Bull. Aust. Math. Soc. **103** (2021), 428–437
doi:10.1017/S0004972720001136

ON UNRAMIFIED SOLVABLE EXTENSIONS OF SMALL NUMBER FIELDS

JOACHIM KÖNIG

(Received 19 July 2020; accepted 20 August 2020; first published online 9 November 2020)

Abstract

We investigate unramified extensions of number fields with prescribed solvable Galois group G and certain extra conditions. In particular, we are interested in the minimal degree of a number field K, Galois over $\mathbb{Q}$, such that K possesses an unramified G-extension. We improve the best known bounds for the degree of such number fields K for certain classes of solvable groups, in particular for nilpotent groups.

2020 *Mathematics subject classification*: primary 11R32; secondary 12F12.

Keywords and phrases: Galois theory, nilpotent group, solvable group, unramified extension.

1. Introduction

A problem of widespread interest in algebraic number theory is the construction of unramified extensions L/K of number fields with prescribed Galois group. It is well known, for example, as a direct consequence of results on S_n-extensions with squarefree discriminant (see [11, 13]), that such extensions exist for any given group G. A more interesting question is, what is the smallest degree of such a number field K over $\mathbb{Q}$, possibly with additional requirements on K? In the following, we denote by $d(\mathbb{Q}, G)$ the smallest integer d such that there exists a number field K of degree d over $\mathbb{Q}$ which possesses an unramified Galois extension with group G; and by $d'(\mathbb{Q}, G)$ the smallest integer d' as above such that $K/\mathbb{Q}$ is additionally Galois. It is commonly conjectured that every finite group occurs as the Galois group of an unramified Galois extension L/K, where K is a quadratic number field, that is, $d(\mathbb{Q}, G) = d'(\mathbb{Q}, G) = 2$. However, this is a difficult question (in class field theory) even for the case of abelian groups. Detailed heuristics predicting the distribution of such extensions, generalising the Cohen–Lenstra heuristics, have been developed by Wood [12].

For solvable G, it is known from work of Kim building on Shafarevich's method [5, 6] that $d'(\mathbb{Q}, G) \le \exp(G)$, where the *exponent* $\exp(G)$ of G is defined as the least common multiple of all element orders in G. Previously, Nomura [10] had given the bound $d'(\mathbb{Q}, G) \le p \cdot |\Phi(G)|$ for p-groups G with $\Phi(G)$ the Frattini subgroup of G. As noted in [5, Remark 5.2], this bound is always $\ge \exp(G)$.

We additionally define $e(\mathbb{Q}, G)$ as the minimal number e such that $\mathbb{Q}$ admits a tamely ramified G-extension all of whose ramification indices divide e. The relevance of this definition for the original question on unramified G-extensions comes from Abhyankar's lemma, which shows immediately that $d(\mathbb{Q}, G) \leq e(\mathbb{Q}, G)$ [8, Lemma 2.1].

For a finite group G, define the *generator exponent* of G to be

$$\mathrm{ge}(G) := \min_S \mathrm{lcm}\{\mathrm{ord}(x) \mid x \in S\},$$

where S ranges over all generating subsets of G. It is easy to see that $e(\mathbb{Q}, G) \geq \mathrm{ge}(G)$ for all finite groups G. This is because the set of all inertia groups of a (tamely ramified) G-extension has to generate G. The converse is open.

QUESTION 1.1. Let G be a finite group. Does $e(\mathbb{Q}, G)$ equal $\mathrm{ge}(G)$?

Note that while bounds on $e(\mathbb{Q}, G)$ do not automatically yield bounds on $d'(\mathbb{Q}, G)$ in general, they do as soon as the implied tamely ramified G-extensions satisfy certain additional local conditions (see Lemma 2.7). We therefore connect Question 1.1 with the following, which is more accessible than the stronger conjecture $d'(\mathbb{Q}, G) = 2$.

QUESTION 1.2. Let G be a finite group. Is it true that $d'(\mathbb{Q}, G) \leq \mathrm{ge}(G)$?

