ON THE LOCAL BEHAVIOUR OF SPECIALIZATIONS OF FUNCTION FIELD EXTENSIONS

JOACHIM KÖNIG, FRANÇOIS LEGRAND, AND DANNY NEFTIN

ABSTRACT. Given a field k of characteristic zero and an indeterminate T over k, we investigate the local behaviour at primes of k of finite Galois extensions of k arising as specializations of finite Galois extensions $E/k(T)$ (with E/k regular) at points $t_0 \in \mathbb{P}^1(k)$. We provide a general result about decomposition groups at primes of k in specializations, extending a fundamental result of Beckmann concerning inertia groups. We then apply our result to study crossed products, the Hilbert–Grunwald property, and finite parametric sets.

1. INTRODUCTION

1.1. **Grunwald problems.** Given a number field k, *Grunwald problems* concern the structure of completions $L_\mathfrak{p}/k_\mathfrak{p}$ of *G-extensions* L/k at any finitely many given primes $\mathfrak{p}$ of k. Here, a G-extension L/k is a finite Galois extension of k with Galois group G, and $k_\mathfrak{p}$ (resp., $L_\mathfrak{p}$) denotes the completion of k (resp., of L) at $\mathfrak{p}$ (resp., at a prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$)[1]. The original motivation for such problems arose from their key role in the structure theory of finite dimensional division algebras over number fields. Since then, they received much attention, especially due to connections with the regular inverse Galois problem; see [DG11, DG12], and with weak approximation; see, e.g., [Har07, Dem10, LA14, DLAN15].

More precisely, given a finite set $\mathcal{S}$ of primes of k, and given finite Galois extensions $L^{(\mathfrak{p})}/k_\mathfrak{p}$, $\mathfrak{p} \in \mathcal{S}$, with Galois groups embedding into G, the Grunwald problem $(G, (L^{(\mathfrak{p})}/k_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}})$ asks whether there is a G-extension L/k whose completion $L_\mathfrak{p}$ at $\mathfrak{p}$ is $k_\mathfrak{p}$-isomorphic to $L^{(\mathfrak{p})}$, $\mathfrak{p} \in \mathcal{S}$. If such an extension L/k exists, it is called a *solution* to the Grunwald problem $(G, (L^{(\mathfrak{p})}/k_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}})$. We note that, instead of prescribing the local extensions $L_\mathfrak{p}/k_\mathfrak{p}$, $\mathfrak{p} \in \mathcal{S}$, weaker versions ask for the existence of a G-extension L/k with prescribed local degrees $[L_\mathfrak{p} : k_\mathfrak{p}]$, $\mathfrak{p} \in \mathcal{S}$, or with prescribed local Galois groups $\mathrm{Gal}(L_\mathfrak{p}/k_\mathfrak{p})$, $\mathfrak{p} \in \mathcal{S}$. These weaker versions usually suffice for applications to classical problems, see, e.g., [Wan50, Corollary 2] and [Sch68].

Date: August 26, 2017.

Key words and phrases. Galois theory, local behaviour, specializations, Grunwald problems, crossed products, parametric sets.

[1]Recall that the latter is independent of the choice of $\mathfrak{P}$ (up to $k_\mathfrak{p}$-isomorphism).

Examples of Grunwald problems $(G, (L^{(\mathfrak{p})}/k_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}})$ with no solution L/k occur already for cyclic groups G, when $\mathcal{S}$ contains a prime of k lying over 2 [Wan48]. However, it is expected [Har07, §1] that, for solvable groups G, every Grunwald problem $(G, (L^{(\mathfrak{p})}/k_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}})$ has a solution, provided $\mathcal{S}$ is disjoint from some finite set $\mathcal{S}_{\mathrm{exc}}$ of "exceptional" primes of k, depending only on G and k. This is known when (1) G is abelian, and $\mathcal{S}_{\mathrm{exc}}$ is the set of primes of k dividing 2 [NSW08, (9.2.8)]; (2) G is an iterated semidirect product $A_1 \rtimes (A_2 \rtimes \cdots \rtimes A_n)$ of finite abelian groups, and $\mathcal{S}_{\mathrm{exc}}$ is the set of primes of k dividing $|G|$; see [Har07, Théorème 1] and [DLAN15, Theorem 1.1]; (3) G is solvable of order prime to the number of roots of unity in k, and $\mathcal{S}_{\mathrm{exc}} = \emptyset$ [NSW08, (9.5.5)]; and (4) there exists a *generic extension* for G over k, and $\mathcal{S}_{\mathrm{exc}} = \emptyset$ [Sal82, Theorem 5.9]. Among the above, the latter is the only method which applies to non-solvable groups. However, the family of non-solvable groups for which a generic extension is known is quite restrictive, e.g., it is unknown whether the alternating group A_n has a generic extension for $n \geq 6$. See [JLY02] for an overview on generic extensions.

The main source of realizations of non-solvable groups G over k is via *k-regular G-extensions*, that is, via G-extensions $E/k(T)$, where T is an indeterminate over k and k is algebraically closed in E. Indeed, by *Hilbert's irreducibility theorem*, every non-trivial k-regular G-extension $E/k(T)$ has infinitely many linearly disjoint *specializations* E_{t_0}/k, $t_0 \in \mathbb{P}^1(k)$, with Galois group G. Many groups have been realized by this method; see, e.g., [MM99], and references within, as well as [Zyw14] for more recent examples.

This specialization process provides a natural way to attack Grunwald problems for *k-regular Galois groups*, that is, for finite groups G admitting a k-regular G-extension of $k(T)$. Namely, given such an extension $E/k(T)$, it is natural to ask for the local behaviour of specializations E_{t_0}/k, $t_0 \in \mathbb{P}^1(k)$. That is, which local extensions $L^{(\mathfrak{p})}/k_\mathfrak{p}$, which local Galois groups $\mathrm{Gal}(L^{(\mathfrak{p})}/k_\mathfrak{p})$, and which local degrees $[L^{(\mathfrak{p})} : k_\mathfrak{p}]$ arise by completing the specialization E_{t_0}/k at primes $\mathfrak{p}$ of k, when t_0 runs over $\mathbb{P}^1(k)$? For points $t_0 \in \mathbb{P}^1(k)$ which are $\mathfrak{p}$-adically far from *branch points* of $E/k(T)$, this approach was deeply investigated by Dèbes and Ghazi [DG11, DG12][2], and applies only to unramified local extensions. Namely, given a k-regular G-extension $E/k(T)$, a finite set $\mathcal{S}$ of primes of k, disjoint from some finite set $\mathcal{S}_{\mathrm{exc}}$ (depending only on $E/k(T)$), and unramified extensions $L^{(\mathfrak{p})}/k_\mathfrak{p}$ with Galois group embedding into G, $\mathfrak{p} \in \mathcal{S}$, [DG12] provides $t_0 \in k$ such that E_{t_0}/k is a solution to the Grunwald problem $(G, (L^{(\mathfrak{p})}/k_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}})$.

1.2. **Main results.** The goal of this paper is to study the local behaviour at a prime $\mathfrak{p}$ of k of specializations E_{t_0}/k, when t_0 is $\mathfrak{p}$-adically close to a branch point of $E/k(T)$.

1.2.1. *Background.* A first related conclusion can be derived from the algebraic cover theory of Grothendieck. Namely, if $\mathfrak{p}$ is not in some finite set $\mathcal{S}_{\mathrm{exc}}$ of primes of k, depending only on $E/k(T)$, and if $\mathfrak{p}$ ramifies in the specialization E_{t_0}/k, then t_0 and

[2]See [DG12, §1.6] for a review of related previous results.

some branch point t_i of $E/k(T)$ *meet modulo* $\mathfrak{p}$. In the special case where t_i is k-rational and $v_\mathfrak{p}(t_0)$ is non-negative, this means that $a_\mathfrak{p} := v_\mathfrak{p}(t_0 - t_i)$ is positive, where $v_\mathfrak{p}$ denotes the normalized $\mathfrak{p}$-adic valuation. A fundamental theorem by Beckmann [Bec91, Con00] then asserts that the inertia group $I_{t_0,\mathfrak{p}}$ of E_{t_0}/k at $\mathfrak{p}$ is determined by the inertia group I_{t_i} at a fixed prime of E lying over the prime $\mathcal{P}_i$ of $k[T-t_i]$ generated by $T-t_i$. Namely, $I_{t_0,\mathfrak{p}}$ is conjugate to $I_{t_i}^{a_\mathfrak{p}}$. We refer to §3 for more details.

1.2.2. *Decomposition groups of specializations.* Given $t_0 \in \mathbb{P}^1(k)$, assumed to meet the branch point t_i modulo $\mathfrak{p}$, we show that the entire decomposition group at $\mathfrak{p}$ of the specialization E_{t_0}/k is determined by the local behaviour at t_i, thus extending Beckmann's theorem. Namely, suppose for simplicity that t_i is k-rational, and let D_{t_i} denote the geometric decomposition group at a fixed prime of E lying over the geometric prime $\mathcal{P}_i$. Recall that the specialization E_{t_i}/k has Galois group D_{t_i}/I_{t_i}; let $\varphi_i : D_{t_i} \to D_{t_i}/I_{t_i}$ be the natural projection. Let $D_{t_i,\mathfrak{p}}$ be the decomposition group at a prime $\mathfrak{P}$ of E_{t_i} lying over $\mathfrak{p}$; this is a subgroup of D_{t_i}/I_{t_i}. Note that, up to conjugation, the subgroup $\varphi_i^{-1}(D_{t_i,\mathfrak{p}})$ of G is independent of the choice of an arithmetic prime $\mathfrak{P}$ lying over $\mathfrak{p}$ and a geometric prime lying over $\mathcal{P}_i$.

Theorem 1.1. *Suppose that the given prime $\mathfrak{p}$ of k is outside some finite set $\mathcal{S}_{\mathrm{exc}}$ depending only on $E/k(T)$. Moreover, suppose that the given branch point t_i is k-rational, that t_0 and t_i meet modulo $\mathfrak{p}$, and that the exponent $a_\mathfrak{p}$ is coprime to $|I_{t_i}|$. Then the decomposition group of E_{t_0}/k at $\mathfrak{p}$ is conjugate by an element of G to $\varphi_i^{-1}(D_{t_i,\mathfrak{p}})$.*

Note that $\varphi_i^{-1}(D_{t_i,\mathfrak{p}})$ is the group generated by I_{t_i} and a lift of the Frobenius of E_{t_i}/k at $\mathfrak{p}$. We refer to Theorem 4.1 for a more general version of Theorem 1.1, where we relax the assumptions on t_i and $a_\mathfrak{p}$, and which is stated over more general base fields.

1.2.3. *Solving Grunwald problems.* Theorem 1.1 shows that the decomposition group of E_{t_0}/k at $\mathfrak{p}$ is determined by the local data $(\varphi_i, D_{t_i,\mathfrak{p}})$ at t_i, when t_0 and t_i meet modulo $\mathfrak{p}$. Theorem 1.2 below shows that this is the only constraint on completions of E_{t_0}/k at $\mathfrak{p}$ for such specialization points t_0.

Theorem 1.2. *Suppose that $\mathcal{S}$ is a finite set of primes of k disjoint from some finite set of primes $\mathcal{S}'_{\mathrm{exc}}$ depending only on $E/k(T)$. For each $\mathfrak{p} \in \mathcal{S}$, fix a k-rational branch point $t_{i(\mathfrak{p})}$ of $E/k(T)$ and a finite Galois extension $L^{(\mathfrak{p})}/k_\mathfrak{p}$ with Galois group (resp., inertia group) $\varphi_{i(\mathfrak{p})}^{-1}(D_{t_{i(\mathfrak{p})},\mathfrak{p}})$ (resp., $I_{t_{i(\mathfrak{p})}}$). Then there exists $t_0 \in k$ such that E_{t_0}/k is a solution to the Grunwald problem $(G, (L^{(\mathfrak{p})}/k_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}})$.*

See Theorem 4.4 for a more general version of Theorem 1.2, where the assumption on the branch points is relaxed, and where k is not necessarily a number field.

Given a single homomorphism $\varphi_i : D_{t_i} \to D_{t_i}/I_{t_i}$ at a (k-rational) branch point t_i of $E/k(T)$, Theorem 1.2 provides a solution to all Grunwald problems $(G, (L^{(\mathfrak{p})}/k_\mathfrak{p})_{\mathfrak{p}\in\mathcal{S}})$,

where, for each $\mathfrak{p}$ in $\mathcal{S}$, the local extension $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$ has inertia group I_{t_i} and decomposition group $\varphi_i^{-1}(D_{t_i,\mathfrak{p}})$. Such results are especially applicable when the primes are allowed to vary and the decomposition groups are fixed, as described in §1.3.

1.2.4. *About the proof.* Let R be the ring of integers of k. Our approach to Theorems 1.1 and 1.2 considers the fraction field F of the completion $R_{\mathfrak{p}}[[T]]$ of (the two dimensional) domain $R[T]$ at the ideal generated by $\mathfrak{p}$ and $T - t_i$. We use a theorem of Eisenstein, recalled as Theorem 2.4, to show that, for all but finitely many primes $\mathfrak{p}$ of k, the group $\mathrm{Gal}(E \cdot F/F)$ is determined by the local data $(\varphi_i, D_{t_i,\mathfrak{p}})$ at t_i. On the other hand, we show that by reducing the extension $E \cdot F/F$ modulo a prime over $(T - t_0)$, the resulting extension of residue fields is the completion of E_{t_0}/k at $\mathfrak{p}$, giving the desired connection between $D_{t_0,\mathfrak{p}}$ and the local data at t_i. The above method is considerably different from that of Dèbes and Ghazi, which, to our knowledge, does not apply to ramified extensions; see [DG12, §1.6], and which is based on specializations of extensions of $k_{\mathfrak{p}}(T)$.

