ON THE MALLE CONJECTURE AND THE SELF-TWISTED COVER

PIERRE DÈBES

ABSTRACT. For a large class of finite groups G, the number of Galois extensions $E/\mathbb{Q}$ of group G and discriminant $|d_E| \leq y$ is shown to grow at least like a power of y, for some specified positive exponent. The groups G are the regular Galois groups over $\mathbb{Q}$ and the counted extensions $E/\mathbb{Q}$ are obtained by specializing a given regular Galois extension $F/\mathbb{Q}(T)$. The extensions $E/\mathbb{Q}$ can further be prescribed any unramified local behavior at each suitably large prime $p \leq \log(y)/\delta$ for some $\delta \geq 1$. This result is a step toward the Malle conjecture on the number of Galois extensions of given group and bounded discriminant. The local conditions further make it a notable constraint on regular Galois groups over $\mathbb{Q}$. The method uses a new version of Hilbert's irreducibility theorem that counts the specialized extensions and not just the specialization points. A main tool for it is the self-twisted cover that we introduce.

1. MAIN RESULTS

Given a finite group G and a real number $y > 0$, there are only finitely many Galois extensions $E/\mathbb{Q}$ (inside a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$) of group G and discriminant $|d_E| \leq y$ (Hermite's theorem). Estimating their number $N(G, y)$ is a classical topic (§1.1). Here we consider the extensions $E/\mathbb{Q}$ obtained from a given $\mathbb{Q}$-regular[1] Galois extension $F/\mathbb{Q}(T)$ of group G by specializing the indeterminate T. We obtain estimates for the number of those which satisfy the above group and ramification conditions (theorem 1.1). Our lower bound (obviously also a lower bound for $N(G, y)$) already has the conjectural growth for $N(G, y)$: a power of y (§1.2). Furthermore the extensions $E/\mathbb{Q}$ we produce satisfy some additional local conditions at a finite – but growing with y – set of primes. This provides noteworthy constraints

Date: August 25, 2016.

2010 *Mathematics Subject Classification.* Primary 11R58, 12F12, 14H30, 12E25, 11R44, ; Secondary 14Gxx, 11Rxx, 12Fxx.

Key words and phrases. Galois extensions, inverse Galois theory, Malle conjecture, Grunwald problem, Tchebotarev theorem, covers, specialization, twisting.

[1] "$\mathbb{Q}$-regular" means that $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$.

(though unknown yet not to be non-vacuous) on the initial groups G, the *regular Galois groups over* $\mathbb{Q}$, related to analytic issues around the Tchebotarev theorem (§1.4). Our specialization method involves a new version of Hilbert's irreducibility theorem that counts not just the specialization points but the specialized extensions (theorem 1.3). The *self-twisted cover* comes in this part, as is explained in §1.3.

1.1. **The Malle conjecture** is a classical landmark in this context. It predicts that for some constant $a(G) \in]0,1]$, specifically defined by Malle (recalled in §4.1), and for all $\varepsilon > 0$,

$$(*) \qquad c_1(G)\, y^{a(G)} \leq N(G,y) \leq c_2(G,\varepsilon)\, y^{a(G)+\varepsilon} \quad \text{for all } y > y_0(G,\varepsilon)$$

for some positive constants $c_1(G)$, $c_2(G,\varepsilon)$ and $y_0(G,\varepsilon)$ [Mal02]. A more precise asymptotic for $N(G,y)$ (as $y \to \infty$) is even offered in [Mal04], namely $N(G,y) \sim c(G)\, y^{a(G)}\, (\log(y))^{b(G)}$, for some other specified constant $b(G) \geq 0$, and an another (unspecified) constant $c(G) > 0$.

The lower bound in (*) is a strong statement; it implies in particular that G is the Galois group of at least one extension $E/\mathbb{Q}$, which is an open question for many groups – the so-called *Inverse Galois Problem.* Relying on the Shafarevich theorem solving the IGP for solvable groups, Klüners and Malle proved the conjecture (*) for nilpotent groups [KM04]. Klüners also established the lower bound for dihedral groups of order $2p$ with p an odd prime [Klü06]. As to the more precise asymptotic for $N(G,y)$, it has only been proved for abelian groups [Wri89], [Mäk85], for S_3 [BF10] [BW08] and for generalized quaternion groups [Klü05b, ch.7, satz 7.6].[2]

1.2. **Statement of the main result.** Besides solvable groups, there is another classical class of finite groups known to be Galois groups over $\mathbb{Q}$: the *regular Galois groups* over $\mathbb{Q}$, *i.e.*, those groups G for which there is a $\mathbb{Q}$-regular Galois extension $F/\mathbb{Q}(T)$ of group G. In addition to abelian and dihedral groups, this class includes many non solvable groups, *e.g.* all symmetric and alternating groups and many simple groups. We obtain for all these groups a lower bound in y^α for $N(G,y)$ (with $\alpha > 0$), as predicted by the Malle estimate (*).

[2]We point out that there is a more general form of the conjecture for *not necessarily Galois extensions* $E/\mathbb{Q}$ for which there are further significant results, notably in the case the group (of the Galois closure) is S_n (with $n = [E:\mathbb{Q}]$): results of Davenport-Heilbronn [DH71] and Datskovsky-Wright [DW88] ($n=3$), Bhargava [Bha05], [Bha10] ($n = 4,5$), Ellenberg-Venkatesh [EV06] (upper bounds). There is also a counter-example to this more general form of the conjecture [Klü05a]. Finally there are quite interesting investigations on analogs of the problem over function fields of finite fields [EV05], [VE10], [EVW].

In addition to being of group G and discriminant $\leq y$, we can prescribe their local behavior at many primes to the Galois extensions $E/\mathbb{Q}$ that we produce. The following notation helps phrase these "local conditions". Given a finite group G, a finite set S of primes and for each $p \in S$, a non-empty union $\mathcal{F}_p \subset G$ of conjugacy classes of G, the collection $\mathcal{F} = (\mathcal{F}_p)_{p\in S}$ is called a *Frobenius data* for G on S. The number of Galois extensions $E/\mathbb{Q}$ of group G, of discriminant $|d_E| \leq y$ and which are unramified with Frobenius $\mathrm{Frob}_p(E/\mathbb{Q}) \in \mathcal{F}_p$ ($p \in S$) is denoted by $N(G, y, \mathcal{F})$.

The parameter $\delta(G)$ that appears below is the *minimal affine branching index* of $\mathbb{Q}$-regular realizations of G over $\mathbb{Q}$, that is, the minimal degree of the discriminant $\Delta_P(T)$ of a polynomial $P \in \mathbb{Q}[T, Y]$, monic in Y, that realizes G regularly over $\mathbb{Q}$ [3]; see §4.1 for more on $\delta(G)$.

Theorem 1.1. *Let G be a regular Galois group over $\mathbb{Q}$, non trivial. There is a constant $p_0(G) > 0$ with the following property. Fix $\delta > \delta(G)$ and consider the set $\mathcal{S}_y$ of primes in $[p_0(G), \log(y)/\delta]$. If y is suitably large (depending on G, δ), for every Frobenius data $\mathcal{F}_y$ on $\mathcal{S}_y$, we have*

$$N(G, y, \mathcal{F}_y) \geq y^{\alpha(G,\delta)} \qquad \textit{with} \;\; \alpha(G, \delta) = (1 - 1/|G|)/\delta.$$

Furthermore, the desired extensions $E/\mathbb{Q}$ can be obtained by specializing some $\mathbb{Q}$-regular realization $F/\mathbb{Q}(T)$ of G.

If $P \in \mathbb{Q}[T, Y]$, monic in Y, realizes G regularly over $\mathbb{Q}$, one can take $\delta = 2|G| \deg_T(P)$, or, more intrinsically, $\delta = 3r\,|G|^4 \log|G|$ with r the branch point number of the extension $F/\mathbb{Q}(T)$ (§4.1). Whence, for example, this simple lower bound for the Malle conjecture:

$$N(G, y) \geq y^{\frac{1-1/|G|}{2|G|\deg_T(P)}} \quad (\text{for } y \geq y_0(P))$$

To our knowledge, theorem 1.1 is a new step toward the Malle conjecture. Expectedly our exponent $\alpha(G, \delta)$ is smaller than its Malle counterpart $a(G)$[4]: our approach only takes into account those extensions which are specializations of a $\mathbb{Q}$-regular extension. Still it is interesting to already get the right growth for $N(G, y)$ from a single extension $F/\mathbb{Q}(T)$.

A more precise form of theorem 1.1 is stated in §4 (theorem 4.3) which starts from any given $\mathbb{Q}$-regular realization $F/\mathbb{Q}(T)$ of G and which shows other features of our result: ramification can also be prescribed at any finitely many suitably large primes under the assumption that $F/\mathbb{Q}(T)$ has at least one $\mathbb{Q}$-rational branch point; the exponent $\alpha(G, \delta)$ can be replaced by $1/\delta$ under Lang's conjecture and if the genus

[3] *i.e.* $F = \mathbb{Q}(T)[Y]/\langle P\rangle$ is a $\mathbb{Q}$-regular Galois extension of $\mathbb{Q}(T)$ of group G.

[4] A general proof of this is given in lemma 4.1, following a suggestion of G. Malle.

of F is ≥ 2; the Hilbert irreducibility aspect is expanded; and there is an upper bound part.

Remark 1.2. Theorem 1.1 (and theorem 4.3) will be extended to arbitrary number fields (instead of $\mathbb{Q}$) in a later work. As each finite group is known to be a regular Galois group over some suitably big number field, a consequence will be that the same is true for the lower bound part in the Malle conjecture: *given any finite group, there is a number field k_0 such that a lower bound like in* (*) *(appropriately generalized) holds over every number field containing k_0.*

1.3. **A "Hilbert-Malle theorem" and the self-twisted cover.** Our approach starts with a $\mathbb{Q}$-regular realization $F/\mathbb{Q}(T)$ of G. In this situation, Hilbert's irreducibility theorem classically produces "many" $t_0 \in \mathbb{Q}$ such that the specialized extensions $F_{t_0}/\mathbb{Q}$ are Galois of group G. Beyond making more precise these "many $t_0 \in \mathbb{Q}$" and controlling the corresponding discriminants, our goal requires a further step which is to show that many of these extensions are distinct.

A key tool of our method is the twisting lemma from [DG12], which reduces the search of specializations of a given type to that of rational points on a certain twisted cover. We use it twice, first over $\mathbb{Q}_p$ as in [DG12], to construct specializations $F_{t_0}/\mathbb{Q}$ with group G and with a specified local behavior. This stage rests on the Lang-Weil estimate for the number of rational points on a curve over a finite field. We obtain many good specialisations $t_0 \in \mathbb{Z}$ and a lower bound for their number.

The main ingredient for the final stage — showing that many of the extensions $F_{t_0}/\mathbb{Q}$ are distinct — is the following result which we extracted from our method and which may be interesting for its own sake. We call it a *"Hilbert-Malle theorem"*: beyond Hilbert's irreducibility theorem, it gives lower bounds not just for the number of good specialization points t_0 but for the corresponding specialized extensions $F_{t_0}/\mathbb{Q}$, in the spirit of the Malle conjecture.

