THREE STAGE TOWERS OF 5-CLASS FIELDS

DANIEL C. MAYER

Abstract. With $K = \mathbb{Q} \left( \sqrt{3812377} \right)$ we give the first example of an algebraic number field possessing a 5-class tower of exact length $\ell_5 K = 3$. The rigorous proof is conducted by means of the $p$-group generation algorithm, showing the existence of a unique finite metabelian 5-group $\Phi$ with abelianization $[5, 5]$ having the kernels $(M_1, \Phi^5)$ and targets $([25, 5, 5], [5, 5]^5)$ of Artin transfers $T_1 : \Phi \rightarrow M_i / M_i'$ to its six maximal subgroups $M_i$, prescribed by arithmetical invariants of $K$. Thus, $\Phi$ must be the second 5-class group $G_2^5 K$ of the real quadratic field $K$ but cannot be its 5-class tower group $G_5^\infty K$, since the relation rank $d_2 \Phi = 4$ is too big. We provide evidence of exactly five non-isomorphic extensions $G$ of $\Phi$ having the required relation rank $d_2 G = 3$ and derived length $\text{dl}(G) = 3$ whose metabelianization $G/G''$ is isomorphic to $\Phi$. Consequently, $G_5^\infty K$ must be one of the five non-metabelian groups $G$.

1. Introduction

Given a prime number $p \geq 2$, a positive integer $n \geq 1$, and an algebraic number field $K$, the nth Hilbert $p$-class field $F_p^n K$ of $K$ is the maximal unramified Galois extension of $K$ whose automorphism group $G_p^n K := \text{Gal} (F_p^n K / K)$ is a finite $p$-group of derived length $\text{dl}(G_p^n K) \leq n$. In particular, the first Hilbert $p$-class field $F_1^1 K$ of $K$ is the maximal abelian unramified $p$-extension of $K$. Its Galois group $G_1^1 K$ is isomorphic to the $p$-class group $\text{Cl}_p K := \text{Syl}_p \text{Cl}(K)$ of $K$, according to the Artin reciprocity law of class field theory $[1]$.

The projective limit $\lim_{\leftarrow n \geq 1} G_p^n K$ of all nth $p$-class groups $G_p^n K$ of $K$ is isomorphic to the possibly infinite topological Galois group $G := G_5^\infty K$ of the maximal unramified pro-$p$ extension $F_5^\infty K := \bigcup_{n \geq 1} F_p^n K$, that is the Hilbert $p$-class tower, of $K$. Conversely, the nth $p$-class group can be obtained as the nth derived quotient $G / G^{(n)} \simeq G_5^\infty K$ of the $p$-class tower group $G$ of $K$.

The length of the $p$-class tower of $K$ is defined as the derived length of $G$,

$$\ell_p K := \text{dl} \left( G_5^\infty K \right).$$

For each $n \geq 2$, inclusively $n = \infty$, the commutator subgroup of $G_p^n K$ is isomorphic to $\text{Gal} (F_p^n K / F_p^1 K)$, and the abelianization of $G_p^n K$ is isomorphic to the $p$-class group $\text{Cl}_p K$ of $K$,

$$G_p^n K / (G_p^n K) \simeq G_1^1 K \simeq \text{Cl}_p K,$$

in particular, the generator rank $d_1 (G_p^n K) := \dim_{\mathbb{F}_p} H^1 (G_p^n K, F_p)$ of $G_p^n K$ coincides with the $p$-class rank $r_p K := \dim_{\mathbb{F}_p} \left( \text{Cl}_p K \otimes \mathbb{F}_p \mathbb{F}_p \right)$ of $K$, according to Burnside’s basis theorem.

After the preceding clarification of the technical framework for this article, we devote a minimum of space to an outline of the historical evolution of finding $p$-class towers with increasing finite length. Thereby, we use the notation of the SmallGroups database $[4]$, $[5]$, and partially give more details than the original papers of the cited authors.

We have $\ell_p K = 0$ if and only if the class number $\# \text{Cl}(K)$ of the field $K$ is not divisible by $p$. 

Date: April 23, 2016.

2000 Mathematics Subject Classification. Primary 11R37, 11R29, 11R11, 11R20; Secondary 20D15, 20–04.

Key words and phrases. 5-class towers, 5-class groups, 5-capitulation, real quadratic fields, dihedral fields of degree 10; finite 5-groups with two generators; descendant tree, $p$-group generation algorithm, nuclear rank, bifurcation, $p$-multiplicator rank, relation rank, generator rank, Shafarevich cover, Artin transfers, partial order of Artin patterns. Research supported by the Austrian Science Fund (FWF): P 26008-N25.
If the $p$-class group $\mathrm{Cl}_p K > 1$ is cyclic, then we have a single stage tower with $\ell_p K = 1$, by Formula (1.2). If $K = \mathbb{Q} \left( \sqrt{d} \right)$ is a quadratic field and $p \geq 3$ is odd, the converse is also true \cite{23} Thm. 4.1, (1), p. 486. However, for the discriminant $d = -84 = -2^2 \cdot 3 \cdot 7$, we have $\mathrm{Cl}_2 K \simeq [2, 2]$ but nevertheless only $\ell_2 K = 1$ \cite{20} (ii), p. 277, \cite{23} § 9, pp. 501–503.

In 1930, Hasse \cite{17} § 27, pp. 173–174 gave the first example of $\ell_2 K \geq 2$ for a field of type $[4, 2]$, due to private communications by Furtwängler and Artin. It has discriminant $d = -260 = -2^2 \cdot 5 \cdot 13$, $\mathrm{G}_2^2 K \simeq (2^4, 6)$, and in fact $\ell_2 K = 2$. A field of type $[2, 2]$ with $\ell_2 K = 2$ is given by $d = -120 = -2^3 \cdot 5 \cdot 3$ with $(4) = -1$, and has $\mathrm{G}_2^2 K \simeq (2^3, 4)$ the quaternion group \cite{20} (vi.a,b), p. 278. However, a field of type $[2, 2]$ can never have a 2-class tower of length bigger than two.

Consequently, the first field with $\ell_2 K = 3$ of type $[4, 2]$. It was discovered in 2003 by Bush \cite{10} Prop. 2, p. 321 and has discriminant $d = -1780 = -2^2 \cdot 5 \cdot 89$. Its 2-tower group is one of two candidates $(2^8, 426|427)$ with class 5 and coclass 3. In 2006, Noper provided evidence of $\ell_2 K = 3$ for a field of type $[2, 2, 2]$ with $d = -3135 = -3 \cdot 5 \cdot 11 \cdot 19$ and four candidates for $\mathrm{G}_2^2 K$ of order 213, class 7 and coclass 6 \cite{9} § 3.4, pp. 7–8, \cite{34} Prop. 5, p. 239.

Now we turn to odd primes $p \geq 3$. In 1934, Scholz and Taussky \cite{37} § 3, pp. 39–41] manually calculated the first occurrences of $\ell_3 K = 2$ for $d = -4027$ of type $[3, 3]$, resp. $d = -3299$ of type $[9, 3]$. The corresponding 3-class tower groups are the Schur $\sigma$-groups $(3^5, 5)$, resp. one of the two candidates $(3^5, 14|15)$. However, they also claimed a two stage tower for $d = -9748 = 2^2 \cdot 2437$ \cite{37} § 3, p. 41], where neither of the two candidates $(3^5, 302|306)$ for the second 3-class group is a Schur $\sigma$-group \cite{21}. This claim was corrected by Bush and ourselves \cite{11} Cor. 4.1.1, p. 775] in 2015. We proved the first sufficient criterion for complex quadratic fields $K$ with $\ell_3 K = 3$, and provided two candidates $\mathrm{G}_3^3 K \simeq (3^5, 54) - #2; 2|6$ for $d = -9748$, in the notation of the ANUQP package \cite{13}. These were the first non-metabelian Schur $\sigma$-groups. They have order $3^8$, class 5, coclass 3, derived length 3, and are discussed in more detail in \cite{26} (70), p. 190], [26] Fig. 10, p. 191], and [28] §§ 6–7, p. 751–756).

The first occurrences of $\ell_3 K = 2$, resp. $\ell_7 K = 2$, were discovered in 2013 by ourselves for $d = -11199$ \cite{25} Tbl. 3.13, p. 450], resp. $d = -63499$ \cite{25} Tbl. 3.14, p. 450]. The corresponding groups $\mathrm{G}_3^3 K \simeq (5^3, 12)$, resp. $\mathrm{G}_7^7 K \simeq (7^3, 14|16)$ with two candidates, are metabelian Schur $\sigma$-groups. Our attempt to prove $\ell_7 K = 3$ for $d = -62632$ with two candidates $\mathrm{G}_7^7 K \simeq (5^5, 564) - #1; 1|23$, resp. $d = -67063$ with six candidates $\mathrm{G}_3^3 K \simeq (5^3, 564) - #1|8|9|11|12|14|15$, was not successful, since we could not find suitable Schur $\sigma$-groups $\mathrm{G}_3^3 K$.

