HILBERT SPECIALIZATION RESULTS WITH LOCAL CONDITIONS

FRANÇOIS LEGRAND

ABSTRACT. Given a field $k$ and an indeterminate $T$, the main topic of the paper is the construction of specializations of any given finite separable extension of $k(T)$ with the Hilbert Specialization Property and with specified local behavior at any finitely many given primes of $k$. First we give a full non Galois analog of a result with a ramified type conclusion from a preceding paper and next we prove an unifying statement which conjoins our results and several previous works devoted to the unramified part of the problem.

1. Introduction

Given a field $k$, an indeterminate $T$, a finite separable extension $E/k(T)$ of degree $n$ and a point $t_0 \in \mathbb{P}^1(k)$, not a branch point, the specialization of $E/k(T)$ at $t_0$ is a $k$-étale algebra of degree $n$, i.e. a product $\prod_i F_i/k$ of finite separable extensions of $k$ such that $\sum_i [F_i:k] = n$ (see §2.1 for basic terminology). For example, if $E/k(T)$ is given by a monic (with respect to $Y$) irreducible separable polynomial $P(T,Y) \in k[T][Y]$, it is the product of extensions of $k$ corresponding to the irreducible factors of $P(t_0,Y)$ (for all but finitely many $t_0 \in k$).

The main topic of the paper is the construction of specializations satisfying the Hilbert Specialization Property, i.e. which consist of a single degree $n$ field extension of $k$, and with specified local behavior (ramified or unramified) at any finitely many given primes of $k$. By “with specified local behavior”, we mean, in the case the extension $E/k(T)$ is Galois, with specified inertia groups or Frobenius and, in the general case, with specified ramification indices or residue degrees.

The unramified part of this problem has been studied in [DL12] for arbitrary finite separable extensions of $k(T)$ (see also [DG11] [DG12] [DL13]) whereas the ramified case has been studied in [Leg13b] for extensions $E/k(T)$ that are regular (i.e. $E \cap \overline{k} = k$) and Galois. The aim of this paper consists first in handling the ramified case for arbitrary finite separable extensions and next in providing unifying statements.

Date: February 3, 2015.
1.1. The ramified part of the problem should be studied within some classical limitations we recall briefly below. We refer to §2.2 for precise statements (the “Specialization Inertia Theorem” and proposition 2.6), more details and references.

Let $k$ be the quotient field of a Dedekind domain $A$ (of characteristic zero), $E/k(T)$ a finite separable extension, $\hat{E}/k(T)$ its Galois closure and $\{t_1, \ldots, t_r\}$ its branch point set. Recall that:

- a necessary condition for a given prime $P$ of $A$ (up to finitely many depending on $E/k(T)$) to ramify in at least one specialization of $E/k(T)$ requires $P$ to be a prime divisor of the irreducible polynomial $m_{i_P}(T)$ over $k$ of some branch point $t_{i_P}$, i.e. $m_{i_P}(t_0, P)$ has positive $P$-adic valuation for at least one point $t_0, P \in k$,

- the inertia group at $P$ of the specialization at $t_0$ of the extension $E/k(T)$ is the set of all lengths of disjoint cycles involved in the cycle decomposition in $S_d$ of the image of $g_{i_P}^{a_P}$ via the action $\nu$ of the Galois group $\text{Gal}(\hat{E}/k(T))$ on all $k(T)$-embeddings of $E\hat{k}$ in a given algebraic closure of $\hat{k}(T)$ (with $d = [E\hat{k} : \hat{k}(T)]$).

In [Leg13b], we have provided some converse to the Galois conclusion. Fix a finite set $\mathcal{S}$ of primes $\mathcal{P}$ of $A$ (up to finitely many), each given with a couple $(i_P, a_P)$ where $i_P$ is an index in $\{1, \ldots, r\}$ such that $P$ is a prime divisor of $m_{i_P}(T)$ and $a_P$ is a positive integer. Then:

- [Leg13b, corollary 3.3] has shown that, if the Galois closure $\hat{E}/k(T)$ is regular and $k$ is hilbertian\(^1\), then, for infinitely many distinct points $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \ldots, t_r\}$, the specialization of $\hat{E}/k(T)$ at $t_0$ has Galois group $\text{Gal}(\hat{E}/k(T))$ and inertia group at $\mathcal{P}$ generated by $g_{i_P}^{a_P}$ ($P \in \mathcal{S}$),

\(^1\)e.g. $k$ is a number field or a finite extension of a rational function field $\kappa(X)$ with $\kappa$ an arbitrary field and $X$ an indeterminate.
Actually theorem 3.2 also extends [Leg13b, corollary 3.3] to the case the Galois closure $\hat{E}/k(T)$ is not necessarily regular\(^2\) (the same conclusion holds word for word) and holds if the base field $k$ has positive tame characteristic. Furthermore, under some g-complete hypothesis and as in [Leg13b], the hilbertianity assumption can be relaxed (theorem 3.3).

1.2. **The mixed situation.** In §4, we prove an unifying statement which conjoins our results from §3 and those from the already alluded to previous works devoted to the unramified part of our problem when the base field $k$ is a number field\(^3\). Theorem 4.1 gives our precise result.

Moreover, in the special case $k = \mathbb{Q}$, explicit bounds on the discriminant of our specializations can be added to our conclusions (§4.3.1). For instance, we obtain the following result (§4.3.2).

**Theorem 2.** Let $E/\mathbb{Q}(T)$ be a regular finite extension of degree $n$ with at least one $\mathbb{Q}$-rational branch point and such that the Galois closure $\hat{E}/\mathbb{Q}(T)$ is regular. Let $G$ be the Galois group of $\hat{E}/\mathbb{Q}(T)$. Then there exist three positive constants $m_0$, $\alpha$ and $\beta$ (depending only on $E/\mathbb{Q}(T)$) satisfying the following. Given two disjoint finite sets $S_{\text{ra}}$ and $S_{\text{ur}}$ of primes $p > m_0$, there exist some rational numbers $t_0$ such that

1. the specialization of $E/\mathbb{Q}(T)$ at $t_0$ consists of a single degree $n$ field extension $E_{t_0}/\mathbb{Q}$ and the Galois closure $\hat{E}_{t_0}/\mathbb{Q}$ has Galois group $G$,
2. each prime $p \in S_{\text{ra}}$ ramifies in $E_{t_0}/\mathbb{Q}$,
3. no prime $p \in S_{\text{ur}}$ ramifies in $E_{t_0}/\mathbb{Q}$,
4. the discriminant $d_{E_{t_0}}$ of $E_{t_0}/\mathbb{Q}$ satisfies
   \[
   \prod_{p \in S_{\text{ra}}} p \leq |d_{E_{t_0}}| \leq \alpha \cdot (\prod_{p \in S_{\text{ra}}} p \cdot \prod_{p \in S_{\text{ur}}} p)^\beta
   \]

In addition to many regular Galois extensions of $\mathbb{Q}(T)$ with various Galois groups (e.g. abelian groups of even order, symmetric groups, alternating groups, some other non abelian simple groups (including the Monster group), etc.), several non Galois finite extensions of $\mathbb{Q}(T)$ satisfy the assumptions of theorem 2. For instance, given a positive integer $n \geq 3$, this is true of the finite extension of $\mathbb{Q}(T)$ generated by one root of the irreducible trinomial $Y^n - Y - T$ (in which case $G = S_n$) [Ser92, §4.4]. See also [Sch00, §2.4] (or §3.2) for another examples with $G = S_n$ ($n \geq 3$) and [Ser92, §4.5] for examples with $G = A_n$ ($n \geq 5$).

