Hurwitz Number Fields

David P. Roberts, U. of Minnesota, Morris
Akshay Venkatesh, Stanford University

Notation: $NF_m(\mathcal{P})$ is the set of isomorphism classes of degree m number fields ramified only within $\mathcal{P}$ and with associated Galois group all of A_m or S_m.

1. Sets $NF_m(\mathcal{P})$ and mass heuristics

2. First example

3. 10000 fields in $NF_{25}(\{2,3,5\})$

4. Generalities I: Families

5. Generalities II: Specialization

6. 2000 fields in $NF_{202}(\{2,3,5\})$

7. Concluding remarks

1. Sets $NF_m(\mathcal{P})$ and mass heuristics. Let $F_{\mathcal{P}}(m) = |NF_m(\mathcal{P})|$. Some known cases:

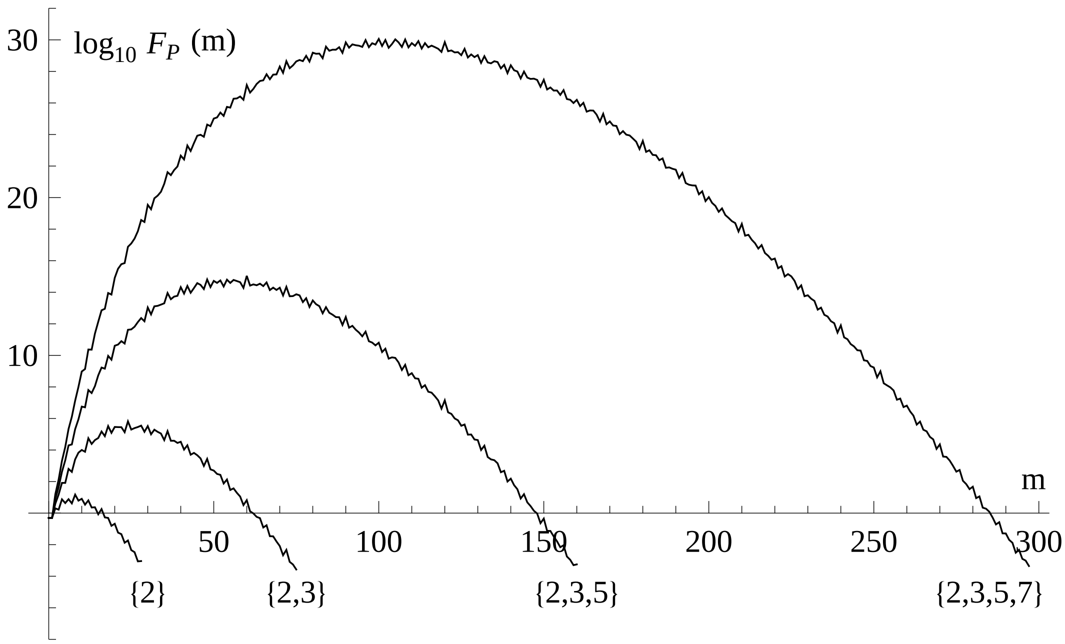
$\mathcal{P}$	1	2	3	4	5	6	7
$\{\}$	1	0	0	0	0	0	0
$\{2\}$	1	3	0	0	0	0	0
$\{2,3\}$	1	7	9	23	5	62	10
$\{2,3,5\}$	1	15	32	144	1415		
$\{2,3,5,7\}$	1	31	108	906	11465		
$\{2,3,5,7,11\}$	1	63	360	5488			
$\{2,3,5,7,11,13\}$	1	127	1168	31684			

E.g., $NF_5(\{2,3\}) = \{\mathbb{Q}[x]/f_i(x)\}_{i=1,\ldots,5}$ with

$$\begin{aligned}
f_1(x) &= x^5 - 2x^4 + 4x^3 - 6x + 12 \\
f_2(x) &= x^5 - 2x^4 + 2x^3 + 4x^2 - 5x + 2 \\
f_3(x) &= x^5 - x^4 - 2x^3 + 6x^2 - 6x + 6 \\
f_4(x) &= x^5 - 2x^3 - 4x^2 - 9x - 4 \\
f_5(x) &= x^5 - x^4 + 4x^3 - 12x^2 + 12x - 12
\end{aligned}$$

A local-global mass heuristic lets one predict $F_{\mathcal{P}}(m)$. For example, it predicts $F_{\{2,3,5,7\}}(5) \approx 15561$ while in fact $F_{\{2,3,5,7\}}(5) = 11465$. It seems reasonable to expect that the prediction is asymptotically correct as one goes down a column.

