THE HILBERT–GRUNWALD SPECIALIZATION PROPERTY OVER NUMBER FIELDS

JOACHIM KÖNIG AND DANNY NEFTIN

Abstract. Given a finite group $G$ and a number field $K$, we investigate the following question: Does there exist a Galois extension $E/K(t)$ with group $G$ whose set of specializations yields solutions to all Grunwald problems for the group $G$, outside a finite set of primes? Following previous work, such a Galois extension would be said to have the “Hilbert–Grunwald property”. In this paper we reach a complete classification of groups $G$ which admit an extension with the Hilbert–Grunwald property over fields such as $K = \mathbb{Q}$. We thereby also complete the determination of the “local dimension” of finite groups over $\mathbb{Q}$.

1. Introduction and main results

Given a number field $K$, a finite group $G$, a finite set $S$ of primes of $K$ and for each $p \in S$ a Galois extension $L(p)/K_p$ whose Galois group embeds into $G$, the Grunwald problem $(G, (L(p)/K_p), p \in S)$ is the question whether there exists a Galois extension of $K$ with group $G$ whose completion at $p$ equals $L(p)/K_p$ for each $p \in S$. Such an extension is then called a solution to the underlying Grunwald problem. Following [18] and [19], we say that a Galois extension $E/F$ of (transcendence degree $d \geq 1$) function fields over a number field $K$ with group $G$ has the Hilbert–Grunwald property if the following holds:

(HG) There exists a finite set $S_0$ of primes of $K$ such that every Grunwald problem $(G, (L(p)/K_p), p \in S)$, with $S$ disjoint from $S_0$, has a solution inside the set of specializations $E_{t_0}/K$ of $E/F$ at degree-1 places $t_0$ of $K$.

The terminology was introduced (with a more restrictive meaning) in [18], which proved the following: Given any $K$-regular $G$-extension $E/K(t)$, there exists a finite set $S_0$ of primes of $K$ such that for every finite set $S$ of primes disjoint from $S_0$ and every unramified Grunwald problem on $S$ (i.e., where all the prescribed local extensions are unramified), there exists a solution inside the set of specializations of $E/K(t)$.
Extending this property to the case of ramified Grunwald problems meets some obvious obstacles. These come (among others) from the so-called Specialization Inertia Theorem (cf. Proposition 2.1), which, as a special case, implies that primes \( p \) of \( K \) for which no branch point of \( E/K(t) \) is \( K_p \)-rational cannot ramify in any specialization of \( E/K(t) \) (with possibly finitely many exceptional \( p \)). Using this fact, \[20\] shows that for every group \( G \) which occurs as the Galois group of a \( K \)-regular extension \( E/K(t) \), one can construct another \( K \)-regular \( G \)-extension \( \tilde{E}/K(t) \) which does not have the Hilbert–Grunwald property.

In view of this, it is natural to investigate the Hilbert–Grunwald property not with respect to a given extension, but with respect to merely a given group (and number field), i.e., to ask the following:

Question 1. Given a number field \( K \), for which groups \( G \) does there exist a Galois extension \( E/F \) of transcendence degree 1 over \( K \) with group \( G \) which has the Hilbert–Grunwald property?

In this paper, we will answer Question 1 in full for large classes of number fields \( K \) (in particular, including the case \( K = \mathbb{Q} \)). Concretely we show:

**Theorem 1.1.** Let \( K \subset \mathbb{R} \) be a real number field such that the cyclotomic extensions \( K(\zeta_p) \), with \( p \) running through the prime numbers, are pairwise distinct. Then the following are equivalent:

i) There exists a \( K \)-regular Galois extension \( E/K(t) \) with group \( G \) possessing the Hilbert–Grunwald property.

ii) \( G \) is either a cyclic group of order 2 or an odd prime power; or \( G \) is a Frobenius group whose kernel and complement both are cyclic groups of order either 2 or an odd prime power.

Remark 1. Recall that a Frobenius group \( G \) is a transitive permutation group whose non-identity elements all have either no or one fixed point, with the latter case occurring at least once. It is well known that the set of fixed point free elements of a Frobenius group together with the identity forms a normal subgroup \( K \), called the Frobenius kernel, and that \( G = K \rtimes H \), where \( H \) is a point stabilizer, also known as Frobenius complement. In particular, it is not difficult to see that a semidirect product \( G = K \rtimes H \) is Frobenius with complement \( H \) if and only if \( C_G(k) \cap H = \{1\} \) for every \( k \in K \setminus \{1\} \). With that in mind, a Frobenius group with cyclic kernel and complement of odd prime power order (or order 2) is the same as a semidirect product \( C_p \rtimes C_Q \) of two cyclic groups of prime power order, where \( C_Q \) acts as a group.

---

\[1\]This is a consequence of Theorem 3.1 and Proposition 3.5 of \[20\], together with the Specialization Inertia Theorem.
of automorphisms not only on \( C_P \) but also on its prime-order subgroup (call that prime \( p \)). Since \( \text{Aut}(C_P) \) and \( \text{Aut}(C_p) \) are cyclic, the latter of order \( p - 1 \), which is also the prime-to-\( p \) part of the further, it follows that our condition is equivalent to \( G \cong C_P \rtimes C_Q \), where \( P \) and \( Q \) are of coprime prime power order (or order 2) and \( C_Q \) acts as a group of automorphisms on \( C_P \). This is how Condition b) above is worded and used in Section 4.

Over more general number fields, determining the precise list of groups \( G \) with the Hilbert–Grunwald property can vary in somewhat delicate ways. Just to give one example, over a field \( K \) containing the \( n \)-th roots of unity, the extension \( K(t^{1/n})/K \) is Galois with group \( C_n \) and is a generic extension for this group, meaning that all \( C_n \)-extensions, and in particular all possible local behaviors, occur among its specializations. In particular, it has the Hilbert–Grunwald property over \( K \), whereas Theorem 1.1 shows that, for most \( n \), there is no such extension over fields such as \( \mathbb{Q} \). We will see in the proof of Theorem 1.1 that the implication ii)\( \Rightarrow \)i) always holds, see Theorem 1.3, whereas conversely a group with a non-cyclic abelian subgroup can never have (a transcendence degree-1 extension with) the Hilbert–Grunwald property, see Corollary 3.1. Below, we give one more class of fields over which the groups with the Hilbert–Grunwald property are (almost-)completely determined:

**Theorem 1.2.** Let \( K \) a number field containing \( \sqrt{-1} \) such that the cyclotomic extensions \( K(\zeta_p) \), with \( p \) running through the prime numbers, are pairwise distinct. Suppose \( G \) is a finite group for which there exists a \( K \)-regular \( G \)-extension \( E/K(t) \) with the Hilbert–Grunwald property. Then \( G \) is either a cyclic group of prime power order, a Frobenius group whose kernel and complement are both cyclic of prime power order, or a generalized quaternion group. Moreover, the converse holds as long as \( G \) possesses a generic extension over \( K \).\(^2\)

Question 1 and Theorems 1.1 and 1.2 should be viewed in the broader context of a series of papers investigating (in various senses) the “arithmetic-geometric complexity” of the Galois theory of a given finite group over a given field \( K \). Specifically, the following question is raised in [15] (and formalized in [19]): What is the minimal integer \( d \) such that there exist finitely many \( G \)-extensions \( E_i/F_i \) (\( i = 1, \ldots, r \)) of étale algebras of transcendence degree \( \leq d \) over \( K \) (equivalently, Galois extensions of transcendence degree-\( d \) fields \( E_i/F_i \) with Galois group embedding into \( G \)) whose specializations provide solutions to all Grunwald problems for \( G \), possibly outside

\(^2\)The existence of generic extensions over number fields containing \( \sqrt{-1} \) is known for all of the above groups, except possibly the generalized quaternion groups of order \( 2^k \) (\( k \geq 5 \)); cf. [23, Theorem 2.1] for the cyclic groups, and [14, Theorem 1.4] for the generalized quaternion groups of order 8 and 16.
some finite set of primes? This dimension is called the *Hilbert–Grunwald dimension* $\text{hgd}_K(G)$ of $G$ over $K$. In these terms, Question 1 asks to classify all groups of Hilbert–Grunwald dimension 1. In particular, any result of the form “There is no transcendence degree 1 extension $E/F$ possessing the Hilbert–Grunwald property” is first and foremost a statement about the complexity of the Galois theory of the group $G$: in this case, the local Galois theory of $G$ (i.e., over completions of the field $K$) is too complex to be captured by a one-dimensional object (i.e., covers of curves).

The quantity $\text{hgd}_K(G)$ is intimately connected with the *local dimension* $\text{ld}_K(G)$ of $G$ over $K$ (see again [19]), defined as the minimal integer $d$ such that there exist finitely many $G$-extensions $E_i/F_i$ ($i = 1, \ldots, r$) of transcendence degree $\leq d$ over $K$ such that, for all but finitely many completions $K_p$ of $K$, all Galois extensions $L/K_p$ of group embedding into $G$ occur as a specialization of some $E_i/F_i$ (after base change from $K$ to $K_p$). In this context, [19, Theorem 1] showed that $\text{ld}_K(G) \leq 2$ for all groups $G$ and number fields $K$, while furthermore $\text{ld}_K(G) \leq \text{hgd}_K(G)$ holds trivially with equality possible in general [3]. In fact, in Theorem 4.1 we achieve a full classification of groups $G$ with $\text{ld}_K(G) = \text{hgd}_K(G) = 1$ for fields such as $K = \mathbb{Q}$.

One of our main tools is a result on the local behavior of Galois extensions arising via specialization of a given function field extension, shown in [18] and recalled in Proposition 2.2. It was noted already in [18, Theorem 6.2] that this result implies a negative answer to Question 1 (over any number field $K$) for all groups $G$ possessing a non-cyclic abelian subgroup. In Section 3, we develop this approach further and exhibit some newly discovered obstructions to the Hilbert–Grunwald property (Lemmas 3.2 and 3.3). These, together with the well-known classification of Sylow-cyclic finite groups, suffice to prove the implication i) $\Rightarrow$ ii) in Theorem 1.1.

To show that these are the only obstructions, that is, to obtain the implication ii) $\Rightarrow$ i), we construct function field extensions with prescribed local behavior using the existence of generic extensions [23] and again the specialization criteria obtained in [18]; cf. Section 4.

On the other extreme, when $K$ contains the $p$-th roots of unity for all $p | |G|$, we show the obstructions obtained in Section 3 are also the only obstructions for the Hilbert–Grunwald property for abelian groups, see Theorem 4.6. Our construction makes use of embedding problems for quadratic extensions into cyclic extensions [8, §16.5], following Geyer–Jansen [9] and Arason–Fein–Schacher–Sonn [2], and even uses an idea from the construction of polynomials having a root mod $p$ for all $p$.

