Lightly ramified number fields with Galois group $S.M_{12}.A$.

David P. Roberts
University of Minnesota, Morris

1. **Invariants of polynomials**

2. **Inverse Galois problems**

3. **The group M_{12} and its extensions**

4. **Construction of fields via specialization of three-point covers**

5. **Six partition triples**

6. **Number Fields I**

7. **Number Fields II**

8. **Number Fields III**

1. Invariants of polynomials. Given a degree n irreducible polynomial $f(x) \in \mathbb{Q}[x]$, two important associated quantities are its *Galois group* $G \subseteq S_n$ and its *field discriminant* $D \in \mathbb{Z}$. Both depend only on the *number field* $\mathbb{Q}[x]/f(x)$ associated to f.

There are many algorithms for computing G and D. As an example, $x^{12}-x-1$ has invariants

$$\begin{aligned} G &= S_{12}, \\ D &= -9201412118867 \\ &= -1237 \cdot 7438489991. \end{aligned}$$

"Most" polynomials behave exactly like this: G is all of S_n, and D is divisible by at least one large prime.

2. Inverse Galois problems. The classical inverse Galois problem is, *Given a finite group G, prove that there is a polynomial with Galois group G.* This problem is solved for many groups, for example all 26 sporadic groups except for M_{23} [MM].

There are many variants of the classical problem. For example, the *explicit* problem is to exhibit a polynomial with Galois group G. For the sporadic groups, this is solved for M_{11}, M_{12}, M_{22}, and M_{24} in [MZ], [MZ], [Ma], and [Gr]. For the monster, one would need a polynomial of degree $97,239,461,142,009,186,000$.

Another variant is to pay attention to ramification. For a given (G, D) the corresponding set $NF(G, D)$ of number fields is finite. For small (G, D), many $NF(G, D)$ are completely known [JR2]. For small G, the asymptotics of the numbers $|NF(G, D)|$ are known [Bh]. The inverse Galois problem at this refined level is asking for the global structure of the set of all number fields.

For large G, where complete results are out of reach, it is natural to seek fields with the smallest ramification possible in various senses. Here it is convenient to replace discriminants D with root discriminants $|D|^{1/n}$. When one considers all fields, ordered by root discriminant, thus $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(i)$, ..., the first cluster point is expected to be modestly above the Serre-Odlyzko constant $8\pi e^{\gamma} \approx 44.7632$.

Three notions of minimality:
Minimal root discriminant δ;
Minimal Galois root discriminant Δ;
Minimal prime p *for which* $|D|$ *has form* p^k.
The GRD's Δ are hardest to compute and [JR1] assists.

Examples where quantities are known [JR2]:

	A_6	S_6
δ	$2 \cdot 67^{1/3} \approx 8.12$	$14731^{1/6} \approx 4.95$
Δ	$2^{13/6}3^{16/9} \approx 31.66$	$2^{9/4}3^{4/5}5^{2/3} \approx 33.50$
p	1579	197

3. M_{12} **and its extensions.** Invariants associated to the Mathieu groups M_n are [ATLAS]:

n	$\lvert M_n \rvert$	S	A
11	$11{\cdot}10{\cdot}9{\cdot}8 = 2^4{\cdot}3^2{\cdot}5{\cdot}11$	1	1
12	$12{\cdot}11{\cdot}10{\cdot}9{\cdot}8 = 2^6{\cdot}3^3{\cdot}5{\cdot}11$	2	2
22	$22{\cdot}21{\cdot}20{\cdot}48 = 2^7{\cdot}3^2{\cdot}5{\cdot}7{\cdot}11$	12	2
23	$23{\cdot}22{\cdot}21{\cdot}20{\cdot}48 = 2^7{\cdot}3^2{\cdot}5{\cdot}7{\cdot}11{\cdot}23$	1	1
24	$24{\cdot}23{\cdot}22{\cdot}21{\cdot}20{\cdot}48 = 2^{10}{\cdot}3^3{\cdot}5{\cdot}7{\cdot}11{\cdot}23$	1	1

M_{12} and M_{22} contrast:

$M_{22}.2 \subset S_{22}$ but $M_{12}.2 \not\subset S_{12}$. This means that M_{12} dodecic fields have an extra nice feature: they come in twin pairs. It also means that one needs a degree 24 polynomial to define $M_{12}.2$ fields.

