Probabilistic Galois Theory

Lior Bary-Soroker
Tel Aviv University

2nd French-German Summer School
GALOIS THEORY AND NUMBER THEORY
Dresden, July 2019

Outline

Outline

1. **Irreducibility in the Large Box Model**
   - Elementary Approach
   - Mahler Measure Approach
   - Good bound

2. **Galois group**
   - Elementary Approach
   - Open Porblems

Setting

Notation

- $H(\sum_i a_i X^i) = \max\{|a_i|\}$
- $M_d(B) = \{f = X^d + \sum_{i=0}^{d-1} a_i X^i : H(f) \leq B\}$
- $R_d(B) = \dfrac{\#\{f \in M_d(B) : f \text{ is reducible}\}}{(2B+1)^d}$

Setting

Notation

- $H(\sum_i a_i X^i) = \max\{|a_i|\}$
- $M_d(B) = \{f = X^d + \sum_{i=0}^{d-1} a_i X^i : H(f) \leq B\}$
- $R_d(B) = \dfrac{\#\{f \in M_d(B) : f \text{ is reducible}\}}{(2B+1)^d}$

Objective

To find non-trivial bounds on $R_d(B)$

Setting

Notation

- $H(\sum_i a_i X^i) = \max\{|a_i|\}$
- $M_d(B) = \{f = X^d + \sum_{i=0}^{d-1} a_i X^i : H(f) \leq B\}$
- $R_d(B) = \dfrac{\#\{f \in M_d(B) : f \text{ is reducible}\}}{(2B+1)^d}$

Objective

To find non-trivial bounds on $R_d(B)$

Remarks

- Obviously $1 \geq R_d(B) \gg B^{-1}$
- After Koukoulopoulos talks we restrict to: $B \to \infty$

Quadratic Polynomials: Discriminant Approach

First bound

$$\mathbb{P}(X^2 + bX + c \text{ reducible}) = \mathbb{P}(b^2 - 4c = \square) \ll B^{-1/2}$$

Quadratic Polynomials: Discriminant Approach

First bound

$$\mathbb{P}(X^2 + bX + c \text{ reducible}) = \mathbb{P}(b^2 - 4c = \square) \ll B^{-1/2}$$

Proof

$$\sum_{\substack{|b|,|c|\leq B \\ b^2-4c=\square}} 1 \leq \sum_{|b|\leq B} \sum_{\substack{k \\ |b^2-k^2|\leq 4B}} 1$$

.

Quadratic Polynomials: Discriminant Approach

First bound

$$\mathbb{P}(X^2 + bX + c \text{ reducible}) = \mathbb{P}(b^2 - 4c = \square) \ll B^{-1/2}$$

Proof

$$\sum_{\substack{|b|,|c|\leq B\\ b^2-4c=\square}} 1 \leq \sum_{|b|\leq B} \sum_{\substack{k\\ |b^2-k^2|\leq 4B}} 1$$

$$\leq \sum_{|b|<\sqrt{4B}} 4B + \sum_{\sqrt{4B}\leq|b|\leq B} \#\{b^2 - 4B \leq \square \leq b^2 + 4B\}$$

.

Quadratic Polynomials: Discriminant Approach

First bound

$$\mathbb{P}(X^2 + bX + c \text{ reducible}) = \mathbb{P}(b^2 - 4c = \Box) \ll B^{-1/2}$$

Proof

$$\begin{aligned}
\sum_{\substack{|b|,|c|\le B\\ b^2-4c=\Box}} 1 &\le \sum_{|b|\le B} \sum_{\substack{k\\ |b^2-k^2|\le 4B}} 1\\
&\le \sum_{|b|<\sqrt{4B}} 4B + \sum_{\sqrt{4B}\le|b|\le B} \#\{b^2-4B\le\Box\le b^2+4B\}\\
&\ll B^{3/2}.
\end{aligned}$$

Quadratic Polynomials: Roots Approach

Heuristic

$X^2 + bX + c$ reducible iff $= (X - \alpha)(X - \beta)$, $\alpha, \beta \in \mathbb{Z}$. Not both can be large, so we expect $R_2(B) \approx B^{-1}$

