# On the set of specializations of a Galois cover

Joachim König

KAIST, Daejeon

Bar Ilan University, June 19th 2019

1 Background
- The inverse Galois problem and its variants
- Specialization sets

2 Specialization sets: The local point of view
- The Grunwald Problem
- The Admissibility Problem

3 The global point of view

1 Background
- The inverse Galois problem and its variants
- Specialization sets

2 Specialization sets: The local point of view
- The Grunwald Problem
- The Admissibility Problem

3 The global point of view

# General background: The inverse Galois problem

**IGP**

Given a finite group $G$, is there a Galois extension $K/\mathbb{Q}$ with Galois group $G$?

- The general "hope" is that the answer to this question is not just "yes", but rather "yes, and for systematic reasons"!

# General background: RIGP and specializations

One particular "systematic reason" for $G$ to occur as a Galois group over $\mathbb{Q}$:

## Regular IGP (RIGP)

Given a finite group $G$, is there a $\mathbb{Q}$-**regular** $G$-extension $E/\mathbb{Q}(t)$ (i.e. $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$) ?

- Hilbert 1892: If RIGP holds for $G$, then so does IGP. Reason: **Specialization**.
- More precisely, there are then infinitely many $t_0 \in \mathbb{Q}$ such that the **residue extension** $E_{t_0}/\mathbb{Q}$ still has group $G$.

# General background: RIGP and specializations

- At first view, RIGP might look harder than IGP. But advantage: Galois theory over $\mathbb{Q}(t)$ allows the use of methods from topology, geometry, complex analysis.
- In particular, there is a **1-to-1 correspondence** between **regular Galois extensions** $E/\mathbb{Q}(t)$ and **Galois covers** $f : X \to \mathbb{P}^1$ **of compact Riemann surfaces / algebraic curves** (defined over $\mathbb{Q}$).

# General background: The inverse Galois problem with local restrictions

Another "systematic" approach to the inverse Galois problem:
Galois theory over the $p$-adic fields $\mathbb{Q}_p \supset \mathbb{Q}$ is much better understood than over $\mathbb{Q}$.
**Hope**: Galois extensions of $\mathbb{Q}$ with prescribed Galois group can be constructed from extensions of $\mathbb{Q}_p$, $p \in \mathbb{P}$, fulfilling certain conditions.

## IGP with local restrictions

Given a finite group $G$, a set $S$ of primes and for each $p \in S$ a "**local condition**" $P(p)$.
Can we then find a Galois extension $K/\mathbb{Q}$ with group $G$ fulfilling the conditions $P(p)$ $p \in S$?

- Answer depends on "reasonable" choice of set $S$ and the local conditions $P(p)$ (e.g., if $S$ is the set of **all** primes, then general answer will be "no" for "trivial" reasons.

# Local conditions, inertia and decomposition groups

**Some more background facts**:

- Given a Galois extension $K/\mathbb{Q}$ with group $G$, the extension $K \cdot \mathbb{Q}_p/\mathbb{Q}_p$ is also Galois group, with group embedding into $G$. This group is called the **decomposition group** of $K/\mathbb{Q}$ at $p$.
- Furthermore, $K_p := K \cdot \mathbb{Q}_p/\mathbb{Q}_p$ contains a unique "maximal unramified extension" $K_p^{ur}$. The Galois group of $K_p/K_p^{ur}$ is called the **inertia group** of $K/\mathbb{Q}$ at $p$ (a subgroup of the decomposition group).
- Given $K/\mathbb{Q}$, the inertia group at all but finitely many primes is trivial ("unramified primes").
- A corresponding theory of completion, ramification etc. also exists for function field extensions $E/\mathbb{Q}(t)$ (rather than number field extensions $K/\mathbb{Q}$), with **branch points** taking the roles of **primes**.

# Local conditions, inertia and decomposition groups

So what do we mean by "local condition" $P(p)$?
**Answer**: This is any prescribed property which should be fulfilled by the **completion** $K \cdot \mathbb{Q}_p/\mathbb{Q}_p$ of the extension $K/\mathbb{Q}$.

**Examples of local conditions**:

- We might simply demand the completion $K_p := K \cdot \mathbb{Q}_p/\mathbb{Q}_p$ to be isomorphic to some prescribed extension.
- Somewhat weaker: we might prescribe the **decomposition group** at $p$.
- Or we might prescribe the **inertia group** at $p$.
- Or combinations of the above, etc. etc.

