The Inverse Galois problem with local restrictions

Joachim König

KAIST, Daejeon

Guangdong Technion I.I.T, Jan 8th, 2019

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"!
- In particular, Galois theory over $\mathbb{Q}_p$ 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.

General background: The inverse Galois problem

IGP with local restrictions

Given a finite group G, a set S of primes and for each $p \in S$ a Galois extension $K^p/\mathbb{Q}_p$ fulfilling a certain condition $P(p)$.
Can we then find a Galois extension $K/\mathbb{Q}$ with group G and with completion $K_p = K^p$ for all $p \in S$?

- Answer depends of course on "reasonable" choice of set S and local conditions $P(p)$.
- If S is finite: **Grunwald problem**.
- If S is infinite: Need to be "reasonable" with conditions $P(p)$, due to e.g. Chebotarev's density theorem.
  Reasonable example: Make local restrictions only about the **ramified** primes
  (i.e., $S = \mathbb{P}$, and $P(p) =$ "either $K_p/\mathbb{Q}_p$ is unramified or ...")

General background: RIGP and specializations

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

Regular IGP

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 nfinitely many $t_0 \in \mathbb{Q}$ such that the residue extension $E_{t_0}/\mathbb{Q}$ still has group G.
- Natural question: Can this specialization approach also be used to solve IGP with local restrictions?

Ramification conditions

A few examples of local restriction concerning only the **inertia groups** at ramified primes:

a) Restrict the ramification indices. In particular, ask for the minimal number e such that there exists a tamely ramified G-extension of $\mathbb{Q}$ all of whose ramification indices divide e.

b) Restrict the subgroups that are allowed to occur as inertia subgroups of G-extensions. I.e., given any set S of cyclic subgroups of G with whose normal closure is G: Do there exist G-extensions of $\mathbb{Q}$ all of whose inertia subgroups are in G?

Importance and evidence

Importance of a): Solution automatically yields number fields F of degree e such that F possesses an unramified G-extension.

Regarding a):

Conjecture

The minimal e in a) is $e = gexp(G)$ ("generator exponent"), which is defined as the minimal value of $\mathrm{lcm}_{x \in S} ord(S)$, where S is a generating set of G.

Evidence:
Ideally, one likes to obtain evidence for statements about $\mathbb{Q}$ via an analogy with global function fields $\mathbb{F}_p(t)$. A weaker, but still fruitful analogy is with function fields $k(t)$, where k is an "ample" field.

Definition

k is called ample if every absolutely irreducible curve over k has either zero or infinitely many k-points.

Theorem

If k is an ample field of characteristic 0, and S is any set of cyclic subgroups with normal closure G, then there exist infinitely many tame G-extensions of $k(t)$ with all inertia groups in S. In particular there exist infinitely many tame G-extensions of $k(t)$ with all ramification indices dividing $gexp(G)$.

A general specialization criterion

Theorem

Assume $E/\mathbb{Q}(T)$ is a $\mathbb{Q}$-regular Galois extension with group G, with all inertia groups at **finite** *prime ideals in some prescribed set S, and with no "universally ramified" finite primes. (Meaning that for every p, there is a specialization $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ which is unramified at p)*
Then among the specializations of $E/\mathbb{Q}(T)$, there are infinitely many G-extensions of $\mathbb{Q}$ with all inertia groups at finite primes in the set S.

Some new results

Theorem (K-Rabayev-Sonn 2018, K-Neftin-Sonn 2019)

There are infinitely many G-extensions of $\mathbb{Q}$ with all ramification indices dividing 2 in the following cases:

a) $G = A_5$, $PSL_2(7)$, $PGL(2,7)$, M_{11}, *etc.*

b) $G = \Gamma \wr S_n$ *where* Γ *is any of the groups in a).*

Galois realizations with k-free discriminants

Special case of b): For $G = S_n$, it is well-known (Yamamoto, Kedlaya, Bhargava, ...) that there exist infinitely many tame G-extensions of $\mathbb{Q}$ all of whose inertia subgroups are generated by transpositions. This is the same as saying there exist infinitely many degree-n number fields with squarefree discriminant.
Obvious generalization:

Question

Given $k \geq 2$, for which G is it true that there exists a (tame) G-extension of $\mathbb{Q}$ (i.e., an extension whose Galois closure has group G) with k-free discriminant (i.e., not divisible by any prime power p^k)?

