Hurwitz Number Fields

David P. Roberts
University of Minnesota, Morris

1. Context coming from mass formulas

2. Sketch of definitions and key properties

3. A full Hurwitz number field with Galois group A_{25} and discriminant $d = 2^{56}\,3^{34}\,5^{30}$

4. Results and open problems

1. Context coming from mass formulas. The mass of an Q-algebra F is by definition $\mu(F) = 1/|\mathrm{Aut}(F)|$. Examples:

$$\begin{array}{rclcrcl} F & = & \mathbb{R} & : & \mu(\mathbb{R}^r \times \mathbb{C}^s) & = & \frac{1}{r!s!2^s} \\ F & = & \mathbb{Q}_p & : & \mu(\mathbb{Q}_{p^f}) & = & \frac{1}{f} \end{array}$$

The mass of a class of Q-algebras is the sum of the masses of one representing algebra for each isomorphism type. For example, the class of all unramified $\mathbb{Q}_p$-algebras of degree n has total mass 1, as in the case $n = 3$:

$$\mu(\mathbb{Q}_{p^3})+\mu(\mathbb{Q}_{p^2}\mathbb{Q}_p)+\mu(\mathbb{Q}_p\mathbb{Q}_p\mathbb{Q}_p) = \frac{1}{3}+\frac{1}{2}+\frac{1}{6} = 1.$$

More generally, for any tame partition $\tau \vdash n$ the class of $\mathbb{Q}_p$-algebras with ramification partition τ has total mass 1.

Total mass $\mu_n(\mathbb{Q}_v)$ of $\mathbb{Q}_v$-algebras of degree n:

$v \backslash n$	1	2	3	4	5	6	7	8	9
∞	1	1	.66	.47	.22	.11	.05	.02	.01
2	1	4	5	36	40	145	180	1572	1712
3	1	2	9	11	19	83	99	172	1100
5	1	2	3	5	27	31	55	82	130

Let $NF_n(d)$ be the number of degree n number fields of absolute discriminant d, which are full in the sense that $G \in \{A_n, S_n\}$. Some average cardinalities $|NF_n(d)|$:

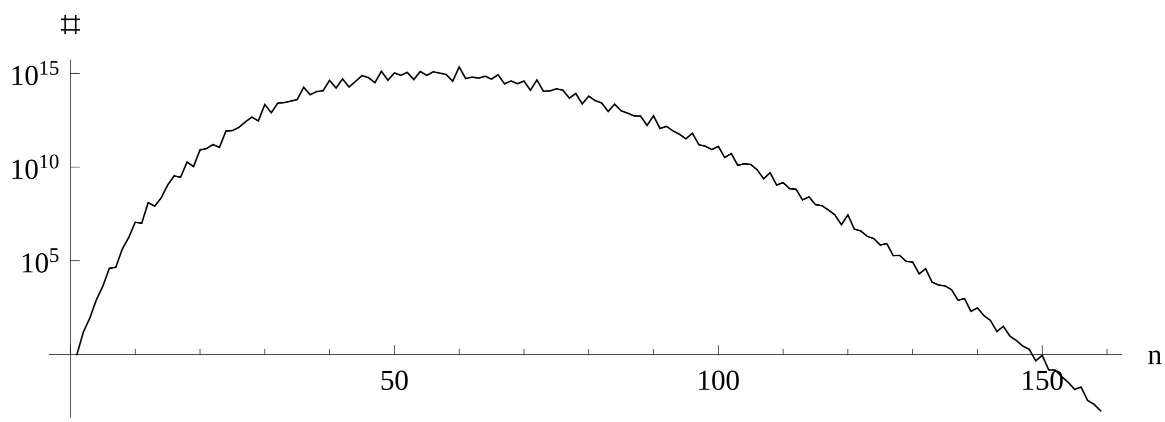
	1 -1000	1001 -2000	2001 -3000	3001 -4000	Limit			
5	.000	.003	.004	.006	$\cdots$	$\approx$	.150	[B]
4	.018	.043	.052	.056	$\cdots$	$\approx$	.253	[B]
3	.154	.177	.184	.197	$\frac{1}{3\zeta(3)}$	$\approx$	.277	[DH]
2	.607	.611	.602	.613	$\frac{1}{\zeta(2)}$	$\approx$	.608	

A natural local-global heuristic for $n \geq 3$ is that on average

$$|NF_n(\prod_p p^{c_p})| \approx \frac{1}{2}\mu_n(\mathbb{R}) \prod_p \mu_n(\mathbb{Q}_p, p^{c_p}).$$

Here $\mu_n(\mathbb{Q}_p, p^{c_p})$ is the total mass of $\mathbb{Q}_p$-algebras of degree n and discriminant p^{c_p}. For $n = 3$, 4, and 5, this heuristic is exactly right in the limit of large $|d|$.