# General background: Grunwald problem

- If the set $S$ is finite, the corresponding IGP with local restrictions is called a **Grunwald problem**.

**Definition (Grunwald problem)**

Given a group $G$, a finite set $S$ of primes, and for each $p \in S$ a local condition $P(p)$ (e.g., a prescribed extension of $\mathbb{Q}_p$ with group embedding into $G$): is there a $G$-extension of $\mathbb{Q}$ satisfying all these local conditions?

- Here, the expected answer to the above question is (usually) "yes".
- A positive answer is known classically for abelian groups (Grunwald-Wang theorem), and very recently for the larger class of **supersolvable** groups (Harpaz-Wittenberg).

# Specialization sets: General set-up

- Let $E/\mathbb{Q}(t)$ be a regular Galois extension with group $G$.
- For a rational number $t_0$, denote by $E_{t_0}/\mathbb{Q}$ the "residue extension at $t_0$".
  If $E/\mathbb{Q}(t)$ is the splitting field of a polynomial $f(t, X)$, just think of $E_{t_0}/\mathbb{Q}$ as the splitting field of $f(t_0, X)$!
- $\mathcal{S}(E) := \{K/\mathbb{Q} \mid K/\mathbb{Q} = E_{t_0}/\mathbb{Q}$ for some $t_0 \in \mathbb{Q}\}$.
- Hilbert says that $\mathcal{S}(E)$ contains many $G$-extensions of $\mathbb{Q}$. We (often) restrict to counting only the extensions inside $\mathcal{S}(E)$ which have group $G$, and denote that set by $\mathcal{S}(E; G)$.

- A natural question: How "big" exactly is the set $\mathcal{S}(E;G)$ compared to the set of **all** $G$-extensions of $\mathbb{Q}$? In particular, a "greedy" question is

**Question 1**

Is the set $\mathcal{S}(E;G)$ equal to the set of **all** $G$-extensions of $\mathbb{Q}$?

- In particular, a natural question is: Can this specialization approach also be used to solve IGP with local restrictions? I.e.,

**Question 2**

Given an instance of IGP with local restrictions for $G$ (e.g., "Grunwald problem"), can we solve it using only extensions from the specialization set $\mathcal{S}(E;G)$?

# Some warm-up examples

In the following, take $G = C_2$, i.e., **quadratic** extensions.

- Let $E/\mathbb{Q}(t) = \mathbb{Q}(\sqrt{t})/\mathbb{Q}(t)$. Then $\mathcal{S}(E; G)$ is the set of **all** quadratic extensions of $\mathbb{Q}$.
- Let $E/\mathbb{Q}(t)$ the function field extension of an elliptic curve over $\mathbb{Q}$. Then $\mathcal{S}(E; G)$ contains infinitely many quadratic extensions of $\mathbb{Q}$, but it also misses infinitely many. Goldfeld's conjecture predicts that it contains exactly 50 percent of all quadratic extensions (with the appropriate way of counting).
- Let $E/\mathbb{Q}(t) = \mathbb{Q}(\sqrt{t^2+1})/\mathbb{Q}$. Since $t^2+1$ is always positive, $\mathcal{S}(E; G)$ cannot contain any **imaginary-quadratic** extensions of $\mathbb{Q}$. (This is an example of a **local condition** that cannot be satisfied: the completion at the prime $p = \infty$ is always the trivial extension $\mathbb{R}/\mathbb{R}$, never the extension $\mathbb{C}/\mathbb{R}$).

So the questions 1 and 2 above were indeed too greedy, and we need to reformulate in a more modest way:

**Question 1'**

Does there **exist** a $G$-extension $E/\mathbb{Q}(t)$ whose specialization set $\mathcal{S}(E;G)$ equals the set of all $G$-extensions of $\mathbb{Q}$? ("Parametricity problem")

( First Answer (K.-Legrand (2018), K.-Legrand-Neftin (2019)): For many $G$, still "no".)

**Question 2'**

Does there **exist** a $G$-extension $E/\mathbb{Q}(t)$ whose specialization set fully solves a given instance of IGP with local restrictions for $G$ (e.g., Grunwald problem)?

