THE ASYMPTOTICS OF NILPOTENT GALOIS GROUPS

JÜRGEN KLÜNERS

Abstract. We prove an upper bound for the asymptotics of counting functions of number fields with nilpotent Galois groups.

1. THE COUNTING FUNCTION

Let \( G \leq S_n \) be a finite transitive permutation group with \( n > 1 \) and \( k \) be a number field. 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 of \( G \). By abuse of notation we will write \( \text{Gal}(K/k) = G \) in this situation. We let

\[
Z(k, G; x) := \left| \left\{ K/k \mid \text{Gal}(K/k) = G, \ N_{k/\mathbb{Q}}(d_{K/k}) \leq x \right\} \right|
\]

to be the number of field extensions of \( k \) (inside a fixed algebraic closure \( \bar{\mathbb{Q}} \)) of degree \( n \) with Galois group permutation isomorphic to \( G \) and norm of the discriminant \( d_{K/k} \) bounded above by \( x \). Note that there are only finitely many number fields of given degree and bounded discriminant, hence \( Z(k, G; x) \) is finite for all \( G, k, x \). The goal of this note is to give the asymptotics of \( Z(k, G; x) \) for \( x \to \infty \) for certain groups \( G \). Gunter Malle [13, 14] has proposed a precise conjecture about the asymptotic behavior of the function \( Z(k, G; x) \) for \( x \to \infty \). In order to state it, we introduce some group theoretic invariants of permutation groups.

Definition 1.1. Let \( G \leq S_n \) be a transitive subgroup acting on \( \Omega = \{1, \ldots, n\} \).

(i) For \( g \in G \) we define the index \( \text{ind}(g) := n - \) the number of orbits of \( g \) on \( \Omega \).

(ii) \( \text{ind}(G) := \min \{ \text{ind}(g) : \text{id} \neq g \in G \} \), \( a(G) := \text{ind}(G)^{-1} \).

Since all elements in a conjugacy class \( C \) of \( G \) have the same index we can define \( \text{ind}(C) \) in a canonical way. The absolute Galois group of \( k \) acts on the set of conjugacy classes of \( G \) via the action on the \( \bar{\mathbb{Q}} \)-characters of \( G \). The orbits under this action are called \( k \)-conjugacy classes.

Definition 1.2. For a number field \( k \) and a transitive subgroup \( G \leq S_n \) we define:

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

Now we can state the conjecture of Malle [14], where \( f(x) \sim g(x) \) is a notation for \( \lim_{x \to \infty} f(x)/g(x) = 1 \).

Conjecture 1.3. (Malle) For all number fields \( k \) and all transitive permutation groups \( G \leq S_n \) 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.

2010 Mathematics Subject Classification. Primary 11R37; Secondary 11Y40.
This conjecture has been proved for abelian groups [19]. Assuming that $G$ is regular, i.e. we count normal nilpotent number fields, we have shown [9, Thm. 6.3]:

$$\lim_{x \to \infty} \frac{\log Z(k,G;x)}{\log x} = a(G).$$

This shows the correctness of the $a$-constant for those groups.

In the following we use the notation $f(x) = O(g(x))$, if $\lim \sup_{x \to \infty} f(x)/g(x) < \infty$. For all number fields $k$, all prime numbers $\ell$, and all $\ell$-groups $G$ it is shown in [9, Cor. 7.3] that

$$Z(k,G;x) = O(x^{a(G)+\epsilon})$$

for all $\epsilon > 0$.

We remark that [1, Cor. 1.8] is able to prove this upper bound for all nilpotent groups in all transitive representations.

Unfortunately, there are counterexamples [8] with respect to $b(k,G)$. There are no known counterexamples for nilpotent groups.

The goal of this article is to extend the results of [1, 9]. In Theorem 5.8 we are able to replace the upper bound of type $x^{a(G)+\epsilon}$ for all $\epsilon > 0$ by $x^{a(G)\log(x)d(k,G)-1}$.

**Theorem 1.4.** Let $G \leq S_n$ be a transitive nilpotent group and $k$ be a number field. Then there exists a constant $d(k,G) \geq b(k,G)$ such that

$$Z(k,G;x) = O(x^{a(G)\log(x)d(k,G)-1}).$$

For a discussion of the constant $d(k,G)$ we refer to the discussion starting at Remark 5.9. We show in Lemma 5.13 that $d(k,G) = b(k,G)$ for all nilpotent groups for which all elements of minimal index lie in the center. This trivially includes the abelian groups and the generalized quaternion groups. All elements of minimal index are of prime order $\ell$. We remark that $d(k,G)$ is only depending on the Sylow $\ell$-subgroup of $G$ and therefore we can construct many more examples as direct products of $p$-groups, for which our method yields the conjectured bound.

These upper bounds are valid for all transitive nilpotent groups and we think that the proof of the results are much easier compared to the proofs given in [9].

We mention that there is some active research about these conjectures and we refer the reader to the survey articles [3, 5, 18].

### 2. Analytic tools

In this section we develop some tools for the asymptotic behavior of sums corresponding to Euler products. In principle these tools are known, but it is very difficult to find good references. [7, Lemma 5.4 and 5.5] consider Euler products of the form $Z(s) = \prod_p W(p, p^{-s})$, where $W \in \mathbb{Z}[x,y]$ is a polynomial with constant term 1. We only need the classical case that the $x$-degree of $W$ is 0. They prove the area of convergence and that there is a meromorphic continuation to the left. Unfortunately, they do not give the order of the pole. Knowing these properties is necessary to get the asymptotic behavior of the corresponding series.

We give a version of a Tauberian theorem which is useful for our applications. This version is based on [6] and also proved in [16, page 121].

**Theorem 2.1** (Tauberian theorem of Delange). Let

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$
be a convergent Dirichlet series for \( s \in \mathbb{C} \) with \( \Re(s) > a > 0 \) with real \( a_n \geq 0 \). Furthermore, we assume in the area of convergence for a positive \( z \in \mathbb{R} \):

\[
f(s) = \frac{g(s)}{(s-a)^z} + h(s),
\]

where \( g \) and \( h \) are analytic functions in the half plane \( \Re(s) \geq a \) with \( g(a) \neq 0 \). Then we get for \( x \to \infty \):

\[
\sum_{n \leq x} a_n = \left( \frac{g(a)}{a \Gamma(z)} + o(1) \right) x^a \log(x)^{z-1},
\]

where \( \Gamma \) denotes the Gamma–function. This is equivalent to

\[
\sum_{n \leq x} a_n \sim \frac{g(a)}{a \Gamma(z)} x^a \log(x)^{z-1}.
\]

We remark that [16] also proves a version where we get \( \log(\log(x)) \)-factors in the asymptotics. These cases do not occur in this work. As an example the Riemann \( \zeta \)-function can be written as \( \zeta(s) = 1/(s-1) + h(s) \), where \( h(s) \) is analytic for \( \Re(s) > 0 \). In this special case the asymptotic behavior can be proved without using the Tauberian theorem. We need a similar result for number fields and we also want to restrict to prime ideals with certain congruence properties. Before we state the theorem we need the following lemma. In the following we use the notation \( \mathbb{P} \) for the prime numbers and the notation \( \mathbb{P}(k) \) for the (finite) prime ideals of the maximal order \( \mathcal{O}_k \) of \( k \).