Galois realizations with k-free discriminants

Necessary condition: $G \leq S_n$ needs to be generated by permutations of index at most $k-1$.

Recall that the index $ind(\sigma)$ is defined as n minus number of orbits of $\langle\sigma\rangle$, or alternatively as the minimal number of transpositions needed to write σ as a product.

Conjecture

This condition is also sufficient.

k-free discriminants

Theorem (K., 2018 (submitted))

The above conjecture holds for $k = 3$, and "probably" for $k = 4$. I.e., for every group G generated by transpositions, double transpositions and/or 3-cycles, there are infinitely many G-extensions with cubefree discriminant.

Ingredients:

a) Classification of groups generated by elements of small index [elementary]
b) A general arithmetic-geometric criterion reducing the problem to constructing extensions of $\mathbb{Q}(t)$ with analogous properties

k-free discriminants

Regarding part a)

- The only groups generated by elements of index 1 (transpositions) are S_n.
- The only groups generated by elements of index 1 and 2 are A_n, $C_2 \wr S_n (= C_2^n \rtimes S_n)$, $(C_2 \wr S_n) \cap A_{2n}$ and a few small-degree exceptions.

Sample applications: The symmetric and alternating groups

Let $f = (X - \alpha_1) \cdots (X - \alpha_n)$ with $\alpha_i \in \mathbb{Q}$ distinct. It is easy to show that "generically", $f(X) - T$ has Galois group S_n over $\mathbb{Q}(T)$, and at the same time all inertia groups at finite primes are generated by transpositions. Furthermore, no prime is universally ramified, since the residue extension at $T \mapsto 0$ is the trivial extension $\mathbb{Q}/\mathbb{Q}$ (because f splits completely).

In a similar spirit, a famous construction by Mestre shows (technically, for even n) that for "almost all" such f, there exists g of degree $< n$ such that $f(X) - Tg(X)$ has Galois group A_n, with all inertia groups generated by 3-cycles. Universally ramified primes do not exist for the same reason as above.

Sample application: The wreath product case

Theorem

Let $G = C_2 \wr S_n$. Then there are infinitely many G-extensions of $\mathbb{Q}$ with cubefree discriminant.

Proof.

Start with S_n-extensions of $\mathbb{Q}(T)$ as above. This gives a degree-n function field extension $\mathbb{Q}(X)/\mathbb{Q}(T)$, totally ramified at $T \mapsto \infty$ and totally split at $T \mapsto 0$. Next, extend this by a quadratic extension $E/\mathbb{Q}(X)$ with the following properties:

a) No two branch points of $E/\mathbb{Q}(X)$ extend the same point, or a branch point, of $\mathbb{Q}(X)/\mathbb{Q}(T)$.
b) No branch points of $E/\mathbb{Q}(X)$ extend $T \mapsto 0$.
c) $T \mapsto \infty$ is totally ramified in E.
d) All points of $\mathbb{Q}(X)$ extending $T \mapsto 0$ have residue extensions unramified at primes dividing $2n$.

a) guarantees that the Galois group of $E/\mathbb{Q}(T)$ is the full wreath product $C_2 \wr S_n$, and all inertia groups at finite primes are generated by transpositions or double transpositions.
b)-d) guarantee that no prime ramifies in both specializations at $T \mapsto 0$ and $T \mapsto \infty$.
Therefore, the main specialization criterion is applicable $\square$

Speculations about distribution

- So how many G-extensions with squarefree, cubefree etc. discriminant are there?
- Proper way to count these is to count number of extensions of discriminant up to B, and then $B \to \infty$.
- Existing conjecture for squarefree extensions of degree n: There should be asymptotically $c \cdot B$, for a positive constant c (**Bhargava**). Known only for very small n.
- Conjecture for cubefree: There should be roughly as many such G-extensions as there are cubefree "candidates" for G-discriminants; i.e., $\sim B$ if $G \not\subset A_n$, and $\sim B^{1/2}$ if $G \leq A_n$.

