THE DISTRIBUTION OF NUMBER FIELDS WITH WREATH PRODUCTS AS GALOIS GROUPS

JÜRGEN KLÜNERS

Abstract. Let G be a wreath product of the form $C_2 \wr H$, where C_2 is the cyclic group of order 2. Under mild conditions for H we determine the asymptotic behavior of the counting functions for number fields K/k with Galois group G and bounded discriminant. Those counting functions grow linearly with the norm of the discriminant and this result coincides with a conjecture of Malle. Up to a constant factor these groups have the same asymptotic behavior as the conjectured one for symmetric groups.

1. Introduction

Let k be a number field and $K = k(\alpha)$ be a finite extension of degree n with minimal polynomial f of α. By abuse of notation we define $\mathrm{Gal}(K/k) := \mathrm{Gal}(f)$. This means that we associate a Galois group even to a non-normal extension. Therefore the Galois group of K/k is a transitive permutation group $G \leq S_n$.

Denote by $\mathcal{N} = \mathcal{N}_{k/\mathbb{Q}}$ the norm function on ideals of k. Let

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

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 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 $x \in \mathbb{R}$. We are interested in the asymptotic behavior of this function for $x \to \infty$. Gunter Malle [15, 16] has given a precise conjecture how this asymptotics should look like. Before we can state it we need to introduce some group theoretic definitions.

Definition 1. Let $1 \neq G \leq S_n$ be a transitive subgroup acting on $\Omega = \{1, \dots, n\}$.

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

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

1991 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R16, 11R32.

Definition 2. For a number field k and a transitive subgroup $1 \neq G \leq S_n$ we define:

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

Now we can state the conjecture of Malle [16], where we write $f(x) \sim g(x)$ for $\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Conjecture 1. *(Malle) For all number fields k and all transitive permutation groups $1 \neq G \leq S_n$ 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 known to hold for all abelian groups and the groups $S_3 \leq S_3$ and $D_4 \leq S_4$. Let us state some easy properties of the constants $a(G)$ and $b(k,G)$ which are already given in [15, 16]. It is easy to see that $a(G) \leq 1$ and equality occurs if and only if G contains a transposition. It is an easy exercise (see Lemma 5) that all transpositions are conjugated in a transitive permutation group. Therefore we obtain $b(k,G) = 1$, if $a(G) = 1$. Since the symmetric group always contains a transposition, Malle's conjecture implies that the counting function $Z(k,n;x)$ for degree n extensions with bounded discriminant as above behaves like $c(n)x$ for some $c(n) > 0$. The latter conjecture is proven for $n \leq 5$, see [5, 2, 3], but nothing is known for $n \geq 6$.

One result of this paper is that for every even n there exists a group G such that $Z(k,G;x) \sim c(k,G)x$ with $c(k,G) > 0$. This group G will be a wreath product of type $C_2 \wr H$, where $H \leq S_{n/2}$, see Corollaries 5 and 6. There are mild conditions for H, but those are fulfilled if H is nilpotent or regular for instance.

The main results will be Theorems 6 and 7. Let H be a permutation group which fulfills the mild conditions of Theorem 6. Then the counting function of $G := C_2 \wr H$ behaves like

$$Z(k, C_2 \wr H; x) \sim c(k,G)x, \text{ where } c(k,G) > 0.$$

Furthermore, the corresponding Dirichlet series has a simple pole at 1 and has a meromorphic continuation to real part larger than $5/6$.

Note that in [10] we have given a counter example to Conjecture 1. In these counter examples it might happen that the exponent at the log-factor is bigger than $b(k,G) - 1$ when certain subfields of cyclotomic extensions occur as intermediate fields. Nevertheless, the main philosophy of this conjecture is still expected to be true.

2. Zeta functions, Hecke L–series, and ray class groups

In this section we collect some properties about Hecke L–series. For a number field k we denote by $\mathbb{P}(k)$ the set of prime ideals of the ring of integers $\mathcal{O}_k$ of k. We denote by

$$\zeta_k(s) := \prod_{\mathfrak{p}\in\mathbb{P}(k)} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})^s}\right)^{-1}, \quad \Re(s) > 1$$

the Dedekind zeta function of k which converges absolutely and locally uniformly for $\Re(s) > 1$. This function has a simple pole at $s = 1$ and we get the following estimates.

Lemma 1. *Let k be a number field of degree m with absolute discriminant d_k. Then:*

1 $|\zeta_k(s)| \leq \zeta_{\mathbb{Q}}(\Re(s))^m$ *for all s with $\Re(s) > 1$.*
2 *For all $0 < \epsilon \leq 1$:*

$$\mathrm{res}_{s=1}\zeta_k(s) \leq 2^{1+m}(d_k\pi^{-m/2})^\epsilon \epsilon^{1-m} \leq 2^{1+m} d_k^\epsilon \epsilon^{1-m}.$$

Proof. The first assertion is Corollary 3 in [18, p. 326]. The second one is Corollary 3 in [18, p. 332]. □

For an ideal $\mathfrak{c} \subseteq \mathcal{O}_k$ we consider a character χ of the ray class group $\mathrm{Cl}_{\mathfrak{c}}$, i.e. a homomorphism from $\mathrm{Cl}_{\mathfrak{c}}$ to $\mathbb{C}^*$. This character is only defined for ideals coprime to $\mathfrak{c}$. Let $S := \{\mathfrak{p} \in \mathbb{P}(k) : \mathfrak{p} \mid \mathfrak{c}\}$ be the exceptional set. For $\mathfrak{p} \in S$ we define $\chi(\mathfrak{p}) = 0$. Therefore we multiplicatively extend this character to all ideals. Now we are able to define the Hecke L–series:

$$L_k(\chi, s) := \prod_{\mathfrak{p}\in\mathbb{P}(k)} \left(1 - \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^s}\right)^{-1}.$$

As the Dedekind zeta function this product converges absolutely and locally uniformly for $\Re(s) > 1$. For further properties we refer the reader to [18, p. 343].