**Lemma 2.2.** Let \( k \) be a number field, \( \ell \in \mathbb{P}, U := \{ p \in \mathbb{P}(k) \mid N(p) \equiv 0 \text{ or } 1 \mod \ell \} \), and \( \zeta_\ell \) be an \( \ell \)-th root of unity. For \( d, m \in \mathbb{N} \) we define for \( s \in \mathbb{C} \) with \( \Re(s) > 1/d \):

\[
f(s) := \prod_{p \in U} \left( 1 + \frac{m}{N(p)^{ds}} \right) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.
\]

Then we get with \( c := \frac{m}{[\mathbb{Q} (\zeta_\ell) : \mathbb{Q}]} \) and a constant \( c(k, \ell, d, m) > 0 \) for \( x \to \infty \):

\[
\sum_{n \leq x} a_n \sim c(k, \ell, d, m) x^{1/d} \log(x)^{e-1}.
\]

**Proof.** We have the following identity for all \( p \in U \):

\[
(1 + mN(p)^{-ds})(1 - N(p)^{-ds})^m = 1 - \left( \frac{m+1}{2} \right) N(p)^{-2ds} + \cdots - mN(p)^{-(m+1)ds}.
\]

We get with an easy computation or by [11, Lemma 5.4] that

\[
g(s) := \prod_{p \in U} \left( 1 - \left( \frac{m+1}{2} \right) N(p)^{-2ds} + \cdots - mN(p)^{-(m+1)ds} \right)
\]

is a convergent product for \( \Re(s) \geq 1/d \). We have

\[
f(s) = \prod_{p \in U} \left( 1 + \frac{m}{N(p)^{ds}} \right) = g(s) \prod_{p \in U} (1 - N(p)^{-ds})^{-m}.
\]

Now we write \( U = U_0 \cup U_1 \), where \( U_i \) contains the prime ideals which are congruent to \( i \) mod \( \ell \). Note that \( U_0 \) is a finite set and therefore

\[
g_0(s) := \prod_{p \in U_0} (1 - N(p)^{-ds})^{-m}
\]
Proof. \textit{we define} $(1 - \mathcal{N}(p)^{-s})^{-m} = \prod_{\mathfrak{p} \mid p} (1 - \mathcal{N}(\mathfrak{p})^{-s})^{-e}$. \\
Let $\hat{U}_1 \subset \mathbb{P}(k(\zeta))$ be the set of prime ideals lying over prime ideals of $U_1$. We get:
\begin{equation}
\prod_{p \in U_1} (1 - \mathcal{N}(p)^{-ds})^{-m} = \prod_{p \in \hat{U}_1} (1 - \mathcal{N}(p)^{-ds})^{-e} = \zeta_{k(\zeta)}(ds)^e \prod_{p \not\in \hat{U}_1} (1 - \mathcal{N}(p)^{-ds})^{-e}.
\end{equation}
Altogether we have for $s \in \mathbb{C}$ with $\Re(s) > 1/d$:
\begin{equation}
f(s) = \prod_{p \in U} \left(1 + \frac{m}{\mathcal{N}(p)^{ds}}\right) = g(s)g_0(s)\zeta_{k(\zeta)}(ds)^e \prod_{p \not\in \hat{U}_1} (1 - \mathcal{N}(p)^{-ds})^{-e}.
\end{equation}
All prime ideals in $\mathbb{P}(k)$ not lying in $\hat{U}_1$, lie over $\ell$, are ramified or have an inertia degree which is at least $2$. Since there are only finitely many prime ideals which are ramified or which lie over $\ell$, this Euler product is convergent for $s = 1/d$ and has a value between $0$ and $1$. Now we study the behavior of $\zeta_{k(\zeta)}(ds)^e$. Using the fact that the Dedekind $\zeta$-function has a simple pole at $s = 1$ we choose $a := 1/d$ and $z := e$ and we apply the Tauberian Theorem \ref{Tauberian} to get the desired result. \hfill $\square$

The following sums will occur in our applications. We remark that the $B_i$ come from the fact that in a cyclic extension of degree $\ell$ only prime ideals above $\ell$ and prime ideals congruent to $1$ modulo $\ell$ can ramify. Therefore by choosing $\ell_i = 2$ we get the asymptotics without congruence condition. We see that the congruence condition changes the log-part of the asymptotics. For the rest of the paper we denote by $\omega(a)$ the number of different prime ideal factors of $a$.

\begin{lemma}
Let $k$ be a number field, $m_1, \ldots, m_r, d_1, \ldots, d_r \in \mathbb{N}$, and $\ell_1, \ldots, \ell_r \in \mathbb{P}$. We define $n_{\ell_i} := [k(\zeta_{\ell_i}) : k]$, $d := \min(d_1, \ldots, d_r)$, $e := \sum \frac{m_i}{n_{\ell_i}}$, and \[B_i := \{p \in \mathbb{P}(k) \mid \mathcal{N}(p) \equiv 0, 1 \mod \ell_i\}.\]
Then we get for a suitable constant $c > 0$:
\[\sum_{\mathcal{N}(a_i) \leq x} m_1^{\omega(a_i)} \cdots m_r^{\omega(a_r)} x^{1/d} \log(x)^{c-1},\]
where the sum is over all squarefree ideals $a_i$ such that $p \mid a_i \Rightarrow p \in B_i$.
\end{lemma}
\begin{proof}
The corresponding Dirichlet series $F(s)$ can be written as a product
\[F(s) = \prod_{i=1}^r F_i(s), \text{ where } F_i(s) = \prod_{p \in B_i} \left(1 + \frac{m_i}{\mathcal{N}(p)^{d_is}}\right).\]
Using Lemma \ref{convergence} we see that $F_i$ are convergent for $\Re(s) > 1/d_i$ with corresponding $z_i := m_i/n_{\ell_i}$. The functions with $d_i > d$ are convergent Euler products at $s = 1/d$ and therefore holomorphic with $F_i(1/d) \neq 0$. For the application of Theorem \ref{Tauberian} we define $a := 1/d$ and $z$ to be the sum of the $z_i$ and note that $z = e$. Altogether, $F(s) = \zeta_{k(\zeta)}(ds)^e G(s)$, where $G(s)$ is holomorphic at $s = 1/d$ and $G(1/d) \neq 0$. \hfill $\square$
3. Class group bounds

We denote by \( \text{rk}_\ell(\text{Cl}_k) := \dim_{\mathbb{F}_\ell}(\text{Cl}_k / \text{Cl}_k^0) \) the \( \ell \)-rank of the class group \( \text{Cl}_k \) of the maximal order \( \mathcal{O}_k \) of \( k \) and by \( r_1 \) the number of real places of \( k \).

**Lemma 3.1.** Let \( k \) be a number field, \( \ell \in \mathbb{P} \), and \( S \subseteq \mathbb{P}(k) \) be a finite set of prime ideals. Then there are at most \( \frac{\ell^s - 1}{\ell - 1} \) \( C_\ell \)-extensions of \( k \) which are unramified outside \( S \), where

\[
\ell^s = \begin{cases} 
\text{rk}_\ell(\text{Cl}_k) + |S| + [k : \mathbb{Q}] & \ell > 2, \\
\text{rk}_\ell(\text{Cl}_k) + |S| + [k : \mathbb{Q}] + r_1 & \ell = 2.
\end{cases}
\]

**Proof.** The idea of the proof is to find an ideal \( \mathfrak{a} \) such that all wanted \( C_\ell \)-extensions are a subfield of the ray class field of \( \mathfrak{a} \) and the at most \( r_1 \) real places of \( k \). Certainly, we can define \( \mathfrak{a} := \prod_{\mathfrak{p} \in S} \mathfrak{p}^{a_\mathfrak{p}} \) for a suitable choice of the numbers \( a_\mathfrak{p} \geq 1 \). Denote the ray class group of \( \mathfrak{a} \) and the infinite places by \( A \). We would like to analyze the group \( A/\text{Cl}_k \) and we use the notation of [12], pp. 123. Let \( \mathfrak{c} \) be the cycle which is divisible by all real places and has finite part \( c_0 := a \). We get [12, p. 126]:

\( A/\text{Cl}_k \cong (k(\mathfrak{c})/k_\mathfrak{c}) / (U/U_\mathfrak{c}) \).

We remark that

\( k(\mathfrak{c})/k_\mathfrak{c} \cong (\mathcal{O}_k/\mathfrak{a})^\times \times \mathbb{C}_2^{r_1} \)

in our notation, where the latter part is coming from the \( r_1 \) real places.