\(^2\)Recall that this extension is not regular in general, even if $E/k(T)$ is regular.

\(^3\)The situation of a base field which is a rational function field $\kappa(X)$ with coefficients in a field $\kappa$ with suitable arithmetic properties (and $X$ an indeterminate) can also be considered. We refer to [DG11, §4] for more on this case.
Acknowledgments. This research was partially supported by the Israel Science Foundation (grant No. 40/14) and the Open University of Israel. The author also wishes to thank Pierre Dèbes for his valuable comments on a preliminary version of the paper.

2. Basics

2.1. Basics on finite separable extensions of $k(T)$. Given a field $k$, fix an algebraic closure $\overline{k}$ of $k$. Denote the separable closure of $k$ inside $\overline{k}$ by $k_{sep}$ and the absolute Galois group by $G_k$. For more on this subsection, we refer for example to [Dèb09, chapters 2 and 3].

2.1.1. Generalities. A given finite separable extension $E/k(T)$ is said to be regular if $E \cap k = k$. In general, there is some constant extension in $E/k(T)$, which we denote by $k_E/k$ and define by $k_E = E \cap \overline{k}$ (the special case $k_E = k$ corresponds to the situation $E/k(T)$ is regular).

Denote the Galois closure of $E/k(T)$ by $\hat{E}/k(T)$. The Galois group $\text{Gal}(\hat{E}/k(T))$ is denoted by $G$ and called the Galois group of $E/k(T)$. Next denote by $\hat{E}k$ the compositum of $\hat{E}$ and $k$ (in a fixed algebraic closure of $k(T)$). The Galois group $\text{Gal}(\hat{E}k/k(T))$ is denoted by $G$ and called the geometric Galois group of $E/k(T)$; it is a normal subgroup of $G$ (these two groups coincide if and only if $\hat{E}/k(T)$ is regular).

Via its action on all $\overline{k}(T)$-embeddings of $\hat{E}k$ in a given algebraic closure of $\overline{k}(T)$, the geometric Galois group $G$ may be viewed as a subgroup of the permutation group of all these embeddings. Up to some numerotation of them, it may be viewed as a subgroup of $S_d$ (with $d = [E\overline{k} : \overline{k}(T)]$); denote the corresponding morphism by $\nu : G \to S_d$ and call it the embedding morphism of $G$ in $S_d$.

2.1.2. Branch points. Denote the integral closure of $\overline{k}[T]$ (resp. of $\overline{k}[1/T]$) in $\hat{E}k$ by $\mathcal{B}$ (resp. by $\mathcal{B}^\sim$). A point $t_0 \in \overline{k}$ (resp. $\infty$) is said to be a branch point of $E/k(T)$ if the prime $(T - t_0)\mathcal{B}[T]$ (resp. $(1/T)\mathcal{B}[1/T]$) ramifies in $\mathcal{B}$ (resp. in $\mathcal{B}^\sim$). Classically $E/k(T)$ has only finitely many branch points, denoted by $t_1, \ldots, t_r$, and they lie in $\mathbb{P}^1(\overline{k})$.

Remark 2.1. We will always assume that the following conditions hold:

1. $t_1, \ldots, t_r \in \mathbb{P}^1(k_{sep})$,
2. for each point $t_0 \in \mathbb{P}^1(k_{sep}) \setminus \{t_1, \ldots, t_r\}$, the residue field of any prime lying over $t_0$ in $\hat{E}k_{sep}/k_{sep}(T)$ is equal to $k_{sep}$.

Both conditions hold if $k$ is perfect (in particular if $k$ has characteristic zero as in [Leg13b]). In the general case, condition (2) holds for all but finitely many points $t_0 \in \mathbb{P}^1(k_{sep}) \setminus \{t_1, \ldots, t_r\}$ [Leg13a, lemma B.1.2].
2.1.3. Inertia canonical invariants. Here we assume that the characteristic $p$ of $k$ does not divide the order of $G$. For each integer $n$ which is prime to $p$, fix a primitive $n$-th root of unity $\zeta_n$ and assume that the system $\{\zeta_n\}_n$ is coherent, i.e. $\zeta_n^m = \zeta_m$ for any integers $n$ and $m$ (that are prime to $p$).

To each $t_i$ can be associated a conjugacy class $C_i$ of $G$, called the inertia canonical conjugacy class (associated with $t_i$), in the following way. The inertia groups of $\hat{E}k/k(T)$ at $t_i$ are cyclic conjugate groups of order equal to the ramification index $e_i$. Furthermore each of them has a distinguished generator corresponding to the automorphism $(T - t_i)^{1/e_i} \mapsto \zeta_{e_i}(T - t_i)^{1/e_i}$ of $k((T - t_i)^{1/e_i})$ (replace $T - t_i$ by $1/T$ if $t_i = \infty$). Then $C_i$ is the conjugacy class of all the distinguished generators of the inertia groups at $t_i$. The unordered $r$-tuple $(C_1, \ldots, C_r)$ is called the inertia canonical invariant of $\hat{E}/k(T)$.

Denote by $C^S_d$ the conjugacy class of $S_d$ corresponding to $C_i$ via the embedding morphism $\nu : G \to S_d \ (i \in \{1, \ldots, r\})$. The unordered $r$-tuple $(C_1^S, \ldots, C_r^S)$ is called the inertia canonical invariant of $E/k(T)$.

2.1.4. Specializations. Let $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \ldots, t_r\}$.

(a) Galois case. The residue field of some prime lying over $t_0$ in the extension $\hat{E}/k(T)$ is denoted by $\hat{E}_{t_0}$ and we call the extension $\hat{E}_{t_0}/k$ the specialization of $\hat{E}/k(T)$ at $t_0$ (this does not depend on the choice of the prime above $t_0$ since the extension $\hat{E}/k(T)$ is Galois). It is a Galois extension of $k^4$ of Galois group a subgroup of $G$, namely the decomposition group of the extension $\hat{E}/k(T)$ at $t_0$.

(b) General case. Denote the primes lying over $t_0$ in the extension $E/k(T)$ by $P_1, \ldots, P_s$. For each index $l \in \{1, \ldots, s\}$, the residue field at $P_l$ is denoted by $E_{t_0,l}$ and the extension $E_{t_0,l}/k$ is called a specialization of $E/k(T)$ at $t_0$. The $k$-étale algebra $\prod_{l=1}^s E_{t_0,l}/k$ of all residue extensions at $t_0$ is called the specialization algebra of $E/k(T)$ at $t_0$. The compositum in $\bar{k}$ of the Galois closures of all specializations of $E/k(T)$ at $t_0$ is the specialization of the Galois closure $\hat{E}/k(T)$ at $t_0$.

If $E/k(T)$ is given by a polynomial $P(T,Y) \in k[T][Y]$, the following lemma, which is [Leg13a, lemma B.1.3], is useful:

**Lemma 2.2.** Let $P(T,Y) \in k[T][Y]$ be a monic (with respect to $Y$) separable polynomial which is irreducible over $k(T)$ such that $E$ is the field generated over $k(T)$ by one of its roots. Then, for any $t_0 \in k$ such that $P(t_0,Y)$ is separable over $k$, one has these conclusions.

