Density of specialization sets and Hasse principle in families of twisted Galois covers

(joint with Francois Legrand)

Joachim König

KAIST, Daejeon

Lille Number Theory Days, July 11th, 2019

Regular Inverse Galois problem

k a number field (especially, $k = \mathbb{Q}$), G a finite group.
An extension $E/k(t)$ is called k-regular if $E \cap \overline{k} = k$.

Regular Inverse Galois Problem

Does there exist a k-regular Galois extension $E/k(t)$ with group G, for each finite group G?
(Equivalently, does there exist a Galois cover $X \to \mathbb{P}^1$ of smooth projective curves, with group G, defined over k?)

Regular Inverse Galois problem

k a number field (especially, $k = \mathbb{Q}$), G a finite group.
An extension $E/k(t)$ is called k-regular if $E \cap \overline{k} = k$.

Regular Inverse Galois Problem

Does there exist a k-regular Galois extension $E/k(t)$ with group G, for each finite group G?
(Equivalently, does there exist a Galois cover $X \to \mathbb{P}^1$ of smooth projective curves, with group G, defined over k?)

Motivation: Positive answer to **RIGP** implies positive answer to **IGP**, by Hilbert's irreducibility theorem.
Concretely: Given $E/k(t)$ Galois with group G, there are infinitely many $t_0 \in k$ such that the **specialization** E_{t_0}/k (=residue field extension at prime $t \mapsto t_0$) has Galois group G.

Regular Inverse Galois problem

Basic question: To what extent can Hilbert's irreducibility theorem solve the inverse Galois problem over k?

Regular Inverse Galois problem

Basic question: To what extent can Hilbert's irreducibility theorem solve the inverse Galois problem over k?

Concrete questions

- Does every G-extension of k "lift" to a G-cover of k (i.e., occur as a specialization of some suitable G-cover)? (**Beckmann-Black problem**)

Regular Inverse Galois problem

Basic question: To what extent can Hilbert's irreducibility theorem solve the inverse Galois problem over k?

Concrete questions

- Does every G-extension of k "lift" to a G-cover of k (i.e., occur as a specialization of some suitable G-cover)? (**Beckmann-Black problem**)
- Is there even a cover of $\mathbb{P}^1_k$, resp., of $\mathbb{P}^d_k$ which lifts all G-extensions at once? (**"Parametric extension"**)

Regular Inverse Galois problem

Basic question: To what extent can Hilbert's irreducibility theorem solve the inverse Galois problem over k?

Concrete questions

- Does every G-extension of k "lift" to a G-cover of k (i.e., occur as a specialization of some suitable G-cover)? (**Beckmann-Black problem**)
- Is there even a cover of $\mathbb{P}^1_k$, resp., of $\mathbb{P}^d_k$ which lifts all G-extensions at once? (**"Parametric extension"**)
- More generally, given a G-cover over k: what is the structure of the set of specializations?

Examples

- $k(\sqrt{t})/k(t)$ is a parametric extension for the group C_2. It is even **generic** (i.e., parametric over all extensions of k).
- $E/\mathbb{Q}(t)$ the function field of an elliptic curve: This specializes to a quadratic field $\mathbb{Q}(\sqrt{d})$ if and only if the d-th quadratic twist of the curve has a non-trivial $\mathbb{Q}$-point.
  So this extension is not parametric. Moreover, when counting by discriminant the fields $\mathbb{Q}(\sqrt{d})$ which occur as specializations, Goldfeld's ("average rank 1/2") conjecture predicts that 50% of them occur.

Previous results

Theorem (K.-Legrand 2018, K.-Legrand-Neftin 2019)

For "many" finite groups G: There is no $\mathbb{Q}$-regular G-extension $E/k(t)$ which specializes to all G-extensions of k.

Previous results

Theorem (K.-Legrand 2018, K.-Legrand-Neftin 2019)

For "many" finite groups G: There is no $\mathbb{Q}$-regular G-extension $E/k(t)$ which specializes to all G-extensions of k.

