On the arithmetic-geometric complexity of the Grunwald problem

Joachim König
(KNUE, Cheongju)

France-Korea Number Theory Webinar, Oct.17th 2022

G-extensions and coverings

- For G a finite group, by a G-**extension** of a field K, we mean a Galois extension L/K of étale algebras ($=$ a direct product of isomorphic Galois extensions of fields) with Galois group G.

  (Informally, one may think of a Galois extension of K whose Galois group embeds into G.)
- By a G-**Galois cover**, we mean a finite ramified Galois covering $f : X \to Y$ of (smooth, quasiprojective, irreducible) varieties X, Y over K, whose Galois group is isomorphic to G (equivalently, its function field extension E/F is a Galois extension with group G.)

Specialization

- For a cover $f : X \to Y$ and for each K-point p of Y away from the ramification locus of f, the specialization of f at p is the residue extension $K(f^{-1}(p))/K$, and is a G-extension in the étale algebra sense.
  (When $Y = \mathbb{P}^d$ and f is given by a polynomial $F(t_1, \dots, t_d, X)$, specialization ("mostly") simply corresponds to evaluating the variables $t_1, \dots, t_d$.)

A central question

When specializing a fixed G-Galois cover as above, which G-extensions can you actually get?

- E.g., over a number field K, G-Galois covers $f : X \to \mathbb{P}^d_K$ with X absolutely irreducible always specialize to infinitely many distinct G-extensions of K (Hilbert's irreducibility theorem).

Grunwald problems

- K a number field, G a finite group.
- Pick a finite set $\mathcal{S}$ of primes of K, and for each p a Galois extension L^p/K_p (of the completion K_p) with group embedding into G.
- The **Grunwald problem** associated to $(G, \mathcal{S}, (L^p/K_p)_{p\in\mathcal{S}})$ is the question whether there exists a Galois extension of K with group G whose completions at p are isomorphic to L^p/K_p for all $p \in \mathcal{S}$.
- **Grunwald-Wang theorem**: When G is cyclic, there always exists a finite set $\mathcal{S}_0$ of primes of K such that all Grunwald problems for G away from the set $\mathcal{S}_0$ have a solution. However, when $8||G|$, the conclusion would become false upon dropping the set $\mathcal{S}_0$.
- Nowadays, similar conclusions are known for much larger classes of groups, notably **supersolvable groups** (Harpaz-Wittenberg), or groups possessing a "generic extension" over K (Saltman).

Grunwald problems and specialization: the unramified case

Theorem (Dèbes-Ghazi, 2012)

Let K be a number field and $f : X \to \mathbb{P}^1$ be a regular G-cover over K. Then there exists an (explicitly describable) finite set $\mathcal{S}_0$ of primes of K such that any **unramified** *Grunwald problem $(G, \mathcal{S}, (L^p/K_p)_{p \in \mathcal{S}})$ for G with $\mathcal{S}$ disjoint from $\mathcal{S}_0$ has a solution among the set of specializations of f.*

Later results by Dèbes and Motte: $\to$ asymptotic lower bound for solutions to given unramified Grunwald problem among specializations of f (e.g., when ordered by discriminant).

Hilbert–Grunwald property for a group G (general case)

- **Obvious observation**: In general, given a Galois cover $f: X \to \mathbb{P}^1$ (with group G) one cannot hope to solve *all* Grunwald problems for G via specializations of f (e.g., depending on the precise branch point locus, some primes may be unramified in all specializations, etc.)
- $\Rightarrow$ A better question: Given G and (a number field) K, does there **exist** a G-cover $f: X \to \mathbb{P}^1$ (over K) whose K-specializations yield solutions to all Grunwald problems away from some finite set of primes (depending on G)?

Definition (Hilbert-Grunwald property)

Let us say that G has the Hilbert-Grunwald property over K if there exists $f: X \to \mathbb{P}^1$ as above.

Some easy examples

- E.g., $f : \mathbb{P}^1 \to \mathbb{P}^1$, $f(x) = x^2$ very obviously has this property for $G = C_2$; more generally, if G is a group with a **one-parameter generic extension** over K, then G has the Hilbert-Grunwald property over K.
- Groups with one parameter generic extensions are very rare, but other examples also occur (e.g., cyclic groups of prime order over all number fields)!

Grunwald problems and specializations: the ramified case

Theorem (K.-Legrand-Neftin, 2019)

Let G be a finite group containing a non-cyclic abelian subgroup. Let $E/K(t)$ be a Galois extension with group G. Then there are infinitely many primes p of K, and for each p at least one Galois extension L^p/K_p with group embedding into G such that L^p/K_p is not a specialization of $E/K(t)$. In particular, G does not have the Hilbert-Grunwald property over K.

Varieties parameterizing Galois extensions

General question

Given field K, a finite group G and a set $\mathcal{S}$ of Galois extensions F/L with group $\leq G$ (and $L \supseteq K$), what is the smallest dimension of varieties X, Y over K allowing a Galois cover $f : X \to Y$ with group G and such that all extensions in $\mathcal{S}$ occur as specializations of f?