$\tilde{M}_{12} \subset S_{24}$ while $\tilde{M}_{22} \not\subset S_{44}$ (because M_{11}, not having a double cover, splits in $\tilde{M}_{12}$, while $M_{21} = SL_3(4)$, having a double cover, doesn't split in $\tilde{M}_{22}$). In fact $\tilde{M}_{22}$ first embeds in S_{352}.

Generators giving M_{12} inside of S_{12} are

$$g_0 = (1,2,3)(4,5,6)(7,8,9)(10,11,12),$$
$$g_1 = (3,4)(5,7)(8,10)(11,12),$$
$$g_\infty = (1,4,6,7,9,10,11,8,5,3,2)(12).$$

Any two suffice since $g_0 g_1 g_\infty = 1$.

Conjugacy classes [ATLAS]:

C	λ_{12}	$\|C\|$	$\|C\|/95040$	
$1A$	1^{12}	1	1/95040	
$2A$	$2^6 1^4$	396	240	
$2B$	$2^4 1^4$	495	192	
$3A$	$3^3 1^3$	1760	54	
$3B$	3^4	2640	36	
$4A$	$4^2 2^2$	2970	32	↕ (Twin classes)
$4B$	$4^2 1^4$	2970	32	
$5A$	$5^2 1^2$	9504	10	
$6A$	6^2	7920	12	
$6B$	6321	15840	6	
$8A$	84	11880	8	↕ (Twin classes)
$8B$	8211	11880	8	
$10A$	(10)2	9504	10	
$11A$	(11)1	8640	11	↕ (Twin classes)
$11B$	(11)1	8640	11	

4. Construction of fields via specialization of three point covers. In general, let Γ be a transitive group of S_n. Let g_0 and g_1 generate Γ and define g_∞ by $g_0 g_1 g_\infty = 1$. Then one has a corresponding cover $F : X \to \mathbb{P}^1$ of connected complex curves, ramified only over $\{0, 1, \infty\}$.

Algebraic computation of F starts from the associated cycle partitions λ_0, λ_1, and λ_∞. The Euler characteristic χ and genus g of X are

$$\chi = |\lambda_0| + |\lambda_1| + |\lambda_\infty| - n = 2 - 2g.$$

Computation is easiest when $g = 0$.

Example. (g_0, g_1, g_∞) from the previous slide gives

$$\begin{aligned} \lambda_0 &= 3333, \\ \lambda_1 &= 22221111, \\ \lambda_\infty &= (11)1. \end{aligned}$$

Thus $\chi = 4 + 8 + 2 - 12 = 2$ and $g = 0$. This is Case D in the next section.

The cover X has two canonical points on it, the points of $F^{-1}(\infty)$ covering ∞ with local degrees 11 and 1 respectively. Coordinatize X by making these points ∞ and 0 respectively, and also requiring that the four points in $F^{-1}(0)$ have sum 1. Then F has the form

$$F(x) = \frac{A(x)^3}{ex} = \frac{(x^4 - x^3 + bx^2 + cx + d)^3}{ex}$$

with 1 being a critical value of multiplicity four.