Computational evidence suggests more: Compared with the set of all G-extensions, the set of specializations of a given regular extension seems "very small".

The Malle conjecture

Let G be a finite group, k be a number field and $B \in \mathbb{N}$. Let $N(G,k,B)$ be the number of G-extensions L/k such that the discriminant $\Delta(L/k)$ is of norm at most B.

Conjecture (Malle; 2002, 2004)

There are constants C_1 (depending on G and k) and C_2 (depending on G, k and $\epsilon > 0$) such that

$$C_1 B^{1/\alpha(G)} \leq N(G,k,B) \leq C_2 B^{1/\alpha(G)+\epsilon}.$$

Here $\alpha(G) := \frac{p-1}{p}|G|$, where p is the smallest prime divisor of $|G|$.

The Malle conjecture

Let G be a finite group, k be a number field and $B \in \mathbb{N}$. Let $N(G, k, B)$ be the number of G-extensions L/k such that the discriminant $\Delta(L/k)$ is of norm at most B.

Conjecture (Malle; 2002, 2004)

There are constants C_1 (depending on G and k) and C_2 (depending on G, k and $\epsilon > 0$) such that

$$C_1 B^{1/\alpha(G)} \leq N(G, k, B) \leq C_2 B^{1/\alpha(G)+\epsilon}.$$

Here $\alpha(G) := \frac{p-1}{p}|G|$, where p is the smallest prime divisor of $|G|$.

The conjecture is known to hold for all nilpotent groups G (but of course open in general, since it implies the inverse Galois problem over k).

Specialization and "lower bound Malle"

Theorem (Dèbes, 2017)

Let $E/k(t)$ be a k-regular G-extension. Then the number of G-extensions of k, with discriminant of norm $\leq B$, **and which arise as specializations of** *$E/k(t)$, is $\gg B^{\alpha(E)}$, where $\alpha(E)$ is an (explicitly given) positive constant depending on $E/k(t)$.*

Remarks:

- In fact, $\alpha = \beta(G)/R$, where $\beta(G)$ depends only on G and R is the number of branch points of $E/k(t)$.
- Obvious question: Can we also give a (reasonably non-trivial) **upper bound** exponent?

The *abc*-conjecture

Definition

The **radical** $rad(N)$ of a positive integer N is the product of all prime divisors of N, without multiplicities.

abc-conjecture

For every $\epsilon > 0$, there are only finitely many triples (a, b, c) of coprime positive integers with $a + b = c$, such that

$$rad(abc) \leq c^{1-\epsilon}.$$

A result about quadratic twists of hyperelliptic curves

Let C be a hyperelliptic curve over $\mathbb{Q}$, given by $Y^2 = f(T)$ ($f \in \mathbb{Z}[T]$ separable). Recall that the d-th quadratic twist C_d of C is given by $dY^2 = f(T)$.

A result about quadratic twists of hyperelliptic curves

Let C be a hyperelliptic curve over $\mathbb{Q}$, given by $Y^2 = f(T)$ ($f \in \mathbb{Z}[T]$ separable). Recall that the d-th quadratic twist C_d of C is given by $dY^2 = f(T)$.

Theorem (Granville, 2007)

Assume that the abc-conjecture holds.
Let C be a hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$. Then the number of squarefree integers $d \in [-N, ..., N]$ such that the d-th quadratic twist C_d of C has a non-trivial rational point is asymptotically smaller than $N^{1/(g-1)+\epsilon}$.
In particular, if $g \geq 3$, the density of squarefree integers such that C_d has a non-trivial rational point is 0.

