JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

David P. ROBERTS

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

Tome 28, n° 2 (2016), p. 435-460.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_2_435_0>

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 435–460

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

par David P. ROBERTS

Résumé. Par spécialisation de divers revêtements à trois points, on trouve des corps de nombres ayant groupe de Galois M_{12}, $M_{12}.2$, $2.M_{12}$, ou $2.M_{12}.2$ et petite ramification selon divers aspects. Un de ces corps, de groupe de Galois $2.M_{12}.2$, a la propriété remarquable de n'être ramifié qu'en 11.

Abstract. We specialize various three-point covers to find number fields with Galois group M_{12}, $M_{12}.2$, $2.M_{12}$, or $2.M_{12}.2$ and light ramification in various senses. One of our $2.M_{12}.2$ fields has the unusual property that it is ramified only at the single prime 11.

1. Introduction

The Mathieu group $M_{12} \subset S_{12}$ is the second smallest of the twenty-six sporadic finite simple groups, having order $95{,}040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$. The outer automorphism group of M_{12} has order 2, and accordingly one has another interesting group $\mathrm{Aut}(M_{12}) = M_{12}.2 \subset S_{24}$. The Schur multiplier of M_{12} also has order 2, and one has a third interesting group $\tilde{M}_{12} = 2.M_{12} \subset S_{24}$. Combining these last two extensions in the standard way, one gets a fourth interesting group $\tilde{M}_{12}.2 = 2.M_{12}.2 \subset S_{48}$.

In this paper we consider various three-point covers, some of which have appeared in the literature previously [13, 15, 16]. We specialize these three-point covers to get number fields with Galois group one of the four groups $S.M_{12}.A$ just discussed. Some of these number fields are unusually lightly ramified in various senses. Of particular interest is a number field with Galois group $\tilde{M}_{12}.2$, ramified only at the single prime 11. Our general goal, captured by our title, it to get as good a sense as currently possible of the most lightly ramified fields with Galois group $S.M_{12}.A$ as above.

Section 2 provides some general background information. Section 3 introduces the three-point covers that we use. Section 4 describes the specialization procedure. Section 5 focuses on M_{12} and $M_{12}.2$ and presents number fields with small root discriminant, small Galois root discriminant, and

Manuscrit reçu le 2 avril 2014, révisé le 26 août 2014, accepté le 5 septembre 2014.
Mathematics Subject Classification. 11R21, 11R29, 11R32, 11G32.
Mots-clefs. Number field, Discriminant, Ramification, Mathieu group.
We thank the Simons Foundation for partially supporting this work through grant #209472.

small number of ramifying primes. These last three notions are related but inequivalent interpretations of "lightly ramified." Finally, Section 6 presents some explicit lifts to $\tilde{M}_{12}$ and $\tilde{M}_{12}.2$.

2. General background

This section provides background information to provide some context for the rest of this paper. It begins with generalities about number field tabulation and concludes with details about the group M_{12} and its extensions.

2.1. Tabulating number fields. Let $G \subseteq S_n$ be a transitive permutation group of degree n, considered up to conjugation. Consider the set $\mathcal{K}(G)$ of isomorphism classes of degree n number fields K with splitting field K^g having Galois group $\mathrm{Gal}(K^g/\mathbb{Q})$ equal to G. The inverse Galois problem is to prove that all $\mathcal{K}(G)$ are non-empty. The general expectation is that all $\mathcal{K}(G)$ are infinite, except for the special case $\mathcal{K}(\{e\}) = \{\mathbb{Q}\}$.

To study fields K in $\mathcal{K}(G)$, it is natural to focus on their discriminants $d(K) \in \mathbb{Z}$. A fundamental reason to focus on discriminants is that the prime factorization $\prod p^{e_p}$ of $|d(K)|$ measures by e_p how much any given prime p ramifies in K. In a less refined way, the size $|d(K)|$ is a measure of the complexity of K. In this latter context, to keep numbers small and facilitate comparison between one group and another, it is generally better to work with the root discriminant $\delta(K) = |d(K)|^{1/n}$.