The Hecke L–series have a meromorphic continuation to the left. In the following we need upper estimates for $L_k(\chi, s)$ in strips of the form $a < \Re(s) \leq 1$. The following theorem follows directly from [9, equation 5.20]. The proof is similar to the proof of Theorem 7.4. in [18, p. 350], where we need to apply the convexity principle [14, p. 265].

Theorem 1. *Let k be a number field of degree m, $\mathfrak{f} \neq (0)$ be an ideal of $\mathcal{O}_k$, χ be a character of the ray class group $\mathrm{Cl}_{\mathfrak{f}}$, and $D := d_k\mathcal{N}(\mathfrak{f})$. Define $\delta := 1$ if χ is the trivial character and $\delta := 0$ otherwise. Then for all $\epsilon > 0$ and all s with $0 \leq \sigma := \Re(s) \leq 1$ we get the following estimate:*

$$|(s-1)^\delta L_k(s,\chi)| \leq c(\epsilon, m)(D|1+s|^m)^{(1-\sigma)/2+\epsilon}.$$

We can prove the following corollary.

Corollary 1. *With the same notations as in Theorem 1 we get for all $\epsilon > 0$:*

$$|L_k(s,\chi) - \frac{R(\chi)}{s-1}| \leq c(\epsilon, m)(D|1+s|^m)^{(1-\sigma)/2+\epsilon},$$

where $R(\chi)$ denotes the residue of $L_k(s,\chi)$ at $s = 1$. We define $R(\chi) = 0$, if χ is not the trivial character.

Proof. If χ is not trivial this is Theorem 1. For the trivial character χ with exceptional set S we get:

$$L_k(s,\chi) = \zeta_k(s) \prod_{\mathfrak{p}\in S} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})^s}\right).$$

Using Lemma 1 we get for our residue:

$$|R(\chi)| \leq \tilde{c}(\epsilon, m) d_k^\epsilon \text{ for all } \epsilon > 0.$$

Using Theorem 1 and by applying the triangular inequality we find a new constant $c(\epsilon, m)$ with

$$(s-1)L_k(s,\chi) - R(\chi) \leq c(\epsilon, m)(D|1+s|^m)^{(1-\sigma)/2+\epsilon}.$$

Since $L_k(s,\chi) - R(\chi)/(s-1)$ is analytic in $s=1$, we get the desired estimate for small $|s-1|$ using the maximum principle. $\square$

For our main results we need upper bounds for the number of cyclic extensions of a number field k which are at most ramified in a given finite set S of prime ideals. We refer the reader to [14, p.123-126] for properties of ray class groups which we use in the proof of the next theorem. In the following we denote by $\mathrm{rk}_\ell(\mathrm{Cl}_k)$ the ℓ–rank of the class group of k. We remark that we need the following result only for $\ell = 2$.

Theorem 2. *Let k be an algebraic number field of degree m with r_1 real embeddings, ℓ be a prime number, S be a finite set of prime ideals of $\mathcal{O}_k$, and*

$$S_1 := \{\mathfrak{p} \in S \mid \ell \notin \mathfrak{p}\}.$$

Define

$$s := \begin{cases} \mathrm{rk}_\ell(\mathrm{Cl}_k) + |S_1| + 2m & \ell > 2 \\ \mathrm{rk}_\ell(\mathrm{Cl}_k) + |S_1| + 2m + r_1 & \ell = 2 \end{cases}.$$

Then there exist at most $\frac{\ell^s - 1}{\ell - 1}$ C_ℓ–extensions of k which are at most ramified in S.

Proof. The idea of the proof is to choose a module $\mathfrak{m}$ in such a way that all C_ℓ–extensions are subfields of the ray class field of $\mathfrak{m}$. The infinite places are only important when $\ell = 2$. Each real infinite place may increase the 2–rank by at most 1. In case $\ell = 2$ we insert all real infinite places in $\mathfrak{m}_\infty$ and define

$$\mathfrak{m}_0 := \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_\mathfrak{p}},$$

where $e_\mathfrak{p} = 1$ for $\mathfrak{p} \in S_1$. For $\mathfrak{p} \in S \setminus S_1$ we have wild ramification and the following estimates are valid for arbitrary $e_\mathfrak{p} > 1$. In the following we compute upper bounds for the ℓ–rank of $(\mathcal{O}_k/\mathfrak{m}_0)^*$. Using the chinese remainder theorem we get:

$$(\mathcal{O}_k/\mathfrak{m}_0)^* \cong \prod_{\mathfrak{p} \in S} (\mathcal{O}_k/\mathfrak{p}^{e_\mathfrak{p}})^* \text{ for } \mathfrak{m}_0 = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_\mathfrak{p}}.$$