Theorem 1.3. *There exist positive constants* E, C, γ *depending only on* $F/\mathbb{Q}(T)$ *with the following property. Suppose given an integer* $B \geq 1$ *and a subset* $\mathcal{H}_B \subset [1, B]$ *consisting of integers* t_0 *such that* $\mathrm{Gal}(F_{t_0}/\mathbb{Q})$ *is the whole group* G*. We have the following lower bounds for the number* $\mathcal{N}(\mathcal{H}_B)$ *of the corresponding specialized field extensions* $F_{t_0}/\mathbb{Q}$*:*

$$\begin{cases} \mathcal{N}(\mathcal{H}_B) \geq \dfrac{|\mathcal{H}_B| - \mathrm{E}}{B^{1/|G|}(\log B)^{\gamma}} & \textit{unconditionnally} \\ \\ \mathcal{N}(\mathcal{H}_B) \geq C\,(|\mathcal{H}_B| - \mathrm{E}) & \begin{array}{c}\textit{under Lang's conjecture and}\\ \textit{if the genus of } F \textit{ is} \geq 2\end{array} \end{cases}$$

To prove this result, first we reduce to counting integral points of a given size on certain twisted covers. This is our second use of the twisting lemma, over $\mathbb{Q}$ this time. For the count of the integral points, we use a result of Walkowiak [Wal05] based on a method of Heath-Brown [HB02]. We need to slightly improve Walkowiak's result to get the right exponent $\alpha(G, \delta)$ in theorem 1.1; see §3.4. More importantly we have to face the following difficulty: the bounds from [Wal05] involve the height of the defining polynomials, which here depend on the specializations $F_{t_0}/\mathbb{Q}$; we have to control the dependence in t_0. This is where enters the *self-twisted cover*, which as we will see, is a family of covers, depending only on the original extension $F/\mathbb{Q}(T)$ and which has all the twisted covers among its fibers. As a result, a bound of the form $c_1 t_0^{c_2}$ for the height of the polynomials above will follow with c_1 and c_2 depending only on $F/\mathbb{Q}(T)$.

1.4. **On the local conditions.** Regarding the local aspect, theorem 1.1 improves on a previous work, with N. Ghazi, about the Grunwald problem. From [DG12], if G is a regular Galois group over $\mathbb{Q}$, then every *unramified Grunwald problem* for G at some finite set $\mathcal{S}$ of primes $p \geq p_0(G)$ can be solved, *i.e.* every collection of unramified extensions $E^p/\mathbb{Q}_p$ of group $H_p \subset G$ ($p \in \mathcal{S}$) is induced by some Galois extension $E/\mathbb{Q}$ of group G. Theorem 1.1 does more: it provides, for every given discriminant size, a big number of such extensions $E/\mathbb{Q}$, a number that grows as in Malle's predictions.

Malle had suggested that his estimates should hold with some local conditions [Mal04, Remark 1.2]. However, unlike his, ours have a set of primes, $\mathcal{S}_y$, which grows with y. We focus below on this.

1.4.1. *Optimality of* $\mathcal{S}_y$. The set of primes where the local behavior can be prescribed as in theorem 1.1 cannot be expected to be much bigger than the set $\mathcal{S}_y$:

- indeed, that every possible Frobenius data on $\mathcal{S}_y$ occurs in at least one extension $E/\mathbb{Q}$ counted by $N(G, y)$ already gives $N(G, y) \geq c^{u(y)}$, with c the number of conjugacy classes of G and $u(y)$ the number of primes in $\mathcal{S}_y = \{p_0(G) < p \leq \log(y)/\delta\}$. Now $c^{u(y)}$ compares to the conjectural upper bounds for $N(G, y)$: $\log c^{u(y)} \sim \log(y)/\log(\log y)$ and $\log(y^{a(G)+\varepsilon}) \sim \log y$ (up to multiplicative constants).
- the restriction that the primes p be suitably large ($p > p_0(G)$) cannot be removed either as the famous Wang's counter-example shows [Wan69]: no Galois extension $E/\mathbb{Q}$ of group $\mathbb{Z}/8\mathbb{Z}$ is unramified at 2 with Frobenius of order 8. Other counter-examples with other primes than 2 have been recently produced by Neftin [Nef13].

1.4.2. *A further connection with the Tchebotarev density theorem.* The following definition helps explain the connection.

Definition 1.4. Given a real number $\ell \geq 0$, we say that a finite group G is of *Tchebotarev exponent* $\leq \ell$, which we write $\mathrm{tch}(G) \leq \ell$, if there exist real numbers $m, \delta > 0$ such that for every $x > m$ and every *Frobenius data* $\mathcal{F}_x = (\mathcal{F}_p)_{m<p\leq x}$ for G, there exists *at least one* Galois extension $E/\mathbb{Q}$ of group G such that these two conditions hold:
1. for each $m < p \leq x$, $E/\mathbb{Q}$ is unramified and $\mathrm{Frob}_p(E/\mathbb{Q}) \in \mathcal{F}_p$,
2. $\log|d_E| \leq \delta x^\ell$.

Fix $\delta > \delta(G)$ and m suitably large (in particular $m \geq p_0(G)$). Theorem 1.1 for $y = e^{\delta x}$ provides many[5] extensions $E/\mathbb{Q}$ satisfying conditions of definition 1.4 with $\ell = 1$.

Corollary 1.5. *If a finite group G is a regular Galois group over $\mathbb{Q}$, then* $\mathrm{tch}(G) \leq 1$.

On the other hand there is a universal lower bound for $\mathrm{tch}(G)$. Some famous estimates on the Tchebotarev theorem [LMO79] (see also [LO77], [Ser81]) show that, under the General Riemann Hypothesis, for every finite group G, we have

(**) $$\mathrm{tch}(G) > (1/2) - \varepsilon, \text{ for every } \varepsilon > 0.$$ [6]

(More precisely, they show that if a Galois extension $E/\mathbb{Q}$ is of group G and $\log|d_E| \leq x^{1/2}/\log x$, there are at least $\pi(x) - 2x/(|G|\log x)$ non totally split primes $p \leq x$ in $E/\mathbb{Q}$ (with $\pi(x)$ is the number of primes $p \leq x$). As $\pi(x) - 2x/(|G|\log x) \to +\infty$, the trivial totally split behavior — $\mathcal{F}_p = \{1\}$ for each $m < p \leq x$ — does not occur if $x \gg 1$).

1.4.3. *Prospective comments.* Corollary 1.5 raises the question of whether $\mathrm{tch}(G) > 1$ for some group G, in which case G could not be a regular Galois group over $\mathbb{Q}$. Such a group may not exist (if the so-called Regular Inverse Galois Problem is true), while at the other extreme it cannot be ruled out at the moment that $\mathrm{tch}(G) = \infty$ for some group G. Many possibilities exist in between for Galois groups G over $\mathbb{Q}$: that realizations exist that satisfy the local conditions of definition 1.4 (1) or not, that the corresponding discriminants can be bounded as in definition 1.4 (2), for some $\ell \in [1/2, \infty[$ or not. Somehow

[5] at least $e^{\gamma x}$ with $\gamma = 1 - 1/|G|$ (for $x \gg 1$).

[6] [LMO79] also has an unconditional conclusion, which, using our terminology, leads to $\mathrm{tch}(G) \geq (\log\log x)/(2\log x)$ (with definition 1.4 extended to allow ℓ to be a function of x).

the Tchebotarev exponent provides a measure of the gap (possibly empty) between the *classical* and *regular* Inverse Galois Problems.

Gaining information on Tchebotarev exponents however seems difficult. Even for $G = \mathbb{Z}/2\mathbb{Z}$ and the case of the totally split behavior, for which the problem amounts to bounding the least square-free integer $d_m(x)$ that is a quadratic residue modulo each prime $m < p \leq x$. Changing 1/2 to 1 in (**), the remaining possible improvement (as $\mathbb{Z}/2\mathbb{Z}$ is a regular Galois group over $\mathbb{Q}$), is plausible as some easy heuristics show but relates to deep questions in number theory (*e.g.* [Ser81, §2.5]).

Acknowledgement. I am grateful to J. Klüners and G. Malle for their interest in the paper and some valuable comments. In particular the proof of lemma 4.1 (b) follows a suggestion of G. Malle.

The paper is organized as follows. §2 gives the construction of the self-twisted cover and §3 the proof of theorem 1.3. In §4 we state theorem 4.3 and deduce theorem 1.1. §5 proves theorem 4.3.

The following terminology is used throughout the paper.

Given a field k of characteristic 0, an extension $F/k(T)$ is said to be *k-regular* if $F \cap \overline{k} = k$. A *(regular) k-cover of* $\mathbb{P}^1$ is a finite and generically unramified morphism $f : X \to \mathbb{P}^1$ defined over k with X a normal and geometrically irreducible variety.

We work without distinction with a k-regular extension $F/k(T)$ or with the associated k-cover $f : X \to \mathbb{P}^1$: f is the normalization of $\mathbb{P}^1_k$ in F and F is the function field $k(X)$ of X. We also work with *affine models*: by this we mean the irreducible polynomial $P(T, Y)$ of some primitive element of $F/k(T)$. The k-cover $f : X \to \mathbb{P}^1$ is said to be *Galois* if the field extension $k(X)/k(T)$ is Galois; if in addition $f : X \to \mathbb{P}^1$ is given together with an isomorphism $G \to \mathrm{Gal}(k(X)/k(T))$, it is called a (regular) k-G-*Galois cover* of group G.

By *group* and *branch point set* of a k-cover f, we mean those of the $\overline{k}$-cover $f \otimes_k \overline{k}$: the group of a $\overline{k}$-cover $X \to \mathbb{P}^1$ is the Galois group of the Galois closure of the extension $\overline{k}(X)/\overline{k}(T)$. The branch point set of $f \otimes_k \overline{k}$ is the (finite) set of points $t \in \mathbb{P}^1(\overline{k})$ such that the associated discrete valuations are ramified in the extension $\overline{k}(X)/\overline{k}(T)$.

Given a k-regular Galois extension $F/k(T)$ and $t_0 \in \mathbb{P}^1(k)$, the *specialization of $F/\mathbb{Q}(T)$ at t_0* is the residue extension of an (arbitrary) prime above $\langle T - t_0 \rangle$ in the integral closure of $\mathbb{Q}[T]_{\langle T-t_0 \rangle}$ in F (as usual use $\mathbb{Q}[1/T]_{\langle 1/T \rangle}$ instead if $t_0 = \infty$). We denote it by F_{t_0}/k.

2. The self-twisted cover

In §2.1, we recall the twisting operation on covers and the twisting lemma (§2.1.2). §2.2.1 explains the motivation for introducing the self-twisted cover while the rest of §2.2 is devoted to its construction. Covers are viewed here as fundamental group representations. The correspondence is briefly recalled in §2.1.1.

2.1. **Twisting G-Galois covers.** For this subsection, we refer to [DG12].

2.1.1. *Fundamental groups representations of covers.* Given a field k, denote its absolute Galois group by G_k. If E/k is a Galois extension of group G, an epimorphism $\varphi : \mathrm{G}_k \to G$ such that E is the fixed field of $\ker(\varphi)$ in $\overline{k}$ is a called a G_k*-representation* of E/k.

Given a finite subset $\mathbf{t} \subset \mathbb{P}^1(\overline{k})$ invariant under G_k, the k-fundamental group of $\mathbb{P}^1 \setminus \mathbf{t}$ is denoted by $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k$; here t denotes the fixed *base point*, which corresponds to choosing an embedding of $k(T)$ in an algebraically closed field Ω. The $\overline{k}$-fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k}}$ is defined as the Galois group of the maximal algebraic extension $\Omega_{\mathbf{t},k}/\overline{k}(T)$ (inside Ω) unramified above $\mathbb{P}^1 \setminus \mathbf{t}$ and the k-fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k$ as the group of the Galois extension $\Omega_{\mathbf{t},k}/k(T)$.

Degree d k-covers of $\mathbb{P}^1$ (resp. k-G-Galois covers of $\mathbb{P}^1$ of group G) with branch points in $\mathbf{t}$ correspond to transitive homomorphisms $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to S_d$ (resp. to epimorphisms $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_k, t) \to G$), with the extra regularity condition that the restriction of ϕ to $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_k, t)_{\overline{k}}$ remains transitive (resp. remains onto). These corresponding homomorphisms are called the *fundamental group representations* (or π_1-*representations* for short) of the cover f (resp the G-cover f).