A result about quadratic twists of hyperelliptic curves

- Translation into specialization of Galois covers: Given $C : Y^2 = f(T)$, with $f \in \mathbb{Z}[T]$ separable, C_d has a non-trivial rational point if and only if the hyperelliptic (degree-2) cover $C \to \mathbb{P}^1$ has the field $\mathbb{Q}(\sqrt{d})$ as a specialization.
- In total, there are of course $\Omega(N)$ quadratic fields of discriminant (of absolute value) $\leq N$.
- So Granville's result says that (conditionally on abc), a hyperelliptic curve of genus $g \geq 3$ has "very few" quadratic fields as specializations. In particular, the proportion of such fields is 0.

Twists of Galois covers

Let $f : X \to \mathbb{P}^1$ be a Galois cover with group G, defined over k. Let $\varphi : Gal_k \to G$ be a continuous epimorphism (yielding a G-extension F/k). Then there exists a cover $f^\varphi : \tilde{X} \to \mathbb{P}^1$, defined over k (but not necessarily Galois), with the following properties:

- A fiber $(f^\varphi)^{-1}(t_0)$ contains a rational point if and only if the specialization of f at t_0 equals φ.
- After extension of constants from k to F, the covers f^φ and f become isomorphic.

f^φ is called the **twisted cover** of f by φ.
Special case: If $G = C_2$ and $f : C \to \mathbb{P}^1_{\mathbb{Q}}$ is a hyperelliptic cover, then the twist of f by (the epimorphism corresponding to) $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ yields the d-th quadratic twist of C.

Rational points on twisted covers

Theorem (K., Legrand (submitted, 2019))

Let $f : X \to \mathbb{P}^1$ be a Galois cover defined over $\mathbb{Q}$, with group G, with R branch points. If the abc-conjecture holds, then the number of distinct specializations $L/\mathbb{Q}$ of f of discriminant $\leq B$ is asymptotically bounded from above by

$$B^{\frac{2}{\tilde{\alpha}(f)(R-4)}+\epsilon}.$$

Here $\tilde{\alpha}(f) := \frac{p-1}{p}|G|$, where p is the smallest prime divisor of any ramification index of f.

(In particular, as soon as $R \geq 5$, we have an upper bound $B^{\gamma(G)/R}$, where $\gamma(G)$ depends only on G.)

Outline of proof

Important tool: Ramification in specializations of covers:

Theorem (Beckmann, 1991)

Let $f : X \to \mathbb{P}^1$ be a Galois cover defined over a number field k, with Galois group G, function field extension $E/k(t)$, and with branch points $t_1, \dots, t_r \in \overline{k}$. Then there is a finite set $\mathcal{S}$ of primes of k ("bad primes") such that for all primes $p \notin \mathcal{S}$, the following holds:
p can only ramify in E_{t_0}/k of t_0 and t_i meet modulo p (for some $i \in \{1, \dots, r\}$), and in this case, the inertia group at p in E_{t_0}/k is generated by $x^{\nu_p(t_0 - t_i)}$, where x generates an inertia group at $t \mapsto t_i$ in $E/k(t)$.

Outline of proof

- Let $t_1, ..., t_r \in \mathbb{P}^1(\overline{\mathbb{Q}})$ be the branch points of f and let $F(X,Y) = \prod_{i=1}^{r}(X - t_i Y) \in \mathbb{Z}[X,Y]$ the homogenized product of their minimal polynomials ($\deg(F) = R$).
  Let $t_0 = \frac{r}{s} \in \mathbb{Q}$, $n := \max\{|r|, |s|\}$.
- By Beckmann's theorem, the specialization $f_{t_0}/\mathbb{Q}$ is ramified at most at the prime divisors of $F(r,s)$, and possibly some fixed finite set ("bad primes").
  Conversely, if a "good" prime q divides $F(r,s)$, but q^p does not divide, then q is ramified in $f_{t_0}/\mathbb{Q}$, and with ramification index at least p.
  Well-known discriminant formula then gives $|\Delta(f_{t_0}/\mathbb{Q})| > C \cdot (\prod q)^{\tilde{\alpha}(f)}$ (with some constant $C > 0$), where the product is over all primes dividing $F(r,s)$ such that q^p does not divide.