To study a given $\mathcal{K}(G)$ computationally, a methodical approach is to explicitly identify the subset $\mathcal{K}(G, C)$ consisting of all fields with root discriminant at most C for as large a cutoff C as possible. Often one restricts attentions to classes of fields which are of particular interest, for example fields with $|d(K)|$ a prime power, or with $|d(K)|$ divisible only by a prescribed set of small primes, or with complex conjugation sitting in a prescribed conjugacy class c of G. All three of these last conditions depend only on G as an abstract group, not on the given permutation representation of G. In this spirit, it is natural to focus on the Galois root discriminant Δ of K, meaning the root discriminant of K^g. One has $\delta \leq \Delta$. To fully compute Δ, one needs to identify the inertia subgroups $I_p \subseteq G$ and their filtration by higher ramification groups.

Online tables associated to [10] and [11] provide a large amount of information on low degree number fields. The tables for [10] focus on completeness results in all the above settings, with almost all currently posted completeness results being in degrees $n \leq 11$. The tables for [11] cover many more groups as they contain at least one field for almost every pair (G, c) in degrees $n \leq 19$. For each (G, c), the field with the smallest known δ is highlighted.

There is an increasing sequence of numbers $C_1(n)$ such that $\mathcal{K}(G, C_1(n))$ is known to be empty by discriminant bounds for all $G \subseteq S_n$. Similarly, if one assumes the generalized Riemann hypothesis, there are larger numbers $C_2(n)$ for which one knows $\mathcal{K}(G, C_2(n))$ is empty. In the limit of large n, these numbers tend to $4\pi e^\gamma \approx 22.3816$ and $8\pi e^\gamma \approx 44.7632$ respectively. This last constant especially is useful as a reference point when considering root discriminants and Galois root discriminants. See e.g. [14] for explicit instances of these numbers $C_1(n)$ and $C_2(n)$.

Via class field theory, identifying $\mathcal{K}(G, C)$ for any solvable G and any cutoff C can be regarded as a computational problem. For G abelian, one has an explicit description of $\mathcal{K}(G)$ in its entirety. For many non-abelian solvable G one can completely identify very large $\mathcal{K}(G, C)$. Identifying $\mathcal{K}(G, C)$ for nonsolvable groups is also in principle a computational problem. However run times are prohibitive in general and only for a very limited class of groups G have non-empty $\mathcal{K}(G, C)$ been identified.

2.2. Pursuing number fields for larger groups. When determining complete non-empty lists for a given group G is currently infeasible, one would nonetheless like to produce as many lightly ramified fields as possible. One can view this as a search for best fields in $\mathcal{K}(G)$ in various senses. Here our focus is on the smallest root discriminant δ, the smallest Galois root discriminant Δ, and the smallest prime p for which there is a field ramified only at p.

For the twenty-six sporadic groups G in their smallest permutation representations, the situation is as follows. The set $\mathcal{K}(G)$ is known to be infinite for all groups except for the Mathieu group M_{23}, where it is not even known to be non-empty [13]. One knows very little about ramification in these fields. Explicit polynomials are known only for M_{11}, M_{12}, M_{22}, and M_{24}. The next smallest degrees come from the Hall-Janko group HJ and Higman-Sims group HS, both in S_{100}. The remaining sporadic groups seem well beyond current reach in terms of explicit polynomials because of their large degrees.

For M_{11}, M_{12}, M_{22}, and M_{24}, one knows infinitely many number fields, by specialization from a small number of parametrized families. In terms of known lightly ramified fields, the situation is different for each of these four groups. The known M_{11} fields come from specializations of M_{12} families satisfying certain strong conditions and so instances with small discriminant are relatively rare. On [11], the current records for smallest root discriminant are given by the polynomials

$$f_{11}(x) = x^{11} + 2x^{10} - 5x^9 + 50x^8 + 70x^7 - 232x^6 + 796x^5 + 1400x^4 - 5075x^3 + 10950x^2 + 2805x - 90,$$

$$f_{12}(x) = x^{12} - 12x^{10} + 8x^9 + 21x^8 - 36x^7 + 192x^6 - 240x^5 - 84x^4 + 68x^3 - 72x^2 + 48x + 5.$$

