ACTA ARITHMETICA
172.2 (2016)

Reduction and specialization of polynomials

by

Pierre Dèbes (Lille)

1. Presentation. The main topic is the irreducibility of polynomials obtained by reduction or specialization from a polynomial $P \in A[T,Y]$ with coefficients in an integral domain A and assumed to be irreducible over the algebraic closure $\overline{k}$ of the fraction field k of A. By "reduction" we mean reduction of the coefficients modulo some prime ideal $\mathfrak{p} \subset A$, and "specialization" means specialization of the indeterminate T to some value $t \in A$ ([1]). The case that A is the ring of integers of some number field k is a typical situation. Another one is when $A = R[X_1, \dots, X_s]$ is a polynomial ring in s new indeterminates $X_1, \dots, X_s$ over some coefficient ring R, and $\mathfrak{p}$ is the ideal generated by $X_1 - x_1, \dots, X_s - x_s$ with $x_1, \dots, x_s \in R$. We then think of P as a *family of polynomials* parametrized by the affine space $\mathbb{A}^s$ and the reduction is a "specialization of the parameters".

The Bertini–Noether theorem for reduction—P modulo $\mathfrak{p}$ is irreducible over the algebraic closure $\overline{\kappa_\mathfrak{p}}$ of the fraction field $\kappa_\mathfrak{p}$ of $A/\mathfrak{p}$, for all primes $\mathfrak{p}$ but in a proper closed Zariski subset of $\mathrm{Spec}(A)$—and Hilbert's irreducibility theorem (HIT) for specialization—if A is the ring of integers of some number field k, then $P(t,Y)$ is irreducible in $k[Y]$ for infinitely many $t \in A$—are the fundamental results. Among existing methods for these two results, some have a common trend which is to reduce modulo "good primes". This mainly refers to the Grothendieck good reduction theorem (GRT) and the so-called congruence approach to HIT, notably developed by Eichler [Eic39], Fried [Fri74], Fried–Jarden [FJ04, §13.3], Ekedahl [Eke90], Colliot-Thélène and Serre [Ser92, §3.5].

2010 *Mathematics Subject Classification*: Primary 12E05, 12E25, 14E20, 12Yxx; Secondary 12E30, 12Fxx, 14Gxx.
Key words and phrases: polynomials, reduction, specialization, Bertini–Noether theorem, Hilbert irreducibility theorem, Grothendieck good reduction criterion.
Received 26 May 2015; revised 18 September 2015.
Published online 3 December 2015.

([1]) Specialization is also a reduction of P, but viewed as a polynomial in Y with coefficients in $A[T]$; to avoid confusion we prefer to use two different words.

DOI: 10.4064/aa8176-12-2015

We contribute to this trend. Our approach rests on the same fundamental results but introduces a certain tool that somewhat unifies both the reduction and specialization questions. We obtain fully explicit statements, phrased in terms of polynomials rather than the corresponding algebraic covers ([2]) and which have new applications to issues around the effective Hilbert irreducibility theorem. The following statement gives an idea of our results.

(THEOREM 3.1) *Assume k is a number field. There exist integers N, B, C and a finite extension $L/\mathbb{Q}$ such that the following holds. If $p_1, \dots, p_N$ are N distinct prime numbers satisfying*

$(*)$ *$p_i \nmid B$, $p_i \geq C$ and p_i is totally split in $L/\mathbb{Q}$, $i = 1, \dots, N$,*

then for any multiple $a \in \mathbb{Z}$ of $p_1 \cdots p_N$, there exists $b \in \mathbb{N}$ such that the polynomial $P(am + b, Y)$ is irreducible in $k[Y]$ for every integer m.

N, B, C, L are precisely given in §3, making Theorem 3.1 totally explicit and improving on previous results which only showed the existence of some cosets $a\mathbb{Z} + b$ satisfying the conclusion.

The main ingredients are the GRT and the last variant of the congruence approach, developed in [DG12], [DL13], [DL12], which we adjust and recast in our context; Theorem 3.1 is an explicit polynomial version of [DL12, Corollary 4.5].

Our new tool is the *bad prime divisor* of P. It is a certain non-zero parameter $\mathcal{B}_P \in A$, which is directly computable from the coefficients of P through elementary operations, starting with the discriminant $\Delta_P \in A[T]$ of P relative to Y (see §2), and which articulates both the reduction and specialization issues. The integer B of Theorem 3.1 can be taken to be the norm $N_{k/\mathbb{Q}}(\mathcal{B}_P)$.

The point of $\mathcal{B}_P$ is this. When A is a Dedekind domain of characteristic 0, the non-zero prime ideals $\mathfrak{p} \subset A$ dividing $\mathcal{B}_P$ are those for which some of the distinct roots of Δ_P become equal or infinite modulo $\mathfrak{p}$. Such a prime ideal is called *bad* and the other ones are the *good* primes. Our bad/good primes relate to more geometric versions previously introduced; an advantage of $\mathcal{B}_P$ is that *it behaves well under morphisms*: if $\mathfrak{p}$ is a good prime such that $\deg_Y(P)! \notin \mathfrak{p}$, we have

(THEOREM 2.6-a) $\mathcal{B}_{P \bmod \mathfrak{p}} = \mathcal{B}_P \bmod \mathfrak{p}$ *and is non-zero in $A/\mathfrak{p}$.*

This is one conclusion of Theorem 2.6, which contains the gist of the whole reduction-specialization approach. For $\mathfrak{p}$ as above, we have the Bertini–Noether conclusion:

([2]) The difference is that the notion of cover identifies all the polynomial equations of a given cover. This is illustrated by the example of $P = Y^2 - 4T$ which, depending on whether it is viewed as a cover or a polynomial, has good reduction at 2 or not.

(2.6-b) *The polynomial P modulo $\mathfrak{p}$ is irreducible in $\overline{\kappa_{\mathfrak{p}}}[T,Y]$* ([3]).

Furthermore, when A is the ring of integers of a number field k, we have the following "Chebotarev" conclusion ([4]): if in addition $\mathfrak{p}$ is of suitably large norm (a condition leading to the integer C of Theorem 3.1) and satisfies one last assumption (below), then

(2.6-c) *Each element of the Galois group $\mathcal{G}$ of P over $\overline{k}(T)$ is the Frobenius at $\mathfrak{p}$ of the splitting field of some specialization $P(t_0,Y)$ ($t_0 \in A$).*

The last assumption on $\mathfrak{p}$ involves another important phenomenon: the possible appearance of new constants in the splitting field of P over $k(T)$, and the assumption is that $\mathfrak{p}$ be totally split in the field of new constants (the field L of Theorem 3.1). For example, for $P = Y^n - T \in \mathbb{Q}[T,Y]$, nth roots of unity appear. Proposition 2.8 collects some information on this phenomenon, some of it new to our knowledge. But it remains mysterious and hard to control. In "most cases" however, no constant extension occurs and so the condition on $\mathfrak{p}$ disappears. By "most cases" we mean that this holds if $\mathcal{G} = S_n$ (with $n = \deg_Y(P)$), which in various senses is the generic case.

We postpone the proof of Theorem 2.6 to §5 and prefer to show first how this statement leads to explicit versions of Hilbert's irreducibility theorem, for one polynomial in §3, and for a family of polynomials in §4.

Theorem 3.1 discussed above is a first application. For $k = \mathbb{Q}$, we deduce bounds for the least integer $t \geq 0$ such that $P(t,Y)$ is irreducible in $\mathbb{Q}[Y]$, along with some algorithms to find it. Bounds known so far [Dèb96], [SZ95], [Wal05], [DW08], involve these parameters:

$$\deg_Y(P) = n, \quad \deg_T(P) = m \quad \text{and} \quad H(P) = \text{height of } P.$$

Finding a bound not depending on $H(P)$ and so depending only on the degree of P is an important problem. It is in particular a non-trivial test for the far-reaching Lang conjecture on the rational points on an algebraic variety of general type over a number field; this conjecture is indeed known to imply that such a bound exists [DW08, §5]. Our bounds only involve the degree n and the discriminant Δ_P:

(Corollaries 3.6 & 3.8) *The bounds we obtain depend on*

$$n = \deg_Y(P), \quad \rho = \textit{number of distinct roots of } \Delta_P$$

([3]) A proof of this, not using the GRT as we do but in the special case that the residue characteristic is positive, can be found in [Zan97].

([4]) This conclusion already appears in some form in earlier papers without the explicit conditions on $\mathfrak{p}$ [FJ04, Lemma 13.3.4], [Eke90, Lemma 1.2]. Our explicitness precisely follows from the use of the GRT which replaces the ineffective use of the Bertini–Noether theorem.

and

$$\begin{cases} \textit{the number } \beta \textit{ of bad primes of } P & \textit{in ``most cases''},\\ \textit{the bad primes of } P \textit{ and the prime factors} & \\ \quad \textit{of some non-zero integral value } \Delta_P(\tau) & \textit{in all cases } ([5]). \end{cases}$$

Our bounds are larger than those of [Wal05] which are more appropriate for an algorithmic use. The interest of ours lies in the parameters they depend on. First, the dependence on n, ρ is better than that on n, m: indeed, $\rho \le \deg(\Delta_P) \le (2n-1)m$. Furthermore, in the generic case $\mathcal{G} = S_n$, the parameters n, ρ, β are numerical degrees which do not involve the height of the coefficients of P. Finally, the bounds we obtain when n, ρ, β are fixed still concern infinitely many polynomials, while there are only finitely many $P \in \mathbb{Z}[T,Y]$ with n, m, $H(P)$ bounded: for example for $P_a = Y^n - aY - T$ ($a \in \mathbb{Z}$), for which $\mathcal{G} = S_n$, we have $\rho = n-1$ and the bad primes are the prime divisors of $n(n-1)a$.

In §4, in the context of a family of polynomials—$P \in A[T,Y]$ with $A = R[X_1, \dots, X_s]$ and R the ring of integers of some number field k—our goal is to investigate to what extent the bounds given by §3 for each individual polynomial $P(x_1, \dots, x_s, T, Y) \in R[T,Y]$ depend on $(x_1, \dots, x_s) \in R^s$. An ideal conclusion would be to have a constant global bound. Using non-standard analysis, Yasumoto could reach this goal for $s = 1$ [Yas87]; he mentioned that the case $s > 1$ seemed very difficult. In the general situation $s \ge 1$, our approach leads to a "family of bounds". In the generic case $\mathcal{G} = S_n$, these bounds involve polynomials in $(x_1, \dots, x_s)$ with coefficients in R. Some of these polynomials can be made constant, for example $\deg(P(x_1, \dots, x_s, T, Y)) \le \deg_{(T,Y)}(P)$, but there remains one that is not, which is the bad prime divisor. Our result shows some progress for $s > 1$ but the ideal goal remains to be attained.

