Journal de Théorie des Nombres
de Bordeaux **18** (2006), 607–615

Asymptotics of number fields and the Cohen–Lenstra heuristics

par JÜRGEN KLÜNERS

Dedicated to Michael Pohst on the occasion of his 60th birthday

RÉSUMÉ. Nous étudions les conjectures de Malle pour les groupes diédraux D_ℓ d'ordre 2ℓ, où ℓ est un nombre premier impair. Nous prouvons que les bornes inférieures sont celles attendues. Pour les bornes supérieures, nous montrons qu'il y a un lien avec les groupes de classes des corps quadratiques. Le comportement asymptotique de ces groupes de classes est prédit par les heuristiques de Cohen–Lenstra. Sous ces hypothèses, nous pouvons montrer que les bornes supérieures sont celles attendues.

ABSTRACT. We study the asymptotics conjecture of Malle for dihedral groups D_ℓ of order 2ℓ, where ℓ is an odd prime. We prove the expected lower bound for those groups. For the upper bounds we show that there is a connection to class groups of quadratic number fields. The asymptotic behavior of those class groups is predicted by the Cohen–Lenstra heuristics. Under the assumption of this heuristic we are able to prove the expected upper bounds.

1. Introduction

Let k be a number field and $G \leq S_n$ be a transitive permutation group on n letters. We say that a finite extension K/k has Galois group G if the normal closure $\hat{K}$ of K/k has Galois group isomorphic to G and K is the fixed field in $\hat{K}$ under a point stabilizer. By abuse of notation we write $\mathrm{Gal}(K/k) = G$ in this situation. We let

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

be the number of field extensions of k (inside a fixed algebraic closure $\bar{\mathbb{Q}}$) of relative degree n with Galois group permutation isomorphic to G (as explained above) and norm of the discriminant $d_{K/k}$ bounded above by x. It is well known that the number of extensions of k with bounded norm of the discriminant is finite, hence $Z(k, G; x)$ is finite for all G, k and $x \geq 1$. We are interested in the asymptotic behavior of this function for $x \to \infty$.

Manuscrit reçu le 13 décembre 2005.

Gunter Malle [10, 11] has given a precise conjecture how this asymptotic should look like. Before we can state it we need to introduce some group theoretic definitions.

Definition. Let $1 \neq G \leq S_n$ be a transitive subgroup acting on $\Omega = \{1, \ldots, n\}$ and $g \in G$. Then

(1) The index $\operatorname{ind}(g) := n -$ the number of orbits of g on Ω.
(2) $\operatorname{ind}(G) := \min\{\operatorname{ind}(g) : 1 \neq g \in G\}$.
(3) $a(G) := \operatorname{ind}(G)^{-1}$.
(4) Let C be a conjugacy class of G and $g \in C$. Then $\operatorname{ind}(C) := \operatorname{ind}(g)$.

The last definition is independent of the choice of g since all elements in a conjugacy class have the same cycle shape. We define an action of the absolute Galois group of k on the $\bar{\mathbb{Q}}$-characters of G. The orbits under this action are called k–conjugacy classes. We remark that we get the ordinary conjugacy classes when k contains all m-th roots of unity for $m = |G|$.

Definition. For a number field k and a transitive subgroup $1 \neq G \leq S_n$ we define:

$$b(k, G) := \#\{C : C \text{ } k\text{-conjugacy class of minimal index } \operatorname{ind}(G)\}.$$

Now we can state the conjecture of Malle [11], where we write $f(x) \sim g(x)$ for $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Conjecture 1.1. *(Malle) For all number fields k and all transitive permutation groups $1 \neq G$ there exists a constant $c(k, G) > 0$ such that*

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

where $a(G)$ and $b(k, G)$ are given as above.

We remark that at the time when the conjecture was stated it was only known to hold for all Abelian groups and the groups S_3 and $D_4 \leq S_4$.