---

4The extension $\hat{E}_{t_0}/k$ is separable thanks to our assumption (2) in remark 2.1.
The point $t_0$ is not a branch point of $E/k(T)$.

Consider the factorization $P(t_0, Y) = P_1(Y) \ldots P_s(Y)$ of $P(t_0, Y)$ in irreducible polynomials $P_i(Y) \in k[Y]$ and denote the field generated over $k$ by one of the roots of $P_i(Y)$ by $F_i$ ($l \in \{1, \ldots, s\}$). Then the specialization algebra of $E/k(T)$ at $t_0$ is the $k$-étale algebra $\prod_{i=1}^s F_i/k$.

2.2. Basics on ramification in specializations. Now we recall some classical facts on ramification in specializations of finite separable extensions of $k(T)$ (Galois or not). The aim of this subsection is the Specialization Inertia Theorem which is a slightly more precise version of two results of Beckmann [Bec91, proposition 4.2 and theorem 5.1] and handles both Galois and non Galois situations. For more details on this subsection, we refer to [Bec91] and [Leg13b, §2.2-3].

Let $A$ be a Dedekind domain, $k$ its quotient field and $\mathcal{P}$ a prime of $A$. Denote the valuation of $k$ corresponding to $\mathcal{P}$ by $v_\mathcal{P}$.

**Definition 2.3.** Given two points $t_0$ and $t_1 \in \mathbb{P}^1(k^\text{sep})$, we say that $t_0$ and $t_1$ meet modulo $\mathcal{P}$ if there exist some finite separable extension $F/k$ and some prime $\mathcal{P}_F$ of $F$ lying over $\mathcal{P}$ such that $t_0, t_1 \in \mathbb{P}^1(F)$ and either one of the following two conditions holds:

1. $v_{\mathcal{P}_F}(t_0) \geq 0$, $v_{\mathcal{P}_F}(t_1) \geq 0$ and $v_{\mathcal{P}_F}(t_0 - t_1) > 0$,
2. $v_{\mathcal{P}_F}(t_0) \leq 0$, $v_{\mathcal{P}_F}(t_1) \leq 0$ and $v_{\mathcal{P}_F}((1/t_0) - (1/t_1)) > 0$.

In this paper, the irreducible polynomial over $k$ of any point $t_1 \in \mathbb{P}^1(k^\text{sep})$ will be denoted by $m_{t_1}(T)$ (set $m_{t_1}(T) = 1$ if $t_1 = \infty$).

Fix $t_1 \in \mathbb{P}^1(k^\text{sep})$. Assume that the constant coefficient $a_{t_1}$ of $m_{t_1}(T)$ satisfies $v_\mathcal{P}(a_{t_1}) = 0$ in the case $t_1 \neq 0$ to make the intersection multiplicity well-defined in definition 2.4 below. Let $t_0 \in \mathbb{P}^1(k)$.

**Definition 2.4.** The intersection multiplicity $I_\mathcal{P}(t_0, t_1)$ of $t_0$ and $t_1$ at $\mathcal{P}$ is $I_\mathcal{P}(t_0, t_1) = \begin{cases} v_\mathcal{P}(m_{t_1}(t_0)) & \text{if } v_\mathcal{P}(t_0) \geq 0, \\ v_\mathcal{P}(m_{1/t_1}(1/t_0)) & \text{if } v_\mathcal{P}(t_0) \leq 0. \end{cases}$

Given a finite separable extension $E/k(T)$, denote the Galois closure by $\widehat{E}/k(T)$, the branch point set by $\{t_1, \ldots, t_r\}$, which, according to our assumption (1) in remark 2.1, is contained in $\mathbb{P}^1(k^\text{sep})$, the constant extension in $\widehat{E}/k(T)$ by $k_{\widehat{E}}/k$ and the geometric Galois group $\text{Gal}(\widehat{E}/k(T))$ by $\overline{G}$.

**Definition 2.5.** We say that $\mathcal{P}$ is a bad prime for $E/k(T)$ if $\mathcal{P}$ is one of the finitely many primes satisfying at least one of these conditions:

---

5Identify $\mathbb{P}^1(k)$ and $k \cup \{\infty\}$ and set $1/\infty = 0$, $1/0 = \infty$, $v_\mathcal{P}(\infty) = -\infty$, $v_\mathcal{P}(0) = \infty$. 

(1) $|\mathcal{G}| \in \mathcal{P}$,
(2) two different branch points meet modulo $\mathcal{P}$,
(3) $\hat{E}/k(T)$ has vertical ramification at $\mathcal{P}$, i.e. the prime $\mathcal{P}A[T]$ of $A[T]$ ramifies in the integral closure of $A[T]$ in $\hat{E}$,
(4) $\mathcal{P}$ ramifies in the separable extension $k_{\hat{E}}(t_1, \ldots, t_r)/k$.
Otherwise $\mathcal{P}$ is called a good prime for $E/k(T)$.

From now on, assume that the characteristic of $k$ does not divide the order of $\mathcal{G}$. Denote the inertia canonical invariant of $\hat{E}/k(T)$ by $(C_1, \ldots, C_r)$ and, with $d = [E\overline{k} : k(T)]$, the inertia canonical invariant of $E/k(T)$ by $(C_1^{S_d}, \ldots, C_r^{S_d})$.

Given a $k$-étale algebra $\prod_i F_i/k$, say that a positive integer $e$ is a ramification index of $\prod_i F_i/k$ at $\mathcal{P}$ if there exists some index $l$ such that $e$ is the ramification index of some prime of $F_l$ above $\mathcal{P}$.

**Specialization Inertia Theorem.** Let $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \ldots, t_r\}$.

1. If $\mathcal{P}$ ramifies in at least one specialization of $E/k(T)$ at $t_0$, then $\hat{E}/k(T)$ has vertical ramification at $\mathcal{P}$ or $\mathcal{P}$ ramifies in the constant extension $k_{\hat{E}}/k$ or $t_0$ meets some branch point modulo $\mathcal{P}$.
2. Fix $j \in \{1, \ldots, r\}$ such that $t_0$ and $t_j$ meet modulo $\mathcal{P}$. Assume $\mathcal{P}$ is a good prime for $E/k(T)$ and $\mathcal{P}$ “unitizes” $t_j$, i.e. $t_j$ and $1/t_j$ are integral over the localization $A_\mathcal{P}$ of $A$ at $\mathcal{P}$. Then the following holds.

   a. The inertia group at $\mathcal{P}$ of the specialization $\hat{E}_{t_0}/k$ of $\hat{E}/k(T)$ at $t_0$ is generated by some element of $C_{j^{l_{P(t_0,t_j)}}}(= \{h_{j^{l_{P(t_0,t_j)}}}/h_j \in C_j\})$.
   b. Assume that $\text{Gal}(\hat{E}_{k_{\hat{E}}(t_0)/k_{\hat{E}}}) = \mathcal{G}$. Then the set of all ramification indices at $\mathcal{P}$ of the specialization algebra $\prod_i E_{t_0,i}/k$ of $E/k(T)$ at $t_0$ is the same as the set of all lengths of disjoint cycles involved in the cycle decomposition in $S_d$ of any element of $(C_j^{S_d})^{l_{P(t_0,t_j)}}$.

