SPECIALIZATIONS OF GALOIS COVERS OF THE LINE

PIERRE DÈBES AND NOUR GHAZI

Abstract. The main topic of the paper is the Hilbert-Grunwald property of Galois covers. It is a property that combines Hilbert's irreducibility theorem, the Grunwald problem and inverse Galois theory. We first present the main results of our preceding paper which concerned covers over number fields. Then we show how our method can be used to unify earlier works on specializations of covers over various fields like number fields, PAC fields or finite fields. Finally we consider the case of rational function fields $\kappa(x)$ and prove a full analog of the main theorem of our preceding paper.

1. Inroduction

The Hilbert-Grunwald property of Galois covers over number fields was defined and studied in our previous paper [DG10]. It combines several topics: the Grunwald-Wang problem, Hilbert's irreducibility theorem and the Regular Inverse Galois Problem (RIGP). Roughly speaking our main result there, which is recalled below as theorem 2.1 showed how, under certain conditions, a Galois cover $f : X \to \mathbb{P}^1$ provides, by specialization, solutions to Grunwald problems. We next explained how to deduce an obstruction (possibly vacuous) for a finite group to be a regular Galois group over some number field K, *i.e.* the Galois group of some regular Galois extension $E/K(T)$ (corollary 1.5 of [DG10]). A refined form of this obstruction led us to some statements that question the validity of the Regular Inverse Galois Problem (RIGP) (corollaries 1.6 and 4.1 of [DG10]).

The aim of this paper is threefold:
- in §2: we present in more details the contents of [DG10]. This first part corresponds to the lecture given by the first author at the Alexandru Myller Mathematical Seminar Centennial Conference in Iasi.

Date: February 16, 2011.

2000 *Mathematics Subject Classification.* Primary 14H30, 11R32, 12F12, 12E25; Secondary 14Gxx, 14Dxx, 14H10.

Key words and phrases. Inverse Galois theory, Grunwald's theorem, Hilbert's irreducibility theorem, algebraic covers, local and global fields.

- in §3: we explain the starting lemma of our approach and show how it can be used to unify earlier works over various fields like PAC fields and finite fields. For example Fried's Čebotarev theorem for rational function fields $\kappa(x)$ over a finite field κ and Colliot-Thélène's result that varieties over a number field with the "weak weak approximation property" have the Hilbert property can be obtained as special cases of our approach.
- in §4: we use the method of [DG10] to show the analog of the main theorem of [DG10] with the number field K replaced by the function field $\kappa(x)$ in one variable over a field κ that either is PAC and has "enough cyclic extensions", or is finite and large enough (theorem 4.2).

2. The Hilbert-Grunwald property of Galois covers

2.1. **The Grunwald problem.** Given a Galois cover $f : X \to \mathbb{P}^1$ over some field K and a point $t_0 \in \mathbb{P}^1(K)$ not a branch point, what we call the *specialization* of f at t_0 is the residue field, denoted by $K(X)_{t_0}$, of some point in X above t_0 (see §3.1).

Given a field K, a finite set S of independent non-trivial discrete valuations of K and a finite group G, the *Grunwald problem*, is whether there exist Galois extensions E/K with group G which have prescribed v-completions E_v/K_v $(v \in S)$. More precisely, define the set of Galois extensions of some field k with Galois group G (resp. with Galois group contained in G) by $\mathrm{Ext}_G(k)$ (resp. by $\mathrm{Ext}_{\leq G}(k)$. Then the question is: given a collection $\underline{E} = (E^v/K_v)_{v\in S} \in \prod_{v\in S} \mathrm{Ext}_{\leq G}(K_v)$ — called a *Grunwald problem* —, does there exist an extension $E/K \in \mathrm{Ext}_G(K)$ — called a *solution to the Grunwald problem* — which induces the local extensions E^v/K_v by base change from K to K_v $(v \in S)$?

Recall that if K is a number field, every Grunwald problem has a solution when G is cyclic of odd order (see [NSW08, (9.2.8)]) or when G is solvable of order prime to the number of roots of 1 in K (Neukirch [Neu79], [NSW08, (9.5.5)]).

