+\frac{1}{p^2}-\frac{1}{p^3}-\frac{1}{p^4}\right) .$$

Using our method, we can compute exactly

$$N_{\mathbb{Q},4}(S_4, 10^7) = 6541232 .$$

3 More General Results

Our methods enable us to attack essentially all solvable groups. For example, Wright's result gives for a prime number ℓ

$$N_{K,\ell}(C_\ell, X) \sim c_K(C_\ell)\, X^{1/(\ell-1)}\, (\log X)^{(\ell-1)/[K_z:K]-1}$$

for some constant $c_K(C_\ell)$, but we have computed this constant in a completely explicit manner, see [7], [8].

We have also shown that (for ℓ an odd prime)

$$N_{K,\ell}(D_\ell, X) \sim c_K(D_\ell)\, X^{2/(\ell-1)}\ ,$$

where the exponent is in agreement with Malle's conjecture.

References

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

[2] K. Belabas, A fast algorithm to compute cubic fields, Math. Comp. **66** (1997), 1213–1237.

[3] H. Cohen, F. Diaz y Diaz and M. Olivier, Density of number field discriminants, in preparation.

[4] H. Cohen, F. Diaz y Diaz and M. Olivier, Construction of tables of quartic fields using Kummer theory, Proceedings ANTS IV, Leiden (2000), Lecture Notes in Computer Science **1838**, Springer-Verlag, 257–268.

[5] H. Cohen, F. Diaz y Diaz and M. Olivier, On the density of discriminants of quartic number fields, in preparation.

[6] H. Cohen, F. Diaz y Diaz and M. Olivier, Enumeratic quartic dihedral extensions, submitted.

[7] H. Cohen, F. Diaz y Diaz and M. Olivier, Densité des discriminants des extensions cycliques de degré premier, C. R. Acad. Sci. Paris **330** (2000), 61–66.

[8] H. Cohen, F. Diaz y Diaz and M. Olivier, On the density of discriminants of cyclic extensions of prime degree, preprint.

[9] H. Cohen, A course in computational algebraic number theory (third printing), GTM **138**, Springer-Verlag, 1996.

[10] H. Cohen, Advanced topics in computational number theory, GTM **193**, Springer-Verlag, 2000.

[11] H. Cohen, Comptage exact de discriminants d'extensions abéliennes, submitted.

[12] H. Cohn, The density of abelian cubic fields, Proc. Amer. Math. Soc. **5** (1954), 476–477.

[13] B. Datskovsky and D. J. Wright, Density of discriminants of cubic extensions, J. Reine Angew. Math. **386** (1988), 116–138.

[14] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields I, Bull. London Math. Soc. **1** (1969), 345–348.

[15] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, Proc. Royal. Soc. A **322** (1971), 405–420.

[16] G. Malle, On the distribution of Galois groups, preprint.

[17] T. Shintani, On Dirichlet series whose coefficients are class numbers of integral binary cubic forms, J. Math. Soc. Japan **24** (1972), 132–188.

[18] T. Shintani, On zeta-functions associated with the vector space of quadratic forms, J. Fac. Sci. Univ. Tokyo, Sec. 1a **22** (1975), 25–66.

[19] D. J. Wright, Distribution of discriminants of Abelian extensions, Proc. London Math. Soc. (3) **58** (1989), 17–50.

[20] D. J. Wright and A. Yukie, Prehomogeneous vector spaces and field extensions, Invent. Math. **110** (1992), 283–314.

[21] A. Yukie, Density theorems related to prehomogenous vector spaces, preprint.