PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 5, May 2008, Pages 1581–1587
S 0002-9939(07)09171-X
Article electronically published on October 12, 2007

THE DENSITY OF DISCRIMINANTS OF S_3-SEXTIC NUMBER FIELDS

MANJUL BHARGAVA AND MELANIE MATCHETT WOOD

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. We prove an asymptotic formula for the number of sextic number fields with Galois group S_3 and absolute discriminant $< X$. In addition, we give an interpretation of the constant in the formula in terms of the asymptotic densities of given local completions among these sextic fields. Our proof gives analogous results when we count S_3-sextic extensions of any number field, and also when finitely many local completions have been specified for the sextic extensions.

1. INTRODUCTION

Given a number field K, let $d(K) := |\operatorname{disc}_{K/\mathbb{Q}}|$, and let $\widetilde{K}$ be the Galois closure of K. Let $G \subset S_n$ be a permutation group and let $\mathcal{F}(G)$ denote the set of isomorphism classes of number fields K such that the $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$-action on the embeddings of K into $\bar{\mathbb{Q}}$ is isomorphic to G. The aim is to understand the asymptotics of

$$N(X, G) := \#\{K \in \mathcal{F}(G) \mid d(K) < X\}$$

as $X \to \infty$.

These asymptotics are known for abelian groups in their regular representation (Mäki, [13]; see also Wright, [15]), S_3 in its natural permutation representation (Davenport–Heilbronn, [9]), D_4 as a subgroup of S_4 (Cohen–Diaz y Diaz–Olivier, [7]), S_4 in its natural permutation representation (Bhargava, [4]), and S_5 in its natural permutation representation (Bhargava, [5]). Klüners and Malle have found the order of growth of $N(X, G)$ up to a factor of X^ϵ for nilpotent groups in their regular representation [12]. Malle [14] gives a heuristic for the order of growth of $N(X, G)$ for any group G, which is verified in all of the above examples, but to which Klüners [11] has found a counterexample in the case $G = C_3 \wr C_2$. We use $f(X) \sim g(X)$ to denote that $\lim_{X\to\infty} \frac{f(X)}{g(X)} = 1$.

As an example, we have the following in the case when G is S_3 in its natural permutation representation. (We denote this permutation group simply by S_3.)

Theorem 1 (Davenport–Heilbronn, [9]). *We have* $N(X, S_3) \sim \dfrac{1}{3\zeta(3)} X$.

In this paper we examine the case when G is the group S_3 in its regular representation, which we denote by $S_3(6)$. Fields in $\mathcal{F}(S_3(6))$ are called S_3-*sextic fields*, and they are Galois over $\mathbb{Q}$. We are able to obtain an exact asymptotic in this case:

Received by the editors December 19, 2006 and, in revised form, March 24, 2007.
2000 *Mathematics Subject Classification.* Primary 11R21, 11R45.

Theorem 2. *We have*

$$N(X, S_3(6)) \sim \left(\frac{1}{3}\prod_p c_p\right) X^{1/3},$$

where the product is over primes, $c_p = (1 + p^{-1} + p^{-4/3})(1 - p^{-1})$ *for* $p \neq 3$*, and* $c_3 = (\frac{4}{3} + \frac{1}{3^{5/3}} + \frac{2}{3^{7/3}})(1 - \frac{1}{3})$.

To compare with Theorem 1, we may write

$$\frac{1}{\zeta(3)} = \prod_p (1 + p^{-1} + p^{-2})(1 - p^{-1}).$$

To prove Theorem 2, we relate counting S_3-sextic fields to counting non-Galois cubic fields with certain local completions, where we can apply the result of Davenport and Heilbronn. We need to apply a uniformity result of Belabas, Bhargava, and Pomerance [1, Lemma 3.3], which was used in the proof of the best known error term for $N(X, S_3)$. We remark that Theorem 2 has also recently been obtained (independently) by Belabas and Fouvry [2] as a result of a much deeper study of S_3-sextic fields. We give a simple proof and further give an interpretation of the constants in Theorems 1 and 2 and how they are related. In Section 6, we discuss how our method gives generalizations of Theorem 2, e.g., for S_3-sextic extensions of any base number field, or when counting such extensions by invariants other than the discriminant.