Little progress was achieved for real quadratic fields until we developed new techniques for determining their $p$-class tower in \cite{27}. We found $\ell_3 K = 2$ for $d = 422573$ with $\mathrm{G}_3^3 K \simeq (3^5, 5)$ \cite{23} Tbl. 4, p. 498], and $\ell_5 K = 2$ for $d = 4954652$ with $\mathrm{G}_5^5 K \simeq (5^5, 12)$. With extensive computational effort we succeeded in proving $\ell_3 K = 3$ for $d = 957013$, which has $\mathrm{G}_3^3 K \simeq (3^7, 273)$ with class 5, coclass 2, and relation rank 3 \cite{27} Ex. 6.3, pp. 306–307]. However, the attempt to prove that the quintic analogue $d = 12562849$ has $\ell_3 K = 3$ with either of the two candidates $(5^9, 680) - #1; 1|2$ for $\mathrm{G}_3^3 K$, having order $5^7$, class 5 and coclass 2, failed, due to a complete exhaustion of RAM during the construction of two successive unramified cyclic quintic extensions of the real quadratic field $K$, that is an extension of absolute degree 50.

Exploring $p$-groups of coclass 1 instead of coclass 2, which would be useless for finding 3-class towers of three stages, turned out to be the crucial idea how to circumvent such hopeless number theoretic computations of high complexity and to conduct a purely group theoretic proof of the principal results of this article, which are the following statements, in a succinct coarse form.

**Theorem 1.1.** Let $K$ be a real quadratic field with 5-class group $\mathrm{Cl}_5 K$ of type $[5, 5]$ and denote by $L_1, \ldots, L_6$ its six unramified cyclic quintic extensions. If $K$ possesses the 5-capitulation type

\begin{equation}
\chi(K) \sim (1, 0, 0, 0, 0, 0), \text{ with fixed point 1,}
\end{equation}

in the six extensions $L_i$, and if the 5-class groups $\mathrm{Cl}_5 L_i$ are given by

\begin{equation}
\tau(K) \sim ([25, 5, 5, 5], [5, 5], [5, 5], [5, 5], [5, 5], [5, 5]),
\end{equation}
The minimal fundamental discriminant \( 5 \) with order \( 5 \) by Shafarevich \cite{36}, come into the play in \( \S \S \) five candidates for the \( 5 \)-class tower group

\[
G_5^2 K \simeq \langle 15625, 635 \rangle
\]

with order \( 5^6 \), class 5, coclass 1, derived length 2, and relation rank 4, and one of the following five candidates for the \( 5 \)-class tower group

\[
G_5^\infty K = G_5^3 K \simeq \langle 78125, n \rangle, \quad \text{where } n \in \{361, 373, 374, 385, 386\},
\]

with order \( 5^7 \), class 5, coclass 2, derived length 3, and relation rank 3.

**Example 1.1.** The minimal fundamental discriminant \( d \) of a real quadratic field \( K = \mathbb{Q}(\sqrt{d}) \) satisfying the conditions \( \langle 1.3 \rangle \) and \( \langle 1.4 \rangle \) is given by

\[
d = 3 \cdot 812 \cdot 377 = 991 \cdot 3 \cdot 847.
\]

The next occurrence is \( d = 19 \cdot 621 \cdot 905 = 3 \cdot 5 \cdot 307 \cdot 4261 \), which is currently the biggest known example, whereas \( d = 21 \cdot 281 \cdot 673 = 3 \cdot 7 \cdot 53 \cdot 19 \cdot 121 \) satisfies \( \langle 1.4 \rangle \) but has a different \( \kappa(K) \sim (2, 0, 0, 0, 0, 0) \), without fixed point.

The organization of this paper is as follows. In \( \S \) 2 we show how the arithmetical invariants \( \kappa(K) \) and \( \tau(K) \) of an algebraic number field \( K \) (e.g., the data in Formula \( \langle 1.3 \rangle \) and \( \langle 1.4 \rangle \)) can be translated into group theoretic information \( \kappa(\mathfrak{G}) \) and \( \tau(\mathfrak{G}) \) on the second \( p \)-class group \( \mathfrak{G} = G_5^2 K \) of \( K \), following the ideas indicated in Artin’s paper \cite{2}, which led to Furtwängler’s proof \cite{13} of the famous Principal Ideal Theorem and were expanded in detail by Hasse \cite{17}.

\( \S \) 3 is devoted to the study of the interplay between the Artin pattern \( AP(G) = (\tau(G), \kappa(G)) \) of finite \( p \)-groups \( G \) on a descendant tree \( T(R) \) with root \( R \) and the partial order \( G > \pi G \) induced by the (child, parent)-pairs \( (G, \pi G) \) of the tree, which was discovered recently in \cite{30}. These monotony properties of \( \tau(G) \) and \( \kappa(G) \) are employed in the \( p \)-group generation algorithm by Newman \cite{33} and O’Brien \cite{25} for identifying the unique metabelianization \( \mathfrak{G} = G_5^2 K = G/G'' \simeq \langle 15625, 635 \rangle \) of the \( 5 \)-class tower group \( G = G_5^\infty K \) of \( K \) by the strategy of pattern recognition via Artin transfers in \( \S \) 4. An unexpected bifurcation in the tree \( T ((25, 2)) \) enabled the discovery of five non-isomorphic possibilities \( G \simeq \langle 78125, n \rangle \) with \( n \in \{361, 373, 374, 385, 386\} \) and derived length \( d(G) = 3 \) for \( G \) itself.

The termination condition for the algorithm is expressed by the growth of the \( \tau(G) \)-component beyond a break-off bound. At this stage it is still open whether the length of the \( 5 \)-class tower of \( K \) is \( \ell_5 K = 3 \) or \( \ell_5 K = 2 \), since only group theoretic information was used up to this point.

Therefore, arithmetical constraints for \( G \) in form of the relation rank, which has been determined by Shafarevich \cite{35}, come into the play in \( \S \S \) 5 and 6, and eliminate the possibility of a metabelian tower with length \( \ell_5 K = 2 \) for a real quadratic field \( K \).

**2. Pattern recognition via Artin transfers**

**2.1. Translation from number theory to group theory.** We start with an arithmetical situation where Artin patterns play an important role. Let \( p \geq 2 \) be a prime number. Suppose we are given an algebraic number field \( K/\mathbb{Q} \) with non-trivial \( p \)-class group \( \text{Cl}_p K > 1 \). Then the intermediate fields \( L \) between \( K \) and its Hilbert \( p \)-class field \( F_p^1 K \) are exactly the (finitely many) abelian unramified extensions of \( K \) with degree a power of \( p \). For each of them, we denote by \( j_{L|K} : \text{Cl}_p K \to \text{Cl}_p L \) the class extension homomorphism.

**Definition 2.1.** By the restricted Artin pattern of \( K \) we understand the pair consisting of the family \( \tau(K) \) of the \( p \)-class groups of all extensions \( K < L < F_p^1 K \) as its first component and the \( p \)-capitulation type \( \kappa(K) \) as its second component,
\[(2.1)\quad \text{AP}(K) := (\tau(K), \varkappa(K)), \quad \tau(K) := (\text{Cl}_pL)_{K < L < \mathbb{F}_p^jK}, \quad \varkappa(K) := (\ker j_{L[K]})_{K < L < \mathbb{F}_p^jK}.\]

**Remark 2.1.** It is convenient to replace the group objects in the unordered family \(\tau(K)\), resp. \(\varkappa(K)\), by ordered abelian type invariants, resp. ordered numerical identifiers, accepting the drawback of dependence on the selected ordering (indicated by using the symbol \(\sim\) instead of \(=\)).

In the case \(p = 5\) and \(C := \text{Cl}_5K \simeq [5, 5]\), which is relevant for this paper, let \(L_1, \ldots, L_6\) be the six intermediate fields between \(K\) and \(\mathbb{F}_5^1K\) and denote by \(N_i := \text{Norm}_{L_i/K}(\text{Cl}_5L_i)\) their norm class groups, which are exactly the six cyclic subgroups of index 5 in \(C\). In this sense, the notation of the 5-capitulation type in Formula (1.3) (where 0 means a total capitulation) is an abbreviation for

\[(2.2)\quad \varkappa(K) \sim (N_1, C, C, C, C, C).\]

Now we turn to the group theoretic aspect of Artin patterns. Let \(G\) be a finite \(p\)-group or an infinite topological pro-\(p\) group with finite abelianization \(G/G'\). For each of the (finitely many) intermediate groups \(M\) between the commutator subgroup \(G'\) and the group \(G\), we denote by \(T_{G,M} : G \to M/M'\) the Artin transfer homomorphism from \(G\) to the abelianization \(M/M'\) of \(M\) [20] Dfn. 3.1, p. 5.

**Definition 2.2.** By the **restricted Artin pattern** of \(G\) we understand the pair consisting of the **transfer target type** (TTT) \(\tau(G)\) as its first component and the **transfer kernel type** (TKT) \(\varkappa(G)\) as its second component,

\[(2.3)\quad \text{AP}(G) := (\tau(G), \varkappa(G)), \quad \tau(G) := (M/M')_{G' < M < G}, \quad \varkappa(G) := (\ker T_{G,M})_{G' < M < G}.\]

**Remark 2.2.** Again, we usually replace the group objects in the unordered family \(\tau(G)\), resp. \(\varkappa(G)\), by ordered abelian type invariants, resp. ordered numerical identifiers.