As said in [Leg13b, §2.2.3], the Galois part (a) is a version of [Bec91, proposition 4.2] with less restrictive hypotheses (see also [Flo02, chapter 1]) and [Leg13a, §1.2.1.4] offers a proof in the case the Galois closure $\hat{E}/k(T)$ is regular and $k$ has characteristic zero. Details to extend it to the present more general situation are left to the reader. As to the general part (b), it is a slightly more general version of [Bec91, theorem 5.1] and, as explained in [Bec91, §5], it follows from the Galois part.

However the condition $\text{Gal}(\hat{E}_{k_{\hat{E}}(t_0)/k_{\hat{E}}}) = \mathcal{G}$ in part (b) above does not appear in [Bec91], but seems to be missing for the proof of theorem 5.1 of this paper to work. Indeed assume for simplicity that $k_{\hat{E}} = k$ (as explained in [Bec91, §5], the proof may be reduced to this case). It is used in the proof there that, with our notation and as a consequence of
the Galois part of the result, the set of all inertia groups of primes above \( \mathcal{P} \) in the specialization \( \hat{E}_{t_0}/k \) of \( \hat{E}/k(T) \) at \( t_0 \) is exactly the set of all conjugates in \( G = \text{Gal}(E/k(T)) \) of \( \langle g_j^{f_r(t_0,t_j)} \rangle \) (with \( g_j \) the distinguished generator of the inertia groups at \( t_j \)). To our knowledge, this claim is true for all conjugates in \( \text{Gal}(\hat{E}_{t_0}/k) \), but it seems unclear if it holds for all conjugates in \( G \), thus leading to our extra assumption.

Finally we recall a preliminary criterion at one prime given in [Leg13b]. Recall that the prime \( \mathcal{P} \) is said to be a prime divisor of a non constant polynomial \( P(T) \in k[T] \) if \( v_\mathcal{P}(P(t_0)) > 0 \) for at least one point \( t_0 \in k \).

In proposition 2.6 below, which generalizes [Leg13b, corollary 2.12], set \( m_\mathcal{P}(T) = \prod_{i=1}^r m_{t_i}(T) \) and \( m_{1/\mathcal{P}}(T) = \prod_{i=1}^r m_{1/t_i}(T) \).

**Proposition 2.6.** Assume that \( \mathcal{P} \) is a good prime for \( E/k(T) \) unitizing each branch point. Then the following two conditions are equivalent:

1. \( \mathcal{P} \) ramifies in at least one specialization of \( E/k(T) \),
2. \( \mathcal{P} \) is a prime divisor of \( m_\mathcal{P}(T) \cdot m_{1/\mathcal{P}}(T) \).

3. Specializations with specified ramified local behavior

Let \( A \) be a Dedekind domain, \( k \) its quotient field and \( E/k(T) \) a finite separable extension of degree \( n \). This section is devoted to the construction of specialization points \( t_0 \in \mathbb{P}^1(k) \) at which the specialization algebra of \( E/k(T) \) consists of a single degree \( n \) field extension of \( k \) and has specified ramified local behavior at any finitely many given primes of \( A \), within the limitations of the Specialization Inertia Theorem. Theorems 3.2 and 3.3 give our precise results.

**3.1. Data.** First we fix some notation for this section. Denote the Galois closure of \( E/k(T) \) by \( \hat{E}/k(T) \), the constant extension in \( \hat{E}/k(T) \) by \( k_{\hat{E}}/k \), the Galois group \( \text{Gal}(\hat{E}/k(T)) \) by \( G \), the geometric Galois group \( \text{Gal}(\hat{E}_{\mathbb{F}}(T)/k(T)) \) by \( \overline{G} \), with order assumed to be relatively prime to the characteristic of \( k \), the branch point set by \( \{t_1, \ldots, t_r\} \) and the inertia canonical invariant of \( \hat{E}/k(T) \) (resp. of \( E/k(T) \)) by \( (C_1, \ldots, C_r) \) (resp. by \( (C_1^{S_1}, \ldots, C_r^{S_r}) \)).

Let \( s \geq 1 \) be an integer, \( \mathcal{P}_1, \ldots, \mathcal{P}_s \) \( s \) distinct good primes for \( E/k(T) \) and \( (i_1, a_1), \ldots, (i_s, a_s) \) \( s \) couples where, for each index \( j \in \{1, \ldots, s\} \),

(a) \( i_j \) is an index in \( \{1, \ldots, r\} \) such that \( \mathcal{P}_j \) is a prime divisor of the polynomial \( m_{t_{i_j}}(T) \cdot m_{1/t_{i_j}}(T) \) and unitizes \( t_{i_j} \),

(b) \( a_j \) is a positive integer.

**Remark 3.1.** For some index \( j \), there may be no index \( i \) such that \( \mathcal{P}_j \) is a prime divisor of the polynomial \( m_{t_i}(T) \cdot m_{1/t_i}(T) \). In this case, if \( \mathcal{P}_j \)
unitizes each branch point, then no specialization of $E/k(T)$ ramifies at $P_j$ (proposition 2.6). As explained in [Leg13b, remark 3.2], this fact and our results below may be conjoined to obtain specializations of $E/k(T)$ which are unramified at any finitely many given primes of $A$.

For each index $j \in \{1, \ldots, s\}$, denote the set of all lengths of disjoint cycles involved in the cycle decomposition of any element of $(C_{ij}^a_i)_j$ by $S(i_j, a_j)$ and, given a finite extension $F/k$, consider the following:

(Ram$/P_j$/S(i_j, a_j)) the following two conditions hold:

1. the set of all ramification indices at $P_j$ of $\prod_{l=1}^{s'} F_l/k$ is $S(i_j, a_j)$,
2. the inertia group at $P_j$ of the compositum $\hat{F}_1 \ldots \hat{F}_{s'}/k$ of the Galois closures of $F_1/k, \ldots, F_{s'}/k$ is generated by an element of $C_{ij}^a_i$.

3.2. Main results. These results extend those from [Leg13b, §3.1].

Theorem 3.2. Assume that $k$ is hilbertian. Then, for infinitely many distinct points $t_0 \in k \setminus \{t_1, \ldots, t_r\}$ in some arithmetic progression,

1. the specialization algebra $\prod_l E_{t_0,l}/k$ of $E/k(T)$ at $t_0$ consists of a single degree $n$ field extension $E_{t_0}/k$ and the Galois group $\text{Gal}(\hat{E}_{t_0}/k)$ satisfies $G \subseteq \text{Gal}(\hat{E}_{t_0}/k) \subseteq G$,
2. $E_{t_0}/k$ satisfies condition (Ram$/P_j$/S(i_j, a_j)) for each index $j \in \{1, \ldots, s\}$.

Moreover the extensions $\hat{E}_{t_0}k_E/k_E$ may be required to be linearly disjoint.