What about the vertical rather than horizontal direction? Let $NF_n(\mathcal{P})$ be the set of full fields of degree n ramified within a given finite set $\mathcal{P}$ of primes. The heuristic gives e.g. the following predictions for $|NF_n(\{2,3,5\})|$.



In fact, for any fixed $\mathcal{P}$, the heuristic says that $|NF_n(\mathcal{P})|$ is eventually zero.

However with Venkatesh we expect that "Hurwitz number fields" form an enormous exception to the mass heuristic:

Conjecture. *Suppose $\mathcal{P}$ contains the set of primes dividing a finite nonabelian simple group. Then* $\limsup |NF_n(\mathcal{P})| = \infty$.

2. Sketch of definitions and key properties.

A *Hurwitz parameter* is a triple $h = (G, C, \nu)$ where

G is a finite centerless group,
$C = (C_1, \ldots, C_r)$ is a list of conjugacy classes,
$\nu = (\nu_1, \ldots, \nu_r)$ is a list of positive integers,
The quotient elements $[C_i]$ generate G^{ab}
and satisfy $\prod [C_i]^{\nu_i} = 1$.

A Hurwitz parameter h determines an unramified covering of complex algebraic varieties:

$$\pi_h : \mathrm{Hur}_h \to \mathrm{Conf}_\nu.$$

Here the cover Hur_h is a Hurwitz variety parameterizing certain covers of the complex projective line P^1 of type h. The base is the variety whose points are tuples $(D_1, \ldots, D_r)$ of disjoint divisors D_i in P^1, with D_i consisting of ν_i distinct points. The map π_h sends a cover to its branch locus.

Let $\mathcal{G}_h$ be the set of tuples

$(g_{1,1}, \ldots, g_{1,\nu_1}, \ \ldots, \ g_{r,1}, \ldots, g_{r,\nu_r}) \in C_1^{\nu_1} \times \cdots \times C_r^{\nu_r}$

which generate G and have product 1. Then G acts $\mathcal{G}_h$ by conjugation and the fiber $\mathsf{Hur}_{h,u}$ above any base point u can be identified with $\mathcal{F}_h = \mathcal{G}_h/G$.

A canonical approximation to the degree $n_h = |\mathcal{F}_h|$ is

$$\widehat{n}_h = \frac{\prod_{i=1}^r |C_i|^{\nu_i}}{|G||G'|}.$$

When enough sufficiently different C_i are present, in fact $n_h = \widehat{n}_h$.

The fundamental group $\pi_1(\mathsf{Conf}_\nu, u)$ can be identified with a classical braid group Br_ν. Under suitable hypotheses—most crucially that G is close to being a nonabelian simple group—the action of Br_ν on $\mathsf{Hur}_{h,u}$ is full, in the sense of having image all of A_n or S_n.

If all the C_i are rational, then the map π_h canonically descends to a map of varieties over $\mathbb{Q}$. Fibers $\mathsf{Hur}_{h,u}$ above rational points $u \in \mathsf{Conf}_\nu(\mathbb{Q}) \subset \mathsf{Conf}_\nu$ are the root-sets of Hurwitz number algebras $F_{h,u}$. If π_h is full, then $F_{h,u}$ is full for generic u, by the Hilbert irreducibility theorem.

The cover π_h has good reduction outside of $\mathcal{P}_G$, the set of primes dividing $|G|$. Let $\mathbb{Z}[1/\mathcal{P}]$ be the set of rational numbers having denominator divisible only by primes in $\mathcal{P}$. Then for $u \in \mathsf{Conf}_\nu(\mathbb{Z}[1/\mathcal{P}])$ the algebra can have bad reduction only at primes in $\mathcal{P}_G \cup \mathcal{P}$.

The sets $\mathsf{Conf}_\nu(\mathbb{Z}[1/\mathcal{P}_G])$ can be arbitrarily big in the way needed by the conjecture. So either the conjecture is true or specialization to $u \in \mathsf{Conf}_\nu(\mathbb{Z}[1/\mathcal{P}_G])$ behaves in an extremely non-generic way.