2. Preliminaries

Any S_3-sextic field K_6 contains a unique (up to conjugation) non-Galois cubic subfield K_3. Conversely, any non-Galois cubic field K_3 has a unique Galois closure K_6, which is an S_3-sextic field. Let K_3 and K_6 be such for the rest of the paper. Let $v_p(n)$ denote the exponent of the largest power of p that divides n. If K_3 is nowhere totally or wildly ramified, then $d(K_6) = d(K_3)^3$. If this were always the case, then the asymptotics of $N(X, S_3(6))$ would follow immediately from Theorem 1. However, at a tame rational prime p, the possible ramification types in K_3 are $\mathfrak{p}_1^2\mathfrak{p}$ *and* $\mathfrak{p}^3$, and $v_p(d(K_3))$ is 1 and 2 in these cases, respectively. These give, respectively, splitting types $\wp_1^2\wp_2^2\wp_3^2$ and $\wp_1^3\wp_2^3$ in K_6, and hence $v_p(d(K_6))$ is 3 and 4 in these cases, respectively. We call primes p of the second type *overramified* in K_3 (or K_6).

If tamely overramified primes exist, then evidently $d(K_3)^3 \neq d(K_6)$. To prove Theorem 2, we define transitional discriminants $d_Y(K_6)$ for K_6 that "correct" $d(K_3)^3$ to $d(K_6)$ at the primes less than Y:

Definition. Let $d_Y(K_6)$ be the positive integer such that

$$v_p(d_Y(K_6)) = \begin{cases} v_p(d(K_6)) & \text{if } p \text{ is a prime} < Y, \\ v_p(d(K_3)^3) & \text{if } p \text{ is a prime} \geq Y. \end{cases}$$

3. Asymptotics of $N_Y(X)$

Davenport and Heilbronn [9] prove Theorem 1 by using a correspondence between cubic rings and binary cubic forms. In fact, a stronger version of Theorem 1 follows from their work. For an integer m, let ϕ_m be the map that takes binary cubic forms with integer coefficients to binary cubic forms with coefficients in $\mathbb{Z}/m\mathbb{Z}$, via reduction of the coefficients modulo m. For each of *finitely many* rational primes p_i, let us specify a set Σ_i of étale cubic $\mathbb{Q}_{p_i}$-algebras and let Σ_i' be the corresponding set of maximal $\mathbb{Z}_{p_i}$-orders. For some $m = \prod_i p_i^{n_i}$, there are sets U and S of binary cubic forms with coefficients in $\mathbb{Z}/m\mathbb{Z}$ such that $\phi_m^{-1}(U)$ is the set of forms which correspond to rings that are maximal at all p_i and $\phi_m^{-1}(S)$ is the set of forms which correspond to rings that are maximal at all p_i and whose p_i-adic completions are in Σ_i'. We define the *relative density* of $\{\Sigma_i\}_i$ to be $\#S/\#U$. By the Chinese Remainder Theorem, this relative density is simply the product of the *relative p_i-adic densities* of the individual Σ_i, defined as above in the case that $\{p_i\}_i$ has one element. The strengthened version of Theorem 1 we require is that

$$\begin{aligned}(1)\qquad &\#\{K \in \mathcal{F}(S_3) \mid d(K) < X \text{ and } K \otimes \mathbb{Q}_{p_i} \in \Sigma_i \text{ for all } i\} \\ &\qquad\qquad \sim \text{(relative density of } \{\Sigma_i\}_i) \cdot \frac{X}{3\zeta(3)}.\end{aligned}$$

(For further details on this strengthened Theorem 1, see [9, Section 5].) Since $d_Y(K_6)$ only differs from $d(K_3)^3$ at finitely many primes, we can compute the asymptotics of $N_Y(X) := \#\{K_6 \mid d_Y(K_6) < X\}$ directly from such a strengthened version of Theorem 1.