This paper is dedicated to Moshe Jarden who greatly influenced our research for many years to come. The authors thank Howard Neur for helpful discussions. The

---

3 If equality holds in general, then the inverse Galois problem has an affirmative answer.
second author is grateful for support of the Israel Science Foundation, grant no. 353/21, and the support and hospitality of the Institute for Advanced Studies.

2. Preliminaries

2.1. Completions of number fields. Let $K$ be a number field. For a prime $p$ of (the ring of integers $\mathcal{O}_K$ of) $K$, let $N(p) := |\mathcal{O}_K/p|$ be its norm, and $K_p$ the completion of $K$ at $p$. Let $\mu$ denote the $e$-th roots of unity in an algebraic closure of $K$, and $\zeta_e \in \mu$ a primitive $e$-th root of unity.

Recall that the Galois group $G_{tr}$ of the maximal tamely ramified extension $M_p$ of $K_p$ is (profinitely) generated by two generators $\sigma$ and $\tau$ subject to the single relation $\sigma^{-1} \tau \sigma = \tau^q$, where $q = N(p)$. Its inertia subgroup is the cyclic group generated by $\tau$, so that the conjugation action of $\sigma$ on $\langle \tau \rangle / \langle \tau^e \rangle$ is equivalent to its action on $\mu$ for all $e$ coprime to $p$. In particular, the abelianization of $G_{tr}$ is isomorphic to $\mu_{q-1} \times \hat{\mathbb{Z}}$, with the inertia group mapping to $\mu_{q-1}$, and furthermore $\mu_{q-1}$ is the group of roots of unity in $K_p$ of order coprime to $p$.

We note that $K_p$ admits a degree $d$ cyclic extension with ramification index $e$ if and only if $\zeta_e \subseteq K_p$. Indeed, in view of the above isomorphism, the cyclic group $C_d$ of order $d$ is the Galois group of an extension with ramification index $e$, for $e$ coprime to $q$, if and only if there exists an epimorphism $\mu_{q-1} \times \hat{\mathbb{Z}} \rightarrow C_d$ which maps $\mu_{q-1}$ to $C_e$. Such an epimorphism exists if and only if $e$ divides $q-1$, that is, if and only if $\zeta_e \subseteq K_p^\times$.

2.2. Basics about function field extensions. Let $R$ be a Dedekind domain with field of fractions $F$, let $E/F$ be a finite Galois extension and $S$ the integral closure of $R$ in $F$. For any prime ideal $p$ of $R$ and any prime ideal $\mathfrak{P}$ of $S$ extending $p$, the specialization of $E/F$ at $\nu$ is the extension $S_{\mathfrak{P}}/R_p$ of residue fields at the respective prime ideals. Note that this specialization is independent of the choice of prime ideal extending $p$ since $E/F$ is Galois. In particular, in the key case of a rational function field $F = K(t)$ over a field $K$, we denote by $E_{t_0}/K$, for $t_0 \in \mathbb{P}^1(K)$, the specialization of $E/K(t)$ at the $K$-rational place $t \mapsto t_0$, i.e., at the ideal $(t - t_0)$ of $K[t - t_0]$. We also denote the set of all specializations $E_{t_0}/K$, for $t_0 \in \mathbb{P}^1(K)$, by $Sp(E/K(t))$.

If $K \subseteq F$ is a field which is algebraically closed in $E$, we say that the extension $E/F$ is $K$-regular.

Now let $K$ be of characteristic zero, and let $E/K(t)$ be a (not necessarily $K$-regular) Galois extension with group $G$. Such an extension has finitely many branch

\footnote{If $t_0 = \infty$, one should read $t - t_0$ as $1/t$.}
points \(p_1, ..., p_r \in \mathbb{P}^1(\overline{K})\), and associated to each branch point \(p_i\) is a unique conjugacy class \(C_i\) of \(G\), corresponding to the automorphism \((t - p_i)^{1/e_i} \mapsto \zeta(t - p_i)^{1/e_i}\) of the Laurent series field \(\overline{K}((t - p_i)^{1/e_i})\), where \(e_i\) is minimal such that \(E\) embeds into \(\overline{K}(((t - p_i)^{1/e_i}))\), and \(\zeta\) is a primitive \(e_i\)-th root of unity. This \(e_i\) is the ramification index at \(p_i\), and equals the order of elements in the class \(C_i\), which in turn are the generators of inertia subgroups at places extending \(t \mapsto p_i\) in \(E\).

2.3. Local behavior of specializations. Let \(K\) be a number field and \(E/K(t)\) a (not necessarily \(K\)-regular) Galois extension with group \(G\), and \(t_0 \in \mathbb{P}^1_K\). We will make extensive use of previous results relating inertia groups, residue fields, etc., at primes \(p\) in the specialized extension \(E_{t_0}/K\) to those in the extension \(E/K(t)\).

In the following proposition we state the well-known criterion of Beckmann [4, Prop. 4.2] relating ramification in Galois extensions of \(K(t)\) to ramification in their specializations. We first introduce some notation: For \(a_0 \in \mathbb{P}^1(\overline{K})\), let \(f \in K[X]\), resp., \(\tilde{f} \in K[\overline{K}]\) be the minimal polynomial of \(a_0\), resp., of \(1/a_0\).\(^5\) Define the intersection multiplicity \(I_p(a, a_0)\) as the \(p\)-adic valuation \(\nu_p(f(a))\) in case \(a_0\) is of non-negative \(p\)-adic valuation, resp., as \(\nu_p(\tilde{f}(1/a))\) otherwise. Obviously, we have \(I_p(a, a_0) \neq 0\) only for finitely many prime ideals \(p\) of \(K\).

**Proposition 2.1.** Let \(K\) be a number field and \(E/K(t)\) be a Galois extension with Galois group \(G\). Suppose \(a \in K\) is not a branch point of \(E/K(t)\). For all but finitely many primes \(p\) of \(K\), with the exceptional set depending on \(E/K(t)\), the following condition is necessary for \(p\) to be ramified in the specialization \(E_{t_0}/K\):

\[
e_i := I_p(t_0, t_i) > 0\text{ for some (unique up to conjugation) branch point } t_i.
\]

Furthermore, the inertia group of a prime extending \(p\) in the specialization \(E_{t_0}/K\) is then conjugate in \(G\) to \((\tau^{t_i})\), where \(\tau\) is a generator of an inertia subgroup over the branch point \(t \mapsto t_i\) of \(E/K(t)\).

**Remark 2.** Note that Proposition 2.1 is often stated with the additional assumption of \(E/K(t)\) being \(K\)-regular, which is however not necessary after possibly increasing the finite set of exceptional primes. Indeed, if \(\kappa\) is the algebraic closure of \(K\) inside \(E\), one may apply the result for the \(\kappa\)-regular extension \(E/\kappa(t)\) and then deduce it for \(E/K(t)\), via noting the following elementary facts: from the definition, inertia groups at a given branch point \(t \mapsto t_i\) are the same in \(E/K(t)\) and in \(E/\kappa(t)\), up to conjugacy in \(G\); furthermore, as long as \(p\) is unramified in \(\kappa/K\), intersection multiplicities at \(p\) and at some (hence any, since \(\kappa/K\) is Galois) prime extending \(p\) in \(\kappa\) are identical; finally, inertia groups at \(p\) in \(E_{t_0}/K\) and \(E_{t_0}/\kappa\) are also identical (up to conjugacy) as long as \(p\) is unramified in \(\kappa/K\).

\(^5\)We define the minimal polynomial of infinity as 1.
Next, we deal with residue fields at ramified primes in specializations. For a Galois extension $E/K(t)$, a value $t_0 \in \mathbb{P}^1_K$ and a prime $p$ of $K$, we use the notation $I_{t_0,p}$ and $D_{t_0,p}$ for the inertia and decomposition group at (a prime extending) $p$ in the residue field extension $E_{t_0}/K$.

The following result is used as the main tool in [18] (and occurs there in a somewhat more general setting as Theorem 4.1). It relates the residue field, decomposition group etc. at ramified primes in specializations to the respective data at a branch point in the underlying function field extension. Just like Proposition 2.1, it is stated only for $K$-regular Galois extensions in [18]; however, its proof makes no use of this regularity assumption other than invoking Proposition 2.1; thus, the assumption may be dropped by Remark 2.5

**Proposition 2.2.** Let $K$ be a number field and $E/K(t)$ a Galois extension with group $G$. Let $t_i \in K \cup \{\infty\}$ be a branch point of $E/K(t)$, and set $E':= E(t_i)$ and $K':= K(t_i)$. Let $p$ be a prime of $K$, away from an explicit finite set of “exceptional” primes depending only on $E/K(t)$, and assume that there exists a prime $p'$ extending $p$ in $K'$ with relative degree 1.

Let $t_0 \in K$ be a non-branch point such that $I_p(t_0,t_i) > 0$. Denote by $I$ and $D$ the inertia and decomposition group at (a fixed place extending) $t \mapsto t_i$ in $E'/K'(t)$. Then the following hold:

i) The completion at $p'$ of $E'_t/K'$ is contained in the completion at $p$ of $E_{t_0}/K$. In particular, the residue extension at $p'$ in $E'_t/K'$ is contained in the residue extension at $p$ in $E_{t_0}/K$.

ii) The identification of the decomposition group $D_{t_0,p}$ with a subgroup of $D$ (up to conjugacy in $G$) fulfills $\varphi(D_{t_0,p}) = D_{t_i,p'}$, where $\varphi : D \to D/I$ is the canonical epimorphism.

In particular, if in addition $I_p(t_0,t_i)$ is coprime to $e_i := |I|$, then the following hold:

iii) The decomposition group $D_{t_0,p}$ equals $\varphi^{-1}(D_{t_i,p'})$ where $\varphi : D \to D/I$ is the canonical epimorphism. Furthermore, the residue extension at $p$ in $E_{t_0}/K$ equals the residue extension at $p'$ in $E'_t/K'$.

The above result, which gives necessary conditions on the local behavior of specializations, is complemented by the following (see [18, Theorem 4.4]), showing that all local extensions of a certain form are indeed realizable.

---

Note that, due to the definition of intersection multiplicity, the existence of such a $p'$ is a necessary condition for $I_p(t_0,t_i) > 0$ for any $t_0 \in K$. 

Proposition 2.3. Let $K$ be a number field, $E/K(t)$ a finite Galois extension, and $t_1 \in \overline{K} \cup \{\infty\}$ a branch point.

Let $D, I,$ and $N/K(t_1)$ be the Galois group, inertia group, and residue extension, respectively, of the completion at $t \mapsto t_1$. Let $\mathfrak{p}$ be a prime away from the finite exceptional set of Proposition 2.2, with a degree 1 prime $\mathfrak{p}'$ of $K(t_1)$ lying over it, and define $D'$ as $\varphi^{-1}(D_{t_1, \mathfrak{p}'})$, with the notation of Proposition 2.2. Let $T_{\mathfrak{p}}/K_{\mathfrak{p}}$ be a $D'$-extension such that $T_{\mathfrak{p}}/K_{\mathfrak{p}} \cong NK(t_1)_{\mathfrak{p}'}/K(t_1)_{\mathfrak{p}'} (\cong NK_{\mathfrak{p}}/K_{\mathfrak{p}})$.

