

1) Counting wildly ramified extensions of fraction fields (Barn, 1 May 2021)

Context: Counting field extensions with given Galois group G :
→ Over number fields: Malle's conjecture
Quantitative version of inverse Galois theory

→ Over $\mathbb{F}_q(T)$, $q = p^d$:

• If $p \nmid |G|$: all ramification is tame
Expected behaviour $\approx$ Malle's conjecture
Confirmed by work of ETW, LL (topology of Hurwitz spaces)

• If G is a p -group: all ramification is wild!
→ Abelian p -groups $\rightarrow$ solved using class field theory
Lagemann, Klüners-Müller, Pothoff, Gundlach, DT (today!)

→ Today: We deal with non-abelian p -groups!
Specifically, to make things easy:

- exponent $p \rightarrow$ not necessary, but avoid Witt vectors
- nilpotency class 2 $\rightarrow [G, G] \subseteq Z(G)$
"as close as possible to abelian"
- $p \geq 3$ everywhere

We actually include étale algebras which are not fields, so we parametrize $H^1(\Gamma_K, G)$.

absolute Galois group of a field K $\rightarrow$ discrete (finite) group

trivial action

non-abelian continuous group cohomology

$= G$ -conjugacy classes of continuous morphisms $\Gamma_K \rightarrow G$.
(not nec. surjective!)

1. The last-jump invariant

K global field, $L|K$ G -extension
 $[L_p] \in H^1(\Gamma_K, G)$

For any place p : completion K_p , $L_p = L \otimes_K K_p (= \prod_{q|p} L_q)$
 $[L_p] \in H^1(\Gamma_{K_p}, G)$ (restriction)

each Γ_{K_p} has a natural ramification filtration (in upper numbering)

$$\Gamma_{K_p} = (\Gamma_{K_p})^{-1} \supseteq (\Gamma_{K_p})^0 \supseteq \dots \supseteq \dots \supseteq \dots$$

(inertia) (wild inertia) (etc.)

We define $\text{lastjump}(L_p|K_p) = \inf \{v > 0 \mid f_p(\Gamma_{K_p}^v) = 1\}$
 $\text{lastjump}(L|K) = \sum_p \deg p \cdot \text{lastjump}(L_p|K_p)$

Rk:

- for abelian extensions, $\text{lastjump}(L_p|K_p)$ is almost the conductor (off-by-one) $\leadsto$ ASC.
- relation with discriminant:

$$\delta(L_p|K_p) = \int_0^{+\infty} (|f_p(\Gamma_{K_p}^v)| - 1) [f_p(\Gamma_{K_p}) : f_p(\Gamma_{K_p}^v)] dv$$

$$\delta(L|K) = \sum_p \deg p \cdot \delta(L_p|K_p)$$

$$\| \text{Disc}(L|K) \|_p = \prod_p \delta(L_p|K_p)$$
- So:

discriminant $\approx$	sum of sizes of non-trivial norm-gr
lastjump $\approx$	# of " (L ⁰ -norm)

2. Groups & Lie algebras

$\mathfrak{g}$: a finite Lie $\mathbb{F}_p$ -algebra of nilpotency class 2

i.e. $Z(\mathfrak{g}) \subseteq \mathfrak{g}$; nondegenerate bilinear alternating form
 "center"
 $\mathbb{F}_p$ -modules $\mathfrak{g}/Z(\mathfrak{g}) \otimes \mathfrak{g}/Z(\mathfrak{g}) \xrightarrow{[-,-]} Z(\mathfrak{g})$.

We equip $\mathfrak{g}$ with a group law $\circ$ via:

$$x \circ y := x + y + \frac{1}{2} [x, y]$$

(Baker-Campbell-Hausdorff)

We get a p -group $G := (\mathfrak{g}, \circ)$ of exponent p , nilp. class ≤ 2 .
 (if $[-, -] = 0$ is the trivial bracket, then $\circ = +$, G abelian)

Fact (Lazard correspondence): every such G arises in this way.

(More precisely: $\mathfrak{g} \mapsto (\mathfrak{g}, \circ)$ defines an equivalence of categories ...)

This equivalence preserves exact sequences; subgroups $\leftrightarrow$ Lie subalgebras
 normal subgroups $\leftrightarrow$ Lie ideals

3. Parametrization of extensions

Lazard correspondence $\Rightarrow$ we replace groups by Lie $\mathbb{F}_p$ -algs.

Let $\mathfrak{g}$ be a finite Lie $\mathbb{F}_p$ -alg. of nilp. class ≤ 2 .

($\mathfrak{g}/Z(\mathfrak{g})$ is abelian).

Fix K of char. p , $\bar{K}$ a separable closure, $\Gamma_K = \text{Gal}(\bar{K}/K)$.