We define $q_Y(K_6)$ to be the product of all primes less than Y that are tamely overramified in K_6. Given $K_3 \otimes \mathbb{Q}_p$, the $\mathbb{Q}_p$-algebra $K_6 \otimes \mathbb{Q}_p$ is determined up to isomorphism—it is the "S_3-closure" of $K_3 \otimes \mathbb{Q}_p$ (see [3, Section 2.1]). For a $\mathbb{Q}_p$-algebra A, let $D(A)$ denote the discriminant of A as a power of p; and for a cubic $\mathbb{Q}_p$-algebra A, let $\bar{A}$ denote the S_3-closure of A. Then for $Y > 3$, we observe that

$$(2)\qquad d_Y(K_6) = \frac{D(\overline{K_3 \otimes \mathbb{Q}_2})D(\overline{K_3 \otimes \mathbb{Q}_3})}{D(K_3 \otimes \mathbb{Q}_2)^3 D(K_3 \otimes \mathbb{Q}_3)^3} \frac{d(K_3)^3}{q_Y(K_6)^2}.$$

Therefore,

$$\begin{aligned}N_Y(X) = \sum_q \sum_{A,B} \#\{K_6 \mid q_Y(K_6) = q, K_3 \otimes \mathbb{Q}_2 = A, K_3 \otimes \mathbb{Q}_3 = B,& \\ d(K_3) < \frac{D(A)D(B)}{D(\bar{A})^{1/3}D(\bar{B})^{1/3}} q_Y(K_6)^{2/3} X^{1/3}\},&\end{aligned}$$

where the first sum is over all square-free $q < Y$, and the second sum is over all étale cubic $\mathbb{Q}_2$- and $\mathbb{Q}_3$- algebras A and B respectively. Equation (1) gives the asymptotics of each of the finitely many summands:

$$\begin{aligned}\lim_{X\to\infty} \frac{N_Y(X)}{X^{1/3}} = &\sum_{q,A,B} \mu_2(A)\mu_3(B) \prod_{p \mid q} \frac{p^{-2}}{1+p^{-1}+p^{-2}} \\ &\times \prod_{3<p<Y, p\nmid q} \frac{1+p^{-1}}{1+p^{-1}+p^{-2}} \frac{D(A)D(B)}{D(\bar{A})^{1/3}D(\bar{B})^{1/3}} \prod_{p\mid q} p^{2/3} \frac{1}{3\zeta(3)}\end{aligned}$$

where $\mu_2(A)$ and $\mu_3(B)$ denote the relative 2-adic and 3-adic densities of A and B respectively, and the products are over primes p with the factors in the first and second products giving the relative p-adic densities of étale cubic $\mathbb{Q}_p$-algebras that are overramified at p and not overramified at p, respectively. These relative p-adic densities can be computed by the same method as in Lemmas 1 and 2 (using Lemma 11 and Proposition 4) in [9].

Collecting terms into one Euler product, we obtain

$$\lim_{X\to\infty}\frac{N_Y(X)}{X^{1/3}}=\sum_{A,B}\mu_2(A)\mu_3(B)\frac{D(A)D(B)}{D(\bar{A})^{1/3}D(\bar{B})^{1/3}}\prod_{3<p<Y}\frac{1+p^{-1}+p^{-4/3}}{1+p^{-1}+p^{-2}}\frac{1}{3\zeta(3)}.$$

Using a database of local fields [10], we compute that

$$c_{2,3}:=\sum_{A,B}\mu_2(A)\mu_3(B)\frac{D(A)D(B)}{D(\bar{A})^{1/3}D(\bar{B})^{1/3}}=\frac{c_2c_3}{(1-2^{-3})(1-3^{-3})}$$

where c_2 and c_3 are as given in the Introduction.