Example. Let ℓ be an odd prime and $D_\ell \leq S_\ell$ be the dihedral group of order 2ℓ. In this case the non-trivial elements of D_ℓ are of order 2 or ℓ. In the latter case the index is $\ell - 1$. Elements of order 2 have 1 fixed point and therefore the index is $(\ell-1)/2$. All elements of order 2 are conjugated. Therefore we get:

$$a(D_\ell) = \frac{2}{\ell - 1} \text{ and } b(k, D_\ell) = 1 \text{ for all } k.$$

With the same arguments we get for $D_\ell(2\ell) \leq S_{2\ell}$:

$$a(D_\ell(2\ell)) = \frac{1}{\ell} \text{ and } b(k, D_\ell(2\ell)) = 1 \text{ for all } k.$$

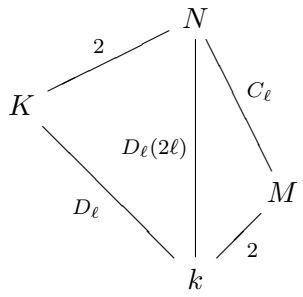
In [7] we have given counter examples to the conjecture. In these counter examples the log-factor is bigger than expected when certain subfields of cyclotomic extensions occur as intermediate fields. Nevertheless the main philosophy of this conjecture should still be true.

The goal of this paper is to prove the conjectured lower bounds for dihedral groups D_ℓ, where ℓ is an odd prime. We are able to prove the conjectured upper bounds when we assume a weak version of the Cohen–Lenstra heuristics [3]. Furthermore we show that the Cohen–Lenstra heuristics is wrong when the conjectured upper bound for dihedral groups is broken.

2. Dihedral groups of order 2ℓ

In this section we collect some results about dihedral groups of order 2ℓ, where ℓ is an odd prime. Let k be a number field, M/k be an extension of degree 2, N/M be an extension of degree ℓ such that N/k is normal with Galois group D_ℓ. Denote by K/k a subfield of degree ℓ and define $d := \frac{\ell-1}{2}$. Then we get the following discriminant relation [6]:

$$d_{K/k} = d_{M/k}^{d} \mathcal{N}_{M/k}(d_{N/M})^{1/2}. \tag{1}$$



Using this discriminant relation the same approach will work for the group $D_\ell(2\ell) \leq S_{2\ell}$ and $D_\ell \leq S_\ell$. The reason is that up to isomorphy there exists a unique field K/k with Galois group D_ℓ corresponding to (contained in) a given N/k with Galois group $D_\ell(2\ell)$.

Denote by $\mathcal{D}_{k,\ell}$ the set of $D_\ell(2\ell)$–extensions of k and by I_k the set of ideals of k. Then we can define the following mapping:

$$\Psi : \mathcal{D}_{k,\ell} \to I_k^2, N/k \mapsto \left(d_{M/k}, \mathcal{N}_{M/k}(d_{N/M})^{1/(2(\ell-1))}\right).$$

In order to define the $2(\ell-1)$th root properly we need the following lemma:

Lemma 2.1. *$\mathcal{N}_{M/k}(d_{N/M})$ is a $2(\ell-1)$th power in I_k.*

Proof. N/M is a cyclic extension of prime degree. Therefore we have the relation $d_{N/M} = \mathfrak{c}_{N/M}^{\ell-1}$, where $\mathfrak{c}_{N/M}$ is the conductor of N/M. Let $\mathfrak{p} \subseteq \mathcal{O}_k$ be a prime ideal dividing $\mathcal{N}_{M/k}(d_{N/M})$. When $\mathfrak{p}$ is split in M then both prime ideals must divide $\mathfrak{c}_{N/M}$ which shows that $\mathfrak{p}^{2(\ell-1)} \mid \mathcal{N}_{M/k}(d_{N/M})$.

When $\mathfrak{p}$ is inert, i.e. $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}$, we have $\mathcal{N}_{M/k}(\mathfrak{P}) = \mathfrak{p}^2$ and we get the desired result. The last case is when $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}^2$. In this case $\mathfrak{P}$ is wildly ramified and therefore $\mathfrak{P}^2 \mid \mathfrak{c}_{N/M}$. □

We remark that the statement of this lemma is much weaker than [1, Theorem 10.1.25]. In this theorem it is proven that the conductor $\mathfrak{c}_{N/M} = \mathfrak{c}\mathcal{O}_M$ for some ideal $\mathfrak{c} \subseteq \mathcal{O}_k$. Using this result Lemma 2.1 follows easily.