2. Bad prime divisor. Let A be an integrally closed domain with fraction field k.

2.1. Reduced polynomial. The *reduced* form Δ^{red} of a non-zero polynomial $\Delta \in A[T]$ is defined as follows. Denote the leading coefficient of Δ by Δ_0 and its distinct roots by $t_1, \dots, t_\rho \in \overline{k}$. Then

$$\Delta^{\mathrm{red}} = \Delta_0^{\rho} \prod_{1 \le i \le \rho} (T - t_i)$$

and Δ^{red} is defined to be 1 if $\Delta \in A$ (i.e. $\rho = 0$).

([5]) There is an intermediate situation: if the genus of the splitting field of P is at least 2, the bound depends only on n, ρ and the bad primes of P (Corollary 3.7).

Consider the factorization $\Delta = \Delta_0 \prod_{j=1}^{\ell} Q_j^{\alpha_j}$ of Δ in $k[T]$ with $Q_1, \dots, Q_\ell$ the distinct irreducible and monic factors in $k[T]$. We will use several times the following condition on Δ:

(∗) *The polynomials $Q_1, \dots, Q_\ell$ are separable, i.e. have no multiple roots in $\overline{k}$.*

This holds in particular if k is of characteristic 0 or greater than $\deg(\Delta)$.

LEMMA 2.1. *Assume that the polynomial Δ satisfies (∗). Then*

$$\Delta^{\mathrm{red}} = \Delta_0^{\rho} \prod_{1 \le j \le \ell} Q_j = \Delta_0^{\rho-1} \frac{\Delta}{\gcd(\Delta, \Delta')}$$

where the gcd is calculated in the ring $k[T]$ and made monic by multiplying by a suitable non-zero constant. Furthermore, Δ^{red} is a polynomial with coefficients in A.

Proof. The two polynomials in the first equality have only simple roots (by (∗)) and have the same sets of roots. The equality follows since they also have the same leading term. The second equality rests on the fact that if $\Delta = \Delta_0 \prod_{j=1}^{\rho} (T - t_j)^{\beta_j}$ with $\beta_1, \dots, \beta_\rho \ge 1$, then, up to some non-zero factor in k, $\gcd(\Delta, \Delta') = \prod_{j=1}^{\rho} (T - t_j)^{\beta_j - 1}$. Finally, $\Delta_0 t_1, \dots, \Delta_0 t_\rho$ are integral over A. Hence so are the coefficients of $\Delta^{\mathrm{red}} = \prod_{1 \le i \le \rho} (\Delta_0 T - \Delta_0 t_i)$. As they are also in k, and A is integrally closed, they are in A. ∎

REMARK 2.2. The second formula, which makes it possible to calculate Δ^{red} thanks to the Euclidean algorithm, is useful in practice.

2.2. Reduced discriminant and bad prime divisor. Let $P \in A[T, Y]$ be a polynomial such that $\deg_Y(P) = n \ge 1$ and assumed to be monic and separable in Y.

REMARK 2.3. A standard transformation makes it possible to reduce to the situation where P is monic in Y. Namely replace

$$P(T, Y) = P_0 Y^n + P_1 Y^{n-1} + \cdots + P_n$$

with $P_0, P_1, \dots, P_n \in A[T]$ by

$$Q(T, Y) = P_0^{n-1} P(T, Y/P_0) = Y^n + P_1 Y^{n-1} + \cdots + P_0^{n-1} P_n.$$

It is convenient, for the theory and in practice, to start with this transformation when studying the reduction and reducibility properties of a polynomial P. The factor P_0 is retrieved and so is implicitly kept track of in the discriminant of the polynomial $Q(T, Y)$.

Denote the *discriminant* of P relative to Y by

$$\Delta_P = \mathrm{disc}_Y(P).$$

It is a non-zero polynomial in $A[T]$ of degree $\leq (2n-1)\deg_T(P)$. Consider the *reduced discriminant*

$$\Delta_P^{\mathrm{red}} = (\Delta_{P,0})^{\rho} \prod_{i=1}^{\rho} (T - t_i) \in A[T]$$

where $\Delta_{P,0}$ is the leading coefficient of Δ_P and $t_1, \dots, t_\rho$ are the distinct roots of Δ_P in $\overline{k}$. Assume further that Δ_P satisfies condition $(*)$. Then $\Delta_P^{\mathrm{red}} \in A[T]$ and its discriminant

$$\mathrm{disc}(\Delta_P^{\mathrm{red}}) = (\Delta_{P,0})^{2\rho(\rho-1)} \prod_{1 \leq i \neq j \leq \rho} (t_j - t_i)$$

is an element of A, non-zero since by construction Δ_P^{red} has no multiple root in $\overline{k}$ ([6]). Define then an element $\mathcal{B}_P$ by

$$\mathcal{B}_P = \Delta_{P,0} \cdot \mathrm{disc}(\Delta_P^{\mathrm{red}}).$$

We have $\mathcal{B}_P \in A$ and $\mathcal{B}_P \neq 0$.

Definition 2.4. The maximal ideals $\mathfrak{p} \subset A$ that contain $\mathcal{B}_P$ are called the *bad primes* of $P \in A[T,Y]$, and $\mathcal{B}_P$ is called the *bad prime divisor*. Maximal ideals $\mathfrak{p} \subset A$ that are not bad are said to be *good*.

Remark 2.5. (a) If $A_0 \subset A$ is an integrally closed subring and P is in $A_0[T,Y]$, the bad prime divisors relative to A_0 and to A coincide.

(b) The resultant

$$\mathrm{res}(\Delta_P^{\mathrm{red}}, (\Delta_P^{\mathrm{red}})')$$

is an alternative definition of $\mathcal{B}_P$. It is indeed equal to the discriminant $\mathrm{disc}(\Delta_P^{\mathrm{red}})$ multiplied by the leading term $\Delta_{P,0}^{\rho}$ of Δ_P^{red}, and so the set of bad primes remains the same. Similarly the polynomial $\mathrm{res}(P, P')$ can be used instead of Δ_P at the beginning of the construction. In practice, it can be advantageous to use the resultant rather than the discriminant; the former is indeed easier to compute from its Sylvester definition as a determinant. In the same vein, one may replace $\Delta_{P,0}^{\rho}$ by $\Delta_{P,0}^{\rho'}$ with some $\rho' \geq \rho$ (e.g. $\rho' = \deg(\Delta_P)$) in the definition of Δ_P^{red}; this will not affect the set of prime divisors of $\mathcal{B}_P$.

2.3. The central result. Retain the notation introduced in §2 and assume further that A is a Dedekind domain.

Let $\mathcal{G}$ be the Galois group of the splitting field of P over $\overline{k}(T)$; $\mathcal{G}$ is called the *monodromy group* of P, it is a transitive subgroup of S_n with $n = \deg_Y(P)$. Also denote by $\widehat{k}_P/k$ the constant extension in the splitting field $\widehat{F}/k(T)$ of the polynomial P, i.e. $\widehat{k}_P = \widehat{F} \cap \overline{k}$.

([6]) When $\Delta_P \in A$, e.g. when $\deg_T(P) = 0$, then $\Delta_P^{\mathrm{red}} = 1$ and $\mathrm{disc}(\Delta_P^{\mathrm{red}}) = 1$.

If $\mathfrak{p} \subset A$ is a non-zero prime ideal, denote the residue field $A/\mathfrak{p}$ by $\kappa_\mathfrak{p}$, the reduction map by $s_\mathfrak{p} : A \to \kappa_\mathfrak{p}$, the localized ring of A by $\mathfrak{p}$ by $A_\mathfrak{p}$, and the polynomial obtained by reducing the coefficients of P by $s_\mathfrak{p}(P)$.

THEOREM 2.6. *Assume k is of characteristic 0 or greater than $\deg(\Delta_P)$. Let $\mathfrak{p} \subset A$ be a good prime of P such that $|\mathcal{G}| \notin \mathfrak{p}$. Then we have these three conclusions:*

(Good Behaviour) *We have*

$$\Delta^{\mathrm{red}}_{s_\mathfrak{p}(P)} = s_\mathfrak{p}(\Delta^{\mathrm{red}}_P) \neq 0, \qquad \mathcal{B}_{s_\mathfrak{p}(P)} = s_\mathfrak{p}(\mathcal{B}_P) \neq 0.$$

(GRT) *If P is irreducible in $\overline{k}(T)[Y]$, the polynomial $s_\mathfrak{p}(P)$ is monic, separable in Y, irreducible in $\overline{\kappa_\mathfrak{p}}[T, Y]$ and of monodromy group $\mathcal{G}$.*

Assume further that k is a number field and A is its ring of integers.

(Chebotarev) *If $\mathfrak{p}$ is totally split in the extension $\widehat{k}_P/k$ and of norm $N_{k/\mathbb{Q}}(\mathfrak{p}) \geq (\rho+1)^2|\mathcal{G}|^2$, then for every $\omega \in \mathcal{G}$, there is an element $t_\mathfrak{p} \in A$ such that $\Delta_P(t_\mathfrak{p}) \notin \mathfrak{p}$ and for every $t \in A_\mathfrak{p}$ with $t \equiv t_\mathfrak{p}$ modulo $\mathfrak{p}$ the Frobenius at $\mathfrak{p}$ of the splitting field of $P(t, Y)$ over $\widehat{k}_P$ is conjugate to ω in $\mathcal{G}$.*

The condition $\mathcal{B}_{s_\mathfrak{p}(P)} = s_\mathfrak{p}(\mathcal{B}_P) \neq 0$ can be equivalently rephrased as saying that no distinct roots t_i and t_j of Δ_P coincide modulo $\mathfrak{p}$, and none of the roots t_i is ∞ modulo $\mathfrak{p}$.

Theorem 2.6 and its Addendum 2.8 below are proved in §5. The GRT part is essentially the Grothendieck good reduction criterion. The Chebotarev part is deduced from revisiting the results of [DG12] and making them explicit. The Good Behaviour part is new.

2.4. First two examples. We give two examples illustrating Theorem 2.6.

2.4.1. *Specializations $P(t, Y)$ with no root.* The first one is an immediate consequence of the Chebotarev part. Assume $k = \mathbb{Q}$ for simplicity.

COROLLARY 2.7. *If $\mathfrak{p} = p\mathbb{Z}$ is as in* (Chebotarev)*, there is a coset $p\mathbb{Z}+b \subset \mathbb{Z}$ such that for each $t \in p\mathbb{Z}+b$, $P(t, Y)$ has no roots in $\mathbb{Q}$.*

Proof. The subgroup $\mathcal{G} \subset S_n$ being transitive, there classically exists $\omega \in \mathcal{G}$ with no fixed points. The result follows from the Chebotarev conclusion applied to this ω. ∎

2.4.2. *Successive specializations.* Let $P \in k[X_1, \ldots, X_s][T, Y]$ be a polynomial, monic, separable in Y and assumed to be irreducible in the ring $\overline{k(X_1, \ldots, X_s)}[T, Y]$. Consider its bad prime divisor $\mathcal{B}_P \in k[X_1, \ldots, X_s]$. Theorem 2.6 can be applied to P viewed as being in $k(X_1, \ldots, X_{s-1})[X_s]$

$[T,Y]$. The bad prime divisor of P relative to $k(X_1,\dots,X_{s-1})[X_s]$ is the same as relative to the smaller ring $k[X_1,\dots,X_s]$ (Remark 2.5). Hence it is the polynomial $\mathcal{B}_P$ in $k[X_1,\dots,X_s]$ introduced above.