1 Background
- The inverse Galois problem and its variants
- Specialization sets

2 Specialization sets: The local point of view
- The Grunwald Problem
- The Admissibility Problem

3 The global point of view

# Specialization sets: the local point of view

A more systematic reason why in general the set $\mathcal{S}(E;G)$ will not contain all $G$-extensions comes from the investigation of the behaviour of specializations $E_{t_0}/\mathbb{Q}$, viewed over $\mathbb{Q}_p$. The two main results are (in simplified form):

**Theorem (Beckmann, 1991)**

*Let $E/\mathbb{Q}(t)$ be $\mathbb{Q}$-regular, $t_0$ be a rational number, and $p$ be a prime number (not in some finite exceptional set). Then either $p$ is unramified in $E/\mathbb{Q}(t)$, or its* **ramification** *behaviour can be "read off" from the ramification behaviour of some branch point of $E/\mathbb{Q}(t)$.*

*Explicitly, if $\langle x\rangle$ is the inertia group at a branch point $t_i \in \overline{\mathbb{Q}}$, $f(X,Y) \in \mathbb{Z}[X,Y]$ is the (homogenized) minimal polynomial of $t_i$, and $t_0 = a/b \in \mathbb{Q}$ is a specialization value such that $f(a,b)$ is strictly divisible by $p$, then the inertia group at $p$ in $E_{t_0}/\mathbb{Q}$ is also $\langle x\rangle$*

# Specialization sets: the local point of view

**Theorem (K-Legrand-Neftin, 2019)**

*Let $E/\mathbb{Q}(t)$ be $\mathbb{Q}$-regular, $t_0$ be a rational number, and $p$ be a prime number (not in some finite exceptional set). Then either $p$ is unramified in $E/\mathbb{Q}(t)$, or the* **decomposition group** *at $p$ can be "read off" from the decomposition group / the residue extension at some branch point of $E/\mathbb{Q}(t)$.*

*Explicitly, if $\langle x \rangle$ is the inertia group at a branch point $t_i \in \overline{\mathbb{Q}}$, $F/K$ is the residue extension of $E/\mathbb{Q}(t)$ at $t_i$, $f(X,Y) \in \mathbb{Z}[X,Y]$ is the (homogenized) minimal polynomial of $t_i$, and $t_0 = a/b \in \mathbb{Q}$ is a specialization value such that $f(a,b)$ is strictly divisible by $p$, then the inertia group at $p$ in $E_{t_0}/\mathbb{Q}$ is generated by. $\langle x \rangle$ and $Frob_p(F/K)$.*

# Grunwald problems and specialization

A partial **positive** result:

**Theorem (Dèbes-Ghazi, 2012)**

*Given a $G$-extension $E/\mathbb{Q}(t)$ and any finite set of primes $S$, disjoint from some fixed finite set ("bad primes of $E$"), the set $\mathcal{S}(E;G)$ contains solutions to all* **unramified** *Grunwald problems for $G$ on $S$ (i.e., where the prescribed local extensions are all unramified extensions).*

A **negative** result:

**Theorem (K.-Legrand-Neftin (2019))**

*If $G$ contains any non-cyclic abelian subgroup, then there is* **no** *$G$-extension $E/\mathbb{Q}(t)$ whose specialization set provides solutions to* **all** *Grunwald problems for $G$!*

# $\mathbb{Q}$-admissibility

**Definition (Admissibility)**

A finite group $G$ is called $K$-admissible if there exists a division algebra $D \supset K$, central over $K$, and a maximal subfield $F \subset D$ which is Galois over $K$ with group $G$.

**Theorem ((Consequence of) Brauer-Hasse-Noether)**

*Cyclic groups are $\mathbb{Q}$-admissible.*

**Theorem (Schacher, 1968)**

*A $\mathbb{Q}$-admissible group $G$ has to be* **Sylow-metacyclic**, *i.e., all Sylow groups have to be extensions of a cyclic group by a cyclic group.*

# $\mathbb{Q}$-admissibility

**Conjecture**

All Sylow-metacyclic groups are $\mathbb{Q}$-admissible.

- The conjecture has been shown for solvable groups (Sonn, 1980s), and for some isolated non-solvable groups such as $PSL_2(7)$, $PSL_2(11)$, $M_{11}$.
- It was noted already by Schacher that to show the conjecture for a given group $G$, it suffices to find a $G$-extension $F/\mathbb{Q}$ containing full Sylow subgroups as decomposition groups (at suitable primes).
- If the Sylow subgroup is **cyclic**, then this comes for free ("Chebotarev density theorem")

# $\mathbb{Q}$-admissibility of projective linear groups

**Theorem (K-Legrand-Neftin, 2019)**

*All groups $G = PSL_2(p)$ and $G = PGL_2(p)$ with $p \equiv 3$ or $5$ mod $8$ are $\mathbb{Q}$-admissible. More precisely, there are infinitely many linearly disjoint admissible $G$-extensions $F/\mathbb{Q}$, and they can be chosen as specializations of a single $\mathbb{Q}$-regular $G$-extension.*