Let $N \in \mathcal{D}_{k,\ell}$ and K be one of the subfields of N of degree ℓ. Using $d_{N/k} = d_{M/k}^{\ell}\mathcal{N}_{M/k}(d_{N/M})$ and equation (1) we get:

$$d_{N/k} = \mathfrak{a}^{\ell}\mathfrak{b}^{2(\ell-1)} \text{ and } d_{K/k} = \mathfrak{a}^{d}\mathfrak{b}^{\ell}, \tag{2}$$

where $\Psi(N) = (\mathfrak{a}, \mathfrak{b})$.

Clearly not every element of I_k^2 is in the image of Ψ. Let $(\mathfrak{a}, \mathfrak{b}) \in I_k^2$ be in the image of Ψ. Then $\mathfrak{a}$ is squarefree when we ignore prime ideals lying over 2. In other words $\mathfrak{p}^2 \mid \mathfrak{a}$ implies that the prime ideal $\mathfrak{p}$ contains 2. The ideal $\mathfrak{b}$ is squarefree when we ignore prime ideals lying above ℓ. Furthermore, the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ is only divisible by prime ideals lying above ℓ. We remark that these statements are easy to prove, e.g. see [1, Prop. 10.1.26]. Furthermore in the case $k = \mathbb{Q}$ it can be proven that $\mathfrak{b}$ itself must be squarefree.

The idea of our proof will be to count elements of I_k^2 with the above properties. Unfortunately Ψ is not injective. In the following we give upper estimates for the number of quadratic extensions M/k corresponding to a given ideal $\mathfrak{a}$. In a second step we will give upper estimates for the number of extensions N/M which correspond to the pair $(\mathfrak{a}, \mathfrak{b})$ when we assume that M/k is fixed. Altogether we get an upper estimate for the number of elements in $\mathcal{D}_{k,\ell}$ which map to the same pair $(\mathfrak{a}, \mathfrak{b})$.

The following lemma is an easy consequence of [1, Theorem 5.2.9].

Lemma 2.2. *Let k be a number field and $\mathfrak{a} \subseteq \mathcal{O}_k$ be an ideal. Denote by r_u the unit rank of k and by r_c the 2–rank of the class group Cl_k. Then there are at most $2^{r_c+r_u+1}$ quadratic extensions M/k which have discriminant $d_{M/k} = \mathfrak{a}$.*

We remark that in the case $k = \mathbb{Q}$ we get the upper estimate 2 for the number of extensions with the same discriminant. We remark that this is the right answer for ideals of the form $8 \cdot a \cdot \mathbb{Z}$, where a is odd and squarefree since in this case we have the extensions $\mathbb{Q}(\sqrt{2a})$ and $\mathbb{Q}(\sqrt{-2a})$ which correspond to our ideal.

Lemma 2.3. *Let M/k be a quadratic extension such that the ℓ–rank of the class group of M is r. Then the number of $D_\ell(2\ell)$–extensions $N/M/k$ which are subfields of the ray class field of $\mathfrak{b}\mathcal{O}_M$ is bounded from above by $\frac{\ell^{r+\omega(\mathfrak{b})}-1}{\ell-1}$, where $\omega(\mathfrak{b})$ denotes the number of different prime factors of $\mathfrak{b}$.*

Proof. Define $H := \mathrm{Gal}(M/k) = \langle\sigma\rangle$ and consider the ray class group of $\mathfrak{b}\mathcal{O}_M$ modulo ℓth powers as an H-module. In [6, Sections 5 and 6] it is proved that D_ℓ-extensions correspond to invariant subspaces of dimension 1 and eigenvalue -1. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$ not lying over ℓ. We distinguish two cases. First we assume that $\mathfrak{p}$ decomposes in M. In this case the ℓ-rank of the residue class ring $\mathcal{O}_M/\mathfrak{b}\mathcal{O}_M$ is 2 or 0 depending on $\ell \mid |(\mathcal{O}_k/\mathfrak{p})^\times|$ or not. If the rank is 2 then σ interchanges the two prime ideals lying over $\mathfrak{p}$ and we find a 1-dimensional subspace with eigenvalue 1 and one with eigenvalue -1. In case that $\mathfrak{p}$ is inert the ℓ-rank of the ray class group increases by at most 1. Similar arguments show the same result for prime ideals $\mathfrak{p}$ lying over ℓ. □

We remark that in the above lemma we give an upper estimate for all C_ℓ–extensions N/M such that the conductor is a divisor of $\mathfrak{b}$.

