On the number of ramified primes in specializations

François Legrand

School of Mathematical Sciences, Tel Aviv University
Department of Mathematics and Computer Science, The Open University of Israel

Konstanz - July 23, 2015

Let $E/\mathbb{Q}(T)$ be a (non-trivial) regular finite Galois extension.

$$\begin{array}{ccc} E & & E_n \\ \Big| & \underset{\rightsquigarrow}{T = n \in \mathbb{N} \setminus \{0\}} & \Big| \\ \mathbb{Q}(T) & & \mathbb{Q} \end{array}$$

Given a positive integer n, let

$$\mathrm{Ram}(n)$$

be the number of ramified prime numbers in the specialization $E_n/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at n.

Three kinds of results:

(1) results for suitable positive integers n,

(2) results for a given positive integer n,

(3) statistical properties of the function Ram (joint work with Bary-Soroker).

1. Results for suitable positive integers n

2. Result(s) for a given positive integer n

3. Statistical properties
   - Statement of the main result
   - First part of the proof
   - Second part of the proof (for the mean value)
   - Second part of the proof (general case)

Grunwald Problem. *Let*
- G be a (non-trivial) finite group,
- $\mathcal{S}$ a finite set of prime numbers,
- for each prime number $p \in \mathcal{S}$, $F_p/\mathbb{Q}_p$ a finite Galois extension with Galois group contained in G.
Can we find some finite Galois extension $F/\mathbb{Q}$ with group G such that the completion at each prime number $p \in \mathcal{S}$ is the extension $F_p/\mathbb{Q}_p$?

The Grunwald Problem
- holds if G has odd order (Grunwald in the cyclic case, Neukirch in the general case),
- does not hold if $G = \mathbb{Z}/8\mathbb{Z}$ (Wang).

Proposition

Let G be a (non-trivial) finite group. Assume that the Grunwald Problem holds for the finite group G. Then the following holds:

$(*)$ *given a positive integer m, there exists at least one Galois extension $F/\mathbb{Q}$ with group G and at least m ramified primes.*

It is not clear that any finite group G which occurs as a Galois group over $\mathbb{Q}$ satisfies condition $(*)$. For example, given a "general" prime number p, the group $\mathrm{PSL}_2(\mathbb{F}_p)$ is a Galois group over $\mathbb{Q}$ but all known realizations of this group over $\mathbb{Q}$ ramify only at 2 and p (Zywina).

Theorem (L.)

Let $E/\mathbb{Q}(T)$ be a (non-trivial) regular finite Galois extension with group G. Then, given a finite set $\mathcal{S}$ of large enough "suitable" primes (depending on the extension $E/\mathbb{Q}(T)$), there exist infinitely many positive integers n such that
(1) $\mathrm{Gal}(E_n/\mathbb{Q}) = G$,
(2) *the extension $E_n/\mathbb{Q}$ ramifies at each prime of $\mathcal{S}$.*

Moreover, for at least one such n, we can require the discriminant d_{E_n} of $E_n/\mathbb{Q}$ to satisfy

$$\prod_{p \in \mathcal{S}} p \leq |d_{E_n}| \leq \alpha \cdot \prod_{p \in \mathcal{S}} p^{\beta}$$

for some positive constants α and β (depending only on $E/\mathbb{Q}(T)$).

Remark

(1) *A prime p is "suitable" if p satisfies some necessary condition to ramify in at least one specialization of $E/\mathbb{Q}(T)$ at a positive integer. This necessary condition is related to the arithmetic of the branch points of $E/\mathbb{Q}(T)$.*

(2) *At least infinitely many primes are "suitable". Hence, given a positive integer m, there exist positive integers n such that $\mathrm{Gal}(E_n/\mathbb{Q}) = G$ and $\mathrm{Ram}(n) \geq m$ (in particular, condition $(*)$ holds for any non-trivial regular Galois group over $\mathbb{Q}$).*

(3) *If $E/\mathbb{Q}(T)$ has at least one branch point in $\mathbb{Q}$, then any prime is "suitable". Examples: abelian groups of even order, S_n ($n \geq 2$), A_n ($n \geq 4$), many non abelian simple groups...*

Let $N \geq 3$ and $E/\mathbb{Q}(T)$ be the splitting extension of the trinomial $Y^N - Y^{N-1} - T$. The extension $E/\mathbb{Q}(T)$ has Galois group S_N, is regular and has branch points 0, ∞ and $-(N-1)^{N-1}/N^N$.