Assumption (a) holds in particular if the inertia canonical conjugacy class set $\{C_i / i \in I\}$ is itself g-complete. Several finite separable extensions of $k(T)$ are known to satisfy this last condition. For example,
given positive integers \( n, m, q \) and \( v \) such that \( n \geq 3, 1 \leq m \leq n, (m,n) = 1 \) and \( q(n-m) - vn = 1 \) and if the characteristic of \( k \) does not divide \( mn(n-m) \), this is true of the degree \( n \) regular separable extension of \( k(T) \) generated by one root of the irreducible trinomial \( Y^n - T^nY^m + T^n \) which has branch point set \( \{0, \infty, m^nn^{-n}(n-m)^{n-m}\} \) with corresponding inertia groups generated by the disjoint product of an \( m \)-cycle and an \((n-m)-cyc\)le at \( 0 \), an \( n \)-cycle at \( \infty \) and a transposition at \( m^{n}n^{-n}(n-m)^{n-m} \). See [Sch00, §2.4].

Moreover assumption (b) holds in each of the following situations:
(i) each \( t_i (i \in I) \) is \( k \)-rational and \( A \) has infinitely many distinct primes,
(ii) either \( k \) is a number field (this follows from the Tchebotarev density theorem) or \( k \) is a finite extension of a rational function field \( \kappa(X) \) with \( \kappa \) an arbitrary algebraically closed field and \( X \) an indeterminate (as explained in [Leg13a, §3.1.2.2]).

### 3.3. Proof of theorems 3.2 and 3.3.

The proof rests on that of [Leg13b, corollaries 3.3-4] which are theorems 3.2 and 3.3 here in the case the extension \( E/k(T) \) is regular and Galois. We reproduce this proof below with the necessary adjustments for the bigger generality.

#### 3.3.1. A central lemma

The following lemma, which summarizes the core of the proof given in [Leg13b, §3.4], will be used on several occasions in the rest of this paper.

Denote the set of all indices \( j \in \{1, \ldots, s\} \) such that \( t_i \neq \infty \) by \( S \)
and, for each index \( j \in \{1, \ldots, s\} \), let \( x_{\mathcal{P}_j} \in A \) be a generator of the
maximal ideal \( \mathcal{P}_jA_{\mathcal{P}_j} \) of \( A_{\mathcal{P}_j} \).

**Lemma 3.4.** There is an element \( \theta \in k \) such that, for each element \( u \) of \( k \) lying in \( \bigcap_{i=1}^s A_{\mathcal{P}_i} \) and with \( t_{0,u} = \theta + u \cdot \prod_{i \in S} x_{\mathcal{P}_i}^{a_{i+1}}, \) one has \( I_{\mathcal{P}_j}(t_{0,u}, t_{i}) = a_j \) for each index \( j \in \{1, \ldots, s\} \). Moreover such an element \( \theta \) may be required to lie in \( A \) if \( S = \{1, \ldots, s\} \) (in particular if \( \infty \) is not a branch point).

The following consequence will be used on several occasions in the rest of this paper. Fix a point \( t_{0,u} \) as above and assume it is not a branch point. From [Leg13b, lemma 2.5], the point \( t_{0,u} \) meets the branch point \( t_{i,j} \) modulo \( \mathcal{P}_j \) for each index \( j \in \{1, \ldots, s\} \). Hence, if we show that \( \text{Gal}((\hat{E}_k^{\widehat{\mathcal{P}}})_{t_{0,u}}/k_{\mathcal{P}}) = \overline{\mathcal{P}} \), applying part (2) of the Specialization Inertia Theorem will provide that the specialization algebra of \( E/k(T) \) at \( t_{0,u} \) satisfies condition (Ram/\( \mathcal{P}_j/S(i_j, a_j) \)) for each index \( j \in \{1, \ldots, s\} \).

#### 3.3.2. Proof of theorem 3.2

Assume \( k \) is hilbertian and fix an element \( \theta \) as in lemma 3.4. From [Gey78, lemma 3.4], there exist infinitely many distinct elements \( u \in \bigcap_{i=1}^s A_{\mathcal{P}_i} \) such that the specializations \( \hat{E}_{t_{0,u}}/k \)
of \( \hat{E}/k(T) \) at \( t_{0,u} = \theta + u \cdot \prod_{l \in S} \delta_{\hat{P}^l} \) have Galois group \( G \). Hence the corresponding specialization algebras of \( E/k(T) \) consist of a single degree \( n \) field extension of \( k \). Moreover, for such a point \( t_{0,u} \), one has \( (\hat{E}_{t_{0,u}})^G = k_{\hat{E}}, \) i.e. \( \text{Gal}((\hat{E}_{k_{\hat{E}}})_{t_{0,u}}/k_{\hat{E}}) = \overline{G} \), thus ending the proof.

3.3.3. **Proof of theorem 3.3.** For each \( i \in I \), pick a prime divisor \( \mathcal{P}'_i \) of \( m_{t_i}(T) \cdot m_{1/t_i}(T) \) that is a good prime for \( E/k(T) \) unitizing \( t_i \) (assumption (b)); we may require \( \mathcal{P}'_i \) (for each \( i \in I \)) and \( \mathcal{P}_1, \ldots, \mathcal{P}_s \) to be distinct.

Apply lemma 3.4 to the larger set \( \{ \mathcal{P}_j / j \in \{1, \ldots, s\} \} \cup \{ \mathcal{P}'_i / i \in I \} \) of primes, each \( \mathcal{P}_j \) given with the couple \( (i_j, a_j) \) from \( \S 3.1 \) and each \( \mathcal{P}'_i \) with the couple \( (i, 1) \). With \( S' \) the set of all indices \( i \in I \) such that \( t_i \neq \infty \), there is an element \( \theta \in k \) such that, for any \( u \in k \) satisfying \( v_{\mathcal{P}_j}(u) \geq 0 \) for each \( j \in \{1, \ldots, s\} \) and \( v_{\mathcal{P}'_i}(u) \geq 0 \) for each \( i \in I \) and with \( t_{0,u} = \theta + u \cdot (\prod_{l \in S} \delta_{\hat{P}^l} \cdot \prod_{l \in S'} \delta_{\mathcal{P}'_i}^2) \), one has \( I_{\mathcal{P}_j}(t_{0,u}, t_{i_j}) = a_j \) for each index \( j \in \{1, \ldots, s\} \) and \( I_{\mathcal{P}'_i}(t_{0,u}, t_i) = 1 \) for each index \( i \in I \).

Fix such a point \( t_{0,u} \) and assume that it is not a branch point. Next apply [Legl3b, lemma 2.5] to obtain that, for each \( j \in \{1, \ldots, s\} \) (resp. for each \( i \in I \)), there is a prime \( \mathcal{Q}_j \) (resp. \( \mathcal{Q}'_i \)) of \( k_{\hat{E}} \) above \( \mathcal{P}_j \) (resp. above \( \mathcal{P}'_i \)) such that \( t_{0,u} \) and \( t_{i_j} \) meet modulo \( \mathcal{Q}_j \) (resp. \( t_{0,u} \) and \( t_i \) meet modulo \( \mathcal{Q}'_i \)). Moreover one may assume that \( I_{\mathcal{Q}_j}(t_{0,u}, t_{i_j}) = I_{\mathcal{P}_j}(t_{0,u}, t_{i_j}) \) for each \( j \in \{1, \ldots, s\} \) and \( I_{\mathcal{Q}'_i}(t_{0,u}, t_i) = I_{\mathcal{P}'_i}(t_{0,u}, t_i) \) for each \( i \in I \). Next apply the Galois part of the Specialization Inertia Theorem to the extension \( \hat{E}k_{\hat{E}}/k_{\hat{E}}(T) \) and the set \( \{ \mathcal{Q}_j / j \in \{1, \ldots, s\} \} \cup \{ \mathcal{Q}'_i / i \in I \} \) of primes to obtain that \( \text{Gal}((\hat{E}k_{\hat{E}})_{t_{0,u}}/k_{\hat{E}}) \) contains an element of each \( C_i \) (\( i \in I \)) and each \( C_j^{a_j} \) (\( j \in \{1, \ldots, s\} \)). Hence \( \text{Gal}((E_{k_{\hat{E}}})_{t_{0,u}}/k_{\hat{E}}) = \overline{G} \) (assumption (a)). Then condition (2) in the conclusion holds with \( t_0 = t_{0,u} \) (as explained in \( \S 3.3.1 \)). As \( \text{Gal}((E_{k_{\hat{E}}})_{t_{0,u}}/k_{\hat{E}}) = \overline{G} \) and \( E/k(T) \) is assumed to be regular (and so the image \( \nu(\overline{G}) \) of \( \overline{G} \) via the morphism \( \nu : \overline{G} \to S_n \) is a transitive subgroup of \( S_n \)), condition (1) in the conclusion holds with \( t_0 = t_{0,u} \), thus ending the proof.