In the case \(p = 5\) and \(G/G' \simeq [5, 5]\), which will be of concern in this paper, let \(M_1, \ldots, M_6\) be the six intermediate groups between \(G'\) and \(G\) and we write the transfer kernel type corresponding to Formula (1.3) as

\[(2.4)\quad \varkappa(G) \sim (M_1, G, G, G, G, G) \quad \text{or briefly} \quad \varkappa(G) \sim (1, 0, 0, 0, 0, 0).\]

Finally, we combine the number theoretic and group theoretic view of Artin patterns.

**Theorem 2.1.** Let \(p\) be a prime number. Assume that \(K\) is a number field, and let \(\mathfrak{O} := G_p^2K\) be the second \(p\)-class group of \(K\). Then \(\mathfrak{O}\) and \(K\) share a common restricted Artin pattern,

\[(2.5)\quad \text{AP}(\mathfrak{O}) = \text{AP}(K), \quad \text{that is} \quad \tau(\mathfrak{O}) = \tau(K) \quad \text{and} \quad \varkappa(\mathfrak{O}) = \varkappa(K).\]

**Proof.** A sketch of the proof is indicated in [32] and [23] § 2.3, pp. 476–478], but the precise proof has been given by Hasse in [17] § 27, pp. 164–175]. We have elaborated Hasse’s proof on Wikipedia:

https://en.wikipedia.org/wiki/Principalization_(algebra) \(\square\)

### 2.2. Metabelian \(p\)-groups of maximal class.

Generally, let \(G\) be a finite \(p\)-group, for an arbitrary prime number \(p \geq 2\). Assume that \(G\) is of order \(|G| = p^n\), where \(n\) is the logarithmic order, of nilpotency class \(c = \text{cl}(G) = m = 1\), where \(m\) is the index of nilpotency, and of coclass \(r = \text{cc}(G) = n - c = n - m + 1\). Denote the descending **lower central series** of \(G\) by

\[(2.6)\quad G = \gamma_1G > \gamma_2G > \gamma_3G > \ldots > \gamma_{m-1}G > \gamma_mG = 1,
\]

where \(\gamma_jG = [\gamma_{j-1}G, G]\), for \(j \geq 2\), and the ascending **upper central series** of \(G\) by

\[(2.7)\quad 1 = \zeta_0G < \zeta_1G < \zeta_2G < \ldots < \zeta_{c-1}G < \zeta_cG = G,
\]
where $\zeta_j G/\zeta_{j-1} G = \text{Centre}(G/\zeta_{j-1} G)$, for $j \geq 1$.

Now let $G$ be a metabelian $p$-group of coclass $r = \text{cc}(G) = 1$, whence $n = m$. Then the abelianization $G/G'$ is of type $[p, p]$ and $G = \langle x, y \rangle$ can be generated by two elements $x, y$. Suppose that $m \geq 3$, i.e., $G$ is non-abelian. Denote the two-step centralizer, that is the centralizer of the two-step factor group $\gamma_2 G/\gamma_4 G$ of the lower central series, by

$$\chi_2^G := \{ g \in G \mid [g, u] \in \gamma_4 G \quad \text{for all} \quad u \in \gamma_2 G \},$$

that is,

$$\chi_2^G/\gamma_4 G = \text{Centralizer}_{G/\gamma_4 G}(\gamma_2 G/\gamma_4 G).$$

$\chi_2^G$ is the biggest subgroup of $G$ such that $[\chi_2^G, \gamma_2^G] \leq \gamma_4^G$. It is characteristic, contains the commutator subgroup $\gamma_2^G$, and coincides with $G$ if and only if $m = 3$, whence we have $\gamma_2^G < \chi_2^G < G \iff m \geq 4$. Select normalized generators of $G = \langle x, y \rangle$ such that

$$x \in G \setminus \chi_2^G, \quad y \in \chi_2^G \setminus \gamma_2^G.$$ 

Starting with the main commutator $s_2 := [y, x] \in \gamma_2^G$ define the higher iterated commutators recursively by $s_j := [s_{j-1}, x] \in \gamma_j^G$, for $j \geq 3$.

The general theory of $p$-groups of maximal class can be found in Huppert [19, § 14, p. 361] and Berkovich [3, § 9, p. 114].

In the isomorphism class of a metabelian $p$-group $G$ of maximal class, and of order $|G| = p^m$, there exists a representative $G_a^m(z, w)$ whose normalized generators satisfy the following relations with a fixed system of parameters $a = (a(m-k), \ldots, a(m-1), w), z$; according to Blackburn [6] and Miech [31, p. 332]:

- parametrized commutator relations with parameters $0 \leq a(m-\ell) \leq p-1$ for $1 \leq \ell \leq k$, in particular, with non-vanishing parameter $a(m-k) > 0$,

$$[s_j, y] = \begin{cases} \prod_{\ell=1}^{k-j+2} s_a^{a(m-j+2-\ell)} \in [\gamma_j G, \chi_2 G] = \gamma_{m-k+j-2} G, & \text{for } 2 \leq j \leq k+1, \\ 1, & \text{for } j \geq k + 2, \end{cases}$$

- parametrized relations for $p$th powers of the generators $x, y$ and of higher commutators $s_j$, with parameters $0 \leq w, z \leq p-1$, and $v := a(m-k)$ if $k = p-2$, but $v := 0$ if $k \leq p-3$,

$$x y^{j} = s_{m-1}^{w+z+j+v^2} \in \zeta_1 G, \quad \text{for } 0 \leq j \leq p-1$$

(2.11)

$$s_{j+1}^p \prod_{\ell=2}^p s_{\ell}^{(\ell)} = s_{m-1}^{z} \in \zeta_1 G,$$

$$s_j^p \prod_{\ell=2}^p s_{j+\ell}^{(\ell)} = 1, \quad \text{for } 1 \leq j \leq m-2,$$

- parametrized nilpotency relations with parameter $m \geq 3$ (the index of nilpotency),

$$s_j \neq 1, \quad \text{for } j \leq m-1, \quad \text{but } s_j = 1, \quad \text{for } j \geq m,$$

expressing the polycyclic structure $\gamma_j G = \langle s_j, \gamma_{j+1} G \rangle$, $\gamma_j G/\gamma_{j+1} G \simeq C_p$, for $j \geq 2$ and $j \leq m-1$, with cyclic factors (CF) of the lower central series, which coincides here with the reverse upper central series, $\zeta_j G = \gamma_{m-j} G$, for $0 \leq j \leq m-1$.

- and trivial metabelian relations within $G'$,

(2.13) $[s_i, s_j] = 1$, for all $i, j \geq 2$.

In the case of an index of nilpotency $m \geq 4$, the commutator relation for $s_2$ in Formula (2.10) explicitly describes the properties of the two-step centralizer $\chi_2 G = \langle y, \gamma_2 G \rangle$, which are implicitly postulated by Formula (2.8):
Definition 2.3. \[ p(2.16) \]

A polarized with a single two-step centralizer to the polarization of the transfer target type.

The maximal normal subgroups \( M_i \) of \( G \) contain the commutator subgroup \( \gamma_2G \) of \( G \) as a normal subgroup of index \( p \) and thus are of the shape \( M_i = \langle g_i, \gamma_2G \rangle \). We define a standard ordering by \( g_1 = y \) and \( g_i = xy^{i-2} \) for \( 2 \leq i \leq p + 1 \). In particular, \( M_1 = \langle y, \gamma_2G \rangle = \chi_2G \) is the two-step centralizer. In summary:

\[ M_1 = \langle y, \gamma_2G \rangle = \chi_2G, \quad \text{and} \quad M_i = \langle xy^{i-2}, \gamma_2G \rangle \quad \text{for} \quad 2 \leq i \leq p + 1. \]

### 2.3. Polarization of the transfer target type

The transfer target type \( \tau(G) \) of a non-abelian \( p \)-group \( G \) whose second derived quotient \( G/G'' \) is of maximal class has a particularly simple form with a single polarized component and \( p \) fixed components of type \( [p, p] \). The polarization is due to the two-step centralizer \( \chi_2G \) of the metabelianization \( \mathfrak{G} := G/G'' \) of \( G \) [25 § 3.1.1, p. 412].

**Definition 2.3.** Let \( p \) be a prime number and \( e \geq p - 1 \) be an integer. By the nearly homocyclic abelian \( p \)-group of order \( p^e \) we understand the abelian group

\[ (2.17) \quad A(p, e) := \left( \underbrace{p^q, \ldots, p^q}_{r \text{ times}}, \underbrace{p^{q+1}, \ldots, p^{q+1}}_{p - 1 - r \text{ times}} \right), \]

with \( r \) invariants \( p^{q+1} \) and \( p - 1 - r \) invariants \( p^q \), where \( q \geq 1 \) and \( 0 \leq r < p - 1 \) denote the quotient and remainder of the Euclidean division \( e = q \cdot (p - 1) + r \) of \( e \) by \( p - 1 \). Additionally, let

\[ (2.18) \quad A(p, r) := \left( \underbrace{p, \ldots, p}_{r \text{ times}} \right), \]

be the elementary abelian \( p \)-group of rank \( r \) for \( 1 \leq r < p - 1 \), and \( A(p, 0) := 1 \) the trivial group.

The abelian group \( A(p, e) \) is homocyclic if and only if \( e \) is a multiple of \( p - 1 \) or \( 1 \leq e < p - 1 \).