Outline of proof

- Now use a consequence of the abc-conjecture:

Theorem (Langevin, Granville)

Let $F(X, Y)$ be a homogeneous polynomial of degree d over $\mathbb{Z}$, and let $\epsilon > 0$. Then

$$rad(F(r,s)) \geq \max\{|r|,|s|\}^{d-2-\epsilon}$$

for all but finitely many coprime $r, s \in \mathbb{Z}$.

- This gives bounds from below on the product P of all primes which divide $F(r,s)$ to a power less than p, namely

$$P \geq n^{R-2-2/(p-1)-\epsilon} (\geq n^{R-4-\epsilon}).$$

- Substituting in the above discriminant formula, with some elementary manipulations, gives the assertion.

Some consequences

Corollary

Assume the abc-conjecture and the Malle conjecture for the group G. If $f : X \to \mathbb{P}^1$ is a Galois cover with group G over $\mathbb{Q}$, with at least 7 branch points, then f cannot be parametric. More precisely, the proportion of G-extensions of $\mathbb{Q}$ which arise as specializations from f converges to 0 (when counted by discriminant).

Some consequences

Corollary

Assume the abc-conjecture and the Malle conjecture for the group G. If $f : X \to \mathbb{P}^1$ is a Galois cover with group G over $\mathbb{Q}$, with at least 7 branch points, then f cannot be parametric. More precisely, the proportion of G-extensions of $\mathbb{Q}$ which arise as specializations from f converges to 0 (when counted by discriminant).
Worded differently, the set of all twists of f (by G-extensions of $\mathbb{Q}$) which have an unramified rational point is of density 0 (when counted by discriminant).

Some consequences

Corollary

Assume the abc-conjecture and the Malle conjecture for the group G. If $f : X \to \mathbb{P}^1$ is a Galois cover with group G over $\mathbb{Q}$, with at least 7 branch points, then f cannot be parametric. More precisely, the proportion of G-extensions of $\mathbb{Q}$ which arise as specializations from f converges to 0 (when counted by discriminant).
Worded differently, the set of all twists of f (by G-extensions of $\mathbb{Q}$) which have an unramified rational point is of density 0 (when counted by discriminant).

In particular, the case $G = C_2$ regains Granville's result on twists of hyperelliptic curves.

Some consequences

Combination with the lower bound results (Dèbes) yield that two G-covers f_1, f_2 with "sufficiently different" branch point number must have different sets of specializations (conditional on abc).

Corollary

Let G be a finite group. Assume that the abc-conjecture holds. Then there exists a constant $N \in \mathbb{N}$ (depending on G) such that for every Galois cover $f : X \to \mathbb{P}^1$, defined over $\mathbb{Q}$ and with at least N branch points, the following holds: The proportion of G-extensions of $\mathbb{Q}$ which arise as specializations from f converges to 0 (when counted by discriminant).

What we expect vs what we know

Conjecture I

Let $f : X \to \mathbb{P}^1$ be an arbitrary Galois cover with group G over $\mathbb{Q}$ (or indeed, over any number field), of genus ≥ 2. Then G specializes to 0% of all G-extensions of $\mathbb{Q}$.

Our evidence:

- Conditional on abc, we show Conjecture I, with the bound $g \geq 2$ replaced by $g \geq 2|G| - 1$.
- In joint work with Dèbes, Legrand and Neftin, we showed (unconditionally!) a **geometric analog** of this conjecture, where the field $\mathbb{Q}$ is replaced by $\mathbb{C}(t)$, the notion of specialization is replaced by "rational pullback", and the "density" notion is replaced by a notion in the Zariski topology on moduli spaces of Galois covers.

What we expect vs what we know

Definition

Let $f : X \to \mathbb{P}^1$ be a connected cover, given by an equation $F(t, X) = 0$. Let $T(U) \in \mathbb{C}(U)$ be a non-constant rational function. Then the cover f^U given by $F(T(U), X) = 0$ is called the rational pullback of f by $T(U)$.