In case $e_\mathfrak{p} = 1$ we get that $(\mathcal{O}_k/\mathfrak{p})^*$ is the multiplicative group of a finite field which is therefore cyclic. This explains the $|S_1|$-part in our formula. In case $e_\mathfrak{p} > 1$ we get $(\mathcal{O}_k/\mathfrak{p}^{e_\mathfrak{p}})^* \cong (\mathcal{O}_k/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^{e_\mathfrak{p}})$. This case can only occur when $\mathfrak{p}$ is wildly ramified and therefore lies over ℓ. In this case the order of the multiplicative group of the residue field is coprime to ℓ. The second factor is an ℓ–group which can be generated by at most $[k_\mathfrak{p} : \mathbb{Q}_\ell] + 1$ elements (see e.g. [8]). Since

$$\sum_{\ell \in \mathfrak{p}} [k_\mathfrak{p} : \mathbb{Q}_\ell] = m$$

we get the worst case when all prime ideals above ℓ are contained in S and all corresponding completions have degree 1. In that case we can estimate the contribution to the rank of those prime ideals by $2m$. The contribution of the unramified extensions to the ℓ–rank is estimated by the ℓ–rank of the class group. $\square$

Unfortunately we do not know good estimates for the ℓ–rank of the class group. The best thing we can do in general is to bound $\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_k)} \leq |\,\mathrm{Cl}_k\,|$. The latter expression can be bounded by the following (see [18, p. 153]).

Theorem 3. *For all $\epsilon > 0$ and all $m \in \mathbb{N}$ there exist constants $c(m)$ and $c(m,\epsilon)$ such that for all number fields $k/\mathbb{Q}$ of degree m we have:*

$$|\operatorname{Cl}_k| \le c(m) d_k^{1/2} \log(d_k)^{m-1} \text{ and}$$

$$|\operatorname{Cl}_k| \le c(m,\epsilon) d_k^{1/2+\epsilon}.$$

In Section 5 we need the following estimate for an ideal $\mathfrak{a} \subseteq \mathcal{O}_k$. Denote by $\omega(\mathfrak{a})$ the number of different prime ideal factors and by $t_k(\mathfrak{a})$ the number of different ideal factors of $\mathfrak{a}$.

Lemma 2. *Let $b \in \mathbb{N}$. Then for all $\epsilon > 0$ there exist constants $c(\epsilon, m)$ and $c(\epsilon, m, b)$ such that for all number fields k of degree m the following estimates hold:*

1 $t_k(\mathfrak{a}) \le c(\epsilon, m)\mathcal{N}(\mathfrak{a})^\epsilon$,
2 $b^{\omega(\mathfrak{a})} \le c(\epsilon, m, b)\mathcal{N}(\mathfrak{a})^\epsilon$.

Proof. The first part is Lemma 2.2 in [11]. Let $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ be the factorization of $\mathfrak{a}$. Then:

$$t_k(\mathfrak{a}) = \prod_{\mathfrak{p}} (e_{\mathfrak{p}} + 1) \text{ and } b^{\omega(\mathfrak{a})} = \prod_{\mathfrak{p}} b.$$

Therefore we have $b^{\omega(\mathfrak{a})} < t_k(\mathfrak{a}^{b-1}) \le c_1(\epsilon, m)\mathcal{N}(\mathfrak{a})^{(b-1)\epsilon}$ using the first part of our lemma. Now our assertion follows easily. □

Later on we need some estimates about squarefull numbers. A positive integer N is called squarefull, if $p \mid N$ implies $p^2 \mid N$. Note that a squarefull integer can be uniquely written as $N = N_1^3 N_2^2$, where N_1 is squarefree. Therefore we get the generating Dirichlet series:

$$\sum_{N=1}^{\infty} \frac{a_N}{N^s} = \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)},$$

where $\zeta(s)$ is the Riemann ζ-function and $a_N = 1$ if and only if N is squarefull and $a_N = 0$ otherwise. Denote by $S(x)$ the number of squarefull numbers below x. As a consequence of a Theorem of Erdös and Szekeres (e.g. also see [1, Theorem 1], [19, exercise 10, p.54]) we know that there exists a constant A such that

$$S(x) \le A x^{\frac{1}{2}} \text{ for } x \ge 1. \tag{1}$$

We denote by $\omega(N)$ the number of different prime factors of an integer N. Then we use (see [19, Section 5.3, page 83]):

$$\omega(N) \le (1 + o(1)) \log N / \log\log N (N \to \infty). \tag{2}$$

This certainly implies that

$$\omega(N) \le B \frac{\log N}{\log\log(N+2)} \tag{3}$$

for any $N \ge 1$ for some constant B. Now we are able to prove:

Lemma 3. *Let $d \ge 1$ be a real number and denote by $T(x)$ the set of squarefull numbers below x. Then there exists for all $\epsilon > 0$ a constant $c(d,\epsilon)$ such that*

$$\sum_{N \in T(x)} d^{\omega(N)} \le c(d,\epsilon) x^{\frac{1}{2}+\epsilon} \text{ for every } x \ge 1.$$

