Rational Points Coming From Ramified Covers

BIRS Workshop "Specialisation and Effectiveness in Number Theory"

Lior Bary-Soroker, August 29, 2022

TEL AVIV UNIVERSITY

Motivational Example

- Let $f(X) \in \mathbb{Q}[X]$ of $\deg(f) > 0$ nonsquare polynomial
- What can we say about the set $T = \{x \in \mathbb{Q} : f(x) = \square\}$?
- **Qualitative smallness:** $T \neq \mathbb{Q}$; moreover, $\#(\mathbb{Q} \setminus T) = \infty$
- **Quantitative smallness:** $\#(T \cap \{1, \ldots, N\}) = O(\sqrt{N})$
- **Group Theoretic (GT-)smallness:** $\mathbb{Z} \setminus T$ contains an arithmetic progression
- **Infinite extensions:**
  - $\#(\mathbb{Q}^{ab} \setminus \{x \in \mathbb{Q}^{ab} : f(x) \in (\mathbb{Q}^{ab})^2\}) = \infty$; **but**
  - $\#(\mathbb{Q}^{sol} \setminus \{x \in \mathbb{Q}^{sol} : f(x) \in (\mathbb{Q}^{sol})^2\}) = \emptyset$
  - What about $\mathbb{Q}^{sol}(\alpha)$, $\alpha^5 - \alpha - 1 = 0$?

Hilbert's Irreducibility Theorem

- Let $f_i\colon Y_i \to \mathbb{A}^n_{\mathbb{Q}}$ be a finite surjective morphism of degree > 1 with Y_i irreducible
- Any $T \subseteq \cup_i f_i(Y_i(\mathbb{Q})) \cup Z(\mathbb{Q}) \subseteq \mathbb{Q}^n$, Z Zariski closed is called a **thin set**
- Hilbert's irreducibility theorem (Hilbert 1896): $\mathbb{Q}^n$ is not thin—**Qualitative smallness**
- Connection to irreducibility: The set $\{a \in \mathbb{A}^n(\mathbb{Q}) : f^{-1}(a)$ is $\mathbb{Q}$-reducible$\}$ is thin
- S.D. Cohen 1981: $\#(T \cap \{1,\dots,N\}^n) = O(N^{n-1/2})$—**Quantitative smallness**
- Eichler 1939: $\mathbb{Z}^n \setminus T$ contains a finite index coset of $\mathbb{Z}^n$—**GT smallness**
- Kuyk 70: Abelian extension, Weissauer 80: Galois extension+epsilon, Haran 99: Diamond theorem, LBS-Fehm-Wiese 16: Galois representations—**Infinite extensions**
- **The theorem has an abundance of applications in Galois theory, number theory, arithmetic geometry, and algebra**

Algebraic Groups

Varieties of Hilbert type

$X(K) \notin \cup_i f_i(Y_i(K)) \cup Z(K)$ **for** $f_i\colon Y_i \to X$, $\deg f_i \geq 2$, Y_i **irreducible**

- Let X/K be an irreducible variety over a field K. It is of **Hilbert Type (HT)** if $X(K)$ is not thin (**Qualitative Smallness**)
- K is **Hilbertian** if $\mathbb{A}^1$ is HT (if any variety over K is HT, then so is $\mathbb{A}^1_K$)
- Linear groups over a Hilbertian field (Colliot-Thélène-Sansuc, LBS-Fehm-Petersen)
- Abelian varieties over number fields are **not** HT due to the weak Mordell-Weil Theorem: $E(K) = \cup_i (c_i + 2E(K)))$
- No GT-smallness: $\Gamma = \langle 4^n \rangle \subseteq \mathbb{G}_m$ is Zariski dense, but also $\Gamma \subseteq T = \{\square \in \mathbb{Q}^*\}$
- **Ramification obstruction.** Corvaja-Zannier 2017: if X is **HT** and **normal, projective** over a number field, then X is simply connected
- Correction: **ramified thin set** and **weak Hilbert Type (wHT)**

Varieties of Hilbert type

$X(K) \subsetneq \cup_i f_i(Y_i(K)) \cup Z(K)$ **for** $f_i\colon Y_i \to X$, $\deg f_i \geq 2$, Y_i **irreducible+ramified**