2.2. **The main theorem.** Some further notation is needed to state the main theorem from [DG10]. Fix K, S and G as above. For each place v of K, denote the valuation ring of K_v by $\mathcal{O}_v$, the valuation ideal by $\mathfrak{p}_v$, the residue field by κ_v and the order and the characteristic of κ_v by q_v and p_v respectively. The constant $c(|G|, r)$ (resp. $c(G)$) that appears below only depends on the order of G and the branch point number r (resp. on the group G); they are defined in [DG10]. Condition (good-red) is explained right after the statement. A Grunwald problem $\underline{\varphi}$ is said to be *unramified* if $\mathrm{Gal}(\overline{K_v}/K_v^{\mathrm{ur}}) \subset \ker(\varphi_v)$ $(v \in S)$.

Theorem 2.1. *Assume that K is a number field, that $p_v \not| |G|$ and $q_v \geq c(|G|, r)$ ($v \in S$). Let $f : X \to \mathbb{P}^1$ be a Galois cover of group G and r branch points, defined over K (as G-cover) and satisfying the following* good reduction *condition:*

(good-red) *for each $v \in S$, the branch divisor $\mathbf{t} = \{t_1, \ldots, t_r\}$ is étale and there is no vertical ramification in the cover f at v.*

Then f has the following Hilbert-Grunwald specialization *property:*

(HGr-spec) *For every unramified Grunwald problem there exist specializations of f at points $t_0 \in \mathbb{A}^1(K) \setminus \mathbf{t}$ that are K-solution to it. More precisely the set of all such t_0 contains a subset $\mathbb{A}^1(K) \cap \prod_{v \in S \cup S_0} U_v$ where each $U_v \subset \mathbb{A}^1(\mathcal{O}_v)$ is a coset of $\mathcal{O}_v$ modulo $\mathfrak{p}_v$ and S_0 is a finite set of finite places $v \notin S$ which can be chosen depending only on f.*

Furthermore, if $p_v \not| 6|G|$ and $q_v \geq c(G)$ ($v \in S$), there exist a Galois extension L/K totally split in K_v ($v \in S$) and a G-cover $f : X \to \mathbb{P}^1$ of group G, defined over L that satisfies both the good reduction condition (good-red) *and the Hilbert-Grunwald specialization property* (HGr-spec) *with K replaced by L.*

More explicitly "$\mathbf{t} = \{t_1, \ldots, t_r\}$ étale" in condition (good-red) means that no two $\overline{K}$-points $t_i, t_j \in \overline{K} \cup \{\infty\}$ *coalesce* at v, and coalescing at v that $|t_i|_{\overline{v}} \leq 1$, $|t_j|_{\overline{v}} \leq 1$ and $|t_i - t_j|_{\overline{v}} < 1$, or else $|t_i|_{\overline{v}} \geq 1$, $|t_j|_{\overline{v}} \geq 1$ and $|t_i^{-1} - t_j^{-1}|_{\overline{v}} < 1$, where $\overline{v}$ is any prolongation of v to $\overline{K}$. As to non-vertical ramification, a practical definition is this: for each $v \in S$, if an affine equation $P(t, y) = 0$ of X is given with t corresponding to f and P monic in y with integral coefficients (relative to v), then v is unramified in f if the discriminant $\Delta(t)$ of P with respect to y is non-zero modulo the valuation ideal of v (see [DG10, §2] for a more intrinsic definition). The (good-red) condition is indeed a good reduction criterion: if $\mathbf{t}$ is étale and $p_v \not| |G|$, f acquires good reduction at v after some finite scalar extension L/K [Ful69]; under the extra non-vertical ramification assumption, one can take $L = K$ (*e.g.* [DG10, §2]).

2.3. **Application to the RIGP.** The following statement is a consequence of theorem 2.1. Given a Galois extension $E/\mathbb{Q}$, its discriminant is denoted by d_E and, for every real number $x \geq 1$, the number of primes $p \leq x$ that are <u>not</u> totally split or are ramified in $E/\mathbb{Q}$ by $\pi^E_{\mathrm{nts}}(x)$. The function $\pi(x)$ denotes the number of primes $\leq x$.

Corollary 2.2. *Let G be a finite group and assume G is a Galois group of some regular[1] Galois extension $F/\mathbb{Q}(T)$. Then there exist two*

[1] that is: $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$.

constants $m_0, \delta > 0$ *with the property that for every* $x \geq m_0$*, there are infinitely many* $t_0 \in \mathbb{Q}$ *such that the specialization* $F_{t_0}/\mathbb{Q}$ *of* $F/\mathbb{Q}(T)$ *at* t_0 *satisfies the following conditions:*

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

(ii) *all primes* $p \leq x$ *but those that are* $\leq m_0$ *are totally split in* $F_{t_0}/\mathbb{Q}$*; consequently* $\pi_{\mathrm{nts}}^{F_{t_0}}(x) \leq \pi(m_0)$,

(iii) $\log |d_{F_{t_0}}| \leq \delta\, x$.