Lemma 1: $\rho: \mathfrak{g} \otimes K \rightarrow \mathfrak{g} \otimes \bar{K}$ is surjective.

$$x \mapsto \underbrace{\sigma(x)}_{x \mapsto x \text{ parts on } K} \circ \underbrace{(-x)}_{\text{also multiplicative inverse of } x}$$

Pf: if $\mathfrak{g}$ abelian $\rightarrow "x^p - x = y"$ is a separable eqⁿ in x .

Otherwise: $1 \rightarrow Z(\mathfrak{g}) \otimes K \rightarrow \mathfrak{g} \otimes K \rightarrow \mathfrak{g}/Z(\mathfrak{g}) \otimes K \rightarrow 1$ (*)

$$\text{let } x \in \mathfrak{g} \otimes K \xrightarrow{\text{proj.}} \bar{x} \in \mathfrak{g}/Z(\mathfrak{g}) \otimes K \xrightarrow{\text{abelian case}} \sigma(\bar{y}_0) \circ (-\bar{y}_0) \quad y_0 \in \mathfrak{g} \otimes K$$

$$\text{so } \bar{x} - \rho(y_0) \in Z(\mathfrak{g}) \otimes K \quad \text{and } \bar{x} = \rho(y_0) + \rho(y_1)$$

$$= \rho(y_1) \text{ by the abelian case} \quad = \rho(y_0 + y_1) \text{ because } y_1 \text{ is abelian}$$

Lemma 2: $H^1(\Gamma_K, (G \otimes \bar{K}, 0)) = \{1\}$ "H90"

Pf: G abelian $\rightarrow$ "additive H90"
 otherwise $\rightarrow$ use the sequence $(\star)$ again.

Define an action of $(G \otimes K, 0)$ on $G \otimes K$:
 $g \cdot m := \sigma(g) \circ m \circ (-g)$,
 and let $G \otimes K / (G \otimes K, 0)$ be the set of orbits.

Theorem: We have a bijection

$$\underbrace{H^1(\Gamma_K, (G, 0))}_{(G, 0) = G\text{-ext. of } K} \xleftrightarrow{\sim} \underbrace{G \otimes K / (G \otimes K, 0)}_{\text{concrete data.}}$$

$G \otimes K \cong K^n$ where $n = \dim_{\mathbb{F}_p} G$.

(Idea: $[P] = [\tau \mapsto g^{-1}\tau(g)] \mapsto [\rho(g)]$)

So instead of studying extensions, we study orbits of $G \otimes K$.

Ex: Artin — Schreier theory $G = \mathbb{F}_p$, $H = \mathbb{Z}/p\mathbb{Z}$.

$$\{\mathbb{Z}/p\mathbb{Z}\text{-ext. of } K\} \cong K / \rho(K)$$

4. Local extensions: fundamental domain & ramification filtration

$\downarrow$ local f^n field

$K = K((\pi))$, K finite field.

$$\mathcal{O}^\circ = \bigoplus_{a \in \{0\} \cup \mathbb{N} \setminus p\mathbb{N}}$$

$$K \pi^{-a}$$

$$\mathcal{O} = \bigoplus_{a \in \mathbb{N} \setminus p\mathbb{N}}$$

$$K \pi^{-a}$$

$\nearrow$
 pr : natural projection (forget $a=0$)
 "the unramified part"

2

Claim: There is a bijection

$$\underbrace{\mathcal{O} \otimes K // (\mathcal{O} \otimes K, 0)}_{G\text{-ext. of } K} \xleftrightarrow{\sim} \mathcal{O} \otimes \mathbb{D} // (\mathcal{O} \otimes K, 0)$$

G-ext. of K

*finite group!
almost one element per orbit*

(Idea: "Modulo, $x^p = x$, we can chase p -th powers.")

Claim: There is a $|\mathcal{O} \otimes K|$ -to-one surjection

$$\mathcal{O} \otimes \mathbb{D} // (\mathcal{O} \otimes K, 0) \twoheadrightarrow \mathcal{O} \otimes \mathbb{D} // (\mathcal{O} \otimes K, 0)$$

$$[m] \xrightarrow{\quad} [pr(m)]$$

where $(\mathcal{O} \otimes K, 0)$ acts on $\mathcal{O} \otimes \mathbb{D}$ via:

$$g \cdot \mathbb{D} = \mathbb{D} - \frac{1}{2} [\mathbb{D}, \sigma(g) + g].$$

Theorem (consequence of Abrashkin '98):