Assume k is of characteristic 0 for simplicity; the condition $|\mathcal{G}|\notin\mathfrak{p}$ then always holds. Let $x_s\in k$ be such that $\mathcal{B}_P(X_1,\dots,X_{s-1},x_s)\neq 0$. From Theorem 2.6, $P(X_1,\dots,X_{s-1},x_s,T,Y)$ is monic, separable in Y and irreducible in $\overline{k(X_1,\dots,X_{s-1})}[T,Y]$, and its bad prime divisor is $\mathcal{B}_P(X_1,\dots,X_{s-1},x_s)\in k[X_1,\dots,X_{s-1}]$. Theorem 2.6 can then be applied to $P(X_1,\dots,X_{s-1},x_s,T,Y)$ to specialize X_{s-1}. An inductive argument finally leads to this conclusion:

(∗) *If $(x_1,\dots,x_s)\in k^s$ satisfies $\mathcal{B}_P(x_1,\dots,x_s)\neq 0$ in k, then the polynomial $P(x_1,\dots,x_s,T,Y)\in k[T,Y]$ is irreducible in $\overline{k}[T,Y]$.*

A variant of this argument will be used in §4.4.

2.5. More on the extension $\widehat{k}_P/k$. Let $F/k(T)$ be the extension generated by some root of P (as a polynomial in Y). Recall that the *constant extension* in $F/k(T)$ is the extension $F\cap\overline{k}/k$. If the polynomial P is irreducible in $\overline{k}[T,Y]$, we have $F\cap\overline{k}=k$; the extension $F/k(T)$ is then said to be *regular over k*. The extension $\widehat{k}_P/k$ is the constant extension in the Galois closure $\widehat{F}/k(T)$ of $F/k(T)$. It need not be trivial even though $F/k(T)$ is regular over k. In general, if $\mathcal{G}_{\rm a}=\mathrm{Gal}(\widehat{F}/k(T))$, the extension $\widehat{k}_P/k$ is Galois of group $\mathcal{G}_{\rm a}/\mathcal{G}$.

Addendum 2.8 (on the constant extension).

(a) *We have $\widehat{k}_P=k$ in each of the following situations:*
  (a-1) *P is irreducible in $\overline{k}(T)[Y]$ and the extension $F/k(T)$ is Galois and regular over k,*
  (a-2) *$\mathcal{G}=S_n$.*

(b) (Complement to (GRT)) *If P is irreducible in $\overline{k}(T)[Y]$, $\mathfrak{p}$ a good prime of P and $|\mathcal{G}|\notin\mathfrak{p}$, then the residue extension of $\widehat{k}_P/k$ at some/any prime above $\mathfrak{p}$ contains the constant extension in the splitting field of $s_{\mathfrak{p}}(P)$ over $\kappa_{\mathfrak{p}}(T)$.*

(c) *If k is a number field and $\widehat{F}$ is a function field of genus ≥ 2, then $\widehat{k}_P/k$ is one from the finite list of extensions of k of degree $\leq|\mathrm{Nor}_{S_n}(\mathcal{G})|/|\mathcal{G}|$ and unramified at each good prime of P.*

In §3 and §4, we use Theorem 2.6 and its Addendum 2.8 to deduce quite precise versions of HIT for a single polynomial and for a family of polynomials over number fields.

3. Hilbert irreducibility theorem. We retain the notation introduced in previous sections and assume further that k is a number field, A is its ring of integers and $P \in A[T,Y]$ is irreducible in $\overline{k}[T,Y]$.

3.1. From Chebotarev to Hilbert. A standard argument easily connects the Chebotarev conclusion from Theorem 2.6 to a Hilbert conclusion. Namely if $C_1,\dots,C_N$ are N conjugacy classes of $\mathcal{G}$ and $\mathfrak{p}_1,\dots,\mathfrak{p}_N$ are N non-zero prime ideals of A that are good, of norm $N_{k/\mathbb{Q}}(\mathfrak{p}) \geq (\rho+1)^2|\mathcal{G}|^2$ and totally split in the extension $\widehat{k}_P/k$, then the Chebotarev conclusion combined with the Chinese remainder theorem provides an element $b \in A$ with the following property:

(∗) *For every $t \in A_{\mathfrak{p}_1} \cap \cdots \cap A_{\mathfrak{p}_N}$, in particular for every $t \in A$, if $t \equiv b \bmod \mathfrak{p}_1 \cdots \mathfrak{p}_N$, then the Galois group over $\widehat{k}_P$ of the polynomial $P(t,Y)$ contains elements of each of the conjugacy classes $C_1,\dots,C_N$.*

Furthermore, under the assumption that the respective prime numbers $p_1,\dots,p_n \in \mathbb{Z}$ below $\mathfrak{p}_1,\dots,\mathfrak{p}_N$ are totally split in the extension $\widehat{k}_P/\mathbb{Q}$ (and not just $\mathfrak{p}_1,\dots,\mathfrak{p}_N$ in $\widehat{k}_P/k$), then b can be chosen in $\mathbb{Z}$.

Hence if $C_1,\dots,C_N$ are initially chosen so that

(∗∗) *for any $(g_1,\dots,g_N) \in C_1 \times \cdots \times C_N$, the subgroup $\langle g_1,\dots,g_N\rangle \subset \mathcal{G}$ acts transitively on $\{1,\dots,n\}$,*

then the Galois group of $P(t,Y)$ acts transitively on $\{1,\dots,n\}$; consequently, $P(t,Y)$ is irreducible in $\widehat{k}_P[Y]$ and *a fortiori* in $k[Y]$.

Such a choice of $C_1,\dots,C_N$ is always possible: from a classical lemma of Jordan [Jor72], (∗∗) holds if $C_1,\dots,C_N$ are all the non-trivial conjugacy classes of $\mathcal{G}$; and then even more holds since in this case we have in fact $\langle g_1,\dots,g_N\rangle = \mathcal{G}$. Therefore if $N_{\mathcal{G}}$ is the smallest integer N such that (∗∗) holds and $\mathrm{cc}(\mathcal{G})$ is the number of conjugacy classes of $\mathcal{G}$, then

$$N_{\mathcal{G}} < \mathrm{cc}(\mathcal{G}) \leq |\mathcal{G}| \leq n!.$$

However $N_{\mathcal{G}}$ can be smaller than these bounds: for example, if $\mathcal{G}$ contains an n-cycle, then $N_{\mathcal{G}} = 1$.

3.2. Main result. We obtain the following version of Hilbert's irreducibility theorem.

THEOREM 3.1. *For the integers N, B, C and the finite extension $L/\mathbb{Q}$ specified below, we have the following. If $p_1,\dots,p_N$ are N distinct prime numbers satisfying*

(∗) *$p_i \nmid B$, $p_i \geq C$ and p_i is totally split in $L/\mathbb{Q}$, $i = 1,\dots,N$,*

then for any multiple $a \in \mathbb{Z}$ of $p_1 \cdots p_N$, there exists $b \in \mathbb{N}$ such that $P(am+b, Y)$ is irreducible in $k[Y]$ for every integer m.

ADDENDUM 3.2 (on the constants). *One can take*

(a) $N = N_{\mathcal{G}}$ (*see* §3.1),
(b) $B = N_{k/\mathbb{Q}}(\mathcal{B}_P)$ (*norm of the bad prime divisor*),
(c) $C = (\rho+1)^2|\mathcal{G}|^2$ (ρ *is the number of distinct roots of the discriminant* Δ_P *and* $\mathcal{G}$ *is the monodromy group of* P),
(d) $L = \widehat{k}_P$ (*constant extension in Galois closure*).

REMARK 3.3 (on the constants). (a) One can also take for B the product of all distinct primes $p \in \mathbb{N}$ dividing $N_{k/\mathbb{Q}}(\mathcal{B}_P)$.

(b) Recall some estimates which relate our parameters to other classical ones; here $D = \deg(P)$, r is the branch point number of the extension $F/k(T)$ associated with $P(T, Y)$ and g its genus, i.e. the genus of the curve $P(t, y) = 0$:

$$\begin{cases} r \le \rho + 1 \le \deg(\Delta_P) + 1 \le (2n-1)m + 1 \quad (\rho = \deg(\Delta_P^{\mathrm{red}}); \S 2) \\ r/2 + 1 - n \le g \le rn/2 + 1 - n - r/2 \quad \text{(Riemann–Hurwitz)} \\ g \le \frac{1}{2}(D-1)(D-2) \quad [\text{FJ04, Corollary 5.3.5}]. \end{cases}$$

REMARK 3.4 (on the statement). (a) Denote by $\mathcal{H}_P$ the Hilbert subset of all $t \in k$ such that $P(t, Y)$ is irreducible in $k[Y]$. The conclusion of Theorem 3.1 can be rephrased as saying that for any multiple $a \in \mathbb{Z}$ of $p_1 \cdots p_N$, the Hilbert subset $\mathcal{H}_P$ contains at least one coset modulo a, or equivalently that, for some $b \in \mathbb{N}$, the Hilbert subset associated with the polynomial $P(aT + b, Y)$ contains all integers.

(b) The statement readily extends to several polynomials $P_1, \dots, P_\ell \in A[T, Y]$: if N_j, B_j, C_j, L_j are given by Theorem 3.1 for the polynomial P_j, then taking $N = N_1 + \cdots + N_\ell$, $B = B_1 \cdots B_\ell$, $C = \max(C_1, \dots, C_\ell)$ and $L/\mathbb{Q}$ the compositum of the extensions $L_1/\mathbb{Q}$, …, $L_\ell/\mathbb{Q}$ and using the Chinese remainder theorem yields the conclusion of Theorem 3.1 with $\mathcal{H}_{P_1} \cap \cdots \cap \mathcal{H}_{P_\ell} \cap \mathbb{Z}$ replacing $\mathcal{H}_P \cap \mathbb{Z}$.

(c) Using (b) one can relax the assumption that $P(T, Y)$ is irreducible in $\overline{\mathbb{Q}}[T, Y]$ to only assume that it is irreducible in $k[T, Y]$. A classical reduction [Dèb09, lemme 5.1.3] indeed shows that

$$\mathcal{H}_P \supset \mathcal{H}_{P_1} \cap \cdots \cap \mathcal{H}_{P_\ell} (\text{up to some finite set } ([7]))$$

with $P_1, \dots, P_\ell$ the irreducible factors of P in $\overline{\mathbb{Q}}[T, Y]$. This reduction involves a finite extension of the base field k and so requires to apply Theorem 3.1 to that bigger number field.