We get that the \( \ell \)-rank of \( A \) is at most \( \text{rk}_\ell(\mathcal{O}_k/\mathfrak{a})^\times + \text{rk}_\ell(\text{Cl}_k) + r_1 \). This explains the \( \text{rk}_\ell(\text{Cl}_k) \) and the \( r_1 \)-part of the formula in the claim. We define \( S_1 := \{ \mathfrak{p} \in S \mid \ell \not\equiv \mathfrak{p} \} \). Then by the Chinese remainder theorem we can write:

\[
(\mathcal{O}_k/\mathfrak{a})^\times \cong \prod_{\mathfrak{p} \in S} (\mathcal{O}_k/\mathfrak{p}^{a_\mathfrak{p}})^\times = \prod_{\mathfrak{p} \in S_1} (\mathcal{O}_k/\mathfrak{p}^{a_\mathfrak{p}})^\times \times \prod_{\mathfrak{p} \in S \setminus S_1} (\mathcal{O}_k/\mathfrak{p}^{a_\mathfrak{p}})^\times.
\]

Therefore we have to study \( (\mathcal{O}_k/\mathfrak{p}^{a_\mathfrak{p}})^\times \) which is isomorphic to

\[
(\mathcal{O}_k/(\mathfrak{p}^{a_\mathfrak{p}}))^\times \cong (\mathcal{O}_{k_\mathfrak{p}}/\mathfrak{p})^\times \times (1 + \mathfrak{p})/(1 + \mathfrak{p}^{a_\mathfrak{p}}),
\]

where we denote the unique prime ideal of \( \mathcal{O}_{k_\mathfrak{p}} \) by \( \mathfrak{p} \) as well. The group \( (\mathcal{O}_{k_\mathfrak{p}}/\mathfrak{p})^\times \) has size \( N(\mathfrak{p}) - 1 \) and \((1 + \mathfrak{p})/(1 + \mathfrak{p}^{a_\mathfrak{p}})\) is a \( p \)-group, where \( p \in \mathfrak{p} \cap \mathcal{P} \).

For \( p \in S_1 \) we have \( p \neq \ell \) and \( \text{rk}_\ell((\mathcal{O}_k/\mathfrak{p}^{a_\mathfrak{p}})^\times) \leq 1 \), since \( (\mathcal{O}_{k_\mathfrak{p}}/\mathfrak{p})^\times \) is a cyclic group of order \( N(\mathfrak{p}) - 1 \) and the order of the second factor of \( \mathfrak{p} \) is coprime to \( \ell \).

For \( p \in S \setminus S_1 \) we have \( p = \ell \). The order of the first group is coprime to \( \ell \). Using [17, Theorem 5.21] we get that \( \text{rk}_\ell((1 + \mathfrak{p})/(1 + \mathfrak{p}^{a_\mathfrak{p}})) \leq \lceil k_\mathfrak{p} : \mathbb{Q}_\ell \rceil + 1 \). Since \( [k : \mathbb{Q}] = \sum_{p
mid \ell} [k_p : \mathbb{Q}_\ell] \) we finish the proof.

It was not necessary in the above proof to compute the numbers \( a_\mathfrak{p} \). We remark that for prime ideals \( \mathfrak{p} \in S_1 \) we can choose \( a_\mathfrak{p} = 1 \), since bigger exponents do not change the \( \ell \)-rank of \( \mathfrak{p} \). The difficult part of the above lemma was to prove the upper bound for prime ideals lying over \( \ell \). If not all prime ideals above \( \ell \) are contained in \( S \) we can improve the \( [k : \mathbb{Q}] \)-part in the above lemma. In case \( S = S_1 \) we can omit this part completely.

In the following we also need a good upper bound for the number of \( C_\ell \)-extensions which are exactly ramified in prime ideals in \( S \). asymptotics.

**Theorem 3.2.** Let \( k \) be a number field, \( \ell \in \mathbb{P} \), and \( S, T \subseteq \mathbb{P}(k) \) be finite sets of prime ideals of \( \mathcal{O}_k \) with empty intersection. Then there exists a constant \( c(k, \ell) \)
such that the number of \( C_t \)-extensions of \( k \) which are ramified in all prime ideals of \( S \) and are unramified outside of \( S \cup T \) is bounded above by

\[
\ell^{(k, \ell) + |T|} \ell (\ell - 1)^{|S|}.
\]

**Proof.** Denote by \( M \) the composite of all \( C_t \)-extensions of \( k \) which are unramified outside \( S \cup T \). Let \( \text{Gal}(M/k) \cong C_t \). Note that all the wanted \( C_t \)-extensions of the claim are subfields of \( M/k \). In the following we would like to construct \( C_t \)-extensions \( k_1, \ldots, k_t \) of \( k \) such that the composite \( k_1 \cdots k_t = M \) and the fields \( k_i \) have nice properties. We define \( S_1 := \{ p \in S \mid \ell \notin p \} \). Note that if \( p \) is unramified in \( M/k \) for one \( p \in S_1 \), then there are no \( C_t \)-extensions with the desired properties.

For this we choose \( p_1 \in S_1 \). Let \( k_1 \leq M \) be one \( C_t \)-extension which is ramified in \( p_1 \). We claim that we can choose \( k_2, \ldots, k_t \) in a way such that \( k_2, \ldots, k_t \) are unramified in \( p_1 \). Certainly, we can find extensions \( k_2, \ldots, k_t \) such that \( M = k_1 \cdots k_t \). Now assume that \( k_i \) is ramified in \( p_1 \) and consider \( L := k_1 k_i \). By Abhyankar’s lemma [17 Cor. 4.p. 229], we see that \( L/k_1 \) is unramified over prime ideals lying above \( p_1 \) and therefore there exists a subfield (the inertia field) \( k \leq k_1 \leq L \) such that \( k_1/k \) is unramified in \( p_1 \). Now we replace \( k_i \) by \( k \). Now we choose \( p_2 \in S_1 \) such that \( p_2 \) is ramified in at least one of the fields \( k_2, \ldots, k_t \). Applying the same procedure as above we can assume that \( p_2 \) is ramified in \( k_2 \) and unramified in \( k_3, \ldots, k_t \). By replacing \( k_1 \) with \( k_1 \) in \( k_1 k_2 \) we can assume that \( k_1 \) is still ramified in \( p_1 \) and unramified in \( p_2 \). We continue this process as long we can find a prime ideal \( p_i \in S_1 \) which is ramified in at least one of the fields \( k_i, \ldots, k_t \).

When the process is finished we have chosen \( r \leq |S_1| \) prime ideals \( p_1, \ldots, p_r \in S_1 \) and \( C_t \)-extensions \( k_1, \ldots, k_t \) with \( M = k_1 \cdots k_t \) and the property that for \( 1 \leq i \leq r \) the prime ideal \( p_i \) is ramified in \( k_i \) and it is unramified in \( k_j \) for \( j \neq i \) and \( 1 \leq j \leq t \). Note that it is possible that \( r < |S_1| \). This happens for an example if \( p_1 \neq p \in S_1 \) is only ramified in \( k_1 \), but not in \( k_2, \ldots, k_t \).