Pullback can be viewed as specialization from $\mathbb{C}(U)(T)$ into $\mathbb{C}(U)$, where the initial cover was **isotrivial**.

Definition (Hurwitz space)

Let $\underline{C}$ be a class vector of length r in the group G. The set of all Galois covers of $\mathbb{P}^1$ with ramification type $\underline{C}$ is called the Hurwitz space $\mathcal{H}(G, \underline{C})$. It is a finite (possibly empty) union of r-dimensional varieties over $\mathbb{C}$.

(Recall:) Conjecture I

Let $f : X \to \mathbb{P}^1$ be an arbitrary Galois cover with group G over $\mathbb{Q}$ (or indeed, over any number field), of genus ≥ 2. Then G specializes to 0% of all G-extensions of $\mathbb{Q}$.

Theorem (Dèbes-K.-Legrand-Neftin (2018))

Let $g \geq 2$, and let $\mathcal{S}_g$ be **any** *set of genus-g covers $X \to \mathbb{P}^1$ with group G. Then $\mathcal{S}_g$ pulls back to 0% of all G-covers in the following sense: Given any sufficiently long class vector $\underline{C}$ of G with non-empty Hurwitz space, the set of all covers in $\mathcal{H}(G, \underline{C})$ which are rational pullbacks from $\mathcal{S}_g$ (by* **any** *rational function) is contained in the complement of a Zariski-dense open subset of $\mathcal{H}(G, \underline{C})$.*

What we expect vs what we know

Conjecture II

Let f, g be two Galois covers of $\mathbb{P}^1$ with group G, defined over $\mathbb{Q}$, of genus ≥ 2, and not "equivalent". Then f and g have different sets of specializations (in other words, the set of specializations identifies the cover!).

- Once again, we showed a weaker statement: If f and g have "sufficiently different" branch point numbers, then their specialization sets are different.
- The "pullback" analog of this conjecture is trivial: Since f is a pullback of itself, f and g could only have the same set of pullbacks if they are mutual pullbacks of each other. Riemann-Hurwitz genus formula shows that such a thing is impossible, unless the pullback maps are trivial.

Hasse principle

Hasse principle (for curves)

Let C be a curve over $\mathbb{Q}$ with a non-singular point over every $\mathbb{Q}_p$ (including the infinite prime). Then C has a rational point.

- Hasse principle is known to hold for some important special cases (e.g., quadratic forms), but fails in general.
- E.g., Bhargava et al. have shown that a positive proportion of hyperelliptic curves of a fixed genus fail the Hasse principle.

Hasse principle

Hasse principle (for covers)

Let f be a Galois cover over $\mathbb{Q}$ with an unramified $\mathbb{Q}_p$-point for all p. Then f has an unramified rational point.

Question

How many twists of a given Galois cover fail the above Hasse principle, i.e., have an (unramified) point everywhere locally, but no (unramified) $\mathbb{Q}$-point?

Hasse principle

Hasse principle (for covers)

Let f be a Galois cover over $\mathbb{Q}$ with an unramified $\mathbb{Q}_p$-point for all p. Then f has an unramified rational point.

Question

How many twists of a given Galois cover fail the above Hasse principle, i.e., have an (unramified) point everywhere locally, but no (unramified) $\mathbb{Q}$-point?

- In the hyperelliptic case: Conditional on abc, infinitely many quadratic twists of a given genus ≥ 3 hyperelliptic curve violate the Hasse principle (Clark, Watson 2018).

An unconditional result:

Theorem (K., in preparation)

Let G be a finite abelian, but non-cyclic group, and k be a number field. Let f be a G-cover of $\mathbb{P}^1$, defined over k. Then the proportion of twists of f by G-extensions of k which do not have a point everywhere locally equals 100%, when extensions are counted by **conductor***.*
In other words, for 100% of G-extensions L/k, there is a prime p of k such that f does not specialize to L/k, even after base field extension to k_p.