We use the theory of Brauer embedding problems to determine the extensions $M/k_{\mathfrak{p}}$ which satisfy the constraints imposed by Theorem 1.1 on completions of specializations $(E_{t_0})_{\mathfrak{p}}$, and the above reduction process to show that such fields M are obtained as specializations $(E_{t_0})_{\mathfrak{p}}$.

1.3. **Applications.** Theorem 1.1 is then used to study crossed product division algebras, the Hilbert–Grunwald property, and finite parametric sets.

1.3.1. *Prescribing decomposition groups and crossed products.* Recall that the Galois group D of a tamely ramified extension of $k_{\mathfrak{p}}$ is *metacyclic*, that is, D admits a cyclic normal subgroup I such that D/I is cyclic. The following application of Theorem 1.1 describes the appearance of metacyclic subgroups of G as decomposition groups of specializations of the k-regular G-extension $E/k(T)$.

Theorem 1.3. *Given a branch point t_i of $E/k(T)$, let D_{t_i} (resp., I_{t_i}) denote the decomposition (resp., inertia) group at t_i, and let τ be an element of D_{t_i}. Then there exist infinitely many primes $\mathfrak{p}$ of k, and, for each such prime $\mathfrak{p}$, infinitely many $t_0 \in k$ such that E_{t_0}/k is a G-extension with decomposition group $\langle I_{t_i}, \tau \rangle$ at $\mathfrak{p}$.*

We refer to Theorem 4.5 for a generalization of Theorem 1.3, where we consider finitely many primes of k at the same time.

We then apply this result to prove the existence of *G-crossed product* division algebras over number fields for various finite groups G. Recall that a finite dimensional division algebra over its center k is a *G-crossed product* if it admits a maximal subfield L that is finite and Galois over k, and such that $\mathrm{Gal}(L/k) = G$. A G-crossed product division algebra is equipped with an explicit structure, which plays a key role in the theory of central simple algebras. By Schacher's result [Sch68, Theorem 4.1], the existence of a

G-crossed product division algebra with center $\mathbb{Q}$ implies that G has metacyclic Sylow subgroups. The converse is a long standing open conjecture, originating in [Sch68]: for every finite group G with metacyclic Sylow subgroups, there exists a G-crossed product division algebra with center $\mathbb{Q}$. Although this conjecture has been extensively studied, cf. [ABGV11, Section 11.A], the only finite non-abelian simple groups for which the conjecture is known to hold are $A_5 \cong \mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_5)$ [GS79, Theorem 1], $A_6 \cong \mathrm{PSL}_2(\mathbb{F}_9)$ [FS91, Theorem 6], A_7 [FS91, Theorem 6], $\mathrm{PSL}_2(\mathbb{F}_7)$ [AS01, Proposition 5], $\mathrm{PSL}_2(\mathbb{F}_{11})$ [AS01, Theorem 2], and the Mathieu group M_{11} [KN17].

Given a k-regular G-extension $E/k(T)$ with suitable properties, we use Theorem 1.3 to establish a general criterion for the existence of specialization points $t_0 \in k$ such that E_{t_0} is a maximal subfield of a G-crossed product. We refer to Theorem 5.2 for our precise result. We then use this criterion to derive the first infinite family of finite non-abelian simple groups G with a G-crossed product division algebra over $\mathbb{Q}$.

Theorem 1.4. *Let p be a prime number such that either $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$. Then there exists a $\mathrm{PSL}_2(\mathbb{F}_p)$-crossed product division algebra with center $\mathbb{Q}$.*

See Theorem 5.3 where we show more generally that Theorem 1.4 holds over an arbitrary number field k (instead of $\mathbb{Q}$), provided primitive 4-th roots of unity are not in k. See also Theorem 5.4 where a similar conclusion is shown to hold for prime numbers lying in other arithmetic progressions.

1.3.2. *On the Hilbert-Grunwald property.* Following a terminology due to Dèbes and Ghazi, and motivated by the partial positive answer provided by Theorem 1.2, one may ask whether a given k-regular G-extension $E/k(T)$ has the *Hilbert-Grunwald property*, that is, whether there exists a finite set $\mathcal{S}_{\mathrm{exc}}$ of primes of k such that every Grunwald problem $(G, (L^{(\mathfrak{p})}/k_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{S}})$, with $\mathcal{S}$ disjoint from $\mathcal{S}_{\mathrm{exc}}$, has a solution inside the set of specializations of $E/k(T)$. Recall that this property is always fulfilled, provided we restrict to unramified Grunwald problems [DG11, DG12].

In contrast, our results on the local behaviour of (ramified) specializations show in particular that, for many finite groups G, no k-regular G-extension of $k(T)$ has the Hilbert-Grunwald property:

Theorem 1.5. *Assume that G has a non-cyclic abelian subgroup. Then no k-regular G-extension of $k(T)$ has the Hilbert–Grunwald property.*

We refer to Theorem 6.2 for a more general version with finitely many k-regular G-extensions at the same time. Groups with a non-cyclic abelian subgroup have been classified in the literature relatively explicitly; see, e.g., the classical papers [Zas35] and [Suz55]. Examples of such groups contain, in addition to the obvious S_n for $n \geq 4$ and D_n with n even, all non-abelian simple groups; see the proof of Corollary 6.6. In particular, these groups satisfy the conclusion of Theorem 1.5. Recall that there are

many non-abelian simple groups G such that the only known realizations of G over k are specializations of k-regular G-extensions of $k(T)$, and only finitely many k-regular G-extensions of $k(T)$ are known[3]. For such finite groups G, Theorem 1.5 implies that one cannot solve all Grunwald problems for the group G over the number field k by using only the currently known realizations of G over k.

1.3.3. *Non-existence of finite parametric sets.* Given a finite group G, recall that a set S of k-regular G-extensions $E/k(T)$ is *parametric* if every G-extension of k occurs as a specialization of some extension $E/k(T)$ in S; see Definition 7.1. If S consists of a single extension $E/k(T)$, the extension $E/k(T)$ is called *parametric*. This is a generalization of the *Beckmann-Black problem* (over k), which, with our phrasing, asks whether every finite group G has a parametric set over k [4]. Here, we ask whether a given finite group G has a *finite* parametric set over k.

On the one hand, a given finite group G has a parametric extension over k, provided G has a *one parameter generic polynomial* over k. However, this latter condition is very restrictive. For example, in the case $k = \mathbb{Q}$, only the subgroups of the symmetric group S_3 have a one parameter generic polynomial; see [JLY02, §2.1 & §8.2] [5]. On the other hand, no finite group G was known to have no finite parametric set over the given number field k, until a recent joint work by the first two authors [KL16]. However, the "global" strategy developed in that paper requires G to have a non-trivial proper normal subgroup which satisfies some further properties. In particular, this cannot be used for finite simple groups.

As a further application of our "local" results, we obtain the first examples of finite non-abelian simple groups without finite parametric sets:

Theorem 1.6. *Let $n \geq 4$ be an integer. Then the alternating group A_n has no finite parametric set over k.*

We refer to Theorem 7.2 where we show more generally that a given finite group G has no finite parametric set over the number field k, provided G has a non-cyclic abelian subgroup and some very weak Grunwald property holds. This last property holds in particular if $G = A_n$, by Mestre [Mes90]; see Corollary 7.3.

Acknowledgments. This work is partially supported by the Israel Science Foundation (grant No. 577/15), and the Technion startup grant.

[3] Of course, up to obvious manipulations such as changes of variable, or translates by rational extensions $k(s)/k(t)$, both of which do not yield new specializations.

[4] See, e.g., the survey paper [Dèb01] for more on the Beckmann-Black problem.

[5] Note that no finite group G with a finite parametric set over k, but with no one parameter generic polynomial over k, is available in the literature.

2. Notation and preliminaries

The section is organized as follows. §2.1 is devoted to standard background on Dedekind domains, while we recall classical material on function field extensions in §2.2.

2.1. **Basics on Dedekind domains.** For more on below, we refer to [Ser79].

2.1.1. *Residue, localization, and completion.* Let R be a domain of characteristic zero, and k its fraction field. Given a *prime* $\mathfrak{p}$ of k, i.e., given a non-zero prime ideal $\mathfrak{p}$ of R, the *residue field* $\overline{k}_{\mathfrak{p}}$ of R at $\mathfrak{p}$ is the fraction field $\mathrm{Frac}(R/\mathfrak{p})$ of $R/\mathfrak{p}$. *We shall assume that* $\overline{k}_{\mathfrak{p}}$ *is perfect.* The local ring $R_{(\mathfrak{p})} := \{x/y \,:\, (x,y) \in R^2 \text{ and } y \notin \mathfrak{p}\}$ is the *localization* of R at $\mathfrak{p}$. The unique maximal ideal of $R_{(\mathfrak{p})}$ is $\mathfrak{p}R_{(\mathfrak{p})}$, and the corresponding residue field $R_{(\mathfrak{p})}/\mathfrak{p}R_{(\mathfrak{p})}$ is canonically isomorphic to $\overline{k}_{\mathfrak{p}}$. If $\mathfrak{p}R_{(\mathfrak{p})}$ is principal, there is a discrete valuation $v_{\mathfrak{p}}$ on k whose valuation ring is $R_{(\mathfrak{p})}$. Let $k_{\mathfrak{p}}$ be the *completion* of k with respect to $v_{\mathfrak{p}}$. There is a unique valuation on $k_{\mathfrak{p}}$ extending $v_{\mathfrak{p}}$, the residue field of which coincides with $\overline{k}_{\mathfrak{p}}$ (up to canonical isomorphism).

2.1.2. *Dedekind domains.* From now on, we assume that R is a Dedekind domain.

Let L/k be a finite extension. The integral closure S of R in L is also a Dedekind domain. Let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$. The residue field $\overline{L}_{\mathfrak{P}}$ $(= S/\mathfrak{P})$ is a finite extension of $\overline{k}_{\mathfrak{p}}$. The *residue degree* of L/k at $\mathfrak{P}$ is the degree $f_{\mathfrak{P}|\mathfrak{p}} := [\overline{L}_{\mathfrak{P}} : \overline{k}_{\mathfrak{p}}]$ of this finite extension. The maximal positive integer $e := e_{\mathfrak{P}|\mathfrak{p}}$ for which $\mathfrak{P}^e$ is contained in $\mathfrak{p}S$ is the *ramification index* of $\mathfrak{P}$ in L/k. The prime $\mathfrak{p}$ is *ramified* in L/k if there exists a prime $\mathfrak{P}$ lying over it with ramification index $e_{\mathfrak{P}|\mathfrak{p}} > 1$, and *unramified* otherwise. It is *totally ramified* if $e_{\mathfrak{P}|\mathfrak{p}} = [L : k]$ for the unique prime $\mathfrak{P}$ lying over $\mathfrak{p}$, and *totally split* in L/k if $\mathfrak{p}$ is unramified in L/k, and if $f_{\mathfrak{P}|\mathfrak{p}} = 1$ for every prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$.

From now on, we assume that the extension L/k is Galois with Galois group G. The subgroup of G which consists of all elements σ such that $\sigma(\mathfrak{P}) = \mathfrak{P}$ is the *decomposition group* $D_{\mathfrak{P}}$ of L/k at $\mathfrak{P}$. The residue extension $\overline{L}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}}$ is Galois, and the restriction map $D_{\mathfrak{P}} \to \mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}})$ is an epimorphism, whose kernel is the *inertia group* $I_{\mathfrak{P}}$ of L/k at $\mathfrak{P}$. The decomposition groups $D_{\mathfrak{P}_1}$ and $D_{\mathfrak{P}_2}$ (resp., the inertia groups $I_{\mathfrak{P}_1}$ and $I_{\mathfrak{P}_2}$) of two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ lying over $\mathfrak{p}$ in L/k are conjugate in G. When a prime $\mathfrak{P}$ lying over $\mathfrak{p}$ is fixed, we set $D_{\mathfrak{p}} := D_{\mathfrak{P}}$ and $I_{\mathfrak{p}} := I_{\mathfrak{P}}$. One has $I_{\mathfrak{p}} \trianglelefteq D_{\mathfrak{p}}$, the cardinalities $|I_{\mathfrak{p}}|$ and $|D_{\mathfrak{p}}|$ are independent of the choice of the prime $\mathfrak{P}$ lying over $\mathfrak{p}$, and are equal to $e_{\mathfrak{P}|\mathfrak{p}}$ and $e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$, respectively. Similarly, the residue extension $\overline{L}_{\mathfrak{P}}/\overline{k}_{\mathfrak{p}}$ of L/k at $\mathfrak{P}$ does not depend on the choice of $\mathfrak{P}$ (up to $\overline{k}_{\mathfrak{p}}$-isomorphism); we therefore denote it by $\overline{L}_{\mathfrak{p}}/\overline{k}_{\mathfrak{p}}$. The following basic lemma describes explicitly the residue field $\overline{L}_{\mathfrak{p}}$.

Lemma 2.1. *Let $f(X) \in R[X]$ be a monic separable polynomial of positive degree n and splitting field L over k. Denote the roots of $f(X)$ by $y_1, \ldots, y_n$. Let $\mathfrak{p}$ be a prime of k*

such that the discriminant of f is not contained in $\mathfrak{p}$. Then one has $\overline{L}_\mathfrak{p} = \overline{k}_\mathfrak{p}(\overline{y_1}, \dots, \overline{y_n})$, where $\overline{x}$ denotes the reduction of $x \in L$ modulo a prime of L lying over $\mathfrak{p}$.