If $\mathbb{D} \in \mathcal{O} \otimes \mathbb{D}$ *Do play ~~no~~ role!* corresponds to an extension $L|K$,
 $= \sum \mathbb{D}_b \pi^{-b}$

then:

$$\text{labjump}(L|K) < v \Leftrightarrow$$

$$\mathbb{D}_b = -\frac{1}{2b} \sum_{\substack{a_1, a_2 \in \mathbb{N}/p\mathbb{N} \\ b = a_1 + a_2 \\ a_1, a_2 < v}} a_1 [\mathbb{D}_{a_1}, \mathbb{D}_{a_2}] \quad \text{if } b \geq v \quad (E1)$$

$$\sum_{\substack{a_1, a_2 \in \mathbb{N}/p\mathbb{N} \\ b = a_1 + a_2}} a_1 [\mathbb{D}_{a_1}, \mathbb{D}_{a_2}] = 0 \quad \text{if } b < v \quad (E2)$$

$$\sum_{\substack{a_1, a_2 \in \mathbb{N}/p\mathbb{N} \\ b = a_1 p^i + a_2}} a_1 [\sigma^i(\mathbb{D}_{a_1}), \mathbb{D}_{a_2}] = 0 \quad \text{for all } i \geq 0 \text{ such that } b \geq v p^i. \quad (E3)$$

Point of view: for fixed v ,
 count solution tuples $(\mathbb{D}_b)$

$\approx$ number of extensions with $\text{labjump} < v$.

5. Analysis of the equations

v fixed $\pi = \dim_{\mathbb{F}_p} \mathcal{O}$

$\{(E1) \rightarrow$ expresses the elements $(D_b)_{b \geq v}$ in terms of $(D_b)_{b < v}$
 $\{(E2-E3)$ only involve $(D_b)_{b < v}$

$\Rightarrow$ we only need to solve for $(D_b)_{b < v}$.

$\Rightarrow$ a closed subvariety $\mathcal{D}_v \subseteq \mathbb{A}_{\mathbb{F}_p}^{\pi(\lceil v \rceil - \lceil v/p \rceil)}$ defined by (E2-E3)

"moduli space" $\leadsto \mathcal{D}_v(\mathbb{F}_q) \cong G\text{-ext. of } \mathbb{F}_q((\pi)).$

More precisely:

$$\begin{aligned} |\mathcal{D}_v(\mathbb{F}_q)| &= |\{D \in \mathcal{O} \otimes \mathcal{O} \mid \text{last jump } D < v\}| \\ &= \frac{1}{|\mathcal{O} \otimes \kappa|} |\{D \in \mathcal{O} \otimes \mathcal{O}^\circ \mid \text{last jump } D < v\}| \\ &= \sum_{\substack{L \mid \mathbb{F}_q((\pi)) \\ G\text{-ext.} \\ \text{last jump} < v}} \frac{1}{|Aut_{\mathbb{F}_q((\pi))}(L)|} \end{aligned}$$

For local extⁿ: we have reduced to point-counting on $\mathcal{D}_v$.

For global extⁿ: we prove an exact local-global principle:

$$K = \mathbb{F}_q((T)) \leadsto \sum_{\substack{L \mid K \\ G\text{-ext.}}} \frac{1}{|Aut_K(L)|} \times \text{last jump}(L|K) = \prod_{\substack{p \text{ place} \\ \text{of } K}} \sum_{\substack{L_p \mid K_p \\ G\text{-ext.}}} \frac{1}{|Aut_{K_p}(L_p)|} \times \text{last jump}(L_p|K_p)$$

So our main remaining goal is to estimate $|\mathcal{D}_v(\mathbb{F}_q)|$.

Natural bound: $|\mathcal{D}_v(\mathbb{F}_q)| \leq q^{\pi(\lceil v \rceil - \lceil v/p \rceil)}$

$\rightarrow$ enough for "large v " (most extensions have no places with large local last jumps...)
 $\rightarrow$ small v ??

6. Small v

Consider (E3) for $v \leq p$:

for fixed $i \geq 1$, any $b \geq vp^i$ can be written in at most one way as $a_1 p^i + a_2$ with $a_1, a_2 < v$:

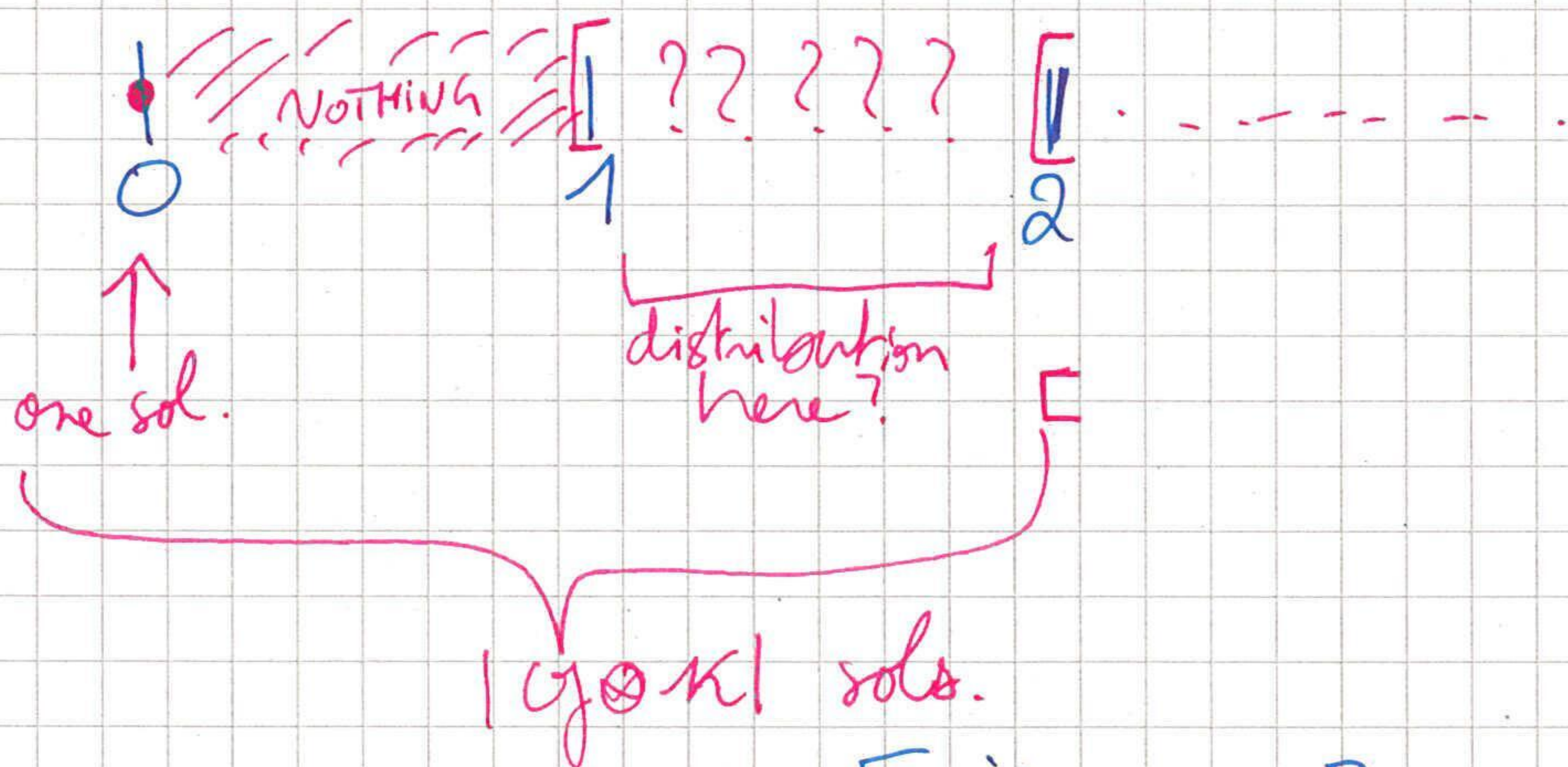
$$a_1 = \lfloor v \rfloor, \quad a_2 = b \bmod p$$

($\lfloor v \rfloor \Rightarrow v \notin \mathbb{Z}$)

(E3) becomes (E'3): $[\sigma^i(D_{\lfloor v \rfloor}), D_a] = 0$
 for all $i \geq 1$ s.t. $a p^{-i} \geq v - \lfloor v \rfloor$.
 if v is not an integer

Examples:

- unramified extⁿ: $\boxed{v=0}$
 No indeterminates! $\leadsto$ unique solution.
- $\boxed{v=1}$ $\rightarrow$ (E2) is vacuous $\leadsto$ same.
 $\Rightarrow$ Nothing between 0 and 1.
- $\boxed{v=2}$ D_1 determines everyone
 $\leadsto |G \otimes K|$ solutions.



Let $v \in]1, 2[$. (E3) says: $[\sigma^i(D_1), D_1] = 0$ for all $i \geq 1$
 s.t. $p^{-i} \geq v - 1$.
 ($a=1, \lfloor v \rfloor=1$)

$\Rightarrow$ all jumps occur at $1, 1 + 1/p, 1 + 1/p^2, 1 + 1/p^3, \text{ etc}$

$|\{D \mid \text{last jump } D < 1 + 1/p^i\}| = |\{D_1 \in G \otimes K \mid D_1 \text{ commutes with } \sigma(D_1), \dots, \sigma^i(D_1)\}| \leadsto$ counting elements with their Frobenius