([7]) Of cardinality depending only on $\deg(P)$.

(d) Combining (b) and (c) shows that Theorem 3.1 extends to the situation where $\mathcal{H}_P$ is replaced by a general Hilbert subset of k, i.e. the intersection of several subsets $\mathcal{H}_P$ with P irreducible in $k[T,Y]$.

(e) Proceeding as in §3.1 but with a bigger set $\{\mathfrak{p}_1,\dots,\mathfrak{p}_N,\mathfrak{q}_1,\dots,\mathfrak{q}_M\}$ of primes (satisfying the assumptions of the Chebotarev conclusion of Theorem 2.6), one obtains an improved conclusion of Theorem 3.1 for which in addition to $P(am+b,Y)$ being irreducible in $k[Y]$, the Frobenius of the splitting field of $P(am+b,Y)$ over $\widehat{k}_P$ at each prime $\mathfrak{q}_j$ can be prescribed to be conjugate to an arbitrarily given element of $\mathcal{G}$, $j=1,\dots,M$. This yields the type of conclusions that are given in previous papers in a geometric context; see for example [DL12, Corollary 4.5].

3.3. Bounds for the least specialization in $\mathcal{H}_P$. Assume $k=\mathbb{Q}$. Denote by β the number of bad primes of P, i.e. the number of prime factors of $\mathcal{B}_P$. The general idea is to minimize $N_{\mathcal{G}}$ and evaluate the minimum integer M such that the interval $[(\rho+1)^2|\mathcal{G}|^2,M]$ contains $\beta+N_{\mathcal{G}}$ primes that are totally split in $\widehat{\mathbb{Q}}_P/\mathbb{Q}$. This interval then automatically contains $N_{\mathcal{G}}$ primes satisfying condition $(*)$ from Theorem 3.1, which then produces a coset $a\mathbb{Z}+b\subset\mathcal{H}_P$ with a the product of $N_{\mathcal{G}}$ such primes.

In §3.3.1 and §3.3.2, we focus on the search of the integer a. This leads to bounds for the least positive integer in $\mathcal{H}_P$. In §3.3.3, we make some further algorithmic comments on the search of b.

3.3.1. *Special case $\widehat{\mathbb{Q}}_P=\mathbb{Q}$.* In this case the condition that the primes are totally split in $\widehat{\mathbb{Q}}_P/\mathbb{Q}$ disappears and we obtain this statement.

Corollary 3.5. *If $\widehat{\mathbb{Q}}_P=\mathbb{Q}$, e.g. in each of the situations* (a-1) *and* (a-2) *from Addendum* 2.8*, the Hilbert subset $\mathcal{H}_P$ contains a coset $a\mathbb{Z}+b$ with a and b smaller than some bound depending only on n, ρ and β.*

In particular, when $\mathcal{G}=S_n$, we have $\widehat{\mathbb{Q}}_P=\mathbb{Q}$ and $N_{\mathcal{G}}=1$.

Corollary 3.6. *Assume $k=\mathbb{Q}$ and $\mathcal{G}=S_n$. Then for every good prime number $p\geq((\rho+1)n!)^2$, there is a coset $p\mathbb{Z}+b\subset\mathbb{Z}$ such that $P(t,Y)$ is irreducible in $\mathbb{Q}[Y]$ for every $t\in p\mathbb{Z}+b$. Furthermore, p and b can be taken as follows and can be bounded in terms of n, ρ, β:*

- *p: the first good prime of P that is $\geq((\rho+1)n!)^2$;*
- *b: any integer such that $P(b,Y)$ modulo p is irreducible in $\mathbb{F}_p[Y]$.*

Proof. Here the general strategy applies with $N_{\mathcal{G}}=1$ and C_1 the conjugacy class of n-cycles. For p chosen as indicated, the method guarantees the existence of integers b such that $\Delta_P(b)\notin p\mathbb{Z}$ and the Frobenius of the splitting field of $P(b,Y)$ at p is an n-cycle. Due to the condition $\Delta_P(b)\notin p\mathbb{Z}$, this is equivalent to $P(b,Y)$ modulo p being irreducible in $\mathbb{F}_p[Y]$, whence the result. ∎

3.3.2. *General case* $\widehat{\mathbb{Q}}_P \supset \mathbb{Q}$. In this case, explicit information is needed on the primes that are totally split in the extension $\widehat{\mathbb{Q}}_P/\mathbb{Q}$. For this, one can use effective versions of the Chebotarev density theorem [LO77], [LMO79], [Ser81]. These results involve the order of the Galois group $\mathrm{Gal}(\widehat{\mathbb{Q}}_P/\mathbb{Q})$ and the discriminant $|d_{\widehat{\mathbb{Q}}_P}|$, and so lead to bounds depending on n, ρ and $|d_{\widehat{\mathbb{Q}}_P}|$. The parameter $|d_{\widehat{\mathbb{Q}}_P}|$ may however be hard to control. We offer an alternative approach leading to the following results.

COROLLARY 3.7. *Assume that $k = \mathbb{Q}$ and $\widehat{F}$ is the function field of a curve of genus $\widehat{g} \geq 2$. Then the Hilbert subset $\mathcal{H}_P$ contains a coset $a\mathbb{Z} + b$ with a and b smaller than some bound depending only on n, ρ and the set of bad primes of P.*

Proof. From Addendum 2.8, $\widehat{\mathbb{Q}}_P/\mathbb{Q}$ is one from the finite list of extensions of $\mathbb{Q}$ of degree $\leq |\mathrm{Nor}_{S_n}(\mathcal{G})|/|\mathcal{G}|$ and possibly ramified only at the bad primes of P. Therefore the first $N_{\mathcal{G}}$ primes satisfying condition $(*)$, and so the integers a and b from Theorem 3.1, can be bounded in terms n, ρ and the set of bad primes of P. ∎

When $0 \leq \widehat{g} \leq 1$, one can reduce to the situation $\widehat{g} \geq 2$, at the cost of losing the conclusion that $\mathcal{H}_P$ contains a whole coset.

COROLLARY 3.8. *Assume $k = \mathbb{Q}$. Let $\tau \in \mathbb{Z}$ be such that $\Delta_P(\tau) \neq 0$. Then the Hilbert subset $\mathcal{H}_P$ contains a positive integer t_0 smaller than some bound depending on n, ρ, the set of bad primes of P and the set of prime factors of $\Delta_P(\tau)$.*

Proof. We adjust a reduction argument given in [DW08, §5.1]. More specifically, it follows from [Dèb92, Lemma 0.1] and $\Delta_P(\tau) \neq 0$ that for every integer $h \geq 1$, the polynomial

$$P_h(T, Y) = P(T^h + \tau, Y)$$

is irreducible in $\overline{\mathbb{Q}}[T, Y]$. The Riemann–Hurwitz formula then shows that the genus g_h of the curve with affine equation $P(t^h + \tau, y) = 0$ satisfies

$$2g_h - 2 \geq -2n + h.$$

Thus for $h = 2n+2$, we obtain $g_h \geq 2$, and so is the genus $\widehat{g}_h$ of the splitting field of P_h since $\widehat{g}_h \geq g_h$. From Corollary 3.7, there exists $b \in \mathbb{Z}$ less than a bound depending only on $\deg_Y(P_h)$, $\deg(\Delta^{\mathrm{red}}_{P_h})$ and the set of bad primes of P_h such that

$$P_h(b, Y) = P(b^h + \tau, Y)$$

is irreducible in $\mathbb{Q}[Y]$. Clearly $\deg_Y(P_h) = \deg_Y(P) = n$, and it is easily checked that

$$\Delta^{\mathrm{red}}_{P_h}(T) = \Delta^{\mathrm{red}}_P(T^h + \tau).$$

From Remark 2.5, $\mathrm{disc}(\Delta_{P_h}^{\mathrm{red}})$ has the same set of prime divisors as the resultant of $\Delta_{P_h}^{\mathrm{red}}$ and of $(\Delta_{P_h}^{\mathrm{red}})'$. We have

$$\mathrm{res}(\Delta_{P_h}^{\mathrm{red}}, (\Delta_{P_h}^{\mathrm{red}})') = (\mathrm{res}(\Delta_P^{\mathrm{red}}, (\Delta_P^{\mathrm{red}})'))^h \cdot \Delta_P^{\mathrm{red}}(\tau).$$

We conclude that the bad primes of P_h consist of the bad primes of P and of the prime factors of $\Delta_P^{\mathrm{red}}(\tau)$. ∎

3.3.3. *Algorithmic remarks to find b.* Assume that $N_{\mathcal{G}}$ good primes $p_1, \ldots, p_{N_{\mathcal{G}}} \geq (\rho+1)^2|\mathcal{G}|^2$, totally split in $\widehat{\mathbb{Q}}_P/\mathbb{Q}$, have been found. From Theorem 3.1, for a the product of these primes, the Hilbert subset $\mathcal{H}_P$ contains a coset $a\mathbb{Z}+b$ for some integer $b \in [1, a]$.

(a) An obvious option to find an element $b \in \mathcal{H}_P$ is to test all polynomials $P(t, Y)$, $t = 1, \ldots, a$; there are efficient irreducibility algorithms for polynomials in one indeterminate. At least one of these polynomials $P(t, Y)$ is irreducible in $\mathbb{Q}[Y]$.

(b) When $\mathcal{G} = S_n$, Corollary 3.6 provides a simple algorithm to find an element of $\mathcal{H}_P$. This algorithm can be applied in the general context as a first step: for p chosen as indicated, if $P(b, Y)$ modulo p is irreducible in $\mathbb{F}_p[Y]$ for some $b \in \{1, \ldots, p\}$, then *a fortiori*, $P(b, Y)$ is irreducible in $\mathbb{Q}[Y]$; and if no polynomial $P(b, Y)$ modulo p is irreducible in $\mathbb{F}_p[Y]$ ($b \in \{1, \ldots, p\}$), then one should conclude that $\mathcal{G} \neq S_n$ and apply the method in a more refined way.

(c) In Corollary 3.6, the assumption that $\mathcal{G}$ contains an n-cycle made it simple to determine the integer b; it can be generalized to assume that

(∗∗) *the group $\mathcal{G}$ contains N elements $\omega_1, \ldots, \omega_N$ with the property that any N elements $g_1, \ldots, g_N \in S_n$ conjugate to $\omega_1, \ldots, \omega_N$ in S_n (respectively) generate a transitive subgroup of S_n.*

Assumption (∗∗) holds if $\mathcal{G}$ contains an n-cycle and in other situations. For example, the group $\mathcal{G}$ being transitive, it contains an element σ with no fixed points. Hence if $\mathcal{G}$ also contains an $(n-1)$-cycle (or more generally the product of an m-cycle and an $(n-m)$-cycle ($0 \leq m \leq n$) with supports non-stable under σ), then condition (∗∗) holds. However (∗∗) does not always hold: for example it does not if $\mathcal{G} \subset S_n$ is the regular representation and $\mathcal{G}$ is a non-cyclic p-group.