But what about going to the right on a row, i.e. the behavior of $F_{\mathcal{P}}(m)$ for fixed $\mathcal{P}$ and increasing m? The literal predictions of the mass heuristic are as follows in some examples:



This might lead one to expect that, for any fixed $\mathcal{P}$, no matter how large, $F_{\mathcal{P}}(m)$ is eventually zero. This may be indeed be correct for "small" $\mathcal{P}$. For example, the largest m for which $\begin{cases} F_{\{2\}}(m) \\ F_{\{2,3\}}(m) \end{cases}$ is known to be nonzero is $\begin{cases} m = 2 \\ m = 64 \end{cases}$.

However. . .

For Γ a non-abelian finite simple group, let $\mathcal{P}_\Gamma$ be the set of primes dividing $|\Gamma|$. Note that the only such $\mathcal{P}_\Gamma$ with $|\mathcal{P}_\Gamma| \leq 3$ are $\{2, 3, p\}$ with $p \in \{5, 7, 13, 17\}$.

Define $\mathcal{P}$ to be *large* if $\mathcal{P}$ contains some $\mathcal{P}_\Gamma$ and *small* otherwise. So if $|\mathcal{P}| \leq 2$ or $2 \notin \mathcal{P}$ then $\mathcal{P}$ is small.

This talk is about a systematic (and rather classical!) construction of what we call *Hurwitz number algebras.* Their ramifying primes are very well controlled and evidence points strongly to Galois groups being generically the full alternating or symmetric groups on the degree. Accordingly we now think,

Conjecture. *For any fixed large $\mathcal{P}$, the number $F_{\mathcal{P}}(m)$ can be arbitrarily large.*

2. First example. Consider polynomials in $\mathbb{C}[y]$ of the form

$$g(y) = y^5 + by^3 + cy^2 + dy + e.$$

The four critical values are given by the roots of the resultant

$$r(t) = \mathrm{Res}_y(g(y) - t, g'(y)).$$

Explicitly, this resultant works out to

$$\begin{aligned}
r(t) = {} & \\
& 3125t^4 \\
& +1250(3bc - 10e)t^3 \\
& + \left(108b^5 - 900b^3d + 825b^2c^2 - 11250bce + 2000bd^2\right. \\
& \qquad \left. +2250c^2d + 18750e^2\right) t^2 \\
& -2 \left(108b^5e - 36b^4cd + 8b^3c^3 - 900b^3de + 825b^2c^2e + 280b^2cd^2\right. \\
& \qquad -315bc^3d - 5625bce^2 + 2000bd^2e + 54c^5 + 2250c^2de \\
& \qquad \left. -800cd^3 + 6250e^3\right) t \\
& + \left(108b^5e^2 - 72b^4cde + 16b^4d^3 + 16b^3c^3e - 4b^3c^2d^2 - 900b^3de^2\right. \\
& \qquad +825b^2c^2e^2 + 560b^2cd^2e - 128b^2d^4 - 630bc^3de + 144bc^2d^3 \\
& \qquad -3750bce^3 + 2000bd^2e^2 + 108c^5e - 27c^4d^2 + 2250c^2de^2 \\
& \qquad \left. -1600cd^3e + 256d^5 + 3125e^4\right).
\end{aligned}$$

To find all polynomials $g(y)$ whose critical values are, say, -2, 0, 1, 2, we need to solve $r(t) = 3125(t+2)t(t-1)(t-2)$ for (b, c, d, e). The twenty-five e that arise are the roots of

$$F(e) \quad = \quad 2^{98}3^{8}e^{25} + \cdots + 4543326944239835953052526892234,$$

which is irreducible over $\mathbb{Z}$.