The resulting algebraic equations have five solutions (b_j, c_j, d_j, e_j). Solutions 1 and 2 are in $\mathbb{Q}(\sqrt{-11})$ and conjugate and Solutions 3, 4, and 5 are likewise algebraically conjugate. The product

$$f_{D2}(t,x) = (A_1(x) - te_1x)(A_2(x) - te_2x) \in \mathbb{Q}[x]$$

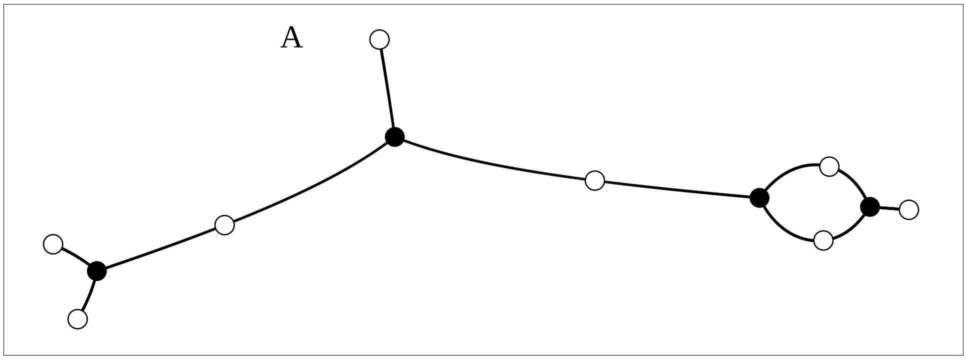
has generic Galois group $M_{12}.2$, as designed. The rest $\prod_{j=3}^{5}(A_j(x) - te_jx) \in \mathbb{Q}[x]$ has generic Galois group $A_{12}^3.2.S_3$. Specialization to $t \in \mathbb{Q}$ then gives number fields with these Galois groups and well-controlled field discriminants D [Ro].

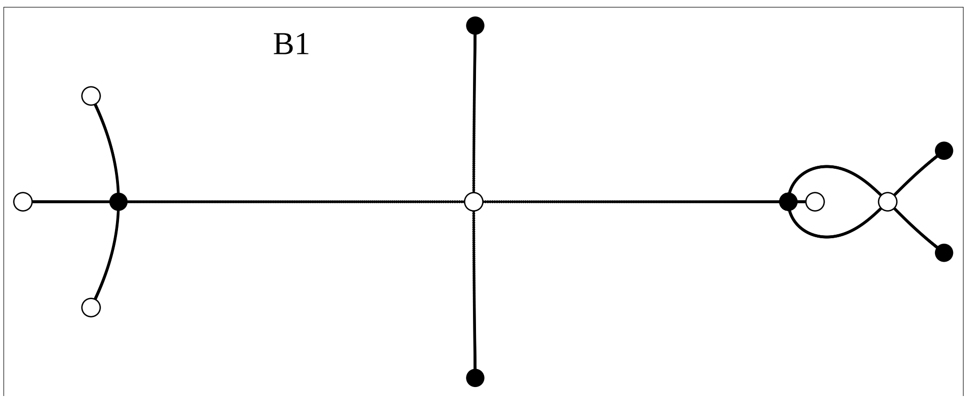
5. Six partition triples. For the group $\Gamma = M_{12}$, six $(\lambda_0, \lambda_1, \lambda_\infty)$ are promising. All give two M_{12} covers, conjugate over a quadratic field. All specialize to many number fields with discriminant of the form $\pm 2^a 3^b p^c$, with ramification typically being wild at each prime. Each has its own interesting features.