**Theorem 2.2.** Let \( p \) be a prime number and \( G \) be a \( p \)-group whose second derived quotient \( \mathfrak{G} := G/G'' \) is of coclass \( cc(\mathfrak{G}) = 1 \), nilpotency class \( c := \text{cl}(\mathfrak{G}) \geq 2 \), and defect \( k := k(\mathfrak{G}) \), but is neither isomorphic to the extra special \( p \)-group \( G_{3, 0}^0(1, 1) \) of order \( p^3 \) and exponent \( p^2 \) nor to the Sylow \( p \)-subgroup \( G_p^{p+1}(1, 0) \simeq \text{Syl}_p A_{p^2} \) of the alternating group of degree \( p^2 \), with odd \( p \geq 3 \). Then the transfer target type of \( G \) is given by

\[ (2.18) \quad \tau(G) = \left( A(p, c - k), [p, p], \ldots, [p, p] \right). \]

**Proof.** According to Theorem 6.2, \( G \) and \( \mathfrak{G} \) share a common restricted Artin pattern, \( AP(G) = AP(\mathfrak{G}) \). In particular they share the same transfer target type \( \tau(G) = \tau(\mathfrak{G}) \). Thus we have reduced the claim to the metabelian \( p \)-group \( \mathfrak{G} \) of maximal class, as discussed in § 2.2.

We use the standard ordering of the maximal subgroups \( M_i \leq \mathfrak{G} \) in Formula (2.15) and recall from [23 Cor. 3.1, p. 476] that the commutator subgroups \( M_i' \) are given by

\[ (2.19) \quad M_i' = \gamma_{m-k}\mathfrak{G}, \quad \text{and} \quad M_i' = \gamma_3\mathfrak{G} \quad \text{for} \quad 2 \leq i \leq p + 1. \]

We start by showing that \( M_i/M_i' \simeq [p, p] \) for \( 2 \leq i \leq p + 1 \). To this end, we observe that \( M_i = \langle xy^{i-2}, \gamma_2\mathfrak{G} \rangle \) and \( \gamma_2\mathfrak{G} = \langle s_2, \gamma_3\mathfrak{G} \rangle \), and thus \( M_i/M_i' = \langle xy^{i-2}, s_2, \gamma_3\mathfrak{G} \rangle/\gamma_3\mathfrak{G} \) where \( x, y \) are
the normalized generators in Formula (2.11) and $s_2 = [y, x]$ is the main commutator of $\mathfrak{G}$. We have to determine the order of the elements $xy^{i-2}$, with $2 \leq i \leq p + 1$, and $s_2$ modulo $\gamma_3 \mathfrak{G}$. The third equation in Formula (2.11) yields $s_2^p \prod_{i=2}^{p} s_{i+1}^{(y)} = 1$, for $j = 1$, and thus $s_2^p \in \gamma_3 \mathfrak{G}$, i.e., $\text{ord}(s_2) = p$.

The first equation in the same formula gives $(xy^j)^p = s_{m+1}^{w_j+1}$, for $0 \leq j \leq p - 1$, which is an element of $\gamma_3 \mathfrak{G}$ when $m - 1 \geq 3$, that is $m \geq 4$. For $m = 3$, however, we certainly have $k = 0$ and thus $v = 0$, but we must distinguish between the two extra special groups $G_0(0, 0)$, where $z = w = 0$ and $(xy^j)^p = 1$, and $G_0(0, 1)$, where $z = 0$, $w = 1$ and $(xy^j)^p = s_2$. In summary, we have $\text{ord}(xy^{i-2}) = p^2$ and $M_1/M_1' \simeq [p^2]$ for $G_0(0, 1)$, but $\text{ord}(xy^{i-2}) = p$ otherwise, which proves our claim.

We continue by showing that $M_1/M_1' \simeq A(p, c-k)$, where $c = m - 1$. In this case, we have $M_1 = \langle y, \gamma_2 \mathfrak{G} \rangle$, $\gamma_2 \mathfrak{G} = \langle s_2, \ldots, s_{m-k-1}, \gamma_{m-k} \mathfrak{G} \rangle$, and thus $M_1/M_1' = \langle y, s_2, \ldots, s_{m-k-1}, \gamma_{m-k} \mathfrak{G} \rangle/\gamma_{m-k} \mathfrak{G}$. We put $N := m - k$ and use the third equation in Formula (2.11), that is,

$$s_{j+1}^p \cdot s_{j+2} \cdots s_{j+p-1} \cdot s_{j+p} = 1,$$

for $1 \leq j \leq m - 2$.

These power relations enable us to compute the order of the elements $y$ and $s_j$, with $2 \leq j \leq N - 1$, modulo $\gamma_N \mathfrak{G}$ by a finite nested double induction with respect to the quotient $q \geq 0$ and the remainder $0 \leq r < p - 1$ of the Euclidean division $N - 1 = q \cdot (p - 1) + r$. Thereby we always have to observe that $s_j \in \gamma_N \mathfrak{G}$, i.e., $\text{ord}(s_j) = 1$, for $j \geq N$, and that the binomial coefficients $\binom{p}{j}$ are multiples of $p$ for $1 \leq j < p - 1$.

The first inner induction on the remainders successively yields $s_{N-1}^p = 1$, $s_{N-2}^p \cdot s_{N-1}^{\binom{p}{2}} = 1$, and so on until $s_{N-p+1}^p \cdot s_{N-p+2} \cdots s_{N-1}^{\binom{p}{p-1}} = 1$, that is, we can determine the orders $\text{ord}(s_j) = p$, for $N - (p - 1) \leq j \leq N - 1$, recursively.

The second inner induction on the remainders successively yields $s_{N-p}^p \cdot s_{N-2} = 1$, $s_{N-p-1}^p \cdot s_{N-p-2} \cdots s_{p-1}^{\binom{p}{p}} = 1$, and so on until $s_{N-p+2}^p \cdot s_{N-p+3} \cdots s_{N-p} \cdot s_{N-p+1}^p = 1$, that is, we can determine the orders $\text{ord}(s_j) = p^2$, for $N - 2(p - 1) \leq j \leq N - (p - 1) - 1$, recursively, but also expressions for $s_j$ with $N - (p - 1) \leq j \leq N - 1$ in terms of $s_{\ell}$ with $\ell < j$.

In the same manner, we continue to obtain the orders $\text{ord}(s_j) = p^3$, for $N - 3(p - 1) \leq j \leq N - 2(p - 1) - 1$, and so on until

$$\text{ord}(s_j) = p^q,$$

for $N - q(p - 1) \leq j \leq N - (q - 1)(p - 1) - 1$, by outer induction on the quotients.

The last inner induction on the remainders will in general be shorter than the previous inner inductions and yields

$$\text{ord}(s_j) = p^{q+1},$$

for $N - q(p - 1) - r \leq j \leq N - q(p - 1) - 1$,

but the recursive process terminates when we reach $N - q(p - 1) - (r - 1) = 2$, that is,

$$s_2^p \cdot s_3^{(p)} \cdots s_{p-1}^{(p)}, s_{p} = 1,$$

which shows that the higher commutators $s_{p+1}, \ldots, s_{N-1}$ can be expressed in terms of $s_2, \ldots, s_p$.

Finally, we employ the second equation in Formula (2.11), that is,

$$y^p \cdot s_2^{(p)} \cdots s_{p-1}^{(p)}, s_p = s_{m-1}^p,$$

which formally corresponds to $N - q(p - 1) - r = 1$ when we put $s_1 := y$, but now the right side is $s_{m-1}^p$ instead of $1$. Here we must be careful and distinguish the exceptional case of the Sylow $p$-subgroup $G_0^{+1}(1, 0) \simeq \text{Syl}_p \mathfrak{A}_p$ of the alternating group of degree $p^2$, if $p \geq 3$ is an odd prime. In this special case, we have $m = p + 1$, $z = 1$, and thus $s_{m-1}^p = s_p$, which has the unique effect that $s_p$ cancels and cannot be expressed in terms of $y, s_2, \ldots, s_{p-1}$. All elements $y, s_2, \ldots, s_{p-1}, s_p$ are of order $p$ and generate an elementary abelian $p$-group of rank $p$, bigger than the rank $p - 1$ of all nearly homocyclic abelian $p$-groups.
In all other cases, the higher commutators \( s_p, s_{p+1}, \ldots, s_{N-1} \) can be expressed in terms of \( y, s_2, \ldots, s_{p-1} \), and the Formulas \((2.20)\) and \((2.21)\) show that \( M_1/M_1' \) is isomorphic to the nearly homocyclic abelian \( p \)-group \( A(p, c-k) \) of logarithmic order \( N - 1 = m - k - 1 = c - k \). \(\square\)

Note that Theorem 2.2 is more general than Blackburn’s Theorem \[6, Thm. 3.4, p. 68\], since we have used Theorem 6.2 and therefore the \( p \)-group \( G \) need not be of maximal class.