Corollary

Let $\mathcal{S}$ be a finite set of primes $p > N$. Then there exist infinitely many positive integers n such that

(1) $\mathrm{Gal}(E_n/\mathbb{Q}) = S_N$,

(2) *the extension $E_n/\mathbb{Q}$ ramifies at each prime of $\mathcal{S}$.*

Let $N \geq 3$ and $E/\mathbb{Q}(T)$ be the splitting extension of the trinomial $Y^N - Y^{N-1} - T$. The extension $E/\mathbb{Q}(T)$ has Galois group S_N, is regular and has branch points 0, ∞ and $-(N-1)^{N-1}/N^N$.

Corollary

Let $\mathcal{S}$ be a finite set of primes $p > N$. Then there exist infinitely many positive integers n such that

(1) $\mathrm{Gal}(E_n/\mathbb{Q}) = S_N$,

(2) *the extension $E_n/\mathbb{Q}$ ramifies at each prime of $\mathcal{S}$.*

Theorem (Bary-Soroker and Schlank)

There exist positive integers n such that

(1) $\mathrm{Gal}(E_n/\mathbb{Q}) = S_N$,

(2) $\mathrm{Ram}(n) \leq 3$.

Natural question. *What can we expect for a given positive integer n (such that the specialization $E_n/\mathbb{Q}$ has Galois group G)?*

1. Results for suitable positive integers n

2. Result(s) for a given positive integer n

3. Statistical properties
   - Statement of the main result
   - First part of the proof
   - Second part of the proof (for the mean value)
   - Second part of the proof (general case)

Proposition

Let $E/\mathbb{Q}(T)$ be a regular finite Galois extension. Then there exists some positive real number C (depending only on the extension $E/\mathbb{Q}(T)$) such that

$$\mathrm{Ram}(n) \leq C \cdot \log(n)$$

for any positive integer $n \geq 2$ (not a branch point).

Proof.

Let $P(T, Y) \in \mathbb{Z}[T][Y]$ be a monic separable polynomial with splitting field E over $\mathbb{Q}(T)$ and $\Delta(T) \in \mathbb{Z}[T]$ its discriminant. If n is large enough, the specialization $E_n/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at n is the splitting extension over $\mathbb{Q}$ of $P(n, Y)$. We then obtain that any prime p ramifying in $E_n/\mathbb{Q}$ divides $\Delta(n)$. Hence

$$\mathrm{Ram}(n) \leq \omega(\Delta(n)) := |\{p \ : \ p \,|\, \Delta(n)\}|$$

As any positive integer m satisfies trivially $m \geq 2^{\omega(m)}$, we have

$$\mathrm{Ram}(n) \leq \frac{\log(|\Delta(n)|)}{\log 2}$$

It then remains to use that $|\Delta(n)| \leq \alpha \cdot n^{\beta}$ for some positive real numbers α and β (not depending on n) to finish the proof. □

Next step: study $\lim_{n\to\infty} \mathrm{Ram}(n)$, give an asymptotic as $n \to \infty$...

Next step: study $\lim_{n\to\infty} \mathrm{Ram}(n)$, give an asymptotic as $n \to \infty$...

Example

Take $E/\mathbb{Q}(T) = \mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$. For any positive integer n, one has $E_n/\mathbb{Q} = \mathbb{Q}(\sqrt{n})/\mathbb{Q}$.

(1) If $n = \square$, then $\mathrm{Ram}(n) = 0$.

(2) If n is a prime, then $\mathrm{Ram}(n) = 1 \text{ or } 2$.

(3) If $n = p_1 \dots p_s$ with n $\square$-free, then $\mathrm{Ram}(n) = s \text{ or } s + 1$.

Next step: study $\lim_{n\to\infty} \mathrm{Ram}(n)$, give an asymptotic as $n \to \infty$...

Example

Take $E/\mathbb{Q}(T) = \mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$. For any positive integer n, one has $E_n/\mathbb{Q} = \mathbb{Q}(\sqrt{n})/\mathbb{Q}$.

(1) If $n = \square$, then $\mathrm{Ram}(n) = 0$.

(2) If n is a prime, then $\mathrm{Ram}(n) = 1 \text{ or } 2$.

(3) If $n = p_1 \ldots p_s$ with n $\square$-free, then $\mathrm{Ram}(n) = s \text{ or } s + 1$.