In an earlier paper [8], Question 1.1 was investigated using function field methods, with a focus on nonsolvable groups, in particular reaching the best possible bound $d(\mathbb{Q}, G) = e(\mathbb{Q}, G) = \mathrm{ge}(G) = 2$ for several new groups.

Here, we instead focus on solvable groups. For certain classes of groups, in particular for so-called regular p-groups, $\mathrm{ge}(G) = \exp(G)$, meaning that already the aforementioned results [5, 6] yield a positive answer to Questions 1.1 and 1.2 for such groups. In particular, since it is known that all p-groups of nilpotency class $\leq p - 1$ are regular, it follows that $d'(\mathbb{Q}, G) \leq e(\mathbb{Q}, G) = \mathrm{ge}(G)$ for those groups.

The main goal of this note is to extend this observation beyond the special case $\exp(G) = \mathrm{ge}(G)$. In particular, we prove the following result.

THEOREM 1.3. *Let G be a nilpotent group of nilpotency class $\leq p$, where p is the smallest prime divisor of $|G|$. Then $d'(\mathbb{Q}, G) \leq e(\mathbb{Q}, G) = \mathrm{ge}(G)$. More precisely, there exist infinitely many cyclic number fields K of degree $\leq \mathrm{ge}(G)$ such that K possesses an unramified G-extension.*

Note that groups of nilpotency class p include many groups for which $\mathrm{ge}(G)$ is strictly smaller than $\exp(G)$, making Theorem 1.3 an improvement over previously available bounds. An easy example (but far from the only one) is the wreath product $G = C_p \wr C_p$ $(= (C_p)^p \rtimes C_p)$, which has nilpotency class p, generator exponent p and exponent p^2. (Indeed, the nilpotency class of a p-group of order p^k $(k \geq 2)$ is always bounded from above by $k - 1$ and, in the case of nilpotency class $< p$, the discrepancy between exponent and generator exponent would be impossible; see Section 2.)

Before proving Theorem 1.3 in Section 4.2, we discuss some methods allowing generalisations in Section 4.1, in particular providing positive answers to Questions 1.1 and 1.2 for certain classes of p-groups of arbitrarily high nilpotency class.

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

2. Some prerequisites

We recall some standard notions and elementary results, mostly from group theory, which will be used later. The first is the notion of a regular p-group. One of several equivalent definitions is the following (see [4, Ch. III.10]).

DEFINITION 2.1 (Regular p-group). A p-group G is called regular if for every $a, b \in G$ there exists c in the derived subgroup of $\langle a, b\rangle \leq G$ such that $a^p b^p = (ab)^p c^p$.

We will only use the following two consequences of regularity (see Corollary 4.13 and Theorem 4.26 in [3]).

PROPOSITION 2.2. *Every p-group of nilpotency class $< p$ is regular.*

PROPOSITION 2.3. *In a regular p-group G, the order of a product of any finitely many elements cannot exceed the orders of all these elements. In particular,* $\exp(G) = \mathrm{ge}(G)$.

We will also make use of higher commutators and their role in calculating powers of products of group elements.

DEFINITION 2.4. Let G be a finite group and $a, b \in G$. Denote by $[a, b] := a^{-1}b^{-1}ab$ the commutator of a and b. Iteratively, a *commutator of weight i* in a and b is defined as follows.

- The commutators of weight 1 are a and b.
- The commutators of weight $i \geq 2$ are $[x, y]$, where x and y are commutators of weights j and $i - j$ for some $j \in \{1, \dots, i-1\}$.