3. A full Hurwitz number field with Galois group A_{25} and discriminant $d = 2^{56}\,3^{34}\,5^{30}$.

Take

$$\begin{aligned} h &= (G, C, \nu) = (S_5, (2111, 5), (4, 1)), \\ u &= (D_1, D_2) = (\{-2, 0, 1, 2\}, \{\infty\}). \end{aligned}$$

The definition requires us to look at

$$g(z) = z^5 + z^4 + bz^3 + cz^2 + dz + e$$

with critical values $\{-2, 0, 1, 2\}$. Explicitly, we need to find solutions $(b, c, d, e, w) \in \mathbb{C}^5$ to

$$\mathrm{Res}_z(g(z) - t, g'(z)) = w(t+2)t(t-1)(t-2).$$

Finding these solutions takes $\approx$ one second.

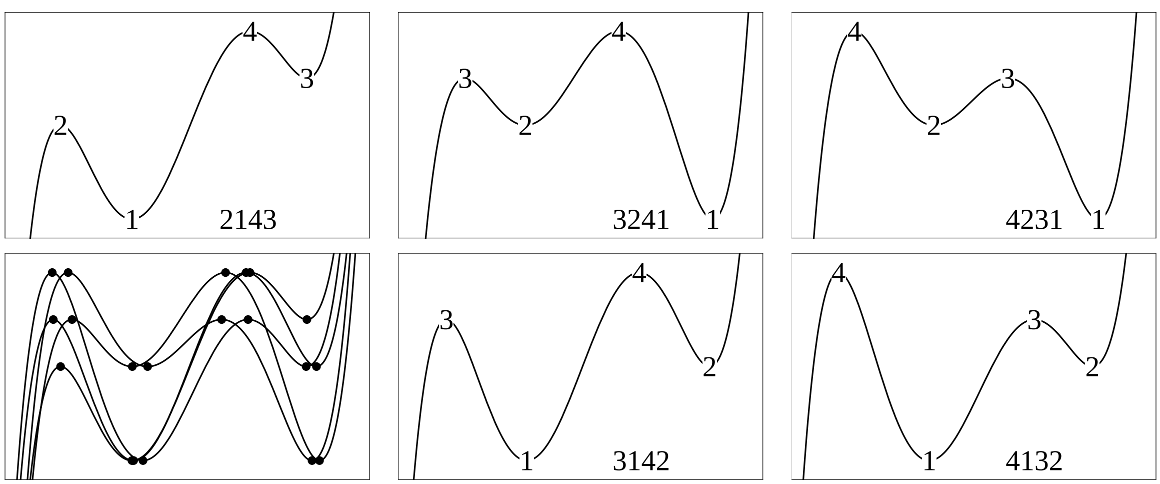
Exactly 25 different e work. They are the roots of an irreducible degree 25 polynomial $f(x)$. The Hurwitz number field

$$F_{h,u} = \mathbb{Q}[x]/f(x)$$

has discriminant $d = 2^{56}\,3^{34}\,5^{30}$. Fixing h but varying $u \in \mathrm{Conf}_{4,1}(\mathbb{Z}[1/\{2, 3, 5\}])$ gives more than ten thousand different $F_{h,u}$. All have $d = \pm 2^a 3^b 5^c$ and Galois group in $\{A_{24}, S_{24}, A_{25}, S_{25}\}$.

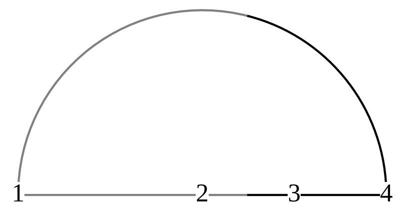
The intuitive reason that a Hurwitz number field $F_{h,u} = \mathbb{Q}[x]/f(x)$ is special is that each root of a defining polynomial $f(x)$ is not just a complex number. Rather "behind" this complex number is a delicate geometric situation: the unique covering of P^1_t with a prescribed topology.

For the five real e, the coverings $\mathsf{P}^1_z \to \mathsf{P}^1_t$ are as follows (drawn in the real z-t plane and also superimposed).