Under assumption (∗∗), pick N good primes $p_1, \ldots, p_N \geq (\rho+1)^2|\mathcal{G}|^2$, totally split in $\widehat{\mathbb{Q}}_P/\mathbb{Q}$, and $b_1, \ldots, b_N \in \mathbb{Z}$ such that $\Delta_P(b_i) \notin p_i\mathbb{Z}$ and the factorization type of $P(b_i, Y)$ modulo p_i is in the conjugacy class C_i of ω_i, $i = 1, \ldots, N$. The Frobenius $g_i \in \mathcal{G}$ of the splitting field of $P(b_i, Y)$ at p_i then lies in C_i, $i = 1, \ldots, N$. From (∗∗), $g_1, \ldots, g_N$ generate a transitive subgroup of S_n. We conclude that if b is an integer such that $b \equiv b_i \bmod p_i$, $i = 1, \ldots, N$, then $a\mathbb{Z}+b \subset \mathcal{H}_P$.

4. Families of polynomials. As in §3, k is a number field. Denote its ring of integers by R and consider the polynomial ring $A = R[X_1, \dots, X_s]$ in s new indeterminates $X_1, \dots, X_s$ over R. Set $X = X_1, \dots, X_s$ to simplify the notation; so $A = R[X]$.

Fix a polynomial $\mathcal{F}(X, T, Y) \in R[X, T, Y]$, irreducible in $\overline{k(X)}[T, Y]$ and monic in Y. Set $\deg_Y(\mathcal{F}) = n$ and $\deg_T(\mathcal{F}) = m$, assume $n \geq 1$ and let $\mathcal{G}$ be the *monodromy group* of $\mathcal{F}$, i.e. the Galois group of $\mathcal{F}(X, T, Y)$ over $\overline{k(X)}(T)$.

4.1. Qualitative statement of the main result. As for Theorem 3.1, we start with a qualitative statement and specify the parameters involved in a second stage.

THEOREM 4.1. *We produce below:*

- *a non-zero polynomial $\mathcal{B}_\mathcal{F} \in R[X]$,*
- *two integers N and C,*
- *a finite Galois extension L of $k(X)$,*

with the following property. For every $x \in R^s$ such that $\mathcal{B}_\mathcal{F}(x) \neq 0$,

(a) *the polynomial $\mathcal{F}(x, T, Y)$ is irreducible in $\overline{k}[T, Y]$,*

(b) *if $p_1, \dots, p_N$ are distinct prime numbers satisfying*

(∗) *$p_i \nmid N_{k/\mathbb{Q}}(\mathcal{B}_\mathcal{F}(x))$, $p_i \geq C$ and p_i is totally split in the residue field L_x of L at $X = x$, $i = 1, \dots, N$,*

and a is any multiple of $p_1 \cdots p_N$, then there exists $b \in \mathbb{Z}$ such that $\mathcal{F}(x, t, Y)$ is irreducible in $k[Y]$ for every t in the coset $a\mathbb{Z} + b$.

For every $x \in \overline{k}^s$, set

$$P_x(T, Y) = \mathcal{F}(x, T, Y).$$

From the Bertini–Noether theorem, for every $x \in R^s$ but in a proper Zariski closed subset $\mathcal{E}_\mathcal{F} \subset \mathbb{A}^s(\overline{k})$, the polynomial $\mathcal{F}(x, T, Y)$ is irreducible in $\overline{k}[T, Y]$. If $x \in R^s \setminus \mathcal{E}_\mathcal{F}$, Theorem 3.1 can be applied to the polynomial $P_x(T, Y) \in R[T, Y]$.

Consider the integers N_x, B_x, C_x and the finite extension $L_x/\mathbb{Q}$ that are given by Theorem 3.1. Our goal is to investigate to what extent they depend on x. Recall that N_x, B_x, C_x and L_x can be bounded in terms of $\deg_Y(P_x)$ and further parameters involving the discriminant relative to Y and the bad prime divisor of P_x. Note right away that the first one can be bounded independently of x: indeed, $\deg_Y(P_x) = \deg_Y(\mathcal{F}) = n$.

4.2. The Zariski closed subset $\mathcal{E}_\mathcal{F}$ and the polynomial $\mathcal{B}_\mathcal{F}$. Theorem 2.6 explicitly provides a proper Zariski closed subset $\mathcal{E}_\mathcal{F}$. Denote by $\mathcal{B}_\mathcal{F}$ the bad prime divisor of $\mathcal{F}(X, T, Y)$. It is a non-zero element of $R[X]$.

Furthermore one can bound $\deg(\mathcal{B}_{\mathcal{F}})$. Namely, it follows from

$$\begin{cases} \deg_T(\Delta_{\mathcal{F}}) \leq (2n-1)m, \\ \deg_X(\Delta_{\mathcal{F}}) \leq (2n-1)\deg_X(\mathcal{F}) \end{cases}$$

that

$$\begin{cases} \deg_T(\Delta_{\mathcal{F}}^{\mathrm{red}}) \leq (2n-1)m, \\ \deg_X(\Delta_{\mathcal{F}}^{\mathrm{red}}) \leq (2n-1)^2 m \deg_X(\mathcal{F}). \end{cases}$$

The first inequality is obvious as $\deg_T(\Delta_{\mathcal{F}}^{\mathrm{red}}) \leq \deg_T(\Delta_{\mathcal{F}})$. The second one follows from the inequality $\deg_X(\Delta_{\mathcal{F}}^{\mathrm{red}}) \leq \deg_T(\Delta_{\mathcal{F}})\deg_X(\Delta_{\mathcal{F}})$ (which is left as an exercise using Gauss' lemma and $\Delta_{\mathcal{F}}^{\mathrm{red}} \in R[X][T]$). The definition $\mathcal{B}_{\mathcal{F}} = \Delta_{\mathcal{F},0} \cdot \mathrm{disc}_T(\Delta_{\mathcal{F}}^{\mathrm{red}})$ then leads to

$$\begin{aligned} \deg(\mathcal{B}_{\mathcal{F}}) &\leq (2n-1)^2 m \deg_X(\mathcal{F}) + \big(2(2n-1)m - 1\big)(2n-1)^2 m \deg_X(\mathcal{F}) \\ &\leq 16n^3 m^2 \deg_X(\mathcal{F}). \end{aligned}$$

Denote the zero set of $\mathcal{B}_{\mathcal{F}}$ in $\overline{k}^s$ by $\mathcal{Z}(\mathcal{B}_{\mathcal{F}})$. Applying Theorem 2.6 to $\mathcal{F}(X,T,Y) \in A[T,Y]$ with $A = \overline{k}[X]$ and $\mathfrak{p} = \langle X - x \rangle \subset A$ with $x \in \overline{k}^s$ yields:

(∗) *If $x \notin \mathcal{Z}(\mathcal{B}_{\mathcal{F}})$, then $\mathcal{F}(x,T,Y) = P_x(T,Y)$ is irreducible in $\overline{k}[T,Y]$, of monodromy group $\mathcal{G}$, and we have*

$$\Delta_{P_x}^{\mathrm{red}} = \Delta_{\mathcal{F}}^{\mathrm{red}}(x), \qquad \mathcal{B}_{\mathcal{F}}(x) = \mathcal{B}_{P_x} \neq 0.$$

In particular, one can take $\mathcal{E}_{\mathcal{F}} = \mathcal{Z}(\mathcal{B}_{\mathcal{F}})$.

Fix $x \in R^s \setminus \mathcal{Z}(\mathcal{B}_{\mathcal{F}})$. We study below each of N_x, B_x, C_x, L_x.

4.3. The integer N_x. From Addendum 3.2, one can take

$$N_x = N_{\mathcal{G}}.$$

In particular, N_x can be bounded independently of x.

4.4. The integer B_x. From Addendum 3.2, one can take

$$B_x = N_{k/\mathbb{Q}}(\mathcal{B}_{P_x})$$

where $\mathcal{B}_{P_x}$ is the bad prime divisor of P_x considered in $R[T,Y]$. From Remark 2.5, it is the same if P_x is considered in $\overline{k}[T,Y]$. Use then (∗) above to conclude that the integer B_x can be taken to be

$$B_x = N_{k/\mathbb{Q}}(\mathcal{B}_{\mathcal{F}}(x)),$$

which is the norm of the value at x of the polynomial $\mathcal{B}_{\mathcal{F}} \in R[X]$ which depends only on the original polynomial $\mathcal{F}(X,T,Y)$.

4.5. The integer C_x. By construction, we have $\Delta_{\mathcal{F}}^{\mathrm{red}} \in R[X,T]$ and $\Delta_{P_x}^{\mathrm{red}} \in R[T]$, and from $(*)$ above, $\Delta_{P_x}^{\mathrm{red}} = \Delta_{\mathcal{F}}^{\mathrm{red}}(x)$. Denote by ρ the degree of these polynomials in T. From Addendum 3.2, one can take

$$C_x = (\rho+1)^2|\mathcal{G}|^2.$$

In particular C_x can be bounded independently of x.

4.6. The extension $L_x/\mathbb{Q}$. From Addendum 3.2, one can take

$$L_x = \widehat{k}_{P_x},$$

the constant extension in the splitting field of P_x over $k(T)$.

Consider the constant extension $\widehat{k}_{\mathcal{F}}/k(X)$ in the splitting field of $\mathcal{F}$ over $k(X,T)$. From Addendum 2.8, the field extension $\widehat{k}_{P_x}/k$ is contained in the residue extension, say $(\widehat{k}_{\mathcal{F}})_x/k$, of $\widehat{k}_{\mathcal{F}}/k(X)$ at some/any prime above the prime $X=x$ of $A=R[X]$. The conclusion of Theorem 2.6 holds *a fortiori* with $L_x = (\widehat{k}_{\mathcal{F}})_x$. Thus in Theorem 4.1 one can take

$$L = \widehat{k}_{\mathcal{F}}.$$

Furthermore, $L = k(X)$ and so $L_x = k$, under each of the two assumptions (a-1) and (a-2) from Addendum 2.8. We rewrite them in the family context:

(a-1) *$\mathcal{F}$ is irreducible in $\overline{k(X)}(T)[Y]$ and the splitting field of $\mathcal{F}$ over $k(X,T)$ is regular over $k(X)$,*
(a-2) $\mathcal{G} = S_n$.

In these cases, the condition from Theorem 4.1 that p_i be totally split in the extension $L_x/\mathbb{Q}$ reduces to p_i being totally split in $k/\mathbb{Q}$, $i=1,\dots,N$.