A better defining polynomial for $\mathbb{Q}[e]/F(e)$ is

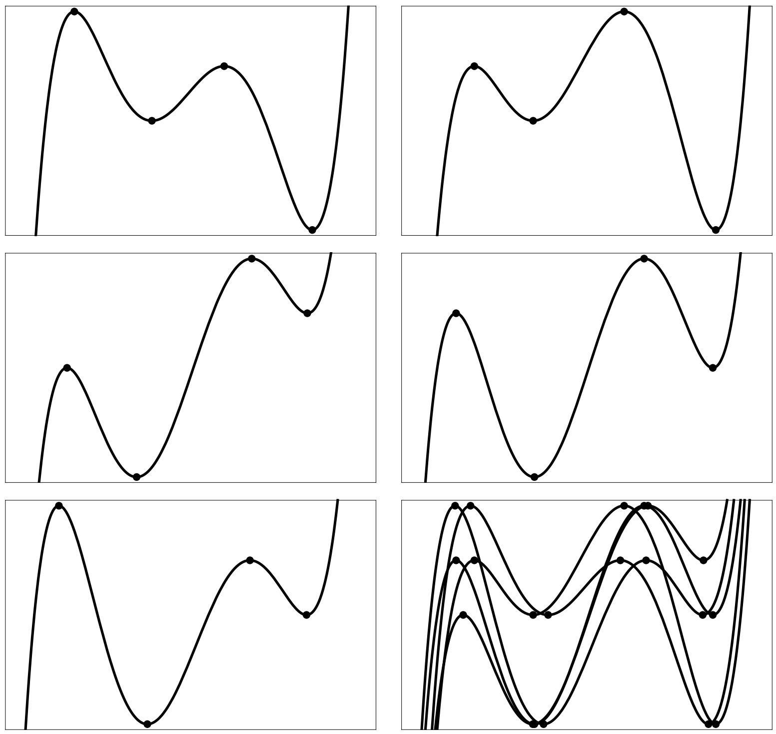
$$\begin{aligned} f(x) = & \\ & x^{25} - 5x^{24} + 15x^{23} - 5x^{22} - 380x^{21} + 1290x^{20} - 4500x^{19} \\ & -28080x^{18} + 183510x^{17} + 74910x^{16} - 3033150x^{15} + 4181370x^{14} \\ & +27399420x^{13} - 48219480x^{12} - 124127340x^{11} + 266321580x^{10} \\ & +466602765x^{9} - 592235505x^{8} - 905951965x^{7} + 1232529455x^{6} \\ & +2423285640x^{5} + 664599470x^{4} - 814165000x^{3} \\ & -517891860x^{2} - 58209720x + 2436924. \end{aligned}$$

Its field discriminant is known *a priori* to be of the form $\pm 2^{*}3^{*}5^{*}$ and is in fact

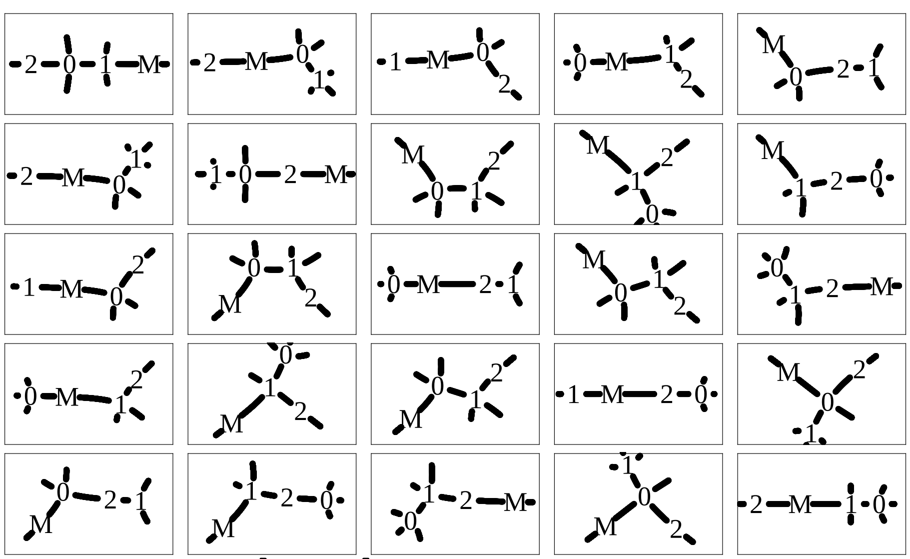
$$\begin{aligned} D &= 111918671858621262436761600000000000000000000000000000 \\ &= 2^{56}3^{34}5^{30}. \end{aligned}$$

Not much is known *a priori* about the Galois group of $f(x)$. It works out to A_{25}.