Proof. We have the inequalities

$$\sum_{N \in T(x)} d^{\omega(N)} \leq S(x) \max_{N \leq x} d^{\omega(N)} \leq A x^{1/2} d^{B \log x / \log\log(x+2)}$$

using equations (1) and (3). Now we have

$$d^{\frac{B \log x}{\log\log(x+2)}} = x^{\frac{B \log(d)}{\log\log(x+2)}} = O_{d,\epsilon}(x^{\epsilon})$$

for all $\epsilon > 0$. Putting this together we get the wanted estimate. □

3. Quadratic extensions

The asymptotics of quadratic extensions of a number field k is well studied and known. Let us define the following Dirichlet series corresponding to $Z(k, C_2; x)$:

$$\Phi_{k,C_2}(s) := \sum_{[K:k]=2} \frac{1}{\mathcal{N}(d_{K/k})^s} = \sum_{N=1}^{\infty} \frac{a_N}{N^s}.$$

It is known that this Dirichlet series converges for $\Re(s) > 1$. Here a_N is the number of quadratic extensions K/k such that $\mathcal{N}(d_{K/k}) = N$. This means that $a_N \geq 0$ for all $N \in \mathbb{N}$. The following theorem is proved in [4]:

Theorem 4 (Cohen, Diaz y Diaz, Olivier)**.** *Let k be a number field with $i(k)$ complex embeddings. Then we get for $\Re(s) > 1$:*

$$\Phi_{k,C_2}(s) = -1 + \frac{2^{-i(k)}}{\zeta_k(2s)} \sum_{\mathfrak{c} | 2\mathcal{O}_k} \mathcal{N}(2\mathcal{O}_k/\mathfrak{c})^{1-2s} \sum_{\chi} L_k(s, \chi),$$

where χ runs over the quadratic characters of the ray class group $\mathrm{Cl}_{\mathfrak{c}^2}$ and $L_k(s,\chi)$ is the Hecke L–series of k corresponding to χ.

Using a Tauberian theorem (see e.g. [17, p. 121]) the following corollary is proved in [4].

Corollary 2 (Cohen, Diaz y Diaz, Olivier)**.**

$$Z(k, C_2; x) \sim 2^{-i(k)} \frac{\mathrm{res}_{s=1} \zeta_k(s)}{\zeta_k(2)} x,$$

where $2^{-i(k)} \frac{\mathrm{res}_{s=1}\zeta_k(s)}{\zeta_k(2)}$ equals the residue in $s = 1$ of Φ_{k,C_2}.

Our Dirichlet series has a simple pole at $s = 1$ and has a meromorphic continuation to the left. The proof of the following theorem comes from the properties of Hecke L–series. The number of characters, i.e. the number of summands can be bounded by the size of the ray class group which can be bounded up to a constant term depending on $[K : k]$ by the size of the class group of k. The latter one we bound by $O_{\epsilon,m}(d_k^{1/2+\epsilon})$, where $m = [k : \mathbb{Q}]$. Altogether we get:

Theorem 5. *$\Phi_{k,C_2}(s)$ has a meromorphic continuation for $\Re(s) > 1/2$. In this area it has only one pole at $s = 1$ with residue $R(k) = \frac{2^{-i(k)} \mathrm{res}_{s=1}\zeta_k(s)}{\zeta_k(2)}$. Furthermore, the function $g_k(s) := \Phi_{k,C_2}(s) - \frac{R(k)}{s-1}$ is analytic for $\Re(s) > 1/2$ and we get for all $\epsilon > 0$ and $\Re(s) > 1/2$:*

$$|g_k(s)| \leq c(\epsilon, m)(d_k |1+s|^m)^{(1-\sigma)/2+\epsilon} d_k^{1/2}.$$

4. Wreath products

Let $H_1 \leq S_e$ and $H_2 \leq S_d$ be two transitive groups and assume $n = ed$. Then the wreath product $H_1 \wr H_2 \cong H_1^d \rtimes H_2 \leq S_n$ is a semidirect product, where $H_2 \leq S_d$ permutes the d copies of H_1. For a formal definition we refer the reader to [6, p. 46]. The wreath product has a nice field theoretic interpretation in Galois theory. Assume that we have a field tower $L/K/k$ such that $\mathrm{Gal}(L/K) = H_1$ and $\mathrm{Gal}(K/k) = H_2$. Then we get that $\mathrm{Gal}(L/k) \leq H_1 \wr H_2$, see [13].

We want to study the asymptotic behavior of our counting function $Z(k, G; x)$ for wreath products $G = H_1 \wr H_2$ when we assume that we have some information for the corresponding counting functions for H_1 and H_2. First results in this direction already appear in [15]. The $a(G)$-part of the following lemma is [15, Lemma 5.1].

Lemma 4. *Let k be a number field and $H_1 \leq S_e, H_2 \leq S_d$ be transitive groups. Let $G := H_1 \wr H_2$. Then*