5. Proof of Theorem 2.6 and Addendum 2.8. We return to the general hypotheses of §2.3: A is a Dedekind domain with fraction field k, P in $A[T,Y]$ is a polynomial, monic and separable in Y, and $n = \deg_Y(P) \geq 1$. We freely use the notation introduced in §2.

Assume k is of characteristic 0 or greater than $\deg(\Delta_P)$. Let $\mathfrak{p} \subset A$ be a good prime of P (i.e. $\mathcal{B}_P = \Delta_{P,0} \cdot \mathrm{disc}(\Delta_P^{\mathrm{red}}) \notin \mathfrak{p}$) and such that $|\mathcal{G}| \notin \mathfrak{p}$.

5.1. Good Behaviour part. Consider the irreducible factorization

$$(**) \qquad \Delta_P = \delta \prod_{h=1}^{\ell} \mathcal{Q}_h^{\alpha_h}$$

of $\Delta_P \in A[T]$ in the unique factorization domain $A_{\mathfrak{p}}[T]$; $\delta \in A_{\mathfrak{p}} \setminus \{0\}$, $\mathcal{Q}_1,\dots,\mathcal{Q}_\ell$ are the distinct irreducible factors in $A_{\mathfrak{p}}[T] \setminus A_{\mathfrak{p}}$ and $\alpha_1,\dots,\alpha_\ell$

are positive integers. As $\Delta_{P,0}$ is invertible in $A_{\mathfrak{p}}$, so are δ and the leading coefficients of $\mathcal{Q}_1, \dots, \mathcal{Q}_\ell$. Hence one can take $\delta = \Delta_{P,0}$ and assume that $\mathcal{Q}_1, \dots, \mathcal{Q}_\ell$ are monic. We deduce that

$$\Delta_P^{\mathrm{red}} = (\Delta_{P,0})^\rho \prod_{h=1}^{\ell} \mathcal{Q}_h$$

where ρ is the number of distinct roots of Δ_P in $\overline{k}$. Mod out $(**)$ by $\mathfrak{p}$, and note that $s_{\mathfrak{p}}(\Delta_P) = \Delta_{s_{\mathfrak{p}}(P)}$ and that $s_{\mathfrak{p}}(\Delta_{P,0})$ is the leading term $\Delta_{s_{\mathfrak{p}}(P),0}$ of $\Delta_{s_{\mathfrak{p}}(P)}$ to conclude that $\Delta_{s_{\mathfrak{p}}(P)} \neq 0$ and

$$\Delta_{s_{\mathfrak{p}}(P)} = \Delta_{s_{\mathfrak{p}}(P),0} \prod_{h=1}^{\ell} s_{\mathfrak{p}}(\mathcal{Q}_h)^{\alpha_h}.$$

For $h = 1, \dots, \ell$, each polynomial $s_{\mathfrak{p}}(\mathcal{Q}_h)$ has only simple roots in $\overline{\kappa_{\mathfrak{p}}}$, and for distinct $h, h' \in \{1, \dots, \ell\}$, we have $s_{\mathfrak{p}}(\mathcal{Q}_h) \neq s_{\mathfrak{p}}(\mathcal{Q}_{h'})$: indeed, otherwise $\mathrm{disc}(s_{\mathfrak{p}}(\Delta_P^{\mathrm{red}})) = s_{\mathfrak{p}}(\mathrm{disc}(\Delta_P^{\mathrm{red}}))$ would be 0, contradicting $\mathrm{disc}(\Delta_P^{\mathrm{red}}) \notin \mathfrak{p}$. It follows that $s_{\mathfrak{p}}(P)$ satisfies condition $(*)$ from Lemma 2.1 and

$$\Delta_{s_{\mathfrak{p}}(P)}^{\mathrm{red}} = (\Delta_{s_{\mathfrak{p}}(P),0})^\rho \prod_{h=1}^{\ell} s_{\mathfrak{p}}(\mathcal{Q}_h) = s_{\mathfrak{p}}(\Delta_P^{\mathrm{red}}).$$

We conclude that $\mathrm{disc}(\Delta_{s_{\mathfrak{p}}(P)}^{\mathrm{red}}) = s_{\mathfrak{p}}(\mathrm{disc}(\Delta_P^{\mathrm{red}}))$ and $\mathcal{B}_{s_{\mathfrak{p}}(P)} = s_{\mathfrak{p}}(\mathcal{B}_P)$.

5.2. The Grothendieck good reduction theorem. We recall below the good reduction criterion for covers, due to Grothendieck, in the context where we will be using it: finite extensions of $k(T)$. For consistency we stick to the field extension terminology but indicate in footnotes the original geometric formulation.

Assume from now on that P is irreducible in $\overline{k}(T)[Y]$. Denote by $F/k(T)$ the function field extension associated with the polynomial $P \in k(T)[Y]$ ([8]). It is regular over k. Let $t_1, \dots, t_r \in \mathbb{P}^1(\overline{k})$ be the branch points of $F/k(T)$ (more exactly of $F\overline{k}/\overline{k}(T)$). Recall that $t_1, \dots, t_r$ are elements of the set $\{t_1, \dots, t_\rho, \infty\}$ with $t_1, \dots, t_\rho$ the distinct roots of Δ_P (but not all elements of this set are branch points in general).

Given a prime ideal $\mathfrak{p} \subset A$, denote the completion of A (resp. of k) at $\mathfrak{p}$ by $\widetilde{A}_{\mathfrak{p}}$ (resp. by $\widetilde{k}_{\mathfrak{p}}$), the algebraic closure of $\widetilde{k}_{\mathfrak{p}}$ by $C_{\mathfrak{p}}$ and fix an embedding $\overline{k} \subset C_{\mathfrak{p}}$.

Fix a prime ideal $\mathfrak{p} \subset A$ and let B be the integral closure of $\widetilde{A}_{\mathfrak{p}}[T]$ in the field $F\widetilde{k}_{\mathfrak{p}}$.

([8]) Geometrically, $F/k(T)$ corresponds to a branched cover $f : \mathcal{C} \to \mathbb{P}^1_k$.

GROTHENDIECK GOOD REDUCTION THEOREM. *Assume that:*

(a) $|\mathcal{G}| \notin \mathfrak{p}$,

(b) *there is no vertical ramification at* $\mathfrak{p}$ *in the extension* $F/k(T)$, *i.e.* B *is unramified over the prime* $\mathfrak{p}\widetilde{A}_{\mathfrak{p}}$ ([9]),

(c) *no two different branch points of* $F/k(T)$ *coincide modulo* $\mathfrak{p}$.

Then the extension $F/k(T)$ *has good reduction at* $\mathfrak{p}$, *that is,* $\mathfrak{p}B$ *is a prime ideal of* B *and the fraction field* ε *of* $B/\mathfrak{p}B$ *is a separable extension of* $\kappa_{\mathfrak{p}}(T)$ *and satisfies*

$$[\varepsilon : \kappa_{\mathfrak{p}}(T)] = [\overline{\kappa_{\mathfrak{p}}}\varepsilon : \overline{\kappa_{\mathfrak{p}}}(T)] = [F : k(T)] = \deg_Y(P) \text{ ([10])}.$$

This is a special case of the general result of Grothendieck on reduction of covers. We refer to [Gro71] and [GM71]. In our proof, we apply Grothendieck's theorem to both the extension $F/k(T)$ and its Galois closure. To this end, the following lemma is useful.

LEMMA 5.1. *Under the assumption* $|\mathcal{G}|\mathcal{B}_P \notin \mathfrak{p}$, *both the extension* $F/k(T)$ *and its Galois closure* $\widehat{F}/k(T)$ *satisfy conditions* (a)–(c) *of the Grothendieck good reduction theorem.*

Proof. Assume $|\mathcal{G}|\mathcal{B}_P \notin \mathfrak{p}$. Consider the extension $F/k(T)$. Grothendieck's assumption (a) obviously holds. Assumption (b) is guaranteed by $s_{\mathfrak{p}}(\Delta_P) \neq 0$ in $\kappa_{\mathfrak{p}}[T]$ (which follows from $s_{\mathfrak{p}}(\Delta_{P,0}) \neq 0$). Assumptions (a) and (c) then automatically hold for $\widehat{F}/k(T)$, which has the same monodromy group and the same branch points as $F/k(T)$. It remains to show assumption (b) for $\widehat{F}/k(T)$.

Let $\mathcal{Y}_1, \mathcal{Y}_2$ be two distinct roots of P in $\overline{k(T)}$. The discriminant Δ_P is in $A[T]$ and is the discriminant of $1, \mathcal{Y}_1, \ldots, \mathcal{Y}_1^{n-1}$. Let B_1 be the integral closure of $A[T]$ in $k(T, \mathcal{Y}_1)$, and $P_2 \in k(T, \mathcal{Y}_1)[Y]$ be the irreducible polynomial of $\mathcal{Y}_2$ over $k(T, \mathcal{Y}_1)$. The discriminant Δ_{P_2} of P_2 is in B_1 and is the discriminant of $1, \mathcal{Y}_2, \ldots, \mathcal{Y}_2^{n_2-1}$ for $n_2 = [k(T, \mathcal{Y}_1, \mathcal{Y}_2) : k(T, \mathcal{Y}_1)]$. The polynomial P_2 divides P in $B_1[Y]$. Consequently, Δ_{P_2} divides Δ_P in B_1, and its norm $N_1(\Delta_{P_2})$ relative to the extension $k(T, \mathcal{Y}_1)/k(T)$ divides Δ_P^n in $A[T]$. Consider the set $\{\mathcal{Y}_1^u \mathcal{Y}_2^v \mid 0 \leq u < n, 0 \leq v < n_2\}$. It is a $k(T)$-basis of $k(T, \mathcal{Y}_1, \mathcal{Y}_2)$ and its discriminant Δ_2, in $A[T]$, is a product of some power of Δ_P and some power of $N_1(\Delta_{P_2})$. Therefore, since the leading term of Δ_P is not in $\mathfrak{p}$, neither is the leading term of Δ_2. Repeat the argument on the extensions obtained by adjoining successively every root of P in $\overline{k(T)}$, and so eventually on the Galois extension $\widehat{F}/k(T)$. We finally obtain this conclusion:

([9]) Geometrically, the normalization $\tilde{f} : \widetilde{\mathcal{C}} \to \mathbb{P}^1_{\widetilde{A}_{\mathfrak{p}}}$ of $\mathbb{P}^1_{\widetilde{A}_{\mathfrak{p}}}$ in F is unramified over $\mathfrak{p}$.

([10]) Geometrically, if $\tilde{f}_0 : \widetilde{\mathcal{C}}_0 \to \mathbb{P}^1_{\kappa_{\mathfrak{p}}}$ is the special fiber of $\tilde{f}$, then $\tilde{f}_0$ is generically étale, $\widetilde{\mathcal{C}}_0$ is geometrically irreducible and $[\overline{\kappa_{\mathfrak{p}}}(\widetilde{\mathcal{C}}_0) : \overline{\kappa_{\mathfrak{p}}}(T)] = [F : k(T)]$.