Condition (i) makes the extension $F_{t_0}/\mathbb{Q}$ a solution to the Inverse Galois Problem over $\mathbb{Q}$ for the given group G. Condition (ii) should be related to the Čebotarev density theorem according to which a majority of primes are not totally split in a given number field; more precisely, the density of such primes equals $1 - 1/|G|$. As to condition (iii) it is essentially the best possible as the example of $G = \mathbb{Z}/2\mathbb{Z}$ already shows. Indeed in a quadratic number field $E = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square free, condition (ii) amounts to d being a square modulo (almost) all primes $p \leq d$. This leads to $\log |d_E| \sim \log |d| \sim \log(\prod_{p \leq x} p) \sim x$ as $x \to \infty$.

In fact if (iii) is sharpened to (iii+) below, the conclusion of corollary no longer holds. Indeed the following effective version of the Čebotarev theorem is proved in [LO77] (see also [Ser81, §2.2]): for every Galois extension $E/\mathbb{Q}$ of group G

$$(**) \qquad \pi_{\mathrm{nts}}^{E}(x) \geq \pi(x) - \frac{2}{|G|}\frac{x}{\log x} \quad \text{if } \log x \geq \beta\,|G|\,\log^2|d_E|$$

for some absolute constant β. So *for any group* G there can be no number field E satisfying conditions (i), (ii) and

(iii+) $\beta\,|G|\,\log^2|d_E| \leq \log x$.

The question arises then of whether it is true for all groups G that there exists a number field E satisfying conditions (i), (ii) and (iii) from corollary 2.2. If for some group G the answer is "No", then the Regular Inverse Galois Problem has a negative answer (for this group).

It would be interesting to study to what extent the analytic estimate (**) can be improved for a given group G. The difference between (iii) and (iii+) is essentially a "log". We note that a "log" can be gained in a related problem: concerning the least prime ideal in the Čebotarev density theorem (instead of the number of primes), Linnick's theorem precisely shows this difference between the general estimate and that of the specific situation of Dirichlet's theorem (see [LMO79]).

Example 2.3. Here is an example of a situation that would lead to a counter-example to the RIGP. Let G be a p-group (possibly $p = 2$).

Any given Galois extension of group G has p-cyclic sub-extensions. Suppose the structure of G forces the following to happen: for any Galois extension $E/\mathbb{Q}$ of group G, a p-cyclic sub-extension $K/\mathbb{Q}$ can be found such that $\beta p \log^2 |d_K| \leq \log(\log |d_E|/\delta)$ (with β and δ as above). Then for $E = F_{t_0}$ as in corollary 2.2, the extension $K/\mathbb{Q}$ satisfies condition (iii+) and so $\pi^K_{\text{nts}}(x) \geq \pi(x) - (2x)/(p \log x)$ by Lagarias-Odlyzko. Now the primes that are not totally split or ramified in the extension $K/\mathbb{Q}$ are necessarily also so in the extension $E/\mathbb{Q}$. But this contradicts condition (ii) from corollary 2.2 as $\pi(x) - (2x)/(p \log x)$ tends to ∞ (even when $p = 2$).

Corollary 2.2 has the following more general version (also proved in [DG10]), which shows that the assumption that a group G is a regular Galois group over $\mathbb{Q}$ has even stronger implications on Galois extensions of $\mathbb{Q}$: conclusions from corollary 2.2 extend to any kind of residual behaviour.

Corollary 2.4. *Let G be a finite group and assume G is a Galois group of some regular Galois extension $F/\mathbb{Q}(T)$. Then there exist two constants $m_0, \delta > 0$ with the property that for every real number $x \geq 1$ and for any choice of a conjugacy class $C_p \subset G$ for each prime p with $m_0 < p \leq x$, there are infinitely many $t_0 \in \mathbb{Q}$ such that the specialization $F_{t_0}/\mathbb{Q}$ of $F/\mathbb{Q}(T)$ at t_0 satisfies the following conditions:*
(i) $\text{Gal}(F_{t_0}/\mathbb{Q}) \simeq G$,
(ii) *for each prime p with $m_0 < p \leq x$, the extension $F_{t_0}/\mathbb{Q}$ is unramified at p and the associated Frobenius is in the conjugacy class C_p,*
(iii) $\log |d_{F_{t_0(x)}}| \leq \delta\, x$.