- Let X/K be an irreducible variety over a field K. It is of **Hilbert Type (HT)** if $X(K)$ is not thin (**Qualitative Smallness**)
- K is **Hilbertian** if $\mathbb{A}^1$ is HT (if any variety over K is HT, then so is $\mathbb{A}^1_K$)
- Linear groups over a Hilbertian field (Colliot-Thélène-Sansuc, LBS-Fehm-Petersen)
- Abelian varieties over number fields are **not** HT due to the weak Mordell-Weil Theorem: $E(K) = \cup_i (c_i + 2E(K)))$
- No GT-smallness: $\Gamma = \langle 4^n \rangle \subseteq \mathbb{G}_m$ is Zariski dense, but also $\Gamma \subseteq T = \{\square \in \mathbb{Q}^*\}$
- **Ramification obstruction.** Corvaja-Zannier 2017: if X is **HT** and **normal, projective** over a number field, then X is simply connected
- Correction: **ramified thin set** and **weak Hilbert Type (wHT)**
- Elliptic curves (using Faltings' theorem) and $\mathbb{G}_m$ (using Siegel's theorem) are wHT

Abelian Varieties

- **Qualitative smallness—**Theorem(Zannier 2010,…,Corvaja–Demeio–Javanpeykar–Lombardo–Zannier 2020): Let A be an abelian variety over a number field K with $A(K)$ Zariski dense. Then A is wHT

- Question: Are abelian varieties are wHT over $\mathbb{Q}^{ab}$?

- **Infinite extensions—**Theorem (LBS-Fehm-Petersen 2022): Let $E/\mathbb{Q}$ be an elliptic curve. Then, $E_{\mathbb{Q}^{ab}}$ is wHT

- The theorem generalizes to an abelian variety A over a finitely generated field K of characteristic 0 and to any abelian extension L/K, as long as we assume that any nonzero homomorphic image A_0 of A has infinite rank over L

- In particular, if we assume the Frey-Jarden conjecture—every abelian variety over $\mathbb{Q}^{ab}$ has infinite rank—we get that any A/K^{ab} has wHP

- The proof necessitates the development of new method, which is based on Weil-decent, and profinite group theory, and then applying a strong version of the CDJLZ theorem

Linear Groups

- Let G be a connected linear group over a number field K, $\Gamma = \langle \Omega \rangle \subseteq G(K)$ Zariski dense subgroup with a finite symmetric generating set Ω ($e \in \Omega$ and $\gamma \in \Omega \Rightarrow \gamma^{-1} \in \Omega$)

- Examples to have in mind: $G = \mathrm{SL}_n$, Sp_{2n}, $\mathbb{A}^n \rtimes \mathrm{SL}_n$, …

- Note that Γ may be contained in a thin set: E.g. $\Gamma = \mathrm{PSL}_n(\mathbb{Z})$ is thin in $\mathrm{PGL}_n(\mathbb{Q})$ (as the image of the isogeny $\mathrm{SL}_n \to \mathrm{PGL}_n$)

- **Qualitative/GT** (Corvaja 2007, Liu 2019): Γ is not contained in a **ramified** thin set