Then there exist infinitely many $t_0 \in K$ such that the completion of $E_{t_0}/K$ at $\mathfrak{p}$ is $T_{\mathfrak{p}}/K_{\mathfrak{p}}$.

Finally, we recall the following well-known result about compatibility of weak approximation and Hilbert’s irreducibility theorem, cf., e.g., [21, Proposition 2.1]. In particular, it justifies treating the Hilbert–Grunwald property “one prime at a time”.

Lemma 2.4. Let $K$ be a number field, $E/K(t)$ a Galois extension with group $G$ and $S$ a finite set of primes of $K$. For each $\mathfrak{p} \in S$, choose a non-branch point $t_\mathfrak{p} \in K_{\mathfrak{p}}$ of $E \cdot K_{\mathfrak{p}}/K_{\mathfrak{p}}(t)$, and denote the specialization at $t_\mathfrak{p}$ by $L_{\mathfrak{p}}/K_{\mathfrak{p}}$. Then there exists $t_0 \in K$ such that $E_{t_0}/K$ has Galois group $G$ and has completion $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ at each prime $\mathfrak{p} \in S$. In particular, if for all but finitely many primes $\mathfrak{p}$ of $K$, every Galois extension of $K_{\mathfrak{p}}$ with group embedding into $G$ is in $Sp(E \cdot K_{\mathfrak{p}}/K_{\mathfrak{p}}(t))$, then $E/K(t)$ has the Hilbert–Grunwald property.

2.4. Embedding problems. Given a Galois extension $L/K$, an embedding problem is an epimorphism $\pi : G \rightarrow \text{Gal}(L/K)$, and a solution is a homomorphism $\psi : G_K \rightarrow G$ such that $\pi \circ \psi$ coincides with the restriction map. A solution is proper if it is surjective. If $\ker \pi$ is contained in the Frattini subgroup of $G$, then the embedding problem $\pi$ is said to be Frattini. In such a case, every solution has to be proper.

3. THREE OBSTRUCTIONS TO LOCAL DIMENSION 1

3.1. Statement of the obstructions. Below, we present three results, Corollary 3.1 and Lemmas 3.2 and 3.3, each of which restricts the possible $K_{\mathfrak{p}}$-specializations of a transcendence degree 1 function field extension $E/F$ over a number field $K$. As will be detailed in the proof of Theorem 4.2 for any “sufficiently complicated” group $G$, these restrictions amount to obstructions to the assertion $\text{ld}_K(G) = 1$; in particular, they ensure that transcendence degree 1 extensions over $K$ with group $G$ can never have the Hilbert–Grunwald property. The three obstructions are, in short, (1) the existence of a non-cyclic abelian subgroup, (2) the existence of an element whose order is not a prime-power, and (3) the existence of an element of order 4.

All of them are applications of Proposition 2.2, the first one already occurred in the
key case $F = K(t)$ in [18, Theorem 6.3], and extended to arbitrary transcendence-degree-1 extensions $E_i/F_i$, $i = 1, \ldots, r$ in [19, Theorem B.1]. The other two, however, are new.

**Corollary 3.1.** Let $G$ be a finite group, and $E_i/F_i$, $i = 1, \ldots, r$, finitely many Galois extensions with group $G$ of transcendence degree 1 function fields over $K$. Then there exists a number field $L \supseteq K$ such that the following holds: If $S$ denotes the set of primes of $K$ which split completely in $L$, then for all $p \in S$ and all degree-1 places $t_0$ of $F_i \cdot K_p$ ($i = 1, \ldots, r$), the specialization $(E_i \cdot K_p)_{t_0}/K_p$ has cyclic decomposition group at $p$.

**Lemma 3.2.** Let $G$ be a finite group, let $q, r$ be distinct prime numbers, and let $K$ be a number field such that $K(\zeta_r)$ does not contain a primitive $q$-th root of unity. Let $E_i/F_i$, $i = 1, \ldots, r$, be finitely many $G$-extensions of transcendence degree 1 function fields over $K$. Then there exists a non-empty Chebotarev set $\mathcal{S}$ of primes $p$ of $K$, completely split in $K(\zeta_r)$, such that the specialization $(E_i \cdot K_p)_{t_0}/K_p$, at any degree-1 place $t_0$ of $F_i \cdot K_p$, for any $i = 1, \ldots, r$, does not fulfill the following condition:

$(E_i \cdot K_p)_{t_0}/K_p$ is tamely ramified of ramification index divisible by $r$, but coprime to $q$; and of residue degree divisible by $q$.

**Lemma 3.3.** Let $G$ be a finite group and let $K \subset \mathbb{R}$ be a real number field. Let $E_i/F_i$, $i = 1, \ldots, r$, be finitely many $G$-extensions of transcendence degree 1 function fields over $K$. Then there exists a non-empty Chebotarev set $\mathcal{S}$ of primes $p$ of $K$ such that, for any $i \in \{1, \ldots, r\}$, the specialization $(E_i \cdot K_p)_{t_0}/K_p$ at any degree-1 place $t_0$ of $F_i \cdot K_p$, does not have inertia group of order 2 which embeds into an order 4 cyclic subgroup of the decomposition group.

We divide the proof of Lemmas 3.2 and 3.3 into three stages. First, we look at the case of a single extension $E/F$ with rational base field $F = K(t)$. Next, we derive the case of an arbitrary (single) extension $E/F$. Finally, we progress to finitely many extensions $E_i/F_i$, $i = 1, \ldots, r$.

**3.2. Proof of Lemmas 3.2 and 3.3** Part 1: The case $r = 1$ and $F_1 = K(t)$. We begin the proof of Lemmas 3.2 and 3.3 by showing that they hold in the special case $r = 1$ and $F := F_1 = K(t)$. Before going into the proofs of the two individual cases, we note that we may furthermore restrict to specializations at non-branch points $t_0$ of $E/K(t)$ (up to excluding finitely many more primes from the respective Chebotarev set $\mathcal{S}$), since the finitely many residue fields at branch points can give ramified completions only at finitely many primes; and that moreover, it suffices to consider $K$-rational specializations $t_0 \in \mathbb{P}^1(K)$ due to Lemma 2.4.
Proof of Lemma 3.2 in the case $F = K(t)$. Let $S'$ be the set of primes of $K$ which split completely in $K(t)$, but not in $K(t')$. Since $K(t')$ is not contained in $K(t)$, this is clearly a non-empty Chebotarev set. Now let $t_1, \ldots, t_r$ be the branch points of $E/K(t)$ and $L/K$ be the Galois closure (over $K$) of the compositum of all residue extensions $E(t_i)/K(t_i)$ at these branch points. Let $S''$ be the set of all primes of $K$ which are unramified in $L(t')/K$ with residue degree coprime to $q$. We claim that $S := S' \cap S''$ is still a non-empty Chebotarev set. Indeed, if a prime $p$ is finite. Up to exempting a finite set of primes, Proposition 2.1 yields the following: $r$ is divisible by $E$ with $t$ coprime to $q$, and residue degree $|D/I|$ divisible by $q$. It suffices to show that $S$ is finite. Up to exponent of a finite set of primes, Proposition 2.1 yields the following: $p$ is a prime $p$ of $K$ for which some specialization $E_{t_0}/K$, with $t_0$ a degree-1 place of $K(t)$, has cyclic inertia group $I$ of order divisible by $r$ and coprime to $q$, and residue degree $|D/I|$ divisible by $q$. It suffices to show that $R \cap S$ is finite. Up to exponent of a finite set of primes, Proposition 2.1 yields the following: $I_p(t_0, t_i)$ of $t_0$ and $t_i$ at $p$ must be positive for some branch point $t_i$ of $E/K(t)$ whose ramification index is divisible by $r$. We first claim that, for $p \in R \cap S$ (up to finitely many), this branch point $t_i$ cannot have ramification index coprime to $q$. Indeed, if it did, then Proposition 2.2 would imply that the only way for $p$ to have residue degree divisible by $q$ in $E_{t_0}/K$ is that there is a prime $p'$ of $K(t_i)$ extending $p$ of relative degree 1 (i.e., $K(t_i)_{p'}$ is identified with $K_p$), and such that the residue degree at $p'$ in $E(t_i)_{t_i}/K(t_i)$ is divisible by $q$. But in this case, the Frobenius of $p$ in $L/K$ is certainly of order divisible by $q$, meaning that $p \notin S$.

Proposition 2.2 thus yields that the only way to obtain a specialization $E_{t_0}/K$ whose decomposition group at $p$ is of order divisible by $qr$ and its ramification index is divisible by $r$ is that the factor $q$ “stems” from the inertia group at $t \mapsto t_i$; i.e., this inertia group contains subgroups $V_1 \leq V_2$ such that $|V_1|$ is divisible by $r$ but not by $q$, $|V_2/V_1|$ is divisible by $q$, $V_1$ surjects onto the inertia group $I$ at $p$ in $E_{t_0}/K$ and $V_2/V_1$ injects into $D/I$ (where $D$ is the decomposition group at $p$ in $E_{t_0}/K$).

But also, since the ramification index at $t \mapsto t_i$ is divisible by $q$, it follows that $\zeta_q$ is contained in the residue extension $E(t_i)_{t_i}$, e.g. by [15, Lemma 2.3]), and thus by Proposition 2.2 also in the completion of $E_{t_0}$ at $p$. But $p$ is non-split in the extension $K(\zeta_q)/K$, whence $D/I$ maps onto a non-trivial subgroup of $\text{Gal}(K(\zeta_q)/K)$.
Finally, this subgroup acts faithfully on the inertia group at $t \mapsto t_i$ via its action on $\mu_q$, and hence (since $|V_1|$ is coprime to $q$) also on $V_2/V_1$, meaning that $D/I$ is non-abelian. This is of course a contradiction, since $D/I$ is always cyclic.

We have therefore shown that, up to excluding finitely many primes (which can be achieved by choosing a suitable proper Chebotarev subset), the set $S$ fulfills the assertion of the theorem.

Proof of Lemma 3.3 in the case $F = K(t)$. Let $S'$ be the set of primes of $K$ which remain inert in $K(\sqrt{-1})$. Let $F/K$ be the Galois closure of the compositum of all residue extensions at branch points of $E/K(t)$. Let $\sigma \in \text{Gal}(F/K)$ be a complex conjugation on $F$ and let $S''$ be the set of primes of $K$ whose Frobenius class in $F/K$ is the class of $\sigma$. It is obvious (upon considering the compositum of $F/K$ and $K(\sqrt{-1})/K$) that $S' \cap S''$ is a non-empty Chebotarev set, so we set $S = S' \cap S''$.