Each k-rational point $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$ provides a section $\mathsf{s}_{t_0} : \mathrm{G}_k \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k$ to the exact sequence

$$1 \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to \mathrm{G}_k \to 1$$

which is uniquely defined up to conjugation by an element in the fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k}}$.

If $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to G$ represents a k-G-Galois cover $f : X \to \mathbb{P}^1$, the morphism $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to G$ is the *specialization representation* of ϕ at t_0. The fixed field in $\overline{k}$ of $\ker(\phi \circ \mathsf{s}_{t_0})$ is the specialization $k(X)_{t_0}/k(T)$ of $k(X)/k(T)$ at t_0.

2.1.2. *The twisting lemma.* Fix a regular k-G-Galois cover $f : X \to \mathbb{P}^1$ of group G. We recall how it can be twisted by some Galois extension E/k of group $H \subset G$. Formally this is done in terms of the associated π_1- and G_k- representations.

Let $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to G$ be a π_1-representation of the regular k-G-cover $f : X \to \mathbb{P}^1$ and $\varphi : \mathrm{G}_k \to G$ be a G_k-representation of the Galois extension E/k.

Denote the right-regular (resp. left-regular) representation of G by $\delta : G \to S_d$ (resp. by $\gamma : G \to S_d$) where $d = |G|$. Define $\varphi^* : \mathrm{G}_k \to G$ by $\varphi^*(g) = \varphi(g)^{-1}$. Consider the map $\widetilde{\phi}^\varphi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to S_d$ defined by the following formula, where r is the restriction map $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to \mathrm{G}_k$ and $\times$ is the multiplication in the symmetric group S_d:

$$\widetilde{\phi}^\varphi(\theta) = \gamma\phi(\theta) \times \delta\varphi^* r(\theta) \qquad (\theta \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k).$$

The map $\widetilde{\phi}^\varphi$ is a group homomorphism with the same restriction on $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k}}$ as ϕ. It is called the *twisted representation* of ϕ by φ. The associated regular k-cover is a k-model of the cover $f \otimes_k \overline{k}$. It is denoted by $\widetilde{f}^\varphi : \widetilde{X}^\varphi \to \mathbb{P}^1$ and called the *twisted cover* of f by φ. The following statement is the main property of the twisted cover.

Twisting lemma 2.1. *Let $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$. Then the specialization representation $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to G$ is conjugate in G to $\varphi : \mathrm{G}_k \to G$ if and only if there exists $x_0 \in \widetilde{X}^\varphi(k)$ such that $\widetilde{f}^\varphi(x_0) = t_0$.*

2.2. **The self-twisted cover.**

2.2.1. *The motivation for the self-twisted cover.* As explained in §1.3, we will have to control the height of some polynomials defining some twisted covers. These twisted covers are obtained by twisting the given G-Galois cover $f : X \to \mathbb{P}^1$ by its own specializations $k(X)_{u_0}/k$ ($u_0 \in k$); we call them the *fiber-twisted covers*. §2.2 shows that the fiber-twisted covers are all members of an algebraic family of covers: the *self-twisted cover*. The practical use for the end of the paper is the following result. It is a consequence of lemma 2.4.

Theorem 2.2. *Given the regular k-G-cover $f : X \to \mathbb{P}^1$, there exists a polynomial $\widetilde{P}(U,T,Y) \in k[U,T,Y]$ irreducible in $\overline{k(U)}(T)[Y]$, monic in Y, and a finite set $\mathcal{E} \subset k$ such that for every $u_0 \in k \setminus \mathcal{E}$,*
(a) *$\widetilde{P}(u_0,T,Y)$ is irreducible in $\overline{k}(T)[Y]$,*
(b) *$\widetilde{P}(u_0,T,Y)$ is an affine model of the fiber-twisted cover of f at u_0,*
(c) *the genus of the curve $\widetilde{P}(u_0,t,y) = 0$ equals the genus g_X of X.*

2.2.2. *The construction data.* Fix a regular k-G-Galois cover $f : X \to \mathbb{P}^1$ of group G and let $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to G$ be a π_1-representation. Let U be a new indeterminate (algebraically independent from T and Y). Fix an algebraically closed field Ω containing $k(T,U)$, which we will use as a common base point t for all fundamental groups involved. The algebraic closures of $k(T,U)$, $k(T)$, $k(U)$ and k should be understood as the ones inside Ω.

2.2.3. *A π_1-representation of $f\otimes_k k(U)$.* As the compositum $\Omega_{\mathbf{t},k}\cdot\overline{k(U)}$ is contained in $\Omega_{\mathbf{t},k(U)}$, there is a restriction morphism

$$\mathrm{res}_{k(U)/k}:\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{k(U)}\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_k,$$

which induces a map between the geometric parts of the fundamental groups:

$$\mathrm{res}_{\overline{k(U)}/\overline{k}}:\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k(U)}}\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k}}$$

We also use the notation $\mathrm{res}_{\overline{k(U)}/\overline{k}}$ for the map $\mathrm{G}_{k(U)}\to\mathrm{G}_k$ induced on the absolute Galois groups.

Lemma 2.3. $\mathrm{res}_{k(U)/k}:\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{k(U)}\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_k$ *is surjective and* $\mathrm{res}_{\overline{k(U)}/\overline{k}}:\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k(U)}}\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k}}$ *is an isomorphism.*

Proof. Every $\sigma\in\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_k$ extends to an element of $\mathrm{G}_{k(T)}$, which extends naturally to an automorphism of $\overline{k(T)}(U)$ fixing U (and $k(T)$), which in turn extends to an element $\tilde{\sigma}\in\mathrm{G}_{k(T,U)}$. As $\mathbf{t}$ is G_k-invariant, $\tilde{\sigma}$ permutes the extensions $F/k(U)(T)$ that are unramified above $\mathbb{P}^1\setminus\mathbf{t}$. Conclude that $\tilde{\sigma}$ factors through $\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{k(U)}$ to provide a preimage of σ *via* the map $\mathrm{res}_{k(U)/k}$, as desired in the first statement.

To show that $\mathrm{res}_{\overline{k(U)}/\overline{k}}:\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k(U)}}\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k}}$ is surjective, it suffices to show that the following morphism is:

$$\mathrm{Gal}(\Omega_{\mathbf{t},k}\cdot\overline{k(U)}/\overline{k(U)}(T))\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k}}=\mathrm{Gal}(\Omega_{\mathbf{t},k}/\overline{k}(T)).$$

This morphism is in fact an isomorphism: indeed extending the base field from $\overline{k}$ to $\overline{k(U)}$ (over which T is transcendental) does not change the group of k-regular Galois extensions.

As k is of characteristic 0, the morphism $\mathrm{res}_{\overline{k(U)}/\overline{k}}:\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k(U)}}\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{\overline{k}}$ is even an isomorphism. More precisely, it follows from [Ser92, theorem 6.3.3] that $\Omega_{\mathbf{t},k(U)}=\Omega_{\mathbf{t},k}\cdot\overline{k(U)}$. □

Set $\phi\otimes_k k(U)=\phi\circ\mathrm{res}_{k(U)/k}$. The epimorphism

$$\phi\otimes_k k(U):\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{k(U)}\to G$$

is a π_1-representation of the regular G-Galois cover $f\otimes_k k(U)$.

2.2.4. *A $\mathrm{G}_{k(U)}$-representation.* Composing $\phi\otimes_k k(U)$ with the section $\mathsf{s}_U:\mathrm{G}_{k(U)}\to\pi_1(\mathbb{P}^1\setminus\mathbf{t},t)_{k(U)}$ associated with the point $U\in\mathbb{P}^1(k(U))$ provides a $\mathrm{G}_{k(U)}$-representation

$$\phi_U:\mathrm{G}_{k(U)}\to G$$

which is the specialization representation of $\phi \otimes_k k(U)$ at $t = U$. It corresponds to the generic fiber of $F/k(T)$. Denote it by $F_U/k(U)$.

2.2.5. *The self-twisted cover.* Twist the representation $\phi \otimes_k k(U)$ by the epimorphism ϕ_U to get the *self-twisted representation*

$$\widetilde{\phi \otimes_k k(U)}^{\phi_U} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{k(U)} \to S_d.$$

We call the corresponding cover

$$\widetilde{f \otimes_k k(U)}^{\phi_U} : \widetilde{X \otimes_k k(U)}^{\phi_U} \to \mathbb{P}^1_{k(U)}$$

the *self-twisted cover* of f.

2.2.6. *The fiber-twisted cover at t_0.* Let $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$. Twist the representation ϕ by the specialization representation $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_k \to G$ to get the twisted representation

$$\widetilde{\phi}^{\phi \mathsf{s}_{t_0}} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k \to S_d$$

which corresponds to a cover

$$\widetilde{f}^{\phi \mathsf{s}_{t_0}} : \widetilde{X}^{\phi \mathsf{s}_{t_0}} \to \mathbb{P}^1_k.$$

We call them respectively the *fiber-twisted representation* and the *fiber-twisted cover* at t_0.

2.2.7. *Description of the self-twisted cover.* Set $\Psi_U = \widetilde{\phi \otimes_k k(U)}^{\phi_U}$. From §2.1.2, for every $\Theta \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{k(U)}$, we have

$$\Psi_U(\Theta) = \gamma((\phi \otimes_k k(U))(\Theta)) \times \delta(\phi_U(R(\Theta))^{-1})$$

where $R : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{k(U)} \to \mathrm{G}_{k(U)}$ is the natural surjection. The element Θ uniquely writes $\Theta = \chi\, \mathsf{s}_U(\sigma)$ with $\chi \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k(U)}}$ and $\sigma \in \mathrm{G}_{k(U)}$. Whence

$$(\phi \otimes_k k(U))(\Theta)) = (\phi \otimes_k k(U))(\chi)\, (\phi \otimes_k k(U))(\mathsf{s}_U(\sigma))$$

and, using that $\phi_U = \phi \otimes_k k(U) \circ \mathsf{s}_U$,

$$\phi_U(R(\Theta)) = (\phi \otimes_k k(U))(\mathsf{s}_U(\sigma)).$$

Finally we obtain the following formula, where, by $\mathrm{conj}(g)$ ($g \in G$), we denote the permutation of G induced by the conjugation $x \to gxg^{-1}$:

$$\Psi_U(\Theta) = \gamma((\phi \otimes_k k(U))(\chi)) \times \mathrm{conj}((\phi \otimes_k k(U))(\mathsf{s}_U(\sigma))).$$

Denote the field extension corresponding to the π_1-representation Ψ_U by $\widetilde{Fk(U)}^{\phi_U}/k(U)(T)$. The field $\widetilde{Fk(U)}^{\phi_U}$ is the fixed field in $\Omega_{\mathbf{t},k(U)}$ of the subgroup $\Gamma_U \subset \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{k(U)}$ of all elements Θ such that $\Psi_U(\Theta)$ fixes the neutral element of G [7]. We obtain

$$\Gamma_U = \ker(\phi \otimes_k k(U)) \cdot \mathsf{s}_U(\mathrm{G}_{k(U)})$$

and $\widetilde{Fk(U)}^{\phi_U}$ is the fixed field in $F\overline{k(U)}$ of all elements in $\mathsf{s}_U(\mathrm{G}_{k(U)})$.