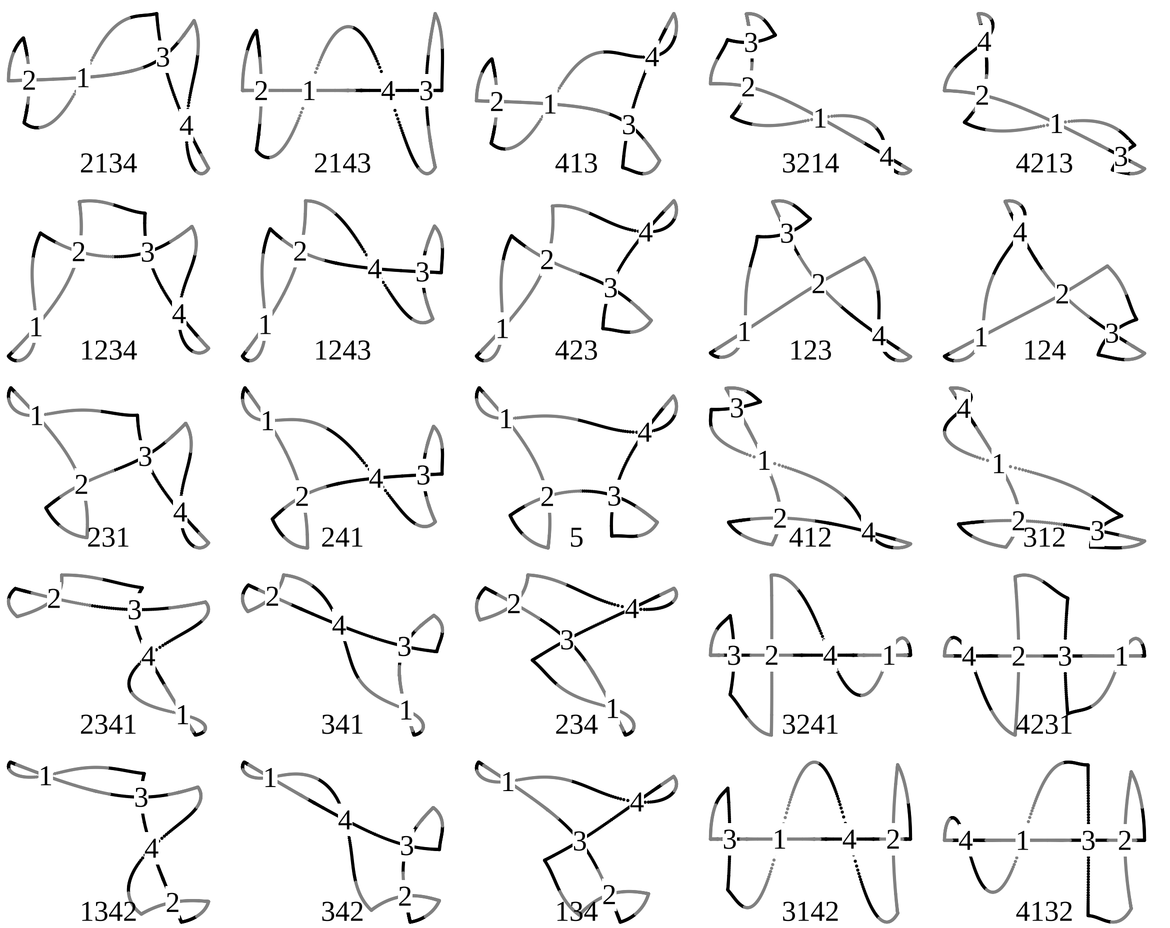


In general, there are $n = [F_{h,u} : \mathbb{Q}]$ different geometric objects, with their arithmetic coordinated by $F_{h,u}$.