Furthermore the constants m_0 and δ depend only on the extension $F/\mathbb{Q}(T)$ and can be explicitly computed. In particular this leads to interesting effective versions of Hilbert's irreducibility theorem.

3. Unifying previous works

3.1. **Basic notation.** For details, see [DD97, §2] and [Dèb99b, §2].

For a field k, we denote by $\overline{k}$ an algebraic closure, its separable closure in $\overline{k}$ by k^{sep} and its absolute Galois group by G_k. If k' is an overfield of k, we use the notation $\otimes_k k'$ for the base change from k to k'.

Given a regular projective geometrically irreducible k-variety B, a *k-mere cover of B* is a finite and generically unramified morphism $f : X \to B$ defined over k with X a normal and geometrically irreducible k-variety. Mere covers $f : X \to B$ over k correspond to finite separable field extensions $k(X)/k(B)$ that are regular over k through the function field functor. The term "mere" is meant to distinguish mere covers from G-covers. By k-G-*cover of* B *of group* G, we mean a Galois cover $f : X \to B$ over k given together with an isomorphism $G \to \mathrm{Gal}(k(X)/k(B))$. G-covers of B of group G over k correspond to regular Galois extensions $k(X)/k(B)$ given with an isomorphism of the Galois group $\mathrm{Gal}(k(X)/k(B))$ with G. By group and branch divisor of a k-cover f, we mean those of the k^{sep}-cover $f \otimes_k k^{\mathrm{sep}}$ [2].

We use the representation viewpoint to work with covers and field extensions: representations of fundamental groups for Galois covers and of absolute Galois groups for Galois extensions.

Galois field extensions E/K of group G correspond to epimorphisms[3] $\varphi : \mathrm{G}_K \to G$. The Grunwald problem translates as follows. Given a collection $\underline{\varphi} = (\varphi_v : \mathrm{G}_{K_v} \to G)_{v\in S} \in \prod_{v\in S} \mathrm{Hom}(\mathrm{G}_{K_v}, G)$ of homomorphisms $\varphi_v : \mathrm{G}_{K_v} \to G$ $(v \in S)$ — the *Grunwald problem* —, does there exist an epimorphism $\varphi : \mathrm{G}_K \to G$ — a *solution to the Grunwald problem* — which, composed with the restriction maps $\mathrm{G}_{K_v} \to \mathrm{G}_K$, yields the local maps φ_v?

Given a reduced positive divisor $D \subset B$, denote the k-fundamental group of $B \setminus D$ by $\pi_1(B \setminus D, t)_k$ where $t \in B(\overline{k}) \setminus D$ is a base point. Mere covers of B of degree d (resp. G-covers of B of group G) with branch divisor contained in D correspond to homomorphisms $\pi_1(B \setminus D, t)_k \to S_d$ such that the restriction to $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ is transitive (resp. to epimorphisms $\pi_1(B \setminus D, t)_k \to G$ such that the restriction to $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ is onto).

Each k-rational point $t_0 \in B(k) \setminus D$ provides a section $\mathrm{s}_{t_0} : \mathrm{G}_k \to \pi_1(B \setminus D, t)_k$ of the exact sequence

$$1 \to \pi_1(B \setminus D, t)_{k^{\mathrm{sep}}} \to \pi_1(B \setminus D, t)_k \to \mathrm{G}_k \to 1$$

well-defined up to conjugation by elements in $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$. Given a mere cover representation $\phi : \pi_1(B \setminus D, t)_k \to S_d$, the morphism $\phi \mathsf{s}_{t_0} : \mathrm{G}_k \to S_d$ is the *arithmetic action* of G_k on the fiber above t_0. If $\phi : \pi_1(B \setminus D, t)_k \to G$ represents a G-cover $f : X \to B$, the morphism $\phi \mathsf{s}_{t_0} : \mathrm{G}_k \to G$ is the *specialization representation* of f at t_0. The fixed field in k^{sep} of $\ker(\phi \mathsf{s}_{t_0})$ is the residue field of the Galois closure of $k(X)/k(B)$ (which is $k(X)/k(B)$ itself for G-covers) at some point

[2] The group of a k^{sep}-cover $X \to B$ is the Galois group of the Galois closure of the extension $k^{\mathrm{sep}}(X)/k^{\mathrm{sep}}(B)$. The branch divisor is the formal sum of all hypersurfaces of B such that the associated discrete valuations are ramified in the extension $k^{\mathrm{sep}}(X)/k^{\mathrm{sep}}(B)$.