**Proof.**

From Schacher's criteria, and our own results on decomposition groups in specializations, we only needed to find a realization of $PSL_2(p)$ (resp. $PGL_2(p)$) over $\mathbb{Q}(t)$ such that the full 2-Sylow subgroup $C_2 \times C_2$ (resp., $D_4$) is contained in the decomposition group at some branch point. Such extensions were available in the literature (although the property had not been noticed or used). □

1 Background
- The inverse Galois problem and its variants
- Specialization sets

2 Specialization sets: The local point of view
- The Grunwald Problem
- The Admissibility Problem

3 The global point of view

# Measuring the size of specialization sets

- Recall that a natural way to count field extensions $F/\mathbb{Q}$ is by their discriminant $\Delta(F) \in \mathbb{Z}$.
  E.g., when counting Galois extensions with group $G$, it makes sense to consider

$$\mathcal{N}(G, B) := |\{F/\mathbb{Q} \mid Gal(F/\mathbb{Q}) = G, |\Delta(F)| \leq B\}|.$$

- This number is always finite for a fixed $B$ (Hermite). One may then consider the asymptotic behavior of $\mathcal{N}(G, B)$ as $B \to \infty$.
- In our treatment of specialization sets, it makes sense to define similarly

$$\mathcal{N}(G, B, E) := |\{F/\mathbb{Q} \mid Gal(F/\mathbb{Q}) = G, |\Delta(F)| \leq B, F/\mathbb{Q} = E_{t_0}/\mathbb{Q}$$
$$\text{for some } t_0 \in \mathbb{Q}\}|.$$

# Counting specializations: the global point of view

**Theorem (K.-Legrand, 2019)**

*Assume the abc-conjecture. Let $E/\mathbb{Q}(t)$ be a $\mathbb{Q}$-regular $G$-extension with $r$ branch points. Then*

$$\mathcal{N}(G, B, E) \leq B^{O(1/r)},$$

*with the implied constant in the exponent depending only on $G$.*

- In particular, the larger the branch point number, the smaller the set of specializations will tend to be.
- Roughly speaking, increasing the branch point number increases the **genus** of $E$. So covers of large genus will tend to have small specialization sets.

(Recall:)

**abc-conjecture**

Denote by $rad(N)$ the product of all prime divisors of an integer $N$ (without multiplicities). Then for any $\epsilon > 0$, there exists a constant $C > 0$ such that for any triple of integers $a, b, c$ with $a + b = c$, one has

$$rad(abc) \geq C \cdot c^{1-\epsilon}.$$

A proof has been announced by Mochizuki, but as of 2019, does not seem to be accepted.

# Counting $G$-extensions: The Malle conjecture

## Conjecture (Malle, 2002)

Let $G$ be a finite group. Then there exists a positive constant $\alpha(G) > 0$ such that number $\mathcal{N}(G, B)$ of $G$-extensions of $\mathbb{Q}$ with discriminant $|\Delta| \leq B$ is asymptotically between $B^{\alpha(G)}$ and $B^{\alpha(G)+\epsilon}$ (for any $\epsilon > 0$) as $B \to \infty$.

- Explicitly, the exponent $\alpha(G)$ is defined as $\frac{p}{(p-1)|G|}$, where $p$ is the smallest prime divisor of $|G|$.
- Easy example: If $G = C_2$, then the conjecture says there should be roughly $B^1$ quadratic extensions of discriminant up to $B$, and that is indeed true:
  There are "roughly" $B$ squarefree numbers $d \leq B$, and for each of them, the discriminant of $\mathbb{Q}(\sqrt{d})$ is "roughly" $d$.
- While the conjecture is wide-open in general (stronger than IGP!), it is solved for certain classes of groups, e.g. abelian groups, or more generally nilpotent groups.

- Compare the two asymptotics:

$$\mathcal{N}(G,B) \gg B^{\alpha(G)}$$

for the set of all $G$-extensions, vs.

$$\mathcal{N}(G,B,E) \ll B^{\beta(G)/r}$$

for the set of all specializations of $E/\mathbb{Q}(t)$ with $r$ branch points.