Quadratic Polynomials: Roots Approach

Heuristic

$X^2 + bX + c$ reducible iff $= (X - \alpha)(X - \beta)$, $\alpha, \beta \in \mathbb{Z}$. Not both can be large, so we expect $R_2(B) \approx B^{-1}$

Proposition

$$\frac{\log B}{B} \ll R_2(B) \ll \frac{\log B}{B}$$

Quadratic Polynomials: Roots Approach

Heuristic

$X^2 + bX + c$ reducible iff $= (X - \alpha)(X - \beta)$, $\alpha, \beta \in \mathbb{Z}$. Not both can be large, so we expect $R_2(B) \approx B^{-1}$

Proposition

$$\frac{\log B}{B} \ll R_2(B) \ll \frac{\log B}{B}$$

Proof.

Exercise $\square$

Rivin's Approach: Nearly The Optimal bound

Theorem

$$R_d(B) \ll d \cdot \frac{\log B}{B}$$

Proof

Rivin's Approach: Nearly The Optimal bound

Theorem

$$R_d(B) \ll d \cdot \frac{\log B}{B}$$

Proof

- $R_d(B) \leq \sum_{k=1}^{d/2} \mathbb{P}(\overbrace{\exists g \mid f, \deg g = k}^{E_k})$

Rivin's Approach: Nearly The Optimal bound

Theorem

$$R_d(B) \ll d \cdot \frac{\log B}{B}$$

Proof

- $R_d(B) \leq \sum_{k=1}^{d/2} \mathbb{P}(\overbrace{\exists g \mid f, \deg g = k}^{E_k})$
- $\mathbb{P}(E_k) \leq B^{-1} + \sum_{0<|a|\leq B} \sum_{|b||a} \mathbb{P}(E_k, g(0) = b | f(0) = a) B^{-1}$

Rivin's Approach: Nearly The Optimal bound

Theorem

$$R_d(B) \ll d \cdot \frac{\log B}{B}$$

Proof

- $R_d(B) \leq \sum_{k=1}^{d/2} \mathbb{P}(\overbrace{\exists g \mid f, \deg g = k}^{E_k})$
- $\mathbb{P}(E_k) \leq B^{-1} + \sum_{0<|a|\leq B} \sum_{|b||a} \mathbb{P}(E_k, g(0) = b | f(0) = a) B^{-1}$
- $\mathbb{P}(E_k, g(0) = b | f(0) = a) \ll B^{-2}$

Rivin's Approach: Nearly The Optimal bound

Theorem

$$R_d(B) \ll d \cdot \frac{\log B}{B}$$

Proof

- $R_d(B) \leq \sum_{k=1}^{d/2} \mathbb{P}(\overbrace{\exists g \mid f, \deg g = k}^{E_k})$
- $\mathbb{P}(E_k) \leq B^{-1} + \sum_{0<|a|\leq B} \sum_{|b||a} \mathbb{P}(E_k, g(0) = b | f(0) = a) B^{-1}$
- $\mathbb{P}(E_k, g(0) = b | f(0) = a) \ll B^{-2}$
- $R_d(B) \ll d(B^{-1} + \cdot B^{-2} \sum_{0<a\leq B} \sum_{b|a} 1) \ll d \cdot \frac{\log B}{B}$

$\square$

What's Wrong with Height?

Problem

$$H(hg) \neq H(h)H(g).$$

So no estimate of the heights of $g \mid f$ in terms of $H(f)$

What's Wrong with Height?