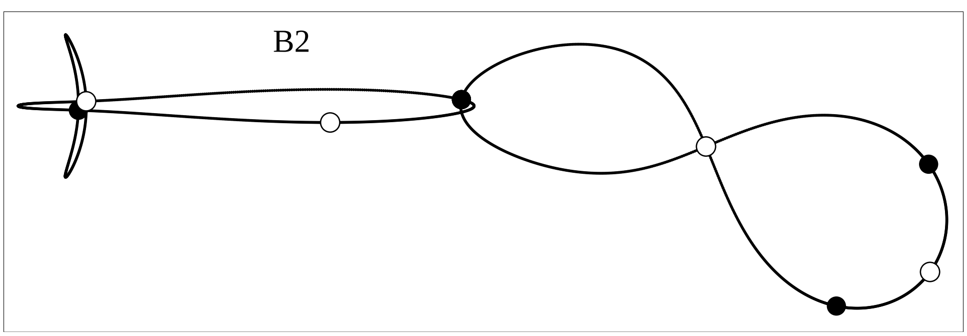
				Source of fields with Galois group G?				Primes and drops			
	λ_0	λ_1	λ_∞	M_{12}	$M_{12}.2$	$\tilde{M}_{12}$	$\tilde{M}_{12}.2$	2	3	5	11
A	3^4	2^4	$(10)2$		$\surd$			W	U	T	
B	4^2	4^2	$(10)2$	$\surd$		$\surd$		U	U	T	
B^t	$4^2 2^2$	$4^2 2^2$	$(10)2$	$\surd$		$\surd$		U	U	T	
C	3^3	2^6	(11)		$\surd$		$\surd$	U	U		T
D	3^4	2^4	(11)		$\surd$		$\surd$	U	U		T
E	3^3	3^3	6^2	$\surd$	$\surd$			W	T		U

A 3-point cover $F : X \to \mathbb{P}^1$ can be understood graphically via its *dessin* $D = F^{-1}([0,1]) \subset X$:

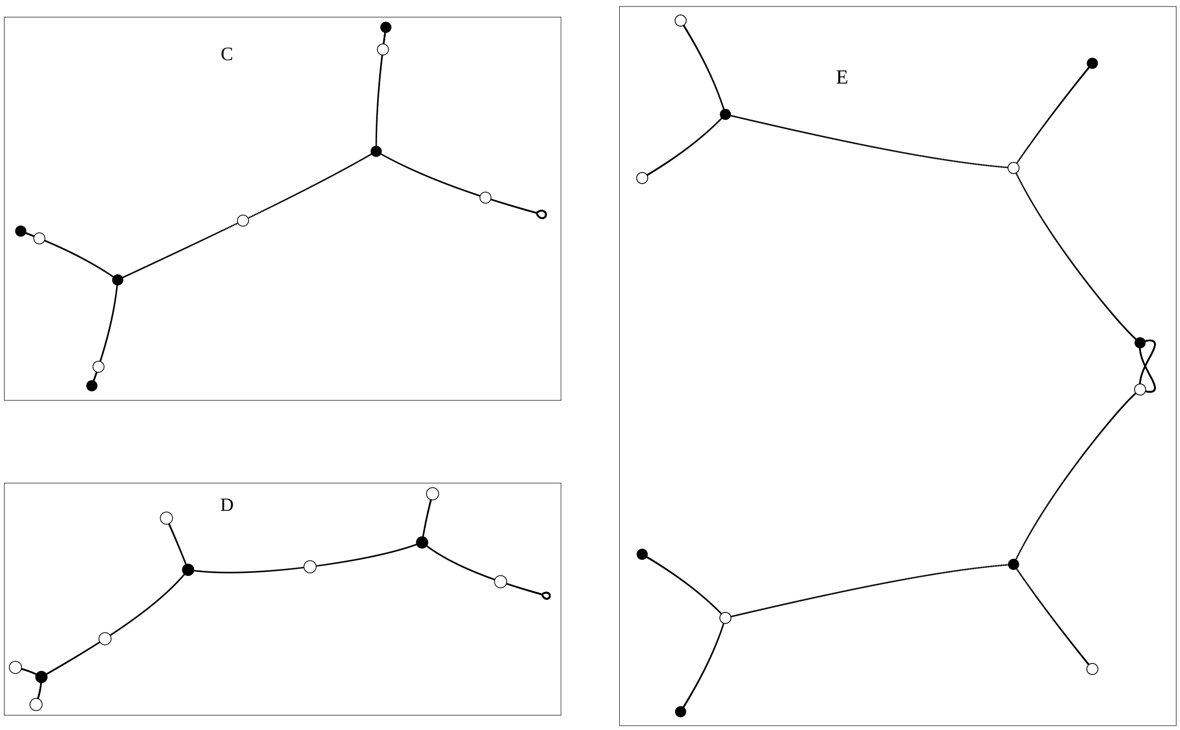
$$\begin{aligned} \text{Black dots} &= F^{-1}(0), \\ \text{White dots} &= F^{-1}(1), \\ \text{Edges} &= F^{-1}((0,1)). \end{aligned}$$