2.2.8. *Description of the fiber-twisted covers.* Let $t_0 \in \mathbb{P}^1(k) \setminus \mathbf{t}$ and set $\phi_{t_0} = \phi \circ \mathsf{s}_{t_0}$ and $\Psi_{t_0} = \widetilde{\phi}^{\phi_{t_0}}$. Every element $\theta \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k$ uniquely writes $\theta = x\,\mathsf{s}_{t_0}(\tau)$ with $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k}}$ and $\tau \in \mathrm{G}_k$. Proceeding exactly as above but with U replaced by t_0, $\phi \otimes_k k(U)$ by ϕ and $\Theta = \chi\,\mathsf{s}_U(\sigma)$ by $\theta = x\,\mathsf{s}_{t_0}(\tau)$, we obtain that

$$\Psi_{t_0}(\theta) = \gamma(\phi(x)) \times \mathrm{conj}(\phi(\mathsf{s}_{t_0}(\tau)))$$

and if $\widetilde{F}^{\phi_{t_0}}/k(T)$ is the field extension corresponding to the π_1-representation Ψ_{t_0}, $\widetilde{F}^{\phi_{t_0}}$ is the fixed field in $F\overline{k}$ of all elements in $\mathsf{s}_{t_0}(\mathrm{G}_k)$.

2.2.9. *Comparison.*

Lemma 2.4. *There is a finite subset $\mathcal{E} \subset k$ such that for each $t_0 \in k \setminus \mathcal{E}$, the fiber-twisted cover $\widetilde{f}^{\phi\mathsf{s}_{t_0}} : \widetilde{X}^{\phi\mathsf{s}_{t_0}} \to \mathbb{P}^1_k$ is k-isomorphic to the specialization of the self-twisted cover $f\,\widetilde{\otimes_k k(U)}^{\phi_U} : X\,\widetilde{\otimes_k k(U)}^{\phi_U} \to \mathbb{P}^1_{k(U)}$ at $U = t_0$.*

Proof. Set $d = |G|$ and $\mathcal{L}_U = \widetilde{Fk(U)}^{F_U}$. By construction, the extension $\mathcal{L}_U/k(U)(T)$ is $k(U)$-regular. From the Bertini-Noether theorem, for every $t_0 \in k$ but in a finite subset $\mathcal{E}$, which we enlarge to contain the branch point set $\mathbf{t}$, the extension $\mathcal{L}_U/k(U)(T)$ specializes at $U = t_0$ to some extension $\mathcal{L}_{t_0}/k(T)$ that is k-regular of degree

$$[\widetilde{Fk(U)}^{F_U} : k(U)(T)] = [Fk(U) : k(U)(T)] = [F : k(T)] = d.$$

Up to enlarging again $\mathcal{E}$, one may also assume that the genus of this specialization is the same as the genus of the function field $\widetilde{Fk(U)}$, which equals the genus of F (or of X). The rest of the proof shows that the specialization $\mathcal{L}_{t_0}/k(T)$ is the extension $\widetilde{F}^{F_{t_0}}/k(T)$.

Pick primitive elements $\mathcal{Y}$ and $\widetilde{\mathcal{Y}}_U$ of the two extensions $F/k(T)$ and $\mathcal{L}_U/k(U)(T)$, integral over $k[T]$ and $k[U,T]$ respectively. As $\mathcal{L}_U \subset F\overline{k(U)}$, one can write

$$\widetilde{\mathcal{Y}}_U = \sum_{i=0}^{d-1} a_i(U)\mathcal{Y}^i$$

[7]Taking any other element of G gives the same field up to $k(U)(T)$-isomorphism.

with $a_0(U),\ldots,a_{d-1}(U) \in \overline{k(U)}$. Enlarge the set $\mathcal{E}$ to contain the points $t\in k$ for which $a_0(U),\ldots,a_{d-1}(U)$ do not specialize at $U=t$. Fix $t_0 \in k\setminus\mathcal{E}$. Consider the specialization $\widetilde{\mathcal{Y}}_{t_0} = \sum_{i=0}^{d-1} a_i(t_0)\mathcal{Y}^i$. The associated extension $k(T,\widetilde{\mathcal{Y}}_{t_0})/k(T)$ is the specialization $\mathcal{L}_{t_0}/k(T)$ of $\mathcal{L}_U/k(U)(T)$ at $U=t_0$. By construction $\widetilde{\mathcal{Y}}_{t_0}\in F\overline{k}$. The last paragraph of the proof below shows that $\widetilde{\mathcal{Y}}_{t_0}$ is fixed by all elements in $\mathsf{s}_{t_0}(\mathrm{G}_k)$. We will then be able to conclude that $k(T,\widetilde{\mathcal{Y}}_{t_0})\subset \widetilde{F}^{\phi_{t_0}}$ and finally that these two fields are equal since $[k(T,\widetilde{\mathcal{Y}}_{t_0}):k(T)] = [\widetilde{F}^{\phi_{t_0}}:k(T)] = d$.

As $U\notin \mathbf{t}$, there exists an embedding

$$\mathcal{L}_U \to \overline{k(U)}((T-U))$$

which maps $\mathcal{Y}_U$ to a formal power series

$$\widetilde{\mathcal{Y}}_U = \sum_{n=0}^{\infty} b_n(U)(T-U)^n \quad \text{with } b_n(U)\in\overline{k(U)}\ (n\geq 0).$$

Furthermore, $\mathcal{L}_U$ is fixed by all elements $\mathsf{s}_U(\sigma)\in\mathsf{s}_U(\mathrm{G}_{k(U)})$, which, by definition of s_U, act *via* the action of $\sigma\in\mathrm{G}_{k(U)}$ on the coefficients $b_n(U)$; conclude that $b_n(U)\in k(U)$ $(n\geq 0)$. Finally from the Eisenstein theorem[8], there exists a polynomial $E(U)\in k[U]$ such that $E(U)^{n+1}\,b_n(U)\in k[U]$ for every $n\geq 0$. Enlarge again the set $\mathcal{E}$ to contain the roots of $E(U)$. For $t_0\in k\setminus\mathcal{E}$, specializing U to t_0 in the displayed formula above produces $\widetilde{\mathcal{Y}}_{t_0}$ as a formal power series in $k[[T-t_0]]$, which amounts to saying that, up to some k-isomorphism, $\widetilde{\mathcal{Y}}_{t_0}$ and so $\widetilde{F}^{\phi_{t_0}}$ are fixed by all elements in $\mathsf{s}_{t_0}(\mathrm{G}_k)$. □

Let $\widetilde{P}(U,T,Y)\in k[U,T,Y]$ be the irreducible polynomial of $\widetilde{\mathcal{Y}}_U$ over $k[U,T]$. Theorem 2.2 holds for this polynomial $\widetilde{P}(U,T,Y)$ (up to enlarging again the finite set $\mathcal{E}$). When $k=\mathbb{Q}$ we may and will choose the element $\widetilde{\mathcal{Y}}_U$ integral over $\mathbb{Z}[T,Y]$ (and not just $\mathbb{Q}(T,Y)$) so that $\widetilde{P}(U,T,Y)$ lies in $\mathbb{Z}[U,T,Y]$ and will assume further that the coefficients of $\widetilde{P}(U,T,Y)$ are relatively prime.

3. Proof of the Hilbert-Malle theorem 1.3

3.1. **Basic data.** Fix the following for the rest of the paper:
- G is a non trivial finite group,
- $F/\mathbb{Q}(T)$ is a $\mathbb{Q}$-regular Galois extension of group G,

[8]This classical result is often stated for formal power series $\sum_{n\geq 0} b_nT^n$, algebraic over $\mathbb{Q}(T)$ and with coefficients $b_n\in\overline{\mathbb{Q}}$, but is true in a bigger generality including the situation where $\mathbb{Q}$ and $\mathbb{Z}$ are respectively replaced by $k(U)$ and $k[U]$. For example, the proof given in [DR79] easily extends to this situation.

- $f : X \to \mathbb{P}^1$ is the corresponding $\mathbb{Q}$-cover,
- $\mathbf{t} = \{t_1, \ldots, t_r\} \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ is the branch point set of $F/\mathbb{Q}(T)$,
- g_X is the genus of the curve X.

3.2. **Reduction to counting integral points on curves.** As in theorem 1.3, suppose given an integer $B \geq 1$ and a subset $\mathcal{H}_B \subset [1, B]$ consisting of integers t_0 such that $\mathrm{Gal}(F_{t_0}/\mathbb{Q})$ is the whole group G.

We will give a lower bound for the number of non conjugate specialization representations $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_{\mathbb{Q}} \to G$ with $t_0 \in \mathcal{H}_B$. Given two such representations, the associated field extensions are equal if and only if the representations have the same kernel, or, equivalently, if they differ by some automorphism of G. Dividing the previous bound by $|\mathrm{Aut}(G)|$ will thus yield the desired bound for $\mathcal{N}(\mathcal{H}_B)$.

Consider the polynomial $\widetilde{P}(U, T, Y) \in \mathbb{Z}[U, T, Y]$ given in theorem 2.2 and its discriminant $\Delta_{\widetilde{P}} \in \mathbb{Z}[U, T]$ (relative to Y). As $\widetilde{P}(U, T, Y)$ is irreducible in $\mathbb{Q}(U, T)[Y]$, $\Delta_{\widetilde{P}}(U, T) \neq 0$. Write it as a polynomial in T of degree N and denote its leading coefficient by $\Delta_{\widetilde{P},N}(U)$; we have $\Delta_{\widetilde{P},N}(U) \in \mathbb{Z}[U]$ and $\Delta_{\widetilde{P},N}(U) \neq 0$.

Drop from the set $\mathcal{H}_B$ the finitely many integers u_0 for which $\widetilde{\Delta}_{\widetilde{P},N}(u_0)$ is 0 or which are in the exceptional set $\mathcal{E}$ from theorem 2.2. Denote the resulting set by $\mathcal{H}'_B$ and the number of dropped elements by E. We may as well assume that $|\mathcal{H}_B| > \mathrm{E}$ and so that $\mathcal{H}'_B \neq \emptyset$.

Fix $u_0 \in \mathcal{H}'_B$ and consider the fiber-twisted cover of f at u_0

$$\widetilde{f}^{\phi \mathsf{s}_{u_0}} : \widetilde{X}^{\phi \mathsf{s}_{u_0}} \to \mathbb{P}^1_{\mathbb{Q}}$$

Let $t_0 \in \mathcal{H}'_B$. From the twisting lemma 2.1, the two representations $\phi \circ \mathsf{s}_{u_0}$ and $\phi \circ \mathsf{s}_{t_0}$ are conjugate in G if and only if there exists $x_0 \in \widetilde{X}^{\phi \mathsf{s}_{u_0}}(\mathbb{Q})$ such that $\widetilde{f}^{\phi \mathsf{s}_{u_0}}(x_0) = t_0$.

We have $\Delta_{\widetilde{P}}(u_0, t_0) \neq 0$ except for at most N integers t_0. For the non-exceptional t_0, the polynomial $\widetilde{P}(u_0, t_0, Y)$ has only distinct roots $y \in \overline{\mathbb{Q}}$ and, from theorem 2.2, the corresponding points (t_0, y) on the affine curve $\widetilde{P}(u_0, t, y) = 0$ exactly correspond to the points x on the smooth projective curve $\widetilde{X}^{\phi \mathsf{s}_{u_0}}$ above t_0. Furthermore, in this correspondence, the $\mathbb{Q}$-rational points x correspond to the couples (t_0, y) with $y \in \mathbb{Q}$. Conclude that up to some term $\leq N$, the number of t_0 for which $\phi \circ \mathsf{s}_{u_0}$ and $\phi \circ \mathsf{s}_{t_0}$ are conjugate in G is equal to the number of $\mathbb{Q}$-rational points (t_0, y) on the affine curve $\widetilde{P}(u_0, t, y) = 0$.

Note further that such a $\mathbb{Q}$-rational point (t_0, y) has necessarily integral coordinates as $t_0 \in \mathbb{Z}$ and $\widetilde{P}(u_0, T, Y) \in \mathbb{Z}[T, Y]$ and is monic in

Y. Therefore we are reduced to estimating the integers $t_0 \in [1, B]$ such that there is an integral point $(t_0, y) \in \mathbb{Z}^2$ on the curve $\widetilde{P}(u_0, t, y) = 0$.