Problem

$$H(hg) \neq H(h)H(g).$$

So no estimate of the heights of $g \mid f$ in terms of $H(f)$

Solution

Approximate $H(f)$ by another $M(f) \in \mathbb{R}_{>0}$ that satisfies

$$M(fg) = M(f)M(g).$$

Mahler Measure

Definition

Let $f(X) = a_d \prod_{i=1}^{d}(X - \alpha_i)$, $\alpha_i \in \mathbb{C}$ and define

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$$

Mahler Measure

Definition

Let $f(X) = a_d \prod_{i=1}^{d}(X - \alpha_i)$, $\alpha_i \in \mathbb{C}$ and define

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$$

Desired multiplicativity

$$M(gh) = M(g)M(h)$$

$M(f)$ vs $H(f)$

Proposition

For $f = \sum_{i=0}^{d} a_i X^i$ of degree d we have

$$\frac{M(f)}{\sqrt{d+1}} \le H(f) \le 2^{d-1} M(f)$$

Proof of upper bound

$M(f)$ vs $H(f)$

Proposition

For $f = \sum_{i=0}^{d} a_i X^i$ of degree d we have

$$\frac{M(f)}{\sqrt{d+1}} \leq H(f) \leq 2^{d-1} M(f)$$

Proof of upper bound

For $\mathbf{i} = \{0 \leq i_1 < i_2 < \cdots < i_k \leq d\}$ put $|\mathbf{i}| = k$ and recall

- $|a_d| \cdot |\alpha_{i_1} \cdots \alpha_{i_k}| \leq M(f)$

$\square$

$M(f)$ vs $H(f)$

Proposition

For $f = \sum_{i=0}^{d} a_i X^i$ of degree d we have

$$\frac{M(f)}{\sqrt{d+1}} \leq H(f) \leq 2^{d-1} M(f)$$

Proof of upper bound

For $\mathbf{i} = \{0 \leq i_1 < i_2 < \cdots < i_k \leq d\}$ put $|\mathbf{i}| = k$ and recall

- $|a_d| \cdot |\alpha_{i_1} \cdots \alpha_{i_k}| \leq M(f)$
- $|a_k| \leq |a_d| \sum_{|\mathbf{i}|=d-k} |\alpha_{i_1} \cdots \alpha_{i_{d-k}}| \leq \binom{d}{k} M(f) \leq 2^{d-1} M(f)$

$\square$

Integral Formula

Want: $M(f) \ll_d H(f)$. Needs: A formula for $M(f)$

Integral Formula

Want: $M(f) \ll_d H(f)$. Needs: A formula for $M(f)$

Jensen's Formula

Let $f(z) \in \mathrm{Hol}(D)$, $f(0) \neq 0$, $D = \{|z| \leq 1\} \subseteq \mathbb{C}$ and let $z_1, \ldots, z_n \in D$ the zeros of f with multiplicities inside D. Then

$$\frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\varphi})| d\varphi = \log |f(0)| - \sum_{k=1}^{n} \log |z_k|.$$

Integral Formula

Want: $M(f) \ll_d H(f)$. Needs: A formula for $M(f)$

Jensen's Formula

Let $f(z) \in \mathrm{Hol}(D)$, $f(0) \neq 0$, $D = \{|z| \leq 1\} \subseteq \mathbb{C}$ and let $z_1, \ldots, z_n \in D$ the zeros of f with multiplicities inside D. Then

$$\frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\varphi})| d\varphi = \log |f(0)| - \sum_{k=1}^{n} \log |z_k|.$$

Corollary

$$M(f) = \exp \int_0^1 \log |f(e^{2\pi it})| dt.$$

Proof of the Integral Formula

Want: $M(f) = \exp \int_0^1 \log |f(e^{2\pi it})| dt$

Proof of the Integral Formula

Want: $M(f) = \exp \int_0^1 \log |f(e^{2\pi it})| dt$

- Multiplicativity in f; so w.l.o.g. $f = X - \alpha$

Proof of the Integral Formula

Want: $M(f) = \exp \int_0^1 \log |f(e^{2\pi it})| dt$

- Multiplicativity in f; so w.l.o.g. $f = X - \alpha$
- Evaluate both sides:

Proof of the Integral Formula

Want: $M(f) = \exp \int_0^1 \log |f(e^{2\pi i t})| dt$

- Multiplicativity in f; so w.l.o.g. $f = X - \alpha$
- Evaluate both sides:
- By Jensen's formula

$$\int_0^1 \log |f(e^{2\pi i t})| dt = \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\varphi})| d\varphi$$
$$= \log |f(0)| - \epsilon \log |\alpha| = (1 - \epsilon) \log |\alpha|$$

with $\epsilon = 0$ if $|\alpha| \geq 1$ and $\epsilon = 1$ if $|\alpha| < 1$

Proof of the Integral Formula

Want: $M(f) = \exp \int_0^1 \log|f(e^{2\pi it})|dt$

- Multiplicativity in f; so w.l.o.g. $f = X - \alpha$
- Evaluate both sides:
- By Jensen's formula

$$\int_0^1 \log|f(e^{2\pi it})|dt = \frac{1}{2\pi}\int_0^{2\pi} \log|f(e^{i\varphi})|d\varphi$$
$$= \log|f(0)| - \epsilon \log|\alpha| = (1-\epsilon)\log|\alpha|$$

with $\epsilon = 0$ if $|\alpha| \geq 1$ and $\epsilon = 1$ if $|\alpha| < 1$

- By definition: $M(f) = |\alpha|^{1-\epsilon}$ □

Proof of Lower Bound

Want: $\dfrac{M(f)}{\sqrt{d+1}} \leq H(f) \leq 2^{d-1} M(f)$

Proof of Lower Bound

Want: $\frac{M(f)}{\sqrt{d+1}} \leq H(f) \leq 2^{d-1} M(f)$

Put $u(t) = 2\log|f(e^{2\pi it})|$.

- By convexity

$$M(f)^2 = \exp\int_0^1 u(t)dt \leq \int_0^1 e^{u(t)}dt = \int_0^1 |f(e^{2\pi it})|^2 dt$$

Proof of Lower Bound

Want: $\frac{M(f)}{\sqrt{d+1}} \leq H(f) \leq 2^{d-1} M(f)$

Put $u(t) = 2 \log |f(e^{2\pi i t})|$.

- By convexity

$$M(f)^2 = \exp \int_0^1 u(t)dt \leq \int_0^1 e^{u(t)} dt = \int_0^1 |f(e^{2\pi i t})|^2 dt$$

- By Parserval equality

$$\int_0^1 |f(e^{2\pi i t})|^2 dt = \sum_{k=0}^{d} |a_k|^2 \leq (d+1) H(f)^2$$

Proof of Lower Bound

Want: $\frac{M(f)}{\sqrt{d+1}} \leq H(f) \leq 2^{d-1}M(f)$

Put $u(t) = 2\log|f(e^{2\pi it})|$.

- By convexity

$$M(f)^2 = \exp\int_0^1 u(t)dt \leq \int_0^1 e^{u(t)}dt = \int_0^1 |f(e^{2\pi it})|^2 dt$$

- By Parserval equality

$$\int_0^1 |f(e^{2\pi it})|^2 dt = \sum_{k=0}^{d} |a_k|^2 \leq (d+1)H(f)^2$$

- Thus $M(f) \leq \sqrt{d+1}H(f)$ □

Bounds on Heights of Products

Corollary

$$e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h), \quad d = \deg(gh)$$

Proof of upper bound

Bounds on Heights of Products

Corollary

$$e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h), \quad d = \deg(gh)$$

Proof of upper bound

Trivial

Bounds on Heights of Products

Corollary

$$e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h), \quad d = \deg(gh)$$

Proof of upper bound

Trivial

Proof of lower bound

- Approximate by Mahler measure:

Bounds on Heights of Products

Corollary

$$e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h), \quad d = \deg(gh)$$

Proof of upper bound

Trivial

Proof of lower bound

- Approximate by Mahler measure:
  - $H(gh) \geq \frac{M(gh)}{\sqrt{d+1}}$

Bounds on Heights of Products

Corollary

$$e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h), \quad d = \deg(gh)$$

Proof of upper bound

Trivial

Proof of lower bound

- Approximate by Mahler measure:
  - $H(gh) \geq \frac{M(gh)}{\sqrt{d+1}}$
  - $M(g)M(h) \geq H(g)H(h)2^{-d+2}$

Bounds on Heights of Products

Corollary

$$e^{-d}H(g)H(h) \le H(gh) \le dH(g)H(h), \quad d = \deg(gh)$$

Proof of upper bound

Trivial

Proof of lower bound

- Approximate by Mahler measure:
  - $H(gh) \ge \frac{M(gh)}{\sqrt{d+1}}$
  - $M(g)M(h) \ge H(g)H(h)2^{-d+2}$
- Multiplicativity: $M(gh) = M(g)M(h)$.