Dessins for Covers A [Mat], B [MZ], and B^t. For Covers A and B, the ambient surface is the plane of the page; for Cover B^t it is a genus two double cover of the plane of the page.



Dessins for Covers C, D, and E [MM]. For C and D, the rightmost black and white vertices, of valence 3 and 2 respectively, are not drawn, so as not to obscure the small loop to the right. For Covers C and D, the ambient surface is the plane of the page; for Cover E it is a genus zero double cover of the plane of the page.

6. Number fields I. The smallest Galois root discriminant found for M_{12} itself was $\Delta = 2^{25/12}3^{10/11}5^{13/10} \approx 93.23$:

$$f_B(5,x) \approx x^{12} - 2x^{11} + 6x^{10} + 15x^8 - 48x^7 + 66x^6 - 468x^5 - 810x^4 + 900x^3 + 486x^2 + 1188x - 1314,$$

$$f_{B^t}(5,x) \approx x^{12} - 2x^{11} + 6x^{10} + 30x^9 - 30x^8 + 60x^7 - 150x^6 + 120x^5 - 285x^4 + 150x^3 - 120x^2 + 90x + 30.$$

The obstruction to lifting for the B family is complicated [Me], [BLV] but vanishes for this specialization, giving the smallest GRD known for $\tilde{M}_{12}$ fields, $\tilde{\Delta} = 5^{1/20}\Delta \approx 100.07$:

$$\tilde{f}_B(5,x) \approx x^{24} - 30x^{20} + 540x^{18} + 945x^{16} - 22500x^{14} - 58860x^{12} + 421200x^{10} + 1350000x^8 - 7970400x^6 + 11638080x^4 - 6480000x^2 + 1166400,$$

$$\tilde{f}_{B^t}(5,x) \approx x^{24} + 40x^{22} + 480x^{20} - 1380x^{18} - 46260x^{16} - 10800x^{14} + 1190340x^{12} - 4429800x^{10} + 65650500x^8 - 324806400x^6 + 588257280x^4 - 398131200x^2 + 58982400.$$

Number Fields II. The smallest Galois root discriminant found for the larger group $M_{12}.2$ was $\Delta = 2^{2/3}3^{25/18}11^{11/12} \approx 65.76$:

$$
\begin{aligned}
&f_{C2}(5^3/2^2, x) \approx \\
&\quad x^{24} - 11x^{23} + 53x^{22} - 154x^{21} + 330x^{20} - 594x^{19} \\
&\quad +1012x^{18} - 2255x^{17} + 6512x^{16} - 17710x^{15} \\
&\quad +42768x^{14} - 89067x^{13} + 154308x^{12} - 237699x^{11} \\
&\quad +351252x^{10} - 483318x^{9} + 623997x^{8} - 753291x^{7} \\
&\quad +733491x^{6} - 520641x^{5} + 278586x^{4} - 104841x^{3} \\
&\quad +15552x^{2} + 2673x + 81.
\end{aligned}
$$

The lifting obstruction vanishes identically in the C family. The lifted field has the smallest GRD known for $\tilde{M}_{12}.2$ fields, $\tilde{\Delta} = 11^{1/24}\Delta \approx 72.67$:

$$
\begin{aligned}
&\tilde{f}_{C2}(5^3/2^2, x) \approx \\
&\quad x^{48} - 22x^{44} + 495x^{40} - 4774x^{36} + 51997x^{32} \\
&\quad -214038x^{28} + 64152x^{26} + 2194852x^{24} \\
&\quad -705672x^{22} - 4044304x^{20} - 30696732x^{18} \\
&\quad +61713630x^{16} + 149602464x^{14} - 9212940x^{12} \\
&\quad +569477304x^{10} + 138870369x^{8} - 484796664x^{6} \\
&\quad +1029399030x^{4} + 39870468x^{2} + 793881.
\end{aligned}
$$