Now let \( L/k \) be a \( C_t \)-extension which is contained in \( k_2 \cdots k_t \). Then \( L/k \) is unramified in \( p_1 \) and therefore we need not count \( L \). In the same way \( L \) is not ramified in \( p_i \) (\( 1 \leq i \leq r \)), if \( L \) is contained in \( \prod_{j \neq i} k_j \). We would like to count the \( C_t \)-extensions of \( M \) which are not contained in \( \prod_{j=1, j \neq i}^t k_j (1 \leq i \leq r) \) since those are not ramified in \( p_i \). By inclusion-exclusion we get for this number:

\[
\frac{\ell^{t-r}}{\ell - 1} \sum_{j=0}^{r}(\ell - j)^r \ell^{(r-j) - 1} = \frac{\ell^{t-r}}{\ell - 1} \sum_{j=0}^{r}(\ell - j)^r \ell^{r-j} - \frac{\ell^{t-r}}{\ell - 1} \sum_{j=0}^{r}(\ell - j)^r \ell^{t-r} = \frac{\ell^{t-r}}{\ell - 1} \ell (\ell - 1)^r - 0 = \frac{(\ell - 1)^r \ell^{t-r}}{\ell - 1} \leq \frac{(\ell - 1)^r (|S_1| - 1) \ell^{(k, \ell) + |T|}}{|S_1|}.
\]

For the last inequality we used that \( k_{r+1} \cdots k_t \) is contained in the maximal elementary abelian \( \ell \)-extension unramified outside \( T \cup S_0 \), where \( S_0 := \{ p \in S \mid \ell \notin p \} \). and we apply Lemma 3.3. Note that we can choose \( c(k, \ell) = \text{rk}_\ell(\text{Cl}_k) + |k : \mathbb{Q}| + |S_0| + r_1 \leq \text{rk}_\ell(\text{Cl}_k) + 3|k : \mathbb{Q}| \).

\[ \square \]

4. Finding all solutions of certain embedding problems

**Definition 4.1.** Let \( K/k \) be a Galois extension of number fields with group \( H \) and

\[ 1 \rightarrow U \rightarrow G \xrightarrow{\kappa} H \rightarrow 1 \]
be an exact sequence of finite groups. Denote by $\bar{k}$ an algebraic closure of $k$ containing $K$ and by $\varphi : \text{Gal}(\bar{k}/k) \to H \cong \text{Gal}(K/k)$ an epimorphism with kernel $\text{Gal}(\bar{k}/K)$. This is called the embedding problem given by $\kappa$ and $\varphi$. An epimorphism $\tilde{\varphi} : \text{Gal}(\bar{k}/k) \to G$ is called (proper) solution to the embedding problem, if $\kappa \circ \tilde{\varphi} = \varphi$. The fixed field $L$ of $\ker(\tilde{\varphi})$ is called solution field. Furthermore, the embedding problem is called central, if $U$ is in the center of $G$.

Suppose that we are given an extension $K/k$ with Galois group $H$ and we want to find all fields $L$ containing $K$ such that $\text{Gal}(L/k) \cong G$. Since the embedding problems depend on $\varphi$ and $\kappa$ these can in general not be obtained as solutions of a single embedding problem.

**Lemma 4.2.** Let $K/k$ be an extension of number fields with Galois group $H$ and let $G$ be a finite central extension of $H$. Then all fields $L/K$ such that $\text{Gal}(L/k) \cong G$ can be found as solutions of finitely many embedding problems, whose number only depends on $G$ and $H$.

**Proof.** Let $\varphi$ be defined as in Definition 4.1. Epimorphisms $\kappa : G \to H$ with the same kernel only differ by automorphisms of $H$. Furthermore, $G$ has only finitely many normal subgroups with quotient isomorphic to $H$. □

Our goal in this section is to describe all solutions to an embedding problem if we assume that we know one solution.

**Definition 4.3.** Let $G_1, G_2, H$ be finite groups and $\kappa_i : G_i \to H$ ($i = 1, 2$) epimorphisms. Then we define the subdirect product

$$G_1 \times_H G_2 := \{(g_1, g_2) \mid g_i \in G_i \ (i = 1, 2), \kappa_1(g_1) = \kappa_2(g_2)\}$$

with componentwise operation.

Note that this construction is also called fiber product or pullback. The order of this group is $|G_1||G_2|/|H|$. Suppose that we have an embedding problem as in Definition 4.1 and we have two different solutions $L_1$ and $L_2$ such that $L_1 \cap L_2 = K$. Then $\text{Gal}(L_1L_2/k) \cong G \times_H G$.

**Lemma 4.4.** Let $G$ be a group extension as in Definition 4.1. We define

$$\Psi : G \to \text{Aut}(U), \ g \mapsto (u \mapsto u^{(s^{-1})} = gu^{-1}).$$

Then

$$G \times_H G \cong U \rtimes G,$$

where the semidirect product is defined via $\Psi$.

**Proof.** We define $\Phi : U \times G \to G \times_H G$, $(u, g) \mapsto (g, ug)$. Since $\kappa(u) = 1$ for $u \in U$ we have $(g, ug) \in G \times_H G$. Furthermore, $\Phi$ is a homomorphism since

$$\Phi(u_1, g_1)\Phi(u_2, g_2) = (g_1, u_1g_1)(g_2, u_2g_2) = (g_1g_2, u_1g_1u_2g_2)$$

and

$$\Phi((u_1, g_1)(u_2, g_2)) = \Phi((u_1^{(g_1^{-1})}, g_1)(u_2, g_2)) = (g_1g_2, u_1u_2^{(g_1^{-1})}g_1g_2) = (g_1g_2, u_1g_1u_2g_2).$$

Finally, $\Phi$ is injective and then, also surjective since both groups have the same finite order. □
In the following we concentrate on embedding problems with abelian kernel $A$:

\[(3)\] $1 \rightarrow A \rightarrow G \twoheadrightarrow H \rightarrow 1$

We interpret $A$ as an $H$-module via $\Psi : H \rightarrow \text{Aut}(A) : h \mapsto (a \mapsto a^{c^{-1}(h)})$. We can take an arbitrary preimage of $h$ since $A$ is abelian. Note that this is not well defined for non-abelian normal subgroups. For given $A$, $H$, and $\Psi : H \rightarrow \text{Aut}(A)$ we construct a semidirect product as above.

The following theorem is the main result of this section. It gives a relation between split and non-split embedding problems with abelian kernel.

**Theorem 4.5.** Let $G$ be a group extension as in (3) and $\Psi : H \rightarrow \text{Aut}(A), h \mapsto (a \mapsto a^{c^{-1}(h)})$. Let $A \rtimes H$ be the corresponding semidirect product. Then:

\[G \times_H G \cong G \times_H (A \rtimes H).\]

Furthermore, $A \rtimes H \cong (G \times H)/\{(a, a) \mid a \in A\}$.

**Proof.** The homomorphism $\Psi$ can be canonically extended to $G$. Using Lemma 4.4 we get $G \times_H G \cong A \rtimes G$. Furthermore, $\Phi : A \times G \rightarrow A \rtimes H, (a, g) \mapsto (a, \kappa(g))$ is a surjective homomorphism since the automorphism corresponding to $h \in H$ is independent of the preimage under $\kappa$. The kernel equals $\{(1, a) \mid a \in A\}$. Using the isomorphism of Lemma 4.4 this kernel will be mapped to $\{(a, a) \mid a \in A\} \leq G \times_H G$.

We get that

\[A \rtimes G \rightarrow G \times_H (A \rtimes H), (a, g) \mapsto (g, (a, \kappa(g)))\]

is an isomorphism. \hfill \Box

The application of this theorem corresponds to the following field diagram:

\[
\begin{array}{ccc}
N & \downarrow & L_1 \\
L_2 & \downarrow & L_3 \\
G & \downarrow & A \rtimes H \\
& \downarrow & \downarrow & \downarrow \\
& k & \sim & H & \sim & L_2 & \sim & L_1 & \sim & N \\
& \sim & \sim & \sim & \sim & \sim & \sim & \sim & \sim & \sim
\end{array}
\]

We assume that $\text{Gal}(L_1/k) \cong \text{Gal}(L_2/k) \cong G$, $L_1 \cap L_2 = K$, and $N = L_1L_2$. Then there exists a field $K \leq L_3 \leq N$ with $\text{Gal}(L_3/k) = A \rtimes H$. Similar, if we know fields $L_1, L_3$ with the above Galois groups (and $L_1L_3 = N, L_1 \cap L_3 = K$) then the theorem gives us $L_2$ with Galois group $G$. Depending on the embedding problem there are more fields $K < L < N$ with Galois group $G$. This number is a group theoretic invariant which can be computed in concrete situations.

In this paper we would like to study nilpotent groups. Since non-trivial nilpotent groups have non-trivial center, we can reduce to the case that $A = C_\ell$ is a cyclic group of prime order in the center. We get:

\[(4)\] $1 \rightarrow C_\ell \rightarrow G \xrightarrow{\kappa} H \rightarrow 1$ central.