Altogether we get the following upper bound for the number of fibers of $(\mathfrak{a}, \mathfrak{b})$ under Ψ:

$$2^{\mathrm{rk}_2(\mathrm{Cl}_k)+r_u+1} \cdot \frac{\ell^{r+\omega(\mathfrak{b})}-1}{\ell-1}, \tag{3}$$

where r is the maximal ℓ–rank of the class group of a quadratic extension M/k of discriminant $\mathfrak{a}$ and r_u is the unit rank of k. Since our ground field k is fixed, we have that $2^{\mathrm{rk}_2(\mathrm{Cl}_k)+r_u+1}$ is a constant depending on k. We will see that $\omega(\mathfrak{b})$ will cause no problems. The critical part in this estimate is the dependency on the class group of a field M which we do not know explicitly.

In order to get good upper estimates we need to control the ℓ–rank of quadratic extensions. In order to simplify the situation let us restrict to the case $k = \mathbb{Q}$. In the general case we get similar results when we assume the corresponding things for relative quadratic extensions M/k. The Cohen–Lenstra–heuristic predicts the behavior of the class group of quadratic number fields. Let us state a special case of this conjecture [3, C6 and C10] which is only proven for $\ell = 3$. In the following conjecture all sums are over fundamental discriminants D. We define $r_D := \mathrm{rk}_\ell(\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})})$.

Conjecture 2.4. *(Cohen-Lenstra)*
The average of $\ell^{r_D}-1$ over all imaginary quadratic fields is 1, i.e.

$$\frac{\sum_{-D\le x} \ell^{r_D}-1}{\sum_{-D\le x} 1} \longrightarrow 1 \text{ for } x \longrightarrow \infty,$$

where only fundamental discriminants are considered in the sums. The average of $\ell^{r_D}-1$ over all real quadratic fields is ℓ^{-1}.

It is well known that $Z(\mathbb{Q}, C_2; x) \sim c(C_2)x$, where $c(C_2)$ is explicitly known, see e.g. [2]. For our purposes it will be enough to assume the

following, where O is the usual Landau symbol.

$$\sum_{-D\leq x} \ell^{r_D} = O(x), \tag{4}$$

$$\sum_{D\leq x} \ell^{r_D} = O(x). \tag{5}$$

Theorem 2.5. *Assume equations* (4) *and* (5). *Then for all odd primes* ℓ *we find constants* $c(\ell)$ *and* $\hat{c}(\ell)$ *such that:*

$$Z(\mathbb{Q}, D_\ell; x) \leq c(\ell)x^{1/d} = c(\ell)x^{a(D_\ell)}, \text{ where } d = \frac{\ell-1}{2},$$

$$Z(\mathbb{Q}, D_\ell(2\ell); x) \leq \hat{c}(\ell)x^{1/\ell} = \hat{c}(\ell)x^{a(D_\ell(2\ell))}.$$

Proof. Since $\mathbb{Z}$ is a principal ideal domain we can parameterize ideals in $\mathbb{Z}$ by positive integers. Using equations (2) and (3) we get:

$$Z(\mathbb{Q}, D_\ell(2\ell), x) \leq \sum_{D^\ell b^{2(\ell-1)}\leq x} \frac{\ell^{\omega(b)+r_D}-1}{\ell-1} + \sum_{(-D)^\ell b^{2(\ell-1)}\leq x} \frac{\ell^{\omega(b)+r_D}-1}{\ell-1},$$

where D runs over the fundamental discriminants, positive in the first sum and negative in the second one. Let us restrict to the first sum. The other one will be estimated in the same way.