8. Number Fields III. The cover in Case D can be put into the form

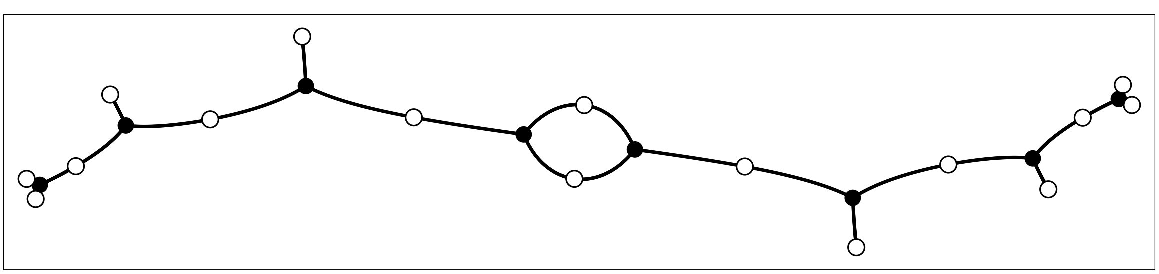
$$f_D(t,x) =$$
$$-11^2u\Big(1188ux^3 + 198ux^2 - 1346ux - 27u$$
$$+594x^4 - 7920x^2 - 1474x + 135\Big)^3$$
$$-2^8 3^{13}(253u - 67)tx$$

with $u = \sqrt{-11}$.

Like in Case C, the lifting obstruction vanishes identically. But here the lifted cover $\tilde{X}$ in $\tilde{X} \stackrel{2}{\to} X \stackrel{12}{\to} \mathbb{P}^1$ has genus zero. Accordingly, equations are simple, in fact just

$$\tilde{f}_D(t,x) = f_D(t,x^2).$$

Geometrically, corresponding to $x \mapsto x^2$, the dessin for D "unwinds" to a dessin for $\tilde{D}$:



Specializing $f_{D2}(t,x) = f_D(t,x)\overline{f}_D(t,x)$ at 394 carefully chosen t gives almost 394 different $M_{12}.2$ fields with discriminant $2^a 3^b 11^c$. One of these specialization points is

$$\begin{aligned} t &= \frac{9090072503}{10101630528} \\ &= \frac{2087^3}{2^6 3^{15} 11} \\ &= 1 - \frac{31805^2}{2^6 3^{15} 11}. \end{aligned}$$

It yields an $M_{12}.2$ field with discriminant 11^{44} (and GRD $11^{219/110} \approx 118.39$).