For example, in the (extreme) case where $\mathcal{S}$ is the set of all G-extensions of all overfields of K, this is called the **essential dimension** of G (over K).

“Hilbert-Grunwald dimension”

Definition (Hilbert-Grunwald dimension)

The Hilbert-Grunwald dimension $hgd_K(G)$ is the smallest integer d such that the following holds: There exists a Galois cover (of group G) $f : X \to Y$ over K of d-dimensional varieties such that every Grunwald problem $(K, G, S, (F^{(p)})_{p \in S})$ with S disjoint from some finite set S_0 of primes of K (depending only on G) has a solution in the set of K-specializations of f.

Local dimension

Definition (Local dimension)

The local dimension $ld_K(G)$ of G over K is the smallest integer d such that there exist finitely many Galois covers $f_i : X_i \to Y_i$ with group G over K and such that, for all but finitely many primes p of K, every G-extension of K_p is a K_p-specialization of some f_i.

- From the definitions, obviously $ld_K(G) \leq hgd_K(G)$.

Results on *hgd*

Theorem (K.-Neftin, '22)

$ld_K(G) \leq 2$ for every finite group G and number field K. If furthermore G has a **generic extension** *over K, then $hgd_K(G) \leq 2$.*

Remarks:

- "Generic extension" $\Leftrightarrow$ $\exists$Galois cover $f; X \to \mathbb{P}^d_K$ with Galois group G, specializing to all G-extensions of K (for **some** $d \in \mathbb{N}$). Above theorem means that, in order to solve Grunwald problems for G, it suffices to restrict f to a suitable cover of **surfaces** .
- Groups with generic extensions include symmetric groups, abelian groups of odd order etc. But there are also known examples of groups without a generic extension.
- Bounding $hgd_K(G)$ from above for **arbitrary** groups is much harder, since even $hgd_K(G) < \infty$ implies that G is a Galois group over K.

Groups of local dimension 1 over $\mathbb{Q}$

Theorem (K., Neftin (to appear))

The following are equivalent:

1) *G has the Hilbert-Grunwald property over $\mathbb{Q}$. I.e., there exists a G-cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ providing solutions to all Grunwald problems for G away from some finite set of primes (depending on G).*
2) $ld_{\mathbb{Q}}(G) = 1$.
3) *G is either cyclic of odd prime power order or of order 2, or a semi-direct product (with faithful action) of two such groups.*

Remarks about other number fields

- The result (and proof) holds in the same way over many number fields, notably all real number fields without cyclotomic subextension.
- Over certain other number fields, the result obviously has to change; e.g., over $K = \mathbb{Q}(\zeta_n)$, the group C_n has a generic extension $K(t^{1/n})/K(t)$, and thus needs to be included.
- At least the implications "3)$\Rightarrow$ 1)$\Rightarrow$ 2)" hold over arbitrary number fields.

Three obstructions to the Hilbert-Grunwald property

Let's call a pair (I, D) of subgroups $I \trianglelefteq D (\leq G)$ an **obstruction** to the assertion $ld_K(G) = 1$, if there exists no finite set of G-covers $f_i : X_i \to Y_i$ over K whose specializations contain all extensions of K_p with inertia group I and decomposition group D, f.a.a. primes p of K.

Lemma

The following pairs (I, D) are obstructions to "$ld_K(G) = 1$" (and hence, to $hgd_K(G) = 1$) as soon as $D \leq G$.

a) $(I, D) = (C_p, C_p \times C_p)$ *for any prime p.*

b) *If $\zeta_q \notin K(\zeta_p)$, then: $(I, D) = (C_p, C_{pq})$ for primes p, q.*

c) *If K has a real embedding, then $(I, D) = (C_2, C_4)$.*

The point of the three obstructions: Proof of "2)⇒3)"

- Note that p-groups without noncyclic abelian subgroups are necessarily cyclic or generalized quaternion. The latter groups contain C_4, so a group avoiding both obstructions 1) and 3) (over e.g. $K = \mathbb{Q}$) has to be Sylow-cyclic.
- Sylow-cyclic groups G are known to be metacyclic. Now use additionally obstruction 2) to see that $G \cong C_P \rtimes C_Q$ with two coprime prime powers P, Q (with necessarily faithful action of C_Q)..

Proof of obstruction b) for covers $X \to \mathbb{P}^1$

- Pick G-extension $E/K(t)$.
- Crucial tool: Result on the possible ramified local behavior of specializations of Galois covers (K-Legrand-Neftin 2019).