The completion $L_\mathfrak{P}$ of L at $\mathfrak{P}$ is Galois over $k_\mathfrak{p}$, with Galois group canonically isomorphic to $D_\mathfrak{P}$ (via restriction from $L_\mathfrak{P}$ to L). One has $L_\mathfrak{P} = L \cdot k_\mathfrak{p}$, where $L \cdot k_\mathfrak{p}$ denotes the compositum of L and $k_\mathfrak{p}$ inside a given algebraic closure $\widetilde{k_\mathfrak{p}}$ of $k_\mathfrak{p}$. Since, up to $k_\mathfrak{p}$-isomorphism, this does not depend on the choice of $\mathfrak{P}$, one can speak of the *completion* of L/k at $\mathfrak{p}$, and denote it by $L_\mathfrak{p}/k_\mathfrak{p}$. The maximal subextension of $L_\mathfrak{p}/k_\mathfrak{p}$ which is unramified at $\mathfrak{p}$ equals $L_\mathfrak{p}^{I_\mathfrak{p}}/k_\mathfrak{p}$, where $L_\mathfrak{p}^{I_\mathfrak{p}}$ denotes the fixed field of $I_\mathfrak{p}$ in $L_\mathfrak{p}$; we denote it by $L_\mathfrak{p}^{\mathrm{ur}}/k_\mathfrak{p}$, and call it the *unramified part* of $L_\mathfrak{p}/k_\mathfrak{p}$. Furthermore, fixing a k-embedding σ of L into $\widetilde{k_\mathfrak{p}}$ induces a choice of a prime $\mathfrak{P}$ lying over $\mathfrak{p}$ in L/k, via $\mathfrak{P} := \{x \in L : v_\mathfrak{p}(\sigma(x)) > 0\}$, where $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation on $k_\mathfrak{p}$, extended to $\widetilde{k_\mathfrak{p}}$.

2.2. **Extensions of function fields.** Let $\widetilde{k}$ denote a fixed algebraic closure of a given field k of characteristic zero, and let T be an indeterminate over k.

2.2.1. *Classical background.* Let $E/k(T)$ be a finite Galois extension with Galois group G, and such that E/k is *regular*, that is, such that $E \cap \widetilde{k} = k$. We then say that $E/k(T)$ is a *k-regular G-extension.*

A point t_0 in $\mathbb{P}^1(\widetilde{k})$ is *a branch point* of $E/k(T)$ if the prime ideal $(T - t_0)\,\widetilde{k}[T - t_0]$ of $\widetilde{k}[T - t_0]$ is ramified in $E \cdot \widetilde{k}/\widetilde{k}(T)$ [6]. The extension $E/k(T)$ has finitely many branch points, denoted by $t_1, \dots, t_r$ (one has $r = 0$ if and only if G is trivial). For each $i \in \{1, \dots, r\}$, denote the decomposition group (resp., the inertia group) of $E(t_i)/k(t_i)(T)$ at (a fixed prime of $E(t_i)$ lying over) $(T - t_i)\,k(t_i)[T - t_i]$ by D_{t_i} (resp., by I_{t_i}).

Given $t_0 \in \mathbb{P}^1(k)$, the residue extension of $E/k(T)$ at $(T - t_0)\,k[T - t_0]$ is denoted by E_{t_0}/k, and called the *specialization of $E/k(T)$ at t_0*. It is a finite Galois extension whose Galois group is canonically isomorphic to D_{t_0}/I_{t_0}, where D_{t_0} (resp., I_{t_0}) denotes the decomposition group (resp., the inertia group) of $E/k(T)$ at $(T - t_0)\,k[T - t_0]$.

If k is the fraction field of a Dedekind domain R, we denote the decomposition group (resp., the inertia group) of the specialization E_{t_0}/k at a given non-zero prime ideal $\mathfrak{p}$ of R such that the residue field $\overline{k}_\mathfrak{p}$ is perfect by $D_{t_0,\mathfrak{p}}$ (resp., by $I_{t_0,\mathfrak{p}}$). Note that $D_{t_0,\mathfrak{p}}$ is canonically isomorphic to a subgroup of D_{t_0}/I_{t_0}.

We recall the following well-known lemma, cf. [PV05], which is a standard consequence of Krasner's lemma and the compatibility between the Hilbert specialization property and the weak approximation property of $\mathbb{P}^1$:

Lemma 2.2. *Assume k is a number field with ring of integers R. Let $\mathcal{S}$ be a finite set of primes of k, and $P(T, Y) \in k[T][Y]$ a monic, separable polynomial with splitting*

[6] Replace $T - t_0$ by $1/T$ if $t_0 = \infty$. The compositum $E \cdot \widetilde{k}$ of E and $\widetilde{k}(T)$ is taken in a fixed algebraic closure of $k(T)$ containing $\widetilde{k}$.

field E over $k(T)$. For each $\mathfrak{p} \in \mathcal{S}$, choose $t_\mathfrak{p}$ in k such that $P(t_\mathfrak{p}, Y)$ is separable, and let $(E_{t_\mathfrak{p}})_\mathfrak{p}/k_\mathfrak{p}$ be the completion of $E_{t_\mathfrak{p}}/k$ at $\mathfrak{p}$. Then there exist infinitely many $t_0 \in k$ such that E_{t_0}/k has Galois group G and its completion at $\mathfrak{p}$ is $(E_{t_\mathfrak{p}})_\mathfrak{p}/k_\mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{S}$. Moreover, one may require these specializations E_{t_0}/k to be pairwise linearly disjoint.

2.2.2. *Laurent series fields and their algebraic extensions.* Given $t_0 \in \mathbb{P}^1(k)$, set $\mathfrak{p} := (T-t_0)\,k[T-t_0]$. The unramified part $E_\mathfrak{p}^{\mathrm{ur}}/k((T-t_0))$ of the completion $E_\mathfrak{p}/k((T-t_0))$ of $E/k(T)$ at $\mathfrak{p}$ is of the form $E_{t_0}((T-t_0))/k((T-t_0))$; see [Ser79, page 55]. Furthermore, one has $E_\mathfrak{p} = E_\mathfrak{p}^{\mathrm{ur}}(\sqrt[e]{\alpha(T-t_0)})$ for some $\alpha \in E_{t_0}$ and some positive integer e. Since $E_\mathfrak{p}$ is the splitting field of $X^e - \alpha(T-t_0)$, the e-th roots of unity are contained in $E_\mathfrak{p}$, and then even in $E_\mathfrak{p} \cap \widetilde{k} = E_{t_0}$, giving the following lemma.

Lemma 2.3. *Let t_i be a branch point of $E/k(T)$ of ramification index e_i. Then the specialization $E(t_i)_{t_i}$ contains all e_i-th roots of unity.*

Setting $k' := k(t_i)$, $E' := E(t_i)$, and $\mathfrak{p}_i := (T-t_i)\,k'[T-t_i]$, the completion $E'_{\mathfrak{p}_i}$ is then a solution to the embedding problem $D_{t_i} \xrightarrow{\varphi} \mathrm{Gal}(E_{\mathfrak{p}_i}^{\prime\mathrm{ur}}/k'((T-t_i)))$, where the image is identified with D_{t_i}/I_{t_i} and φ is the natural projection. Since $E'_{\mathfrak{p}_i}$ is a Kummer extension of $E'_{t_i}((T-t_i))$, the conjugation action of D_{t_i} on I_{t_i} is isomorphic to the action on the group of e_i-th roots of unity in E'_{t_i}. Such an embedding problem is then called a *Brauer embedding problem*. See, e.g., [MM99, Chapter IV, §7] for more details.

Finally, we will make use of a theorem about the structure of algebraic power series, which was first stated over the integers by Eisenstein. For our purposes, let R be an integral domain with fraction field k. The general version below can be found, e.g., in [BBC12, Lemma 2.1].

Theorem 2.4. *Let $\alpha = \sum_{n=0}^{\infty} \alpha_n T^n \in k[[T]]$ be algebraic over $k(T)$. Then there exist r and s in R such that $r \cdot (\alpha_n s^n) \in R$ for each $n \geq 0$. In particular, if R is a Dedekind domain, there exist only finitely many prime ideals $\mathfrak{p}$ of R such that α is not in $R_{(\mathfrak{p})}[[T]]$.*

3. Ramification in specializations

In this section, we recall some classical properties on ramification in specializations of function field extensions.

Let k be the fraction field of a Dedekind domain R of characteristic zero, and let $\mathfrak{p}$ be a non-zero prime ideal of R such that $\overline{k}_\mathfrak{p}$ is perfect. Let $v_\mathfrak{p}$ denote the discrete valuation on k with valuation ring $R_{(\mathfrak{p})}$. Let T be an indeterminate over k and G a finite group.

First, we recall the definition of *meeting modulo* $\mathfrak{p}$:

Definition 3.1. (1) Let F/k be a finite extension, R_F the integral closure of R in F, and $\mathfrak{p}_F$ a non-zero prime ideal of R_F. We say that two distinct points t_0 and t_1 in $\mathbb{P}^1(F)$ *meet modulo* $\mathfrak{p}_F$ if either $v_{\mathfrak{p}_F}(t_0) \geq 0$, $v_{\mathfrak{p}_F}(t_1) \geq 0$, and $v_{\mathfrak{p}_F}(t_0 - t_1) > 0$, or $v_{\mathfrak{p}_F}(t_0) \leq 0$,

$v_{\mathfrak{p}_F}(t_1) \leq 0$, and $v_{\mathfrak{p}_F}((1/t_0) - (1/t_1)) > 0$ (where $v_{\mathfrak{p}_F}$ denotes the discrete valuation on F associated with $\mathfrak{p}_F$)[7].
(2) We say that two distinct points t_0 and t_1 in $\mathbb{P}^1(\widetilde{k})$ *meet modulo* $\mathfrak{p}$ if t_0 and t_1 meet modulo a prime ideal of the integral closure of R in $k(t_0, t_1)$ lying over $\mathfrak{p}$.

Note that, if t_0 and t_1 meet modulo $\mathfrak{p}$ and F/k is a finite extension containing $k(t_0, t_1)$, then t_0 and t_1 meet modulo a prime ideal of the integral closure of R in F lying over $\mathfrak{p}$.

In the case where t_0 is k-rational and meets t_1 modulo $\mathfrak{p}$, the following lemma asserts the existence of a unique degree 1 prime lying over $\mathfrak{p}$ at which t_0 and t_1 meet.

Lemma 3.2. *For every $t_1 \in \mathbb{P}^1(\widetilde{k})$, there exists a finite set $\mathcal{S}_1$ of primes of k, depending only on t_1, which satisfies the following property. Suppose $\mathfrak{p} \notin \mathcal{S}_1$ and let $t_0 \in \mathbb{P}^1(k) \backslash \{t_1\}$ be such that t_0 and t_1 meet modulo $\mathfrak{p}$. Then there exists a unique prime $\mathfrak{p}' := \mathfrak{p}'(t_0, t_1, \mathfrak{p})$ lying over $\mathfrak{p}$ in $k(t_1)/k$ with residue degree $f_{\mathfrak{p}'|\mathfrak{p}} = 1$ at which t_0 and t_1 meet.*

Remark 3.3. (1) If t_1 is k-rational, then one has $\mathfrak{p}'(t_0, t_1, \mathfrak{p}) = \mathfrak{p}$.
(2) For each prime ideal $\mathfrak{p}'$ lying over $\mathfrak{p} \notin \mathcal{S}_1$ in $k(t_1)/k$ with residue degree $f_{\mathfrak{p}'|\mathfrak{p}} = 1$, the weak approximation property of $\mathbb{P}^1$ provides infinitely many $t_0 \in k$ such that $\mathfrak{p}'(t_0, t_1, \mathfrak{p}) = \mathfrak{p}'$.

Proof. By part (1) of Remark 3.3, we may assume $t_1 \neq \infty$. We require the set $\mathcal{S}_1$ to contain the (finite) set of primes $\mathfrak{q}$ of k such that the minimal polynomial $m_{t_1}(T)$ of t_1 over k is either not integral at $\mathfrak{q}$ or not separable modulo $\mathfrak{q}$. In particular, for every prime $\mathfrak{p}'$ of $k(t_1)$ lying over $\mathfrak{p}$, we may assume $v_{\mathfrak{p}'}(t_1) \geq 0$ and $\overline{k(t_1)}_{\mathfrak{p}'}$ is generated over $\overline{k}_{\mathfrak{p}}$ by the reduction modulo $\mathfrak{p}'$ of t_1, by Lemma 2.1.

For the existence part, note that, since t_0 and t_1 meet modulo $\mathfrak{p}$, the above provides a prime ideal $\mathfrak{p}'$ lying over $\mathfrak{p}$ in $k(t_1)/k$ such that $v_{\mathfrak{p}'}(t_0) \geq 0$, $v_{\mathfrak{p}'}(t_1) \geq 0$, and $v_{\mathfrak{p}'}(t_0 - t_1) > 0$. Since $\mathfrak{p}$ is not in $\mathcal{S}_1$, and since the reduction modulo $\mathfrak{p}'$ of t_1 equals the reduction $\overline{t_0}$ modulo $\mathfrak{p}'$ of t_0, we have $\overline{k(t_1)}_{\mathfrak{p}'} = \overline{k}_{\mathfrak{p}}(\overline{t_0}) = \overline{k}_{\mathfrak{p}}$, that is, $f_{\mathfrak{p}'|\mathfrak{p}} = 1$.