3.3. **Diophantine estimates.** The constants c_i, $i > 0$ that will enter in the proof depend only on the extension $F/\mathbb{Q}(T)$. The *height* of a polynomial Q with coefficients in $\mathbb{Q}$ is the maximum of the absolute values of its coefficients and is denoted by $H(Q)$.

The curve $\widetilde{P}(u_0, t, y) = 0$ is of the same genus, say g_X, as the original curve X (theorem 2.2) and we have

$$\begin{cases} \deg(\widetilde{P}(u_0, T, Y)) \leq \deg(\widetilde{P}(U, T, Y)) = c_1 \\ \deg_Y(\widetilde{P}(u_0, T, Y)) = \deg_Y(\widetilde{P}(U, T, Y)) = |G| \\ H(\widetilde{P}(u_0, T, Y)) \leq c_2 u_0^{c_3} \leq c_2 B^{c_3} \end{cases}$$

For real numbers $g, D, H, B \geq 0$ and $d_Y \geq 2$, consider all polynomials $Q \in \mathbb{Z}[T, Y]$, wilth relatively prime coefficients, monic in Y, irreducible in $\overline{\mathbb{Q}}(T)[Y]$, such that $\deg_Y(Q) = d_Y$, of total degree $\leq D$, of height $\leq H$ and such that the affine curve $Q(t, y) = 0$ is of genus $\leq g$. For each such polynomial, the number of integers $t \in [1, B]$ such that there exists $y \in \mathbb{Z}$ such that $Q(t, y) = 0$ is a finite set. Denote by $Z(g, D, d_Y, H, B)$ the maximal cardinality of all these finite sets.

Using the diophantine parameter $Z(g, D, d_Y, H, B)$, conclude that the number of $t_0 \in \mathcal{H}'_B$ such that the two representations $\phi \circ \mathsf{s}_{u_0}$ and $\phi \circ \mathsf{s}_{t_0}$ are conjugate in G is less than or equal to

$$Z(g_X, c_1, |G|, c_2 B^{c_3}, B).$$

and that the number $\mathcal{N}(\mathcal{H}_B)$ satisfies

$$\mathcal{N}(\mathcal{H}_B) \geq \frac{|\mathcal{H}_B| - \mathrm{E}}{|\mathrm{Aut}(G)|\ [Z(g_X, c_1, |G|, c_2 B^{c_3}, B) + N]}$$

Assume that the genus g_X of X is ≥ 2 and that Lang's conjecture holds. This conjecture is that if V is a variety of general type defined over a number field K then the set $V(K)$ of K-rational points is not Zariski-dense in V [Lan86]. We will use it through the following consequence proved by Caporaso, Harris and Mazur [CHM97]: they showed that Lang's conjecture implies that for every number field K and every integer $g \geq 2$, there exists a finite integer $B(g, K)$ such that $\mathrm{card}(C(K)) \leq B(g, K)$ for every curve C of genus g defined over K.

Under this conjecture we obtain, if $g_X \geq 2$,

$$Z(g_X, c_1, |G|, c_2 B^{c_3}, B) + N \leq c_4.$$

In the general case $g_X \geq 0$ we use an unconditional result of Walkowiak [Wal05, §2.4]. From this result (theorem 3.1 in §3.4 below), we deduce

$$Z(g_X, c_1, |G|, c_2 B^{c_3}, B) + N \leq c_5 B^{1/|G|} (\log B)^{c_6}.$$

Conclude that unconditionally:

$$\mathcal{N}(\mathcal{H}_B) \geq \frac{|\mathcal{H}_B| - \mathrm{E}}{B^{1/|G|}(\log B)^{c_7}}$$

and, under Lang's conjecture, for $C = 1/(c_4\,|\mathrm{Aut}(G)|)$:

$$\mathcal{N}(\mathcal{H}_B) \geq C\,(|\mathcal{H}_B| - \mathrm{E})$$

3.4. **Walkowiak's result.** Let $Q \in \mathbb{Z}[T, Y]$ be a polynomial, irreducible in $\mathbb{Z}[T, Y]$. Set $D = \deg(Q)$ and $H^+ = \max(H(Q), e^e)$. The result we use in the proof above is the following.

Theorem 3.1 (Walkowiak)**.** *Assume* $\deg_Y Q \geq 2$. *There exist positive absolute constants* $a_1, \ldots, a_4$ *such that for every real number* $B \geq 1$, *the number of integers* $t_0 \in [1, B]$ *such that* $Q(t_0, Y)$ *has a root in* $\mathbb{Z}$ *is less than*

$$a_1 D^{a_2} (\log H^+)^{a_3} B^{1/\deg_Y(Q)} (\log B)^{a_4}.$$

This result is proved in [Wal05] but with $B^{1/2}$ instead of $B^{1/\deg_Y(Q)}$. We explain here how to modify Walkowiak's arguments to obtain the better exponent $1/\deg_Y(Q)$. The only change to make is in the final stage of the proof in [Wal05, §2.2-2.3].

Proof. Walkowiak's central result is the following bound for the number $N(Q, B)$ of $(t, y) \in \mathbb{Z}^2$ such that $\max(|t|, |y|) \leq B$ and $Q(t, y) = 0$:

$$N(Q, B) \leq 2^{36} D^5 \log^3(1250 d^{11} B^{5D-1}) \log^2(B)\, B^{1/D}.$$

To prove theorem 3.1, his basic idea is to use Liouville's inequality to get upper bounds $|y| \leq B'$ for roots $y \in \mathbb{Z}$ of polynomials $Q(t_0, Y)$ with $t_0 \in [1, B]$; the bound above for $N(Q, B)$ with B taken to be B' provides then a bound for the desired set. The main terms that appear in the resulting bound come from $(B')^{1/D}$. They may be too big however in some cases and Walkowiak uses a trick to obtain his final bound in $B^{1/2}$. In order to obtain $B^{1/n}$ instead, Walkowiak's trick should be modified as follows.

Set $L_1 = \log(H^+)$, $L_2 = \log(\log(H^+))$, $m = \deg_T Q$ and $n = \deg_Y Q$; one may assume $m > 0$. Let $t_0 \in [1, B]$ such that $Q(t_0, Y)$ has a root $y \in \mathbb{Z}$. Liouville's inequality gives

$$|y| \leq 2(m + 1) H^+ B^m = B'.$$

The main terms in $(B')^{1/D}$ are $(H^+)^{1/D}$ and $(B^m)^{1/D}$.

Case 1: $mnL_1/L_2 \leq D$. On the one hand, we have $1/D \leq L_2/L_1$ and so $(H^+)^{1/D} \leq (H^+)^{L_2/L_1} = \log(H^+)$. On the other hand $m/D \leq 1/n$ and so $B^{m/D} \leq B^{1/n}$. The upper bound for $N(Q, B')$ is indeed as announced in the statement of theorem 3.1.

Case 2: $mnL_1/L_2 > D$. Set $E = [mnL_1/L_2] + 1$ and consider the polynomial $G \in \mathbb{Z}[T, Y]$ defined by $G(T, Y) = Q(T, T^E + Y)$. For $y' = y - t_0^E$ we have $G(t_0, y') = 0$ and

$$|y'| \leq 2(m+1)H^+B^m + B^E \leq 2(m+1)H^+B^E = B''.$$

Use then the upper bound for $N(Q, B)$ with Q and B respectively taken to be G and B''. As $\deg_Y G = \deg_Y Q = n$ and $nE \leq \deg G \leq nE+m$, the main terms are in this case

$$(H^+)^{1/\deg(G)} \leq (H^+)^{1/nE} \leq (H^+)^{L_2/L_1} = \log(H^+)$$
$$\text{and} \quad B^{E/\deg G} \leq B^{1/n}.$$

Again the upper bound for $N(G, B'')$ is as announced. □

4. The specialization version of theorem 1.1

In this section we state theorem 4.3 (in §4.2) which is a more precise version of theorem 1.1 and which emphasizes the specialization aspect. In §4.3, we show how to deduce theorem 1.1 from theorem 4.3, which itself will be proved in §5. The initial subsection §4.1 elaborates on the parameter $\delta(G)$ which was introduced in our opening section §1.

4.1. The minimal affine branching index $\delta(G)$.

Given a $\mathbb{Q}$-regular extension $F/\mathbb{Q}[T]$, consider an affine model $P(T, Y) \in \mathbb{Q}[T, Y]$, monic in Y. Denote the discriminant of P relative to Y by $\Delta_P \in \mathbb{Q}[T]$ and its degree by δ_P. The minimal degree δ_P obtained in this manner is called the *minimal affine branching index of* $F/\mathbb{Q}(T)$ and denoted by $\delta_{F/\mathbb{Q}(T)}$. For any affine model $P(T, Y)$ of $F/\mathbb{Q}(T)$, monic in Y, we have

$$\delta_{F/\mathbb{Q}(T)} \leq \delta_P < 2|G| \deg_T(P).$$

If G is a regular Galois group over $\mathbb{Q}$, the parameter $\delta(G)$ involved in theorem 1.1 is the minimum of all $\delta_{F/\mathbb{Q}[T]}$ with $F/\mathbb{Q}[T]$ running over all $\mathbb{Q}$-regular realizations of G. As to Malle's exponent, it is defined as $a(G) = (|G|(1 - 1/\ell))^{-1}$ where ℓ is the smallest prime divisor of $|G|$.

Lemma 4.1. *Let G be a non trivial regular Galois group over $\mathbb{Q}$.*

(a) *If $F/\mathbb{Q}(T)$ is a $\mathbb{Q}$-regular realization of G with r branch points and g_F is the genus of F, then*

$$\delta(G) < 3(2g_F + 1)|G|^3 \log|G| \leq 3r\,|G|^4 \log|G|.$$

(b) *Furthermore we have* $\quad \delta(G) \geq 1/a(G).$

Proof of lemma 4.1. (a) The first inequality follows from a result of Sadi [Sad99, §2.2] which provides an affine model $P(T,Y)$ of $F/\mathbb{Q}(T)$, monic in Y, such that

$$\deg_T(P) \leq (2g_F+1)|G|^2 \log|G|/\log 2.$$

The second inequality follows from the Riemann-Hurwitz formula.