Denote by $R$ the set of primes $p$ of $K$ at which some specialization $E_{t_0}/K$ has inertia group $I = I_{t_0,p}$ of order 2 and decomposition group $D = D_{t_0,p}$ containing a cyclic overgroup of $I$ of order 4. Note that this readily forces $D$ to be cyclic since it centralizes a group $I$ with cyclic quotient. In analogy to the proof of Lemma 3.2 we aim at concluding that $R \cap S$ is finite.

Proposition 2.2 yields once again that for all but finitely many $p \in R$, there must be a branch point $t_i$ and a prime $p'$ extending $p$ of relative degree 1 in $K(t_i)$; furthermore this branch point $t_i$ either has ramification index strictly divisible by 2 and residue extension $E(t_i)/K(t_i)$ of even local degree at $p'$; or it has ramification index divisible by 4.

We now claim that furthermore, for $p \in R \cap S$, each such $t_i$ must be such that the field $K(t_i)$ has a real embedding. Indeed, this is due to the fact that (due to Proposition 2.1 and up to exempting finitely many $p$) for the inertia group at $p$ in the specialization $E_{t_0}/K$ to be a non-trivial subgroup of some inertia group at $t_i$ in $E/K(t)$, it is necessary that $t_0$ and $t_i$ meet at $p$. This in turn implies that the Frobenius of $p$ in the Galois closure of $K(t_i)/K$ is an element fixing at least one conjugate of $t_i$. But since for $p \in S$, this Frobenius class is the class of complex conjugation, its elements have a fixed point if and only if $K(t_i)$ has a real embedding.

We may and will therefore assume $K(t_i) \subset \mathbb{R}$ whenever a particular branch point $t_i$ is chosen in the following.

For $t_i$ as above, let $M := E(t_i)_{t_i}$ be the residue extension at $t_i$, and $L := M \cap \mathbb{R}$. Note the inclusion $K \subseteq K(t_i) \subseteq L$. We now claim the following:

(*) For $p \in R \cap S$ (exempting finitely many), there exists at least one $t_i$ as above such that the extension $M/L$ embeds into a $C_4$-extension.
Since this is trivial if $M = L$, we may assume $M = L(\sqrt{a})$ (with a non-square $a \in L$) for the moment. Let $q$ be a prime of $L$ extending $p'$ of degree 1 (such a prime exists, due to the fact that the Frobenius at $p$ has the same cycle structure as complex conjugation; after all, $M \subset \mathbb{R}$ has a real embedding extending the real embedding of $K(t_i)$). In particular, we may identify $M_q/L_q$ with $M_{p'/K(t_i)p'}$.

Now assume $I_{t_0, q}$ and $D_{t_0, p}$ are cyclic of order 2 and divisible by 4, respectively, which is possible by the choice of $\mathcal{R}$. Since $t_0$ and $t_i$ are assumed to meet at $p'$, in particular they meet at $q$. Consider thus the specialization $(EL)_{t_0}/L$ of $EL/L(t)$ at $t_0$. Since $M_q/L_q$ is cyclic of order 2, the residue degree at $q$ in this specialization is even. Furthermore, the ramification index of $q$ in $(EL)_{t_0} = E_{t_0} \cdot L$ is the same as the one of $p$ in $E_{t_0}$, since we may without loss of generality assume that $p$ is unramified in $L/K$. But the decomposition group at $q$ in $(EL)_{t_0}/L$ is isomorphic to a subgroup of the one at $p$ in $E_{t_0}/K$, and therefore by the above must be cyclic of order divisible by 4. But Proposition 2.2 identifies the decomposition group $D_{t_0, q}$ of $q$ in $(EL)_{t_0}/L$ with a subgroup $U$ of the decomposition group $D$ at $t \mapsto t_i$ in $EL/L(t)$ (namely, a subgroup mapping onto $D_{t, q}$ under the canonical epimorphism $D \to D/I$). Since the order of $D_{t, q}$ is in fact the full residue degree of $EL/L$ at $t_i$ (namely, 2), this yields a subextension $\hat{EL}U$ of the completion $\hat{EL}/L((t - t_i))$ such that $\hat{EL}/\hat{EL}U$ has cyclic Galois group $U$ of order divisible by 4, $\hat{EL}$ has residue field $M$ and $\hat{EL}U$ has residue field $L$. With a suitable parameter $s$ of the Laurent series field $\hat{EL}U$, this extension is then of the form $M((\sqrt{bs})) \supset M((s)) \supset L((s))$ for some even integer $d$ and $b \in M$. In particular, $M((s))/L((s)) = L((s))(\sqrt{a})/L((s))$ embeds into a $C_4$-extension, which is possible if only if $a$ is a sum of two squares in $L((s))$ (cf. [8, Proposition 16.5.1]), and then (via comparing the lowest coefficient) even in $L$; hence $M/L$ also embeds into a $C_4$-extension.

But now note that if $M/L$ were a proper (and then automatically non-real) extension, it could not possibly embed into a $C_4$-extension, or otherwise complex conjugation would have to extend to an order-4 automorphism. Hence, $M = L$ is a real Galois extension of $K(t_i)$. Firstly, since the residue extension $E(t_i)_{t_i}$ at a branch point $t_i$ of ramification index $e$ always contains the $e$-th roots of unity, this already forces $e = 2$. But secondly, $M = L$ implies that for any $p \in \mathcal{S}$, the above chosen prime $p'$ of $K(t_i)$, extending $p$, has an extension to $M$ of degree 1, due to our choice of Frobenius class at $p$ (as in the argument for choosing $p'$). However, due to $M/K(t_i)$ being Galois, this already forces $p'$ to be completely split in $M$. Therefore, the residue extension at $p'$ in $E(t_i)_{t_i}/K(t_i)$ is trivial. Proposition 2.2 then implies

If the two squares happen to have a pole at $s = 0$, this comparison yields a representation of 0 as a sum of two squares in $L$, at least one of which is nonzero. Such a representation of 0 is impossible since $L$ is real.
that for any \( t_0 \in K \) meeting \( t_i \) at \( p \), the decomposition group at \( p \) in \( E_{t_0}/K \) is a subgroup of the inertia group at \( t_i \), and thus of order dividing \( e = 2 \). In particular, this decomposition group cannot contain a cyclic group of order 4. \( \square \)

3.3. Proof of Lemmas 3.2 and 3.3. Part 2: The case \( r = 1 \) and \( F_1 \) arbitrary.

We now extend the proof of Lemmas 3.2 and 3.3 to a single extension \( E/F \) with arbitrary, not necessarily rational base fields \( F \). We will make use of the following technical lemma. For our purposes, we will only need conclusion i), but the proof easily yields ii) as well, which may be of interest by itself.

Lemma 3.4. Let \( K \) be field of characteristic 0 with algebraic closure \( \overline{K} \), and \( F \) a (one-variable) function field over \( K \). Let \( \mathcal{R} \) be a finite set of places of \( F \cdot \overline{K} \). Then there exists a non-constant function \( \tau \in F \) such that both of the following hold:

i) The places in \( \mathcal{R} \) lie over pairwise distinct places of \( \overline{K}(\tau) \), all of which are unramified in \( F \cdot \overline{K} \).

ii) \( F/K(\tau) \) is “simply branched”, i.e., every place of \( \overline{K}(\tau) \) which ramifies in \( F \cdot \overline{K} \) has a unique ramified place over it, and the latter has ramification index 2.

Proof. Below we use standard facts from algebraic geometry, general references for which are [10, §4.3],[22, §1.3]. Up to replacing \( K \) by its algebraic closure in \( F \), we may choose a smooth projective, geometrically irreducible curve \( C \) over \( K \) with function field \( F \). Via a suitable projection \( \varphi : C \to \tilde{C} \subseteq \mathbb{P}^2_K \), we may choose a plane curve model of \( C \) having at most double points as singularities, and such that all points \( p \in C \) belonging to places in \( \mathcal{R} \) map to non-singular points \( \varphi(p) \) of \( \tilde{C} \). If \( \tilde{C} \) is the projective curve \( f(X,Y,Z) = 0 \), we may assume \( F \cong K(x,y) \), where \( f(x,y,1) = 0 \). Consider now the projection \( \pi : \tilde{C} \to \mathbb{P}^1, (x : y : z) \mapsto (y + \epsilon x : z) \) with \( \epsilon \in K \).

Setting \( \tau = \tau(\epsilon) := y + \epsilon x \), this yields an extension \( F/K(\tau) \). Now note that each of the following is a finite set:

1) The set of tangents to the curve \( \tilde{C} \) passing through some point \( \varphi(p) \) (with \( p \) corresponding to a place in \( \mathcal{R} \), as above); 2) the set of lines in \( \mathbb{P}^2 \) passing through some point \( \varphi(p) \) as well as some singular point of \( \tilde{C} \); 3) the set of lines passing through more than one \( \varphi(p) \); 4) the set of “bitangents” to \( \varphi(C) \) (i.e., tangents at two different points); 5) the set of tangents to \( \tilde{C} \) passing through a singular point of \( \tilde{C} \); and 6) the set of lines intersecting \( \tilde{C} \) with multiplicity \( \geq 3 \) at some point (indeed, we have assumed that \( \tilde{C} \) has at most double points, whence the latter lines are only the tangent lines at a singularity or a flex).

Therefore, up to choosing \( \epsilon \in K \) appropriately, we may assume that none of the lines \( Y + \epsilon X = \alpha Z \), \( \alpha \in K \), in \( \mathbb{P}^2 \) are of the above form. But note that the intersection
of any such line with \( \tilde{C} \) is the fiber \( \pi^{-1}(a) \). The above 1)-6) thus ensure that all \( \varphi(p) \) lie in distinct fibers, each of these fibers has maximal cardinality \([F : K(\tau)]\); and any other fiber has (at most one double point, hence) cardinality at least \([F : K(\tau)] - 1\). The former observation implies i), while the latter implies ii). □

Assume that \( E/F \) is a \( G \)-extension of transcendence degree 1-function fields over \( K \). Let \( \mathcal{R} \) be the set of places of \( F \cdot \overline{K} \) ramifying in \( E \cdot \overline{K} \).

By Lemma 3.4 there exists a non-constant function \( \tau \in F \) such that the places in \( \mathcal{R} \) extend pairwise distinct points \( \tau \mapsto \tau_0 \in \mathbb{P}^1(\overline{K}) \), and the latter are all unramified in \( F/K(\tau) \).

Consider now the Galois closure \( \Omega/K(\tau) \) of \( E/K(\tau) \), and let \( \Gamma \) be its Galois group. Let \( t_0 \) be a \( K_p \)-rational place of \( F \cdot K_p \) and \( \tau_0 \) the underlying place of \( K_p(\tau) \). Applying Proposition 2.1 to \( \Omega/K(\tau) \) and to the Galois closure of \( F/K(\tau) \), we obtain the following conclusion for all but finitely many primes \( \mathfrak{p} \) of \( K \), with the exceptional set depending on \( \Omega \) but not on the particular choice of specialization point \( \tau_0 \).