$$a(G) = a(H_1) \text{ and } b(k, G) = b(k, H_1).$$

Proof. Let $g = (h_1, h_2) \in H_1 \wr H_2$ where $h_1 = (h_{1,1}, \ldots, h_{1,d}) \in H_1^d$ and h_2 is the image of g under the projection to the complement H_2. If $h_2 \neq 1$ then g interchanges at least two blocks. Therefore the number of orbits is at most $(d-2)e+e = (d-1)e$. On the other hand, if $h_2 = 1, h_{1,2} = \cdots = h_{1,d} = 1$ then g has at least $(d-1)e+1$ orbits. Thus we may assume that $h_2 = 1$ and elements with minimal index have the property that $d-1$ of the $h_{1,i}$ equal 1. By conjugating with a suitable element of type $(1, \tilde{h}_2) \in G$ we can assume that $h_{1,2} = \cdots = h_{1,d} = 1$. Now let $h \in H_1$ be an element of minimal index $e-\ell$. Then $\mathrm{ind}(((h, 1, \ldots, 1), 1)) = n-(d-1)e-\ell = e-\ell$. This shows $a(H_1) = a(G)$. It is clear that h and $\tilde{h} \in H_1$ are conjugated in H_1 if and only if $((h, 1, \ldots, 1), 1)$ and $((\tilde{h}, 1, \ldots, 1), 1)$ are conjugated in $G = H_1 \wr H_2$. h and $\tilde{h}$ are in the same k–conjugacy class if a suitable power $\tilde{h}^a$ is conjugated to h. This statement remains true in the wreath product representation. Therefore we get the second statement. □

5. Wreath products of the form $C_2 \wr H$

In this section we prove Conjecture 1 for groups $G = C_2 \wr H$, where we need to assume weak properties of the asymptotic function for $H \leq S_d$. The proofs are inspired by the methods described in [4], where the corresponding results were shown for $G = D_4 \cong C_2 \wr C_2$.

Let L/k be an extension with Galois group $G = C_2 \wr H$. Then there exists a subfield $K \leq L$ such that $\mathrm{Gal}(L/K) = C_2$ and $\mathrm{Gal}(K/k) = H$. In a first step of our proof we will count all "field towers" of this type, i.e. we count all extensions L/k such that there exists an intermediate field K with $\mathrm{Gal}(L/K) = C_2$ and $\mathrm{Gal}(K/k) = H$. We remark that $\mathrm{Gal}(L/k) \leq C_2 \wr H$ using a theorem of Krasner and Kaloujnine [13]. In a second step of the proof we show that the asymptotics of proper subgroups which occur in such field towers is strictly less.

In [11, Proposition 8.3] we already proved the following upper bound for wreath products of this type. This proof is based on Proposition 5.2. and Corollary 5.3. in [15] with $\delta_0 = 1/2$ coming from Theorem 3. We remark that we weakened the assumption by replacing the exponent $a(H) + \delta$ by $1 + \delta$. The same proof gives the new result.

Proposition 1. *Let k be a number field, $H \le S_d$ be a transitive permutation group such that $Z(k,H;x) \le c(k,H,\delta)\, x^{1+\delta}$ for all $\delta > 0$. Then for any $\epsilon > 0$ there exists a constant $c(k, C_2 \wr H, \epsilon)$ such that*

$$Z(k, C_2 \wr H; x) \le c(k, C_2 \wr H, \epsilon)\, x^{a(C_2 \wr H)+\epsilon}\,.$$

We remark that $a(C_2 \wr H) = a(C_2) = 1$ by Lemma 4. Furthermore we remark that the proof counts all fields towers $L/K/k$ as above. Therefore the same upper bound applies.

In the following let us assume that for all $\epsilon > 0$ we have

$$Z(k,H;x) \le c(k,H,\epsilon)x^{1+\epsilon}.$$

We remark that using the results in [11] this assumption is true for all p-groups. Using results proved in [7] this assumption is also true for all regular H, i.e. when K/k is normal. For the first step we define the corresponding counting function

$$\tilde{Z}(k, C_2 \wr H; x) := \#\{L/k \mid \exists K : \mathrm{Gal}(L/K) = C_2, \mathrm{Gal}(K/k) = H, \mathcal{N}(d_{L/k}) \le x\}.$$

Using our assumption on H and Proposition 1 we get for all $\epsilon > 0$ that

$$\tilde{Z}(k, C_2 \wr H; x) \le c(k,H,\epsilon)x^{1+\epsilon}.$$

Let us associate the corresponding Dirichlet series $\Phi(s)$ to $\tilde{Z}(k, C_2 \wr H; x)$ which is absolutely convergent for $\Re(s) > 1$. Define

$$\mathcal{K}_H := \{K/k \mid \mathrm{Gal}(K/k) = H\}.$$

Using the equality $\mathcal{N}(d_{L/k}) = \mathcal{N}(d_{K/k})^2 \mathcal{N}(d_{L/K})$ and that Φ is absolutely convergent for $\Re(s) > 1$ we get in that area:

$$\Phi(s) = \sum_{K \in \mathcal{K}_H} \frac{\Phi_{K,C_2}(s)}{\mathcal{N}(d_{K/k})^{2s}}, \tag{4}$$

where $\Phi_{K,C_2}(s)$ is the Dirichlet series associated to $Z(K, C_2; x)$.

Theorem 6. *Assume that there exists at least one extension of k with Galois group H and that the following estimate holds for all $\epsilon > 0$:*

$$Z(k,H;x) = O_{k,H,\epsilon}(x^{1+\epsilon}).$$

Then the function $\Phi(s)$ defined in equation (4) has a meromorphic continuation to $\Re(s) > 5/6$. In this area it has exactly one pole at $s = 1$.