(b) Let $F/\mathbb{Q}(T)$ be a $\mathbb{Q}$-regular realization of G, $d_F \in \mathbb{Q}[T]$ be the absolute discriminant of $F/\mathbb{Q}(T)$ (the discriminant of a $\mathbb{Q}[T]$-basis of the integral closure of $\mathbb{Q}[T]$ in F) and $P(T,Y)$ be an affine model of $F/\mathbb{Q}(T)$. Inequality (b) follows from the following ones:

$$\delta_P \geq \deg(d_F) \geq |G|(1-1/\ell) = a(G).$$

The first inequality $\deg(d_F) \leq \delta_P$ is standard. Classically the polynomial d_F is a generator of the ideal $N_{F/\mathbb{Q}(T)}(\mathcal{D}_{F/\mathbb{Q}(T)})$ where $\mathcal{D}_{F/\mathbb{Q}(T)}$ is the different and $N_{F/\mathbb{Q}(T)}$ is the norm relative to the extension $F/\mathbb{Q}(T)$ [Ser62, III, §3]. From [Ser62, III, §6], in the prime ideal decomposition $\mathcal{D}_{F/\mathbb{Q}(T)} = \prod_{\mathcal{P}} \mathcal{P}^{u_{\mathcal{P}}}$, we have $u_{\mathcal{P}} \geq e_{\mathcal{P}} - 1$ for each prime $\mathcal{P}$, where $e_{\mathcal{P}} = e_{\mathfrak{p}}$ is the corresponding ramification index, which only depends on the prime $\mathfrak{p}$ below $\mathcal{P}$. The following inequalities, where $f_{\mathcal{P}}$ denotes the residue degree of $\mathcal{P}$, finish the proof:

$$\deg(d_F) \geq \sum_{\mathfrak{p}} \sum_{\mathcal{P}|\mathfrak{p}} f_{\mathcal{P}}(e_{\mathcal{P}}-1) = \sum_{\mathfrak{p}} |G| - |G|/e_{\mathfrak{p}} \geq |G|(1-1/\ell)$$

□

Remark 4.2. Our parameter $\delta(G)$ can also be compared to the minimum, say $\rho(G)$, of all branch point numbers r of $\mathbb{Q}$-regular realizations $F/\mathbb{Q}(T)$ of G: for such an extension $F/\mathbb{Q}(T)$ we have $\deg(d_F) \geq r-1$ which gives $\delta(G) \geq \rho(G)-1$. But the inequality $a(G) \geq 1/(\rho(G)-1)$ does not hold in general. For example the symmetric group S_n can be regularly realized over $\mathbb{Q}$ with 3 branch points so $\rho(S_n)=3$ while $a(S_n) = 2/n!$ The analog of theorem 1.1 with $r-1$ replacing $\delta_{F/\mathbb{Q}(T)}$ is false if the upper bound part of Malle's conjecture is true.

4.2. **The specialization result.** Theorem 4.3 is our most precise and most general but also most technical statement. It gives explicit estimates as provided by our approach. The asymptotic estimates of theorem 1.1 can then easily be deduced from them, as explained in §4.3. In §4.4, we give a weaker but more practical form of theorem 4.3.

In addition to §3.1, we will use the following notation and data.

4.2.1. *Further notation.*

- for a Frobenius data $\mathcal{F}$ on a set of primes S (see §1.2), the product of all ratios $|\mathcal{F}_p|/|G|$ with $p \in S$ – the *density* of $\mathcal{F}$ – is denoted by $\chi(\mathcal{F})$,
- for a finite set S of primes, set $\Pi(S) = \prod_{p\in S} p$,

- we also use the classical functions $\pi(x)$ and $\Pi(x)$ to denote respectively the number of primes $\leq x$ and the product of all primes $\leq x$. We have the classical asymptotics at ∞: $\pi(x) \sim x/\log(x)$ and $\log \Pi(x) \sim x$,
- given a k-regular Galois extension $F/k(T)$, we say a prime p is *good* for $F/\mathbb{Q}(T)$ if $p \not| \, |G|$, the branch divisor $\mathbf{t} = \{t_1, \ldots, t_r\}$ is étale at p and there is no vertical ramification at p; and it is *bad* otherwise. We refer to [DG12] for the precise definitions. We only use here the standard fact that there are only finitely many bad primes.

4.2.2. *Further data.* Fix the following:
- a prime p_0 as follows. Let p_{-1} be the biggest prime p such p is bad for $F/\mathbb{Q}(T)$ or $p < r^2|G|^2$. Then choose p_0 such that the interval $]p_{-1}, p_0]$ contains at least as many primes as there are non-trivial conjugacy classes of G.
- $\delta_{F/\mathbb{Q}(T)}$ or δ_F for short is the minimal affine branching index of $F/\mathbb{Q}(T)$,
- $P(T, Y)$ is an affine model of $F/\mathbb{Q}(T)$, monic in Y, such that $\delta_P = \delta_F$ (with δ_P the degree of the discriminant Δ_P); we further assume as we may that the coefficients of P are in $\mathbb{Z}$ and are relatively prime.
- if a branch point is $\mathbb{Q}$-rational, it will be possible to also prescribe ramification at finitely many primes in the specializations $F_{t_0}/\mathbb{Q}$. To this end we fix a finite set S of primes subject to these conditions:
(a) if no branch point of f is in $\mathbb{Z}$ then $S = \emptyset$.
(b) if at least one of the branch points of f, say t_1, is in $\mathbb{Z}$, then S is a finite set of good primes p, not dividing t_1 and not in $]p_{-1}, p_0]$.
(If at least one branch point is $\mathbb{Q}$-rational, one can reduce to the assumption in (b) *via* a simple change of the variable T).
- S_x is the set of primes p such that $p_0 < p \leq x$ and $p \notin S$; we assume $x > \max(p_0, \max(S))$.

4.2.3. *Statement.* Let $\mathcal{F}_x$ be a Frobenius data on S_x and $N_F(x, S, \mathcal{F}_x)$ be the number of specializations $F_{t_0}/\mathbb{Q}$ at points $t_0 \in \mathbb{Z}$ that satisfy
(i) $\mathrm{Gal}(F_{t_0}/\mathbb{Q}) = G$,
(ii) for each $p \in S_x$, $F_{t_0}/\mathbb{Q}$ is unramified and $\mathrm{Frob}_p(F_{t_0}/\mathbb{Q}) \in \mathcal{F}_p$,
(iii) for each $p \in S$, $F_{t_0}/\mathbb{Q}$ is ramified at p.

Theorem 4.3. (a) *There exist constants C_1, C_2, C_3, C_4 only depending on $P(T, Y)$ such that for every $x > \max(p_0, \max(S))$, we have*

$$N_F(x, S, \mathcal{F}_x) \geq C_1 \frac{\chi(\mathcal{F}_x)}{\Pi(S)^2} \frac{\Pi(x)^{1-1/|G|}}{(\log \Pi(x))^{C_2} C_3^{\pi(x)}} - C_4$$

so $\quad \log(N_F(x, S, \mathcal{F}_x))$ *is bigger than a function* $\lambda(x) \sim (1 - 1/|G|)x$.

(b) *Furthermore the specializations $F_{t_0}/\mathbb{Q}$ counted by the lower bound can be taken to be specializations at integers $t_0 \in [1, \Pi(S)\,\Pi(x)]$.*

(c) *Under Lang's conjecture on rational points on a variety of general type and if $g \geq 2$, we have this better inequality*

$$N_F(x, S, \mathcal{F}_x) \geq \ C_5 \, \frac{\chi(\mathcal{F}_x)}{\Pi(S)^2} \ \frac{\Pi(x)}{C_6^{\pi(x)}} - C_7$$

for constants C_5, C_6, C_7 only depending on P, so then

$\log(N_F(x, S, \mathcal{F}_x))$ *is bigger than a function* $\lambda(x) \sim x$.

(d) *We have the following upper bound for the number $\mathcal{N}_F(x, \mathcal{F}_x)$ of integers $t_0 \in [1, \Pi(S_x)]$ such that condition* (ii) *above holds:*

$$\mathcal{N}_F(x, \mathcal{F}_x) \leq \ \chi(\mathcal{F}_x) \, \frac{\Pi(S_x)}{\beta} \ (2 - \lambda)^{|S_x|}$$

where $\lambda = (r|G| - 1)/r^2|G|^2 \in]0, 1/4]$ and β depends only on $F/\mathbb{Q}(T)$.

4.3. **Proof of theorem 1.1 assuming theorem 4.3.** Pick a $\mathbb{Q}$-regular realization $F/\mathbb{Q}(T)$ of G and an affine model $P(T, Y)$, monic in Y, such that $\delta_P = \delta_F = \delta(G)$. Set $p_0(G) = p_0$. Fix $\delta > \delta(G)$ and set $\delta^- = (\delta + \delta(G))/2$. Let $y > 0$ and $x = \log(y)/\delta^-$.

As $\delta^- < \delta$ we have $\mathcal{S}_y = \{p_0(G) < p \leq \log(y)/\delta\} \subset S_x$. Complete the given Frobenius data $\mathcal{F}_y$ on $\mathcal{S}_y$ in an arbitrary way to make it a Frobenius data $\mathcal{F}_x$ on S_x. Apply theorem 4.3 to $\mathcal{F}_x$ and $S = \emptyset$.

Let $t_0 \in [1, \Pi(x)]$ corresponding to one of the specializations $F_{t_0}/\mathbb{Q}$ counted in theorem 4.3. From condition (i), the polynomial $P(t_0, Y)$ is irreducible in $\mathbb{Q}[Y]$. As it is monic and with integral coefficients, its discriminant, which is $\Delta_P(t_0)$, is a multiple of the absolute discriminant $d_{F_{t_0}}$ of the extension $F_{t_0}/\mathbb{Q}$. This leads to

$$|d_{F_{t_0}}| \leq \rho(x) = (1 + \delta_P)\, H(\Delta_P)\, \Pi(x)^{\delta_P}$$

As $\log \rho(x) \sim (\delta_P/\delta^-) \log y$, if y is suitably large, $\rho(x) \leq y$. It follows that $N(G, y, \mathcal{F}_y) \geq N_F(x, \emptyset, \mathcal{F}_x)$ and so $N(G, y, \mathcal{F}_y)$ can be bounded from below by the right-hand side term of the inequality from theorem 4.3 (a) with $x = \log(y)/\delta^-$. The logarithm of this term is asymptotic to $(1 - 1/|G|) \log(y)/\delta^-$. Conclude that for suitably large y, this term is bigger than $y^{(1-1/|G|)/\delta}$.

Remark 4.4 (ramified version of theorem 1.1). In the situation $S \neq \emptyset$, for which it is possible to prescribe ramification at some primes, the assumption that at least one branch point is $\mathbb{Q}$-rational cannot be removed, as explained in Legrand's paper [Legar]. Many groups have a $\mathbb{Q}$-regular realization $F/\mathbb{Q}(T)$ satisfying this assumption, although being of even order is a necessary condition [Legar, §3.2]: abelian groups of even order, symmetric groups S_n ($n \geq 2$), alternating groups A_n ($n \geq 4$), many simple groups (including the Monster), etc.

For these groups, theorem 4.3 leads, *via* the preceding argument, to

$$N(G, S, y, \mathcal{F}_y) \geq y^{(1-1/|G|)/\delta},$$

a generalized theorem 1.1 where $N(G, S, y, \mathcal{F}_y)$ replaces $N(G, y, \mathcal{F}_y)$ to be the number of extensions $E/\mathbb{Q}$ which, in addition to the conditions prescribed in theorem 1.1, are required to ramify at every prime from a finite set S of suitably big primes (and where the set $\mathcal{S}_y$ is of course replaced by $\mathcal{S}_y \setminus S$).

4.4. **A practical form of theorem 4.3.** Next statement is a simplified form of theorem 4.3. Furthermore the bounding condition is about the specialization point t_0 rather than the discriminant of $F_{t_0}/\mathbb{Q}$.

Corollary 4.5. *Given a $\mathbb{Q}$-regular Galois extension $F/\mathbb{Q}(T)$ of group G, there exist some constants p_0 and $C > 1$ such that if B is suitably large, the number of extensions $F_{t_0}/\mathbb{Q}$ with $t_0 \in [1, B] \cap \mathbb{Z}$ that are*
(i) *of group G, and*
(ii) *unramifed and totally split at each prime p with $p_0 \leq p \leq (\log B)/3$,*

is at least $\dfrac{B^{1-1/|G|}}{C^{\log B/\log\log B}}$.

Furthermore the condition "totally split" can be replaced by any other local behavior.