3. Monotony of Artin Patterns on Descendant Trees

**Definition 3.1.** Let \( p \) be a prime and \( G, H \) and \( R \) be finite \( p \)-groups.

1. The lower central series (LCS) of \( G \) is defined recursively by

\[
\gamma_1 G := G, \quad \text{and} \quad \gamma_n G := [\gamma_{n-1} G, G] \quad \text{for} \quad n \geq 2.
\]

2. We call \( G \) an immediate descendant (or child) of \( H \), and \( H \) the parent of \( G \), if \( H \simeq G/\gamma_c G \) is isomorphic to the image of the natural projection \( \pi : G \to G/\gamma_c G \) of \( G \) onto the quotient by the last non-trivial term \( \gamma_c G > 1 \) of the LCS of \( G \), where \( c := \text{cl}(G) \) denotes the nilpotency class of \( G \). In this case, we consider the projection \( \pi \) as a directed edge \( G \to H \) from \( G \) to \( H \simeq \pi G \), and we speak about the parent operator \( \pi \):

\[
\pi : G \to \pi G = G/\gamma_c G \simeq H \quad \text{with} \quad c = \text{cl}(G).
\]

3. We call \( G \) a descendant of \( H \), and \( H \) an ancestor of \( G \), if there exists a finite path of directed edges

\[
(Q_j \to Q_{j+1})_{0 \leq j < \ell} \quad \text{such that} \quad G = Q_0 \text{ and } H = Q_\ell,
\]

where \( \ell \geq 0 \) denotes the path length.

4. The descendant tree of \( R \), denoted by \( \mathcal{T}(R) \), is the rooted directed tree with root \( R \) having the isomorphism classes of all descendants of \( R \) as its vertices and all (child, parent)-pairs \((G, H)\) among the descendants \( G, H \) of \( R \) as its directed edges \( G \to \pi G \simeq H \). By means of formal iterations \( \pi^j \) of the parent operator \( \pi \), each vertex of the descendant tree \( \mathcal{T}(R) \) can be connected with the root \( R \) by a finite path of edges:

\[
\mathcal{T}(R) = \{ G \mid G = \pi^0 G \to \pi^1 G \to \pi^2 G \to \ldots \to \pi^\ell G = R \quad \text{for some} \quad \ell \geq 0 \}.
\]

The restricted Artin pattern enjoys the following monotony property on a descendant tree.

**Theorem 3.1.** Let \( \mathcal{T}(R) \) be the descendant tree with root \( R > 1 \), a finite non-trivial \( p \)-group, and let \( G \to \pi G \) be a directed edge of the tree. Then the restricted Artin pattern \( \text{AP} = (\tau, \kappa) \) satisfies the following monotonicity relations

\[
\tau(G) \geq \tau(\pi G),
\]

\[
\kappa(G) \leq \kappa(\pi G),
\]

that is, the TTT \( \tau \) is an isotonic mapping and the TKT \( \kappa \) is an antitonic mapping with respect to the partial order \( G > \pi G \) induced by the directed edges \( G \to \pi G \).

**Proof.** An abelian \( p \)-group \( A \) has the trivial group \( \pi A = A/\gamma_c A \simeq 1 \) as its parent, because the last non-trivial lower central \( \gamma_c A = \gamma_1 A = A \) of \( A \) coincides with \( A \). Since the tree root \( R > 1 \) is supposed to be non-trivial, none of its proper descendants \( G > R \) can be abelian. \( G \) must be of class \( c = \text{cl}(G) \geq 2 \). Consequently, if \((G, \pi G)\) is a (child, parent)-pair of the tree \( \mathcal{T}(R) \), then the last non-trivial lower central of the child \( G \) is contained in the commutator subgroup of \( G \), i.e., \( \ker(\pi) = \gamma_c G \leq \gamma_2 G = G' \), as pointed out in \[30, Thm. 5.3, p. 85\].

The restricted Artin pattern of a finite \( p \)-group \( G \) is the pair \( \text{AP}(G) = (\tau(G), \kappa(G)) \) consisting of the transfer target type \( \tau(G) = (U/U')_{G' < U < G} \) and the transfer kernel type \( \kappa(G) = \)
Proof. Let $G$ be a pro-$p$ group, with an odd prime $p \geq 3$, and let $\pi : G \rightarrow \pi G$ be the parent operator of $G$ with $c = \text{cl}(G)$.

(1) If $G$ is a $\sigma$-group, then $\pi G$ is also a $\sigma$-group.

(2) If $G$ is a finite $p$-group and let $\pi : G \rightarrow \pi G$ be the parent operator $\pi G = G/\gamma_c G$ with $c = \text{cl}(G)$,

- The nilpotency class increases exactly by 1 from the parent $\pi G$ to the child $G$.
- If $s$ denotes the step size from parent $\pi G$ to child $G$, then the coclass of $G$ is given by $\text{cc}(G) = \text{cc}(\pi G) + (s - 1)$, in particular, $\text{cc}(G) = \text{cc}(\pi G)$ for $s = 1$.
- The derived length of $\pi G$ is not bigger than the derived length of $G$.

\[
\text{cl}(G) = \text{cl}(\pi G) + 1, \quad \text{cc}(G) = \text{cc}(\pi G) + (s - 1), \quad \text{dl}(G) \geq \text{dl}(\pi G).
\]

(3) If $G$ is a finite metabelian $p$-group of maximal class and $\pi$ is the parent operator, then the defect of the parent $\pi G$ is not bigger than the defect of the child $G$, that is, $k(\pi G) \leq k(G)$, more precisely

\[
k(\pi G) = \begin{cases} k(G) & \text{if } k(G) = 0, \\ k(G) - 1 & \text{if } k(G) \geq 1, \end{cases}
\]

which can also be expressed in the form $k(\pi G) = \max(0, k(G) - 1)$.

Proof. Let $d := \text{dl}(G)$ be the derived length of $G$ and

\[G = G^{(0)} > G^{(1)} > \ldots > G^{(d-1)} > G^{(d)} = 1\]
be the derived series of \( G \), defined recursively by \( G^{(0)} := G \) and \( G^{(j)} := [G^{(j-1)}, G^{(j-1)}] \) for \( j \geq 1 \). For any homomorphism \( \pi : G \to H \) of groups, the proof of [39] Cor. 7.2, Appendix, p. 100] has shown that \( \langle \pi G \rangle^{(j)} = \pi \langle G^{(j)} \rangle \) for \( j \geq 0 \), and similarly for the lower central series \( \gamma_j \langle \pi G \rangle = \pi \langle \gamma_j G \rangle \) for \( j \geq 1 \).

1. The inheritance of a GI-automorphism has been proved in [39] Thm. 7.2, App., p. 102.

2. The lower central series of \( \pi G \) is given by

\[
\pi G > \gamma_2 \pi G = \gamma_2 G/\gamma_c G > \ldots > \gamma_{c-1} \pi G = \gamma_{c-1} G/\gamma_c G > \gamma_c \pi G \cong 1,
\]

whence \( \mathrm{cl}(\pi G) = c - 1 \).

Let \( n \) be the logarithmic order of \( G \), that is \( |G| = p^n \). If \( |\gamma_c G| = p^s \), then we have \( |\pi G| = (G : \gamma_c G) = p^{n-s} \) and \( \pi G \) is of logarithmic order \( n - s \). Consequently, the coclass of \( \pi G \) is given by \( \text{cc}(\pi G) = (n - s) - (c - 1) = (n - c) - (s - 1) = \text{cc}(G) - (s - 1) \).

The image of the last non-trivial term \( G^{(d-1)} \) of the derived series of \( G \) under \( \pi \) is given by \( \pi G^{(d-1)} = \pi G^{(d-1)} \ker \pi / \gamma_c \pi G \), where \( \ker \pi = \gamma_c G \). If we denote by \( d' := \text{dil}(\pi G) \) the derived length of \( \pi G \), then the derived series of \( \pi G \) is given by

\[
\pi G = G^{(0)} > \pi G^{(1)} > \ldots > \pi G^{(d-1)} > \pi G^{(d')} = 1,
\]

where \( d' < d \) if \( G^{(d-1)} \leq \gamma_c \), and \( d' = d \) otherwise.

3. If the order of \( G \) is given by \( |G| = p^n \), then the two-step centralizer of \( G \) satisfies the condition \( [\chi_2 G, \gamma_2 G] = \gamma_{m-k} G \), where \( k := k(G) \leq m - 4 \) denotes the defect of \( G \).

Application of the epimorphism \( \pi \) yields

\[
[\pi \chi_2 G, \pi \gamma_2 G] = \pi [\chi_2 G, \gamma_2 G] = \pi \gamma_{m-k} G = \gamma_{m-k} \pi G,
\]

where

\[
\gamma_{m-k} \pi G = \begin{cases} 1 & \text{if } k = 0, \\ \gamma_{(m-1)-(k-1)} \pi G & \text{if } k \geq 1. \end{cases}
\]

This proves the claim, since the step size for coclass 1 is \( s = 1 \) and thus \( |\pi G| = p^{n-1} \).

Here, we have used that \( \pi \chi_2 G = \chi_2 \pi G \), since applying the surjection \( \pi \) to the equation

\[
\chi_2 G = \{ g \in G \mid [g, u] \in \gamma_4(G) \text{ for all } u \in \gamma_2(G) \}
\]

and observing that \( \pi \gamma_2 G = \gamma_2 \pi G \) and \( \pi \gamma_4 G = \gamma_4 \pi G \) yields

\[
\pi \chi_2 G = \{ \pi g \in \pi G \mid [\pi g, \pi u] \in \pi \gamma_4 G \text{ for all } \pi u \in \pi \gamma_2 G \}.
\]

\[ \square \]

4. Proof of the main results

We are now in the position to prove Theorem 1.1 and Corollary 1.1 simultaneously. The dominant part of the proof is valid for any number field \( K \) and admits two possibilities \( \ell_5 K \in \{2, 3\} \) for the length of its 5-class tower. The final specialization to a real quadratic field \( K = \mathbb{Q}(\sqrt{d}) \) with discriminant \( d > 0 \) will enforce the fixed length \( \ell_5 K = 3 \).