[3] All profinite group homomorphisms are tacitly assumed to be continuous.

above t_0. We denote it by $k(X)_{t_0}$ and call the extension $k(X)_{t_0}/k$ the *specialization* of f at t_0.

3.2. **Twisting G-covers.** The main starting tool used in [DG10] is the "twisting operation".

Let k be a field and $f : X \to B$ be a k-G-cover. Let $\phi : \pi_1(B \setminus D, t)_k \to G$ be the epimorphism corresponding to the G-cover f and let $\varphi : \mathrm{G}_k \to G$ be an homomorphism (not necessarily onto).

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 $\widetilde{\phi}^\varphi : \pi_1(B \setminus D, t)_k \to S_d$ defined by the following formula, where r is the restriction map $\pi_1(B \setminus D, t)_k \to \mathrm{G}_k$ and $\times$ is the multiplication in the symmetric group S_d:

$$\widetilde{\phi}^\varphi(X) = \gamma\phi(X) \times \delta\varphi^* r(X) \qquad (X \in \pi_1(B \setminus D, t)_k)$$

It is easily checked that $\widetilde{\phi}^\varphi$ is a group homomorphism with the same restriction on $\pi_1(B \setminus D, t)_{k^{\mathrm{sep}}}$ as ϕ. The associated mere cover is a K-model of the mere cover $f \otimes_k k^{\mathrm{sep}}$. We denote it by $\widetilde{f}^\varphi : \widetilde{X}^\varphi \to B$ and call it the *twisted cover* of f by φ. The following statement contains the main property of the twisted cover.

Twisting lemma 3.1. *Let $t_0 \in B(k) \setminus D$. The specialization of the G-cover f at t_0 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 $\widetilde{f}^\varphi(x_0) = t_0$.*

Proof. For self-containedness, recall the key point of ($\Leftarrow$), which will be the only part used in the paper (see [DG10] for a full proof). Existence of $x_0 \in \widetilde{X}^\varphi(k)$ such that $\widetilde{f}^\varphi(x_0) = t_0$ is equivalent to existence of some common fixed point $\omega \in G$ for all permutations $\widetilde{\phi}^\varphi(\mathsf{s}_{t_0}(\tau))$ ($\tau \in \mathrm{G}_k$). The definition of $\widetilde{\phi}^\varphi$ then yields the equivalent condition $\phi(\mathsf{s}_{t_0}(\tau))\,\omega\,\varphi(\tau)^{-1} = \omega$, or $\phi(\mathsf{s}_{t_0}(\tau)) = \omega\,\varphi(\tau)^{-1}\omega^{-1}$ ($\tau \in \mathrm{G}_k$). □

3.3. **The Ekedahl-Colliot-Thélène result.** We explain how the twisting lemma 3.1 provides a simple proof of the following result, due independently to Colliot-Thélène [Ser92, §3] and Ekedahl [Eke90].

Recall the definition of the two properties involved in the statement. Given a number field K, a K-variety B is said to satisfy the *weak weak approximation property* (WWA) if for some finite set Σ of places of K, $B(K)$ is dense is $\prod_{v\in S} B(K_v)$ for all finite sets S that are disjoint from Σ. The K-variety B is said to satisfy the *Hilbert specialization property* if $B(K)$ is not thin, in the sense of [Ser92]. This is equivalent to showing that every G-cover $f : X \to B$ defined over K has specializations $K(X)_{t_0}/K$ with the same Galois group as f at all points t_0 in a subset of $B(K)$, Zariski dense in B. (The main point in this equivalence is to restrict to geometric G-covers, *i.e.* those corresponding to function field extensions that are regular over K; this follows from a classical use of the Čebotarev theorem).

Corollary 3.2 (Colliot-Thélène, Ekedahl)**.** *Let K be a number field. Then every K-variety B with the WWA property satisfies the Hilbert specialization property.*

Proof. We first reduce to the situation that B is smooth projective and geometrically integral (as assumed in §3.1) : for this we use the fact that both the WWA property and the Hilbert property are birational properties [Ser92, §3.5].