For the uniqueness part, assume that t_0 and t_1 meet modulo two distinct primes $\mathfrak{p}'_1$ and $\mathfrak{p}'_2$ of $k(t_1)$ lying over $\mathfrak{p}$, both with residue degree 1. Since $m_{t_1}(T)$ is separable modulo $\mathfrak{p}$, the primes $\mathfrak{p}'_1$ and $\mathfrak{p}'_2$ correspond to distinct linear factors $T - a_1$ and $T - a_2$ of the reduction of $m_{t_1}(T)$ in $\overline{k}_{\mathfrak{p}}[T]$, so that $t_1 \equiv a_j$ modulo $\mathfrak{p}'_j$ for each $j \in \{1, 2\}$. As t_0 and t_1 meet modulo $\mathfrak{p}'_j$, the difference $t_0 - t_1$ is in $\mathfrak{p}'_j$. Hence $t_0 - a_j$ is in $\mathfrak{p}'_j \cap k = \mathfrak{p}$. We then get $a_1 \equiv a_2$ modulo $\mathfrak{p}$, which cannot happen. □

Now, we recall the definition of *intersection multiplicity at* $\mathfrak{p}$. Below, the minimal polynomial over k of any given element $t_1 \in \mathbb{P}^1(\widetilde{k})$ is denoted by $m_{t_1}(T)$ (we set $m_{t_1}(T) = 1$ if $t_1 = \infty$). Denote the constant coefficient of $m_{t_1}(T)$ by a_{t_1}. Then the minimal polynomial of $1/t_1$ over k is

[7]We set $1/\infty = 0$, $1/0 = \infty$, $v_{\mathfrak{p}}(\infty) = -\infty$, and $v_{\mathfrak{p}}(0) = \infty$.

- $m_{1/t_1}(T) = (1/a_{t_1})\, T^{\deg(m_{t_1}(T))}\, m_{t_1}(1/T)$ if $t_1 \in \widetilde{k} \setminus \{0\}$,
- $m_{1/t_1}(T) = 1$ if $t_1 = 0$,
- $m_{1/t_1}(T) = T$ if $t_1 = \infty$.

Let t_1 be in $\mathbb{P}^1(\widetilde{k})$ and t_0 in $\mathbb{P}^1(k)$. Assume $v_{\mathfrak{p}}(a_{t_1}) = 0$ if $t_1 \neq 0$ to make the intersection multiplicity well-defined in Definition 3.4 below.

Definition 3.4. *The intersection multiplicity $I_{\mathfrak{p}}(t_0, t_1)$ of t_0 and t_1 at $\mathfrak{p}$* is

$$I_{\mathfrak{p}}(t_0, t_1) = \begin{cases} v_{\mathfrak{p}}(m_{t_1}(t_0)) & \text{if} \quad v_{\mathfrak{p}}(t_0) \geq 0, \\ v_{\mathfrak{p}}(m_{1/t_1}(1/t_0)) & \text{if} \quad v_{\mathfrak{p}}(t_0) \leq 0. \end{cases}$$

Lemma 3.5 below, which is [Leg16b, Lemma 2.5], connects Definitions 3.1 and 3.4.

Lemma 3.5. *Let t_1 be in $\mathbb{P}^1(\widetilde{k})$ and t_0 in $\mathbb{P}^1(k)$. Assume $v_{\mathfrak{p}}(a_{t_1}) = 0$ if $t_1 \neq 0$.*

(1) *If $I_{\mathfrak{p}}(t_0, t_1) > 0$, then t_0 and t_1 meet modulo $\mathfrak{p}$.*
(2) *The converse in* (1) *holds, provided $m_{t_1}(T)$ is in $R_{(\mathfrak{p})}[T]$.*

Finally, we recall the following classical result on ramification in specializations; see, e.g., [Bec91, Proposition 4.2], [Con00], and [Leg16b, §2.2.3].

Let $E/k(T)$ be a k-regular G-extension with branch points $t_1, \dots, t_r$. For every $i \in \{1, \dots, r\}$, denote the inertia group of $E(t_i)/k(t_i)(T)$ at $(T - t_i)\, k(t_i)[T - t_i]$ by I_{t_i}.

Specialization Inertia Theorem. *Assume that $\mathfrak{p}$ is not in some finite set $\mathcal{S}_{\mathrm{bad}}$ of prime ideals of R (depending only on $E/k(T)$)*[8]*. Let $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$.*

(1) *If $\mathfrak{p}$ ramifies in E_{t_0}/k, then t_0 meets some branch point t_i of $E/k(T)$ modulo $\mathfrak{p}$.*
(2) *Suppose that t_0 and t_i meet modulo $\mathfrak{p}$. Then $I_{t_0,\mathfrak{p}}$ is conjugate to $I_{t_i}^{I_{\mathfrak{p}}(t_0,t_i)}$.*

4. Main results

In this section, we state and prove Theorems 4.1, 4.4, and 4.5, which are the most general versions of Theorems 1.1, 1.2, and 1.3, respectively. Throughout this section, we use the notation of §2-3. Let k be the fraction field of a Dedekind domain R of characteristic zero such that, for every prime ideal $\mathfrak{p}$ of R, the residue field $\overline{k}_{\mathfrak{p}}$ is perfect. Given an indeterminate T over k and a finite group G, let $E/k(T)$ be a k-regular G-extension with branch points $t_1, \dots, t_r$. Fix $i \in \{1, \dots, r\}$. Recall that D_{t_i} (resp., I_{t_i}) is the decomposition group (resp., the inertia group) of $E(t_i)/k(t_i)(T)$ at $(T - t_i)\, k[T - t_i]$, and that $D_{t_i,\mathfrak{p}'}$ is the decomposition group of $(E(t_i))_{t_i}/k(t_i)$ at a prime $\mathfrak{p}'$ of $k(t_i)$, so that $D_{t_i,\mathfrak{p}'}$ is canonically identified with a subgroup of D_{t_i}/I_{t_i}. Set $e_i := |I_{t_i}|$, and let $\varphi : D_{t_i} \to D_{t_i}/I_{t_i}$ be the natural projection.

[8] See, e.g., [Leg16b, §2.2.3] for an explicit description of these "bad" primes.

4.1. **Statement of Theorem 4.1.**

Theorem 4.1. *Assume that $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$ and t_i meet modulo a prime $\mathfrak{p}$ of k avoiding a finite set $\mathcal{S}_{\mathrm{exc}}$ of primes of k depending only on $E/k(T)$. Let $\mathfrak{p}' = \mathfrak{p}'(t_0, t_i, \mathfrak{p})$ be the unique prime ideal lying over $\mathfrak{p}$ in $k(t_i)/k$ provided by Lemma 3.2*[9]*.*

(1) *The decomposition group $D_{t_0,\mathfrak{p}}$ is conjugate in G to a subgroup U of D_{t_i} such that $\varphi(U) = D_{t_i,\mathfrak{p}'}$. Moreover, if $I_{\mathfrak{p}}(t_0, t_i)$ is coprime to e_i, one has $U = \varphi^{-1}(D_{t_i,\mathfrak{p}'})$.*
(2) *The unramified part of the completion $E_{t_0} \cdot k_{\mathfrak{p}}$ of E_{t_0} at $\mathfrak{p}$ contains $(E(t_i))_{t_i} \cdot k(t_i)_{\mathfrak{p}'}$, with equality if $I_{\mathfrak{p}}(t_0, t_i)$ is coprime to e_i.*

As the specialization E_{t_0}/k is Galois, the compositum $E_{t_0} \cdot k_{\mathfrak{p}}$ is independent of the embedding of E_{t_0} into a given algebraic closure of $k_{\mathfrak{p}}$. Similarly, $(E(t_i))_{t_i} \cdot k(t_i)_{\mathfrak{p}'}$ is independent of the embedding of $(E(t_i))_{t_i}$ into a given algebraic closure of $k(t_i)_{\mathfrak{p}'}$.

Remark 4.2. (1) Let $\mathfrak{p}$ be a prime of k, not in $\mathcal{S}_{\mathrm{exc}}$, and let $\mathfrak{p}'$ be a prime lying over $\mathfrak{p}$ in $k(t_i)/k$ with residue degree $f_{\mathfrak{p}'|\mathfrak{p}} = 1$. As in part (2) of Remark 3.3, there exist infinitely many $t_0 \in k$ such that t_0 and t_i meet modulo $\mathfrak{p}'$, and such that $I_{\mathfrak{p}}(t_0, t_i)$ is coprime to e_i. Thus, as a consequence part (1) of Theorem 4.1 and of the Specialization Inertia Theorem, there exist infinitely many $t_0 \in k \setminus \{t_1, \dots, t_r\}$ such that $I_{t_0,\mathfrak{p}}$ is conjugate to I_{t_i}, and $D_{t_0,\mathfrak{p}}$ is conjugate to $\varphi^{-1}(D_{t_i,\mathfrak{p}'})$.
(2) Part (2) of Theorem 4.1 implies that the residue degree of $(E(t_i))_{t_i}/k(t_i)$ at $\mathfrak{p}'$ divides that of E_{t_0}/k at $\mathfrak{p}$, with equality if $I_{\mathfrak{p}}(t_0, t_i)$ is coprime to e_i.
(3) The assumption that $I_{\mathfrak{p}}(t_0, t_i)$ is coprime to e_i is necessary in general for the more precise conclusions in parts (1) and (2) of Theorem 4.1, as the following easy example shows. Set $k := \mathbb{Q}$, $E := \mathbb{Q}(\sqrt{T})$, $t_i := 0$, and let p be a prime number. Since $E/\mathbb{Q}(T)$ is totally ramified at t_i, one has $E_{t_i} = \mathbb{Q}$, and $|I_{t_i}| = |D_{t_i}| = 2$. Set $t_0 := \alpha \cdot p^2$, where α denotes a rational number of p-adic valuation 0. Then one has $(E_{t_0})_p = \mathbb{Q}_p$ if α is a square modulo p (and hence $1 = |D_{t_0,p}| < |\varphi^{-1}(D_{t_i,p})| = 2$), whereas $(E_{t_0})_p/\mathbb{Q}_p$ has degree 2 if α is not a square modulo p, and therefore $E_{t_i} \cdot \mathbb{Q}_p \subsetneq E_{t_0} \cdot \mathbb{Q}_p$ in this case.

4.2. **Proof of Theorem 4.1.** By possibly changing the variable T, we may assume that t_i is not equal to ∞, and that t_i is integral over R. For simplicity, set $k' := k(t_i)$, $k'_{\mathfrak{p}'} := k(t_i)_{\mathfrak{p}'}$, $E' := E(t_i)$, $E'_{t_i} := (E(t_i))_{t_i}$, and $S := T - t_i$. From now on, we fix an embedding of E into a given algebraic closure $\widetilde{k'_{\mathfrak{p}'}((S))}$ of $k'_{\mathfrak{p}'}((S))$. Every compositum of fields below has to be understood inside $\widetilde{k'_{\mathfrak{p}'}((S))}$. We break the proof into four steps.

4.2.1. *Step I.* Here we describe the Galois groups of $E' \cdot k'((S))/k'((S))$ and $E' \cdot k'_{\mathfrak{p}'}((S))/k'_{\mathfrak{p}'}((S))$.

First, consider the compositum of E' and $k'((S))$. The restriction of the Galois group $\mathrm{Gal}(E' \cdot k'((S))/k'((S)))$ to $E'/k'(S)$ preserves a prime $\mathfrak{Q}$ of E' lying over the prime

[9]To make this well-defined, we assume in particular that $\mathcal{S}_{\mathrm{exc}}$ contains the set $\mathcal{S}_1$ from Lemma 3.2.

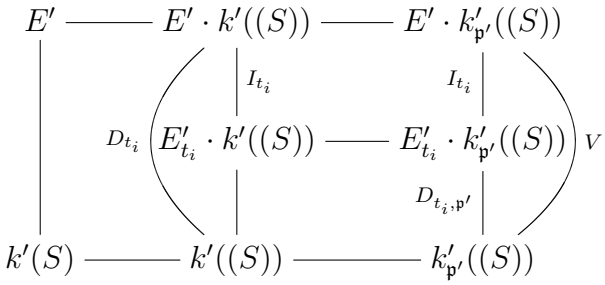
generated by S. Hence we identify $\mathrm{Gal}(E' \cdot k'((S))/k'((S)))$ with the decomposition group D_{t_i} of $E'/k'(S)$ at $\mathfrak{Q}$. Moreover, E'_{t_i}/k' is the residue extension of $E'/k'(S)$ at $\mathfrak{Q}$, and the unramified part of $E' \cdot k'((S))/k'((S))$ is $E'_{t_i} \cdot k'((S))/k'((S))$; see §2.2.2. Thus, $E' \cdot k'((S))/E'_{t_i} \cdot k'((S))$ is totally ramified at the prime generated by S, and its Galois group is identified with the inertia group I_{t_i} of $E'/k'(S)$ at $\mathfrak{Q}$.

Now, consider the compositum $E'_{t_i} \cdot k'_{\mathfrak{p}'}$. This defines an embedding of E'_{t_i} into the algebraic closure of $k'_{\mathfrak{p}'}$ that is contained in $\widetilde{k'_{\mathfrak{p}'}((S))}$, and hence a prime $\mathfrak{P}'$ of E'_{t_i} lying over $\mathfrak{p}'$ such that the restriction of $\mathrm{Gal}(E'_{t_i} \cdot k'_{\mathfrak{p}'}/k'_{\mathfrak{p}'})$ to E'_{t_i}/k' preserves $\mathfrak{P}'$. Therefore, we identify $\mathrm{Gal}(E'_{t_i} \cdot k'_{\mathfrak{p}'}/k'_{\mathfrak{p}'})$ with the decomposition group $D_{t_i,\mathfrak{p}'}$ of E'_{t_i}/k' at $\mathfrak{P}'$.