Bounds on Heights of Products

Corollary

$$e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h), \quad d = \deg(gh)$$

Proof of upper bound

Trivial

Proof of lower bound

- Approximate by Mahler measure:
  - $H(gh) \geq \frac{M(gh)}{\sqrt{d+1}}$
  - $M(g)M(h) \geq H(g)H(h)2^{-d+2}$
- Multiplicativity: $M(gh) = M(g)M(h)$.
- Conclude: $H(gh) \geq \frac{H(g)H(h)}{2^{d-2}\sqrt{d+1}} \geq e^{-d}H(g)H(h)$

$\square$

Kuba's Theorem: Best Bound for Large Height

Theorem (Kuba 2009)

$$R_d(B) \ll C_d B^{-1} \qquad (d \geq 3)$$

Kuba's Theorem: Best Bound for Large Height

Theorem (Kuba 2009)

$$R_d(B) \ll C_d B^{-1} \qquad (d \geq 3)$$

(recall: $e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h)$)

Proof – Step 1: A reduction

- $R_d(B) \leq \sum_{1\leq k\leq d/2} \mathbb{P}(f = gh, \deg g = k)$

Kuba's Theorem: Best Bound for Large Height

Theorem (Kuba 2009)

$$R_d(B) \ll C_d B^{-1} \qquad (d \geq 3)$$

(recall: $e^{-d} H(g)H(h) \leq H(gh) \leq dH(g)H(h)$)

Proof – Step 1: A reduction

- $R_d(B) \leq \sum_{1 \leq k \leq d/2} \mathbb{P}(f = gh, \deg g = k)$
- $\mathbb{P}(f = gh, \deg g = k)$
  $= \mathbb{P}(f = gh, \deg g = k, H(g)H(h) \leq e^d B)$

Kuba's Theorem: Best Bound for Large Height

Theorem (Kuba 2009)

$$R_d(B) \ll C_d B^{-1} \qquad (d \geq 3)$$

(recall: $e^{-d}H(g)H(h) \leq H(gh) \leq dH(g)H(h)$)

Proof – Step 1: A reduction

- $R_d(B) \leq \sum_{1\leq k\leq d/2} \mathbb{P}(f = gh, \deg g = k)$
- $\mathbb{P}(f = gh, \deg g = k)$
  $= \mathbb{P}(f = gh, \deg g = k, H(g)H(h) \leq e^d B)$
- It suffices for prove: $\#\Omega_k \ll_d B^{d-1}$,
  $\Omega_k = \{(h,g) \in \mathbb{Z}[X]^2 :$
  $\deg g = k, \deg h = d-k,\ H(g)H(h) \leq e^d B\}$

Continuation of The Proof: Counting by Height

Need: $\#\Omega_k \ll_d B^{d-1}$

- $T = e^d B$
- $D(T) = \{(x, y) \in \mathbb{R}^2 : x, y \geq 1 \text{ and } xy \leq T\}$

Continuation of The Proof: Counting by Height

Need: $\#\Omega_k \ll_d B^{d-1}$

- $T = e^d B$
- $D(T) = \{(x,y) \in \mathbb{R}^2 : x, y \geq 1 \text{ and } xy \leq T\}$
- $$\#\Omega_k = \sum_{(x,y)\in D(T)\cap\mathbb{Z}^2} \sum_{\substack{\deg g = k, H(g)=x \\ \deg h = d-k, H(h)=y}} 1$$

