Hurwitz Number Fields

David P. Roberts
University of Minnesota, Morris

1. Some background

2. A conjecture on number fields of arbitrarily large degree ramified within a given finite set P of primes

3. A family of HNFs with $P = \{2, 3, 5\}$

4. General definition of HNFs $K_{h,u}$

5. A geometric theorem towards the conjecture

6. Arithmetic evidence supporting the conjecture

1. Some background. Call a degree m number field K *full* if its associated Galois group Gal(K) is all of A_m or S_m. For P a finite set of primes, let $F_P(m)$ be the number of full degree m number fields ramified within P.

Some known values for $F_P(m)$:

P	1	2	3	4	5	6	7	$8 \cdots$	15	$16 \cdots$
$\emptyset$	1	0	0	0	0	0	0	$0 \cdots$	0	$0 \cdots$
$\{2\}$	1	3	0	0	0	0	0	$0 \cdots$	0	
$\{2,3\}$	1	7	9	23	5	62	10			

Also $F_{\{2,3\}}(m) > 0$ for m in

$\{8, 9, 10, 11, 12, 17, 18, 25, 28, 30, 32, 33, 36, 64\}$.

(E.g. $K = \mathbb{Q}[x]/(x^9 + 9x + 8)$ has associated Galois group Gal(K) $= S_9$ and field discriminant disc(K) $= 2^{25}3^{12}$ and so contributes to $F_{\{2,3\}}(9)$.).

Mass heuristics, very successful in other contexts, here suggest that for any fixed P, the series $F_P(m)$ is eventually zero.

2. The conjecture. Say that a finite set of primes P is *anabelian* if it contains the set of primes dividing the order of a nonabelian finite simple group. Thus, e.g. the only anabelian sets of size ≤ 3 are $\{2,3,p\}$ for $p \in \{5,7,13,17\}$.

From Hurwitz number fields—defined shortly!—with Venkatesh we expect

Unboundedness Conjecture. *For anabelian P, the sequence $F_P(m)$ is unbounded.*

Thus instead of $\lim F_P(m) = 0$, we expect $\limsup F_P(m) = \infty$!

A speculative complement to the conjecture is that F_P has finite support for abelian P and density zero support for anabelian P. At any rate, Hurwitz number fields sit in a very extreme position among all known number fields.

3. A degree 25 family of HNFs

Sample problem from a Calc I midterm:

Sketch the graph of a quintic polynomial

$$g(x) = x^5 + bx^3 + cx^2 + dx + e$$

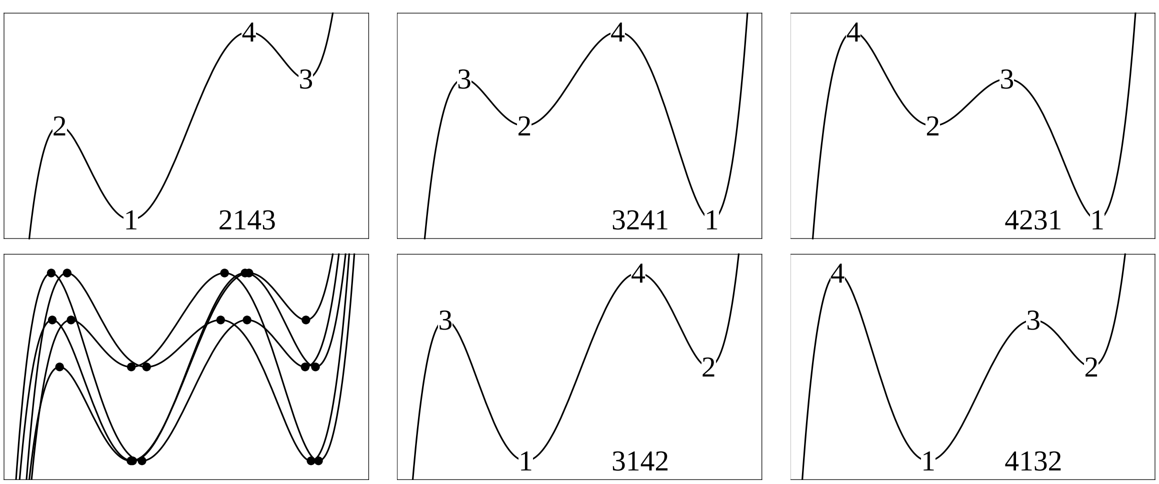
having critical values -2, 0, 1, 2.