THEOREM 2.5 (Hall [3, Theorem 3.1]). *Let G be a finite group and $a, b \in G$. For $i \in \mathbb{N}$, denote by $R_{i,j}$ the iterated commutators of weight i in a and b ($j \in \{1, \dots, n_i\}$ for some $n_i \in \mathbb{N}$), in some prescribed order. Then there exist polynomial functions $f_{i,j}$ such that, for all $n \in \mathbb{N}$,*

$$(ab)^n = a^n b^n \prod_{i \geq 2} \prod_{j=1}^{n_i} R_{i,j}^{f_{i,j}(n)}.$$

Note. The product over $i \geq 2$ is *a priori* infinite and should be interpreted as '$\prod_{2 \leq i < N}(\cdots)$ times an element of the group generated by weight-N commutators' for arbitrarily chosen $N \in \mathbb{N}$. In groups where all suitably high commutators vanish (such as nilpotent groups), there is no ambiguity in the notation. More precisely, $f_{i,j}$ is an integer linear combination of the polynomials

$$\binom{X}{1}, \dots, \binom{X}{i}, \quad \text{where } \binom{X}{d} := \frac{X(X-1)\cdots(X-d+1)}{d!}.$$

We set $G_1 := G$ and iteratively $G_d := [G, G_{d-1}]$ for every $d \geq 2$. In particular, $G_2 = [G, G] = G'$ is the commutator subgroup of G and $G = G_1 > G_2 > \cdots$ is the *lower central series* of G. In particular, if G is nilpotent of class c, then $G_{c+1} = \{1\}$. Then [3, Theorems 2.51 and 2.53] give the following lemma.

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

LEMMA 2.6. $[G_i, G_j] \leq G_{i+j}$ *for all* $i, j \geq 1$. *In particular, every weight-i commutator of G is contained in* G_i.

Finally, we include a number-theoretic lemma which ensures that we have $d'(\mathbb{Q}, G) \leq e(\mathbb{Q}, G)$ under certain extra conditions.

LEMMA 2.7 [7, Lemma 4.5]. *Let G be the Galois group of a tamely ramified extension* $F/\mathbb{Q}$ *all of whose decomposition groups are abelian. Then G occurs as the Galois group of an unramified extension of some cyclic number field L. Moreover, let m denote the least common multiple of all ramification indices at ramified primes in* $F/\mathbb{Q}$. *Then one may choose L such that* $[L : \mathbb{Q}] \leq m$.

3. Shafarevich's method and the constant $r(G)$

The following deep result, due to Shafarevich, solves the inverse Galois problem for solvable groups.

THEOREM 3.1 (Shafarevich [9, Ch. IX.6]). *Let G be a finite solvable group and K be a number field. Then there are infinitely many Galois extensions* L/K *with group G fulfilling the following conditions:*

(i) L/K *is tamely ramified;*
(ii) *all decomposition groups at ramified primes in* L/K *are cyclic and equal to the respective inertia groups.*

Since decomposition groups at unramified primes are automatically cyclic, Theorem 3.1 together with Lemma 2.7 immediately regains the bound $d'(\mathbb{Q}, G) \leq \exp(G)$ for all solvable groups G. In order to improve on this bound and move towards the proof of Theorem 1.3, we recall Shafarevich's method in more detail.

Firstly, at the heart of Shafarevich's proof of Theorem 3.1 is a result on solvability of split embedding problems with nilpotent kernel (see [9, Theorem 9.6.7]), which, given a Galois extension L/K with group H, guarantees the existence of an $N \rtimes H$-extension F/K containing L/K such that all ramified primes of L/K split completely in F/L and all ramified primes of F/L have cyclic decomposition groups equal to the respective inertia group in F/K.

Next, given any solvable group G and normal subgroup $N \triangleleft G$, call a proper subgroup $U < G$ a *partial complement* for N if $NU = G$. Note that in this case G necessarily occurs as a quotient of a suitable semidirect product $N \rtimes U$. Partial complements exist for all normal subgroups N not contained in the Frattini subgroup of G [9, Proposition 9.6.8]. In particular, the Fitting subgroup $F(G)$, defined as the (unique) largest nilpotent normal subgroup of G, always has this property [9, Proposition 9.6.9]. Since $|U| < |G|$, Theorem 3.1 is then derived by induction, since Properties (i) and (ii) are preserved under taking quotients.

This motivates the following definition.