4. **Specializations with specified local behavior**

The aim of this section is theorem 4.1 below which, as already said, conjoins our results from \( \S 3.2 \) and some previous works. Let \( k \) be a number field, \( \mathcal{O} \) the integral closure of \( \mathbb{Z} \) in \( k \) and \( E/k(T) \) a regular finite extension of degree \( n \). Denote the branch point set by \( \{t_1, \ldots, t_r\} \), the Galois closure by \( \hat{E}/k(T) \), the Galois group \( \text{Gal}(\hat{E}/k(T)) \) by \( G \), the geometric Galois group \( \text{Gal}(E\hat{E}/k(T)) \) by \( \overline{G} \), the constant extension in \( \hat{E}/k(T) \) by \( k_{\hat{E}}/k \), the inertia canonical invariant of \( \hat{E}/k(T) \) by \( (C_1, \ldots, C_r) \) and the embedding morphism \( \overline{G} \to S_n \) by \( \nu \).
4.1. **Data.** Below we fix the data for theorem 4.1.

4.1.1. **Data for the Hilbert Specialization Property.** With $\text{cc}(G)$ the number of non trivial conjugacy classes of $G$, pick $\text{cc}(G)$ distinct primes $p_1, \ldots, p_{\text{cc}(G)} \geq r^2|G|^2$ that are totally split in $k_E/Q$ and such that any prime of $O$ lying over one these primes is a good\(^6\) prime for $E/k(T)$\(^7\).

4.1.2. **Data for the ramified part.** Let $S_{ra}$ be a finite set of good primes for $E/k(T)$. For each prime $P \in S_{ra}$,

(a) assume that the ramification index and the residue degree of $P$ in the extension $k/Q$ are equal to 1,

(b) fix a positive integer $a_P$ and an index $i_P \in \{1, \ldots, r\}$ such that $t_{i_P} \neq \infty$, $P$ units $t_{i_P}$ and is a prime divisor of $m_{t_{i_P}}(T) \cdot m_{1/t_{i_P}}(T)$.

4.1.3. **Data for the unramified part.** In condition (b) below, the type of a permutation $\sigma \in S_n$ is the (multiplicative) divisor of all lengths of disjoint cycles involved in the cycle decomposition of $\sigma$ (for example, an $n$-cycle is of type $n^1$).

Let $S_{ur}$ be a finite set of good primes for $E/k(T)$. For each prime $P \in S_{ur}$,

(a) assume that the residue characteristic $p$ satisfies $p \geq r^2|G|^2$ and is totally split in the extension $k_E/Q$,

(b) fix integers $d_{P,1}, \ldots, d_{P,sp}$ such that $d_{P,1}^{1} \ldots d_{P,sp}^{1}$ is the type of an element $\nu(gp)$ of $\nu(G) \subseteq S_n$; denote the conjugacy class of $gp$ in $G$ by $C_P$.

4.2. **Statement of the result.** Denote the residue characteristic of each prime $P \in S_{ra} \cup S_{ur}$ by $p_P$ and assume that the primes $p_P$ ($P \in S_{ra} \cup S_{ur}$) and $p_l$ ($l = 1, \ldots, \text{cc}(G)$) are distinct. Set $\beta = \prod_{l=1}^{\text{cc}(G)} p_l$.

**Theorem 4.1.** There exists some integer $\theta$ satisfying the following. For any integer $t_0$ such that $t_0 \equiv \theta \mod \beta \cdot \prod_{P \in S_{ur}} p_P \cdot \prod_{P \in S_{ur}} p_P^{a_P+1}$, $t_0$ is not a branch point and the following holds.

(1) The specialization algebra $\prod_{l} E_{l,t_0}/k$ of $E/k(T)$ at $t_0$ consists of a single degree $n$ field extension $E_{l,t_0}/k$ and the Galois group $\text{Gal}(\widehat{E_{l_0}}/k)$ of the Galois closure $\widehat{E_{l_0}}/k$ satisfies $G \subseteq \text{Gal}(\widehat{E_{l_0}}/k) \subseteq G$.

(2) For each prime $P \in S_{ra}$, the extension $E_{l,t_0}/k$ satisfies condition $(\text{Ram}/P/S(i_P,a_P))$ from §3.1.

(3) For each prime $P \in S_{ur}$, $P$ does not ramify in $\widehat{E_{l_0}}/k$ and the associated Frobenius is in the conjugacy class $C_P$; moreover the integers $d_{P,1}, \ldots, d_{P,sp}$ are the residue degrees at $P$ of $E_{l_0}/k$.

Theorem 4.1 is proved in §4.4.

\(^6\)Here and in §4.1.3, condition (4) from definition 2.5 can be removed.

\(^7\)Infinitely many such primes exist from the Tchebotarev density theorem.
4.3. The special case \( k = \mathbb{Q} \). In this subsection, assume that \( k = \mathbb{Q} \) and denote the discriminant of a given finite extension \( F/\mathbb{Q} \) by \( d_F \).

4.3.1. Bounds on discriminants. Continue with the data from §4.1.

**Proposition 4.2.** There exist two positive constants \( \gamma \) and \( \delta \) (depending only on \( E/\mathbb{Q}(T) \)) such that the following holds. For at least one specialization point \( t_0 \) from the conclusion of theorem 4.1, one has

\[
|d_{E_{t_0}}| \leq \gamma \cdot \left( \prod_{p \in S_{\text{ur}}} p \cdot \prod_{p \in S_{\text{ra}}} p^{a_p+1} \right)^{\delta}
\]

**Addendum 4.2.** (More on the constants) Given the irreducible polynomial \( P(T, Y) \in \mathbb{Z}[T][Y] \) of some primitive element of \( E/\mathbb{Q}(T) \) assumed to be integral over \( \mathbb{Z}[T] \), denote its discriminant by \( \Delta_P(T) \in \mathbb{Z}[T] \), the degree of \( \Delta_P(T) \) by \( \delta_P \) and its height by \( H(\Delta_P) \). Then, with \( \beta \) the constant introduced before theorem 4.1, one has

\[
|d_{E_{t_0}}| \leq (1 + \delta_P)^{1+\delta_P} \cdot H(\Delta_P) \cdot \beta \cdot \left( \prod_{p \in S_{\text{ur}}} p \cdot \prod_{p \in S_{\text{ra}}} p^{a_p+1} \right)^{\delta} 
\]

Proposition 4.2 is proved in §4.3.3.