**Proof.** Let \( K \) be an arbitrary algebraic number field with 5-class group \( \text{Cl}_5 K \cong [5, 5] \) and 5-capitulation type \( \kappa(K) = (\ker j_{L_i/K})_{1 \leq i \leq 6} \cong (1, 0^{5}) \) in its six unramified cyclic quintic extensions \( L_1, \ldots, L_6 \), and suppose that the 5-class groups of the latter are given by \( \tau(K) = (\text{Cl}_5 L_i)_{1 \leq i \leq 6} \cong ([5], [5, 5], [5, 5]^{5}) \).

Then the restricted Artin pattern of \( K \) is \( \text{AP}(K) = (\tau(K), \kappa(K)) \) and, by Theorem 2.1 Formula 2.6, \( \kappa(K) \) constitutes the translation from number theory to group theory, \( \text{AP}(K) \) coincides with the restricted Artin pattern \( \text{AP}(\mathcal{G}) = (\tau(\mathcal{G}), \kappa(\mathcal{G})) \) of the second 5-class group \( \mathcal{G} = G^2_5 K \), where \( \tau(\mathcal{G}) = (M_i/M_i')_{1 \leq i \leq 6} \) and \( \kappa(\mathcal{G}) = (\ker T_{\mathcal{G}, M_i})_{1 \leq i \leq 6} \) in terms of the six maximal subgroups \( M_1, \ldots, M_6 \) of \( \mathcal{G} \) and the Artin transfers \( T_{\mathcal{G}, M_i} \).

According to Formula 1.1, \( \mathcal{G} \) possesses the abelianization \( \mathcal{G}/\mathcal{G}' \cong \text{Cl}_5 K \cong [5, 5] \). Hence, the metabelian 5-group \( \mathcal{G} \) must be a descendant of the abelian 5-group \( [5^2, 2] \cong [5, 5] \), and for identifying \( \mathcal{G} \) by the strategy of pattern recognition via Artin transfers we therefore have to start the p-group generation algorithm [18] at the root \( R = (5^2, 2) \) and to construct the descendant tree \( T(R) \), always looking for the assigned search pattern \( \text{AP}(\mathcal{G}) \).
The recursive steps of this algorithm by Newman [33] and O’Brien [35] may be monitored on the metabelian skeleton of the coclass-1 subtree $T^1(R)$ in [25, Fig. 3.3, p. 425], on the interface between coclass 1 and 2 in [25, Fig. 3.8, p. 448], and on the pruned descendant tree containing the decisive bifurcation in Figure 1.

In each step, a parent $\pi(G)$ gives rise to several children $G$, and the TTT $\tau(G) \geq \tau(\pi(G))$ is isotonic with respect to the partial order $G > \pi(G)$ induced by the tree edges $G \rightarrow \pi(G)$, whereas the TKT $\kappa(G) \leq \kappa(\pi(G))$ is antitonic, by the fundamental monotony result in Theorem 5.1

The pruning process will run parallel to the recursive tree construction in the following way. A vertex with a first TTT component $\tau_1 > [25, 5, 5, 5]$ or with a higher TTT component $\tau_i > [5, 5]$, for some $2 \leq i \leq 6$, must be discarded together with all its descendants, since their TTT $\tau$ will contain an inadequate component. Similarly, a vertex having any forbidden TKT $\kappa$ different from the only two admissible TKTs, $\kappa \sim (1, 0^5)$ and the biggest possible $\kappa = (0^6)$, must be cancelled together with the entire set of its descendants, since their TKT $\kappa$ will also be forbidden.

An important additional filter must be used to eliminate the numerous metabelian 5-groups of maximal class with positive defect of commutativity, $k \geq 1$, although they share the common admissible TKT $\kappa = (0^6)$, by [24] Thm. 2.5.(3), p. 479. However, all descendants of a parent with $k \geq 1$ will also have $k \geq 1$, by item (3) of Proposition 3.1, Formula (3.8), and a metabelian group of maximal class with $k \geq 1$ reveals a total stabilization of all components of the restricted Artin pattern, according to Theorem [33] Thm. 6.2.(2), p. 92. With the aid of Theorem [24] Formula 6.4, we conclude that non-metabelian 5-groups $G$ of any coclass, whose metabelianization $G/G''$ is of maximal class with $k \geq 1$, will also have the TKT $\kappa = (0^6)$ (and not the desired TKT $\kappa \sim (1, 0^5)$) and, due to $k \geq 1$, the inadequate first TTT component which was determined in Theorem 2.2 (A metabelian $p$-group of maximal class with order $p^m$ has defect $k \geq 1$ if and only if $|\tau| < m - 1$).

After these preliminary considerations, we execute the actual steps for finding successive approximations in form of class-$c$ quotients $G/\gamma_{c+1}G$ for the 5-class tower group $G := G_5^cK$ of the field $K$. The steps are summarized in Table 1.

- The abelian root $R = \langle 5^2, 2 \rangle \simeq C_5 \times C_5$ is the class-1 quotient $G/\gamma_2G$ of $G$, as shown by Formula (1.2). It has $\tau = (5^6)$, $\kappa = (0^6)$, and gives rise to the extra special 5-groups as its 2 children, the capable $\langle 5^3, 3 \rangle \simeq G_5^3(0, 0)$ with $\tau = ([5, 5]^6)$, and admissible $\kappa = (0^6)$, and the terminal $\langle 5^3, 4 \rangle \simeq G_5^3(0, 1)$ with $\tau \sim ([5, 5], [25]^5)$, and forbidden $\kappa = (1^6)$.

  (For a real quadratic field $K$, the group $\langle 5^3, 4 \rangle$ cannot occur as $G_5^3K$ for the additional reason that it is not a $\sigma$-group.)

- The compulsory next parent $\langle 5^3, 3 \rangle \simeq G_5^3(0, 0)$ is the class-2 quotient $G/\gamma_3G$ of $G$ and reveals a bifurcation [26] § 8, p. 168 with 4 metabelian children of step size 1 [25, Fig. 3.3, p. 425], and 12 metabelian children of step size 2 [23, Fig. 3.8, p. 448].

  Among the former, we have a capable vertex $\langle 5^4, 7 \rangle$ with admissible $\kappa = (0^6)$, a single leaf $\langle 5^4, 8 \rangle$ with the desired $\kappa \sim (1, 0^5)$ but too small $\tau \sim ([5, 5, 5], [5, 5]^5)$, and two leaves $\langle 5^4, 9 | 10 \rangle$ with forbidden $\kappa \sim (2, 0^5)$.

  Among the latter, which are of coclass 2, the 11 groups $\langle 5^4, 4 \ldots 14 \rangle$ have forbidden TKTs, and only the group $\langle 5^4, 3 \rangle$ has admissible $\kappa = (0^6)$. However, the last five components of the TTT $\tau = ([5, 5, 5]^6)$ disqualify the group as a possible class-3 quotient of $G$.

- For the class-3 quotient $G/\gamma_4G$ of $G$ we have to take $\langle 5^4, 7 \rangle \simeq G_5^4(0, 0)$ which is the next parent. It has 9 metabelian children, all of step size 1. The capable vertex $\langle 5^5, 30 \rangle$ has admissible $\kappa = (0^6)$. The leaf $\langle 5^5, 31 \rangle$ has the desired $\kappa \sim (1, 0^5)$ but too small $\tau \sim ([5, 5, 5], [5, 5]^5)$. The leaf $\langle 5^5, 32 \rangle$ has forbidden $\kappa \sim (2, 0^5)$, and the 6 groups $\langle 5^5, 33 \ldots 38 \rangle$ have positive defect of commutativity $k = 1$.

  (For a real quadratic field $K$, the groups $\langle 5^5, 31 \ldots 38 \rangle$ cannot occur as $G_5^3K$ for the additional reason that they are not $\sigma$-groups.)

- Now we arrive at the crucial bifurcation [24] § 8, p. 168 of the mandatory next parent $\langle 5^5, 30 \rangle \simeq G_5^5(0, 0)$ which is the class-4 quotient $G/\gamma_5G$ of $G$. It has 21 children of step size 1 (13 of them metabelian) and 115 non-metabelian children of step size 2.
Among the former, we have a capable vertex \((5^6, 630)\) with admissible \(\kappa = (0^6)\), 4 vertices \((5^6, 631 \ldots 634)\) with forbidden \(\kappa \sim (2, 0^5)\), a single group \((5^6, 635)\) with both, the desired \(\kappa \sim (1, 0^5)\) and the desired \(\tau \sim ([25, 5, 5, 5], [5, 5]^5)\), and 7 groups \((5^6, 636 \ldots 642)\) with \(k = 1\).

Among the latter, which are of coclass 2, we have 3 capable vertices \((5^7, 360|372|384)\) with admissible \(\kappa = (0^6)\), 5 leaves \((5^7, 361|373|374|385|386)\) with both, the desired \(\kappa \sim (1, 0^5)\) and the desired \(\tau \sim ([25, 5, 5, 5], [5, 5]^5)\), 32 vertices \((5^7, n)\), where \(n\) is listed in Table 1 with forbidden \(\kappa \sim (2, 0^5)\), and 75 vertices \((5^7, 392 \ldots 466)\) with \(k \geq 1\).