The easiest case is when a primitive $\ell$-th root of unity $\zeta_\ell$ is already contained in $k$. Then the embedding problem corresponding to (4) is a so-called Brauer embedding problem, e.g., see [13] chapter IV.7.

Since $\zeta_\ell \in k$ we then have solution fields $L/K$ of the form $L = K(\sqrt[n]{\alpha})$ for suitable $\alpha \in K$ (Kummer theory). There are other nice properties of Brauer embedding problems, e.g., a local-global principle is valid. For us the following lemma is important. The proof can be found in [13] chapter IV.7.
Lemma 4.6. Let $L = K(\sqrt[\alpha]{\alpha})$ be a solution field of a Brauer embedding problem. Then all solution fields are given by $K(\sqrt[\alpha]{\alpha a})$ with suitable $0 \neq a \in k$.

This lemma was the starting point of the approach in [9]. Via Kummer theory a similar correspondence was shown for fields $k$ not containing $\zeta_\ell$. We show this correspondence using the group theoretic approach we have just developed.

Theorem 4.7. Let $G$ be a central extension as in (2) and $\tilde{G} = C_\ell \times G \cong G \times_H G$. Then for $D := \{(a, b) \in C_\ell \times G \mid \kappa(b) = 1\} \cong C_\ell \times C_\ell$ we get:

(i) $D \leq \mathbb{Z}(G) = C_\ell \times \mathbb{Z}(G)$.

(ii) $D$ has $\ell + 1$ subgroups $U_1, \ldots, U_{\ell+1}$ of order $\ell$. All these subgroups are normal in $\tilde{G}$.

(iii) All quotients $\tilde{G}/U_i$ ($1 \leq i \leq \ell + 1$) except one are isomorphic to $G$. The remaining quotient is isomorphic to $C_\ell \times H$.

Proof. The isomorphy $C_\ell \times G \cong (C_\ell \times H) \times_H G \cong G \times_H G$ is Theorem 4.5. The first two assertions are elementary. Let $a$ be a generator of the kernel of $\kappa$. We remark that we interpret the first factor of the direct product as the subgroup in the kernel of $\kappa$. Then we describe the subgroups $U_i \leq C_\ell \times G$ as follows

$U_i := \langle (a, a^i) \rangle$ (for $1 \leq i \leq \ell$) and $U_{\ell+1} := \langle (1, a) \rangle$.

Clearly, we get $\tilde{G}/U_{\ell+1} \cong C_\ell \times H$. We define the following images under the isomorphism $\Phi$ from the proof of Lemma 4.2:

$\tilde{U}_i = \Phi(U_i) = \langle (a^i, a^{i+1}) \rangle$ for $1 \leq i \leq \ell$.

Using the isomorphism we get $(C_\ell \times G)/U_i \cong (G \times_H G)/\tilde{U}_i$. Let $(g, \tilde{g}) \in G \times_H G$.

Since $\kappa(g) = \kappa(\tilde{g})$ we get $\tilde{g} = ga^j$ for some $j \in \{0, \ldots, \ell - 1\}$.

We choose $l \equiv -j$ mod $\ell$ and get:

$(g, ga^j)(a^i, a^{i+1})^l = (ga^{il}, ga^{j+i+1}a^{i+l}) = (ga^{il}, ga^{l+i+1}) = (ga^{il}, ga^{il})$.

Therefore we find in the quotient $(G \times_H G)/\tilde{U}_i$ representatives for each element, whose components coincide. Therefore this quotient is isomorphic to $G$. \hfill $\square$

This theorem shows that we can describe all solutions of our embedding problem (4), if we know one solution. Let $L/K$ be a solution field and $M/k$ be a $C_\ell$-extension with $[ML : L] = \ell$. Using Theorem 4.7 we get $\ell - 1$ new solution fields of our embedding problem. Two cyclic $C_\ell$-extensions $M_1, M_2$ of $k$ parameterize the same solution fields, if $LM_1 = LM_2$. This condition defines on the set of $C_\ell$-extensions of $k$ an equivalence relation. For technical reasons the trivial extension is contained in the next definition.

$\mathcal{M}_K := \{M/k \mid \text{Gal}(M/k) \leq C_\ell\}/\sim$,

where $M_1 \sim M_2$ if and only if $LM_1 = LM_2$. We see that $\sim$ is only depending on the maximal $\ell$-elementary abelian subextension of $L/k$. For $M_1 \leq L$ we get that $M_1$ is in the trivial class. Let $M_1, M_2$ be not in the trivial class. Then $M_1 \sim M_2$ if and only if $M_1 M_2 \cap L \neq k$.

Since $L/k$ contains only finitely many $C_\ell$-extensions, we get:

Theorem 4.8. Let $K/k$ be a normal extension of number fields with $\text{Gal}(K/k) = H$. Denote by $L/K$ a solution field of our embedding problem (4). We define

$\psi : \{\tilde{L}/K \mid \text{\tilde{L} solution field}\} \to \mathcal{M}_K, \tilde{L} \mapsto [M]$,
where $M/k$ is a cyclic extension with $LM = L\tilde{L}$. Then we get:

(i) $\psi$ is a mapping.

(ii) The trivial class $[M]$ with $M \leq L$ has exactly one preimage. All other classes have exactly $\ell - 1$ preimages.

(iii) Denote by $r$ the $\ell$–rank of the maximal abelian quotient of $G$. Then the trivial class contains exactly $\frac{\ell r - 1}{\ell - 1} + 1$ elements. All other classes have exactly $\ell r$ elements.

Proof. Using Theorem 4.7 and the preceding discussion every solution $\tilde{L}$ corresponds to exactly one class in $M_K$. This shows that $\psi$ is a mapping. Furthermore, only the special solution $L$ corresponds to the trivial class. Using Theorem 4.7 we see that $\ell - 1$ solutions correspond to a non-trivial class. The extension $K/k$ has exactly $\frac{\ell r - 1}{\ell - 1}$ subfields with Galois group $C_\ell$ over $k$. Together with the trivial extension $k$ these fields are the trivial class. For a non-trivial class with representative $M$ we get that $LM$ has $\frac{\ell r + 1}{\ell - 1} - 1$ intermediate fields with Galois group $C_\ell$ over $k$. Exactly $\frac{\ell r - 1}{\ell - 1} - 1$ of those fields are contained in $L$. Therefore we get

\[
\frac{\ell r^+ + 1}{\ell - 1} - 1 = \frac{\ell r - 1}{\ell - 1} - 1 = = \ell r
\]

fields in the equivalence class of $M$. $\square$

Using Theorem 4.8 we parameterize all solutions of a central embedding problem with cyclic kernel of order $\ell$ via cyclic extensions of $k$. In the following we have to solve the following two problems:

(i) How do we choose the special solution $L$?

(ii) How can we compute the discriminant $d_{L/k}$ from $L$ and $M$?

5. Nilpotent groups

5.1. Reduction to $\ell$-groups. Let $G \leq S_n$ be a transitive nilpotent group. It is well known that $G$ is a direct product of its Sylow $\ell$-subgroups. If we consider $G$ as a permutation group, we can prove (e.g. see [10, Lemma 3.1]) that $G$ is a natural direct product of its Sylow $\ell$-subgroups, where the action as permutation groups is given by the action on the blocks.

Lemma 5.1. Let $G_1 \leq S_{n_1}$ and $G_2 \leq S_{n_2}$ be transitive nilpotent groups which are of coprime order and assume $n_1, n_2 > 1$. Define the natural direct product $G = G_1 \times G_2 \leq S_{n_1 n_2}$. Then $a(G) = \max(a(G_1)/n_2, a(G_2)/n_1)$ and the two numbers in the maximum are different.