So Hasse principle holds (but trivially) for 100% of twists. However:

Theorem (K.-Legrand (2019))

Let G be an abelian group, f be a G-cover of $\mathbb{P}^1$, defined over $\mathbb{Q}$, with ≥ 7 branch points. Conditional on abc, 0% of those twists of f which have a point everywhere locally, also have a $\mathbb{Q}$-point.

Remarks:

- The result remains (essentially) true for arbitrary groups G with non-trivial center, under some technical extra assumptions of the cover f.
- In particular, we can generate a huge amount of curves failing the Hasse principle, via twists, starting from a "relatively" general curve.

Idea of proof

- Need to count how many G-extensions $L/\mathbb{Q}$ have the following property: For every prime p, there is a specialization of f which locally at p behaves the same as $L/\mathbb{Q}$.
- For (most) *unramified* primes of $L/\mathbb{Q}$, the following observation suffices: If p is sufficiently large (depending on f), then every unramified behaviour occurs at p in a suitable specialization of f. This is due to:

Theorem (Dèbes, Ghazi (2012))

Let $f : X \to \mathbb{P}^1$ be a G-cover defined over $\mathbb{Q}$. Then for every prime p outside some finite set S_0 (depending only on E) and for every **unramified** *extension $K_p/\mathbb{Q}_p$ with Galois group embedding into G, there are specializations of f whose completion at p equals $K_p/\mathbb{Q}_p$.*

Idea of proof

- So for sufficiently **large** primes p, we always have a $\mathbb{Q}_p$-point on the twist of f by $L/\mathbb{Q}$, as soon as p is unramified in L.
- If p is (large and) ramified in L, then we use (a special case) of a recent result on local behaviour in specializations:

Theorem ((Special case of) K.-Legrand-Neftin, 2019)

Let $f : X \to \mathbb{P}^1$ be a G-cover defined over $\mathbb{Q}$, and $t_i \in \mathbb{P}^1(\overline{\mathbb{Q}})$ be a branch point of f, with inertia group $I \leq G$. Let p be a prime which splits completely in the residue extension of f at t_i. Then every I-extension of $\mathbb{Q}_p$ is a specialization of f $(\otimes\mathbb{Q}_p)$.

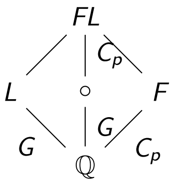
- If p is **small**, then we know less. But at least there is **some** G-extension $L/\mathbb{Q}$ whose twist as a $\mathbb{Q}_p$-point.

Idea of proof

- Therefore, it suffices to estimate the number of G-extensions with the following two conditions:
  i) For some fixed finite set S_0 of primes p, the local behaviour at p is prescribed (according to some specialization of f).
  ii) All further **ramified primes** are in some prescribed positive density set (namely, in the set of primes that ramify in some specialization of f, and completely split in some prescribed number field), and with a prescribed inertia group.

Idea of proof

- Our idea is now to grab **one** such G-extension (namely, a suitable specialization of f), and then change it "slightly" by twisting with a suitable C_p-extension ($C_p \leq Z(G)$), say $F/\mathbb{Q}$, without destroying the local conditions (i.e., without altering the behaviour at the set S_0, and without introducing "forbidden" ramified primes).
- These C_p-extensions can be constructed very explicitly inside certain cyclotomic field $\mathbb{Q}(\zeta_q)$ (introducing only one ramified prime q at a time!), and their discriminant is "under control".



Idea of proof

- Then it can be shown that the proportion of “good” G-extensions of discriminant $\leq N$ (i.e., such that the corresponding twist of f has a point everywhere locally) is at least $1/($ polylogarithmic expression in $N)$.
- On the other hand, due to our assumptions on f, and conditionally on abc, the proportion of twists of f with a **rational** point is $< N^{\alpha}$, for some $\alpha > 0$.