- To make sure that \((5^6, 635) \simeq G_0^5(0, 1)\) is the unique possibility for the metabelianization \(G/G''\) of \(G\), we have to check the next parent \((5^6, 630) \simeq G_0^5(0, 0)\). It has 12 children of step size 1 (9 of them metabelian), but either their \(\tau \sim ([25, 25, 5, 5], [5, 5]^5)\) is too big or they have \(k = 1\). Thus, the break-off condition on the coclass-1 tree is reached.

- It remains to prove that \((5^7, 361|373|374|385|386)\) are the only 5 non-metabelian possibilities for \(G\). For this purpose, we must check the roots \((5^7, 360|372|384)\) of 3 non-metabelian coclass-2 trees, which possess 14, resp. 20, resp. 20, children of step size 1, but either their \(\tau \sim ([25, 25, 5, 5], [5, 5]^5)\) is too big or they have \(k \geq 1\).

The proof for a real quadratic field \(K\) will be finished in Theorem 6.3.

Table 1. Descendants of class-c quotients \(G/\gamma_{c+1}G\) of the 5-class tower group \(G\)

| \(c\) | \(G/\gamma_{c+1}G\) | \# of descendants | \(\kappa = (0^6)\) | \(\kappa \sim (1, 0^5)\) | \(\kappa \sim (2, 0^4)\) | \(\kappa = (0^6)\) |
|-----|-----------------|-----------------|-----------|----------------|----------------|-----------|
| 1   | 5^2             | 2/1             | 1 1 1     | 1              | 8              | 2 10      |
| 2   | 5^4             | 4/1; 12/6       | 1 1 7     | 2              | 3              | 12 6      |
| 3   | 5^3             | 9/2             | 1 1 30    | 4              | 631 \ldots 634 | 15 636 \ldots 650 |
| 4   | 5^5             | 21/2; 115/13    | 1 1 630   | 3              | 361 \ldots 362 | 32 352 \ldots 359 | 75 392 \ldots 466 |
| 5   | 5^6             | 12/2            | 1 1 1287  | 1 1 1288       | 1 1286         | 9 1289 \ldots 1297 |
| 5   | 5^7             | 14/2            | 1 1 2     | 2 1 4          | 1 13           | 10 5 \ldots 14 |
| 5^4 | 372             | 20/2            | 1 1 2     | 1 1 5          | 3 1\[3/4]     | 15 6 \ldots 20 |
| 5^4 | 384             | 20/2            | 1 1 2     | 1 1 5          | 3 1\[3/4]     | 15 6 \ldots 20 |

Remark 4.1. It is very important to point out that, for the sake of homogeneity, we have conducted both, the search for the metabelianization \(\mathfrak{G} = G/G''\) of the 5-class tower group \(G\), and the search for \(G\) itself, within the frame of the \(p\)-group generation algorithm. In two previous papers, we have developed the tools for finding the second 5-class group \(\mathfrak{G}\) much more directly: The metabelian skeleton of the coclass tree \(\mathcal{T}((25, 2))\) in [25, Fig. 3.3, p. 425] is embedded within a sort of coordinate system with the TKT \(\kappa\) as its horizontal axis and the polarized first TTT component \(\tau_1\) as its vertical axis. According to [24 Thm. 2.5.(3), p. 479], the TKT \(\kappa(\mathfrak{G}) \sim (1, 0^5)\) uniquely determines the parameters \(w = 1, z = 0,\) and \(k = 0\) of the metabelian 5-group \(\mathfrak{G} \simeq G^5_w(z, w) = G^5_0(0, 1),\) since \(k = 0\) if and only if \(a\) is the empty family. As second input data we do not even need the exact TTT \(\tau(\mathfrak{G}) = ([25, 5, 5, 5], [5, 5]^5)\). The order of the polarized first TTT component \(|\tau_1| = 25 \cdot 5 \cdot 5 \cdot 5 = 5^5\) sufficiently, since according to [23 Thm. 3.1.(3), p. 475], the relation \(|\tau_1| = |M_1/M'_1| = 5^{m-k-1} = 5^{m-1}\) uniquely determines the index of nilpotency as \(m = 6\). Therefore, we have \(\mathfrak{G} \simeq G_0^5(0, 1),\) and this is exactly the group \((5^6, 635)\).
5. Relation rank and generator rank

**Theorem 5.1.** (Shafarevich) Let $p$ be a prime number and denote by $\zeta$ a primitive $p$th root of unity. Let $K$ be a number field with signature $(r_1, r_2)$ and torsionfree Dirichlet unit rank $r = r_1 + r_2 - 1$, and let $S$ be a finite set of non-archimedean or real archimedean places of $K$. Assume that no place in $S$ divides $p$.

Then the relation rank $d_2G_S := \dim_{\mathbb{F}_p} H^2(G_S, \mathbb{F}_p)$ of the Galois group $G_S := \text{Gal}(K_S|K)$ of the maximal pro-$p$ extension $K_S$ of $K$ which is unramified outside of $S$ is bounded from above by

$$d_2G_S \leq \begin{cases} d_1G_S + r & \text{if } S \neq \emptyset \text{ or } \zeta \not\in K, \\ d_1G_S + r + 1 & \text{if } S = \emptyset \text{ and } \zeta \in K, \end{cases}$$

where $d_1G_S := \dim_{\mathbb{F}_p} H^1(G_S, \mathbb{F}_p)$ denotes the generator rank of $G_S$.

**Proof.** The original statement in [36, Thm. 6, (18')] contained a serious misprint which was corrected in [29, Thm. 5.5, p. 28]. □

6. Covers and Shafarevich covers

We begin with a purely group theoretic concept, which aids in getting an overview of all extensions of a particular kind of an assigned $p$-group.

**Definition 6.1.** Let $p$ be a prime and $\mathfrak{G}$ be a finite metabelian $p$-group. By the **cover** of $\mathfrak{G}$ we understand the set of all (isomorphism classes of) finite $p$-groups whose second derived quotient is isomorphic to $\mathfrak{G}$:

$$(6.1) \quad \text{cov}(\mathfrak{G}) := \{ G \mid \text{ord}(G) < \infty, G/G'' \cong \mathfrak{G} \}.$$ 

By eliminating the finiteness condition, we obtain the **complete cover** of $\mathfrak{G}$,

$$(6.2) \quad \text{cov}_c(\mathfrak{G}) := \{ G \mid G/G'' \cong \mathfrak{G} \}.$$ 

**Remark 6.1.** The unique metabelian element of $\text{cov}(\mathfrak{G})$ is the isomorphism class of $\mathfrak{G}$ itself.

**Theorem 6.1.** The cover of the metabelian $5$-group $\langle 15625, 635 \rangle$ consists of 6 elements,

$$(6.3) \quad \text{cov}(\langle 15625, 635 \rangle) = \{ \langle 15625, 635 \rangle \} \cup \{ \langle 78125, n \rangle \mid n \in \{ 361, 373, 374, 385, 386 \} \}.$$ 

**Proof.** This is a consequence of the presentations in Formulas (7.1) and (7.2) together with §4. □

**Remark 6.2.** We shall not make essential use of the complete cover in this article. The only reason for its introduction is the possibility to express certain assertions in a more general way.

**Theorem 6.2.** Let $\mathfrak{G}$ be a finite metabelian $p$-group. Then all elements of the complete cover of $\mathfrak{G}$ share a common restricted Artin pattern:

$$(6.4) \quad \text{AP}(G) = \text{AP}(\mathfrak{G}), \quad \text{for all } G \in \text{cov}_c(\mathfrak{G}).$$

**Proof.** This is the Main Theorem of [30, Thm. 5.4, p. 86]. □

Motivated by the Shafarevich Theorem 5.1, we connect the group theoretic cover concept with arithmetical information, which will be useful for identifying the $p$-class tower group of an assigned number field.