Proof. Corollary 4.5 follows from theorem 4.3 (a)&(b), applied with $S = \emptyset$ and x a real number such that $\Pi(x)$ is the biggest value of Π which is $\leq B$. Then we have $\Pi(2x) > B$. Using that $\log \Pi(x) \sim x$, it follows that for suitably large B, we have $\log B \leq 3x$ and so the set of primes of corollary 4.5 where some local condition is imposed is contained in that of theorem 4.3. The estimate easily follows. ☐

4.5. On the upper bound part from theorem 4.3.

4.5.1. *A remark.* The upper bound concerns extensions $E/\mathbb{Q}$ that are specializations of a given $\mathbb{Q}$-regular extension $F/\mathbb{Q}(T)$ (at integers t_0) and so does not directly lead to upper bounds for $N(G, y, \mathcal{F}_y)$ which counts extensions $E/\mathbb{Q}$ with no geometric origin *a priori*. A natural hypothesis to make in this context is that G has a generic extension $F/\mathbb{Q}(T)$ (or more generally a parametric extension, as defined in [Legar]): indeed then all Galois extensions $E/\mathbb{Q}$ of group G are specializations of $F/\mathbb{Q}(T)$ (at points $t_0 \in \mathbb{Q}$). But only the four groups $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, S_3 have a generic extension $F/\mathbb{Q}(T)$ [JLY02, p.194].

4.5.2. *A further application.* For every $x > p_0$, let $\mathcal{N}_{\text{tot.split}}(x)$ be the set of all integers $t_0 \geq 1$ such that the specialization $F_{t_0}/\mathbb{Q}$ is totally split at each prime $p_0 < p \leq x$.

Corollary 4.6. *For every $x > p_0$, $\mathcal{N}_{\text{tot.split}}(x)$ is a union of (many) cosets modulo $\Pi(S_x)$ but its density decreases to 0 as $x \to +\infty$.*

Proof. The number $\mathcal{N}_{\text{tot.split}}(x)$ counts integers $t_0 \geq 1$ which satisfy condition (ii) from theorem 4.3 with $\mathcal{F}_p$ taken to be the trivial conjugacy class for each $p \in S_x$. We anticipate on §5 to say that $\mathcal{N}_{\text{tot.split}}(x)$ is a union of cosets modulo $\Pi(S_x)$ (see proposition 5.3 (c)) and focus on the density part of the statement. Every integer $t_0 \in \mathcal{N}_{\text{tot.split}}(x)$ writes $t_0 = u + k\,\Pi(S_x)$ with u one of the elements in $[1, \Pi(S_x)]$ counted by $\mathcal{N}_F(x, \mathcal{F}_x)$ and $k \in \mathbb{Z}$. Let $N \geq 1$ be any integer. If $1 \leq t_0 \leq N$, then $k \leq N/\Pi(S_x)$. It follows then from theorem 4.3 (d) that

$$|\mathcal{N}_{\text{tot.split}}(x) \cap [1, N]| \leq \frac{N}{\Pi(S_x)} \times \mathcal{N}_F(x, \mathcal{F}_x) \leq \frac{N}{\beta} \times \left(\frac{2-\lambda}{|G|}\right)^{|S_x|}$$

which divided by N tends to 0 as $x \to +\infty$. □

Similar density conclusions can be obtained for other local behaviors for which the sets $\mathcal{F}_p$ are not too big compared to G.

5. Proof of theorem 4.3

We retain the notation and data introduced in §3.1 and in §4.2.

Fix $x > \max(p_0, \max(S))$ and a Frobenius data $\mathcal{F}_x$ on S_x.

Fix also a subset S_0 of primes $p \in]p_{-1}, p_0]$, with as many elements as there are non trivial conjugacy classes in G. Associate then in a one-one way a non-trivial conjugacy class $\mathcal{F}_p$ to each prime $p \in S_0$. Set $S_{0x} = S_0 \cup S_x$ and denote the Frobenius data $(\mathcal{F}_p)_{p \in S_{0x}}$ by $\mathcal{F}_{0x}$.

5.1. **First part: many good specializations $t_0 \in \mathbb{Z}$.** The goal of the first part is proposition 5.3 which shows that there are "many" $t_0 \in \mathbb{Z}$ such that conditions (i)-(iii) of theorem 4.3 are satisfied. The second part will then use the Hilbert-Malle theorem 1.3 to show that there are "many" distinct corresponding extensions $F_{t_0}/\mathbb{Q}$.

We use the method of [DG12] for this first part. We re-explain it in the special context of this paper and make the necessary adjustments for this proof. We refer to [DG12] for more details on the main arguments and for references. Working over number fields and even over $\mathbb{Q}$, we can give improved quantitative conclusions (compared to the existence statements of [DG12]). As in [DG12], there is first a local stage followed by a globalization argument.

5.1.1. *Local stage.* Below, given $t_0 \in \mathbb{Q}_p$ we say that $t_0 \notin \mathbf{t}$ modulo p if t_0 does not meet any of the branch points of $F/\mathbb{Q}(T)$ modulo p [9].

Proposition 5.1. *Given our regular $\mathbb{Q}$-G-Galois cover $f : X \to \mathbb{P}^1$, a prime p and a subset $\mathcal{F}_p \subset G$ consisting of a non-empty union of conjugacy classes of G, consider the set*

$$\mathcal{T}(\mathcal{F}_p) = \left\{ t_0 \in \mathbb{Z} \;\middle|\; \begin{array}{l} t_0 \notin \mathbf{t} \text{ modulo } p \\ \mathrm{Frob}_p(F_{t_0}/\mathbb{Q}) \in \mathcal{F}_p \end{array} \right\}.$$

If p is a good prime for f, the set $\mathcal{T}(\mathcal{F}_p)$ is a union of cosets modulo p. Furthermore, the number $\nu(\mathcal{F}_p)$ of these cosets satisfies

$$\nu(\mathcal{F}_p) \geq \frac{|\mathcal{F}_p|}{|G|} \times (p + 1 - 2g\sqrt{p} - |G|(r+1))$$

$$\textit{and} \quad \nu(\mathcal{F}_p) \leq \frac{|\mathcal{F}_p|}{|G|} \times (p + 1 + 2g\sqrt{p}).$$

Proof. We follow the method from [DG12]. Similar estimates though not in this explicit form can also be found in [Eke90].

We may and will assume that the subset $\mathcal{F}_p$ consists of a single conjugacy class.

Set $f_p = f \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and denote the corresponding π_1-representation by $\phi_p : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\mathbb{Q}_p} \to G$. Pick an element $g_p \in \mathcal{F}_p$ and consider the unique unramified epimorphism $\varphi_p : \mathrm{G}_{\mathbb{Q}_p} \to \langle g_p \rangle$ that sends the Frobenius of $\mathbb{Q}_p$ to g_p.

The condition "$t_0 \notin \mathbf{t}$ modulo p" implies that p is unramified in the specialization $F_{t_0}/\mathbb{Q}$. Then $t_0 \in \mathcal{T}(\mathcal{F}_p)$ if and only if the specialization representation $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_{\mathbb{Q}} \to G$ of $F/\mathbb{Q}(T)$ at t_0 is conjugate in G to $\varphi_p : \mathrm{G}_{\mathbb{Q}_p} \to \langle g_p \rangle$. From the twisting lemma 2.1, this is equivalent to the existence of a $\mathbb{Q}_p$-rational point above t_0 in the covering space of the twisted cover $\widetilde{f_p}^{\varphi_p} : \widetilde{X_p}^{\varphi_p} \to \mathbb{P}^1$. As p is a good prime, this last cover has good reduction; denote the special fiber by $\widetilde{\mathsf{f}}_p : \widetilde{\mathsf{X}}_p \to \mathbb{P}^1_{\mathbb{F}_p}$. The last existence condition is then equivalent to the existence of some point $\overline{x} \in \widetilde{\mathsf{X}}_p(\mathbb{F}_p)$ above the coset $\overline{t_0} \in \mathbb{P}^1(\mathbb{F}_p)$ of t_0 modulo p: the direct part is clear while the converse follows from Hensel's lemma.

From the Lang-Weil bound, the number of $\mathbb{F}_p$-rational points on $\widetilde{\mathsf{X}}_p$ is $\geq p + 1 - 2g\sqrt{p}$. Removing the points that lie above a branch point or the point at infinity leads to the announced first estimate, a final observation for this calculation being that for $t_0 \notin \mathbf{t}$ modulo p,

[9]Recall that for two points $t, t' \in \overline{\mathbb{Q}_p} \cup \{\infty\}$, meeting modulo p means that $|t|_{\overline{p}} \leq 1$, $|t'|_{\overline{p}} \leq 1$ and $|t - t'|_{\overline{p}} < 1$, or else $|t|_{\overline{p}} \geq 1$, $|t'|_{\overline{p}} \geq 1$ and $|t^{-1} - (t')^{-1}|_{\overline{p}} < 1$, where $\overline{p}$ is some arbitrary prolongation of the p-adic absolute value v to $\overline{\mathbb{Q}_p}$.

the number of $\mathbb{F}_p$-rational points $\overline{x} \in \widetilde{\mathsf{X}}_p(\mathbb{F}_p)$ above $\overline{t_0}$ is $|\mathrm{Cen}_G(g_p)| = |G|/|\mathcal{F}_p|$: this number is the same as the number of $\omega \in G$ such that $\phi \circ \mathsf{s}_{t_0} = \omega \varphi_p \omega^{-1}$ (as in the proof of the twisting lemma in [DG12]). Using the upper bound part of Lang-Weil leads to the second estimate. □

If in addition $p \geq r^2|G|^2$ (in particular if $p \in S_{0x}$), then the right-hand side term in the inequality of proposition 5.1 is > 0 (use that $g < r|G|/2 - 1$ if $|G| > 1$, which follows from Riemann-Hurwitz).

Proposition 5.2. *Assume that the branch point t_1 of the $\mathbb{Q}$-G-Galois cover $f : X \to \mathbb{P}^1$ is in $\mathbb{Z}$. Given a prime p, consider the set*

$$\mathcal{T}(\mathrm{ra}/p) = \{t_0 \in \mathbb{Z} \mid F_{t_0}/\mathbb{Q} \text{ is ramified at } p\}.$$

If p is a good prime for f, the set $\mathcal{T}(\mathrm{ra}/p)$ contains the coset of $t_1+p \in \mathbb{Z}$ modulo p^2.

Proof. Let $t_0 \in \mathbb{Z}$ such that $t_0 \equiv t_1 + p$ modulo p^2. Then $t_0 - t_1$ is of p-adic valuation 1. As p is good, it follows that $F_{t_0}/\mathbb{Q}$ is ramified at p. This last conclusion is part of the "Grothendieck-Beckmann theorem" for which we refer to [Gro71] and [Bec91, proposition 4.2]; see also [Legar] where this result is discussed together with further developments in the spirit of proposition 5.2. □

5.1.2. *Globalization.* Set

$$\begin{cases} \beta = \Pi(S_0) \\ B(x) = \beta\, \Pi(S)^2\, \Pi(S_x) \end{cases}$$

and consider the intersection

$$\bigcap_{p \in S_{0x}} \mathcal{T}(\mathcal{F}_p) \cap \bigcap_{p \in S} \mathcal{T}(\mathrm{ra}/p).$$

From proposition 5.1, proposition 5.2 and the Chinese remainder theorem, this set contains

$$\mathcal{N}(S, \mathcal{F}_{0x}) = \prod_{p \in S_{0x}} \nu(\mathcal{F}_p)$$

cosets modulo $B(x)$. Denote the set of their representatives in $[1, B(x)]$ by $\mathcal{T}(S, \mathcal{F}_{0x})$; the cardinality of this set is $\mathcal{N}(S, \mathcal{F}_{0x})$.