Continuation of The Proof: Counting by Height

Need: $\#\Omega_k \ll_d B^{d-1}$

- $T = e^d B$
- $D(T) = \{(x,y) \in \mathbb{R}^2 : x, y \geq 1 \text{ and } xy \leq T\}$
- $\#\Omega_k = \sum_{(x,y)\in D(T)\cap\mathbb{Z}^2} \sum_{\substack{\deg g = k, H(g)=x \\ \deg h = d-k, H(h)=y}} 1$

$$\ll \sum_{(x,y)} 2(k+1)(2x+1)^{k-1} 2(d-k+1)(2y+1)^{d-k-1}$$

Continuation of The Proof: Counting by Height

Need: $\#\Omega_k \ll_d B^{d-1}$

- $T = e^d B$
- $D(T) = \{(x,y) \in \mathbb{R}^2 : x, y \geq 1 \text{ and } xy \leq T\}$
- $$\#\Omega_k = \sum_{(x,y)\in D(T)\cap\mathbb{Z}^2} \sum_{\substack{\deg g = k, H(g)=x \\ \deg h = d-k, H(h)=y}} 1$$
  $$\ll \sum_{(x,y)} 2(k+1)(2x+1)^{k-1} 2(d-k+1)(2y+1)^{d-k-1}$$
- Bound by integral:

$$\iint_{D(T)} x^a y^b dxdy \asymp \begin{cases} T^{1+a}, & a > b \geq 0 \\ T^{1+a} \log T, & a = b. \end{cases}$$

Continuation of The Proof: Counting by Height

Need: $\#\Omega_k \ll_d B^{d-1}$

- $T = e^d B$
- $D(T) = \{(x,y) \in \mathbb{R}^2 : x, y \geq 1 \text{ and } xy \leq T\}$
- $$\#\Omega_k = \sum_{(x,y)\in D(T)\cap\mathbb{Z}^2} \sum_{\substack{\deg g = k, H(g)=x \\ \deg h = d-k, H(h)=y}} 1$$
  $$\ll \sum_{(x,y)} 2(k+1)(2x+1)^{k-1} 2(d-k+1)(2y+1)^{d-k-1}$$
- Bound by integral:
  $$\iint_{D(T)} x^a y^b dxdy \asymp \begin{cases} T^{1+a}, & a > b \geq 0 \\ T^{1+a}\log T, & a = b. \end{cases}$$
- $\#\Omega_k \ll_d T^{d-1} \ll_d B^{d-1}$ (since $d > 2$) $\square$

Summary

- We got the best bound in terms of B

$$B^{-1} \ll R_d(B) \ll_d B^{-1}$$

Summary

- We got the best bound in terms of B

$$B^{-1} \ll R_d(B) \ll_d B^{-1}$$

- Dependence of the bounds on d is bad (super exponential in Kuba's and linear in Rivin's)

Summary

- We got the best bound in terms of B

$$B^{-1} \ll R_d(B) \ll_d B^{-1}$$

- Dependence of the bounds on d is bad (super exponential in Kuba's and linear in Rivin's)
- To have good bounds in terms of d, recall Dimitris Koukoulopoulos talk

Summary

- We got the best bound in terms of B

$$B^{-1} \ll R_d(B) \ll_d B^{-1}$$

- Dependence of the bounds on d is bad (super exponential in Kuba's and linear in Rivin's)
- To have good bounds in terms of d, recall Dimitris Koukoulopoulos talk
- What about Galois groups?

Probabilistic Galois Theory

LBS

Outline

Why Galois groups for irreducibility lovers?

- $f = X^d + \sum_{i=0}^{d-1} a_i X^i = \prod_{i=1}^{d} (X - \alpha_i)$

Why Galois groups for irreducibility lovers?

- $f = X^d + \sum_{i=0}^{d-1} a_i X^i = \prod_{i=1}^{d} (X - \alpha_i)$
- $L_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ the splitting field of f

Why Galois groups for irreducibility lovers?