If \( \mathfrak{p} \) ramifies in the specialization of \( EK_p/FK_p \) at \( t_0 \), then the inertia group generator is a power of an inertia group generator at some branch point of \( E/F \). By condition i) of Lemma 3.4 the ramification index at this branch point is in fact the same as the ramification index at the underlying branch point of \( \Omega/K(\tau) \); consequently, the ramification indices at \( \mathfrak{p} \) in \((EK_p)_{t_0}/(FK_p)_{t_0}\) and in \((\Omega K_p)_{\tau_0}/K_p\) are identical.

Furthermore the residue degree at \( \mathfrak{p} \) in \((\Omega K_p)_{\tau_0}/K_p\) is trivially a multiple of the residue degree in \((EK_p)_{t_0}/(FK_p)_{t_0}\). Now, for each of Lemma 3.2 and 3.3 consider the set \( S \) of exceptional primes corresponding to the \( \Gamma \)-extension \( \Omega/K(\tau) \). It then follows immediately from the above that this set \( S \) also fulfills the respective assertion for the \( G \)-extension \( E/F \), so that the assertion follows from the case of a rational base field, treated in Section 3.2.

### 3.4. Proof of Lemmas 3.2 and 3.3: General case

Finally we extend the proof of Lemmas 3.2 and 3.3 from one to finitely many extensions \( E_i/F_i \). This only requires to note that, in the proofs in Section 3.2 we used only that the set of all completions at branch points \( t_i \) of \( E/K(t) \) is a finite set, not actually the fact that those completions come from a common function field extension \( E/\tilde{K}(t) \). This immediately yields the generalization to finitely many fields of the form \( E_i/K(t) \), \( i = 1, \ldots, r \); To get the conclusion for the most general case of finitely many arbitrary \( G \)-extensions \( E_i/F_i \), we perform the reduction argument of Section 3.3 to each of them.

\(^8\)We have ignored the line at infinity for convenience, but note that at any rate a suitable prior transformation on \( \tau \) ensures that \( \pi \) is unramified at \( \tau \mapsto \infty \).
4. Proof of the main results

Here, we will prove our Main Theorems 1.1 and 1.2. In fact, we will prove the following stronger version of Theorem 1.1.

**Theorem 4.1.** Let $G \neq \{1\}$ be a nontrivial finite group, and let $K \subset \mathbb{R}$ be a real number field such that the cyclotomic extensions $K(\zeta_p)$, with $p$ running through the prime numbers, are pairwise distinct. Then the following are equivalent:

i) $\text{ld}_K(G) = 1$.

ii) $\text{hgd}_K(G) = 1$.

iii) There exists a $K$-regular Galois extension $E/K(t)$ with group $G$ possessing the Hilbert–Grunwald property.

iv) $G$ is either a cyclic group of order 2 or an odd prime power; or $G$ is a Frobenius group whose kernel and complement both are cyclic groups of order 2 or an odd prime power.

Note that $\text{ld}_K(G) \leq 2$ was shown in [19, Main Theorem] for all groups $G$ and number fields $K$, whence Theorem 4.1 completely determines the local dimension over fields $K$ as above. While the implications iii)$\Rightarrow$ii)$\Rightarrow$i) are trivial from the definitions, the remaining implications i)$\Rightarrow$iv) and iv)$\Rightarrow$iii) will be shown below as Theorems 4.2 and 4.3.

Firstly, we use the lemmas of the previous section to obtain a necessary condition for a group to be of local dimension 1 over certain real number fields $K \subset \mathbb{R}$.

**Theorem 4.2.** Let $K \subset \mathbb{R}$ be a real number field for which the extensions $K(\zeta_p)$ (with $p$ prime) are pairwise distinct, and let $G$ be a finite group such that $\text{ld}_K(G) = 1$. Then $G \cong C_P \rtimes C_Q$, where $P$ and $Q$ are coprime, each either $\leq 2$ or an odd prime power, and $C_Q$ acts on $C_P$ as a subgroup of $\text{Aut}(C_P)$.

**Proof.** Due to Corollary 3.1 $G$ cannot have a non-cyclic abelian subgroup. Indeed, if it did, then it would also contain a subgroup $C_q \times C_q$ for some prime $q$. Letting $L$ be as in Corollary 3.1 the complete field $K_p$ possesses a $(C_q \times C_q)$-extension for all primes $p$ of $K$ splitting completely in $K(\zeta_q)$, whereas such an extension cannot occur as a $K_p$-specialization of the prescribed finitely many $G$-extensions $E_i/F_i$, $i = 1, \ldots, r$, for all primes $p$ split in $L(\zeta_q)$. This point was already noted in [18, Theorem 6.3], and forces all Sylow subgroups of $G$ to be either cyclic or a generalized quaternion group (see [5, Chapter XII, Theorem 11.6]).

\[\text{9In particular, for each order there is at most one group with this property, due to Aut}(C_P)\text{ being cyclic.}\]
But $G$ also cannot have an element of order 4 due to Lemma $3.3$. Indeed, every field $K_p$ has a $C_4$-extension of ramification index 2, whence Lemma $3.3$ yields an obstruction (over real fields $K$) for all groups $G$ containing a cyclic subgroup of order 4, implying in particular that all Sylow subgroups of $G$ must be cyclic. Then it is known that $G = B.A$ is an extension of a cyclic group $A$ by a cyclic group $B$ of order coprime to that of $A$ (see, e.g., [25, Chapter V, Theorem 11]). Finally, all elements of $G$ have prime power order. Indeed, the set $S$ in Lemma $3.2$ is chosen such that $K_p$ has a totally ramified $C_r$-extension for every $p \in S$ (and of course also an unramified $C_q$-extension), yielding a $C_{qr}$-extension which is not reached via specialization of the prescribed finitely many extensions $E_i/F_i$, $i = 1, \ldots, r$. Therefore $B$ and $A$ above must be cyclic of order 2 or odd prime power order. Since $|A|$ and $|B|$ are coprime, $G = B \rtimes A$, and the induced homomorphism $A \to \text{Aut}(B)$ must be injective since otherwise there would be non-trivial subgroups of $A$ and $B$ commuting, yielding an element whose order is not a prime-power. This concludes the proof.

Remark 3. It was shown in [6] that the set of specializations of a single $K$-regular $G$-extension $E/K(t)$ always provides a positive answer to all unramified Grunwald problems (outside some finite set $S_0$) - i.e., where $L^{(p)}/K_p$ is unramified for all $p \in S$. Theorem 4.2 and the preceding lemmas show in particular that this is no longer true as one passes from unramified to ramified Grunwald problems even when the ramified local extensions are chosen cyclic.

We note that a similar proof gives the forward direction of Theorem 1.2.

Proof of Theorem 1.2 forwarding. As in the proof of Theorem 4.2, Corollary 3.1 implies that the Sylow subgroups of $G$ are either cyclic or a generalized quaternion group, and Lemma 3.2 implies that all elements have prime power order.

If the 2-Sylow subgroups of $G$ are cyclic, then all Sylow subgroups are cyclic, and $G = B.A$ is an extension of a cyclic group $B$ by a cyclic group $A$ of order coprime to that of $B$ by [25, Chapter V, Theorem 11]. Furthermore, as all elements are of prime power order, $A$ and $B$ are of prime power order and the action of $B$ on $A$ is faithful, so that $B$ embeds into $\text{Aut}(A)$.

Assume the 2-Sylow subgroups of $G$ are generalized quaternion groups. Then, as a consequence of the Suzuki-Zassenhaus theorem (see [11], Theorem 6.15 together with Remark 6.16) $G$ has a unique, and hence central, involution $z$. By multiplying by $z$, one obtains an element of non-prime-power order, unless $G$ itself is a 2-group. In the latter case, $G$ itself is therefore a generalized quaternion group. □
We now aim at the converse of Theorem 4.2 by showing that groups of the form $G \cong C_P \rtimes C_Q$ as above do in fact admit $K$-regular $G$-extensions with the Hilbert–Grunwald property.

**Theorem 4.3.** Let $K$ be a number field, and $G = C_P \rtimes C_Q$, where $P$ and $Q$ are coprime, each either $\leq 2$ or an odd prime power, and $C_Q$ acts on $C_P$ faithfully. Then there exists a $K$-regular $G$-extension $E/K(t)$ with the Hilbert–Grunwald property.

The following lemma constructs cyclic extensions of certain complete fields, which will then serve as completions (at suitable branch points) of extensions $E/K(t)$ in the proof of Theorem 4.3. Let $\nu_2 : \mathbb{Q}^\times \to \mathbb{Z}$ denote the normalized 2-adic valuation.

**Lemma 4.4.** Suppose $e \mid d$ are positive integers with the same prime divisors and either $\nu_2(d) = \nu_2(e) \leq 1$ or $\nu_2(e) \geq 2$. Suppose further that $\mu_d \cap K(\zeta_d) = \mu_e$, and let $E = E^{(e,d)}$ be the splitting field of $P(X) = X^d - \zeta_y^{d/e} \in F[X]$ over $F = F^{(e,d)} := K(\zeta_e)((y))$. Then $E/F$ is a $C_d$-extension with ramification index $e$ and residue extension $K(\zeta_d)/K(\zeta_e)$.

**Proof.** Let $x = (\zeta_y^{d/e})^{1/d}$ be a root of $P$. Then $x^e = \zeta_y^{d/e}y$, so that $F(x)$ contains $K(\zeta_d)((y))$. Furthermore, $x$ has $y$-adic valuation $1/e$, so that the extension $F(x)/K(\zeta_d)((y))$ is of degree divisible by $e$. Since in addition $e$ and $d$ have the same prime divisors and $\mu_d \cap K(\zeta_e) = \mu_e$, the degree of $K(\zeta_d)/K(\zeta_e)$ is $d/e$, and hence:

$$[F(x) : F] = [F(x) : K(\zeta_d)((y))] \cdot [K(\zeta_d)((y)) : F] \geq e \cdot d/e = d,$$

This forces equality, and in particular shows the irreducibility of $P$. On the other hand, $F(x) = K(\zeta_d)((y))(x)$ is already a splitting field of $P$. The claims about inertia subgroup and residue extension are obvious from the above treatment.

It remains to show that $E/F$ is cyclic. For a prime $p \mid d$, let $e_p$ and $d_p$ denote the maximal $p$-powers dividing $e$ and $d$, respectively. Note that $E$ contains a field $E_p = F(x_p)$, where $x_p^{d_p} = \zeta_{e_p}y^{d_e/e_p}$ for some primitive $e_p$-th root of unity $\zeta_{e_p}$. By the above, $E_p/F_p$ is Galois of degree $d_p$, and hence $E$ is the compositum of the fields $E_p$, where $p$ runs over prime divisors of $d$. It therefore suffices to show that $E_p/F$ is cyclic for each prime $p \mid d$. As we have reduced the claim to this case, we shall henceforth assume $d$ is a power of a single prime $p$.