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

DEFINITION 3.2. Let G be a solvable group. Set $G_0 := G$. As long as $G_{i-1} \neq \{1\}$, we iteratively define N_i to be a nilpotent normal subgroup of G_{i-1} such that N_i possesses a partial complement G_i in G_{i-1} (that is, $G_i \neq G_{i-1}$ and $N_i G_i = G_{i-1}$). Let s be minimal such that $G_s = \{1\}$. For each $i = 1, \dots, s$, denote by e_i the exponent of the group N_i. Define $r(G) = \min \operatorname{lcm}(e_1, \dots, e_s)$, where the minimum is taken over all series of $(N_i, G_i)_{i=1,\dots,s}$ as above.

Note in particular that $r(G)$ divides $\exp(G)$, as it is the least common multiple of certain element orders of G. For many groups G, $r(G)$ is actually significantly smaller than $\exp(G)$. For example, let $G = C_p \wr (C_p \wr (\cdots \wr C_p)) \cdots)$ be a k-fold iterated wreath product of cyclic groups of order p. Then $\exp(G) = p^k$, whereas $r(G) = p$. To see the latter, simply write $G = (C_p)^n \rtimes H$ with suitable $n \in \mathbb{N}$, set $N_1 := (C_p)^n$, $G_1 := H$ and note that $\exp(N_1) = p$ and G_1 is essentially of the same structure as G, so one can proceed by induction. On the other hand, one always has $r(G) \geq \operatorname{ge}(G)$, since $N_1 \cdots N_r = G$.

The following useful inequality is also straightforward from the definition of $r(G)$.

LEMMA 3.3. *Let G be a p-group, N a normal subgroup of G and U a partial complement of N in G. Then $r(G) \leq \operatorname{lcm}\{\exp(N), r(U)\}$.*

PROOF. Set $N_1 = N$, $G_1 = U$ and continue (N_1, G_1) to a series $((N_i, G_i) \mid i \in \{1, \dots, s\})$ as in Definition 3.2 and such that the series $((N_i, G_i) \mid i \in \{2, \dots, s\})$ inside U reaches the smallest possible value $r(U)$. Set $e_i = \exp(N_i)$ for $i = 1, \dots, s$. We have $r(U) = \operatorname{lcm}(e_2, \dots, e_s)$ and $r(G) \leq \operatorname{lcm}(e_1, \dots, e_s) = \operatorname{lcm}(\exp(N), r(U))$. □

PROPOSITION 3.4. *Let G be a solvable group and k be a number field. Suppose that $((N_i, G_i) \mid i \in \{1, \dots, s\})$ is any series of nilpotent normal subgroups N_i and partial complements G_i as in Definition 3.2, and let $e_i = \exp(N_i)$ for $i = 1, \dots, s$. Then there exist infinitely many tamely ramified Galois extensions F/k with group G such that all ramification indices divide $\operatorname{lcm}(e_1, \dots, e_s)$, and all decomposition groups at ramified primes are cyclic and equal to the inertia groups. Moreover, there exist infinitely many cyclic Galois extensions K/k of degree $[K : k] \leq \operatorname{lcm}(e_1, \dots, e_s)$ such that K possesses an unramified G-extension. In particular, $d'(\mathbb{Q}, G)$ and $e(\mathbb{Q}, G)$ are bounded from above by $r(G)$.*

PROOF. It suffices to prove the first assertion, since the second one follows from Lemma 2.7 and the last one is immediate from the definition of $r(G)$. We proceed by induction over s.

If $s = 1$, then G is nilpotent of exponent e_1 and the assertion is immediate from Theorem 3.1. Now let $s \geq 2$. Then $G = N_1 G_1$ is a quotient of some semidirect product $N_1 \rtimes G_1$. Note that $((N_i, G_i) \mid i \in \{2, \dots, s\})$ is a series as in Definition 3.2 for the group G_1. Thus, we may inductively assume the existence of a G_1-extension F/k yielding the assertion for G_1. By [9, Theorem 9.6.7], there exist infinitely many tamely ramified Galois extensions E/k with group $N_1 \rtimes G_1$ such that all decomposition groups at ramified primes are cyclic, equal to the respective inertia groups, and embed either

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

into $\mathrm{Gal}(F/k)$ or into N_1. Thus, all ramification indices in E/k, and *a fortiori* in its G-subextension, divide $\mathrm{lcm}(e_1, \mathrm{lcm}(e_2, \ldots, e_s))$. This completes the proof. □