Theorem ((Beckmann 1991;) K-Legrand-Neftin 2019)

Given a Galois extension $E/K(t)$, the following holds for all but finitely many primes p of K:
Given any non-branch point t_0 of $E/K(t)$, if p ramifies in the specialization E_{t_0}/K of $E/K(t)$ at $t \mapsto t_0$, then there exists some (essentially unique) branch point $t \mapsto t_i$ of $E/K(t)$ such that

i) *the ("arithmetic") inertia and decomposition group at p in E_{t_0}/K embed into the ("geometric") inertia and) decomposition group at $(t - t_i)$ in $E(t_i)/K(t, t_i)$, and*

ii) *Projection "modulo geometric inertia" maps the arithmetic decomposition group (at p in E_{t_0}/K) onto the decompostion group at (some prime extending) p in $E(t_i)_{t_i}/K(t_i)$.*

Proof of obstruction b)

- Pick set $\mathcal{S}'$ of primes of K non-split in $K(\zeta_q)$ but split in $K(\zeta_p)$ (positive density set due to assumption).
- Reduce $\mathcal{S}'$ further to the subset of primes of residue degree coprime to q in **all** residue extensions at branch points of $E/K(t)$ (still positive density set!).
- Assume existence of K_ℓ-specializations of $E/K(t)$ ($\ell \in \mathcal{S}$) of ramification index p and inertia degree q.
- K-L-N2019 $\Rightarrow$ this local behavior must be "inherited" from a branch point of $E/K(t)$ of ram. index e and res.degree d, where $p|e$ and $pq|de$.
- But also, def. of $\mathcal{S}$ implies that $q|d$ would be "of no use", so necessarily $pq|e$.
- Then, necessarily ζ_q is in the residue extension at that branch point, and hence by def. of $\mathcal{S}$, ℓ is of res.deg. d_ℓ not coprime to $q-1$ in that res.extension.
- K-L-N2019 $\Rightarrow$ Any specialization of $E/K(t)$ in which ℓ "inherits" its local behavior from this branch point has residue degree divisible by d_ℓ at ℓ, contradiction.

From $\mathbb{P}^1$ to arbitrary base curve

- (Simplified) idea: Given G-cover $f : X \to Y$ over K, find "suitable" cover $g : Y \to \mathbb{P}^1_K$ (i.e., find suitable function $\tau \in K(Y)$) separating the branch point locus of f.
- Then, local behavior at branch points of f carries over "reasonably nicely" to local behavior at branch points of (the Galois closure of) $g \circ f$, which is a cover of $\mathbb{P}^1_K$. In particular, obstruction 1),2) or 3) for the latter cover implies the same kind of obstruction for f.

Proof of "3)⇒1)": Construction of covers with Hilbert-Grunwald property

- Note that all groups as in 3) are known to have generic extensions over any number field K. By a result of Saltman, one may then find G-extensions $E/K(t)$ with any prescribed local behavior (in particular., prescribed pair of inertia and decomposition group) at finitely many (geometric!) primes ("solution of Grunwald problems over $K(t)$"!).
- This way, it suffices to check Hilbert-Grunwald property "one (I, D)-pair at a time".
- Crucial case in our setup is for D cyclic of prime power order d (and $I \leq D$ of order $|I| =: e > 1$).
- Easy to realize (I, D) over $K(\zeta_e)((t))$, and if $K(\zeta_e) \cap \mu_d = \mu_e$, then may even pick the unramified part of such an extension to be $K(\zeta_d)/K(\zeta_e)$.
- Suitable specialization of a function field extension with such a completion then realizes **all** D-extensions of K_p f.a.a. p which are totally split in $K(\zeta_e)/K$ and inert in $K(\zeta_d)/K(\zeta_e)$ – on the other hand, those are all the relevant p!

Parametric dimension

Definition

The **parametric dimension** $pd_K(G)$ of a group G over a field K is the smallest number d for which there exist finitely many G-Galois covers $f_i : X_i \to Y_i$ $(i = 1, \dots, n)$ of varieties over K of dimension $\leq d$, such that **every** G-extension of K is the specialization of some f_i at some K-rational point of Y_i.

- Over number fields, one always has $pd_K(G) \geq ld_K(G)$.
- Conjecturally $pd_{\mathbb{Q}}(G) = 1$ only for the very small groups C_2, C_3 and S_3 (which even have generic dimension 1).

Combining our results on Hilbert-Grunwald property / local dimension with some earlier results on parametric dimension (K-Legrand, 2018), we get:

Theorem

If $pd_{\mathbb{Q}}(G) = 1$, then $G \cong C_p \rtimes C_d$ where p is prime and $d \leq 3$.

Open problems

- Note that the above theorem does give some cases in which $ld_{\mathbb{Q}}(G) = hgd_{\mathbb{Q}}(G) = 1 < pd_{\mathbb{Q}}(G)$. Are there also examples in which provably $pd_{\mathbb{Q}}(G) > 2$? (Conjecturally, yes!)
- We know $ld_K(G) \leq 2$ for all (G, K). Does this also hold for *hgd*? I.e., can we solve (most) Grunwald problems via specializations of a suitable cover of **surfaces**?

References

- J.K., D. Neftin, *The Hilbert-Grunwald specialization property over number fields*. To appear in Isr. J. Math. `https://arxiv.org/abs/2112.15467`
- J.K., D. Neftin, *The local dimension of a finite group*. Trans. Amer. Math. Soc. 375(7) (2022), 4783-4808.
- J.K., D. Neftin, F. Legrand, *On the local behavior of specializations of function field extensions*. IMRN Vol.2019 (9), (2019), 2951–2980.