Next, consider the compositum $E' \cdot k'_{\mathfrak{p}'}((S))$. Its Galois group V over $k'_{\mathfrak{p}'}((S))$ is identified with a subgroup of $D_{t_i} = \mathrm{Gal}(E' \cdot k'((S))/k'((S)))$ via restriction. Note that, as $E' \cdot k'((S))/E'_{t_i} \cdot k'((S))$ is totally ramified, the fields $E' \cdot k'((S))$ and $E'_{t_i} \cdot k'_{\mathfrak{p}'}((S))$ are linearly disjoint over $E'_{t_i} \cdot k'((S))$. Hence $\mathrm{Gal}(E' \cdot k'_{\mathfrak{p}'}((S))/E'_{t_i} \cdot k'_{\mathfrak{p}'}((S)))$ is identified with $I_{t_i} = \mathrm{Gal}(E' \cdot k'((S))/E'_{t_i} \cdot k'((S)))$, so that $\varphi(V) = D_{t_i,\mathfrak{p}'}$.

We then obtain the following diagram of inclusions and Galois groups:

(4.1)



4.2.2. *Step II.* Let R' be the integral closure of R in k'. In this step, we describe the unramified part and the Galois group of the extension $E' \cdot F/F$, where F is the fraction field of $R'_{\mathfrak{p}'}[[S]]$ [10]. Note that $F \subseteq k'_{\mathfrak{p}'}((S))$.

Lemma 4.3. *For every finite extension $M/k'(S)$, there exists a finite set $\mathcal{S}_M$ of primes of k' (depending only on $M/k'(S)$) such that, if $\mathfrak{p}'$ is not in $\mathcal{S}_M$, then the fields $M \cdot F$ and $k'_{\mathfrak{p}'}((S))$ are linearly disjoint over F.*

Proof. Up to replacing $M/k'(S)$ by its Galois closure, we may assume that $M/k'(S)$ is Galois. Given an intermediate field $k'(S) \subseteq M_0 \subseteq M$, let $\alpha := \alpha(M_0)$ be a primitive element of $M_0/k'(S)$. We have

$$\alpha = \sum_{i \geq -n_0} \alpha_i \cdot S^{i/e} \tag{4.2}$$

[10] This domain is the completion of $R'[S]$ at the maximal ideal generated by $\mathfrak{p}'$ and S; see, e.g., [Eis95, Exercise 7.11].

for some positive integer e, some non-negative integer n_0, and coefficients α_i, $i \geq -n_0$, which lie in a finite extension K/k'. By possibly replacing α by $S^{n_0}\alpha$, we may assume $n_0 = 0$. As α is algebraic over $k'(S)$, Theorem 2.4 asserts that the set $\mathcal{T}_{M_0}$ of all primes $\mathfrak{q}'$ of k' such that $v_{\mathfrak{Q}'}(\alpha_j) < 0$ for some $j \geq 0$ and some prime $\mathfrak{Q}'$ of K lying over $\mathfrak{q}'$ is finite, and depends only on α, that is, only on M_0.

Set $\mathcal{S}_M := \cup_{M_0}\mathcal{T}_{M_0}$, where M_0 runs over all intermediate fields in $M/k'(S)$. Suppose that $\mathfrak{p}'$ is not in $\mathcal{S}_M$, and set $F_1 := (M \cdot F) \cap k'_{\mathfrak{p}'}((S))$. To prove the lemma, it suffices to show that $F_1 = F$. Since $F \subseteq F_1 \subseteq M \cdot F$, and since the latter is Galois over F, the field $M_1 := F_1 \cap M$ satisfies $M_1 \cdot F = F_1$. Set $\alpha := \alpha(M_1)$. As α is an element of $k'_{\mathfrak{p}'}((S))$, one has $e = 1$ (with the notation of (4.2)), so that α is an element of $R'_{\mathfrak{p}'}[[S]]$ (as $\mathfrak{p}'$ is not in $\mathcal{S}_M$). Thus, α, and hence M_1, are contained in F. Hence, F_1, which is equal to $M_1 \cdot F$, is equal to F, thus ending the proof of the lemma. □

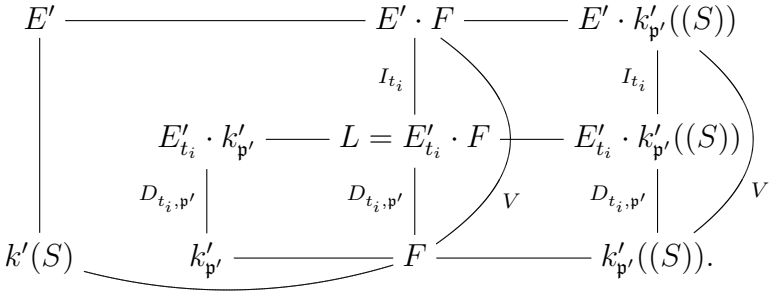
Apply Lemma 4.3 with $M = E' \cdot E'_{t_i}$ to get a finite set $\mathcal{S}_M$ of primes of k', depending only on $E/k(T)$, such that $(E' \cdot E'_{t_i}) \cdot F$ and $k'_{\mathfrak{p}'}((S))$ are linearly disjoint over F, provided $\mathfrak{p}'$ is not in $\mathcal{S}_M$. Set $L := (E'_{t_i} \cdot k'_{\mathfrak{p}'}((S))) \cap (E' \cdot F)$. Since $(E'_{t_i} \cdot F) \cdot k'_{\mathfrak{p}}((S)) \subseteq (E' \cdot F) \cdot k'_{\mathfrak{p}}((S))$, the previous linear disjointness provides $E'_{t_i} \cdot F \subseteq E' \cdot F$. Hence $E'_{t_i} \cdot F \subseteq L$. Conversely, L contains $E'_{t_i} \cdot F$ by its definition and the inclusion $E'_{t_i} \cdot F \subseteq E' \cdot F$. Letting $\mathcal{S}_2$ denote the finite set of primes of k obtained by restricting a prime in $\mathcal{S}_M$, the equality $L = E'_{t_i} \cdot F$ holds, provided $\mathfrak{p} \notin \mathcal{S}_2$. Set $d_{i,\mathfrak{p}'} := [E'_{t_i} \cdot k'_{\mathfrak{p}'} : k'_{\mathfrak{p}'}]$. As F contains $k'_{\mathfrak{p}'} = \mathrm{Frac}(R'_{\mathfrak{p}'})$,

$$d_{i,\mathfrak{p}'} = [E'_{t_i} \cdot k'_{\mathfrak{p}'} : k'_{\mathfrak{p}'}] \geq [E'_{t_i} \cdot F : F] \geq [E'_{t_i} \cdot k'_{\mathfrak{p}'}((S)) : k'_{\mathfrak{p}'}((S))] = d_{i,\mathfrak{p}'},$$

the last equality following from $E'_{t_i} \cdot k'_{\mathfrak{p}'}((S))/k'_{\mathfrak{p}'}((S))$ being unramified. Hence $[E'_{t_i} \cdot F : F] = d_{i,\mathfrak{p}'}$. Moreover, as $E' \cdot F$ and $k'_{\mathfrak{p}'}((S))$ are linearly disjoint over F, the Galois group $\mathrm{Gal}(E' \cdot F/F)$ is identified with V (=$\mathrm{Gal}(E' \cdot k'_{\mathfrak{p}'}((S))/k'_{\mathfrak{p}'}((S)))$; see (4.1)) via restriction. This identification gives $\mathrm{Gal}(E' \cdot F/E'_{t_i} \cdot F) = I_{t_i}$, and $\mathrm{Gal}(E'_{t_i} \cdot F/F) = D_{t_i,\mathfrak{p}'}$.

We then obtain the following diagram of inclusions and Galois groups:

(4.3)



4.2.3. *Step III.* In this step, we reduce the extension $E' \cdot F/F$ modulo $(T - t_0)$. As t_0 and t_i meet modulo $\mathfrak{p}'$ by the definition of $\mathfrak{p}'$, and as t_i is integral over R, one has $v_{\mathfrak{p}'}(t_0 - t_i) > 0$. Hence $T - t_0 = S - (t_0 - t_i)$ is in $R'_{\mathfrak{p}'}[[S]]$. Moreover, as $((t_0 - t_i)^m)_{m \geq 1}$ converges to 0 in $R'_{\mathfrak{p}'}$, the specialization map $R'_{\mathfrak{p}'}[[S]] \to R'_{\mathfrak{p}'}$, which sends S to $t_0 - t_i$, is

well-defined. As it is onto, there is a canonical isomorphism $R'_{\mathfrak{p}'}[[S]]/(T-t_0)\,R'_{\mathfrak{p}'}[[S]] \cong R'_{\mathfrak{p}'}$. In particular, $(T-t_0)\,R'_{\mathfrak{p}'}[[S]]$ is a prime ideal of $R'_{\mathfrak{p}'}[[S]]$. Let $\mathfrak{R}$ be the localization of $R'_{\mathfrak{p}'}[[S]]$ at $(T-t_0)\,R'_{\mathfrak{p}'}[[S]]$. The previous isomorphism shows that the residue field of $\mathfrak{R}$ at $(T-t_0)\,\mathfrak{R}$ is canonically isomorphic to $\mathrm{Frac}(R'_{\mathfrak{p}'}) = k'_{\mathfrak{p}'}$. Let $\mathcal{S}_3$ be the finite set of primes of k which ramify in k'/k. Assuming $\mathfrak{p} \notin \mathcal{S}_3$, and using that $f_{\mathfrak{p}'|\mathfrak{p}} = 1$ by the definition of $\mathfrak{p}'$, we get $k'_{\mathfrak{p}'} = k_{\mathfrak{p}}$. Hence $\mathfrak{R}/(T-t_0)\,\mathfrak{R}$ is canonically isomorphic to $k_{\mathfrak{p}}$. We use this canonical isomorphism to identify the two fields.

The integral closure $\mathfrak{S}$ of $\mathfrak{R}$ in $E' \cdot F$ is a Dedekind domain containing a prime ideal $\mathfrak{M}$ lying over $(T-t_0)\,\mathfrak{R}$. In particular, $\mathfrak{M} \cap E$ is a prime of E lying over $(T-t_0)\,k[T]$. Let $\mathfrak{R}_{t_i}$ (resp., $\mathfrak{M}_{t_i}$) be the restriction to $E'_{t_i} \cdot F$ of $\mathfrak{S}$ (resp., of $\mathfrak{M}$). Since E'_{t_i} and $k'_{\mathfrak{p}'}$ are contained in the residue field $\mathfrak{R}_{t_i}/\mathfrak{M}_{t_i}$, and since $[E'_{t_i} \cdot k'_{\mathfrak{p}'} : k'_{\mathfrak{p}'}] = d_{i,\mathfrak{p}'} = [E'_{t_i} \cdot F : F]$, we have $\mathfrak{R}_{t_i}/\mathfrak{M}_{t_i} = E'_{t_i} \cdot k'_{\mathfrak{p}'}$. Thus, we have the following diagram of inclusions:

$$
\begin{array}{ccc}
E_{t_0} = \overline{E}_{\mathfrak{M}\cap E} & \longrightarrow & \mathfrak{S}/\mathfrak{M} \\
\big| & & \big| \\
 & & \mathfrak{R}_{t_i}/\mathfrak{M}_{t_i} = E'_{t_i} \cdot k'_{\mathfrak{p}'} \\
 & & \big| \\
k & \longrightarrow & \mathfrak{R}/(T-t_0)\,\mathfrak{R} = k_{\mathfrak{p}} = k'_{\mathfrak{p}'}.
\end{array}
\tag{4.4}
$$

Now, we claim that $\mathfrak{S}/\mathfrak{M}$ is equal to the compositum of $k_{\mathfrak{p}}$ and E_{t_0}, provided $\mathfrak{p}$ is not in some finite set of primes of k defined below. Indeed, let $P(T,Y) \in R[T][Y]$ be the minimal polynomial over $k(T)$ of some primitive element of $E/k(T)$, assumed to be integral over $R[T]$. If $P(t_0,Y)$ is not separable, then t_0 belongs to the finite set D of all roots in k of the discriminant $\Delta(T) \in R[T]$ of $P(T,Y)$ which are not branch points of $E/k(T)$. As t_0 and t_i meet modulo $\mathfrak{p}$, the inseparability of $P(t_0,Y)$ implies that $\mathfrak{p}$ is in the finite set $\mathcal{S}_4$ of primes $\mathfrak{q}$ of k such that $v_{\mathfrak{q}'}(d-t_i) > 0$ for some $d \in D$ and some prime $\mathfrak{q}'$ of k' lying over $\mathfrak{q}$. Henceforth, we shall assume that $\mathfrak{p}$ is not in $\mathcal{S}_4$, and then that $P(t_0,Y)$ is separable. Denote the roots of $P(T,Y)$ in E by $y_1,\dots,y_n$, and their reductions modulo $\mathfrak{M} \cap E$ by $\overline{y}_1,\dots,\overline{y}_n$, respectively. As $\Delta(t_0) \neq 0$, the discriminant $\Delta(T)$ is not in $(T-t_0)\,\mathfrak{R}$. Since $E' \cdot F$ is generated by $y_1,\dots,y_n$ over F, the residue field $\mathfrak{S}/\mathfrak{M}$ is generated by $\overline{y}_1,\dots,\overline{y}_n$ over $\mathfrak{R}/(T-t_0)\,\mathfrak{R} = k_{\mathfrak{p}}$ by Lemma 2.1. Thus, one has $\mathfrak{S}/\mathfrak{M} = E_{t_0} \cdot k_{\mathfrak{p}}$, proving the claim. The general containment in part (2) of Theorem 4.1 follows from (4.4), provided $\mathfrak{p}$ is not in $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \mathcal{S}_4$.