Answer from an excellent student who misunderstood "sketch" as "compute."

I need to find solutions $(b, c, d, e, w) \in \mathbb{R}^5$ to

$$\mathrm{Res}_x(g(x) - y, g'(x)) = w(y+2)y(y-1)(y-2).$$

Equating coefficients of y^i, I get five equations in five unknowns. My computer found in under a second that there are five solutions. Graphed and superimposed (in the hope of extra credit) they are as follows:



The student’s five solutions are built from the five real roots of

$$
\begin{aligned}
f(e) \quad = \quad & 20792638970243532758049674326179 84e^{25} \\
& -12995399356402207973781046453862400e^{24} \\
& +93742854732380510644201819471872 00e^{23} \\
& +100171812470626687586960200119091200e^{22} \\
& -20727451405369007540615162930135 0400e^{21} \\
& -24440648485691944168305008949854 2080e^{20} \\
& +101861960013572880719815150235811 8400e^{19} \\
& -12267453212464931721580525199032 3200e^{18} \\
& -23675714046893917304951891067666 43200e^{17} \\
& +18317382831311241748601911539400 70400e^{16} \\
& +26833100210484016144678808440956 51840e^{15} \\
& -39811406344420784211732726917627 90400e^{14} \\
& -76365643082926987208453415795425 2800e^{13} \\
& +39961889470515964727273293854277 63200e^{12} \\
& -14095184028558973442209214433624 06400e^{11} \\
& -18104856943860633561679808562036 12160e^{10} \\
& +15538671755418495275070089128813 76900e^{9} \\
& +56743922361314868816389478767887 800e^{8} \\
& -50559270568048999491263638919404 1700e^{7} \\
& +16549440069297154922091570709368 6900e^{6} \\
& +22273319577181658254915819239436 920e^{5} \\
& -13748301792342333982413241472039 400e^{4} \\
& -13650800003596942907417339419791 75e^{3} \\
& +46454235070189815536040760061695 0e^{2} \\
& +90817899583985126224506334951600e \\
& +4543326944239835953052526892234
\end{aligned}
$$

$K = \mathbb{Q}[e]/f(e)$ is a Hurwitz number field. We are working with quintic polynomials and our specialization polynomial

$$s(y) = (y+2)y(y-1)(y-2)$$

has discriminant $2^8 3^2$. Theory then says disc(K) has the form $\pm 2^* 3^* 5^*$.

Computation says

$$\begin{aligned} \text{disc}(K) &= 2^{56}3^{34}5^{30}, \\ \text{Gal}(K) &= A_{25}. \end{aligned}$$

Hence $F_{\{2,3,5\}}(25) \geq 1$.

Changing the specialization polynomial to other quartic polynomials with bad reduction within $\{2,3,5\}$ gives $F_{\{2,3,5\}}(25) \geq 10983$.

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

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

Notation: $P =$ (Primes dividing $|G|$)
and $n = \sum \nu_i$.

Example from previous section

$$\begin{aligned} h &= (S_5, (2111, 5), (4, 1)) \\ P &= \{2, 3, 5\} \\ n &= 5 \end{aligned}$$

A Hurwitz parameter $h = (G, C, \nu)$ together with a normalization convention determines an unramified covering of $(n-3)$-dimensional $\mathbb{Q}$-varieties

$$\pi_h : X_h \to U_\nu.$$

(of degree m about $\frac{\prod_i |C_i|^{\nu_i}}{|G||G'|}$).