By assumption, if $p = 2$ either $\nu_2(e) = \nu_2(d) = 1$ or $\nu_2(e) \geq 2$. In the former case, $E/F$ is quadratic and hence cyclic. Henceforth assume either $p$ is odd or that $p = 2$ and $4 \mid e$ in which case $\sqrt{-1} \in F$. It follows that $F(\zeta_e^{1/d})/F$ has cyclic Galois group $\langle \tau \rangle$ of order $d$. As $\zeta_e \in F$, the extension $F(y^{1/e})/F$ has cyclic Galois group $\langle \sigma \rangle$ of order $e$. As the first is unramified and the second is totally ramified, these two extensions are linearly disjoint over $F$, and hence $F(\zeta_e^{1/d}, y^{1/e})/F$ is Galois and
its Galois group may be identified with \( \langle \sigma \rangle \times \langle \tau \rangle \), where \( \sigma \) fixes \( \zeta^{1/d}_e \) and \( \tau \) fixes \( y^{1/e} \). Noting that \( \tau^{d/e} \) fixes \( \zeta_d = (\zeta^{1/d}_e)^e \), observe that \( \tau^{d/e}(\zeta^{1/d}_e)/\zeta^{1/d}_e \) and \( \sigma(y^{1/e})/y^{1/e} \) are primitive \( e \)-th roots of unity. We may replace \( \tau \) by a coprime to \( p \) power of \( \tau \) to assume these two roots of unity are equal. In particular, \( \sigma \tau^{−d/e} \) fixes \( x = \zeta^{1/d}_e y^{1/e} \). Since \( \sigma \tau^{−d/e} \) is of order \( e \), the degree of \( F(\zeta^{1/d}_e, y^{1/e})\sigma \tau^{−d/e}/F \) is \( de/e = d = [F(x):F] \). It follows that \( F(x)/F \) is the extension fixed by \( \sigma \tau^{−d/e} \), and hence its Galois group is isomorphic to \( \langle \sigma, \tau \rangle / \langle \sigma \tau^{−d/e} \rangle \). The latter is cyclic, generated e.g. by the coset of \( \tau \), proving the claim. □

Recall that the only primes \( p \) for which \( K_p \) can have a cyclic extension of ramification index \( e' \) are those for which \( \zeta_{e'} \subseteq K_p \), see §2.4. We divide such primes into the sets \( S_{e}^{(d)} \) of all primes \( p \) such that \( \mu_d \cap K_p = \mu_e \), where \( e \) runs over positive integers which divide \( d \) and are divisible by \( e' \). For each set \( S_{e}^{(d)} \), we consider specializations over \( K_p \) for all \( p \in S_{e}^{(d)} \). Letting \( E^{(e,d)} \) be the extension from Lemma 4.4, we have:

**Lemma 4.5.** Let \( e \mid d \) be positive integers with the same prime divisors such that \( \mu_d \cap K(\zeta_e) = \mu_e \), and either \( v_2(e) = v_2(d) \leq 1 \) or \( v_2(e) \geq 2 \). Let \( E/K(t) \) be an extension with completion \( E^{(e,d)}/K(\zeta_e)((y)) \). Then for all but finitely many primes \( p \in S_{e}^{(d)} \), every \( C_d \)-extension of \( K_p \) with ramification index dividing \( e \) is a specialization of \( EK_p/K_p(t) \).

**Proof.** Using Proposition 2.2(ii) and the fact that \( p \) splits completely in \( K(\zeta_e) \), we find (infinitely many) \( t_0 \in K \) such that the completion of \( E_{t_0}/K \) at \( p \) is ramified of index \( e \) and whose residue degree at \( p \) is the residue degree of \( p \) in \( K(\zeta_d)/K(\zeta_e) \). Since \( p \in S_{e}^{(d)} \), this degree is \( d/e \), and hence \( (E_{t_0})_p/K_p \) is of degree \( d \). Since \( E^{(e,d)}/F \) has Galois group \( C_d \), it follows that \( \text{Gal}((E_{t_0})_p/K_p) \) is the entire group \( C_d \).

Using now additionally Proposition 2.3, we obtain that in fact all \( C_d \)-extensions of ramification index \( e' \mid e \) are in \( Sp(E \cdot K_p/K_p(t)) \). This holds for all primes \( p \in S_{e}^{(d)} \) as these split completely in \( K(\zeta_e) \) and remain inert in \( K(\zeta_d)/K(\zeta_e) \). □

**Proof of Theorem 4.3** Following Lemma 2.4, we may treat primes \( p \) of \( K \) separately in what follows. In the following the prime \( p \) is always tacitly assumed to be outside some finite set of exceptional primes arising from Proposition 2.2. Due to [3], for any \( K \)-regular \( G \)-extension \( E/K(t) \) and all but finitely many primes \( p \) of \( K \), all unramified extensions of \( K_p \) with group embedding into \( G \) are in \( Sp(E \cdot K_p/K_p(t)) \). We may therefore focus on (tamely) ramified extensions of \( K_p \).

---

10 Indeed, every \( t_0 \) such that \( t_0 - \zeta_{pe'}(\in K_p!) \) is of \( p \)-adic valuation 1 is good enough.
Note that our group $G$ is chosen such that the only cyclic subgroups are subgroups of $C_p$ or (up to isomorphism) of $C_Q$. Thus, every subgroup of $G$ is of the form $U \rtimes V$ with non-trivial subgroups $U \leq C_p$ and $V \leq C_Q$ such that $V$ acts as a subgroup of $\Aut(U)$. It then suffices to construct an extension $E/K(t)$ fulfilling the following:

(*) For each pair $(e, d)$ such that $e > 1$, $e \mid d$, and $d \mid P$, and for all but finitely many primes $p$ of $K$ such that $K_p$ possesses a $C_d$-extension of ramification $e$, all $C_d$-extensions of $K_p$ with ramification index $e$ are in $Sp(E \cdot K_p/K_p(t))$.  

(**) The same with $P$ replaced by $Q$.  

(***) For every pair $(e, f)$ such that $e, f > 1$, $e \mid P$, and $f \mid Q$, and for all but finitely many primes $p$ of $K$ such that $K_p$ possesses a $(C_e \rtimes C_f)$-extension of ramification index $e$ (with the semidirect product inherited from $C_P \rtimes C_Q$), each such extension is in $Sp(E \cdot K_p/K_p(t))$.  

We start with Condition (*). Since $P$ is either an odd prime power or $P = 2$, the numbers $e$ and $d$ have the same prime divisors for each pair $\pi = (e, d)$ as in (*) and $v_2(e) = v_2(d) \leq 1$. For each such pair $\pi$ such that $\mu_d \cap K(\zeta_e) = \mu_e$, we fix a $K(\zeta_e)$-rational place $t \mapsto t_\pi$ so that the completion at $t \mapsto t_\pi$ is isomorphic to the field $F(\zeta)^{(\pi)} = F(e,d)$ from Lemma 4.4. Moreover, we choose all places $t \mapsto t_\pi$ to be distinct. Since $C_P \rtimes C_Q$ possesses a generic polynomial over $K$ [13, Theorem 7.2.2], a theorem of Saltman [23, Theorem 5.9] implies there exists a $(C_P \rtimes C_Q)$-extension $E/K(t)$ whose completion at each of the places $t \mapsto t_\pi$ is the extension $E(\pi)/F(\pi)$ constructed in Lemma 4.4.

Recall that every prime $p$ of $K$ for which $K_p$ has a tame $C_d$-extension of ramification index $e$ is such that $\zeta_e \subseteq K_p$, for each $e > 1$. Write $\mu_d \cap K_p = \mu_{e'}$ so that $e \mid e'$ and $p \in \mathcal{S}_{e'}(d)$, and set $\pi = (e', d)$. Since $E(\pi)/F(\pi)$ is a completion of $E/K(t)$, Lemma 4.5 then implies that every $C_{e'}$-extension of $K_p$ with ramification index $e$ (dividing $e'$) is a specialization of $EK_p/K_p(t)$, so that (*) holds.

By adding finitely many more analogous completions with $P$ replaced by $Q$, we may assume that it also achieves (**) .

Finally, to fulfill also condition (***) , we add for each $f, e$ as in (**), the $C_e \rtimes C_f$-extension constructed in [13, Corollary 3.6] to the completions of $E/K(t)$. [19, Corollary 3.11] then implies that every $(C_e \rtimes C_f)$-extension of $K_p$ with ramification index $e$ is a specialization of $EK_p/K_p(t)$, for all but finitely many primes $p$ of $K$. □

We can also conclude a proof of Theorem 1.2. As the forward direction was shown earlier in the section, it suffices to show:
Proof of Theorem 1.2, converse assertion. Let \( p \) be an odd prime. We first claim that \( K_p \) has no extensions whose Galois group a generalized quaternion group. Since \( \sqrt{-1} \in K \subseteq K_p \), and the action of Frobenius on the inertia group is equivalent to its action on roots of unity, cf. Section 2.1, the quaternion group does not appear as a Galois group over \( K_p \) or any finite extension of it, and hence the generalized quaternion groups are not Galois groups over \( K_p \).

Thus, whether \( G \) is a generalized quaternion group or \( G = C_P \rtimes C_Q \) for coprime prime powers \( P \) and \( Q \), as in the proof of Theorem 4.2, it suffices to construct an extension \( E/K(t) \) fulfilling:

(*) For each \((e, d)\) such that \( e > 1, e \mid d, \) and \( d \mid P \), and for all but finitely many primes \( p \) of \( K \) such that \( K_p \) possesses a \( C_d \)-extension of ramification index \( e \), all \( C_d \)-extensions of \( K \) with ramification index \( e \) are in \( Sp(E \cdot K_p/K_p(t)) \).

(**) The same with \( P \) replaced by \( Q \).

(***) For every pair \((e, f)\) such that \( e, f > 1, e \mid P, \) and \( f \mid Q \), and for all but finitely many primes \( p \) of \( K \) such that \( K_p \) possesses a \((C_e \rtimes C_f)\)-extension of ramification index \( e \), each such extension is in \( Sp(E \cdot K_p/K_p(t)) \).