$$\sum_{D^\ell b^{2(\ell-1)}\leq x} \frac{\ell^{\omega(b)+r_D}-1}{\ell-1} \leq \sum_{D^\ell b^{2(\ell-1)}\leq x} \ell^{\omega(b)}\ell^{r_D}$$

$$= \sum_{b^{2(\ell-1)}\leq x} \ell^{\omega(b)} \sum_{D\leq \frac{x^{1/\ell}}{b^{2(\ell-1)/\ell}}} \ell^{r_D} \overset{(5)}{\leq} \tilde{c} \sum_{b^{2(\ell-1)}\leq x} \frac{\ell^{\omega(b)}x^{1/\ell}}{b^{2(\ell-1)/\ell}}$$

$$= \tilde{c}x^{1/\ell} \sum_{b^{2(\ell-1)}\leq x} \frac{\ell^{\omega(b)}}{b^{2(\ell-1)/\ell}} = cx^{1/\ell}.$$

The last sum converges since $2(\ell-1)/\ell > 1$. The result for $Z(\mathbb{Q}, D_\ell, x)$ follows in the same way when we sum over $D^d b^{\ell-1} \leq x$. □

As already remarked we can prove similar results for arbitrary ground fields k when we assume corresponding results for the ℓ–rank of the class groups of quadratic extensions M/k. This becomes quite technical which is the reason that we do not give this case here.

Conjecture 2.4 is proved for $\ell = 3$ ([4]) which gives the following corollary.

Corollary 2.6. (1) $Z(\mathbb{Q}, D_3; x) \leq c(\ell)x^{a(D_3)}$.
(2) $Z(\mathbb{Q}, D_3(6); x) \leq c(\ell)x^{a(D_3(6))}$.

We remark that in the paper [4] the stronger result: $Z(k, S_3; x) \sim c(k, S_3)x$ is obtained.

If we want to have unconditional upper bounds for dihedral groups, the best thing we can do at the moment is the following:

$$\ell^{r_D} \leq \#\operatorname{Cl}_{\mathbb{Q}(\sqrt{D})} = O(D^{1/2}\log(D)).$$

If we use this estimate and use the method of the proof of Theorem 2.5 we can prove the following.

Theorem 2.7. *Let ℓ be an odd prime. Then for all $\epsilon > 0$ we can find constants $c(\ell, \epsilon)$ and $\hat{c}(\ell, \epsilon)$ such that:*

$$Z(\mathbb{Q}, D_\ell; x) \leq c(\ell, \epsilon)x^{3a(D_\ell)/2+\epsilon},$$
$$Z(\mathbb{Q}, D_\ell(2\ell); x) \leq \hat{c}(\ell, \epsilon)x^{3a(D_\ell(2\ell))/2+\epsilon}.$$

We remark that the $O(D^{1/2}\log(D))$ bound for ℓ^{r_D} can be improved to $O(\log(D)^{1/2-\epsilon})$ assuming the generelized Riemann hypothesis, see [5].

3. Lower bounds

In this section we are interested in lower bounds for the number of fields with dihedral Galois group. First we show that Cohen–Lenstra heuristic also provides lower bounds for our asymptotics. We prove that the non-validity of equations (4) or (5) implies that the asymptotics conjecture for the corresponding dihedral groups is wrong as well. This shows that the class group of intermediate fields is an important obstruction. As in the preceding section we assume $k = \mathbb{Q}$ to simplify everything. The following lemma is well known.

Lemma 3.1. *Let $M/\mathbb{Q}$ be a quadratic extension and N/M be a cyclic unramified extension of degree ℓ, where $\ell > 2$ is prime. Then* $\operatorname{Gal}(N/\mathbb{Q}) = D_\ell(2\ell)$.