Some pictures illustrating the situation:



Five real polynomials with critical values −2, 0, 1, 2



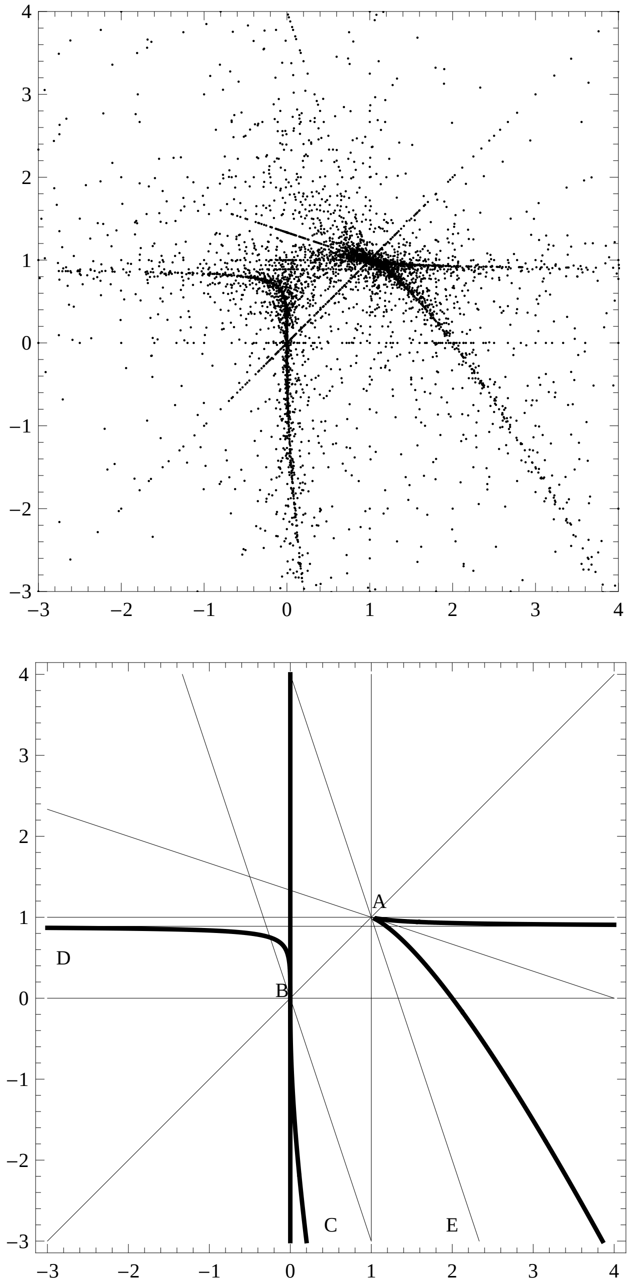
The preimage of $[-2, 2]$ under all twenty-five polynomials

3. 10000 fields in $NF_{25}(\{2,3,5\})$ Our *specialization polynomial* $(t+2)t(t-1)(t-2)$ can be replaced by any quartic polynomial with leading coefficient and discriminant divisible only by 2, 3, and 5. Via changes of coordinates, most cases are covered by the family

$$s(u,v;t) = t^4 - 6ut^2 - 8ut - 3uv.$$

The corresponding moduli polynomial $F(u,v;e)$ has 145 terms with coefficients averaging 37 digits.

A small search gets 11031 pairs (u,v) which keep ramification in $\{2,3,5\}$:

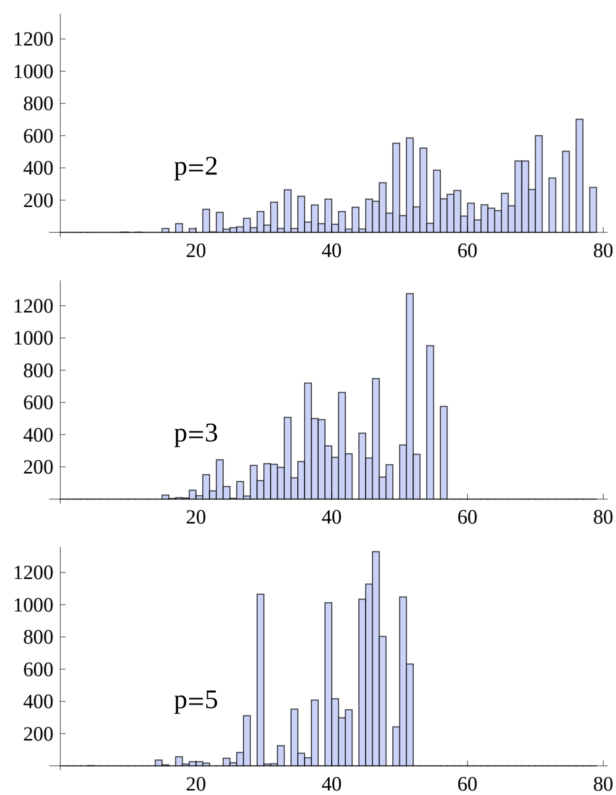


Top: Specialization points (u, v) for $F(u, v; e)$.
Bottom: the discriminant locus (thick) and special lines (thin).

Over each of the special lines, the defining equation can be much simplified. E.g. over $u = v$ it becomes

$$\begin{aligned} f_{AB}(u,x) = {} & 4(1-u)(x+2)\cdot \\ & \big(729x^8 - 486x^7 - 702x^6 - 8x^5 + 105x^4 + 1118x^3 \\ & \quad -1557x^2 + 1296x - 576\big)^3 \\ & -5^{15}u(x-1)^4x^9. \end{aligned}$$

Computation shows that all 11031 specialization points give A_{25} or S_{25} fields. The behavior of the exponents a, b, c in $D = \pm 2^a 3^b 5^c$ is very constrained:



4. Generalities I: Families. In general, a Hurwitz number algebra is indexed by its *parameter*,

$$H = (\lambda_1, \ldots, \lambda_\ell; Z_1, \ldots, Z_\ell; M).$$

The parameter for our first example was

$$H = (2111, 5; \{-2, 0, 1, 2\}, \{\infty\}; S_5).$$

In general, the λ_i are partitions of a given positive integer n, the Z_i are disjoint Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-stable subsets of $\mathbb{P} = \mathbb{C} \cup \{\infty\}$, and M is a transitive degree n permutation group of the form Γ or Γ.2 with Γ non-abelian simple.

Let X_H be the set of degree n covers of $\mathbb{P}$, ramified only over $\cup Z_i$, with local ramification partition λ_i for all $t \in Z_i$, and global monodromy group M. Then Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) acts naturally on X_H and the corresponding Hurwitz number algebra is K_H. Its primes of bad reduction are within the primes of bad reduction for $\cup Z_i$ and the primes dividing $|M|$.

Replacing each Z_i by its size z_i gives the corresponding familial parameter:

$$h = (\lambda_1, \ldots, \lambda_\ell; z_1, \ldots, z_\ell; M).$$

Each h gives a chain of varieties

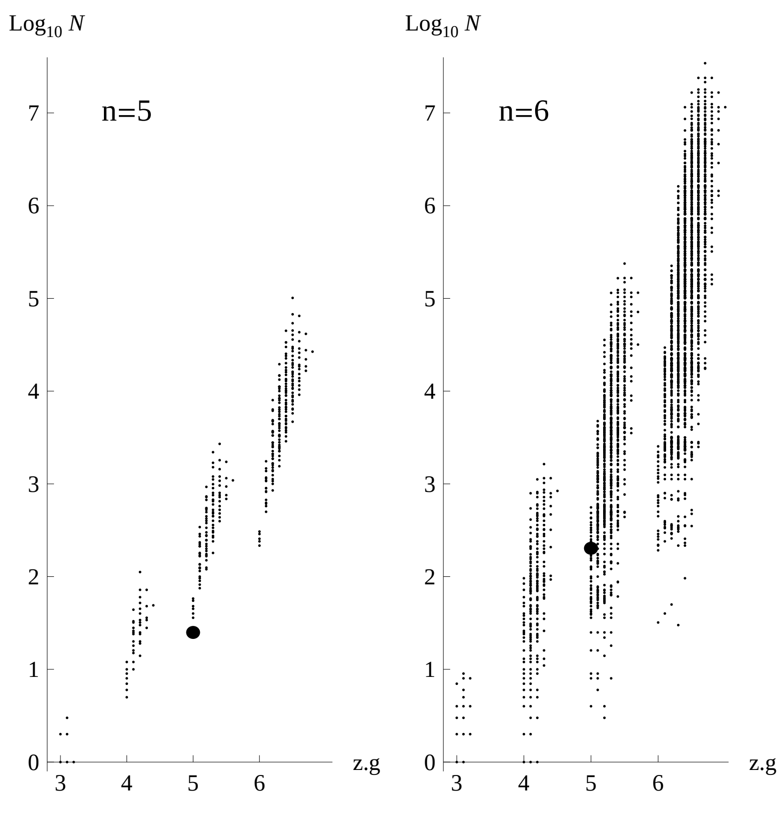
$$Y_h \stackrel{n}{\to} X_h \times \mathbb{P} \to X_h \stackrel{m}{\to} U_{z_1,\ldots,z_\ell}.$$