Let then $\phi : \pi_1(B \setminus D, t)_K \to G$ be an epimorphism onto some finite group G, with D a reduced positive K-divisor. We should show that

(*) *the map $\phi\, \mathsf{s}_{t_0} : \mathrm{G}_K \to G$ is surjective for all points t_0 in a Zariski dense subset of $B(K) \setminus D$,*

where s_{t_0} is the section corresponding to t_0 (see §3.1). For each place v of K, denote the restriction maps $\pi_1(B \setminus D, t)_{K_v} \to \pi_1(B \setminus D, t)_K$ and $\mathrm{G}_{K_v} \to \mathrm{G}_K$ by r_v. Thanks to the WWA property, it suffices to show that for each $g \in G$, there exist infinitely many places $v \notin \Sigma$ such that for all t_0 in a non-empty v-adic open subset of $B(K_v) \setminus D$, we have $g \in (\phi\, r_v\, \mathsf{s}_{t_0})(\mathrm{G}_{K_v})$.

For $g \in G$ fixed, construct an epimorphism $\varphi_g : \mathrm{G}_K \to \langle g \rangle$ (in other words a Galois extension E_g/K with group $\langle g \rangle$). From the Čebotarev theorem, the induced local maps $\varphi_g\, r_v : \mathrm{G}_{K_v} \to \langle g \rangle$ remain surjective for infinitely many places v of K. Furthermore, thanks to the Lang-Weil estimates, for all but finitely many of these places v, the twisted cover $\widetilde{f}^{\varphi_g} : \widetilde{X}^{\varphi_g} \to B$ (which is defined over the global field K) has good reduction at v and $\widetilde{X}^{\varphi_g}(K_v) \neq \emptyset$. The twisting lemma 3.1 concludes the argument. □

Remark 3.3. (a) This provides in particular a proof of Hilbert's irreducibility theorem.

(b) As the proof shows, finding places, possibly big, with given decomposition groups is sufficient for the Hilbert property. Unlikewise dealing with the Grunwald aspect, for which some places are fixed and the local extensions to realize do not have a global origin, requires the more precise method from [DG10] (which we explain and re-use in §4 below). Using it instead of the sole twisting lemma, better versions of corollary 3.2 can be given.

3.4. **PAC fields.** The next result, first proved in [Dèb99a] (for G-covers of $\mathbb{P}^1$), readily follows from the twisting lemma 3.1 and the definition of a PAC field (pseudo algebraically closed): a field is PAC if $V(K) \neq \emptyset$ for each geometrically irreducible variety V defined over K.

Corollary 3.4. *Every G-cover $f : X \to B$ of group G over some PAC field K has the property that every Galois extension E/K of group $H \subset G$ is the specialization of f at all points t_0 from a Zariski dense subset of $B(K) \setminus D$ (depending on E/K).*

A variant of this result for not necessarily Galois extensions can also be given; see [BS09, proposition 1.2].

3.5. **Finite fields.** The next result readily follows from the twisting lemma 3.1 and the Lang-Weil estimates.

Corollary 3.5. *Let $f : X \to B$ be a G-cover of group G and branch divisor D over some finite field $\mathbb{F}_q$. Then there is a constant c depending on G, B and D such that if $q \geq c$, then every Galois extension of $\mathbb{F}_q$ of group a cyclic subgroup $\langle g \rangle \subset G$ is the specialization of f at some point $t_0 \in B(\mathbb{F}_q) \setminus D$.*

Assume $B = \mathbb{P}^1$ for simplicity. The constant c then only depends on $|G|$ and r and one can even count the number N_C of $t_0 \in \mathbb{P}^1(\mathbb{F}_q) \setminus D$ such that the specialization of f at t_0 has a Galois group generated by some element g in a given conjugacy class $C \subset G$ [4]. From the twisting lemma 3.1, the specializations $\mathbb{F}_q(X)_{t_0}/\mathbb{F}_q$ with group $\langle g \rangle$ correspond to rational points over $\mathbb{F}_q$ on the twisted model of X. Using the Lang-Weil estimates, we obtain

$$N_C = \frac{|C|}{|G|} q + O(\sqrt{q})$$

where the constants involved in $O(...)$ depend on $|G|$ and r. Higher dimensional versions have more complicated constants. This Čebotarev theorem for function fields over finite fields first appeared in [Fri74] (in the case $B = \mathbb{P}^1$) and a more general form was given in [Eke90].