Proof. Using Theorem 5 the result is trivial if there are only finitely many extensions of k with Galois group H. We remark that d_K and $\mathcal{N}(d_{K/k})$ only differ by a constant depending on k and H since $d_K = d_k^{[K:k]}\mathcal{N}(d_{K/k})$. Using our assumption we get that the Dirichlet series

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d_{K/k})^s} \tag{5}$$

converges absolutely and locally uniformly for $\Re(s) > 1$. We consider the function

$$g(s) := \sum_{K \in \mathcal{K}_H} \frac{\Phi_{K,C_2}(s) - R(K)/(s-1)}{\mathcal{N}(d_{K/k})^{2s}},$$

where $R(K)$ is the residue of Φ_{K,C_2} at $s = 1$. Using Theorem 5 we get that $g_K(s) := \Phi_{K,C_2}(s) - R(K)/(s-1)$ is an analytic function for $\Re(s) > 1/2$. Furthermore we get by Theorem 5 for all $\epsilon > 0$ and $\Re(s) > 1/2$ the following estimate:

$$|g_K(s)| = O_{\epsilon,[k:\mathbb{Q}]}(|d_K(s+1)^{[K:\mathbb{Q}]}|^{(1-\sigma)/2+\epsilon})d_K^{1/2},$$

where $\sigma = \Re(s)$. The function

$$g(s) = \sum_{K\in\mathcal{K}_H} \frac{g_K(s)}{\mathcal{N}(d_{K/k})^{2s}}$$

converges absolutely and locally uniformly using (5), if $\sigma = \Re(s)$ satisfies the inequality

$$2\sigma - (1/2 + (1-\sigma)/2 + \epsilon) > 1 \Leftrightarrow 5/2\sigma > 2 + \epsilon \Leftrightarrow \sigma > 4/5 + 2/5\epsilon.$$

Therefore $g(s)$ is an analytic function for $\Re(s) > 5/6$.

Using Lemma 1 we have $R(K) = O_{\epsilon,[k:\mathbb{Q}]}(d_K^\epsilon)$ for all $\epsilon > 0$. Since $d_K = d_k^{[K:k]}\mathcal{N}(d_{K/k})$ we get that

$$\frac{1}{s-1}\sum_{K\in\mathcal{K}_H} \frac{R(K)}{\mathcal{N}(d_{K/k})^{2s}}$$

converges absolutely and locally uniformly for all regions which are contained in $\{s \in \mathbb{C} \mid \Re(s) > 5/6 \text{ and } s \neq 1\}$. The absolute convergence of all considered series gives the wished result for

$$\Phi(s) = g(s) + \sum_{K\in\mathcal{K}_H} \frac{R(K)/(s-1)}{\mathcal{N}(d_{K/k})^{2s}}.$$

□

As an application of a suitable Tauberian theorem (see e.g. [17, p. 121]) we immediately get:

Corollary 3. *Using the same assumptions as in Theorem 6 we get:*

$$\tilde{Z}(k, C_2 \wr H; x) \sim \mathrm{res}_{s=1}(\Phi(s))x.$$

In the following we would like to show that

$$\tilde{Z}(k, C_2 \wr H; x) \sim Z(k, C_2 \wr H; x)$$

holds, i.e. extensions which do not have the wreath product as Galois group do not contribute to the main term. We need some group theory.

Definition 3. Let $G \leq S_n$ be a transitive group operating on $\Omega = \{1, \ldots, n\}$. Then $\Delta \subseteq \Omega$ is called a block of G, if $\Delta^g \cap \Delta \in \{\Delta, \emptyset\}$ for all $g \in G$. If G has only blocks of size 1 or n we call G primitive. Otherwise G is called imprimitive.

We remark that a field extension L/k contains non-trivial subfields if and only if $\mathrm{Gal}(L/k)$ is imprimitive. The blocks containing 1 are in 1-1 correspondence to the subfields of L/k.

Lemma 5. *Let $G \leq S_n$ be a transitive group containing a transposition. Then:*

1 *All transpositions are conjugated in G, i.e. $b(k, G) = 1$.*
2 *$G = S_e \wr H$ for some $1 \neq e$, $e \mid n$ and $H \leq S_{n/e}$ transitive.*

Proof. The first part is [16, Lemma 2.2]. If G is primitive the second statement with $e = 1$ and $H = G$ is [6, Theorem 3.3A]. Assume that $\tau = (i, j)$ is a transposition of G and B is a minimal block of size larger than 1 containing i. Then $\tau(i) = j \in B$ since all the other elements in B are fixed by τ. Therefore $G|_B$ contains a transposition and operates primitively on B (B is a minimal block). Therefore the operation of $G|_B$ on B is isomorphic to $S_{|B|}$. Let $\tilde{B}$ be a conjugated block of B. By conjugating τ we can find a transposition in $\tilde{B}$. Therefore we find $n/|B|$ different copies of $S_{|B|}$. Therefore $G \cong S_{|B|} \wr H$, where H is the image of the natural homomorphism $\varphi : G \to S_{n/|B|}$ which permutes the conjugated blocks. □

Now we apply this lemma to our situation of field towers. Having a subfield K with L/K of degree $e = 2$ means that $\mathrm{Gal}(L/k)$ contains a block system of blocks of size 2.

Lemma 6. *Let $L/K/k$ be extensions of number fields with $\mathrm{Gal}(K/k) = H$ and $[L : K] = 2$. Let p be a prime which is unramified in K/k and assume $p||\mathcal{N}(d_{L/K})$. Then $\mathrm{Gal}(L/k) = C_2 \wr H$.*

Note that p unramified in K/k and $p||\mathcal{N}(d_{L/K})$ is equivalent to $p||\mathcal{N}(d_{L/k})$.