Proof. The equality is proved in [10, Lemma 4.1]. Suppose that the two numbers are equal. Using $a(G_i)^{-1} = \text{ind}(G_i)$ we get $n_1 a(G_1) = n_2 a(G_2)$ which is equivalent to

\[ n_1 \text{ind}(G_2) = n_2 \text{ind}(G_1). \]

Since $\gcd(n_1, n_2) = 1$ we get that $n_1 \mid \text{ind}(G_1)$, but by definition we have $1 \leq \text{ind}(G_1) < n_1$, since $G_1$ is not the trivial group. This is a contradiction. $\square$

Putting these results together we get the following proposition.
Proposition 5.2. A transitive nilpotent permutation group \( G \leq S_n \) is permutation isomorphic to the natural direct product of transitive permutation groups \( G_\ell \leq S_{n_\ell} \),
\[
G \simeq \prod_\ell G_\ell \text{ with } n = \prod_\ell n_\ell,
\]
where the \( G_\ell \) are isomorphic to the Sylow \( \ell \)-subgroups of \( G \) and \( n_\ell \) is the maximal \( \ell \)-power dividing \( n \). Furthermore, we have that
\[
a_G = \max(\nu a(G_\ell)/n_\ell \mid \ell \in \mathbb{P}).
\]
The maximum number \( \nu a(G_\ell)/n_\ell \) is attained exactly once.

Proof. This is the content of [10, Lemma 3.1] and the extension of Lemma 5.1 to more than two factors. 

Corollary 5.3. Let \( G \leq S_n \) be a transitive nilpotent group. Then all elements of \( G \) of minimal index have the same order.

Proof. Using Proposition 5.2 we see that all elements of minimal index lie in the same Sylow \( \ell \)-subgroup for some \( \ell \in \mathbb{P} \). An element of minimal index is certainly of prime order, since otherwise a suitable power has more orbits. Therefore all these elements have order \( \ell \). 

5.2. The general case. Let \( G \) be a finite nilpotent group and denote by \( E \) the trivial group. We choose a refinement of an upper central series of \( G \) in a way that each quotient is of prime order. We remark that the refinement is not unique and for the following parts there might be good or bad choices to do the refinement.

Therefore we find groups
\[
E = G_r < G_{r-1} < \ldots < G_i < G_{i-1} < \ldots < G_1 < G_0 = G.
\]

We remark that all \( G_i \) are normal subgroups of \( G \), all quotients \( G_{i-1}/G_i \) are of prime order, and \( G_{i-1}/G_i \) lies in the center of \( G/G_i \) for all \( 1 \leq i \leq r \). Suppose we have an extension \( K/k \) with Galois group \( G \). Then we get a tower of fields \( k = K_0 < \ldots < K_r = K \) such that \( \text{Gal}(K/K_i) = G_i \). Let \( p \) be a prime ideal of \( \mathcal{O}_k \) and \( \mathfrak{P} \) be a prime ideal of \( \mathcal{O}_K \) lying above \( p \). Denote by \( G_\mathfrak{P} \) the inertia group of \( \mathfrak{P} \). We remark that the inertia groups of all prime ideals lying over \( p \) are conjugate.

Now we want to consider the situation that \( p \) firstly becomes ramified in \( K_i \), i.e. \( p \) is ramified in \( K_i \) but not in \( K_{i-1} \). We use the following easy lemma.

Lemma 5.4. The prime ideal \( p \) is unramified in \( K_i \) if and only if \( G_\mathfrak{P} \leq G_i \).

Proof. By Hilbert’s ramification theory, the fixed field \( L \) under \( G_\mathfrak{P} \) is the largest subfield of \( K \), for which \( L \cap \mathfrak{P} \) is unramified over \( p \). Since \( K_i/k \) is normal, \( p \) is unramified when one of the prime ideals lying over \( p \) is unramified. Therefore \( p \) is unramified in \( K_i \) if and only if \( K_i \) is a subfield of \( L \) which is equivalent to \( G_\mathfrak{P} \leq G_i \). 

□
Now we see that $p$ firstly becomes ramified in $K_i$ if and only if $G_p \leq G_{i-1}$ and $G_p \not\subseteq G_i$. This condition becomes much easier in the tamely ramified situation.

**Lemma 5.5.** Let $p$ be a prime ideal of $\mathcal{O}_k$ which is at most tamely ramified in $K$. Denote by $\sigma$ a generator of the cyclic group $G_p$. Then $i$ is minimal such that $p$ ramifies in $K_i$ if and only if $\sigma \in G_{i-1} \setminus G_i$.

**Proof.** If $p$ is not wildly ramified, we know that $G_p = \langle \sigma \rangle$ is cyclic. Therefore $G_p \leq G_i$ is equivalent to $\sigma \in G_i$. \hfill $\square$

If the prime ideal $p$ is at most tamely ramified, we can use the index to describe the $p$-part of the discriminant (see also [13, Section 7]).

**Lemma 5.6.** Let $K/k$ be an extension of number fields with $\text{Gal}(K/k) = G \leq S_n$ and $p \in \mathbb{P}(k)$ be a tamely ramified prime ideal. Denote by $\sigma$ a generator of the (cyclic) inertia group (of the normal closure of $K/k$) and consider $\sigma$ as an element of the permutation group $G$. Then $v_p(\theta_{K/k}) = \text{ind}(\sigma)$.

**Proof.** The proof follows from Dedekind’s different theorem and results about the decomposition of prime ideals in intermediate fields, see [11, Section 6.3]. \hfill $\square$

Let

$$A_i := G_{i-1} \setminus G_i \text{ for } 1 \leq i \leq r, a_i := \min\{\text{ind}(g) \mid g \in A_i\} \text{ and } \ell_i := \frac{|G_{i-1}|}{|G_i|}.$$  

Since the inertia generator must be one of the elements of $A_i$ we get that $v_p(d_{K/k}) \geq a_i$. Define $a_i \subseteq \mathcal{O}_k$ to be the product of the ideals which become firstly ramified in $K_i$. In this way we associate to $K/k$ the tuple of ideals $(a_1, \ldots, a_r)$. Note that all $a_i$ are squarefree and pairwise coprime. Furthermore all prime ideals $p$ dividing $a_i$ are contained in the set $B_i$ of Lemma 2.3. For the discriminant we get the estimate:

$$N(d_{K/k}) \geq N(a_1)^{a_1} \cdots N(a_r)^{a_r}.$$  

In order to obtain our wanted upper bound we have to compute how many fields can be associated to the same tuple of ideals. We remark that from the definition of the tuple we have that the ideals are pairwise coprime. Denote by $I_k$ the group of ideals of $\mathcal{O}_k$ and define the following map using the above notation:

$$\Phi : \{K/k \mid \text{Gal}(K/k) = G\} \to I_k.$$  

As before $\omega(a)$ denotes the number of different prime ideal factors of $a$.

**Theorem 5.7.** Let $k$ be a number field and $G \leq S_n$ be a transitive nilpotent group. We choose the $G_i$ given in (5). Define

$$b_i := \omega(\prod_{j=1}^{i-1} a_j) + c(k, \ell_i),$$

where $c(k, \ell_i)$ defined in Theorem 3.2 only depends on $[k : \mathbb{Q}]$ and $\text{rk}_e(\text{Cl}_k)$. Then, all fibers of the map $\Phi$ described above are finite of size at most

$$b_1^{r_1} \cdots b_r^{r_r} (\ell_1 - 1)^{\omega(a_1)} \cdots (\ell_r - 1)^{\omega(a_r)}.$$  

**Proof.** In Theorem 4.8 we have proved that all solutions of a central embedding problem with kernel $C_\ell$ can be associated to cyclic extensions of order $\ell$ of $k$. In order to get an upper bound we have to count these cyclic extensions which are
at most ramified in the ideals \( \mathfrak{a}_i \). Suppose we are in the \( i \)-th step. Then we have to compute the number of \( C_{\ell_i} \)-extensions which are at most ramified in the ideals dividing \( \mathfrak{a}_1 \cdots \mathfrak{a}_i \) and which are ramified in all ideals dividing \( \mathfrak{a}_i \). Define 
\[
S := \{ \mathfrak{p} \in \mathcal{P}(k) : \mathfrak{p} \mid \mathfrak{a}_1 \cdots \mathfrak{a}_{i-1} \} \quad \text{and} \quad T := \{ \mathfrak{p} \in \mathcal{P}(k) : \mathfrak{p} \mid \mathfrak{a}_i \}
\]
and apply Theorem 5.2. Then we get \( \ell_i^b (\ell_i - 1)^{\omega(\mathfrak{a}_i)} \) for the \( i \)-th step.