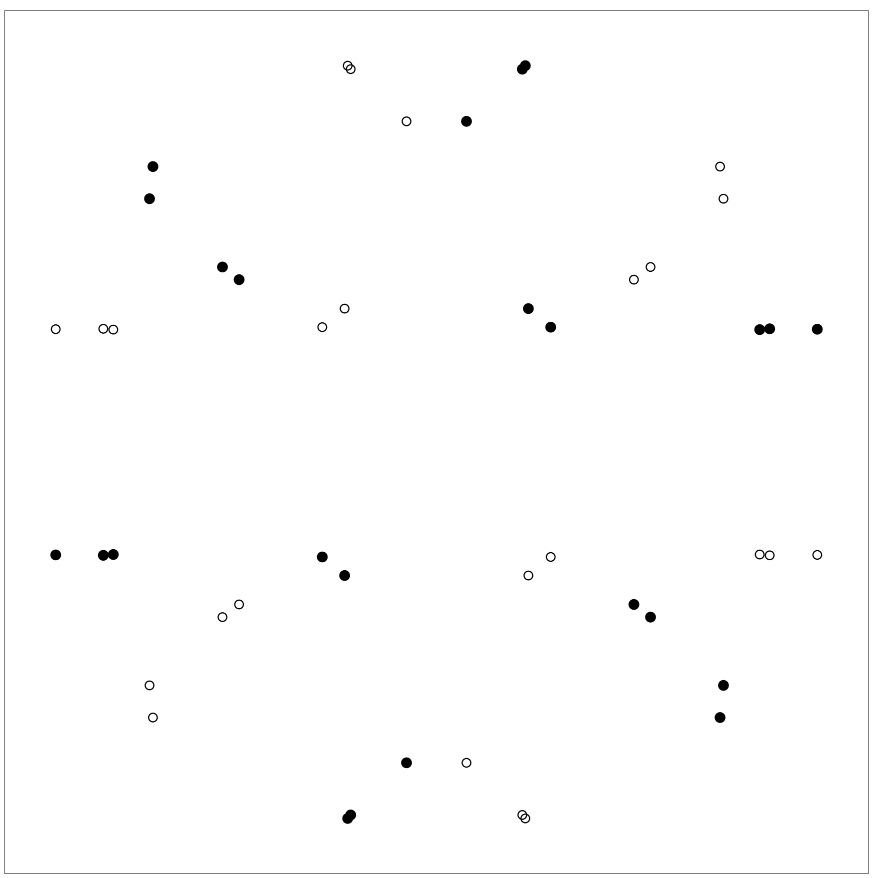
This field makes M_{12} the second sporadic group known to be involved in the Galois group of a field with prime power discriminant. The first is M_{11} for which there is a field of discriminant 661^8 [KM] (and $GRD = 661^{4/5} \approx 180.37$).

Replacing x by x^2 one gets many $\tilde{M}_{12}.2$ fields with discriminant of the form $2^a 3^b 11^c$. For the above particular t the discriminant of the $\tilde{M}_{12}.2$ lift is 11^{88}.

The cover $\tilde{f}_D(t,x)$ also has a fewnomial version which gives a polynomial defining the $\tilde{M}_{12}.2$ field with discriminant 11^{88} having just 15 terms:

$$\tilde{f}_{D2}(9090072503/10101630528, x) \approx$$
$$x^{48} + 2e^3x^{42} + 69e^5x^{36} + 868e^7x^{30} - 4174e^7x^{26}$$
$$+11287e^9x^{24} - 4174e^{10}x^{20} + 5340e^{12}x^{18}$$
$$+131481e^{12}x^{14} + 17599e^{14}x^{12} + 530098e^{14}x^8$$
$$+3910e^{16}x^6 + 4355569e^{14}x^4 + 20870e^{16}x^2 + 729e^{18},$$

with $e = 11$. Its roots are:



Brief References

[ATLAS] Conway et al.; 1985. (Background on groups)

[BLV] Bayer, Llorente, Vila; 1986. (Lifting in Cover B)

[Bh] Bhargava; 2010. (Asymptotics for $|NF(G, D)|$)

[CS] Conway, Sloane; 1999. (Background on M_{12})

[Gr] Granboulan; 1996. (Polynomial for M_{24})

[JR1] Jones, Roberts; online. (Database of local fields)

[JR2] Jones, Roberts; online. (Database of number fields)

[KM] Klüners, Malle; online. (Database of number fields)

[Ma] Malle; 1988. (M_{22} polynomial)

[MM] Malle, Matzat; 1999. (Existence of Cover E)

[Mat] Matzat; 1983. (Polynomial for Cover A)

[MZ] Matzat, Zeh-Marschke; 1986. (Polynomial for Cover B)

[Me] Mestre; 1994. (Lifting in Cover B)

[Ro] Roberts; 2004. (Specialization)