To get images for all 25 different e, we draw



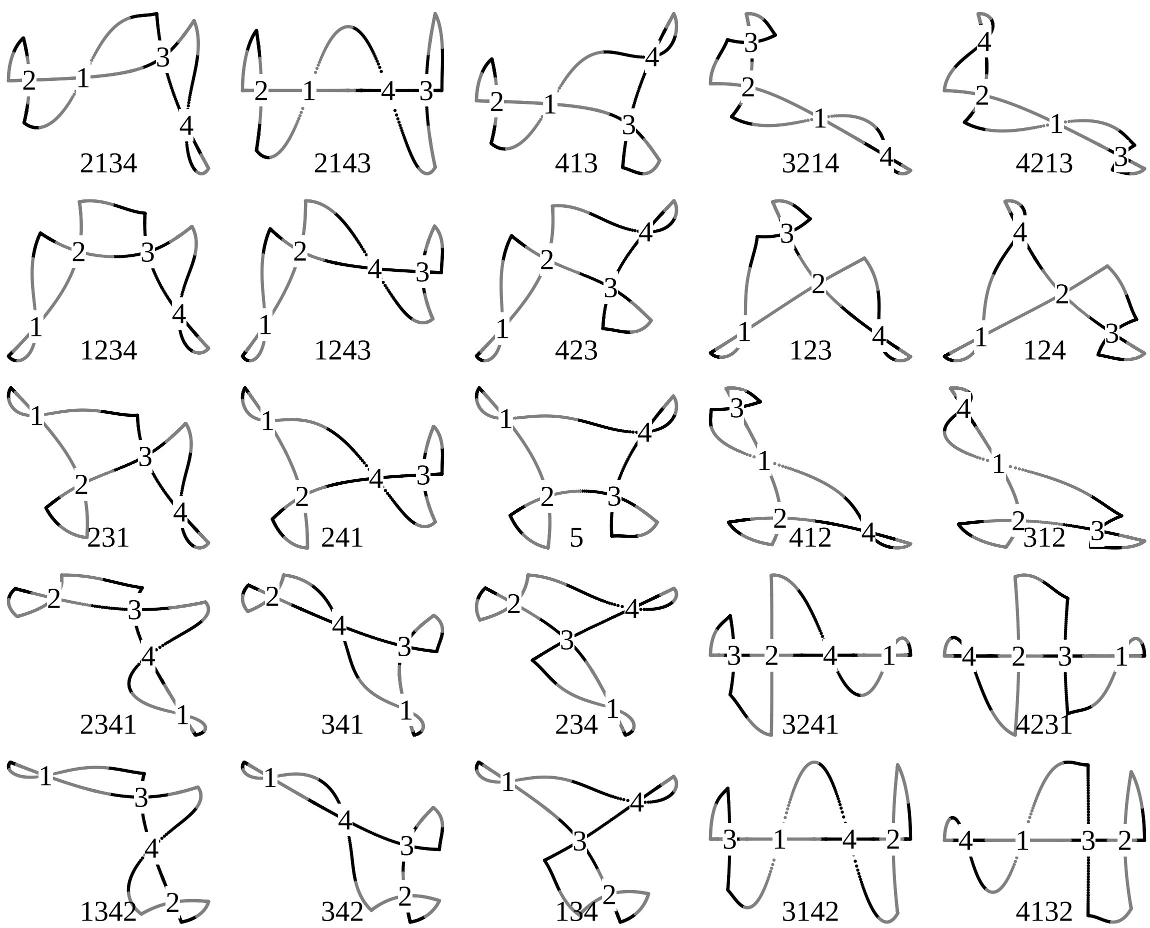
in the t-plane. Then its preimages in the z plane are



$$
\begin{array}{ccccc}
F & \longrightarrow & G & \longrightarrow & H \\
\downarrow & & \downarrow & & \downarrow \\
B3 & \longrightarrow & I & \longrightarrow & C3 \\
\downarrow & & \downarrow & & \downarrow \\
C2 & \longrightarrow & J & \longrightarrow & D2
\end{array}
\qquad
\begin{array}{ccc}
A3 & \longrightarrow & F \\
\downarrow & & \downarrow \\
B2 & \rightarrow & D3 \\
\downarrow & & \downarrow \\
H & \longrightarrow & A2
\end{array}
$$

$$
\begin{array}{ccccc}
E3 & \longrightarrow & J & \longrightarrow & B1 \\
\downarrow & & \downarrow & & \downarrow \\
I & \longrightarrow & E1 & \rightarrow & D1
\end{array}
\qquad
\begin{array}{ccc}
E2 & \rightarrow & C1 \\
\downarrow & & \downarrow \\
G & \longrightarrow & A1
\end{array}
$$

Actions of the standard generators σ_1 (vertical arrows), σ_2 (symbols), and σ_3 (horizontal arrows) of the braid group $\mathrm{Br}_{4,1}$ are given above.



4. Results and Open Problems.

A. Explicit equations for the covers $\mathsf{Hur}_h \to \mathsf{Conf}_\nu$ have been worked out in a broad range of situations:

- exotic groups like $SL_3(3)$, $G_2(2)$, $Sp_4(3)$, M_{12}, . . . ;
- constrained ramification and large degrees like $\{2, 3, 5\}$ and $n = 1200$;
- certain sequences with $G = S_d$ with d and n both increasing without bound.

Further understanding geometry would allow computations in new regimes (higher genus..., more ramification points...)

B. Tame ramification is completely understood: given (h, u) and a tame prime p, the partition of n measuring p-adic ramification in $F_{h,u}$ is given by a universal braid group formula.

Wild ramification experimentally is subject to strong upper bounds. For example, for degree 25 fields of discriminant $\pm 2^a 3^b 5^c$, the locally allowed maxima are $(a, b, c) = (110, 64, 74)$. The largest exponents occurring in the $h = (S_5, (2111, 5), (4, 1))$ family are $(79, 57, 52)$. In larger degree, the bounds are much stronger.

Open problem: get formulas for wild ramification in terms of (h, u) and establish the upper bounds.

C. Specialization has been observed to be near generic to start with and become more generic in higher degrees.

Open problem: control specialization enough to prove the expected $\limsup NF_n(\mathcal{P}) = \infty$!