For the final step note that \( A_i, a_i, \) and \( \ell_i \) are defined in (5).

**Theorem 5.8.** Let \( G \leq S_n \) be a transitive nilpotent group and \( k \) be a number field. Then there exist constants \( d(k, G), b(k, G), c(k, G), c_c(k) > 0 \) such that for all \( x > 1 \):

\[
Z(k, G ; x) \leq c(k, G) x^{a(G)} \log(x)^{d(k, G) - 1}.
\]

**Proof.** Using Theorem 5.7 and the discriminant estimate we get:

\[
Z(k, G ; x) \leq \sum_{N(\mathfrak{a}_1) \cdots N(\mathfrak{a}_r) \leq x} \ell_1^{a_1} \cdots \ell_r^{a_r} (\ell_1 - 1)^{\omega(\mathfrak{a}_1)} \cdots (\ell_r - 1)^{\omega(\mathfrak{a}_r)}
\]

\[
\leq \prod_{i=1}^r \ell_r^{c(k, \ell_i)} \sum_{N(\mathfrak{a}_1) \cdots N(\mathfrak{a}_r) \leq x} m_1^{\omega(\mathfrak{a}_1)} \cdots m_r^{\omega(\mathfrak{a}_r)},
\]

where \( m_r = (\ell_r - 1), m_{r-1} = \ell_r(\ell_{r-1} - 1), \ldots, m_1 = \ell_r \cdots \ell_2(\ell_1 - 1) \). Using Lemma 2.3 we get the desired bound since \( a(G)^{-1} \) is the minimal index which occurs in the group \( G \). Note that \( \mathfrak{p} \mid \mathfrak{a}_i \) implies that \( \mathfrak{p} \in B_i \) in the notation of Lemma 2.3.

Now we compute \( d(k, G) \) which furthermore depends on our chosen groups \( G_i \) in (7). Let \( \ell \) be the order of elements of smallest index, see Corollary 5.3. Using \( a := \min(a_1, \ldots, a_r) \) and \( n_\ell := [k(\zeta_\ell) : k] \) we define

\[
d(G) := \sum_{i : a_i = a} m_i \quad \text{and} \quad d(k, G) := d(G)/n_\ell.
\]

**Remark 5.9.** In the situation of Theorem 5.8 we have for all valid choices in (5):

\[
\# \{ g \in G \mid \text{ind}(g) = \text{ind}(G) \} \leq d(G) \leq |G| - 1.
\]

**Proof.** Using (5) and (9) we see that

\[
G \setminus \{ 1 \} = A_1 \cup \ldots \cup A_r \quad \text{and} \quad m_i = |A_i| = (\ell_i - 1) \prod_{j=i+1}^r \ell_j.
\]

Inserting this in (7) we get the upper bound

\[
d(G) = \sum_{i : a_i = \text{ind}(G)} m_i = \sum_{i : a_i = \text{ind}(G)} |A_i| \leq |G| - 1,
\]

since 1 is not contained in any \( A_i \).

We remark that the constant \( b(k, G) \) of Malle is trivially bounded above by the number of elements with minimal index.

As already mentioned the proven upper bound for \( d(k, G) \) is depending on our choice in (5). In the following we would like to find an optimal choice. As before let \( \ell \) be the order of an element of smallest index in \( G \). In a first step we choose our series of groups \( E = G_r < G_{r-1} < \ldots < G_0 = G \) in a way such that there exists an \( i \) with \( G_i \) is an \( \ell \)-group and \( G/G_i \) is coprime to \( \ell \). This means that \( \text{Gal}(K_r/K_i) \) is an \( \ell \)-group and the minimal index occurs for \( j \) with \( j \geq i \). From this we see that
we can prove the same upper bound for \(d(k,G)\) as we can do for the corresponding Sylow \(\ell\)-subgroup. The \(a(G)\)-constant is certainly independent of the choice of \(G\).

In order to study the values \(d(k,G)\) we restrict to \(\ell\)-groups \(G\). The following examples show that different choices lead to different results. We use equation (6).

**Example 5.10.** Let \(G = \langle a,b \mid a^4 = b^2 = 1, ab = ba \rangle \cong C_4 \times C_2 \leq S_8\). We define \(E = G_3 < G_2 = \langle a^2 \rangle < G_1 = \langle a^2, b \rangle < G_0 = G\). Then \(A_i := G_{i-1} \setminus G_i\) for \(1 \leq i \leq 3\) and \(a_1 := \min_{g \in A_i} \text{ind}(g)\). All elements in \(A_1\) have order 4 and therefore \(\text{ind}(g) = 6\) for all \(g \in A_1\). All elements in \(A_2\) and \(A_3\) have order 2 and therefore \(\text{ind}(g) = 4\) for all \(g \in A_2\) and \(A_3\) have order 2 and their index is 4. Now \(d(k,G) = \#(G) = |A_2| + |A_3| = 2 + 1 = 3 = b(k,G)\) for all number fields \(k\).

If we choose \(E = \langle a^2 \rangle < \langle a \rangle < G\), we get that the corresponding set \(A_1\) contains elements of order 4 and of order 2 and therefore \(a_1 = 4\). Furthermore, we get \(a_2 = 6\) and \(a_3 = 4\). Therefore \(d(k,G) = d(G) = |A_1| + |A_3| = 4 + 1 = 5\).

For an abelian \(\ell\)-group it is clear how to minimize \(d(G)\) and \(d(k,G)\). A trivial lower bound for \(d(G)\) is the number of elements of order \(\ell\) since the minimal index is always attained at an element of prime order. In a transitive abelian group the index of an element is only depending on the order of the element.

**Lemma 5.11.** Let \(G\) be an abelian \(\ell\)-group of order \(\ell^r\) and \(\ell\)-rank \(s\). If we choose the central series in a way such that \(G_{r-s} \cong C_{\ell^s}^s\) then we get that \(d(G) = \ell^s - 1\) and \(d(k,G) = b(k,G)\).

**Proof.** Denote by \(a := \text{ind}(G)\). The sets \(A_1, \ldots, A_{r-s}\) do not contain elements of order \(\ell\) and therefore \(a_i > a\) for \(1 \leq i \leq r-s\). The sets \(A_{r-s+1}, \ldots, A_r\) only contain elements of order \(\ell\) and we get that \(\sum_{i=r-s+1}^{r} |A_i| = |G_{r-s}| - 1 = \ell^s - 1\). Now we have \(d(k,G) := d(G) / n_{\ell}\), where \(n_{\ell} := [k(\zeta_{\ell^s}) : k]\). This shows \(d(k,G) = b(k,G)\). \(\square\)

We remark that Theorem 5.8 proves the correct upper bound including log-factor for abelian groups \(G\). We have seen that our constant \(d(G)\) is bounded below by the number of elements of minimal index. For non-abelian groups Malle conjectures a dependency on conjugacy classes of minimal index. Usually a conjugacy class contains more than one element in the non-abelian case. Therefore we cannot expect to get the expected upper bound for non-abelian nilpotent groups. Sometimes we are lucky.