Taking the limit in Y, we obtain

$$\lim_{Y\to\infty}\lim_{X\to\infty}\frac{N_Y(X)}{X^{1/3}}=\frac{c_{2,3}}{3\zeta(3)}\prod_{p>3}\frac{1+p^{-1}+p^{-4/3}}{1+p^{-1}+p^{-2}}. \tag{3}$$

4. The asymptotics of $N(S_3(6),X)$ (Proof of Theorem 2)

We now compute the asymptotics of $N(X):=N(S_3(6),X)$. The key is to show that we can switch the order of the limits in equation (3). Note that for $Y>3$, we have $N_Y(X)\le N(X)$ and thus

$$\lim_{Y\to\infty}\lim_{X\to\infty}\frac{N_Y(X)}{X^{1/3}}\le\liminf_{X\to\infty}\frac{N(X)}{X^{1/3}}. \tag{4}$$

To obtain an upper bound, let $M(n,X)=\#\{K_3$ overramified at all primes $p|n$, $d(K_3)<X\}$. From [1, Lemma 3.3], we know $M(n,X)=O(n^{-2+\epsilon}X)$. If K_6 is an S_3-sextic field with $d(K_6)<X$, and n is the product of the primes where K_6 is overramified, then equation (2) yields $d(K_3)<cn^{2/3}X^{1/3}$ for some finite absolute constant c given by the behavior of the finitely many 2-adic and 3-adic cubic algebras (in fact, we may take $c=36$). Thus,

$$N(X)\le N_Y(X)+\sum_{n\ge Y}M(n,cn^{2/3}X^{1/3})\le N_Y(X)+d\sum_{n\ge Y}\frac{X^{1/3}}{n^{4/3-\epsilon}}$$

for some constant d. Taking limits in X, we obtain

$$\limsup_{X\to\infty}\frac{N(X)}{X^{1/3}}\le\lim_{X\to\infty}\frac{N_Y(X)}{X^{1/3}}+d\sum_{n\ge Y}\frac{1}{n^{4/3-\epsilon}},$$

and then taking limits in Y, we conclude

$$\limsup_{X\to\infty}\frac{N(X)}{X^{1/3}}\le\lim_{Y\to\infty}\lim_{X\to\infty}\frac{N_Y(X)}{X^{1/3}}. \tag{5}$$

Equations (4) and (5) combine to prove

$$\lim_{X\to\infty}\frac{N(X)}{X^{1/3}}=\lim_{Y\to\infty}\lim_{X\to\infty}\frac{N_Y(X)}{X^{1/3}},$$

which together with equation (3) proves Theorem 2.

5. Interpretation of the constants

In the result of Davenport and Heilbronn (Theorem 1)

$$N(S_3, X) \sim \frac{1}{3}\prod_p (1+p^{-1}+p^{-2})(1-p^{-1})X, \tag{6}$$

each $(1+p^{-1}+p^{-2})$ factor is equal to

$$\sum_{[L:\mathbb{Q}_p]=3} \frac{1}{|\operatorname{Aut}(L)|D(L)},$$

where the sum is over all étale cubic $\mathbb{Q}_p$-algebras L ([6]). This reflects the fact that, among non-Galois cubic fields K_3, an isomorphism class of étale cubic algebras L arises as $K_3 \otimes \mathbb{Q}_p$ (asymptotically) with density proportional to $\frac{1}{|\operatorname{Aut}(L)|D(L)}$. (By *density proportional to* $\frac{1}{|\operatorname{Aut}(L)|D(L)}$, we mean that the ratio of the asymptotic density of fields with completion L_1 to the asymptotic density of fields with completion L_2 is $\frac{|\operatorname{Aut}(L_2)|D(L_2)}{|\operatorname{Aut}(L_1)|D(L_1)}$.) Therefore, the constant in equation (6) may be interpreted as a product of local factors which are sums of the proportional densities of the possible local étale algebras.