4. Rational function fields

In this section, the field K will eventually be taken to be a field $K = \kappa(x)$ of rational functions with coefficients in a field κ. We first

[4] These Galois groups are well-defined up to conjugation in G. That is why we fix the conjugacy class of g and not g itself.

recall a general result from [DG10] valid in a context containing both number fields and rational function fields.

The field K is assumed to be the quotient field of some Dedekind domain R and S is a finite set of places of K corresponding to some prime ideals in R. For every place v, the completion of K is denoted by K_v, the valuation ring by R_v, the valuation ideal by $\mathfrak{p}_v$, the residue field $R_v/\mathfrak{p}_v$ by κ_v, the order of κ_v by q_v and its characteristic by p_v.

Here is the strategy used in [DG10].

Given a Grunwald problem $(\varphi_v : \mathrm{G}_{K_v} \to G)_{v\in S}$ to solve, the general idea of our method is to first use the twisting lemma 3.1 locally, that is, to apply it for each place $v \in S$ to the G-cover $f \otimes_K K_v : X \otimes_K K_v \to \mathbb{P}^1_{K_v}$ and the homomorphism $\varphi_v : \mathrm{G}_{K_v} \to G$, and then to globalize the construction thanks to the approximation property of $\mathbb{P}^1$. The twisting lemma 3.1 reduces the first stage to finding unramified K_v-rational points on the twisted curve $\widetilde{X \otimes_K K_v}^{\varphi_v}$. This is done by first showing that under suitable assumptions, the twisted cover $\widetilde{f \otimes_K K_v}^{\varphi_v}$ has good reduction (using Grothendieck's good reduction criterion), then by finding rational points over the residue field of K_v on the reduction of $\widetilde{X \otimes_K K_v}$ (using the Lang-Weil estimates) and finally by lifting these points to unamified K_v-rational points on $\widetilde{X \otimes_K K_v}$ (using Hensel's lemma). The outcome is the following statement.

Let K, S be as above and G be a finite group.

Theorem 4.1. *Let $f : X \to \mathbb{P}^1$ be a G-cover of group G and r branch points, defined over K and satisfying the* (good-red) *condition from theorem 2.1. Assume further that for each $v \in S$, $p \not| |G|$ and that the field κ_v is either PAC or finite of order $q_v \geq c(|G|, r)$. Then we have the following Hilbert-Grunwald specialization property:*

(HGr-spec) *For every unramified Grunwald problem $(\varphi_v : \mathrm{G}_{K_v} \to G)_{v\in S}$, there exist specializations $K(X)_{t_0}/K$ of f at points $t_0 \in \mathbb{A}^1(K) \setminus \mathbf{t}$ with the property that the Galois group $\mathrm{Gal}(K(X)_{t_0}/K)$ contains a conjugate in G of each of the subgroups $\varphi_v(\mathrm{G}_{K_v}) \subset G$ $(v \in S)$. More precisely the set of all such t_0 contains a subset $\mathbb{A}^1(K) \cap \prod_{v\in S} U_v$ with $U_v \subset \mathbb{A}^1(\mathcal{O}_v)$ a coset of $\mathcal{O}_v$ modulo $\mathfrak{p}_v$ $(v \in S)$.*

Proof. The detailed proof is given in this general context in [DG10, §3], except that only the case that all residue fields κ_v are finite of order $q_v \geq c(|G|, r)$ is considered. But the other case here, for which some of the residue fields κ_v could be PAC, is easy to handle. Indeed what is needed for the proof is to be able to guarantee that rational points can be found on some variety defined over κ_v $(v \in S)$ (more specifically, it is the condition (κ-big-enough) from proposition 2.2 of [DG10] that needs to be satisfied). When the field κ_v is PAC, this is automatic. $\square$

We now consider the special case $K = \kappa(x)$ where x is an indeterminate and κ is a field that is PAC, or finite and big enough. Denote the characteristic of κ by p.

Fix a finite set of points of $\mathbb{P}^1(\kappa)$ and denote by S the set of corresponding valuations of K; denote the point corresponding to v by x_v. For each $v \in S$, fix an homomorphism $\varphi^v : \mathrm{G}_\kappa \to G$, that is, a Galois extension ε^v/κ with group contained in G. The corresponding extension $\varepsilon^v((x - x_v))/\kappa((x - x_v))$ is unramified.