1 Background

2 Conditions on inertia groups

3 Conditions on decomposition groups

Conditions on decomposition groups

- **Problem:** Restrict the subgroups that are allowed to occur as decomposition groups (at ramified primes) of G-extensions.
- **Particular example:** Do there exist G-extensions of $\mathbb{Q}$ in which all decomposition groups are cyclic ("locally cyclic extensions")?
- **Motivation:** We know this is true for *solvable* groups, from Shafarevich's method.
- **Motivation:** "Minimally intersective polynomials".
  Given a finite group G, what is the minimal number of irreducible factors of a polynomial $f \in \mathbb{Q}[X]$ with Galois group G with no rational root, but with a root in every $\mathbb{Q}_p$?

A global function field analog

Theorem

Let G be a finite group. Then there exists $q_0 = q_0(G)$ such that for all $q \geq q_0$, the group G has a Galois realization over $\mathbb{F}_q(T)$ with all decomposition groups cyclic (and equal to the respective inertia groups, for all the ramified primes).

Proof.

- This can be shown via moduli spaces $\mathcal{H}(G, C)$ of Galois covers ("Hurwitz spaces") with a given group G and ramification type C. A standard assumption (without loss) is here that $Z(G) = 1$. Then K-rational points on moduli spaces are in 1-to-1 correpondence with Galois covers defined over K.
- A famous (group-theoretical!) theorem by Conway and Parker yields that, if C contains every conjugacy class of G suffiicently often, then $\mathcal{H}(G, C)$ is an absolutely irreducible variety defined over $\mathbb{Q}$.
- Then it is also defined over all but finitely many $\mathbb{F}_q$ ("good reduction"), and Lang-Weil theorem yields that it has $\mathbb{F}_q$-point for all but finitely many q. **This is how one proves the inverse Galois property for G over almost all $\mathbb{F}_q(T)$.**

□

Proof.

- To get the stronger assertion, let $\mathbb{Q}(H)$ be the function field of the Hurwitz space $\mathcal{H}(G, C)$. Then one has a G-extension $U/\mathbb{Q}(H)(T)$. Let $\mathbb{Q}(H')$ be the compositum of all residue extensions at branch points of this extension. One can show that $\mathbb{Q}(H')$ still corresponds to a variety $\mathcal{H}'/\mathbb{Q}$ which is absolutely irreducible. Therefore again $\mathbb{F}_q$-points by Lang-Weil. This means that the corresponding extension of $\mathbb{F}_q(T)$ has trivial residue extension at all its branch points.

$\square$

The number field situation

A weak version:

Theorem

Assume G possesses a rationally rigid tuple of conjugacy classes. Then there exists a finite set S_0 of primes and infinitely many G-extensions of $\mathbb{Q}$ all of whose decomposition groups **outside of** *S_0 are cyclic.*

Examples of groups fulfilling the condition:
Symmetric groups, “many” linear groups $PSL_2(p)$, “most” sporadic simple groups,...

The case $G = S_5$

Theorem

Let $G = S_5$. Then for every finite set S of finite primes, there exists a G-extension $F/\mathbb{Q}$ such that:

- *$F/\mathbb{Q}$ is unramified inside S, and*
- *All decomposition groups of $F/\mathbb{Q}$ are cyclic.*

The group S_5

Proof.

Consider the splitting field $E/\mathbb{Q}(T)$ of $f(T,X) = X^5 - T(X-1)$. This is an S_5-extension with inertia groups generated by a 5-cycle (at $T = 0$), a 4-cycle (at $T = \infty$) and a transposition (at $T = 256/3125$). The discriminant of f equals ....

It then suffices to find a specialization $t_0 = \frac{a}{b} \in \mathbb{Q}$ such that

- a is a prime congruent 1 mod 5,
- b is a prime congruent 1 mod 4, and
- $256a - 3125b$ is a prime which splits completely in $\mathbb{Q}\sqrt{-2}$ (i.e., which is congruent 3 or 5 mod 8).

In particular, it suffices to consider the set of affine linear forms $5X + 1, 8Y + 1, 256(5X + 1) - 3125(8Y + 1)$. Since these are pairwise non-affinely-dependent, **Green-Tao-Ziegler's theorem** yields infinitely many integer values of X and Y for which all three forms take prime values. This shows the assertion. □

Thank you for your attention!