- Consequence: As soon as $r$ is too large, the ratio $\frac{\mathcal{N}(G,B,E)}{\mathcal{N}(G,B)}$ will converge to 0 as $B \to \infty$. In other words, the specialization set of $E$ is tiny compared to the set of all $G$-extensions.
- Our precise bounds are actually accurate enough to give this conclusion for rather small $r$, e.g. **always** for $r \geq 7$, and for some groups $G$ even for smaller $r$. Since there are group-theoretical lower bounds for the branch point number of a $G$-extension (with given $G$), this often means that **every** $G$-extension $E/\mathbb{Q}(t)$ has a tiny specialization set (conditional on abc-conjecture, and possibly Malle conjecture).

# Lower and upper bounds for the size of a specialization set

Compare also the following (weak version of a) result by Dèbes (2017) - (or Dvornicich-Zannier, Bilu,, ...):

**Theorem**

*If $E/\mathbb{Q}(T)$ is any $\mathbb{Q}$-regular $G$-extension with $r$ branch points, then $\mathcal{N}(G,B,E) \gg B^{\gamma(G)/r}$ for* **some** *positive constant $\gamma(G)$.*

In total, (conditional on abc-conjecture), one has

$$B^{\gamma(G)/r} \ll \mathcal{N}(G,B,E) \ll B^{\beta(G)/r}.$$

# Summary

- Regarding the general (global) question "How large is the specialization set of a regular extension $E/\mathbb{Q}(T)$ compared to the set of all $G$-extensions, our answer is: "Usually, quite small". Concretely, we conjecture

**Conjecture (K.-Legrand, 2019)**

$$\lim_{B\to\infty} \frac{\mathcal{N}(G,B,E)}{\mathcal{N}(G,B)} = 0,$$

as long as $E$ is of genus $\geq 2$ (i.e., as long as the function field extension does not belong to a rational or an elliptic curve).

Note that very few Galois extensions are of genus 0 or 1.

# Summary

- Regarding the general (local) question " How many Grunwald problems can be solved via the specialization of a given regular extension $E/\mathbb{Q}(T)$, our answer is again "Usually, quite few of them", although now "few" is not quite as small as in the first problem.

The logical next step is then to move from extensions $E/\mathbb{Q}(T)$ with just one parameter $T$ (corresponding to function fields of **curves**) to extensions with two or more parameters (function fields of surfaces, etc.)

Then, estimating the size of specialization sets in general becomes much harder.

# Summary

At least, we may ask the analog of the same questions as above in general:

- **Question 1**: Given $G$ and an integer $d \in \mathbb{N}$, is there a $G$-extension of $\mathbb{Q}(T_1, \ldots, T_d)$ whose specialization set contains all $G$-extensions of $\mathbb{Q}$?
- We call the smallest such $d$ the **parametric dimension** of $G$ (since it is the minimal dimension of a covering of varieties which **parameterizes** all $G$-extensions).
- **Question 2**: Given $G$ and an integer $d \in \mathbb{N}$, is there a $G$-extension of $\mathbb{Q}(T_1, \ldots, T_d)$ whose specialization set contains solutions to all Grunwald problems for $G$ (maybe, outside of finitely many primes)?
- We call the smallest such $d$ the **local dimension** of $G$.

# Summary

- Regarding "parametric dimension": This is bounded from above by the related (and well-investigated) notion of **generic dimension**. It is plausible (although evidence is scarce) that more often than not, the two are actually equal. In particular, it should be expected that for "many" groups, specialization sets of $G$-extensions $E/\mathbb{Q}(S,T)$ (function fields of surfaces) are still "small".
- On the other hand, for the "local" problem (solving Grunwald problems for $G$ via specialization), there might be good reason to expect that one can in fact solve all of them via specialization of some $G$-extension$E/\mathbb{Q}(S,T)$.
- In our terminology: The **local dimension** of a finite group $G$ may be expected to always be $\leq 2$.

## Question

Given $G$, is it true that the local dimension of $G$ is $\leq 2$?

Evidence so far:

- At least, the "hard obstructions", which showed that for most $G$ the local dimension is $> 1$, vanish (in a well-defined sense) for 2-dimensional covers, i.e., the assertion can be reduced to a kind of "strong inverse Galois problem" over $\mathbb{Q}(S, T)$ with prescribed decomposition group structure.
- For certain special classes of groups (including groups with a generic extension?), we can show the assertion.
  Note that by Saltman (1982), groups with a generic extension have solutions to all Grunwald problems (i.e., local dimension $< \infty$). We claim that we can actually collect all these solutions as residue extensions of some **surface**.

# Thank you for your attention!