4. Groups satisfying $r(G) = \mathrm{ge}(G)$

4.1. Compatibility with taking direct products and wreath products. Proposition 3.4 shows that the Shafarevich method yields the constant $r(G)$, rather than the in general larger $\exp(G)$, as an upper bound for $e(\mathbb{Q}, G)$ and $d'(\mathbb{Q}, G)$. However, the true value of $r(G)$ is usually hard to determine directly from its definition. We therefore aim at exhibiting examples in which $r(G) = \mathrm{ge}(G)$, thus providing a positive answer to Questions 1.1 and 1.2 for G. We begin with a simple, but useful, observation.

LEMMA 4.1. *Let $G = G_1 \times \cdots \times G_n$ be solvable and assume that $\mathrm{ge}(G_i) = r(G_i)$ for all $i = 1, \ldots, n$. Then $\mathrm{ge}(G) = r(G)$.*

PROOF. Since each generating set of G projects to a generating set of each G_i, and conversely the union of generating sets for each G_i forms a generating set for G, one has $\mathrm{ge}(G) = \mathrm{lcm}(\mathrm{ge}(G_1), \ldots, \mathrm{ge}(G_n))$.

For $r(G)$, let $((N_{ij}, G_{ij}) \mid i \in \{1, \ldots, s\})$ be a series of normal subgroups and partial complements inside G_j as in Definition 3.2 (assumed of the same length s independent of j, via adding trivial subgroups if necessary), reaching the minimum value $r(G_j)$ for $j = 1, \ldots, n$. Then $((\prod_{j=1}^n N_{ij}, \prod_{j=1}^n G_{ij}) \mid i \in \{1, \ldots, s\})$ reaches the value

$$\mathrm{lcm}\Big(\exp\Big(\prod_{j=1}^{n} N_{1j}\Big), \ldots, \exp\Big(\prod_{j=1}^{n} N_{sj}\Big)\Big)$$
$$= \mathrm{lcm}\{\exp(N_{i,j}) \mid i = 1, \ldots, s; j = 1, \ldots, n\} = \mathrm{lcm}(r(G_1), \ldots, r(G_n)).$$

In particular, this shows that

$$r(G) \le \mathrm{lcm}(r(G_1), \ldots, r(G_n)) = \mathrm{lcm}(\mathrm{ge}(G_1), \ldots, \mathrm{ge}(G_n)) = \mathrm{ge}(G).$$

Since always $\mathrm{ge}(G) \le r(G)$, the assertion follows. □

In other words, the equality $r(G) = \mathrm{ge}(G)$ is well behaved under taking direct products. It is also well behaved under taking wreath products, at least under some technical assumptions.

LEMMA 4.2. *Let G and H be solvable groups, with H embedded into S_n, and let $\Gamma = G \wr H = G^n \rtimes H$, with H acting by permuting the n copies of G. If $\mathrm{ge}(G) = r(G)$ and $\mathrm{ge}(H) = r(H)$, then $\mathrm{ge}(\Gamma) = r(\Gamma)$, provided that at least one of the following conditions is fulfilled:*

(a) *$\mathrm{ge}(G)$ divides $\mathrm{ge}(H)$;*
(b) *G has a cyclic quotient C of order $\mathrm{ge}(G)$.*[1]

[1] This is automatic if, for example, G is abelian, and also if $\mathrm{ge}(G)$ is a prime.

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

PROOF. Let $((N_i, G_i) \mid i \in \{1, \dots, s\})$ as in Definition 3.2, achieving the minimal value $\operatorname{lcm}(e_1, \dots, e_s) = r(G)$. Set $\tilde{N}_i = N_i^n \leq G^n$ and $\tilde{G}_i = G_i \wr H$. Then $\tilde{G}_i$ is a partial complement for the normal subgroup $\tilde{N}_i$ of $\tilde{G}_{i-1}$ and $\tilde{G}_s = H$. Continue this sequence by choosing a sequence of normal subgroups and partial complements inside H, achieving the minimal value $r(H)$. Note that $\exp(\tilde{N}_i) = \exp(N_i)$ for all i. Thus, $r(\Gamma) \leq \operatorname{lcm}(\exp(\tilde{N}_1), \dots, \exp(\tilde{N}_s), r(H)) = \operatorname{lcm}(r(G), r(H)) = \operatorname{lcm}(\operatorname{ge}(G), \operatorname{ge}(H))$.