**Remark 4.3.** (1) Some lower bounds can also be given. Indeed, assume for example that the integer \( a_p \) is a multiple of the order of the elements of \( C_{i_p} \) for no prime \( p \in S_{\text{ra}} \). Then, for any specialization point \( t_0 \) from the conclusion of theorem 4.1, each prime \( p \in S_{\text{ra}} \) ramifies in the specialization \( E_{t_0}/\mathbb{Q} \) and one has \( \prod_{p \in S_{\text{ra}}} p \leq |d_{E_{t_0}}| \).

In particular, we obtain some extra limitations on the ramification in our specializations. Namely consider a specialization \( E_{t_0}/\mathbb{Q} \) as in proposition 4.2 and denote the set of all primes \( p \notin S_{\text{ra}} \) that ramify in \( E_{t_0}/\mathbb{Q} \) by \( S_{t_0}^{\prime} \). Then one has \( \prod_{p \in S_{\text{ra}} \cup S_{t_0}^{\prime}} p \leq |d_{E_{t_0}}| \). Conjoining this and the upper bound from proposition 4.2 provides the following:

\[
\prod_{p \in S_{t_0}^{\prime}} p \leq \gamma \cdot \left( \prod_{p \in S_{\text{ur}}} p^{\delta} \right) \cdot \left( \prod_{p \in S_{\text{ra}}} p^{2a_p+\delta-1} \right)
\]

Moreover, if \( E_{t_0}/\mathbb{Q} \) is Galois (this holds in particular if this is true of \( E/\mathbb{Q}(T) \)), then the inequality \( \prod_{p \in S_{\text{ra}} \cup S_{t_0}^{\prime}} p \leq |d_{E_{t_0}}| \) can be replaced by the better one \( \prod_{p \in S_{\text{ra}} \cup S_{t_0}^{\prime}} p^{n/2} \leq |d_{E_{t_0}}| \) [Ser81, §1.4, proposition 6].

(2) Similar bounds on the discriminant of the Galois closure \( \widehat{E_{t_0}}/\mathbb{Q} \) of \( E_{t_0}/\mathbb{Q} \) can also be given as [Ser81, §1] provides

\[
|d_{E_{t_0}}| \leq |d_{\widehat{E_{t_0}}}| \leq |G|^{2} \cdot |d_{E_{t_0}}|^{2}|G|^{2}/2
\]

(3) The above bounds are essentially the best possible as the following evidence shows.
Assume that \( E/\mathbb{Q}(T) \) has at least one \( \mathbb{Q} \)-rational branch point\(^8\), which may be assumed to lie in \( \mathbb{Q} \), and continue with the data from §4.1.1. Let \( m_0 \) be a real number satisfying \( m_0 > p_l \) for each \( l \in \{1, \ldots, \text{cc}(G)\} \) and such that each prime \( p \geq m_0 \) is a good prime for \( E/\mathbb{Q}(T) \). Note that \( m_0 \) can be assumed to depend only on \( E/\mathbb{Q}(T) \).

Given a real number \( x \geq m_0 \), apply theorem 4.1 with \( S_{ur} = \emptyset \) and \( S_{ra} \) taken to be the set of all primes \( p \in [m_0, x] \) (this can be done as the extension \( E/\mathbb{Q}(T) \) is assumed to have at least one \( \mathbb{Q} \)-rational branch point). We then obtain a degree \( n \) field extension \( E_{t_0, x}/\mathbb{Q} \) ramifying at each prime \( p \in [m_0, x] \) (and which also satisfies the remaining properties from the conclusion) and, by proposition 4.2, which may be further assumed to satisfy \( \prod_{p \in [m_0, x]} p \leq |d_{E_{t_0, x}}| \leq \gamma \cdot (\prod_{p \in [m_0, x]} p^2)\delta \) (with the constants \( \gamma \) and \( \delta \) from there). Hence one has \( \alpha \cdot \prod_{p \leq x} p \leq |d_{E_{t_0, x}}| \leq \gamma \cdot (\prod_{p \leq x} p)^{2\delta} \) for some positive constant \( \alpha \) depending only on \( E/\mathbb{Q}(T) \).

It then remains to use that \( \log(\prod_{p \leq x} p) \sim x \) as \( x \to \infty \) to obtain that \( c_1 x \leq \log|d_{E_{t_0, x}}| \leq c_2 x \) for some positive constants \( c_1 \) and \( c_2 \) depending only on \( E/\mathbb{Q}(T) \) (and sufficiently large \( x \)).

4.3.2. On theorem 2 from the introduction. Now we explain how obtaining theorem 2 from the introduction. Assume that the regular degree \( n \) extension \( E/\mathbb{Q}(T) \) satisfies the following two conditions:

(1) \( E/\mathbb{Q}(T) \) has at least one \( \mathbb{Q} \)-rational branch point \( t_i \),

(2) the Galois closure \( \hat{E}/\mathbb{Q}(T) \) is regular\(^9\).

Then all but finitely many primes are prime divisors of the polynomial \( m_{t_i}(T) \cdot m_{1/t_i}(T) \) (assumption (1)) and condition (a) from §4.1.3 only requires \( p \) to be large enough (assumption (2)). Then theorem 2 follows immediately from theorem 4.1, proposition 4.2 and remark 4.3.

4.3.3. Proof of proposition 4.2. Let \( P(T,Y) \in \mathbb{Z}[T][Y] \) be the irreducible polynomial of some primitive element of \( E/\mathbb{Q}(T) \) assumed to be integral over \( \mathbb{Z}[T] \) and continue with the extra notation introduced in addendum 4.2. Pick an integer \( u \in [0, \delta_p] \) such that \( t_0 = \theta + u \cdot \beta \cdot \prod_{p \in S_{ur}} p \cdot \prod_{p \in S_{ra}} p^{\alpha_p+1} \) is not a root of \( \Delta_p(T) \) (with \( \theta \) the integer from theorem 4.1). As \( \theta \) may be assumed to satisfy \( 1 \leq \theta \leq \beta \cdot \prod_{p \in S_{ur}} p \cdot \prod_{p \in S_{ra}} p^{\alpha_p+1} \), one has

\[ |t_0| \leq (1 + \delta_p) \cdot \beta \cdot \prod_{p \in S_{ur}} p \cdot \prod_{p \in S_{ra}} p^{\alpha_p+1} \]

\(^8\)More generally, assume that all but finitely many primes are prime divisors of the polynomial \( m_{t_i}(T) \cdot m_{1/t_i}(T) \) (introduced at the end of §2.2).

\(^9\)This condition holds in particular if either \( G = S_n \) (and then \( G = S_n \) too as \( E/\mathbb{Q}(T) \) is assumed to have degree \( n \)) or \( G \) is a simple group.
From condition (1) in the conclusion of theorem 4.1 and the fact that $\Delta_p(t_0) \neq 0$, the polynomial $P(t_0, Y)$ is irreducible over $Q$ (lemma 2.2).