Theorem 4.2. *Let $f : X \to \mathbb{P}^1$ be a $\kappa(x)$-G-cover of group G and with r branch points. Assume that $p \not| |G|$ and that the* (good-red) *condition from theorem 2.1 holds. Assume the following on the field κ: either*

(i) *κ is PAC and every finite cyclic group is a quotient of G_κ, or*

(ii) *κ is finite of order $q \geq C(|G|, r)$.*

Then the cover f has the Hilbert-Grunwald specialization property:

(HGr-spec) *There exist specializations $\kappa(x)(X)_{t_0(x)}/\kappa(x)$ of f at points $t_0(x) \in \mathbb{A}^1(\kappa(x)) \setminus \mathbf{t}$ with Galois group G and whose residue extension at $x = x_v$ is κ-isomorphic to the prescribed extension ε^v/κ ($v \in S$). Furthermore the set of such $t_0(x)$ contains a subset $\mathbb{A}^1(\kappa(x)) \cap \prod_{v \in S \cup S_0} U_v$ where each $U_v \subset \mathbb{A}^1(\kappa[[x - x_v]])$ is a coset of $\kappa[[x - x_v]]$ modulo the ideal $\langle x - x_v \rangle$ and S_0 is a finite set of finite places $v \notin S$ which can be chosen depending only on f.*

Furthermore, if $p_v \not| 6|G|$ and $q_v \geq c(G)$ ($v \in S$), then there exist a Galois extension $L/\kappa(x)$ totally split in $\kappa((x - x_v))$ ($v \in S$) and a G-cover $f : X \to \mathbb{P}^1$ of group G, defined over L that satisfies both the good reduction condition (good-red) *<u>and</u> the Hilbert-Grunwald specialization property* (HGr-spec) *with $\kappa(x)$ replaced by L.*

Proof. Theorem 4.1 can be used in the special situation considered here and so its conclusion holds true. What remains to explain in order to get the first part of theorem 4.2 is how to guarantee that the Galois groups $\mathrm{Gal}(K(X)_{t_0}/K)$ equal the whole group G. As explained in [DG10, §3.4], this can be done at the cost of throwing in more places in S. The argument which is given in [DG10] in the case K is a number field can be used in the more general situation of corollary 4.2. There is however an arithmetic condition satisfied by number fields that our field K should be here assumed to satisfy:

- *for each cyclic subgroup $H \subset G$, there exist infinitely many places v of K with κ_v PAC or finite of order $\geq C(|G|, r)$, and such that H is the Galois group of some extension of K_v.*
As the residue field of the places we consider here is κ, this condition is guaranteed by the assumption on κ.

As to the final part of the statement of theorem 4.2, the proof is the same as that of theorem 1.3 of [DG10]. There are only two minor changes. In the third step of the proof, it is the definition of PAC fields that should be used to find rational points on the κ_v-variety involved in the case κ_v is PAC (instead of the Lang-Weil estimates). It should also be recalled that as for finite fields, over a PAC field, the field of moduli of a G-cover is a field of definition [DD97, corollary 3.3]. □

References

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

[BS09] Lior Bary-Soroker. Dirichlet's theorem for polynomial rings. *Proc. Amer. Math. Soc.*, 137:73–83, 2009.

[DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers: field of moduli versus field of definition. *Annales Sci. E.N.S.*, 30:303–338, 1997.

[Dèb99a] Pierre Dèbes. Galois covers with prescribed fibers: the Beckmann-Black problem. *Ann. Scuola Norm. Sup. Pisa,* Cl. Sci. (4), 28:273–286, 1999.

[Dèb99b] Pierre Dèbes. Some arithmetic properties of algebraic covers. In *Aspects of Galois Theory*, volume 256 of *London Math. Soc. Lecture Note Series*, pages 66–84. Cambridge University Press, 1999.

[DG10] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *preprint*, 2010.

[Eic39] Martin Eichler. Zum Hilbertschen irreduzibilittssatz. *Math. Ann.*, 116:742–748, 1939.

[Eke90] Torsten Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988)1989*, volume 91 of *Progress in Mathematics*, pages 241–248. Birkhäuser, 1990.

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

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

[Ful69] William Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Annals of Math.*, 90:542–575, 1969.

[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.

[Neu79] Jürgen Neukirch. On solvable number fields. *Invent. Math.*, 53:135–164, 1979.

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

[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.

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

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