- $f = X^d + \sum_{i=0}^{d-1} a_i X^i = \prod_{i=1}^{d} (X - \alpha_i)$
- $L_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ the splitting field of f
- $G_f := \mathrm{Gal}(L_f/\mathbb{Q}) \leq S_d$ (via action on the roots of f)

Why Galois groups for irreducibility lovers?

- $f = X^d + \sum_{i=0}^{d-1} a_i X^i = \prod_{i=1}^{d} (X - \alpha_i)$
- $L_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ the splitting field of f
- $G_f := \mathrm{Gal}(L_f/\mathbb{Q}) \leq S_d$ (via action on the roots of f)

- f irreducible iff G_f transitive

Why Galois groups for irreducibility lovers?

- $f = X^d + \sum_{i=0}^{d-1} a_i X^i = \prod_{i=1}^{d}(X - \alpha_i)$
- $L_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ the splitting field of f
- $G_f := \mathrm{Gal}(L_f/\mathbb{Q}) \leq S_d$ (via action on the roots of f)

- f irreducible iff G_f transitive
- $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ minimal and of degree d iff G_f primitive

Why Galois groups for irreducibility lovers?

- $f = X^d + \sum_{i=0}^{d-1} a_i X^i = \prod_{i=1}^{d} (X - \alpha_i)$
- $L_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ the splitting field of f
- $G_f := \mathrm{Gal}(L_f/\mathbb{Q}) \leq S_d$ (via action on the roots of f)

- f irreducible iff G_f transitive
- $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ minimal and of degree d iff G_f primitive
- f irreducible and $\frac{f(X)}{X-\alpha_1}$ irreducible in $\mathbb{Q}(\alpha_1)[X]$ iff G_f doubly transitive

Why Galois groups for irreducibility lovers?

- $f = X^d + \sum_{i=0}^{d-1} a_i X^i = \prod_{i=1}^{d} (X - \alpha_i)$
- $L_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ the splitting field of f
- $G_f := \mathrm{Gal}(L_f/\mathbb{Q}) \leq S_d$ (via action on the roots of f)

- f irreducible iff G_f transitive
- $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ minimal and of degree d iff G_f primitive
- f irreducible and $\frac{f(X)}{X-\alpha_1}$ irreducible in $\mathbb{Q}(\alpha_1)[X]$ iff G_f doubly transitive
- For large d,
  $f, \frac{f(X)}{X-\alpha_1}, \ldots, \frac{f(X)}{\prod_{i=1}^{5}(X-\alpha_i)}$ are irreducible iff $\frac{f(X)}{X-\alpha_1}, \ldots, \frac{f(X)}{\prod_{i=1}^{d-2}(X-\alpha_i)}$ are irreducible (over the respective fields)
  (uses the classification of finite simple groups)

Most Polynomials Have Full Galois group

Theorem

Let f be a uniformly chosen from $M_d(B)$. Then

$$\lim_{B\to\infty} \mathbb{P}(G_f = S_d) = 1$$

Most Polynomials Have Full Galois group

Theorem

Let f be a uniformly chosen from $M_d(B)$. Then

$$\lim_{B\to\infty} \mathbb{P}(G_f = S_d) = 1$$

Preliminary reduction

- $\lambda_{f \mod p} := (\lambda_1, \ldots, \lambda_d)$, λ_i is the number of irreducible factors of degree i of $f \mod p$
- If there exist p_1, p_2, p_3 such that $\lambda_{f \mod p_1} = (0, \ldots, 0, 1)$, $\lambda_{f \mod p_2} = (d-2, 1, 0, \ldots, 0)$, and $\lambda_{f \mod p_3} = (1, 0 \ldots, 0, 1, 0)$, then $G_f = S_d$
- It suffices to prove that

$$\rho := \mathbb{P}(\lambda_{f \mod p} \neq \lambda, 2 < p < \alpha) \to 0$$

Proof

$$\rho := \mathbb{P}(\lambda_{f \mod p} \neq \lambda, 2 < p < \alpha)$$

- Take uniform $f \in M_d(B)$:

Proof

$$\rho := \mathbb{P}(\lambda_{f \mod p} \neq \lambda, 2 < p < \alpha)$$

- Take uniform $f \in M_d(B)$:
  - If $p \mid 2B + 1$

$$\mathbb{P}(\lambda_{f \mod p}) \leq c.$$

Proof

$$\rho := \mathbb{P}(\lambda_{f \mod p} \neq \lambda, 2 < p < \alpha)$$

- Take uniform $f \in M_d(B)$:
  - If $p \mid 2B+1$
    $$\mathbb{P}(\lambda_{f \mod p}) \leq c.$$
  - If $2B+1 = \prod_{2<p<\alpha} p \asymp e^{\alpha}$
    $$\rho \leq c^{\alpha}$$

Proof

$$\rho := \mathbb{P}(\lambda_{f \mod p} \neq \lambda, 2 < p < \alpha)$$

- Take uniform $f \in M_d(B)$:
  - If $p \mid 2B + 1$
    $$\mathbb{P}(\lambda_{f \mod p}) \leq c.$$
  - If $2B + 1 = \prod_{2<p<\alpha} p \asymp e^{\alpha}$
    $$\rho \leq c^{\alpha}$$
  - For general B, (Black Board)
    $$\rho \leq c^{\alpha} + O(e^{\alpha} B^{-1})$$

Proof

$$\rho := \mathbb{P}(\lambda_{f \mod p} \neq \lambda, 2 < p < \alpha)$$

- Take uniform $f \in M_d(B)$:
  - If $p \mid 2B + 1$
    $$\mathbb{P}(\lambda_{f \mod p}) \leq c.$$
  - If $2B + 1 = \prod_{2<p<\alpha} p \asymp e^{\alpha}$
    $$\rho \leq c^{\alpha}$$
  - For general B,
    $$\rho \leq c^{\alpha} + O(e^{\alpha} B^{-1})$$
- Take $\alpha = \frac{\log B}{2}$,
  $$\rho \ll B^{-\delta} \to 0.$$

$\square$

Sharper Bounds

$$\mathbb{P}(G_f \neq S_d) \ll B^{-\delta}$$

Open Problem

How big can δ be?

Sharper Bounds

$$\mathbb{P}(G_f \neq S_d) \ll B^{-\delta}$$

Open Problem

How big can δ be?

Remarks

- Obviously $\delta \leq 1$
- Results:
  - 1936 Van der Waerden $\delta = 1/6$
  - 1972 Gallagher $\delta = 1/2$
  - 2013 Dietmann $\delta = 2 - \sqrt{2}$
  - 2017 Rivin $\mathbb{P}(G_f \neq A_d, S_d) \leq B^{-1+\epsilon}$
- Common belief $\mathbb{P}(G_f \neq S_d) \sim \mathbb{P}(f \text{ reducible}) \asymp B^{-1}$

Other Groups

Very Hard Open Problems

- $\mathbb{P}(G_f \neq S_d \text{ transitive}) \ll B^{-???}$

Other Groups

Very Hard Open Problems

- $\mathbb{P}(G_f \neq S_d \text{ transitive}) \ll B^{-???}$
- What is the next probable transitive group?

Other Groups

Very Hard Open Problems

- $\mathbb{P}(G_f \neq S_d \text{ transitive}) \ll B^{-???}$
- What is the next probable transitive group?
- How improbable that $G_f = A_d$ (bound $\mathrm{disc}(f) = \square$)?

Other Groups

Very Hard Open Problems

- $\mathbb{P}(G_f \neq S_d \text{ transitive}) \ll B^{-???}$
- What is the next probable transitive group?
- How improbable that $G_f = A_d$ (bound $\mathrm{disc}(f) = \Box$)?
- How improbable the event that G_f is primitive?

Other Groups

Very Hard Open Problems

- $\mathbb{P}(G_f \neq S_d \text{ transitive}) \ll B^{-???}$
- What is the next probable transitive group?
- How improbable that $G_f = A_d$ (bound $\mathrm{disc}(f) = \square$)?
- How improbable the event that G_f is primitive?
- How improbable the event the G_f regular (aka f Galois)?