Now, in case (a), the latter expression simply equals $\operatorname{ge}(H)$, which is a trivial lower bound for $\operatorname{ge}(\Gamma)$, via projecting a generating set onto one of H. In total, $r(\Gamma) \leq \operatorname{ge}(\Gamma)$, giving equality, as claimed. In case (b), Γ projects onto $C \wr H$, which (due to C being abelian) projects onto $C \times H$. Thus, $\operatorname{ge}(\Gamma) \geq \operatorname{ge}(C \times H) = \operatorname{lcm}(\operatorname{ge}(C), \operatorname{ge}(H)) = \operatorname{lcm}(\operatorname{ge}(G), \operatorname{ge}(H))$ with equality $r(\Gamma) = \operatorname{ge}(\Gamma)$ in total. □

REMARK 4.3. Lemmas 4.1 and 4.2 yield a mechanism to construct large classes of groups with a positive answer to Questions 1.1 and 1.2, by beginning with groups as in Theorem 1.3 and taking iterated direct and wreath products. For example, taking iterated wreath products of a p-group G of nilpotency class $\leq p$ yields examples Γ of arbitrarily high nilpotency class, whereas starting with a nilpotent group G of non-prime-power order necessarily yields non-nilpotent examples Γ (see [1]). It should be remarked that the stronger condition $\exp(G) = \operatorname{ge}(G)$, while also preserved under taking direct products, is not at all preserved under taking wreath products. In fact, when taking iterated wreath products of a group G with itself, the generator exponent is preserved, whereas the exponent grows in every iteration. This serves as additional motivation for investigation of the constant $r(G)$, since it allows automatic construction of classes of examples which would be missed by naive considerations investigating only $\exp(G)$.

4.2. Proof of Theorem 1.3. We now turn to the proof of Theorem 1.3. This involves a close inspection of commutators in nilpotent groups.

LEMMA 4.4. *Let G be a p-group of generator exponent $e := \operatorname{ge}(G)$ and nilpotency class c. If $p \geq c$, then $G' = [G, G]$ is of exponent at most e.*

PROOF. We show iteratively that G_d is of exponent at most e for $d = c+1, \dots, 2$ in inverse order. The statement is trivial for $G_{c+1} = \{1\}$.

So, assume that the statement has been shown for G_{d+1} (for some $d \geq 2$). Since G_d is of nilpotency class $\leq c - 1 < p$, it is regular. Thus, by Proposition 2.3, it suffices to show that $\operatorname{ge}(G_d) \leq e$. That is, it suffices to show that every *commutator* in $G_d = [G, G_{d-1}]$ has order dividing e.

Let $\{x_1, \dots, x_n\}$ be a generating set of G with all x_i of order dividing e (which exists by assumption). Using the well-known commutator identity

$$[xz, y] = [z, [y, x]][x, y][z, y] \tag{4.1}$$

iteratively, every commutator $[g, h]$ (with $g \in G$, $h \in G_{d-1}$) can be written as a product of commutators of the form $[x_{n_i}, h_i]$ with $n_i \in \{1, \dots, n\}$ and $h_i \in G_{d-1}$. In particular,

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

$[g,h]^e = (\prod_i [x_{n_i}, h_i])^e$. Again, since G_d is regular, the order of $[g,h]$ cannot exceed all the orders of $[x_{n_i}, h_i]$. It thus suffices to show that $[x_k, y]^e = 1$ for $k \in \{1, \dots, n\}$ and $y \in G_{d-1}$. Now

$$1 = [1,y] = [x_k^e, y] = [x_k, y]^{x_k^{e-1}} \cdot [x_k^{e-1}, y] = [x_k, y]^{x_k^{e-1}} \cdots [x_k, y]^{x_k} \cdot [x_k, y].$$