One starts with a focus on degree n covers of $\mathbb{P}$ and ends with a complicated degree m cover X_h of the very simple variety $U_{z_1,\ldots,z_\ell}$.

One can cut down dimensions by three via the natural $PGL_2(\mathbb{C})$ action. In our degree twenty-five case $h = (2111, 5; 4, 1; S_5)$, the u-v plane is an essential slice of the five-dimensional variety $U_{4,1}$. Over this slice, the cover X_h is given by the equation $F(u, v; e) = 0$.

Important invariants of families are

n, the degree of the original cover
z, the number of ramification points
g, the genus of the original cover
m, the degree of the moduli cover



Dots correspond to families

		$z = 11111$						
n	g	λ_1	λ_2	λ_3	λ_4	λ_5	m	μ
6	1	2	3	22	222	33	69	

		$z = 311$						
n	g	λ_1	λ_1	λ_1	λ_2	λ_3	m	μ
6	0	3	3	3	2	4	96	
6	0	2	2	2	4	5	75	
6	0	2	2	2	4	42	72	
6	0	22	22	22	2	222	60	6.0
6	0	2	2	2	22	6	54	
6	0	2	2	2	32	33	54	
5	0	2	2	2	3	4	48	
5	0	2	2	2	22	4	48	
5	0	2	2	2	3	32	45	
6	0	3	3	3	2	222	44	
6	0	2	2	2	3	6	36	
6	0	2	2	2	4	33	36	
5	0	2	2	2	22	32	36	
6	0	2	2	2	222	5	25	
6	0	2	2	2	222	42		16.0
6	1	222	222	222	2	3	9a	
6	0	2	2	2	222	33	9b	
6	1	222	222	222	2	22		6.0

		$z= 41$						
n	g	λ_1	λ_1	λ_1	λ_1	λ_2	m	μ
6	0	3	3	3	3	22	192	
5	**0**	**2**	**2**	**2**	**2**	**5**	**25**	

		$z = 32$						
n	g	λ_1	λ_1	λ_1	λ_2	λ_2	m	μ
5	0	3	3	3	2	2	55	
6	1	3	3	3	222	222	48	$1.\overline{3}$
5	0	22	22	22	2	2	40	

		$z = 5$						
n	g	λ_1	λ_1	λ_1	λ_1	λ_1	m	μ
6	0	3	3	3	3	3	96	

		$z = 2111$						
n	g	λ_1	λ_1	λ_2	λ_3	λ_4	m	μ
6	**0**	**2**	**2**	**3**	**4**	**32**	**202**	
6	0	3	3	2	22	4	168	
6	0	2	2	3	22	5	125	
6	0	2	2	3	22	42	100	
6	1	22	22	2	222	33	57	10.5
6	1	2	2	32	222	33	60	
6	0	2	2	22	32	222	60	
6	1	3	3	2	222	33	58	
6	0	22	22	2	3	222	57	
6	1	222	222	2	3	32	48	8.0
6	1	2	2	4	222	33	48a	4.5
6	1	222	222	2	3	4	48b	
6	0	2	2	3	32	222	52	
6	0	2	2	3	22	33	48	
6	0	3	3	2	22	222	42	
6	1	222	222	2	22	4	40a	6.0
6	0	2	2	22	4	222	40b	
6	0	2	2	3	4	222	36	