Proof. $\operatorname{Gal}(N/\mathbb{Q})$ is a transitive subgroup of the wreath product $C_\ell \wr C_2$ and therefore one of the following groups: $C_\ell, D_\ell(2\ell)$, or $C_\ell \wr C_2$. Furthermore $\operatorname{Gal}(N/\mathbb{Q})$ is generated by its inertia groups. All ramified primes have order 2 and the dihedral group is the unique group in this list which is generated by elements of order 2. □

Now we count dihedral extensions which are unramified over their quadratic subfield.

$$Y(\mathbb{Q}, D_\ell(2\ell); x) :=$$
$$\#\{N/\mathbb{Q} : \operatorname{Gal}(N/\mathbb{Q}) = D_\ell(2\ell), \mathcal{N}(d_{N/\mathbb{Q}}) \leq x, N/M \text{ unramified}\}.$$

When we define $Y(\mathbb{Q}, D_\ell; x)$ in an analogous way we get:

Theorem 3.2. *Assume Conjecture 2.4. Then*

(1) $Y(\mathbb{Q}, D_\ell(2\ell); x) \sim cx^{1/\ell} = cx^{a(D_\ell(2\ell))}$.
(2) $Y(\mathbb{Q}, D_\ell; x) \sim \tilde{c}x^{2/(\ell-1)} = \tilde{c}x^{a(D_\ell)}$.

Proof. As in the proof of Theorem 2.5 we consider real and complex quadratic fields separately.

$$Y(\mathbb{Q}, D_\ell(2\ell); x) = \sum_{D^\ell \le x} \frac{\ell^{r_D} - 1}{\ell - 1} + \sum_{-D^\ell \le x} \frac{\ell^{r_D} - 1}{\ell - 1}$$

$$= \frac{1}{\ell - 1} \left(\sum_{D \le x^{1/\ell}} \ell^{r_D} - 1 + \sum_{-D \le x^{1/\ell}} \ell^{r_D} - 1 \right).$$

Using conjecture 2.4 we get the formula in our theorem. The second one can be proved in an analogous way. □

Now assume that one of the equations (4) or (5) is wrong. Using the same arguments as in the last proof we get a lower bound for dihedral groups D_ℓ which contradicts the asymptotics conjecture 1.1.

In the last part of this paper we prove the lower bound for dihedral groups unconditionally. We need the following result which is a special case of [4, Theorem 4.2].

Proposition 3.3. *Let ℓ be an odd prime and $p, q \equiv 1 \bmod \ell$ be two primes. Then the number of quadratic extensions $M/\mathbb{Q}$ which are split in p and q grows asymptotically like cx for some explicit constant c.*

The quadratic extensions given in the last proposition have the nice property that they admit a dihedral extension with bounded discriminant.

Lemma 3.4. *Let $M/\mathbb{Q}$ be a quadratic extension which is split in two primes p, q which are congruent to $1 \bmod \ell$ for an odd prime ℓ. Then there exists an extension N/M which is at most ramified in primes lying above p and q such that $\mathrm{Gal}(N/\mathbb{Q}) = D_\ell(2\ell)$.*

Proof. Using Lemma 3.1 we can assume that $\ell \nmid \#\,\mathrm{Cl}_M$. Define $\mathfrak{a} := pq\mathcal{O}_M$ and consider the ray class group $\mathrm{Cl}_\mathfrak{a}$. The multiplicative group of the residue ring $\mathcal{O}_M/\mathfrak{a}$ has ℓ–rank 4. Furthermore the ℓ–rank of the unit group of $\mathcal{O}_M$ is bounded above by 1. Using the canonical diagram for ray class groups, see e.g. [9, p. 126], shows that the ℓ–rank of $\mathrm{Cl}_\mathfrak{a}$ is at least 3. Let σ be the generator of the Galois group of $M/\mathbb{Q}$ and denote by A_ℓ the $\mathbb{F}_\ell[C_2]$–module $\mathrm{Cl}_\mathfrak{a} / \mathrm{Cl}_\mathfrak{a}^\ell$, using the canonical action of σ. Now we can decompose $A_\ell = A_\ell^+ \oplus A_\ell^-$, where $A_\ell^+ := \{a \in A_\ell \mid \sigma(a) = a\}$ and $A_\ell^- := \{a \in A_\ell \mid \sigma(a) = a^{-1}\}$. Using [6, Sections 5 and 6] we know that elements of A_ℓ^+ correspond to $C_2 \times C_\ell$ extensions and elements of A_ℓ^- correspond to $D_\ell(2\ell)$ extensions $N/\mathbb{Q}$. Since $C_2 \times C_\ell$ extensions of $\mathbb{Q}$ admit a subfield with Galois group C_ℓ over $\mathbb{Q}$, we see that $\mathrm{rk}_\ell(A_\ell)^+ = 2$. This implies $\mathrm{rk}_\ell(A_\ell^-) \ge 1$ and therefore the existence of our $D_\ell(2\ell)$ extension. □