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$ which is ramified in L. Consider the prime ideal factorization $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Then Dedekind's discriminant theorem (see e.g. [12, Satz 3.12.11]) implies that $v_\mathfrak{p}(D_{L/k}) \geq (e_1 - 1)f_1 + \cdots (e_r - 1)f_r$, where f_i denotes the inertia degree of $\mathfrak{P}_i/\mathfrak{p}$ and $v_\mathfrak{p}$ is the exponential valuation. Furthermore we get equality when there is no wild ramification, i.e. $p \nmid e_i$ for all i. Since p is unramified in K/k and $p||\mathcal{N}(d_{L/K})$ there is at most one prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ such that $\sum_{i=1}^r (e_i - 1)f_i = 1$. This implies that exactly one $e_i = 2$ and all the other $e_j = 1$. Taking the corresponding inertia group generator, this elements acts as a transposition in $\mathrm{Gal}(L/k)$. Let $\tau = (i, j)$ be such a transposition and B a minimal block of $\mathrm{Gal}(L/k)$ corresponding to K which contains i. When we apply the proof of Lemma 5 to this situation we get the wanted result. □

We remark that we can replace the prime p in the above lemma by any unramified prime ideal $\mathfrak{p} \subseteq \mathcal{O}_k$. This does not improve the following estimates.

In the following we would like to count all field towers $L/K/k$ counted by $\tilde{Z}(k, C_2 \wr H; x)$ such that $\mathrm{Gal}(L/k)$ is a proper subgroup of $C_2 \wr H$. Therefore we define

$$Y(k, C_2 \wr H; x) :=$$
$$\#\{L/K/k \mid \mathrm{Gal}(L/k) \neq C_2 \wr H, \mathrm{Gal}(K/k) = H, [L : K] = 2, \mathcal{N}(d_{L/k}) \leq x\}.$$

We find upper bounds for this function when we count all field towers $L/K/k$ which do not satisfy the assumptions of Lemma 6. Before we examine those field towers we need a definition.

Definition 4. Let $a \in \mathbb{N}$ be a positive integer and $S \subseteq \mathbb{P}$ be a set of primes. Then a^S is defined to be the largest divisor of a coprime to S.

For a field tower $k \subset K \subset L$ we get:

$$\mathcal{N}(d_{L/k}) = \mathcal{N}(d_{K/k}^2)\mathcal{N}(d_{L/K}) \geq \mathcal{N}(d_{K/k}^2)\mathcal{N}(d_{L/K})^{S_K},$$

where $S_K := \{p \in \mathbb{P} \mid p|\mathcal{N}(d_{K/k})\}$. We define

$$\hat{Z}^{S_K}(K, C_2; x) := \#\{L/K \mid \mathrm{Gal}(L/K) = C_2, \mathcal{N}(d_{L/K})^{S_K} \leq x,$$

$$p \mid (\mathcal{N}(d_{L/K}))^{S_K} \Rightarrow p^2 \mid (\mathcal{N}(d_{L/K}))^{S_K} \forall p \in \mathbb{P}\}$$

and get

$$Y(k, C_2 \wr H; x) \leq \sum_{K \in \mathcal{K}_H(x^{1/2})} \hat{Z}^{S_K}(K, C_2; x/\mathcal{N}(d_{K/k}^2)),$$

where $\mathcal{K}_H(x) := \{K \in \mathcal{K}_H \mid \mathcal{N}(d_{K/k}) \leq x\}$. We need an estimate for $\hat{Z}^{S_K}(K, C_2; x)$. For fixed K we denote by a_N the number of fields L of degree 2 over K such that $\mathcal{N}(d_{L/K})^{S_K} = N$. Since we ignore all primes in S_K and all other prime divisors occur with multiplicity at least 2, we get that $a_N = 0$ if N is not squarefull. We choose $S \subseteq \mathbb{P}(K)$ as the set containing all prime ideals which lie over a prime in S_K or over a prime dividing N. We are interested in the number of quadratic extensions of K which are at most ramified in prime ideals contained in S. We get $|S| \leq (\omega(N) + |S_K|)t$, where $\omega(N)$ is the number of different prime factors and $t := [K : \mathbb{Q}]$. Note that $|S_K| \leq \omega(d_{K/k})$ and $\mathcal{N}(d_{K/k}) \leq d_K$. Therefore using Lemma 2 we derive the upper bound $2^{t|S_K|} \leq c(\epsilon, t, 2) d_K^{\epsilon}$, where the constant is not depending on K. Combining this with Theorems 2 and 3 we get with a new constant:

$$a_N \leq 2^{\mathrm{rk}_2(\mathrm{Cl}_K)} 2^{t(\omega(N)+|S_K|)} 2^{3t} \leq c(t, \epsilon) d_K^{1/2+\epsilon} 2^{t\omega(N)}.$$

Note that $a_N = 0$ if N is not squarefull. Therefore we get:

$$\sum_{N \in T(x)} a_N \leq c(t, \epsilon) d_K^{1/2+\epsilon} \sum_{N \in T(x)} 2^{t\omega(N)}.$$