As it is monic and has coefficients in $\mathbb{Z}$, its discriminant $\Delta_P(t_0)$ is a multiple of $d_{E_{t_0}}$. Hence one has

$$|d_{E_{t_0}}| \leq |\Delta_p(t_0)| \leq (1 + \delta_p) \cdot H(\Delta_P) \cdot |t_0|^{\delta_p}$$

Conjoining the two inequalities gives the conclusion of addendum 4.2.

4.4. Proof of theorem 4.1. First we recall how [DL12] handles condition (3) from the conclusion. Given a prime $\mathcal{P} \in \mathcal{S}_{ur}$, denote the order of $g_{\mathcal{P}}$ by $e_{\mathcal{P}}$ and, for simplicity, denote the residue characteristic of $\mathcal{P}$ by $p$. Let $F_{p,e_{\mathcal{P}}}/Q_{p}$ be the unique unramified Galois extension of $Q_{p}$ of degree $e_{\mathcal{P}}$, given together with an isomorphism $f : Gal(F_{p,e_{\mathcal{P}}}/Q_{p}) \rightarrow (g_{\mathcal{P}})$ satisfying $f(\sigma) = g_{\mathcal{P}}$ with $\sigma$ the Frobenius of the extension $F_{p,e_{\mathcal{P}}}/Q_{p}$.

Let $\varphi : G_{Q_{p}} \rightarrow (g_{\mathcal{P}})$ be the corresponding epimorphism. As $p \geq r^2|\mathcal{G}|^2$ and $\mathcal{P}$ is a good prime for $E/k(T)$, [DL12] provides some integer $\theta_{\mathcal{P}}$ such that, for any integer $t \equiv \theta_{\mathcal{P}}$ mod $p$, $t$ is not a branch point and

- the specialization of $E_{Q_{p}}/Q_{p}(T)$ at $t$ corresponds to the epimorphism $\varphi$ (note that $k_{\mathcal{E}}^{\mathcal{P}}Q_{p} = Q_{p}$ as $p$ is assumed to be totally split in $k_{\mathcal{E}}^{\mathcal{P}}/Q_{p}$).
- the specialization algebra of $E_{Q_{p}}/Q_{p}(T)$ at $t$ is equal to $\prod_{t_{i}}^{p} F_{p,d_{\mathcal{P}},l_{i}/Q_{p}}$ where $F_{p,d_{\mathcal{P}},l_{i}/Q_{p}}$ is as above the degree $d_{\mathcal{P},l_{i}}$ unramified extension of $Q_{p}$.

Given $l \in \{1, \ldots, cc(\mathcal{G})\}$, pick a prime $\mathcal{P}_l$ of $\mathcal{O}$ above $p_l$ and associate in a one-one way, a non trivial conjugacy $C_{\mathcal{P}_l}$ of $\mathcal{G}$. For each $l$, [DL12] provides as above an integer $\theta_{l}$ such that, for any integer $t \equiv \theta_{l}$ mod $p_l$, $t$ is not a branch point and the Galois group of the specialization of $E_{Q_{p_l}}/Q_{p_l}(T)$ at $t$ is conjugate in $\mathcal{G}$ to an element of $C_{\mathcal{P}_l}$.

Given a prime $\mathcal{P} \in \mathcal{S}_{ur}$, denote as above the residue characteristic by $p$. From lemma 3.4 (applied over $k$) and condition (a) from §4.1.2 (and as $t_{i_{p}} \neq \infty$), there exists some integer $\theta_{p}$ such that $I_{\mathcal{P}}(t, t_{i_{p}}) = a_{\mathcal{P}}$ for every integer $t$ satisfying $t \equiv \theta_{p}$ mod $p_{i_{p}}^{a_{p}+1}$.

Next use the chinese remainder theorem to find $\theta \in \mathbb{Z}$ such that

- $\theta \equiv \theta_{\mathcal{P}}$ mod $p_{\mathcal{P}}$ for each prime $\mathcal{P} \in \mathcal{S}_{ur}$,
- $\theta \equiv \theta_{l}$ mod $p_{l}$ for each index $l \in \{1, \ldots, cc(\mathcal{G})\}$,
- $\theta \equiv \theta_{p}$ mod $p_{i_{p}}^{a_{p}+1}$ for each prime $\mathcal{P} \in \mathcal{S}_{ur}$.

Fix an integer $t_0$ such that $t_0 \equiv \theta$ mod $\beta \cdot \prod_{\mathcal{P} \in \mathcal{S}_{ur}} p_{\mathcal{P}} \cdot \prod_{\mathcal{P} \in \mathcal{S}_{ur}} p_{\mathcal{P}}^{a_{\mathcal{P}}+1}$.

From the conclusion on $\mathcal{P}_1, \ldots, \mathcal{P}_{cc(\mathcal{G})}$, the Galois group $Gal((E_{k_{\mathcal{E}}})_{t_0}/k_{\mathcal{E}})$ is equal to $\mathcal{G}$. As the extension $E/k(T)$ is assumed to be regular, the specialization algebra of $E/k(T)$ at $t_0$ consists of a single degree $n$ field extension $E_{t_0}/k$. Then conditions (1) and (3) hold. As to condition (2), one has $I_{\mathcal{P}}(t_0, t_{i_{p}}) = a_{\mathcal{P}}$ for each prime $\mathcal{P} \in \mathcal{S}_{ur}$. Conjoining this and $Gal((E_{k_{\mathcal{E}}})_{t_0}/k_{\mathcal{E}}) = \mathcal{G}$ ends the proof (as explained in §3.3.1).
References

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

[Dèb09] Pierre Dèbes. *Arithmétique des revêtements de la droite*. Lecture notes, 2009. At http://math.univ-lille1.fr/~pde/ens.html.

[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.

[DL12] Pierre Dèbes and François Legrand. Twisted covers and specializations. In *Galois-Teichmüller theory and Arithmetic Geometry*, pages 141–162. Proceedings for Conferences in Kyoto (October 2010), H. Nakamura, F. Pop, L. Schneps, A. Tamagawa eds., Advanced Studies in Pure Mathematics 63, 2012.

[DL13] Pierre Dèbes and François Legrand. Specialization results in Galois theory. *Trans. Amer. Math. Soc.*, 365(10):5259–5275, 2013.

[Flo02] Stéphane Flon. *Mauvaises places ramifiées dans le corps des modules d’un revêtement*. PhD thesis, Université des Sciences et Technologies de Lille, France, 2002.

[Fri95] Michael D. Fried. Introduction to modular towers: generalizing dihedral group–modular curve connections. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 111–171. Amer. Math. Soc., Providence, RI, 1995.

[Gey78] Wulf-Dieter Geyer. Galois groups of intersections of local fields. *Israel J. Math.*, 30(4):382–396, 1978.

[Jor72] Camille Jordan. Recherches sur les substitutions. *J. Liouville*, 17:351–367, 1872.

[Leg13a] François Legrand. *Spécialisations de revêtements et théorie inverse de Galois*. PhD thesis, Université Lille 1, France, 2013. At https://sites.google.com/site/francoislegranden/recherche.

[Leg13b] François Legrand. Specialization results and ramification conditions. *Manuscript*, 2013. arXiv:1310.2189.

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Pub. Math. I.H.E.S.*, 54:323–401, 1981.

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

E-mail address: flegrand@post.tau.ac.il

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 6997801, Israel

Department of Mathematics and Computer Science, The Open University of Israel, Ra’anana 4353701, Israel