Since \( G \) has a generic polynomial over \( K \), once again we construct \( E/K(t) \) using [23, Theorem 5.9] so that it has the following completions at distinct places. For each \((e, d)\) as in (*) and (**) satisfying \( \mu_d \cap K(\zeta_e) = \mu_e \), \( E/K(t) \) has a completion isomorphic to the extension \( E^{(e,d)}/F^{(e,d)} \) from Lemma 4.4. (Note that it is possible to apply Lemma 4.4 since \( \sqrt{-1} \in K \).) For each \((e, d)\) as in (***) \( E/K(t) \) should admit a completion isomorphic to the \((C_e \rtimes C_f)\)-extension with ramification \( e \) constructed in [19, Corollary 3.6]. As in the proof of Theorem 4.2 Lemma 4.5 (resp. [19, Corollary 3.11]) implies that \( E/K(t) \) has (*) \( (**) \) (resp. (***)), as desired. \( \Box \)

Finally, we show that there are no further obstructions to \( \text{ld}_K(G) = 1 \) for cyclic groups \( G \) when \( K \) contains the \( p \)-th roots of unity for every prime \( p \mid |G| \), under the further assumption that \( K(\mu_{2^\infty})/K \) is cyclic if \( |G| \) is even.

**Theorem 4.6.** Let \( K \) be a number field, and \( G \) a cyclic group such that \( \zeta_p \in K \) for every prime \( p \mid |G| \). If \( G \) is of even order, further assume that \( K(\mu_{2^\infty})/K \) is cyclic. Then there exists a \( K \)-regular \( G \)-extension \( E/K(t) \) with the Hilbert–Grunwald property. In particular, \( \text{ld}_K(G) = 1 \).

We note that the proof uses the cyclicity of \( K(\mu_{2^\infty})/K \) only in order to ensure that \( G \) has a generic extension. This in turn is used only to assert the existence of an extension \( E/K(t) \) with desired local completions. It is possible that such an extension exists even when \( G \) has no generic extension.
Lemma 4.8. Let \( \pi \) be a positive integer with the same prime divisors, such that \( v_2(d) \geq 2 \) and \( v_2(e) = 1 \). Let \( K \) be a totally complex number field containing \( \zeta_p \) for all primes \( p | e \). Then there exist complete fields \( F_j = F_j^{(e,d)} \) and \( C_d \)-extensions \( E_j^{(e,d)}/F_j, j = 1, 2, 3 \) with ramification index \( e \) and residue extensions \( N_j/M_j, j = 1, 2, 3 \) satisfying:

(i) \( M_j, j = 1, 2, 3 \) are contained in a common biquadratic extension of \( K(\zeta_e) \), and

(ii) \( N_j \) contains the quadratic extension \( M_j(\sqrt{-1})/M_j \) and the extension \( M_j(\zeta_{d'})/M_j \) where \( d' = d/2^{\nu(d)} \), for \( j = 1, 2, 3 \).

We start the proof of Theorem 4.6 by constructing the completions of \( E/K(t) \):

**Proposition 4.7.** Let \( e, d \) be positive integers with the same prime divisors, such that \( v_2(d) \geq 2 \) and \( v_2(e) = 1 \). Let \( K \) be a totally complex number field containing \( \zeta_p \) for all primes \( p | e \). Then there exist complete fields \( F_j = F_j^{(e,d)} \) and \( C_d \)-extensions \( E_j^{(e,d)}/F_j, j = 1, 2, 3 \) with ramification index \( e \) and residue extensions \( N_j/M_j, j = 1, 2, 3 \) satisfying:

(i) \( M_j, j = 1, 2, 3 \) are contained in a common biquadratic extension of \( K(\zeta_e) \), and

(ii) \( N_j \) contains the quadratic extension \( M_j(\sqrt{-1})/M_j \) and the extension \( M_j(\zeta_{d'})/M_j \) where \( d' = d/2^{\nu(d)} \), for \( j = 1, 2, 3 \).

We first construct the residue fields of the above completions:

**Lemma 4.8.** Let \( K \) be a number field such that \( \sqrt{-1} \notin K \), and let \( r \geq 2 \) be an integer. Then there exists a biquadratic extension \( M/K \) such that for each of its quadratic subextensions \( M_j/K, j = 1, 2, 3 \), the extension \( M_j(\sqrt{-1})/M_j \) is a quadratic extension which embeds into a \( C_2 \)-extension.

**Proof.** Let \( s = s(K) \) be the largest integer for which \( \eta_s := \zeta_{2^s} + \zeta_{2^s}^{-1} \) is in \( K \). Let \( S_0(K) \) be the set of even primes \( p \) of \( K \) for which \( K_p(\zeta_{2^{s+1}})/K_p \) is non-cyclic.

By the Grunwald–Wang theorem\(^{[1]} \) [Chp. X, Thm. 5], there exist two disjoint quadratic extensions \( M_1, M_2/K \) whose completions satisfy:

(i) \( (M_1)_p \) and \( (M_2)_p \) are disjoint quadratic extensions with compositum \( K_p(\zeta_{2^{s+1}}) \), at every \( p \in S_0(K) \).

(ii) there exist odd primes \( p_1 \) and \( p_2 \) which split completely in \( K(\zeta_{2^{s+1}}) \) and are inert in \( M_1 \) and \( M_2 \), respectively.

Let \( M = M_1 \cdot M_2 \), and let \( M_3 \) be the third quadratic subextension of \( M/K \). The disjointness of \( M/K \) and \( K(\zeta_{2^{s+1}})/K \) follows from (ii) since in each of the extensions \( M_j/K, j = 1, 2, 3 \), one of the primes \( p_1, p_2 \) is inert while being split completely in \( K(\zeta_{2^{s+1}})/K \).

We claim that for each of the quadratic fields \( M_j = M_j, j = 1, 2, 3 \) the extension \( M_j(\sqrt{-1})/M_j \) embeds into a \( C_2 \)-extension \( N_j/M_j \). Setting \( \Gamma_\nu := \text{Gal}(M_\nu'(\sqrt{-1})/M_\nu') \), we first check that the corresponding local embedding problem \( \pi_\nu : \pi^{-1}(\Gamma_\nu) \rightarrow \Gamma_\nu \) is

\(^{[1]} \) Note that the special case of Grunwald–Wang does not apply to quadratic extensions, and those are the only ones considered here.
solvable at all places $\nu$ of $M'$. Since $M'$ is totally complex, $M'/(\sqrt{-1})$ is unramified away from even primes, and hence $\pi_\nu$ is solvable for every place $\nu$ which does not lie over 2. Next note that since $M/K$ is disjoint from $K(\zeta_{2s+1})/K$ while $M_p/K_p$ and $K_p(\zeta_{2s+1})/K_p$ are not disjoint for $p \in S_0(K)$ by (i), we have $s(M') = s(K)$ and $S_0(M') = \emptyset$. Since $S_0(M') = \emptyset$, for every prime $p$ of $M'$, either $M_p/(\mu_{2s})/M'_p$ is cyclic or $\eta_{s+1} \in M'_p$, where $s = s(M')$. In the former case the embedding problem $\pi_p$ is clearly solvable. In the latter case $M'_p \supseteq \mathbb{Q}_2(\sqrt{2})$. Since the quaternion algebra $(-1, -1)_{\mathbb{Q}_2}$ is split by the extension $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$, one has $-1 = a^2 + b^2$ for some $a, b \in M'_p$. Since $-1$ is a sum of two squares, $M'_p/(\sqrt{-1})/M'_p$ embeds into a $C_4$-extension $[8, \text{Proposition 16.5.1}]$, which further implies that $M'_p/(\sqrt{-1})/M'_p$ embeds into a $C_{2r}$-extension $[9, \text{Thm. 3}]$ or $[2, \text{Proof of Thm. 5}]$. In summary, $\pi_\nu$ is solvable for all places $\nu$ of $M'$. Finally, as in $[9, \text{17.1}]$, since $M'/K$ is linearly disjoint from $K(\zeta_{2s+1})$ and since $\pi : C_{2r} \to \text{Gal}(M'/(\sqrt{-1})/M')$ is locally solvable at all places, $\pi$ is solvable by $[9, \text{Theorem 2}]$. Since $\pi$ is Frattini, every solution is proper, as desired.

Proof of Proposition $4.7$. Note that $r := v_2(d) > 1$, and set $d' := d/2^r$ and $e' := e/2$. By Lemma $4.8$ there exist quadratic extensions $M_j/K(\zeta_e)$, $j = 1, 2, 3$ contained in a common biquadratic extension of $K(\zeta_e)$, and $C_{2r}$-extensions $N'_j/M_j$ containing the quadratic extension $M_j/(\sqrt{-1})/M_j$. Note that since $d'$ and $e'$ have the same prime divisors, $K(\zeta_{d'})/K(\zeta_e)$ and $M_j/K(\zeta_e)$ are linearly disjoint, and the condition $\mu_{d'} \cap M_j = \mu_{e'}$ holds. Thus we may apply Lemma $4.4$ with the base field $M_j$ (instead of $K$) to obtain a $C_{e'}$-extension $E_j^{(e',d')}/F_j$, with ramification index $e'$ and residue extension $M_j(\zeta_{d'})/M_j$, of a complete field $F_j = M_j((y_j))$.

Write $N''_j = N''_j(\sqrt{a_j})$ for the $C_{2r-1}$-subextension $N''_j/M_j$ of $N'_j/M_j$, and $a_j \in N''_j$. Then $N''_jF_j(\sqrt{a_jy_j})$ is a $C_{2r}$-extension of $F_j$ with ramification index 2 which is linearly disjoint from $E_j^{(e',d')}/F_j$, as the latter is Galois of odd degree. Then $E_j := E_j^{(e',d')}/N''_j(\sqrt{a_jy_j})$ is a $C_4$-extension with ramification index $e = 2e'$, containing $N''_j \supseteq M_j/(\sqrt{-1})$ and $M_j(\zeta_{d'})$, as desired.

Lemma 4.9. Let $e \mid d$ be positive integers with the same prime divisors such that $\mu_d \cap K(\zeta_e) = \mu_e$ and $v_2(d) > v_2(e) = 1$. Let $E/K(t)$ be an extension with the above completions $E_j^{(e,d')}/F_j^{(e,d')}$, $j = 1, 2, 3$. Then every $C_4$-extension of $K_p$ with ramification index dividing $e$ is a specialization of $EK_p/K_p(t)$ for all but finitely many primes $p$ satisfying $\mu_d \cap K_p = \mu_e$.

\footnote{Alternatively, this follows from the congruence $-1 \equiv 1^2 + (2 + \sqrt{2})^2 \mod 4\sqrt{2}$ in $\mathbb{Z}_2[\sqrt{2}]$ and Hensel’s lemma.}
Proof. As always, avoiding finitely many primes, we may assume \( p \) is coprime to \( e \). Since \( 4 \mid d, v_2(e) = 1 \) and \( \mu_d \cap K_p = \mu_e \), we deduce that \( K_p \) does not contain \( \sqrt{-1} \).
It follows that there is no \( C_d \)-extension of \( K_p \) with ramification index divisible by 4.