**Definition 6.2.** Let $p$ be a prime and $K$ be a number field with $p$-class rank $q := d_1(\text{Cl}_p(K))$, torsionfree Dirichlet unit rank $r$, and the second $p$-class group $\mathfrak{G} := G^2_pK$. By the **Shafarevich cover**, $\text{cov}(\mathfrak{G}, K)$, of $\mathfrak{G}$ with respect to $K$ we understand the subset of $\text{cov}(\mathfrak{G})$ whose elements $G$ satisfy the following condition for their relation rank:
where the relator word $W$ of these groups are given by
\[(\text{identification), we give the descendant numbers of some relevant capable vertices in the format}
\]
\[
\text{produced by the ANUPQ package \[14\] of GAP \[15\] and MAGMA \[22\]. For addition ease of}
\]
\[
\text{G_k vertices with defect relative identifiers in the form}
\]
\[
\text{brackets, where we omit the order, which is given on the left hand scale. Starting with order 5}
\]
\[
\text{metabelian groups. The symbol } 2^*, \text{metabelian group with bicyclic centre of type (5}
\]
\[
\text{have derived length } dl(G) = 3. The big contour square } \square \text{ denotes the abelian root of the tree,}
\]
\[
\text{full discs } \bullet \text{ denote metabelian groups with cyclic centre of order 5, a contour circle}
\]
\[
\text{denotes a metabelian group with bicyclic centre of type (5, 5), and smaller contour squares } \square \text{ denote non-}
\]
\[
\text{metabelian groups. The symbol } 2^* \text{ means a batch of two siblings with common parent, where only}
\]
\[
\text{one vertex is drawn}
\]
\[
\text{Up to order } 5^7, \text{vertices are labelled by their SmallGroups Library identifiers \[4, 5\] in angle}
\]
\[
\text{brackets, where we omit the order, which is given on the left hand scale. Starting with order 5^8,}
\]
\[
\text{relative identifiers in the form } -\#;s; n, \text{ with step size } s \text{ and counter } n, \text{ are used as in the output}
\]
\[
\text{produced by the ANUPQ package \[14\] of GAP \[15\] and MAGMA \[22\]. For additional ease of}
\]
\[
\text{identification, we give the descendant numbers of some relevant capable vertices in the format}
\]
\[
\text{(N_1/C_1; \ldots; N_\nu/C_\nu) as described in \[20\] (34), p.180], where } \nu \text{ denotes the nuclear rank.}
\]
\[
\text{The diagram in Figure 1 visualizes the lattice of all normal subgroups of the 5-class tower groups}
\]
\[
\text{G}_n := (78125, n) \text{ with } n \in \{361, 373, 374, 385, 386\}. Polycyclic power commutator presentations}
\]
\[
\text{of these groups are given by}
\]
\[
G_n = \langle x, y, s_2, s_3, s_4, s_5, u_5 \mid
\]
\[
\text{s_2 = [y, x], s_3 = [s_2, x], s_4 = [s_3, x], s_5 = [s_4, x],}
\]
\[
x^5 = W, y^5 = s_3^4, u_5 = [s_3, y] = [s_4, y], [s_3, s_2] = u_5^3 \rangle,
\]
\[
\text{where the relator word } W \text{ for the fifth power of the first generator } x \text{ is decisive:}
\]
Three Stage Towers of 5-Class Fields

\[ W = \begin{cases} 
  s_5 & \text{if } n = 361, \\
  s_5u_5 & \text{if } n = 373, \\
  s_5^2u_5 & \text{if } n = 374, \\
  s_5u_5^2 & \text{if } n = 385, \\
  s_5^2u_5^2 & \text{if } n = 386. 
\end{cases} \]

Figure 1. Pruned descendant tree of the abelian root \( \langle 25, 2 \rangle \)
The presentation for the second derived quotient of $G_n$ is obtained by putting $u_5 := 1$. Both resulting relator words $W = s_5$ and $W = s_5^2$ yield the same metabelian group $\langle 15625, 635 \rangle$.

8. Acknowledgements

The author gratefully acknowledges that his research is supported by the Austrian Science Fund (FWF): P 26008-N25.

References

[1] E. Artin, Beweis des allgemeinen Reziprozitätsgesetzes, Abh. Math. Sem. Univ. Hamburg 5 (1927), 353–363, DOI 10.1007/BF02952531.

[2] E. Artin, Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, Abh. Math. Sem. Univ. Hamburg 7 (1929), 46–51, DOI 10.1007/BF02941159.

[3] Y. Berkovich, Groups of prime power order, Vol. I, De Gruyter Expositions in Mathematics, Vol. 46, Walter de Gruyter, Berlin, New York, 2008.
[4] H. U. Besche, B. Eick and E. A. O'Brien, *A millennium project: constructing small groups*, Int. J. Algebra Comput. 12 (2002), 623-644, DOI 10.1142/s0218196702001115.

[5] H. U. Besche, B. Eick, and E. A. O'Brien, *The SmallGroups Library — a Library of Groups of Small Order*, 2005, an accepted and refereed GAP package, available also in MAGMA.

[6] N. Blackburn, *On a special class of p-groups*, Acta Math. 100 (1958), 45–92.

[7] W. Bosma, J. Cannon, and C. Playoust, *The Magna algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[8] W. Bosma, J. J. Cannon, C. Fieker, and A. Steels (eds.), *Handbook of Magma functions* (Edition 2.21, Sydney, 2015).

[9] N. Boston and H. Nover, *Computing pro-p Galois groups*, Proceedings of ANTS 2006, Lecture Notes in Computer Science 4076, 1–10, Springer-Verlag Berlin Heidelberg, 2006.

[10] M. R. Bush, *Computation of Galois groups associated to the 2-class towers of some quadratic fields*, J. Number Theory 100 (2003), 313–325.

[11] M. R. Bush and D. C. Mayer, *3-class field towers of exact length 3*, J. Number Theory 147 (2015), 766–777, DOI 10.1016/j.jnt.2014.08.010.

[12] C. Fieker, *Computing class fields via the Artin map*, Math. Comp. 70 (2001), no. 235, 1293–1303.

[13] Ph. Furtwängler, *Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 7 (1929), 14–36.

[14] G. Gamble, W. Nickel and E. A. O'Brien, *ANU p-Quotient — p-Quotient and p-Group Generation Algorithms*, 2006, an accepted GAP package, available also in MAGMA.

[15] The GAP Group, *GAP — Groups, Algorithms, and Programming — a System for Computational Discrete Algebra*, Version 4.7.8, Aachen, Braunschweig, Fort Collins, St. Andrews, 2015, (http://www.gap-system.org/).

[16] E. S. Golod and I. R. Shafarevich, *On the class field tower* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 261–272. (English transl. in Amer. Math. Soc. Transl. (2) 48 (1965), 91–102.)

[17] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II: Reziprozitätsgesetz*, Jber. der DMV 6 (1930), 1–204

[18] D. F. Holt, B. Eick and E. A. O'Brien, *Handbook of computational group theory*, Discrete mathematics and its applications, Chapman and Hall/CRC Press, 2005.

[19] B. Huppert, *Endliche Gruppen I*, Grundl. Math. Wiss., Vol. 134, Springer-Verlag, Berlin, Heidelberg, New York, 1979.

[20] H. Kisilevsky, *Number fields with class number congruent to 4 mod 8 and Hilbert’s theorem 94*, J. Number Theory 8 (1976), 271–279.

[21] H. Koch und B. B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Astérisque 24–25 (1975), 57–67.

[22] The MAGMA Group, *MAGMA Computational Algebra System*, Version 2.21-11, Sydney, 2016, (http://magma.maths.usyd.edu.au/).

[23] D. C. Mayer, *The second p-class group of a number field*, Int. J. Number Theory 8 (2012), no. 2, 471–505, DOI 10.1142/S179304211250025X.

[24] D. C. Mayer, *Transfers of metabelian p-groups*, Monatsh. Math. 166 (2012), no. 3–4, 467–495, DOI 10.1007/s00605-010-0277-x.

[25] D. C. Mayer, *The distribution of second p-class groups on coclass graphs*, Journal de Théorie des Nombres de Bordeaux 25 (2013), no. 2, 401–456, DOI 10.5802/jtnb.842.

[26] D. C. Mayer, *Periodic bifurcations in descendant trees of finite p-groups*, Adv. Pure Math. 5 (2015), no. 4, 162–195, DOI 10.4236/apm.2015.54020, Special Issue on Group Theory, March 2015.

[27] D. C. Mayer, *Index-p abelianization data of p-class tower groups*, Adv. Pure Math. 5 (2015) no. 5, 286–313, DOI 10.4236/apm.2015.55029, Special Issue on Number Theory and Cryptography, April 2015.

[28] D. C. Mayer, *Periodic sequences of p-class tower groups*, J. Appl. Math. Phys. 3 (2015), no. 7, 746–756, DOI 10.4246/jamp.2015.37090.

[29] D. C. Mayer, *New number fields with known p-class tower*, Tatra Mountains Math. Publ. 64 (2015), 21 – 57, DOI 10.1515/tmmp-2015-0040, Special Issue on Number Theory and Cryptology ’15.

[30] D. C. Mayer, *Artin transfer patterns on descendant trees of finite p-groups*, Adv. Pure Math. 6 (2016), no. 2, 66 – 104, DOI 10.4236/apm.2016.62008, Special Issue on Group Theory Research, January 2016.

[31] R. J. Miech, *Metabelian p-groups of maximal class*, Trans. Amer. Math. Soc. 152 (1970), 331–373.

[32] K. Miyake, *Algebraic investigations of Hilbert’s Theorem 94, the principal ideal theorem and the capitulation problem*, Expo. Math. 7 (1989), 289–346.

[33] M. F. Newman, *Determination of groups of prime-power order*, pp. 73–84, in: Group Theory, Canberra, 1975, Lecture Notes in Math., vol. 573, Springer, Berlin, 1977.

[34] H. Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group C2 × C2 × C2*, J. Number Theory 129 (2009), 231–245.

[35] E. A. O’Brien, *The p-group generation algorithm*, J. Symbolic Comput. 9 (1990), 677–698, DOI 10.1016/S0747-7171(80)80082-X.
[36] I. R. Shafarevich, *Extensions with prescribed ramification points* (Russian), Publ. Math., Inst. Hautes Études Sci. 18 (1964), 71–95. (English transl. by J. W. S. Cassels in Amer. Math. Soc. Transl., II. Ser., 59 (1966), 128–149.)

[37] A. Scholz und O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperzirk*, J. Reine Angew. Math. 171 (1934), 19–41.

Naglergasse 53, 8010 Graz, Austria

E-mail address: algebraic.number.theory@algebra.at

URL: http://www.algebra.at