Conclusion: it seems to be difficult to say more about the number $\mathrm{Ram}(n)$ for a given positive integer n.

Let $E/\mathbb{Q}(T)$ be a (non-trivial) regular finite Galois extension.

Theorem (Bary-Soroker and L.)

(1) *One has*

$$\frac{1}{x} \sum_{0<n\leq x} \mathrm{Ram}(n) \underset{x\to\infty}{\sim}$$

Let $E/\mathbb{Q}(T)$ be a (non-trivial) regular finite Galois extension.

Theorem (Bary-Soroker and L.)

(1) *One has*

$$\frac{1}{x} \sum_{0<n\leq x} \mathrm{Ram}(n) \underset{x\to\infty}{\sim} r \log\log(x)$$

with r the number of branch points in $\overline{\mathbb{Q}}$ modulo the action of $G_{\mathbb{Q}}$.

Let $E/\mathbb{Q}(T)$ be a (non-trivial) regular finite Galois extension.

Theorem (Bary-Soroker and L.)

(1) *One has*

$$\frac{1}{x}\sum_{0<n\leq x}\mathrm{Ram}(n) \underset{x\to\infty}{\sim} r\log\log(x)$$

with r the number of branch points in $\overline{\mathbb{Q}}$ modulo the action of $G_{\mathbb{Q}}$.

(2) *One has*

$$\frac{1}{x}\sum_{0<n\leq x}\left(\mathrm{Ram}(n) - r\log\log(x)\right)^2 \underset{x\to\infty}{\sim} r\log\log(x)$$

Theorem (Bary-Soroker and L.)

For any real number a, one has

$$\lim_{x\to\infty} \frac{1}{x}\left|\left\{0 < n \leq x \,:\, \frac{\mathrm{Ram}(n) - r\log\log(x)}{\sqrt{r\log\log(x)}} \leq a\right\}\right| = I(a)$$

with

$$I(a) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{a} e^{\frac{-t^2}{2}}\, dt$$

The same results hold if we consider the set of all positive integers n such that $0 < n \leq x$ **and** $\mathrm{Gal}(E_n/\mathbb{Q}) = G$ (with $G = \mathrm{Gal}(E/\mathbb{Q}(T))$).

This follows from the main result and the following two facts:

(1) $\mathrm{Ram}(n) \underset{n \to \infty}{=} O(\log(n))$,

(2) $N(x) := |\{n \ : \ 0 < n \leq x \wedge \mathrm{Gal}(E_n/\mathbb{Q}) < G\}| \underset{x \to \infty}{=} O(\sqrt{x})$.

In particular, from

$$\frac{1}{x} \sum_{\substack{0<n\leq x \\ \mathrm{Gal}(E_n/\mathbb{Q})=G}} \mathrm{Ram}(n) \underset{x\to\infty}{\sim} r \log\log(x)$$

we reobtain the following:

Given a positive integer m, there exist positive integers n such that $\mathrm{Gal}(E_n/\mathbb{Q}) = G$ and $\mathrm{Ram}(n) \geq m$.

1. Results for suitable positive integers n
2. Result(s) for a given positive integer n
3. Statistical properties
   - Statement of the main result
   - First part of the proof
   - Second part of the proof (for the mean value)
   - Second part of the proof (general case)

Let $\{t_1, \dots, t_r\}$ be a set of representatives of the branch points of the extension $E/\mathbb{Q}(T)$ lying in $\overline{\mathbb{Q}}$ under the action of the absolute Galois group of $\mathbb{Q}$.

For each index $i \in \{1, \dots, r\}$, denote the ramification index of $\langle T - t_i \rangle$ in $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ by e_i and let $P_i(T) \in \mathbb{Z}[T]$ be an irreducible polynomial such that $P_i(t_i) = 0$. Finally set $P_E(T) = \prod_{i=1}^{r} P_i(T)$.

Proposition (based on Beckmann)

There exists some positive real number p_0 (depending only on the extension $E/\mathbb{Q}(T)$) satisfying the following. For any prime $p > p_0$ and any positive integer n, not a branch point, the following two conditions are equivalent:

(1) *p ramifies in the specialization $E_n/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ at n,*

(2) *there exists a unique index $i \in \{1, \ldots, r\}$ such that p divides $P_i(n)$ and $v_p(P_i(n))$ is not a multiple of e_i.*

This proposition is a natural motivation to introduce the following definition.