4.2.4. *Step IV.* We describe the decomposition group of $E' \cdot F/F$ at a prime lying over $(T-t_0)$ both as a subgroup of V and as a subgroup of D_{t_0}. Assume that $\mathfrak{p} \notin \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \mathcal{S}_4$, so that we are in the situation of (4.3) and (4.4). Up to replacing D_{t_0}

by a conjugate of it, we may assume that D_{t_0} is the decomposition group of $E/k(T)$ at $\mathfrak{M} \cap E$. Let U be the decomposition group of $E' \cdot F/F$ at $\mathfrak{M}$, so that it identifies via restriction with a subgroup of D_{t_0}. As the prime of $k[T]$ generated by $T - t_0$ is unramified in $E/k(T)$, it is also unramified in $E' \cdot F/F$. Thus, U (resp., D_{t_0}) is also the Galois group of $E_{t_0} \cdot k_\mathfrak{p}/k_\mathfrak{p}$ (resp., of E_{t_0}/k). Hence the restriction of U to E_{t_0}/k is the decomposition group of some prime of E_{t_0} lying over $\mathfrak{p}$. Thus, we may identify U with $D_{t_0,\mathfrak{p}}$.

On the other hand, U is a subgroup of $\mathrm{Gal}(E' \cdot F/F)$. The latter is identified with V in Step II (§4.2.2), and hence is a subgroup of D_{t_i} via the identification in Step I (§4.2.1). Moreover, $\varphi(U)$ is the decomposition group of $E'_{t_i} \cdot F/F$ at $\mathfrak{M}_{t_i}$. As shown in Step III (§4.2.3), one has $\mathrm{Gal}(E'_{t_i} \cdot F/F) = \mathrm{Gal}(E'_{t_i} \cdot k_{\mathfrak{p}'}/k_{\mathfrak{p}'})$. But the latter is $D_{t_i,\mathfrak{p}'}$ by Step II. Hence $\varphi(U) = D_{t_i,\mathfrak{p}'}$, thus proving the general case of part (1) of Theorem 4.1.

Finally, assume that $I_\mathfrak{p}(t_0, t_i)$ is coprime to e_i. Let $I_\mathfrak{M}$ denote the inertia group of $E' \cdot F/F$ at $\mathfrak{M}$. Since $E'_{t_i} \cdot F/F$ is unramified at $\mathfrak{M}_{t_i}$, one has $I_\mathfrak{M} \subseteq \mathrm{Gal}(E' \cdot F/E'_{t_i} \cdot F)$ $(= I_{t_i}$; see §4.2.2). Set $\mathcal{S}_{\mathrm{exc}} := \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \mathcal{S}_4 \cup \mathcal{S}_{\mathrm{bad}}$, where $\mathcal{S}_{\mathrm{bad}}$ is the finite set of primes of k from the Specialization Inertia Theorem (§3), and assume that $\mathfrak{p}$ is not in $\mathcal{S}_{\mathrm{exc}}$. As $I_\mathfrak{p}(t_0, t_i)$ is coprime to e_i, one has $|I_{t_0,\mathfrak{p}}| = e_i$ by the Specialization Inertia Theorem. Since the conjugation of U to $D_{t_0,\mathfrak{p}}$ sends $I_\mathfrak{M}$ to $I_{t_0,\mathfrak{p}}$, we also have $|I_\mathfrak{M}| = e_i$. As $I_\mathfrak{M}$ is a subgroup of I_{t_i}, and since $|I_{t_i}| = e_i$, we get the equality $I_\mathfrak{M} = I_{t_i}$. Thus, I_{t_i} is contained in U, and $\mathfrak{M}_{t_i}$ is totally ramified in $E' \cdot F/E'_{t_i} \cdot F$. Hence $U = \varphi^{-1}(D_{t_i,\mathfrak{p}'})$, and $(E_{t_0} \cdot k_\mathfrak{p})^{\mathrm{ur}} = \mathfrak{R}_{t_i}/\mathfrak{M}_{t_i} = E'_{t_i} \cdot k'_{\mathfrak{p}'}$, completing the proof of Theorem 4.1.

4.3. **On specifying completions in specializations.** Theorem 4.1 restricts the structure of the completion $(E_{t_0})_\mathfrak{p}$ at $\mathfrak{p}$ of E_{t_0}. Namely, it implies that $(E_{t_0})_\mathfrak{p}$ contains the field $N^{(\mathfrak{p})} := (E(t_i))_{t_i} \cdot k(t_i)_{\mathfrak{p}'}$ whose Galois group over $k(t_i)_{\mathfrak{p}'}$ is $D_{t_i,\mathfrak{p}'}$, and that the Galois group $\mathrm{Gal}((E_{t_0})_\mathfrak{p}/k_\mathfrak{p})$ is a subgroup of $\varphi^{-1}(D_{t_i,\mathfrak{p}'})$, where $\varphi : D_{t_i} \to D_{t_i}/I_{t_i}$ is the natural projection. The following theorem shows that this is the only restriction for extensions of $k_\mathfrak{p}$ with Galois group $\varphi^{-1}(D_{t_i,\mathfrak{p}'})$:

Theorem 4.4. *Let $\mathcal{S}$ be a finite set of primes of k, disjoint from some finite set $\mathcal{S}'_{\mathrm{exc}}$ depending only on $E/k(T)$. For each $\mathfrak{p} \in \mathcal{S}$, assume that there exists $i := i(\mathfrak{p}) \in \{1, \dots, r\}$ and a prime $\mathfrak{p}'$ lying over $\mathfrak{p}$ in $k(t_i)/k$ with residue degree 1, and let $L^{(\mathfrak{p})}/k_\mathfrak{p}$ be a finite Galois extension containing $N^{(\mathfrak{p})} := (E(t_i))_{t_i} \cdot k(t_i)_{\mathfrak{p}'}$ such that there exists an isomorphism ψ from $\mathrm{Gal}(L^{(\mathfrak{p})}/k_\mathfrak{p})$ to $\varphi^{-1}(D_{t_i,\mathfrak{p}'})$ which maps $\mathrm{Gal}(L^{(\mathfrak{p})}/N^{(\mathfrak{p})})$ onto I_{t_i}. Then there exist infinitely many $t_0 \in k$ such that the completion of E_{t_0}/k at $\mathfrak{p}$ equals $L^{(\mathfrak{p})}/k_\mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{S}$. Moreover, if k is a number field, we may assume that these specializations of $E/k(T)$ have Galois group G.*

Proof. Fix a prime $\mathfrak{p} \in \mathcal{S}$. As in §4.2, set $k' := k(t_i)$, $k'_{\mathfrak{p}'} := k(t_i)_{\mathfrak{p}'}$, $E' := E(t_i)$, $E'_{t_i} := (E(t_i))_{t_i}$, and $S := T - t_i$. Moreover, set $N := N^{(\mathfrak{p})}$, and $\Gamma := \varphi^{-1}(D_{t_i,\mathfrak{p}'})$. As shown in Step I of the proof of Theorem 4.1 (§4.2.1), one has $\mathrm{Gal}(N/k_\mathfrak{p}) = D_{t_i,\mathfrak{p}'}$. Then

all fields $L^{(\mathfrak{p})}$ with the properties mentioned in Theorem 4.4 are solution fields to the embedding problem $\Gamma \xrightarrow{\varphi} \mathrm{Gal}(N/k_{\mathfrak{p}})$. Since I_{t_i} (resp., Γ) is the inertia group (resp., the Galois group) of $E' \cdot k'_{\mathfrak{p}'}((S))/k'_{\mathfrak{p}'}((S))$ (as shown in Step I of the proof of Theorem 4.1 (§4.2.1)), the action of Γ on the cyclic kernel I_{t_i} is isomorphic to the action on e_i-th roots of unity in N (see §2.2.2). The above embedding problem is then a Brauer embedding problem. By [MM99, Chapter IV, Theorem 7.2], if $x \in N$ is chosen such that $N(\sqrt[e_i]{x})$ is a solution field to this embedding problem, then all the solutions fields are of the form $N(\sqrt[e_i]{\beta x})$ with $\beta \in k_{\mathfrak{p}}^{\times}$. Furthermore, upon multiplying β by a suitable e_i-th power, we can require βx to be of positive $\mathfrak{p}$-adic valuation.

The field $E' \cdot k'((S))$ is generated over $E'_{t_i} \cdot k'((S))$ by $\sqrt[e_i]{\alpha S}$ for some $\alpha \in E'_{t_i}$; see §2.2.2. Up to enlarging the set $\mathcal{S}'_{\mathrm{exc}}$, we may assume that α is of $\mathfrak{p}$-adic valuation 0. Set $M := (E'_{t_i} \cdot k'(S))(\sqrt[e_i]{\alpha S})$, and consider the field F from Step II of the proof of Theorem 4.1 (§4.2.2). Assume that $\mathcal{S}'_{\mathrm{exc}}$ contains the set $\mathcal{S}_{\mathrm{exc}}$ from Theorem 4.1. Then $(E' \cdot M) \cdot F$ and $k'_{\mathfrak{p}'}((S))$ are linearly disjoint over F by Lemma 4.3. But one also has $(M \cdot F) \cdot k'_{\mathfrak{p}'}((S)) = E' \cdot k'_{\mathfrak{p}'}((S))$. Hence $M \cdot F = E' \cdot F$.

Thus, we have $E' \cdot F = (E'_{t_i} \cdot F)(\sqrt[e_i]{\alpha S})$. Next, we choose $t_0 \in k_{\mathfrak{p}}$ with $I_{\mathfrak{p}}(t_0, t_i) > 0$ and specialize $E' \cdot F/F$ at $T - t_0$ as in Step III of the proof of Theorem 4.1 (§4.2.3). Since $E'_{t_i} \cdot F$ specializes to $E'_{t_i} \cdot k'_{\mathfrak{p}'}$ and $\sqrt[e_i]{\alpha S}$ specializes to $\sqrt[e_i]{\alpha(t_0 - t_i)}$, Lemma 2.1 yields that all fields of the form $(E'_{t_i} \cdot k'_{\mathfrak{p}'})(\sqrt[e_i]{\alpha\pi})$ $(= N(\sqrt[e_i]{\alpha\pi}))$, with π an element of $k_{\mathfrak{p}} = k'_{\mathfrak{p}'}$ of positive $\mathfrak{p}$-adic valuation, can be reached via specializing T to $t_0 \in k_{\mathfrak{p}}$. Hence, if $N(\sqrt[e_i]{x})$ is one of the fields obtained in this way, then we reach all fields of the form $N(\sqrt[e_i]{\beta x})$, where β is any element of $k_{\mathfrak{p}}^{\times}$ such that βx is of positive $\mathfrak{p}$-adic valuation. As shown above, this covers in particular the extension $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$. Krasner's lemma shows that $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$ can even be obtained by restricting to specialization values $t_{\mathfrak{p}} \in k$. The extension $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$ therefore equals $(E_{t_{\mathfrak{p}}})_{\mathfrak{p}}/k_{\mathfrak{p}}$, the latter being the specialization of $E'_{t_i} \cdot F/F$ at $T - t_{\mathfrak{p}}$.

Finally, choose $t_0 \in k$ sufficiently close $\mathfrak{p}$-adically to every $t_{\mathfrak{p}} \in \mathcal{S}$. This yields the assertion in the general case. In the number field case, Lemma 2.2 provides the conclusion on the Galois group of the produced specializations. □

4.4. **On specifying inertia and decomposition groups of specializations.** Our next result is devoted to a re-occurrence property for subgroups of G appearing as decomposition groups of specializations, in the case where k is a number field.

Theorem 4.5. *Assume that k is a number field, and let s be a positive integer. Given $j \in \{1, \dots, s\}$, choose a branch point $t_{i(j)}$ of $E/k(T)$, and an element $\tau_{i(j)}$ of $D_{t_{i(j)}}$. Then there exist s infinite sets $\mathcal{S}_1, \dots, \mathcal{S}_s$ of primes of k which satisfy the following property. For every tuple $(\mathfrak{p}_1, \dots, \mathfrak{p}_s) \in \mathcal{S}_1 \times \cdots \times \mathcal{S}_s$ of distinct primes, there exist infinitely many t_0 in k for which E_{t_0}/k is a G-extension whose decomposition group (resp., inertia group) at $\mathfrak{p}_j$ is $\langle I_{t_{i(j)}}, \tau_{i(j)} \rangle$ (resp., $I_{t_{i(j)}}$) for $j = 1, \dots, s$.*

Proof. By Lemma 2.2, we may assume $s = 1$, and only prove condition (2). As before, set $i := i(1)$, $t_i := t_{i(1)}$, $\tau := \tau_{i(1)}$, $k' := k(t_i)$, and $E'_{t_i} := (E(t_i))_{t_i}$. Let $\overline{\tau}$ be the image of τ under the natural projection $D_{t_i} \to D_{t_i}/I_{t_i}$, and let C be the conjugacy class in D_{t_i}/I_{t_i} of $\overline{\tau}$. By part (1) of Theorem 4.1 and part (1) of Remark 4.2, it suffices to show that there exists an infinite set $\mathcal{S}$ of primes of k such that, for every $\mathfrak{p} \in \mathcal{S}$, there exists a prime $\mathfrak{p}'$ lying over $\mathfrak{p}$ in k'/k, with residue degree $f_{\mathfrak{p}'|\mathfrak{p}} = 1$, and such that the *Frobenius* $\mathrm{Frob}_{\mathfrak{p}'}(E'_{t_i}/k')$ lies in C. By the Chebotarev density theorem, the natural density of the set $\mathcal{S}'$ of all primes $\mathfrak{p}'$ of k' such that $\mathrm{Frob}_{\mathfrak{p}'}(E'_{t_i}/k')$ lies in C equals $|C| \cdot |I_{t_i}|/|D_{t_i}|$. This remains true for the set $\mathcal{S}'' = \{\mathfrak{p}' \in \mathcal{S}' : f_{\mathfrak{p}'|\mathfrak{p}'\cap k} = 1\}$, since the set of residue degree 1 primes $\mathfrak{p}'$ of k' is of natural density 1, by the prime number theorem for number fields. In particular, the set of all primes $\mathfrak{p}$ of k which are contained in a prime $\mathfrak{p}' \in \mathcal{S}''$ is infinite, completing the proof. □

5. Application to G-crossed products and admissibility

This section is devoted to our application to G-crossed products over number fields. We state and prove our admissibility criterion, Theorem 5.2, in §5.2, and apply it to obtain explicit families of examples in §5.3. For this section, let k be a number field, R its ring of integers, T an indeterminate over k, and G a finite group.