(∗) *There exists a $k(T)$-basis of the extension $\widehat{F}/k(T)$ consisting of products of powers of the roots $\mathcal{Y}_1,\dots,\mathcal{Y}_n$ of P in $\overline{k(T)}$ such that the discriminant, a polynomial $\widehat{\Delta}$ in $A[T]$, has leading term not in the ideal $\mathfrak{p}$.*

This guarantees that there is no vertical ramification at $\mathfrak{p}$ in the extension $\widehat{F}/k(T)$. ∎

5.3. Proof of the GRT part of Theorem 2.6. That $s_\mathfrak{p}(P)$ is monic in Y is obvious and the separability follows from $\Delta_{s_\mathfrak{p}(P)} \neq 0$. For the rest of the proof, denote:

- by $\mathcal{Y}_1,\dots,\mathcal{Y}_n$ the roots of P in $\overline{k(T)}$, and assume that $\mathcal{Y}_1 \in F$,
- by $\widetilde{A}_\mathfrak{p}^{\widehat{k}_P\widetilde{k}_\mathfrak{p}}$ the integral closure of $\widetilde{A}_\mathfrak{p}$ in $\widehat{k}_P\widetilde{k}_\mathfrak{p}$,
- by $\widehat{B}$ the integral closure of $\widetilde{A}_\mathfrak{p}^{\widehat{k}_P\widetilde{k}_\mathfrak{p}}[T]$ in $\widehat{F}\widetilde{k}_\mathfrak{p}$,
- by $(\widehat{k}_P)_\mathfrak{p}/\kappa_\mathfrak{p}$ the residue extension of $\widehat{k}_P/k$ at some/any prime above $\mathfrak{p}$.

The reduction morphism

$$\widetilde{A}_\mathfrak{p}^{\widehat{k}_P\widetilde{k}_\mathfrak{p}}[T] \to (\widehat{k}_P)_\mathfrak{p}(T)$$

that extends the reduction map $\widetilde{A}_\mathfrak{p}^{\widehat{k}_P\widetilde{k}_\mathfrak{p}} \to (\widehat{k}_P)_\mathfrak{p}$ and sends T to itself can be extended to a morphism

$$s_\mathfrak{p} : \widehat{B} \to \overline{\kappa_\mathfrak{p}(T)} \quad \text{(e.g. [Dèb09, lemme 1.7.2])}.$$

From Grothendieck's theorem, $\mathfrak{p}B$ is a prime ideal of B and the fraction field ε of $B/\mathfrak{p}B$ is a separable extension of $\kappa_\mathfrak{p}(T)$. As P is monic, $\mathcal{Y}_1 \in B$ and one can further assume that $s_\mathfrak{p}(\mathcal{Y}_1)$ is the image of $\mathcal{Y}_1$ in

$$B/\mathfrak{p}B \subset \mathrm{Frac}(B/\mathfrak{p}B) \subset \overline{\kappa_\mathfrak{p}(T)}$$

($s_\mathfrak{p}(\mathcal{Y}_1)$ can be chosen to be any root of $s_\mathfrak{p}(P)$: see e.g. [Dèb09, §1.7.3]). Hence $s_\mathfrak{p}(\mathcal{Y}_1) \in \varepsilon$. The ring $\widetilde{A}_\mathfrak{p}[T]$ being integrally closed, we also have

$$\Delta_P B \subset \widetilde{A}_\mathfrak{p}[T] + \widetilde{A}_\mathfrak{p}[T]\mathcal{Y}_1 + \cdots + \widetilde{A}_\mathfrak{p}[T]\mathcal{Y}_1^{n-1},$$

which, together with $s_\mathfrak{p}(\Delta_P) \neq 0$ in $\kappa_\mathfrak{p}[T]$, leads to

$$\varepsilon = \mathrm{Frac}(\kappa_\mathfrak{p}[T, s_\mathfrak{p}(\mathcal{Y}_1)]).$$

As $s_\mathfrak{p}(\mathcal{Y}_1)$ is a root of $s_\mathfrak{p}(P)$ and from Grothendieck's theorem,

$$[\overline{\kappa_\mathfrak{p}}\varepsilon : \overline{\kappa_\mathfrak{p}}(T)] = \deg_Y(P) = \deg_Y(s_\mathfrak{p}(P)),$$

we conclude that the polynomial $s_\mathfrak{p}(P)$ is irreducible in $\overline{\kappa_\mathfrak{p}}[T, Y]$.

In a similar manner, using conclusion (∗) from the proof of Lemma 5.1, we obtain

$$\mathrm{Frac}(s_\mathfrak{p}(\widehat{B})) = \mathrm{Frac}\big((\widehat{k}_P)_\mathfrak{p}[T, s_\mathfrak{p}(\mathcal{Y}_1),\dots,s_\mathfrak{p}(\mathcal{Y}_n)]\big).$$

From Grothendieck's theorem applied to the extension $\widehat{F}/\widehat{k}_P(T)$ (which is regular over $\widehat{k}_P$), $\mathfrak{p}\widehat{B}$ is a prime ideal of $\widehat{B}$, the fraction field $\widehat{\varepsilon}$ of $\widehat{B}/\mathfrak{p}\widehat{B}$ is a separable extension of $(\widehat{k}_P)_\mathfrak{p}(T)$, and

$$[\widehat{\varepsilon}:(\widehat{k}_P)_\mathfrak{p}(T)]=[\overline{\kappa_\mathfrak{p}}\widehat{\varepsilon}:\overline{\kappa_\mathfrak{p}}(T)]=[\widehat{F}\overline{k}:\overline{k}(T)].$$

The extension $\widehat{F}/\widehat{k}_P(T)$ being Galois, the residue field extension above $\mathfrak{p}$ does not depend on the prime ideal above $\mathfrak{p}$. Hence $\mathrm{Frac}(s_\mathfrak{p}(\widehat{B}))=\widehat{\varepsilon}$.

Consequently, $\widehat{\varepsilon}$ is the splitting field of the polynomial $s_\mathfrak{p}(P)$ over $(\widehat{k}_P)_\mathfrak{p}$. The Galois group $\mathrm{Gal}(\overline{\kappa_\mathfrak{p}}\widehat{\varepsilon}/\overline{\kappa_\mathfrak{p}}(T))$ is by definition the monodromy group of $s_\mathfrak{p}(P)$. It is *a priori* a subgroup of $\mathcal{G}$, but is in fact all of $\mathcal{G}$, since its order is

$$[\overline{\kappa_\mathfrak{p}}\widehat{\varepsilon}:\overline{\kappa_\mathfrak{p}}(T)]=[\widehat{F}\overline{k}:\overline{k}(T)]=|\mathcal{G}|.$$

5.4. Proof of Addendum 2.8. (a) Item (a-1) follows from the definitions, and (a-2) from the fact that if $\mathcal{G}=S_n$, then necessarily $\mathcal{G}_\mathrm{a}$ is S_n too.

(b) From the equality

$$[\widehat{\varepsilon}:(\widehat{k}_P)_\mathfrak{p}(T)]=[\overline{\kappa_\mathfrak{p}}\widehat{\varepsilon}:\overline{\kappa_\mathfrak{p}}(T)]$$

shown above, the extension $\widehat{\varepsilon}/(\widehat{k}_P)_\mathfrak{p}(T)$ is regular over $(\widehat{k}_P)_\mathfrak{p}$. This implies that $(\widehat{k}_P)_\mathfrak{p}$ contains the constant extension in $\widehat{\varepsilon}/\kappa_\mathfrak{p}(T)$ (i.e. in the splitting field of $s_\mathfrak{p}(P)$ over $\kappa_\mathfrak{p}(T)$).

(c) Assume k is a number field. If $\mathfrak{p}$ is a good prime of P, then the extension $\widehat{F}/k(T)$ has good reduction at $\mathfrak{p}$. By a result of Deligne–Mumford [DM69, Theorem 1.3], the $\overline{k}$-automorphisms of the extension $\widehat{F}\overline{k}/\overline{k}(T)$ are already defined over the unramified closure $\widetilde{k}_\mathfrak{p}^\mathrm{ur}$ of $\widetilde{k}_\mathfrak{p}$. Hence the extension $\widehat{F}\widetilde{k}_\mathfrak{p}^\mathrm{ur}/\widetilde{k}_\mathfrak{p}^\mathrm{ur}(T)$ is Galois, which implies that $\widehat{k}_P\subset\widetilde{k}_\mathfrak{p}^\mathrm{ur}$. This shows that the ramified primes in $\widehat{k}_P/k$ are among the bad primes. Therefore $\widehat{k}_P/k$ is one from the finite list of extensions of k of degree $\le|\mathrm{Nor}_{S_n}(\mathcal{G})|/|\mathcal{G}|$ and unramified at each good prime of P.

5.5. Proof of the Chebotarev part of Theorem 2.6. Assume $\mathfrak{p}$ is good, not containing $|\mathcal{G}|$, of norm $N_{k/\mathbb{Q}}(\mathfrak{p})\ge(\rho+1)^2|\mathcal{G}|^2$ and totally split in the extension $\widehat{k}_P/k$. Let $\omega\in\mathcal{G}$ and let $E_\omega/\widetilde{k}_\mathfrak{p}$ be the unique unramified extension of Galois group $\langle\omega\rangle\subset\mathcal{G}$.

The result follows from [DG12, Proposition 2.2] applied to the Galois extension $\widehat{F}\widetilde{k}_\mathfrak{p}/\widetilde{k}_\mathfrak{p}(T)$ (viewed there as a G-cover) and the Galois extension $E_\omega/\widetilde{k}_\mathfrak{p}$. The base ring A there should be taken to be the ring $\widetilde{A}_\mathfrak{p}^{\widehat{k}_P\widetilde{k}_\mathfrak{p}}$ introduced in §5.3. The situation in [DG12] is that of a cover of a more general base space, of arbitrary dimension. We review the proof below, which becomes simpler for a cover of $\mathbb{P}^1$.

As $\mathfrak{p}$ is totally split in $\widehat{k}_P/k$, the fraction field of $\widehat{A}_{\mathfrak{p}}^{\widehat{k}_P\widetilde{k}_{\mathfrak{p}}}$ is $\widetilde{k}_{\mathfrak{p}}$ and its residue field is $\kappa_{\mathfrak{p}}$. Denote by p the characteristic of $\kappa_{\mathfrak{p}}$, and by q its order, which is also $N_{k/\mathbb{Q}}(\mathfrak{p})$.