Definition

Given two positive integers a and n, let

$$m_a(n)$$

be the number of primes p such that $v_p(n)$ is a non-zero multiple of a.

Remark: one has $m_1(n) = \omega(n)$ for any positive integer n.

Conjoining the proposition and the definition provides the following.

Proposition

There exists some real number $C \geq 1$ (depending only on the extension $E/\mathbb{Q}(T)$) such that

$$\left|\mathrm{Ram}(n) - \omega(P_E(n)) + \sum_{i=1}^{r} m_{e_i}(P_i(n))\right| \leq C$$

for any positive integer n (not a branch point).

1. Results for suitable positive integers n
2. Result(s) for a given positive integer n
3. Statistical properties
   - Statement of the main result
   - First part of the proof
   - Second part of the proof (for the mean value)
   - Second part of the proof (general case)

By the previous proposition, one has

$$\frac{1}{x}\sum_{0<n\leq x}\mathrm{Ram}(n)=\frac{1}{x}\sum_{0<n\leq x}\omega(P_E(n))$$

$$-\sum_{i=1}^{r}\frac{1}{x}\sum_{0<n\leq x}m_{e_i}(P_i(n))$$

$$+O(1)$$

By the previous proposition, one has

$$\frac{1}{x}\sum_{0<n\leq x}\mathrm{Ram}(n) = \frac{1}{x}\sum_{0<n\leq x}\omega(P_E(n))$$
$$-\sum_{i=1}^{r}\frac{1}{x}\sum_{0<n\leq x} m_{e_i}(P_i(n))$$
$$+O(1)$$

By some classical results, one has

$$\frac{1}{x}\sum_{0<n\leq x}\omega(P_E(n)) \underset{x\to\infty}{\sim} r\log\log(x)$$

It then remains to prove the following result.

Proposition

Let a be an integer ≥ 2 and $P(T) \in \mathbb{Z}[T]$ a non-constant polynomial. Then there exists some positive real number $C(P)$ (depending only on the polynomial $P(T)$) such that

$$\sum_{0<n\leq x} m_a(P(n)) \leq C(P) \cdot x$$

for any positive integer x.

It then remains to prove the following result.

Proposition

Let a be an integer ≥ 2 and $P(T) \in \mathbb{Z}[T]$ a non-constant polynomial. Then there exists some positive real number $C(P)$ (depending only on the polynomial $P(T)$) such that

$$\sum_{0<n\leq x} m_a(P(n)) \leq C(P) \cdot x$$

for any positive integer x.

Remark

(1) *The proposition does not hold if $a = 1$.*
(2) *Key-point in the proof: $a \geq 2 \Longrightarrow m_a(P(n)) \leq \{p \ : \ p^2 | P(n)\}$.*

First we need to generalize the previous proposition.

Proposition

Let a be an integer ≥ 2, k a positive integer and $P(T) \in \mathbb{Z}[T]$ a non-constant polynomial. Then there exists some positive real number $C(P,k)$ (depending only on the polynomial $P(T)$ and the integer k) such that

$$\sum_{0<n\leq x} m_a^k(P(n)) \leq C(P,k) \cdot x$$

for any positive integer x.

Conjoining this proposition and the last proposition from the first part of the proof.

Proposition

Given a positive integer k, there exists some positive real number $C(k)$ (depending only on the integer k and the extension $E/\mathbb{Q}(T)$) such that

$$\left| \sum_{0<n\leq x} \Big(\mathrm{Ram}(n) - \omega(P_E(n))\Big)^k \right| \leq C(k) \cdot x$$

for any positive integer x.

By a result of Halberstam (1956), one has

$$\lim_{x\to\infty} \frac{1}{x} \sum_{0<n\leq x} \left(\frac{\omega(P_E(n)) - r \log\log(x)}{\sqrt{r \log\log(x)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{\frac{-t^2}{2}}\, dt$$

for any positive integer k.

Conjoining this and the previous proposition provides

$$\lim_{x\to\infty} \frac{1}{x} \sum_{0<n\leq x} \left(\frac{\mathrm{Ram}(n) - r \log\log(x)}{\sqrt{r \log\log(x)}} \right)^k = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^k e^{\frac{-t^2}{2}}\, dt$$

for any positive integer k.

Apply this result with $k = 1$ and $k = 2$ to get the results about the mean value and the variance respectively. It then remains to use *the method of moments* to get the result about the probability distribution.