5.1. **Background.** Recall that a group G is called *k-admissible* if there exists a G-crossed product division algebra with center k. A G-extension L/k such that L is a maximal subfield of a G-crossed product division algebra is called *k-adequate.* To prove Theorem 5.2, we need Schacher's admissibility criterion [Sch68, §2] over number fields:

Theorem 5.1. *Let L/k be a G-extension. Then L is k-adequate if and only if, for each prime number p dividing $|G|$, there exist two distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of R such that the decomposition group of L/k at $\mathfrak{p}_i$ contains a p-Sylow subgroup of G for $i = 1, 2$.*

5.2. **A new general admissibility criterion.**

Theorem 5.2. *Assume that G has a k-regular realization $E/k(T)$ such that, for every prime number p such that G has a non-cyclic p-Sylow subgroup, the following holds:*

(H) *for some branch point t_i of $E/k(T)$, the decomposition group D_{t_i} contains a p-Sylow subgroup P of G such that PI_{t_i}/I_{t_i} is cyclic.*

Then there exist infinitely many pairwise linearly disjoint k-adequate G-extensions of k, arising as specializations of $E/k(T)$. In particular, G is k-admissible.

Proof. Let p be a prime number dividing $|G|$, and let P be a p-Sylow subgroup of G. First, assume that P is cyclic. Let $t_p \in k$ be such that E_{t_p}/k has Galois group G. By the Chebotarev density theorem, there exist infinitely many prime ideals $\mathfrak{p}$ of R such that $D_{t_p,\mathfrak{p}}$ contains P. Now, assume that P is not cyclic. Let $t_i(p)$ be a branch point of $E/k(T)$ such that the decomposition group $D_{t_i(p)}$ contains P, and such that

$PI_{t_i(p)}/I_{t_i(p)}$ is cyclic (condition (H)). Then, by Theorem 4.5, there exists an infinite set $\mathcal{S}_p$ of prime ideals of R such that, for each $\mathfrak{p} \in \mathcal{S}_p$, there exist infinitely many $t_p \in k$ such that $D_{t_p,\mathfrak{p}} = PI_{t_i(p)}$. By applying Lemma 2.2, we obtain $t_0 \in k$ such that E_{t_0}/k is a G-extension and, for each p dividing $|G|$, one has $D_{t_0,\mathfrak{p}} = PI_{t_i(p)}$ for at least two distinct primes $\mathfrak{p}$ of k, verifying Theorem 5.1. □

5.3. **Examples.** Roughly speaking, in order to apply Theorem 5.2, one has to produce k-regular realizations of G with "sufficiently large" ramification indices and residue degrees at some branch points. Ramification indices can often be prescribed purely group-theoretically (e.g., via the *rigidity method*). To ensure "large" residue degrees we use Lemma 2.3. This method yields a large class of new examples. Below, we derive the first $\mathbb{Q}$-admissibility results for infinite families of finite non-abelian simple groups. More precisely, Theorems 5.3 and 5.4 below cover 62.5% of the groups $\mathrm{PSL}_2(\mathbb{F}_p)$.

Theorem 5.3. *Assume that k does not contain $\sqrt{-1}$. Let p be a prime number such that either $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$. Then the groups $\mathrm{PSL}_2(\mathbb{F}_p)$ and $\mathrm{PGL}_2(\mathbb{F}_p)$ are k-admissible.*

Proof. Recall that $\mathrm{PGL}_2(\mathbb{F}_p)$ has order $(p-1)p(p+1)$. Then, by our assumption on p, the 2-Sylow subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$ (resp., of $\mathrm{PSL}_2(\mathbb{F}_p)$) have order 8 (resp., 4). By [MM99, Chapter I, Corollary 8.10], there exists a k-regular $\mathrm{PGL}_2(\mathbb{F}_p)$-extension $E/k(T)$ with k-rational branch points t_1, t_2, and t_3, and such that the inertia groups I_{t_1}, I_{t_2}, and I_{t_3} are generated by elements in the conjugacy classes $2B$, $4A$, and pA of $\mathrm{PGL}_2(\mathbb{F}_p)$, respectively (according to the ATLAS notation [C$^+$85]). Consider the branch point t_2 of $E/k(T)$ with ramification index 4. By Lemma 2.3, and as k does not contain $\sqrt{-1}$, the residue degree at this branch point is divisible by 2. It then remains to combine Theorem 5.2 and the classical fact that the Sylow subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$ of odd order are cyclic to get that $\mathrm{PGL}_2(\mathbb{F}_p)$ is k-admissible.

Furthermore, the fixed field of $\mathrm{PSL}_2(\mathbb{F}_p)$ in E is a rational function field, say $k(S)$, by, e.g., [Ser92, Lemma 4.5.1], that has degree 2 over $k(T)$. Denote by s_2 the unique point lying over t_2 in $k(S)/k(T)$. Then s_2 is a branch point of $E/k(S)$ with ramification index 2, and the residue degree at s_2 in $E/k(S)$ is divisible by 2. As above, we conclude that $\mathrm{PSL}_2(\mathbb{F}_p)$ is k-admissible. □

Theorem 5.4. *Let p be a prime number such that the following two conditions hold:*

(1) *either $p \equiv 7 \pmod{16}$ or $p \equiv 9 \pmod{16}$,*
(2) *either $p \equiv 2 \pmod 5$ or $p \equiv 3 \pmod 5$.*

Assume that k contains neither $\sqrt{-1}$ nor $\sqrt{p^\star}$, where $p^\star = (-1)^{(p-1)/2}p$. Then the group $\mathrm{PSL}_2(\mathbb{F}_p)$ is k-admissible.

Proof. By condition (1), the 2-Sylow subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$ have order 8. Moreover, 5 is not a square modulo p by condition (2). By Malle [MM99, Chapter I, Theorem 7.10],

one then has a $\mathbb{Q}$-regular $\mathrm{PSL}_2(\mathbb{F}_p)$-extension of $\mathbb{Q}(T)$ with 4 branch points, and the inertia groups generated by elements in the conjugacy classes $4A$, $4A$, pA, and pB of $\mathrm{PSL}_2(\mathbb{F}_p)$ (according to the ATLAS notation). The proof of that theorem also gives the position of the branch points of this $\mathbb{Q}$-regular extension. Namely, in the notation of that proof, the $\mathbb{Q}$-regular realization of $\mathrm{PSL}_2(\mathbb{F}_p)$ is $E/\mathbb{Q}(v)$, and the branch points with ramification index 4 are the roots of the equation $u^2 - 6u + 25 = 0$, where u is related to v via $v := \sqrt{p^\star}(u+5)/(u-5)$. From the above data, one computes that the fields $\mathbb{Q}(v_i)$, where v_i is a branch point of ramification index 4, do not contain $\sqrt{-1}$. In fact, one has $v_i = \pm 2\sqrt{-p^\star}$. Clearly, all of the above remains true for the extension $E\cdot k/k(v)$ instead of $E/\mathbb{Q}(v)$. In particular, as k contains neither $\sqrt{-1}$ nor $\sqrt{p^\star}$, one has $\sqrt{-1} \notin k(v_i)$. By Lemma 2.3, the residue degree at a branch point of $E \cdot k/k(v)$ with ramification index 4 is divisible by 2. Hence the decomposition group at such a branch point is of order divisible by 8. It then remains to apply Theorem 5.2 to conclude. □

6. Application to the Hilbert-Grunwald property

The present section is devoted to our application to the Hilbert-Grunwald property. We state and prove Theorem 6.2, which is a more general version of Theorem 1.5, and show that it applies to any finite non-abelian simple group; see Corollary 6.6. For this section, let k be a number field, R its ring of integers, T an indeterminate over k, and G a finite group. Given finitely many k-regular G-extensions $E_1/k(T)$, …, $E_s/k(T)$, we are interested in the following question, for which the partial positive answer provided by Theorem 4.4 is a natural motivation:

Question 6.1. *Does there exist a finite set $\mathcal{S}_{\mathrm{exc}}$ of non-zero prime ideals of R such that every Grunwald problem $(G, (L^{(\mathfrak{p})}/k_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{S}})$, with $\mathcal{S}$ disjoint from $\mathcal{S}_{\mathrm{exc}}$, has a solution inside the union of the sets of specializations of $E_1/k(T)$, …, $E_s/k(T)$?*

It follows from earlier works by the first two authors [Leg16a, Kön17] that, for each non-trivial finite group G for which there exists a k-regular G-extension of $k(T)$, there always is one of these realizations for which the answer to Question 6.1 is negative.

In Theorem 6.2 below, we show that the answer to Question 6.1 is in fact *always* negative for many finite groups:

Theorem 6.2. *Assume that G has a non-cyclic abelian subgroup. Then the answer to Question 6.1 is negative for all finite sets of k-regular G-extensions of $k(T)$.*

The proof of Theorem 6.2 requires the following auxiliary result, which strengthens the special case of Theorem 4.5 where $\tau_{i(j)}$ is chosen to be the identity element of $D_{t_{i(j)}}$.

Proposition 6.3. *Let $E/k(T)$ be a k-regular G-extension. Then there exists a number field $F \supseteq k$ that depends only on $E/k(T)$ and that satisfies the following. Let $\mathfrak{p}$ be a prime ideal of R that is totally split in F/k (up to finitely many exceptions depending only on $E/k(T)$). Then the decomposition group of E_{t_0}/k at $\mathfrak{p}$ is cyclic for all $t_0 \in \mathbb{P}^1(k)$.*

Proof. Denote the compositum of the residue fields $(E(t_1))_{t_1}, \dots, (E(t_r))_{t_r}$ of $E/k(T)$ at the branch points $t_1, \dots, t_r$ by F. Let $\mathfrak{p}$ be a non-zero prime ideal of R that is totally split in F/k, and let t_0 be in $\mathbb{P}^1(k)$. First, assume that t_0 is in $\{t_1, \dots, t_r\}$. Then, by the definition of F, the decomposition group $D_{t_0,\mathfrak{p}}$ of E_{t_0}/k at $\mathfrak{p}$ is trivial. Now, assume that t_0 is not in $\{t_1, \dots, t_r\}$. If t_0 does not meet any branch point of $E/k(T)$ modulo $\mathfrak{p}$, then, by the Specialization Inertia Theorem (§3), $\mathfrak{p}$ is unramified in E_{t_0}/k (up to excluding finitely many primes of k). Hence $D_{t_0,\mathfrak{p}}$ is cyclic. So we may assume that t_0 meets some branch point t_i modulo $\mathfrak{p}$. As $\mathfrak{p}$ is totally split in F/k, part (1) of Theorem 4.1 shows that $D_{t_0,\mathfrak{p}}$ is contained in the inertia group I_{t_i} of $E(t_i)/k(t_i)(T)$ at $(T-t_i)\,k(t_i)[T-t_i]$ (up to excluding finitely many primes of k). As I_{t_i} is cyclic, we are done. □

Remark 6.4. If finitely many extensions $E_1/k(T), \dots, E_s/k(T)$ are given, each with a suitable number field F_i as in Proposition 6.3, then the conclusion clearly holds simultaneously for (the specializations of) $E_1/k(T), \dots, E_s/k(T)$, if $\mathfrak{p}$ is totally split in the composite extension $F_1 \cdots F_s/k$ (up to excluding finitely many primes of k).

Proof of Theorem 6.2. Given a positive integer s, let $\{E_1/k(T), \dots, E_s/k(T)\}$ be a finite set of k-regular G-extensions. Let F be a number field containing k such that, for every non-zero prime ideal $\mathfrak{p}$ of R that is totally split in F/k (outside some finite set $\mathcal{S}_{\text{exc}}$ depending only on $E_1/k(T), \dots, E_s/k(T)$), the completion at $\mathfrak{p}$ of every specialization of any of the extensions $E_1/k(T), \dots, E_s/k(T)$ has cyclic Galois group; such a number field exists by Remark 6.4. Let H be a non-cyclic abelian subgroup of G. Without loss of generality, we may assume $H = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ for some prime number q. Let ζ_q be a primitive q-th root of unity, and let $\mathfrak{p}$ be a non-zero prime ideal of R, not in $\mathcal{S}_{\text{exc}}$, that is totally split in $F(\zeta_q)/k$. As $\mathfrak{p}$ is totally split in $k(\zeta_q)/k$, there exists a finite Galois extension $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$ with Galois group H [11]. In particular, $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$ cannot occur as the completion at $\mathfrak{p}$ of a specialization of any of the extensions $E_1/k(T), \dots, E_s/k(T)$, completing the proof. □

Remark 6.5. Our method cannot provide more examples of finite groups such that the answer to Question 6.1 is negative. Indeed, it requires the following assumption on G:

(∗) *G has a non-cyclic subgroup H such that, for every number field F containing k, there exist infinitely many non-zero prime ideals $\mathfrak{p}$ of R such that $\mathfrak{p}$ is totally split in F/k, and such that H occurs as a Galois group over $k_{\mathfrak{p}}$.*

As shown in the proof of Theorem 6.2, condition (∗) holds if G has a non-cyclic abelian subgroup. However, the converse is true, as it is easy to see that any subgroup H of G as in condition (∗) has to be abelian.