Let N/M be such an extension given in the above lemma. Then

$$\mathcal{N}(d_{N/\mathbb{Q}}) \le \mathcal{N}(d_M)^{\ell}(pq)^{2(\ell-1)} \text{ and } \mathcal{N}(d_{K/\mathbb{Q}}) \le \mathcal{N}(d_K)^{(\ell-1)/2}(pq)^{\ell-1}, \tag{6}$$

where K is a subfield of N of degree ℓ. Now we can prove the following theorem.

Theorem 3.5. *Let ℓ be an odd prime. Then there exist positive constants $c_1(\ell), c_2(\ell)$ such that*

(1) $Z(\mathbb{Q}, D_\ell; x) \ge c_1(\ell)x^{a(D_\ell)}$ *for x large enough.*
(2) $Z(\mathbb{Q}, D_\ell(2\ell); x) \ge c_2(\ell)x^{a(D_\ell(2\ell))}$ *for x large enough.*

Proof. Choose primes $p, q \equiv \bmod \ell$. For every quadratic extension $M/\mathbb{Q}$ which is split in p and q we find a D_ℓ extension by Lemma 3.4 which has bounded discriminant as given in (6). Clearly, for different M those D_ℓ extensions are different. Using our discriminant formula we get:

$$Z(\mathbb{Q}, D_\ell; x) \ge \sum_{D^{(\ell-1)/2}(pq)^{\ell-1} \le x} 1 = \sum_{D \le (x/(pq)^{\ell-1})^{2/(\ell-1)}} 1,$$

where we sum only over fundamental discriminants D such that p and q are split in $\mathbb{Q}(\sqrt{D})$. Using Proposition 3.3 we get that the last sum grows asymptotically like $cx^{2/(\ell-1)}$ which proves our first formula. The second one can be proved analogously. □

References

[1] H. Cohen, *Advanced Topics in Computational Number Theory*. Springer, Berlin, 2000.
[2] H. Cohen, F. Diaz y Diaz, M. Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$. Compositio Math. **133** (2002), 65–93.
[3] H. Cohen, H. W. Lenstra, Jr., *Heuristics on class groups of number fields*. In: Number theory, Noordwijkerhout 1983, volume **1068** of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.
[4] B. Datskovsky, D. Wright, *Density of discriminants of cubic extensions*. J. reine angew. Math **386** (1988), 116–138.
[5] J. Ellenberg, A. Venkatesh, *Reflection principles and bounds for class group torsion*. To appear in Int. Math. Res. Not.
[6] J. Klüners, C. Fieker, *Minimal discriminants for small fields with Frobenius groups as Galois groups*. J. Numb. Theory **99** (2003), 318–337.
[7] J. Klüners, *A counterexample to Malle's conjecture on the asymptotics of discriminants*. C. R. Math. Acad. Sci. Paris **340** (2005), 411–414.
[8] J. Klüners, G. Malle, *Counting nilpotent Galois extensions*. J. Reine Angew. Math. **572** (2004), 1–26.
[9] S. Lang, *Algebraic Number Theory*. Springer, Berlin-Heidelberg-New York, 1986.
[10] G. Malle, *On the distribution of Galois groups*. J. Numb. Theory **92** (2002), 315–322.
[11] G. Malle, *On the distribution of Galois groups II*. Exp. Math. **13** (2004), 129–135.

Jürgen Klüners
Heinrich-Heine-Universität Düsseldorf,
Mathematisches Institut
Universitätsstr. 1, 40225 Düsseldorf, Germany
E-mail : klueners@math.uni-duesseldorf.de