		$z= 221$						
n	g	λ_1	λ_1	λ_1	λ_2	λ_3	m	μ
6	0	2	2	22	22	42	128	
6	0	2	2	4	4	3	89	
6	0	2	2	3	3	42	80	
6	0	2	2	3	3	5	75	
6	1	2	2	33	33	22	60a	4.5
6	1	3	3	222	222	22	60b	4.0
6	1	22	22	222	222	3	54a	9.0
6	0	2	2	22	22	33	54b	4.5
6	1	2	2	33	33	3	60	
5	0	2	2	3	3	22	58	
5	0	2	2	22	22	3	48	
6	0	2	2	3	3	33	39	
6	1	2	2	222	222	5	25ab	
6	1	2	2	222	222	42	16ab	
6	1	2	2	222	222	33		8.5
6	0	2	2	222	222	22		8.0
6	0	2	2	222	222	3		4.0

Five-point families with genus ≤ 1 and low degree

5. Generalities II: Specialization. For each partition z, we have a base-stack U_z over $\mathbb{Z}$ which contains our specialization points (after quotient by PGL_2). We are interested in their points $U_z(\mathbb{Z}^{\mathcal{P}})$. These are very explicit sets.

Examples:

$$\begin{aligned} U_{1,1,1,1}(\mathbb{Z}^{\mathcal{P}}) &= \{t \in \mathbb{Z}^{\mathcal{P}\times} : t - 1 \in \mathbb{Z}^{\mathcal{P}\times}\} \\ U_{1,1,1,1}(\mathbb{Z}^{\{2,3\}}) &= S_3\{2, 3, 4, 9\} \quad \text{(21 elements)} \end{aligned}$$

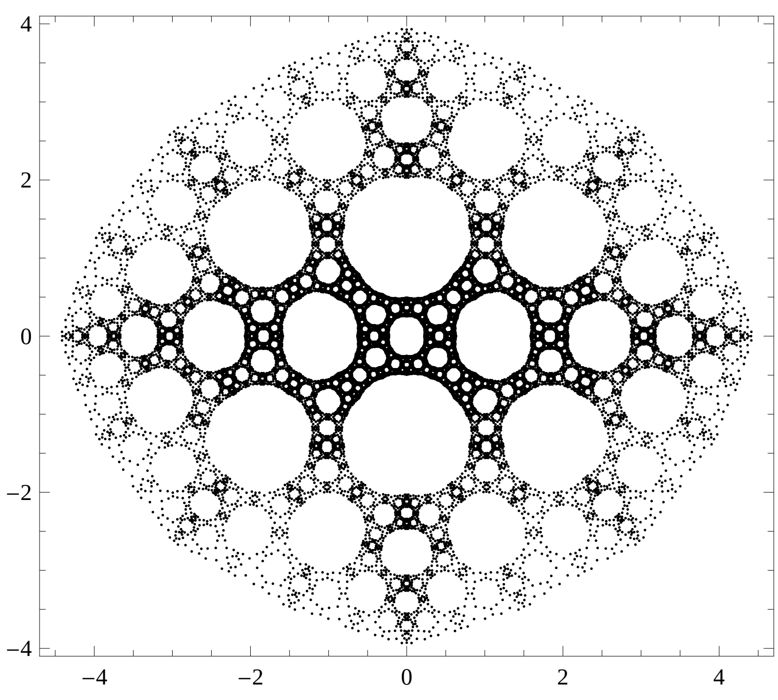
$$\begin{aligned} U_{3,1}(\mathbb{Z}^{\mathcal{P}}) &= \{j\text{-invs for ECs over } \mathbb{Z}^{\mathcal{P}}\} \\ |U_{3,1}(\mathbb{Z}^{\{2,3,5\}})| &= 440 \end{aligned}$$

It's easy to produce elements of these sets. In favorable cases, one can prove that there are no more elements, e.g. for the cases $U_{3^c2^b1^a}(\mathbb{Z}^{\{2,3,5\}})$. For example,

$$|U_{2^{15},1^4}(\mathbb{Z}^{\{2,3,5\}})| = 3,923,023,104,000.$$

For the conjecture, it is important to prove that for all large $\mathcal{P}$, the sets $U_z(\mathbb{Z}^{\mathcal{P}})$ can be arbitrarily large. In fact this is true for all non-empty $\mathcal{P}$, via cyclotomic polynomials and their near-relatives.

Example: the roots of an irreducible near-relative of a cyclotomic polynomial of degree $2^{15} = 43768$ and discriminant of the form $\pm 2^*$. This polynomial gives one of many systematically constructed points in $U_{43768,1,1,1}(\mathbb{Z}^{\{2\}})$.