- The cover $X_h(\mathbb{C})$ parameterizes covers of the projective line P^1 "of type h."

- The base $U_\nu(\mathbb{C})$ is the variety whose points are normalized tuples $(D_1, \ldots, D_r)$ of disjoint divisors D_i of P^1, with D_i consisting of ν_i distinct points.

- The map π_h sends a cover to its branch locus.

In our example, $u = (D_1, D_2) = (\{-2, 0, 1, 2\}, \{\infty\})$ is a point in $U_{4,1}(\mathbb{Q})$. The fiber $\pi_h^{-1}(u) \subseteq X_h(\overline{\mathbb{Q}})$ consists of 25 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate points.

The cover $\pi_h : X_h \to U_\nu$ can be captured by a polynomial equation

$$f_h(u_1, \ldots, u_{n-3}; x) = 0.$$

For $u = (u_1, \ldots, u_{n-3}) \in \mathbb{Q}^{n-3}$ the algebra

$$K_{h,u} = \mathbb{Q}[x]/f_h(u_1, \ldots, u_{n-3}; x)$$

corresponds to the fiber over $\mathbb{Q}$. A Hurwitz number field is a field of the form $K_{h,u}$.

For generic u, the Galois groups $\mathrm{Gal}(K_{h,u}) \subseteq S_m$ all agree with a common group Gal_h computable purely geometrically via braid groups. We say h is *full* if Gal_h is A_m or S_m.

The cover extends smoothly over $\mathbb{Z}[1/P]$. For $u \in U_\nu(\mathbb{Z}[1/P])$, $K_{h,u}$ has bad reduction within P. For fixed nonempty P, the sets $U_\nu(\mathbb{Z}[1/P])$ can be arbitrarily large.

A natural guess is that for $u \in U_\nu(\mathbb{Z}[1/P])$ the fields $K_{h,u}$ are mostly pairwise non-isomorphic and usually $\mathrm{Gal}(K_{h,u}) = \mathrm{Gal}_h$.

5. A geometric theorem towards the conjecture

With Venkatesh we are studying the conditions on $h = (G, C, \nu)$ that make $X_h \to U_\nu$ full (i.e. $\mathrm{Gal}_h \in \{A_m, S_m\}$)

A special case of our theorem:

Theorem. *Suppose*
- G *is simple*
- $\mathrm{Out}(G)$ *is trivial.*
- $H_2(G, \mathbb{Z})$ *is trivial.*

Then $X_h \to U_\nu$ *is full for* $\min_i \nu_i$ *sufficiently large.*

The full theorem weakens all assumptions and gets a more complicated conclusion of the same nature.

The full theorem gives enough covers to prove the unboundedness conjecture, unless specialization to fibers above $U_\nu(\mathbb{Z}[1/P])$ behaves extremely non-generically.

6. Arithmetic evidence supporting the conjecture. Example with $P = \{2, 3, 5\}$:

$$X_{(S_6,(21111,321,3111,411),(2,1,1,1))} \to U_{2,1,1,1}$$

is full and $|U_{2,1,1,1}(\mathbb{Z}[1/P])| = 2947$. In explicit terms, we have a polynomial $f(u_1, u_2, x)$ of degree 202 in x and 2947 pairs

$$u = (u_1, u_2) \in \mathbb{Q}^2$$

which keep all ramification of

$$K_{h,u} = \mathbb{Q}[x]/f(u_1, u_2, x)$$

within $\{2, 3, 5\}$. Computation gives:

A: The 2947 $K_{h,u}$ are all non-isomorphic.
B: They are all full.

Hence $F_{\{2,3,5\}}(202) \geq 2947$. (The mass heuristic gives $\sum_{m \geq 202} F_{\{2,3,5\}}(m) \leq 10^{-15}$).

Specialization at all other studied families is always at or very near generic expectations. To establish the conjecture, one would need only very weak versions of A and B for general h.