[11] Indeed, one can take $L^{(\mathfrak{p})}$ to be the compositum of the fields $L_1^{(\mathfrak{p})}$ and $L_2^{(\mathfrak{p})}$, where $L_1^{(\mathfrak{p})}/k_{\mathfrak{p}}$ is the unique degree q unramified extension of $k_{\mathfrak{p}}$, and $L_2^{(\mathfrak{p})}/k_{\mathfrak{p}}$ is a finite Galois extension with Galois group $\mathbb{Z}/q\mathbb{Z}$ that is totally ramified (such an extension exists; see, e.g., [Ser79, Chapter IV]).

As an immediate consequence of Theorem 6.2, the answer to Question 6.1 is always negative for finite non-cyclic abelian groups, dihedral groups D_n (of order $2n$) with n even, symmetric groups S_n with $n \geq 4$, alternating groups A_n with $n \geq 4$. In Corollary 6.6 below, we show that the same is true for arbitrary finite non-abelian simple groups:

Corollary 6.6. *Assume that G is a finite non-abelian simple group. Then the answer to Question 6.1 is negative for all finite sets of k-regular G-extensions of $k(T)$.*

Proof. By Theorem 6.2, it suffices to show that G has a non-cyclic abelian subgroup. Suppose by contradiction that G does not. Then, by, e.g., [CE56, Chapter XI, Theorem 11.6], every Sylow subgroup of G is either cyclic or a generalized quaternion group. If every 2-Sylow subgroup of G was cyclic, then every Sylow subgroup of G would then be cyclic. As Hölder proved in 1895 (see, e.g., [Rot95, Theorem 7.53] for more details), G would be solvable[12], which cannot happen. One may then apply [Suz55, Theorem C] to get that G has a normal subgroup H which satisfies the following two conditions:

(1) $(G : H) \leq 2$,
(2) $H = H' \times \mathrm{SL}_2(\mathbb{F}_p)$ for some prime number p and some subgroup H' of H whose Sylow subgroups are cyclic.

If $(G : H) = 2$, then H is trivial as G is simple. Hence G has order 2, which cannot happen. Then, by (1), we get $G = H' \times \mathrm{SL}_2(\mathbb{F}_p)$, with H' and p as in (2). As G is simple and $\mathrm{SL}_2(\mathbb{F}_p) \neq \{1\}$, we get $H' = \{1\}$, i.e., $G = \mathrm{SL}_2(\mathbb{F}_p)$. Hence $\mathrm{SL}_2(\mathbb{F}_p)$ is simple, which cannot happen as $\mathrm{SL}_2(\mathbb{F}_2) \cong S_3$, and, for $p \geq 3$, the center of $\mathrm{SL}_2(\mathbb{F}_p)$ has order 2. □

Solvability of Grunwald problems via specialization will be further investigated in upcoming work by the first author, in a context of infinite families of regular extensions.

7. Application to finite parametric sets

This section is devoted to our application to the non-existence of finite parametric sets over number fields, as already mentioned in §1.3.3. In §7.1, we state and prove Theorem 7.2, which is our new general criterion to provide examples of finite groups with no finite parametric set over number fields. Explicit examples, including those given in Theorem 1.6 from the introduction (§1.3.3), are then given in §7.2.

For this section, let k be a number field, R its ring of integers, T an indeterminate over k, and G a finite group.

Let us recall the following definition [KL16]:

Definition 7.1. We say that a set S of k-regular G-extensions of $k(T)$ is *parametric* if every G-extension of k occurs as a specialization of some extension $E/k(T)$ in S.

[12]More precisely, any given finite group whose every Sylow subgroup is cyclic is metacyclic; see, e.g., [Rob96, page 290].

It is shown in [KL16] that certain finite groups do not possess finite parametric sets over the given number field k. However, the "global" strategy developed in that paper requires such finite groups to have a non-trivial proper normal subgroup which satisfies some further properties. In particular, this cannot be used for finite simple groups.

7.1. **A new general criterion for non-parametricity.** Here, we rather use a "local" approach. Namely, in Theorem 7.2 below, we provide a sufficient condition, based on the proof of Theorem 6.2, for the finite group G to have no finite parametric set over k.

Given a prime number q, let ζ_q denote a primitive q-th root of unity.

Theorem 7.2. *Suppose that the following condition holds:*

$(**)$ *there exists a prime number q and a number field F containing $k(\zeta_q)$ such that, for all but finitely non-zero prime ideals $\mathfrak{p}$ of R which are totally split in F/k, there exists a G-extension of k whose completion at $\mathfrak{p}$ has Galois group $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*

Then, given a finite set S of k-regular G-extensions of $k(T)$, there exist infinitely many G-extensions of k each of which is a specialization of no extension $E/k(T)$ in S. In particular, G has no finite parametric set over k.

Proof. Given a positive integer s, let $E_1/k(T), \dots, E_s/k(T)$ be k-regular G-extensions. Pick a prime number q and a number field F as in condition $(**)$. In particular, $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ occurs as a subgroup of G. As in the proof of Theorem 6.2, one shows that there exist infinitely many prime ideals $\mathfrak{p}$ of R which are totally split in F/k, and such that the Galois group of the completion at $\mathfrak{p}$ of any specialization of $E_i/k(T)$ is cyclic ($i = 1, \dots, s$). In particular, for such a $\mathfrak{p}$, a G-extension of k as in condition $(**)$ is a specialization of $E_i/k(T)$ for no $i \in \{1, \dots, s\}$, completing the proof. □

7.2. **Explicit examples.** Corollary 7.3 below contains our main examples of finite groups with no finite parametric set over number fields:

Corollary 7.3. *Assume that either one of the following two conditions holds:*

1. *G has a non-cyclic abelian subgroup, and there exists a finite set $\mathcal{S}_{\mathrm{exc}}$ of non-zero prime ideals of R such that every Grunwald problem $(G, (L^{(\mathfrak{p})}/k_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{S}})$, with $\mathcal{S}$ disjoint from $\mathcal{S}_{\mathrm{exc}}$, has a solution.*
2. *$G = A_n$ ($n \geq 4$).*

Then G has no finite parametric set over k.

Proof. In either case, it suffices to show that condition $(**)$ of Theorem 7.2 holds. This is clear in case (1). Now, assume that we are in case (2). Then $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ occurs as a subgroup of G. It then suffices to show that, for all prime ideals $\mathfrak{p}$ of R, there exists a G-extension of k whose completion at $\mathfrak{p}$ has Galois group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Let $\mathfrak{p}$ be a prime ideal of R, and let $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$ be a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extension. Pick a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extension L/k whose completion at $\mathfrak{p}$ is $L^{(\mathfrak{p})}/k_{\mathfrak{p}}$. By a classical result of Mestre (see [Mes90] and

[KM01, Theorem 3]), L/k occurs as a specialization of some k-regular A_n-extension $E/k(T)$. More precisely, there is a polynomial $P(T,Y) \in k[T][Y]$ which is monic and separable in Y, with splitting field E over $k(T)$, and such that $P(0,Y)$ is separable with splitting field L over k. By Lemma 2.2, we may assume that this specialization of $E/k(T)$ has Galois group A_n (without changing the completion at $\mathfrak{p}$), as needed. □

Remark 7.4. (1) Aside from alternating groups, we are not aware of any other infinite family of non-abelian simple groups which have been shown to satisfy condition (∗∗) of Theorem 7.2. However, by using the same tools, the following variant is derived: *Let G be a finite non-abelian simple group, and let p be a prime number such that $H := \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ occurs as a subgroup of G* [13]*. Then, given a finite set S of k-regular G-extensions of $k(T)$, there exist infinitely many H-extensions of k each of which is a specialization of $E/k(T)$ for no $E/k(T) \in S$.*

(2) Under the expectation of [Har07, §1] mentioned in §1.1, condition (1) of Corollary 7.3 holds (and then the conclusion that G has no finite parametric set over k holds as well), provided G is solvable and has a non-cyclic abelian subgroup.

References

[ABGV11] Asher Auel, Eric Brussel, Skip Garibaldi, and Uzi Vishne. Open problems on central simple algebras. *Transform. Groups*, 16(1):219–264, 2011.

[AS01] Elizabeth Allman and Murray Schacher. Division algebras with $\mathrm{PSL}(2,q)$-Galois maximal subfields. *J. Algebra*, 240(2):808–821, 2001.

[BBC12] Jason Bell, Nils Bruin, and Michael Coons. Transcendence of generating functions whose coefficients are multiplicative. *Trans. Amer. Math. Soc.*, 364(2):933–959, 2012.

[Bec91] Sybilla Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419:27–53, 1991.

[C+85] J .H. Conway et al. *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray.* Oxford University Press, Eynsham, 1985.

[CE56] Henri Cartan and Samuel Eilenberg. *Homological algebra*. Princeton University Press. Princeton, N.J., 1956. xv+390 pp.

[Con00] Brian Conrad. Inertia groups and fibers. *J. Reine. Angew. Math.*, 522:1–26, 2000.

[Dèb01] Pierre Dèbes. Théorie de Galois et géométrie: une introduction. In *Arithmétique des revêtements algébriques (Saint-Étienne, 2000)*, volume 5 of *Sémin. Congr.*, pages 1–26. Soc. Math. France, Paris, 2001.

[Dem10] Cyril Demarche. Groupe de Brauer non ramifié d'espaces homogènes à stabilisateurs finis. (French). *Math. Ann.*, 346(4):949–968, 2010.

[DG11] Pierre Dèbes and Nour Ghazi. Specializations of Galois covers of the line. In *"Alexandru Myller" Mathematical Seminar*, volume 1329 of *AIP Conf. Proc.*, pages 98–108. Amer. Inst. Phys., Melville, NY, 2011.

[DG12] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *Ann. Inst. Fourier (Grenoble)*, 62(3):989–1013, 2012.

[13] Such a prime number p exists by the proof of Corollary 6.6.

[DLAN15] Cyril Demarche, Giancarlo Lucchini Arteche, and Danny Neftin. The Grunwald problem and approximation properties for homogeneous spaces. 2015. To appear in Annales de l'Institut Fourier. arXiv:1512.06308.

[Eis95] David Eisenbud. *Commutative algebra. With a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[FS91] Burton Fein and Murray Schacher. $\mathbb{Q}$-admissibility questions for alternating groups. *J. Algebra*, 142(2):360–382, 1991.

[GS79] Basil Gordon and Murray Schacher. The admissibility of A_5. *J. Number Theory*, 11(4):498–504, 1979.

[Har07] David Harari. Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini. (French). *Bull. Soc. Math. France*, 135(4):549–564, 2007.

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials. Constructive Aspects of the Inverse Galois Problem*. Cambridge University Press, 2002.

[KL16] Joachim König and François Legrand. Non-parametric sets of regular realizations over number fields. *Manuscript*, 2016. arXiv 1612.06577.

[KM01] Jürgen Klüners and Gunter Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196, 2001.

[KN17] Joachim König and Danny Neftin. The admissibility of M_{11} over number fields. 2017. To appear in J. Pure Appl. Algebra.

[Kön17] Joachim König. Non-parametricity of rational translates of regular Galois extensions. *Acta. Arith.*, 179(3):267–275, 2017.

[LA14] Giancarlo Lucchini Arteche. Approximation faible et principe de Hasse pour des espaces homogènes à stabilisateur fini résoluble. (French). *Math. Ann.*, 360(3-4):1021–1039, 2014.

[Leg16a] François Legrand. On parametric extensions over number fields. 2016. To appear in Annali della Scuola Normale Superiore di Pisa - Classe di Scienze. arXiv 1602.06706.

[Leg16b] François Legrand. Specialization results and ramification conditions. *Israel J. Math.*, 214(2):621–650, 2016.

[Mes90] Jean-François Mestre. Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$. *J. Algebra*, 131(2):483–495, 1990.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin, second edition, 2008.

[PV05] Bernat Plans and Núria Vila. Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization. *J. Théor. Nombres Bordeaux*, 17(1):271–282, 2005.

[Rob96] Derek J. S. Robinson. *A Course in the Theory of Groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996. xviii+499 pp.

[Rot95] Joseph J. Rotman. *An Introduction to the Theory of Groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995. xvi+513 pp.

[Sal82] David J. Saltman. Generic Galois extensions and problems in field theory. *Adv. in Math.*, 43(3):250–283, 1982.

[Sch68] Murray M. Schacher. Subfields of division rings. I. *J. Algebra*, 9:451–477, 1968.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. viii+241 pp.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992.

[Suz55] Michio Suzuki. On finite groups with cyclic Sylow subgroups for all odd primes. *Amer. J. Math.*, 77:657–691, 1955.

[Wan48] Shianghaw Wang. A counter-example to Grunwald's theorem. *Ann. of Math. (2)*, 49:1008–1009, 1948.

[Wan50] Shianghaw Wang. On Grunwald's theorem. *Ann. of Math. (2)*, 51:471–484, 1950.

[Zas35] Hans Zassenhaus. Über endliche Fastkörper. (German). *Abh. Math. Sem. Univ. Hamburg*, 11(1):187–220, 1935.

[Zyw14] David Zywina. The inverse Galois problem for orthogonal groups. *Manuscript*, 2014. arXiv 1409.1151.

E-mail address: koenig.joach@technion.ac.il

Department of Mathematics, Technion - Israel Institute of Technology, Haifa 32000, Israel

E-mail address: legrandfranc@technion.ac.il

Department of Mathematics, Technion - Israel Institute of Technology, Haifa 32000, Israel

E-mail address: dneftin@technion.ac.il

Department of Mathematics, Technion - Israel Institute of Technology, Haifa 32000, Israel