Letting \( M_j \) denote the residue field of \( F_j = F_j^{(e,d)} \), we recall that \( M_j / K(\zeta_e) \), \( j = 1, 2, 3 \) are quadratic extensions contained in a common biquadratic extension \( M/K(\zeta_e) \). Avoiding the finitely many primes \( p \)-extension with ramification index \( e \)-prime divisors, such that \( \left( \frac{d}{e} \right) \neq 1 \), and recalling the \( p \)-extension with ramification index \( e \)-prime divisors, such that \( \left( \frac{d}{e} \right) \neq 1 \), and \( \mu_d \cap K(\zeta_e) = \mu_e \). Since \( G \) has a generic polynomial over \( K \), Saltman’s theorem \[23\] Theorem 5.9] implies that there exists a \( G \)-extension \( E/K(t) \) having completions isomorphic to the extensions \( E^{(e,d)}/F^{(e,d)} \) of Lemma \[4.4\] for each of the above \( (e,d) \) satisfying \( v_2(e) = v_2(d) \leq 1 \) or \( v_2(e) > 1 \), and to the extensions \( E_j^{(e,d)}/F_j^{(e,d)} \), \( j = 1, 2, 3 \) of Lemma \[4.3\] for each of the above \( (e,d) \) satisfying \( v_2(e) = 1 < v_2(d) \). By Lemmas \[4.5\] and \[4.9\] every cyclic extension of \( K_p \) of degree \( d \) and ramification index dividing \( e \) is a specialization of \( E \cdot K_p/K_p(t) \) for all but finitely many primes \( p \) with \( \mu_d \cap K_p = \mu_e \).

It remains to recall that the primes \( p \) for which \( K_p \) admits a tamely ramified \( C_d \)-extension with ramification index \( e' \) are those for which \( \mu_d \cap K_p = \mu_e \) with \( e' \mid e \). Thus, the above implies that \( E/K(t) \) specializes to all \( C_d \)-extensions of \( K_p \) for all but finitely many primes \( p \).}

---

\[13\] This idea is inspired by a construction of polynomials with roots modulo \( p \) for all \( p \), cf. \[24\].
APPENDIX A. AN APPLICATION: GROUPS OF PARAMETRIC DIMENSION 1

Our results also allow a near-full classification of groups of \textit{parametric dimension} 1 over a number field, a problem that has been investigated in a series of previous papers. (e.g., [16], [18]). Here, the parametric dimension \(pd_K(G)\) of a group \(G\) over any field \(K\) is defined as the minimal integer \(d\) for which there exist finitely many \(G\)-extensions (of \(\text{\acute{e}tale}\) algebras) \(E_i/F_i, i = 1, \ldots, r\), of transcendence degree \(\leq d\) over \(K\) such that every \(G\)-extension of \(K\) (equivalently, every Galois extension of \(K\) with Galois group embedding into \(G\)) occurs as a specialization of some \(E_i/F_i\).

The following connects parametric and local dimension:

\textbf{Proposition A.1.} For all groups \(G\) and number fields \(K\), one has \(pd_K(G) \geq ld_K(G)\).

\textit{Proof.} Let \(E_i/F_i, i = 1, \ldots, r\), be finitely many \(G\)-extensions of transcendence degree \(d \leq pd_K(G)\), parameterizing all \(G\)-extensions of \(K\) as in the definition above. In particular, for every metacyclic subgroup \(U \leq G\), every Galois extension \(L/K\) with Galois group \(U\) occurs as a \(K\)-specialization of some \(E_i/F_i\). A fortiori, \(L \cdot K_p/K_p\) occurs as a \(K_p\)-specialization of \(E_i/F_i\), for all primes \(p\) of \(K\). Note that metacyclic groups are necessarily supersolvable, whence by a famous result of Harpaz and Wittenberg ([12]), for all but finitely many primes \(p\) of \(K\), all \(U\)-extensions of \(K_p\) do in fact occur as completions of some \(U\)-extension of \(K\). On the other hand, all tame Galois extensions of \(K_p\) are in fact metacyclic. Therefore, up to possibly excluding finitely many more primes \(p\), every Galois extension of \(K_p\) of Galois group embedding into \(G\) is a \(K_p\)-specialization of some \(E_i/F_i\), for all but finitely many \(p\). Thus, \(pd_K(G) \geq ld_K(G)\). \(\square\)

In particular, groups of parametric dimension 1 over e.g. \(K = \mathbb{Q}\) are necessarily of the form \(C_P \rtimes C_Q\) as in Theorem [14]. We may narrow the list down even further, by combining this result with the methods of [16]. In particular, [16, Theorem 5.2] excludes all cyclic groups except the ones of prime order. Note furthermore that, for \(U \leq G\), one has \(pd_K(U) \leq pd_K(G)\) by simply applying the Galois correspondence. We are thus even reduced to groups of the form \(C_p \rtimes C_q\) with both \(p\) and \(q\) prime (or = 1), and \(q|p - 1\). Furthermore, [16, Theorem 5.1] excludes all groups of order coprime to 6.

\textit{Remark 4.} Invoking [16] as above requires a certain amount of care; indeed, the cited theorems are a priori stated only for \(\mathbb{Q}\)-regular extensions \(E_i/\mathbb{Q}(t)\) with purely transcendental base field \(\mathbb{Q}(t)\), whereas we here also need to allow arbitrary extensions of transcendence degree 1 function fields. This is, however, possible via slight adjustments of the proofs in [16, Section 6]. Indeed, the methods apply in complete
analogy for $\mathbb{Q}$-regular extensions $E_i/F_i$ with arbitrary base field $F_i$. To drop also the regularity assumption, start by picking, for each non-regular extension $E_i/F_i$, a prime which is non-split in the constant extension, and restrict attention to only those $G$-extensions of $\mathbb{Q}$ in which all those primes split. Obviously, no such extension can arise as a specialization of some non-regular $E_i/F_i$, so from here on, we may again assume that all $E_i/F_i$ are $\mathbb{Q}$-regular. Now the core argument of the cited results of [16] is the fact that (for the groups $G$ in question) there is some non-trivial normal subgroup $N \triangleleft G$ such that every properly solvable embedding problem induced by $G \to G/N$ has infinitely many proper solutions, whereas the given set of regular extensions can only specialize finitely many of those. It then suffices to construct (infinitely many) solutions in which the finitely many primes chosen above are all split; since all groups $G$ in question are solvable, this can be obtained, e.g. from Shafarevich’s method, see, e.g., [7].

We have thus obtained:

**Theorem A.2.** Let $G$ be a finite group with $\text{pd}_\mathbb{Q}(G) = 1$. Then $G$ is isomorphic to $C_p$ (for some prime $p$), $D_p$ (for some prime $p \geq 3$) or $C_p \times C_3$ (for some prime $p \equiv 1 \text{ mod } 3$).

Note also that comparison of the lists of groups in Theorems 4.1 and A.2 gives examples of groups for which $\text{pd}_\mathbb{Q}(G) > \text{ld}_\mathbb{Q}(G)$, something that was anticipated, but not proven in [19, Appendix A].

In fact, we conjecture that the only groups $G$ with $\text{pd}_\mathbb{Q}(G) = 1$ are $G = C_2, C_3$ and $S_3$. Combining Theorem A.2 with the methods of [17] would get us much closer to this goal, at least conditionally on the abc-conjecture, although going into full detail would lead us too far away.

**References**

[1] A. Adem, R.J. Milgram, *Cohomology of finite groups*, 2nd ed. Grundlehren der Mathematischen Wissenschaften 309, Springer, 2004.
[2] J. K. Arason, B. Fein, M. Schacher, J. Sonn, *Cyclic extensions of $K(\sqrt{-1})/K$*. Trans. Amer. Math. Soc. 313 (1989), 843–851.
[3] E. Artin, J. Tate, *Class field theory*. W. A. Benjamin, Inc., New York-Amsterdam 1968.
[4] S. Beckmann, *On extensions of number fields obtained by specializing branched coverings*. J. reine angew. Math. 419 (1991), 27–53.
[5] H. Cartan, S. Eilenberg, *Homological Algebra*. xv+390 pp. Princeton, NJ: Princeton University Press, 1956.
[6] P. Débes, N. Ghazi, *Galois covers and the Hilbert-Grunwald property*. Ann. Inst. Fourier 62 (3) (2012), 989–1013.
[7] A. Fehm, F. Legrand, A note on finite embedding problems with nilpotent kernel. Preprint (2020). https://arxiv.org/pdf/2011.07536.pdf
[8] M.D. Fried, M. Jarden, Field arithmetic. 3rd edn. Revised by Moshe Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol. 11. Springer, Berlin, 2008.
[9] W.-D. Geyer, C. U. Jensen, Embeddability of quadratic extensions in cyclic extensions. Forum Math. 19 (2007), 707–725.
[10] R. Hartshorne, Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.
[11] T. Hanke, J. Sonn, The location of noncrossed products in Brauer groups of Laurent series fields over global fields. Math. Ann. 350 (2011), 313–337.
[12] Y. Harpaz, O. Wittenberg, Zéro-cycles sur les espaces homogènes et problème de Galois inverse. J. Amer. Math. Soc. 33 (2020), 775–805.
[13] C.U. Jensen, A. Ledet, N. Yui, Generic polynomials: Constructive Aspects of the Inverse Galois Problem. Cambridge Univ. Press (MSRI Publications, Vol. 45) (2002).
[14] M.-C. Kang, Noether’s problem for dihedral 2-groups II. Pacific J. Math. 222(2) (2005), 301–316.
[15] J. König, The Grunwald problem and specialization of families of regular Galois extensions. Ann. Sc. Norm. Super. Pisa, Cl. Sci. Vol. XXI (2020), 1531–1552.
[16] J. König, F. Legrand, Non-parametric sets of regular realizations over number fields. J. Algebra 497 (2018), 302–336.
[17] J. König, F. Legrand, Density results for specialization sets of Galois covers. J. Inst. Math. Jussieu 20 (5) (2021), 1455–1496.
[18] J. König, F. Legrand, D. Neftin, On the local behavior of specializations of function field extensions. Int. Math. Res. Not. Vol. 2019 Issue 9 (2019), 2951–2980.
[19] J. König, D. Neftin, The local dimension of a finite group over a number field. To appear in Trans. Amer. Math. Soc. Preprint at https://arxiv.org/abs/2007.05383
[20] F. Legrand, On parametric extensions over number fields. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) Vol. XVIII (2018), 551–563.
[21] B. Plans, N. Vila, Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization. J. Théor. Nombres Bordeaux 17(1) (2005), 271–282.
[22] F. Russo, On the Geometry of Some Special Projective Varieties. Lecture Notes of the Unione Matematica Italiana, Springer, 2015.
[23] D. J. Saltman, Generic Galois extensions and problems in field theory. Advances in Mathematics 43 (1982), 250–283.
[24] J. Sonn, Polynomials with roots in $\mathbb{Q}_p$ for all $p$. Proc. Amer. Math. Soc. 136 (2008), 1955–1960.
[25] H. Zassenhaus, The theory of groups. 2nd ed. 10 + 265 pp. New York, Chelsea, 1958.