Let us study the non-abelian groups of order 8. Both groups \(G\) have a center \(Z(G)\) of order 2 and therefore the upper central series is given by \(E < Z(G) < G\), where \(G/Z(G)\) is a group of order 4 and we have a choice for the refinement of the upper central series. Since the center contains only one element of order 2, we get \(A_3 = Z(G) \setminus \{1\}\) and therefore \(a_3 = 4\) in all cases. In the case of the quaternion group \(Q_8\) all elements not contained in the center have order 4 and index 6. Independent of the refinement we get \(a_1 = a_2 = 6\) for \(G = Q_8\). Let us consider the dihedral group on 8 points. This group has exactly one cyclic subgroup of order 4. If we choose this group for \(G_1\), we get that \(A_2 = G_1 \setminus Z(G)\) contains two elements of order 4. The set \(A_1 = G \setminus G_1\) contains the remaining elements, all of them have order 2. Altogether, we get \(a_1 = 4\) and \(a_2 = 6\). We proved the correctness of the following examples. If we choose a Klein four group for \(G_1\), then we get \(a_1 = 4 = a_2\). Here we have the problem that \(A_1\) contains elements of order 4 and of order 2, which gives worse exponents for our bound.
Example 5.12.  
(i) Let \( G = Q_8 \). Then we get \( Z(k, G; x) \leq O(x^{a(G)}) \), which is as conjectured. Note that \( a_1 = a_2 = 6 \) and \( a_3 = 4 \).

(ii) Let \( G = D_4 \leq S_4 \). Then we get \( Z(k, G; x) \leq O(x^{a(G)} \log(x)^4) \). Malle predicts exponent 2 instead of 4. Note that \( a_1 = a_3 = 4 \) and \( a_2 = 6 \). The difference between 4 and 2 can be explained by the fact that there are 5 elements of order 2 which lie in 3 conjugacy classes.

For \( Q_8 \) we get a sharp bound. For \( D_4 \leq S_4 \) the problem is that we count many \( C_2 \times C_2 \)-extensions, for which the embedding problem into \( D_4 \) is not solvable.

Note that the bound for \( D_4 \) we got in the last example is optimal for our method. We get that \(|A_4| + |A_3| = 4 + 1 = 5\). Note that \( D_4 \) contains 5 elements of order 2, so we cannot do better with our method. Other choices of refinements would lead to a log-power of \( 7 - 1 \).

When we consider the dihedral group \( D_4 \leq S_4 \) as permutation group on 4 points, the non-trivial central element has index 2 and therefore \( a_3 = 2 \). If we choose the subgroup of order 4 in a way that it contains the central element and the transpositions, we get \( a_2 = 1 \) and \( a_1 = 2 \). Therefore we get \( d(G) = 2 \) and we get \( Z(k, D_4; x) = O(x \log(x)) \) which is one log-factor more than expected. When we choose other refinements, we get \( a_1 = 1 \) and \( d(G) = 4 \). We remark that it is known \[2, 4\] that \( Z(k, D_4; x) \sim cx \).

What is special about \( G = Q_8 \)? The important property is that all elements of minimal index lie in the center of the group. We remark that this is trivially true for abelian groups. Elements in the center of a transitive group are always given in regular representation and therefore their index is only depending on their order. Similar to the abelian case we can prove.

**Lemma 5.13.** Let \( G \leq S_n \) be a transitive nilpotent group such that all elements of minimal index lie in the center of \( G \). Then the number of those elements equals \( \ell^n - 1 \) for a prime number \( \ell \) and \( s \in \mathbb{N} \). If we choose the central series in a way such that one \( G_i \cong C_\ell^s \) then we get that \( d(G) = \ell^s - 1 \) and \( d(k, G) = b(k, G) \).

**Proof.** Note that all elements of minimal index have prime order \( \ell \). Since all these elements lie in the center we can choose one \( G_i \) to exactly contain those elements. We proceed as in the proof of Lemma 5.11. For the final equality note that the size of a conjugacy class of an element in the center is 1. \( \square \)

We remark that a converse of Lemma 5.13 is also true. If at least one element of minimal order does not lie in the center, then the conjugacy class of this element contains more than one element. Since \( d(G) = d(k(\zeta_\ell), G) \) is bounded below by the number of elements of minimal index, we see that \( b(k(\zeta_\ell), G) < d(k(\zeta_\ell), G) \), since \( b(k(\zeta_\ell), G) \) equals the number of conjugacy classes of minimal index.

Let us define the generalized quaternion groups of order \( 4n \) for \( n = 2^k \) for all \( k \geq 1 \):
\[
Q_{4n} := \langle x, y \mid x^{2n} = y^4 = 1, x^n = y^2, y^{-1}xy = x^{-1} \rangle.
\]

Note that \( Q_{4\cdot2} \) is the usual quaternion group and that those groups have only one transitive representation, which is the regular one acting on 4n points. These groups have only one element of order 2, which therefore lies in the center. Lemma 5.13 yields for \( n = 2^k \) with \( k \geq 1 \):
\[
Z(k, Q_{4n}; x) = O(x^{a(Q_{4n})}),
\]
like expected in Conjecture 1.3.
Using Corollary 5.3 we can describe more cases, where our bound \( d(k, G) = b(k, G) \). Let \( \ell \) be the critical prime and \( G_\ell \) be an \( \ell \)-group which fulfills the assumption of Lemma 5.13. Then all direct products of the form \( G_\ell \times H \), where \( \ell \nmid |H| \) and \( \ell \) is still the order of elements of smallest index, will fulfill the assumption of Lemma 5.13. Note that we get conjectured upper bound in all cases.

On the other hand the dihedral group has elements of smallest index not lying in the center, which cannot yield optimal bounds using our method. This is independent on the chosen permutation representation.

ACKNOWLEDGMENT

The author would like to thank Brandon Alberts and Gunter Malle for suggestions on an earlier draft.

REFERENCES

[1] Brandon Alberts. The weak form of Malle’s conjecture and solvable groups. Res. Number Theory, 6(1):Art. 10, 23, 2020.
[2] Andrew Marc Baily. On the density of discriminants of quartic fields. J. Reine Angew. Math., 315:190–210, 1980.
[3] Karim Belabas. Paramétriezation de structures algébriques et densité de discriminants (d’après Bhargava). Number 299, pages Exp. No. 935, ix, 267–299, 2005. Séminaire Bourbaki. Vol. 2003/2004.
[4] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Enumerating quartic dihedral extensions of \( \mathbb{Q} \). Compositio Math., 133(1):65–93, 2002.
[5] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. A survey of discriminant counting. In Algorithmic number theory (Sydney, 2002), volume 2369 of Lecture Notes in Comput. Sci., pages 80–94. Springer, Berlin, 2002.
[6] Hubert Delange. Généralisation du théorème de Ikehara. Ann. Sci. Ecole Norm. Sup. (3), 71:213–242, 1954.
[7] Marcus du Sautoy and Luke Woodward. Zeta functions of groups and rings, volume 1925 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, 2008.
[8] Jürgen Klüners. A counterexample to Malle’s conjecture on the asymptotics of discriminants. C. R. Math. Acad. Sci. Paris, 340(6):411–414, 2005.
[9] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. J. Reine Angew. Math., 572:1–26, 2004.
[10] Jürgen Klüners and Jiuya Wang. \( \ell \)-torsion bounds for the class group of number fields with an \( \ell \)-group as Galois group, 2020. arXiv:2003.12161.
[11] Helmut Koch. Number theory, volume 24 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2000.
[12] Serge Lang. Algebraic Number Theory. Springer, Berlin-Heidelberg-New York, 1986.
[13] Gunter Malle. On the distribution of Galois groups. J. Numb. Theory, 92:315–322, 2002.
[14] Gunter Malle. On the distribution of Galois groups II. Exp. Math., 13:129–135, 2004.
[15] Gunter Malle and B. Heinrich Matzat. Inverse Galois theory. Springer Monographs in Mathematics. Springer, Berlin, 2018.
[16] Władysław Narkiewicz. Number Theory. World Scientific, 1983.
[17] Władysław Narkiewicz. Elementary and Analytic Theory of Algebraic Numbers. Springer, 2004.
[18] Melanie Matchett Wood. Asymptotics for number fields and class groups. In Directions in number theory, volume 3 of Assoc. Women Math. Ser., pages 291–339. Springer, [Cham], 2016.
[19] David Wright. Distribution of discriminants of abelian extensions. Proc. London Math. Soc., 68:17–50, 1989.

University Paderborn, Department of Mathematics, Warburger Str. 100, 33098 Paderborn, Germany

Email address: klueners@math.uni-paderborn.de