To obtain the constant of Theorem 2, we replace the terms $1+p^{-1}+p^{-2} = \sum_{[L:\mathbb{Q}_p]=3} \frac{1}{|\operatorname{Aut}(L)|D(L)}$ with

$$\sum_{[L:\mathbb{Q}_p]=3} \frac{1}{|\operatorname{Aut}(L)|D(\bar{L})^{1/3}} = \begin{cases} 1+p^{-1}+p^{-4/3} & \text{if } p \neq 3, \\ \frac{4}{3} + \frac{1}{3^{5/3}} + \frac{2}{3^{7/3}} & \text{if } p = 3. \end{cases} \tag{7}$$

The new sum (7) corresponds to changing the discriminant exponents from those occurring in $d(K_3)$ to those in $d(K_6)^{1/3}$. The term $\frac{1}{|\operatorname{Aut}(L)|D(\bar{L})^{1/3}}$ is exactly proportional to the density of S_3-sextic fields with p-adic completion $\bar{L}$, analogous to the S_3-cubic field case. (This can be proven by fixing a p-adic completion in Sections 3 and 4.) Hence the factors in the constant of Theorem 2 may be interpreted as sums of densities of local behaviors. As in [6], heuristically the product indicates that the probabilities of various local completions are independent at any finite set of primes. For S_3-sextic fields, this can be proven by fixing specific local completions at a finite number of places throughout the proof of Theorem 2. Note that Theorem 2 gives an affirmative answer to the question posed in [6, Section 8.2] in the case $G = S_3(6)$, which asks whether a heuristic based on assuming that these local probabilities are independent gives the correct asymptotics of $N(G, X)$.

6. Further results

The analogue of Theorem 2 over an arbitrary base number field can also be obtained by these methods, by replacing the work of Davenport and Heilbronn with that of Datskovsky and Wright [8]; the necessary uniformity estimate of [1] is also easily adapted to this context (see [8, Proposition 6.2]). We thus obtain:

Theorem 3. *For a permutation group G and a number field K, let $\mathcal{F}_K(G)$ denote the set of isomorphism classes of field extensions L of K (with M the Galois closure of L over K) such that the* $\operatorname{Gal}(M/K)$*-action on the embeddings of L into $\bar{K}$ is* *isomorphic to G. Let $N_K(X,G) = \#\{L \in \mathcal{F}_K(G) \mid \mathrm{N}_{K/\mathbb{Q}}(\mathrm{disc}_{L/K}) < X\}$. Then*

$$N_K(X, S_3(6)) \sim \frac{1}{2}\left(\frac{2}{3}\right)^{r_1}\left(\frac{1}{6}\right)^{r_2}\mathrm{Res}_{s=1}\,\zeta_K(s)\left(\prod_{\wp} c_{\wp}\right)\cdot X^{1/3},$$

where the product is over prime ideals of K, for $\wp \nmid 6$ we have $c_\wp = (1+\mathrm{N}_{K/\mathbb{Q}}\wp^{-1} + \mathrm{N}_{K/\mathbb{Q}}\wp^{-4/3})(1-\mathrm{N}_{K/\mathbb{Q}}\wp^{-1})$, and for $\wp \mid 6$ we have that $c_\wp$ is a constant depending on the étale cubic $K_\wp$-algebras.

We have the same interpretation of the constants in Theorem 3 as in Theorem 2.

Theorem 2 (or 3) has an obvious corollary for counting non-Galois cubic fields by the cube root of the discriminant of the Galois closure. In this setting, we can view the counting invariant as staying the same at (all but finitely many) primes that are not overramified, and changing from exponent 2 to exponent α at (all but finitely many) overramified primes, where in our case $\alpha = 4/3$. There is a lot of room for generalization in the proof of Theorem 2; e.g., we can replace $4/3$ with any $\alpha > 1$ and modify the proof accordingly to obtain an exact asymptotic (if $\alpha > 2$, then the upper bound is trivial and the $M(n,X)$ terms become part of the lower bound). If we change $4/3$ to an $0 < \alpha \le 1$ (for example, $\alpha = 1$ will count non-Galois cubic fields by the product of the ramified primes), then we obtain an upper bound of $O(X^{1/\alpha+\epsilon})$ and an asymptotic lower bound of cX for any constant c.