Proposition 5.3. (a) *For every integer $t_0 \in \mathcal{T}(S, \mathcal{F}_{0x})$, the extension $F_{t_0}/\mathbb{Q}$ satisfies the three conditions* (i)-(iii) *from theorem 4.3, with* (ii) *even replaced by the following sharper version* (ii+) *of* (ii)*, that is*

(i) $\mathrm{Gal}(F_{t_0}/\mathbb{Q}) = G$*,*

(ii+) $F_{t_0}/\mathbb{Q}$ *is unramified and* $\mathrm{Frob}_p(F_{t_0}/\mathbb{Q}) \in \mathcal{F}_p$ *for every* $p \in S_{0x}$ (and not just for every $p \in S_x$)*,*

(iii) *$F_{t_0}/\mathbb{Q}$ is ramified at p for every $p \in S$,*

(b) *We have* $\mathcal{N}(S, \mathcal{F}_{0x}) \geq \chi(\mathcal{F}_x) \dfrac{B(x)}{\beta \Pi(S)^2} \left(\dfrac{1}{2r|G|}\right)^{|S_x|}$

(c) *The set of integers $t_0 \in \mathbb{Z}$ such that for each $p \in S_x$, $F_{t_0}/\mathbb{Q}$ is unramified and* $\mathrm{Frob}_p(F_{t_0}/\mathbb{Q}) \in \mathcal{F}_p$ *consists of cosets modulo $\Pi(S_x)$ and the set $\mathcal{T}(\emptyset, \mathcal{F}_x)$ of their representatives in $[1, \Pi(S_x)]$ is of cardinality*

$$\mathcal{N}(\emptyset, \mathcal{F}_x) = \prod_{p \in S_x} \nu(\mathcal{F}_p) \leq \chi(\mathcal{F}_x) \frac{\Pi(S_x)}{\beta} (2 - \lambda)^{|S_x|}$$

where $\lambda = (r|G| - 1)/r^2|G|^2$.

Conclusion (c) proves conclusion (d) of theorem 4.3.

Proof. (a) Fix $t_0 \in \mathcal{T}(S, \mathcal{F}_{0x})$ (or more generally congruent modulo $B(x)$ to some element in $\mathcal{T}(S, \mathcal{F}_{0x})$).

Conditions (ii+), (iii) hold by definition of the sets $\mathcal{T}(\mathcal{F}_p)$ and $\mathcal{T}(\mathrm{ra}/p)$.

A classical argument then shows that (i) follows from (ii+): indeed because of the Frobenius condition at the primes $p \in S_0$, the subgroup $\mathrm{Gal}(F_{t_0}/\mathbb{Q}) \subset G$ meets every conjugacy class of G; from a lemma of Jordan [Jor72], it is all of G.

(b) Using proposition 5.1, we obtain

$$\begin{aligned}\mathcal{N}(S, \mathcal{F}_{0x}) &\geq \prod_{y \in S_x} \frac{|\mathcal{F}_p|}{|G|} \times (p + 1 - 2g\sqrt{p} - |G|(r+1)) \\ &\geq \chi(\mathcal{F}_x) \times \prod_{p \in S_x} p \times \prod_{p \in S_x} \left(1 + \frac{1}{p} - \frac{2g}{\sqrt{p}} - \frac{(r+1)|G|}{p}\right)\end{aligned}$$

Using again that $g < r|G|/2 - 1$ (if $|G| > 1$) and that $p \geq r^2|G|^2$ for each $p \in S_x$, we have

$$\begin{aligned}1 + \frac{1}{p} - \frac{2g}{\sqrt{p}} - \frac{|G|(r+1)}{p} &> 1 - \frac{r|G| - 2}{r|G|} - \frac{(r+1)|G|}{r^2|G|^2} \\ &= \frac{2}{r|G|} - \frac{(r+1)|G|}{r^2|G|^2} \\ &= \frac{(r-1)|G|}{r^2|G|^2} \geq \frac{1}{2r|G|}\end{aligned}$$

which yields the announced first estimate.

(c) Here we use the conclusion from proposition 5.1 that for each $p \in S_x$, the set $\mathcal{T}(\mathcal{F}_p)$ consists exactly of $\nu(\mathcal{F}_p)$ cosets modulo p. Combined with the Chinese remainder, this gives that the set $\mathcal{T}(\emptyset, \mathcal{F}_x)$ consists of exactly $\mathcal{N}(\emptyset, \mathcal{F}_x) = \prod_{p \in S_x} \nu(\mathcal{F}_p)$ elements. Proceed then similarly as in (b) but using the upper bound part of proposition 5.1 to obtain the desired estimate. □

Remark 5.4. Consider the situation with $S = \emptyset$ and allowing no local condition at some primes $p \in S_x$ — no restriction on $\mathrm{Frob}_p(F_{t_0}/\mathbb{Q})$ and no unramified condition —. We have $\nu(\mathcal{F}_p) = p$ for such primes and obtain this generalized lower bound: if $S'_x \subset S_x$ is the subset of primes where there *is* a local condition, then

$$\mathcal{N}(\emptyset, \mathcal{F}_{0x}) \geq \chi(\mathcal{F}_x) \, \frac{B(x)}{\beta} \left(\frac{1}{2r|G|} \right)^{|S'_x|}.$$

In particular, the number of integers $t_0 \in [1, B(x)]$ where $\mathrm{Gal}(F_{t_0}/\mathbb{Q}) = G$ (and no further local condition at any prime) is $\geq B(x)/\beta$.

5.2. **Second part: many good specializations $F_{t_0}/\mathbb{Q}$.** To conclude the proof of theorem 4.3, we apply the Hilbert-Malle theorem 1.3 with $B = B(x)$ and $\mathcal{H}_B = \mathcal{T}(S, \mathcal{F}_{0x})$. We obtain

$$\begin{cases} \mathcal{N}(\mathcal{T}(S, \mathcal{F}_{0x})) \geq \dfrac{\mathcal{N}(S, \mathcal{F}_{0x}) - \mathrm{E}}{B(x)^{1/|G|} (\log B(x))^{\gamma}} & \textit{unconditionnally} \\[2ex] \mathcal{N}(\mathcal{T}(S, \mathcal{F}_{0x})) \geq C\, (\mathcal{N}(S, \mathcal{F}_{0x}) - \mathrm{E}) & \begin{array}{c}\textit{under Lang's conjecture and} \\ \textit{if the genus of } F \textit{ is} \geq 2\end{array} \end{cases}$$

where E, C and γ are the constants involved in theorem 1.3. Note that $N_F(x, S, \mathcal{F}_x) \geq \mathcal{N}(\mathcal{T}(S, \mathcal{F}_{0x}))$ and use proposition 5.3 (b) to conclude that unconditionally:

$$N_F(x, S, \mathcal{F}_x) \geq c_8 \, \frac{\chi(\mathcal{F}_x)}{\Pi(S)^2} \, \frac{B(x)^{1-1/|G|}}{(\log B(x))^{c_{10}} \, c_9^{|S_x|}} - c_{11}$$

and, under Lang's conjecture:

$$N_F(x, S, \mathcal{F}_x) \geq c_{12} \, \frac{\chi(\mathcal{F}_x)}{\Pi(S)^2} \, \frac{B(x)}{c_9^{|S_x|}} - c_{11}.$$

where the constants $c_8, \ldots, c_{12}$, and c_{13} below, only depend on P. Note finally that $c_{13}\Pi(x) \leq B(x) \leq \Pi(S)\Pi(x)$, that $|S_x| \leq \pi(x)$ and that $0 < c_9 = 1/(2r|G|) < 1$ to obtain the estimates of theorem 4.3 (a) and (c). Theorem 4.3 (b) follows from the containments $\mathcal{T}(S, \mathcal{F}_{0x}) \subset [1, B(x)] \subset [1, \Pi(S)\Pi(x)]$.

References

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

[BF10] Karim Belabas and Etienne Fouvry. Discriminants cubiques et progressions arithmétiques. *International J. Number Theory*, 6:1491–1529, 2010.
[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.
[Bha10] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.
[BW08] Manjul Bhargava and M. Wood, Melanie. The density of discriminants of S_3-sextic number fields. *Proc. Amer. Math. Soc.*, 136-5:1581–1587, 2008.
[CHM97] Lucia Caporaso, Joe Harris, and Barry Mazur. Uniformity of rational points. *J. Amer. Math. Soc.*, 10:1–35, 1997.
[DG12] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *Ann. Inst. Fourier*, 62/3:989–1013, 2012.
[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic extensions II. *Proc. Roy. Soc. London Ser. A*, 322:405–420, 1971.
[DR79] Bernard Dwork and Philippe Robba. On natural radii of p-adic convergence. *Trans. A.M.S.*, 199-213:199–213, 1979.
[DW88] B. Datskovsky and D. J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math.*, 386:116–138, 1988.
[Eke90] Torsten Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988/89*, volume 91 of *Progress in Mathematics*, pages 241–248. Birkhäuser, 1990.
[EV05] Jordan S. Ellenberg and Akshay Venkatesh. Counting extensions of function fields with bounded discriminant and specified Galois group. In *Geometric methods in algebra and number theory*, volume 235 of *Progr. Math.*, pages 151–168. Birkhäuser Boston, Boston, MA, 2005.
[EV06] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.
[EVW] Jordan S. Ellenberg, Akshay Venkatesh, and C. Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields (I & II). arXiv:0912.0325 & arXiv:1212.0923.
[Gro71] Alexandre Grothendieck. *Revêtements étales et groupe fondamental*, volume 224 of *LNM*. Springer, 1971.
[HB02] D. R. Heath-Brown. The density of rational points on curves and surfaces. *Ann. of Math.*, 155:553–595, 2002.
[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials. Constructive Aspects of the Inverse Galois Problem*. Cambridge University Press, 2002.
[Jor72] Camille Jordan. Recherches sur les substitutions. *J. Liouville*, 17:351–367, 1872.
[Klü05a] Jürgen Klüners. A counter example to Malle's conjecture on the asymptotics of discriminants. *C. R. Acad. Sci. Paris, Ser. I*, 340:411–414, 2005.
[Klü05b] Jürgen Klüners. *Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe*. Shaker Verlag, Habilitationsschrift University Kassel, 2005.
[Klü06] Jürgen Klüners. Asymptotics of number fields and the Cohen-Lenstra heuristics. *J. Théorie des Nombres Bordeaux*, 18:607–615, 2006.
[KM04] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.

[Lan86] Serge Lang. Hyperbolic diophantine analysis. *Bull. A.M.S.*, 42:159–205, 1986.

[Legar] François Legrand. Specialization results and ramification conditions. *Isr. J. Math.*, (to appear). arXiv:1310.2189.

[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.*, 54:271–296, 1979.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic Number Fields*, (A. Fröhlich edit., pages 409–464. Academic Press, New-York, 1977.

[Mäk85] Sirpa Mäki. On the density of abelian number fields. *Ann. Acad. Sci. Fenn. Ser. A I Math. Dissertationes*, 54, 1985.

[Mal02] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92/2:315–329, 2002.

[Mal04] Gunter Malle. On the distribution of Galois groups II. *Experiment. Math.*, 13:129–135, 2004.

[Nef13] Danny Neftin. On the tame and wild Grunwald problems. *Preprint*, 2013.

[Sad99] Bounab Sadi. *Descente effective du corps de définition des revêtements.* Thèse Univ. Lille 1, 1999.

[Ser62] Jean-Pierre Serre. *Corps locaux.* Hermann, Paris, 1962.

[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.* Research Notes in Mathematics. Jones and Bartlett Publishers, 1992.

[VE10] Akshay Venkatesh and Jordan S. Ellenberg. Statistics of number fields and function fields. In *Proceedings of the International Congress of Mathematicians. Volume II*, pages 383–402. Hindustan Book Agency, New Delhi, 2010.

[Wal05] Yann Walkowiak. Théorème d'irréductibilité de Hilbert effectif. *Acta Arith.*, 116/4:343–362, 2005.

[Wan69] Shianghao Wang. A counter-example to Grunwald's theorem. *Annals of Math.*, 90:1008–1009, 1969.

[Wri89] D. J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc.*, 58/1:17–50, 1989.

E-mail address: `Pierre.Debes@math.univ-lille1.fr`

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France