An important tool of our approach is a certain "twisted" form, say $\widetilde{F}_{\mathfrak{p}}^{E_\omega}/\widetilde{k}_{\mathfrak{p}}(T)$, of $\widehat{F}\widetilde{k}_{\mathfrak{p}}/\widetilde{k}_{\mathfrak{p}}(T)$. This twisted extension is precisely defined in [DG12]. It is a $\widetilde{k}_{\mathfrak{p}}$-regular extension that is isomorphic to $\widehat{F}\widetilde{k}_{\mathfrak{p}}/\widetilde{k}_{\mathfrak{p}}(T)$ over the algebraic closure of $\widetilde{k}_{\mathfrak{p}}$ (but not over $\widetilde{k}_{\mathfrak{p}}$ itself, and so $\widetilde{F}_{\mathfrak{p}}^{E_\omega}/\widetilde{k}_{\mathfrak{p}}(T)$ need not be Galois). If $\widetilde{f}_{\mathfrak{p}}^{E_\omega} : \widetilde{X}_{\mathfrak{p}}^{E_\omega} \to \mathbb{P}^1_{\widetilde{k}_{\mathfrak{p}}}$ is the corresponding cover, then the main property of this twisted object is the following:

(∗) *For every $t_0 \in \mathbb{P}^1(\widetilde{k}_{\mathfrak{p}})$ that is not a branch point of $F/k(T)$, the specialized extension $(\widehat{F}\widetilde{k}_{\mathfrak{p}})_{t_0}/\widetilde{k}_{\mathfrak{p}}$ is $E_\omega/\widetilde{k}_{\mathfrak{p}}$ if and only if there is a $\widetilde{k}_{\mathfrak{p}}$-rational point x on $\widetilde{X}_{\mathfrak{p}}^{E_\omega}$ such that $\widetilde{f}_{\mathfrak{p}}^{E_\omega}(x) = t_0$.*

This is the so-called *twisting lemma* [DG12, Lemma 2.1]. When the two equivalent conditions of (∗) are satisfied, the Frobenius at $\mathfrak{p}$ of the specialized extension $\widehat{F}_{t_0}/\widehat{k}_P$ is conjugate to ω in $\mathcal{G}$. Thus the twisting lemma has reduced our problem to finding $\widetilde{k}_{\mathfrak{p}}$-rational points on $\widetilde{X}_{\mathfrak{p}}^{E_\omega}$.

The method consists then in finding $\kappa_{\mathfrak{p}}$-rational points on the $\kappa_{\mathfrak{p}}$-curve obtained by reducing $\widetilde{X}_{\mathfrak{p}}^{E_\omega}$ modulo $\mathfrak{p}$ and lifting them up to $\widetilde{k}_{\mathfrak{p}}$-rational points on $\widetilde{X}_{\mathfrak{p}}^{E_\omega}$ thanks to Hensel's lemma. Proposition 2.2 in [DG12] shows in a general context that this strategy indeed works under three hypotheses, which we explain below in our more specific context.

The first one is $p \nmid |\mathcal{G}|$; it is one of our assumptions.

The second one, which is labelled (good-red) in [DG12], is the conjunction of assumptions (b) and (c) of Grothendieck's theorem (§5.2); hence it is guaranteed by "$\mathfrak{p}$ good" (Lemma 5.1). The point of these two assumptions is that they guarantee that there is good reduction at $\mathfrak{p}$ for the extension $\widehat{F}\widetilde{k}_{\mathfrak{p}}/\widetilde{k}_{\mathfrak{p}}(T)$, but also, as the extension $E_\omega/\widetilde{k}_{\mathfrak{p}}$ is unramified, for the twisted extension $\widetilde{F}_{\mathfrak{p}}^{E_\omega}/\widetilde{k}_{\mathfrak{p}}(T)$.

There is a third hypothesis labelled (κ-big-enough) in [DG12, Prop. 2.2]. As is shown by [DG12, Lemma 2.4], it is guaranteed by the condition that q is suitably large. More specifically, assume (as we do here) that $q \geq (\rho+1)^2|\mathcal{G}|^2$. As justified below, this guarantees that any given $\kappa_{\mathfrak{p}}$-curve of genus $\leq \widehat{g}$ (the genus of the function field $\widehat{F}$ ([11])) has more than $(\rho+1)|\mathcal{G}|$ $\kappa_{\mathfrak{p}}$-rational points.

The justification rests on the standard Lang–Weil estimates and the following inequalities. Assume as we may that $|\mathcal{G}| > 1$ and set $\varrho = \rho + 1$ (to simplify notation). Then

$$\widehat{g} \leq \varrho|\mathcal{G}|/2 - 1 \quad \text{(Riemann–Hurwitz, Remark 3.3)}.$$

([11]) Which is also equal to the genus of $\widetilde{F}_{\mathfrak{p}}^{E_\omega}$.

In particular $\widehat{g} \le \varrho|\mathcal{G}|$, and so under the condition $q \ge \varrho^2|\mathcal{G}|^2$ we have

$$\begin{aligned} q+1-2\widehat{g}\sqrt{q} &\ge \varrho^2|\mathcal{G}|^2+1-2\widehat{g}\varrho|\mathcal{G}| \\ &\ge \varrho^2|\mathcal{G}|^2+1-2(\varrho|\mathcal{G}|/2-1)\varrho|\mathcal{G}| \\ &\ge 2\varrho|\mathcal{G}|+1>(\varrho+1)|\mathcal{G}|. \end{aligned}$$

Consequently, the cover of $\mathbb{P}^1_{\kappa_\mathfrak{p}}$ obtained by (good) reduction from the cover $\widetilde{f}_\mathfrak{p}^{E_\omega} : \widetilde{X}_\mathfrak{p}^{E_\omega} \to \mathbb{P}^1_{\widetilde{k}_\mathfrak{p}}$ has at least one $\kappa_\mathfrak{p}$-rational point on the covering curve that does not lie above any of the ρ classes modulo $\mathfrak{p}$ of the roots of Δ_P or above ∞.

This, together with Hensel's lemma (which makes it possible to lift this $\kappa_\mathfrak{p}$-rational point to a $\widetilde{k}_\mathfrak{p}$-rational point on $\widetilde{X}_\mathfrak{p}^{E_\omega}$) and the twisting lemma (recalled in $(*)$ above), leads to the conclusion that there is at least one coset $t_\mathfrak{p}+\mathfrak{p} \in A/\mathfrak{p}$, with $t_\mathfrak{p} \in A$ with the following property: if $t \in A_\mathfrak{p}$ satisfies $t \equiv t_\mathfrak{p} \bmod \mathfrak{p}$, then $\Delta_P(t) \ne 0$ and the Frobenius at $\mathfrak{p}$ of the specialization $(\widehat{F})_t/\widehat{k}_P$ of $\widehat{F}/\widehat{k}_P(T)$ at $T=t$ is conjugate to ω in $\mathcal{G}$. Recall finally that, as P is monic in Y and $\Delta_P(t) \ne 0$, the specialization $(\widehat{F})_t/\widehat{k}_P$ is the splitting field of $P(t,Y)$ over $\widehat{k}_P$ ([12]).

Acknowledgements. I wish to thank the anonymous referee for his/her thorough reading of the manuscript and my colleagues Arnaud Bodin and Salah Najib for the many valuable discussions about this work.

This work was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01).

References

[Dèb92] P. Dèbes, *On the irreducibility of the polynomials $P(t^m, Y)$*, J. Number Theory 42 (1992), 141–157.

[Dèb96] P. Dèbes, *Hilbert subsets and S-integral points*, Manuscripta Math. 89 (1996), 107–137.

[Dèb09] P. Dèbes, *Arithmétique des revêtements de la droite*, http://math.univ-lille1.fr/~pde/rev_www.pdf.

[DG12] P. Dèbes and N. Ghazi, *Galois covers and the Hilbert–Grunwald property*, Ann. Inst. Fourier (Grenoble) 62 (2012), 989–1013.

[DL12] P. Dèbes and F. Legrand, *Twisted covers and specializations*, in: Galois–Teichmueller Theory and Arithmetic Geometry, H. Nakamura et al. (eds.), Adv. Stud. Pure Math. 63, Math. Soc. Japan, Tokyo, 2012, 141–162.

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

([12]) We refer for example to [DL13, §2.1.4] for this standard point. Basically, $\widehat{F}_t/\widehat{k}$ is the compositum of the Galois closures of the extensions $E_j/\widehat{k}_P$ composing the specialization étale algebra of $F/\widehat{k}_P(T)$ at t, and as $\Delta_P(t) \ne 0$, the extensions $E_j/\widehat{k}_P$ correspond to the irreducible factors of $P(t,Y)$ in $\widehat{k}_P[Y]$.

[DW08] P. Dèbes and Y. Walkowiak, *Bounds for Hilbert's irreducibility theorem*, Pure Appl. Math. Quart. 4 (2008), 1059–1083.

[DM69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Publ. Math. IHES 36 (1969), 75–109.

[Eic39] M. Eichler, *Zum Hilbertschen Irreduzibilitätssatz*, Math. Ann. 116 (1939), 742–748.

[Eke90] T. Ekedahl, *An effective version of Hilbert's irreducibility theorem*, in: Séminaire de Théorie des Nombres (Paris, 1988/89), Progr. Math. 91, Birkhäuser, 1990, 241–248.

[Fri74] M. D. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory 6 (1974), 211–231.

[FJ04] M. D. Fried and M. Jarden, *Field Arithmetic*, 2nd ed., Ergeb. Math. Grenzgeb. 11, Springer, Berlin, 2004.

[Gro71] A. Grothendieck, *Revêtements étales et groupe fondamental*, Lecture Notes in Math. 224, Springer, 1971.

[GM71] A. Grothendieck and J. P. Murre, *The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme*, Lecture Notes in Math. 208, Springer, 1971.

[Jor72] C. Jordan, *Recherches sur les substitutions*, J. Liouville 17 (1872), 351–367.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. 54 (1979), 271–296.

[LO77] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev Density Theorem*, in: Algebraic Number Fields, A. Fröhlich (ed.), Academic Press, New York, 1977, 409–464.

[SZ95] A. Schinzel and U. Zannier, *The least admissible value of the parameter in Hilbert's irreducibility theorem*, Acta Arith. 69 (1995), 293–302.

[Ser81] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES 54 (1981), 323–401.

[Ser92] J.-P. Serre, *Topics in Galois Theory*, Res. Notes in Math., Jones and Bartlett, 1992.

[Wal05] Y. Walkowiak, *Théorème d'irréductibilité de Hilbert effectif*, Acta Arith. 116 (2005), 343–362.

[Yas87] M. Yasumoto, *Hilbert irreducibility sequences and nonstandard arithmetic*, J. Number Theory 26 (1987), 274–285.

[Zan97] U. Zannier, *On the reduction modulo p of an absolutely irreducible polynomial* $f(x, y)$, Arch. Math. (Basel) 68 (1997), 129–138.

Pierre Dèbes
Laboratoire Paul Painlevé
Mathématiques
Université de Lille
59655 Villeneuve d'Ascq Cedex, France
E-mail: Pierre.Debes@math.univ-lille1.fr