Linear Group via Random Walks

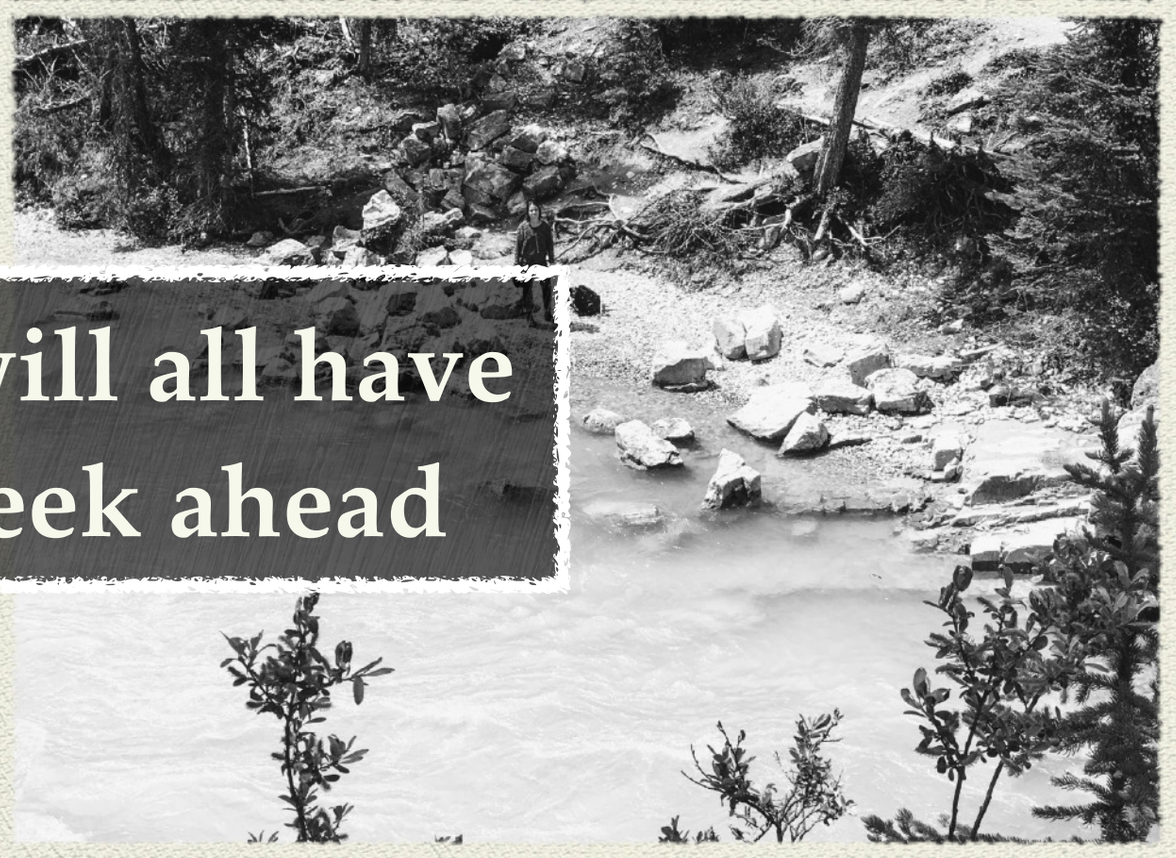
G connected linear group
$\Gamma := \langle \Omega \rangle \leq G(K)$
Ω finite symmetric

- Let ω_k be the random walk on the Cayley graph of Γ
- Assume $G/R_u(G)$ is either trivial or semisimple, $R_u(G)$=the unipotent radical
- Theorem (LBS-Garzoni 2022): Let $T \subsetneq G(K)$ be a ramified thin set. Then $\lim_{n\to\infty} \mathrm{Prob}(\omega_k \in T) = 0$.
- More precisely, $\mathrm{Prob}(\omega_k \in T) \leq \begin{cases} e^{-k/C} & \text{if } G \text{ semisimple} \\ Ck^{-1/10 \dim G} & \text{o/w} \end{cases}$
- Example of an application: Theorem (Rivin 2008, Jouve-Kowalski-Zywina 2013, Lubotsky-Rosenzweig 2014): Let $\chi_k = \det(xI - \omega_k)$ be the characteristic polynomial and let $\Pi(G)$ be a specific extension of the Weyl group $W(G)$. Then $\mathrm{Prob}(\mathrm{Gal}(\chi_k/K) \neq \Pi(G)) \ll e^{-k/c}$
- For example $\Pi(\mathrm{SL}_n) = S_n$, $\Pi(\mathrm{Sp}_{2n}) = C_2 \wr S_n$
- Our proof, as well as JKZ and LR one, uses sieves and the expander property. The main difference is that we do not use any more group theory except the Prasad-Rapinchuk calculation of the generic Galois group of the characteristic polynomial.

What next?

- Many exciting open problems
- For instance: Quantitative GT version for non-semisimple
- **A concrete open problem:** let $\Gamma = \langle (2,3) \rangle \leq \mathbb{G}_m^2$ and let $f(x, y, z) \in \mathbb{Z}[x, y, z]$ irreducible with $\deg_y f > 1$. Assume ramification. Is

$$\lim_{N \to \infty} \text{Prob}(N \geq k \geq 1 : f(2^k, 3^k, y) \text{ irreducible}) = 1?$$



Hope we will all have
a great week ahead