Using the fact that $x_k^{e-1} = x_k^{-1}$, the above equation simplifies to

$$1 = [x_k^e, y] = (x_k \cdot [x_k, y])^e.$$

Writing the last power $(x_k \cdot [x_k, y])^e$ out using Theorem 2.5 and noting that $x_k^e = 1$ leads to $1 = x_k^e\,[x_k, y]^e = [x_k, y]^e$ times terms of the form $R_{i,j}^{f_{i,j}(e)}$, with weight $i\,(\geq 2)$ commutators $R_{i,j}$ of x_k and $[x_k, y]$ and polynomials $f_{i,j}$ which are integer linear combinations of $\binom{X}{1}, \dots, \binom{X}{i}$. In particular, all these higher commutators lie in $[G, [G, G_{d-1}]] = G_{d+1}$. Therefore, they all have order dividing e, by induction. Furthermore, using the fact that $[x_k, y] \in G_d$ and the fact that all higher commutators $R_{i,j}$ as above may be assumed to contain at least one entry $[x_k, y]$, Lemma 2.6 yields $R_{i,j} \in [G_d, G_{i-1}] \leq G_{d+i-1}$. In particular, $R_{i,j}$ vanishes for all $i \geq c - d + 2$. So, we may assume that $i \leq c - d + 1 \leq c - 1 < p$. But then $i!$ is coprime to p and hence $f_{i,j}(e)$ is divisible by e, implying that $R_{i,j}^{f_{i,j}(e)} = 1$.

Therefore finally $[x_k, y]^e = 1$. This shows the assertion. □

THEOREM 4.5. *For any p-group G of nilpotency class $c \leq p$, we have $r(G) = \mathrm{ge}(G)$.*

PROOF. Let $\{x_1, \dots, x_k\}$ be a minimal set of generators such that all x_i have order dividing $e := \mathrm{ge}(G)$. We can assume that $k \geq 2$. Set $H := \langle G', x_k \rangle$ and consider the commutator subgroup H'. Using the commutator identity (4.1) as in the previous proof, one easily verifies that every commutator in $[H, H]$ is a product of commutators of the form $[x_k, z]$ or $[y, z]$ with $y, z \in G'$. In particular, $H' \leq [G, G'] = G_3$.

Therefore, H has nilpotency class at most $c - 1 \leq p - 1$ and so is regular. By Proposition 2.3, for any $a \in \langle x_k \rangle$ and $b \in G'$, the order of ab does not exceed the maximum of the orders of a and b. However, $\mathrm{ord}(a)$ divides e by definition, and $\mathrm{ord}(b)$ divides e by Lemma 4.4. In total, $(ab)^e = 1$ and so $\exp(H)$ divides e. Furthermore, H is a normal subgroup of G (as G/G' is abelian). Finally, H has a partial complement in G, namely $U := \langle x_1, \dots, x_{k-1} \rangle$, which is strictly smaller than G by definition of $\{x_1 \dots, , x_k\}$. Of course U then has generator exponent dividing e, again by definition, and nilpotency class $\leq c$. Inductively, $r(U)$ divides e and, since $\exp(H)$ divides e as shown above, it follows from Lemma 3.3 that $r(G) \leq e$. Since always $r(G) \geq e$, the assertion follows. □

In particular, we find the following consequence, which with Proposition 3.4 readily yields Theorem 1.3.