Using Lemma 3 we can bound the latter sum by $O(x^{1/2+\epsilon})$ for all $\epsilon > 0$ and we get with a new constant $c(t, \epsilon)$:

$$\hat{Z}^{S_K}(K, C_2; x) \leq c(t, \epsilon) d_K^{1/2+\epsilon} x^{1/2+\epsilon}.$$

Inserting this in the above estimate for $Y(k, X_2 \wr H; x)$ we get using $d_K = d_k^2 \mathcal{N}(d_{K/k})$:

$$Y(k, C_2 \wr H; x) \leq \sum_{K \in \mathcal{K}_H(x^{1/2})} c(t, \epsilon)(d_k^2 \mathcal{N}(d_K))^{1/2+\epsilon} \left(\frac{x}{\mathcal{N}(d_{K/k}^2)}\right)^{1/2+\epsilon}$$

$$\leq c(t, \epsilon) d_k^{1+2\epsilon} x^{1/2+\epsilon} \sum_{K \in \mathcal{K}_H(x^{1/2})} \frac{\mathcal{N}(d_{K/k})^{1/2+\epsilon}}{\mathcal{N}(d_{K/k})^{1+2\epsilon}}$$

Using $\mathcal{N}(d_{K/k}) \leq x^{1/2}$ we get:

$$Y(k, C_2 \wr H; x) \leq c(t, \epsilon) d_k^{1+2\epsilon} x^{1/2+\epsilon} x^{1/4+\epsilon} \sum_{K \in \mathcal{K}_H(x^{1/2})} \frac{1}{\mathcal{N}(d_{K/k})^{1+2\epsilon}}.$$

The last sum converges under the assumption for H of Theorem 6. This proves for all $\epsilon > 0$ the following estimate:

$$Y(k, C_2 \wr H; x) \leq c(k, H, t, \epsilon) x^{3/4+2\epsilon}.$$

Using the identity $Z(k, C_2 \wr H; x) + Y(k, C_2 \wr H; x) = \tilde{Z}(k, C_2 \wr H; x)$ and Theorem 6 we proved the following:

Theorem 7. *Assume the same as in Theorem 6. Then the Dirichlet series corresponding to $Z(k, C_2 \wr H; x)$ has a meromorphic continuation to $\Re(s) > 5/6$, where*

$s = 1$ is the only pole in that region. The residue r of that simple pole coincides with the one of the function $\Phi(s)$. We get:

$$Z(k, C_2 \wr H; x) \sim \mathrm{res}_{s=1}(\Phi(s))x.$$

We are able to give an expression for this residue as a convergent sum.

Corollary 4.

$$\mathrm{res}_{s=1}(\Phi(s)) = \sum_{K \in \mathcal{K}_H} \frac{\mathrm{res}_{s=1}\zeta_K(s)}{2^{i(K)} d_K^2 \zeta_K(2)}.$$

These results support our main conjecture.

Corollary 5. *Conjecture 1 is true for all $C_2 \wr H$ and all number fields k such that H fulfills the assumptions of Theorem 6.*

We have already remarked that this assumption is true for all p–groups and all regular permutation groups. Therefore we get the following corollary.

Corollary 6. *For even n there exists a group $G \leq S_n$ with $a(G) = 1$ and*

$$Z(k, G; x) \sim c(k, G)x = c(k, G)x^{a(G)}.$$

Acknowledgments

I would like to thank Étienne Fouvry and Gunter Malle for many discussions about this topic. Furthermore I would like to thank the referee who made many useful comments improving this paper. This project was partially supported by the Deutsche Forschungsgemeinschaft (DFG).

References

[1] P. Bateman, and E. Grosswald. On a theorem of Erdös and Szekeres. *Illinois J.Math*, 2:88–98, 1958.

[2] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[3] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[4] H. Cohen, F. Diaz y Diaz, and M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Math.*, 133(1):65–93, 2002.

[5] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[6] J. Dixon and B. Mortimer. *Permutation groups*. Springer, Berlin-Heidelberg-New York, 1996.

[7] J. Ellenberg and A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math.*, 163:723–741, 2006.

[8] F. Hess, S. Pauli, and M. E. Pohst. Computing the multiplicative group of residue class rings. *Math. Comput.*, 72(243):1531–1548, 2003.

[9] H. Iwaniec and E. Kowalski. *Analytic Number Theory*, volume 53 of *Colloquium Publications*. American Mathematical Society, 2004.

[10] J. Klüners. A counterexample to Malle's conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.

[11] J. Klüners and G. Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.

[12] H. Koch. *Zahlentheorie, algebraische Zahlen und Funktionen*. Vieweg, Braunschweig/Wiesbaden, 1997.

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

[14] S. Lang. *Algebraic Number Theory*. Springer, Berlin-Heidelberg-New York, 1986.

[15] G. Malle. On the distribution of Galois groups. *J. Numb. Theory*, 92:315–322, 2002.

[16] G. Malle. On the distribution of Galois groups II. *Exp. Math.*, 13:129–135, 2004.
[17] W. Narkiewicz. *Number Theory*. World Scientific, 1983.
[18] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer, 1989.
[19] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*. Cambridge Studies in Advanced Mathematics 46, Cambridge University Press, Cambridge, 1995.

E-mail address: `klueners@math.uni-paderborn.de`

Universität Paderborn, Institut für Mathematik, D-33095 Paderborn, Germany.