The same methods can be applied to counting fields whose Galois closure has Galois group S_4. In [4] the analogue of Theorem 1 was obtained for quartic fields, and an appropriate strengthening to fixed local completions at finitely many places also follows from this work. An easy generalization of the uniformity result [4, Proposition 23] from primes to all n may be used, and it applies to some of the several types of ramifying behaviors possible in quartic fields. If we change our counting invariant only for the ramifying behaviors for which such a uniformity is known, we can obtain some asymptotic results. For example, if G is the group S_4 acting on the cosets of $\langle(12),(34)\rangle$, i.e., we are counting S_4-sextic fields K with $\mathrm{Gal}(\widetilde{K}/K) = V_4$, then we obtain

$$X^{1/2}\log X \ll N(X,G) \ll X^{1/2+\epsilon}. \tag{8}$$

In particular, these asymptotic upper and lower bounds are in agreement with the predictions of Malle's conjecture [14]. It appears that the upper bound could be drawn even closer to the lower bound using a tighter version of the uniformity estimate $M(n,X) = O(n^{-2+\epsilon}X)$, perhaps in combination with an effective version of the Chebotarev density theorem for cubic fields.

References

[1] K. Belabas, M. Bhargava, and C. Pomerance, Error terms for the Davenport-Heilbronn theorems, preprint.

[2] K. Belabas and E. Fouvry, Discriminants Cubiques et Progressions Arithmétiques, preprint.

[3] M. Bhargava, Higher composition laws III: The parametrization of quartic rings, *Ann. of Math.* **160** (2004), 1329–1360. MR2113024 (2005k:11214)

[4] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math.* **162** (2005), 1031–1063. MR2183288 (2006m:11163)

[5] M. Bhargava, The density of discriminants of quintic rings and fields, *Ann. of Math.*, to appear.

[6] M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Internat. Math. Research Notices*, (2007), Vol. 2007, Articke ID rnm052, 20 pp.

[7] H. Cohen, F. Diaz y Diaz, and M. Olivier, Counting discriminants of number fields of degree up to four, in *Algorithmic Number Theory* (Leiden, 2000), *Lecture Notes in Comput. Sci.* **1838**, 269–283, Springer-Verlag, New York, 2000. MR1850611 (2002g:11148)

[8] B. Datskovsky and D. J. Wright, Density of discriminants of cubic extensions, *J. Reine Angew. Math.* **386** (1988), 116–138. MR0936994 (90b:11112)

[9] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420. MR0491593 (58:10816)

[10] J. W. Jones and D. P. Roberts, A database of local fields, *J. Symbolic Comput.* **41** (2006), no. 1, 80–97. `http://math.asu.edu/~jj/localfields/` MR2194887 (2006k:11230)

[11] J. Klüners, A counterexample to Malle's conjecture on the asymptotics of discriminants, *C. R. Math. Acad. Sci. Paris*, Ser. I **340** (2005), 411–414. MR2135320 (2005m:11214)

[12] J. Klüners and G. Malle, Counting nilpotent Galois extensions, *J. reine angew. Math.* **572** (2004), 1–26. MR2076117 (2005f:11259)

[13] S. Mäki, On the density of abelian number fields. *Annales Academiae Scientiarum Fennicae. Series A I. Mathematica Dissertationes* **54** (1985), 104 pp. MR791087 (86h:11079)

[14] G. Malle, On the distribution of Galois groups II, *Experiment. Math.* **13** (2004), 129-135, MR2068887 (2005g:11216)

[15] D. J. Wright, Distribution of discriminants of abelian extensions, *Proc. London Math. Soc.* (3) **58** (1989), 17-50. MR969545 (90b:11115)

Department of Mathematics, Princeton University, Princeton, New Jersey 08544

Department of Mathematics, Princeton University, Princeton, New Jersey 08544