COROLLARY 4.6. *Let G be a finite nilpotent group of class c and assume that $p \geq c$, where p is the smallest prime divisor of $|G|$. Then $r(G) = \mathrm{ge}(G)$.*

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

PROOF. Since a nilpotent group is the direct product of its Sylow subgroups, this follows directly from Theorem 4.5 together with Lemma 4.1. □

5. Combination with other methods

The bound $c \leq p$ in Theorem 4.5 is best possible in the sense that there exist p-groups of nilpotency class $p+1$ for which $r(G) > \mathrm{ge}(G)$, the easiest and smallest example being the dihedral group D_8 of order 16. For other small primes p, computer search with Magma [2] provides examples of order $|G| = p^{p+2}$ and it should be possible to give explicit examples for all p. For example, for $p = 3$, six out of 67 groups of order p^{p+2} have nilpotency class $p+1$ and, out of those, two fail to satisfy $r(G) = \mathrm{ge}(G)$. For such groups, additional ideas are required to answer Questions 1.1 and 1.2. One thing to note is that, due to the nature of Shafarevich's method, one may improve on the bound $r(G)$ by replacing any value $r(G_i)$ in the iteration process of Definition 3.2 by any known upper bound for $e(\mathbb{Q}, G_i)$, in case such a bound better than $r(G_i)$ is known. For example, $e(D_n, \mathbb{Q}) = 2$ is known from class field theory (see [13]). Substituting this value in the definition of $r(G)$ whenever a dihedral G_i occurs (and calling the thus altered constant $r'(G)$ for the moment) yields $e(\mathbb{Q}, G) = r'(G) = \mathrm{ge}(G)$ for six of the eight nilpotent groups of order < 64 which fulfil $r(G) > \mathrm{ge}(G)$. The two remaining cases (U_1 = SmallGroup(32,19) and U_2 = SmallGroup(32,20) in Magma's database) both have generator exponent 4 and $r'(U_i) = 8$. However, they both embed as index-two normal subgroups into G = SmallGroup(64,189), which has $r'(G) = 2$. So, there exist tame G-extensions $L/\mathbb{Q}$ with all inertia groups of order two. Choose a quadratic extension $K/\mathbb{Q}$, without loss of generality linearly disjoint to the fixed fields F_i of U_i in L ($i = 1, 2$), such that LK/K is an unramified G-extension. Then LK/F_iK is an unramified U_i-extension and $F_iK/\mathbb{Q}$ is Galois with group $C_2 \times C_2$, whose order equals $\mathrm{ge}(U_i)$. We have therefore at least answered Question 1.2 for U_i and in total have obtained the following result (aided by computer calculation).

THEOREM 5.1. *Question 1.2 has a positive answer for all nilpotent groups of order* < 64.

References

[1] G. Baumslag, 'Wreath products and p-groups', *Math. Proc. Cambridge Philos. Soc.* **55**(3) (1959), 224–231.

[2] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.

[3] P. Hall, 'A contribution to the theory of groups of prime power order', *Proc. Lond. Math. Soc. Ser. 2* **36**(1) (1934), 29–95.

[4] B. Huppert, *Endliche Gruppen, Part I* (Springer, Berlin, 1967).

[5] K.-S. Kim, 'Construction of unramified extensions with a prescribed Galois group', *Osaka J. Math.* **52** (2015), 1039–1050.

[6] K.-S. Kim, 'Construction of unramified extensions with a prescribed solvable Galois group', *Acta Arith.* **190** (2019), 49–56.

[7] K.-S. Kim and J. König, 'On Galois extensions with prescribed decomposition groups', *J. Number Theory*, to appear.

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press

[8] J. König, D. Neftin and J. Sonn, 'Unramified extensions over low degree number fields', *J. Number Theory* **212** (2020), 72–87.
[9] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields* (Springer, Berlin, 2000).
[10] A. Nomura, 'On the existence of unramified p-extensions with prescribed Galois group', *Osaka J. Math.* **47** (2010), 1159–1165.
[11] K. Uchida, 'Unramified extensions of quadratic number fields, II', *Tohoku Math. J.* **22** (1970), 220–224.
[12] M. M. Wood, 'Nonabelian Cohen–Lenstra moments', *Duke Math. J.* **168**(3) (2019), 377–427.
[13] Y. Yamamoto, 'On unramified Galois extensions of quadratic number fields', *Osaka J. Math.* **7** (1970), 57–76.

JOACHIM KÖNIG, Department of Mathematics Education,
Korea National University of Education, Cheongju, South Korea
e-mail: jkoenig@knue.ac.kr

https://doi.org/10.1017/S0004972720001136 Published online by Cambridge University Press