6. 2000 fields in $NF_{202}(\{2,3,5\})$. To construct these fields:

I. Construct family belonging to

$h = (3_0 2_b 1_c, 3_1 111, 4_\infty 11, 21111; 1,1,1,2; S_6)$.

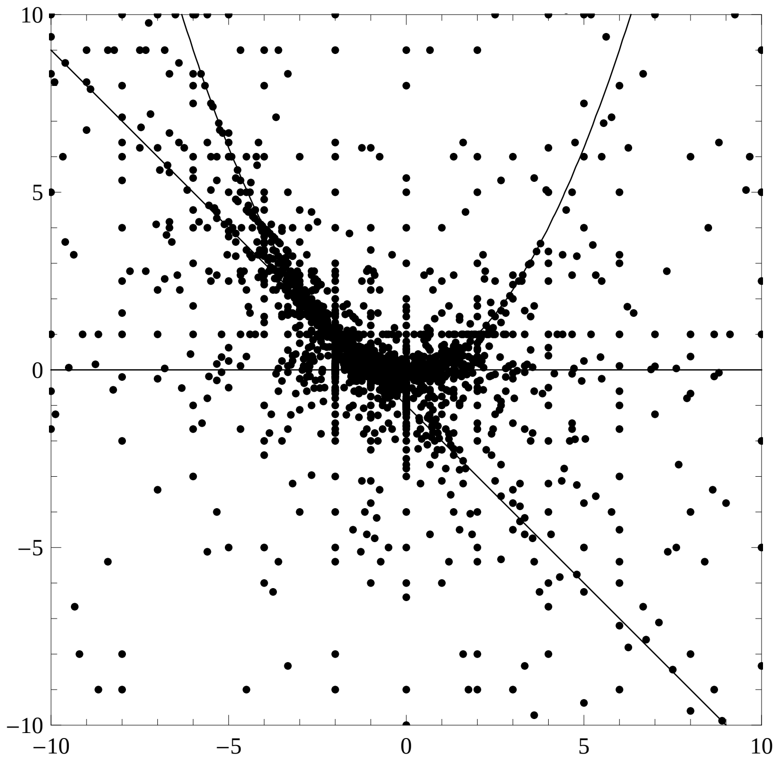
This procedure starts with consideration of

$$g(y) = \frac{ay^3(y-b)^2(y-c)}{y^2+dy+e}$$

with (a,b,c,d,e) chosen so that the critical values are 0, 1, ∞ and the two roots of (t^2+ut+v). The result is a polynomial $F(u,v;b)$ with 9226 terms.

II. Plug in the 2947 elements (u,v) in the specialization set $U_{1,1,1,2}(\mathbb{Z}^{\{2,3,5\}})$. Each gives a degree 202 polynomial of field discriminant of the form $\pm 2^a 3^b 5^c$. To support the conjecture, we would like many of these polynomials to be irreducible with Galois group all of A_{202} or S_{202}.

The specialization set $U_{1,1,1,2}(\mathbb{Z}^{\{2,3,5\}})$ is



For all 2947 specialization points, the Galois group of $F(u, v; b)$ is all of A_{202} or S_{202}.

Even degenerations of our polynomial $F(u, v; b)$ have degrees which are large enough to pose computational challenges. For example

$$F(-2t, t^2; x) = (3x^2-12x+10)^5 f_{32}(t, x)^3 f_{48}(t, x)^2$$

These degenerations give 4-point MNFs.

7. Concluding Remarks.

A. Starting with degree n families of Malle and others, involving the simple groups $\Gamma = PSL_2(7)$, $PSL_2(8)$, $PSL_2(11)$, M_{12}, we get degree m families, still with A_m and S_m as desired, but now with other bad primes, e.g. $\{2, 3, 7\}$.

B. There seems hope for predicting the ramification of Hurwitz number algebras in terms of the placement of the specialization point in the relevant specialization set $U_z(\mathbb{Z}^{\mathcal{P}})$.

C. So what does the sequence of $F_{\mathcal{P}}(m) = |NF_m(\mathcal{P})|$ look like for $\mathcal{P}$ large? We don't know, but perhaps something in the spirit of

$$\ldots, 0, 10^{10}, 0, \ldots, 0, 0, 10^{100}, 0, 0, \ldots, 0, 0, 0, 10^{1000}, 0, 0 \ldots$$