The respective root discriminants are

$$\begin{array}{rcccl} \delta_{11} & = & (2^{18}3^8 5^{18})^{1/11} & \approx & 96.2, \\ \delta_{12} & = & (2^{24}3^{12}29^4)^{1/12} & \approx & 36.9. \end{array}$$

Galois root discriminants are much harder to compute in general, with the general method being sketched in [9]. The interactive website [8] greatly facilitates GRD computations, as indeed in favorable cases it computes GRDs automatically. In the two current cases the GRDs are respectively

$$\begin{array}{rcccl} \Delta_{11} & = & 2^{13/6}3^{7/8}5^{39/20} & \approx & 270.8, \\ \Delta_{12} & = & 2^{43/16}3^{25/18}29^{1/2} & \approx & 159.4. \end{array}$$

The ratios $96.2/36.8 \approx 2.6$ and $270.8/159.5 \approx 1.7$ are large already, especially considering the fact that M_{12} is twelve times as large as M_{11}. But, moreover, the sequence of known root discriminants increases much more rapidly for M_{11} than it does for M_{12}. There is one known family each for M_{22} [12] and M_{24} [7, 18]. The M_{22} family gives some specializations with root discriminant of order of magnitude similar to those above. The M_{24} family seems to give fields only of considerably larger root discriminant.

In this paper we focus not especially on M_{12} itself, but more so on its extension $M_{12}.2$, for which more good families are available. On the one hand, we go much further than one can at present for any other extension $G.A$ of a sporadic simple group. On the other hand, we expect that there are many M_{12} and $M_{12}.2$ fields of comparably light ramification that are not accessible by our approach.

2.3. M_{12} and related groups. To carry out our exploration, we freely use group-theoretical facts about M_{12} and its extensions. The Atlas [5] as always provides a concise reference for group-theoretic facts. Several sections of [6] provide further useful background information, making the very beautiful nature of M_{12} clear. To get a first sense of M_{12} and its extensions, an understanding of conjugacy classes and their sizes is particularly useful, and so we summarize some of the facts in these references in Table 2.1.

Table 2.1 contains information about conjugacy classes in all four of our groups $S.M_{12}.A$. The columns λ_{12}, λ_{12}^t, λ_{24}, λ_{24}^t contain partitions of 12, 12, 24, and 24 respectively. It is through these partitions that we see conjugacy classes in $S.M_{12}.A$, either via cycle partitions of permutations or degree partitions of factorizations of polynomials into irreducibles in $\mathbb{F}_p[x]$. For M_{12}, the partition λ_{12} corresponds to the given permutation representation while λ_{12}^t corresponds to the twin degree twelve permutation as explained

C	λ_{12}	λ_{12}^t	$\tilde{C}$	λ_{24}	λ_{24}^t	freq	$\lvert\tilde{C}\rvert$	§6.3	§6.4
$1A$	1^{12}	1^{12}	$1A1$	1^{24}	1^{24}	1/190080	1	1	0
			$1A2$	2^{12}	2^{12}	1/190080	1	0	1
$2A$	2^6	2^6	$2A4$	4^6	4^6	1/240	792	768	789
$2B$	$2^4 1^4$	$2^4 1^4$	$2B2'$	2^{12}	2^{12}	1/384	495	470	503
			$2B2''$	$2^8 1^8$	$2^8 1^8$	1/384	495	521	515
$3A$	$3^3 1^3$	$3^3 1^3$	$3A3$	$3^6 1^6$	$3^6 1^6$	1/108	1760	1735	1776
			$3A6$	$6^3 2^3$	$6^3 2^3$	1/108	1760	1823	1781
$3B$	3^4	3^4	$3B3$	3^8	3^8	1/72	2640	2702	2578
			$3B6$	6^4	6^4	1/72	2640	2649	2510
$4A$	$4^2 2^2$	$4^2 1^4$	$4A4$	$4^4 2^4$	$4^4 2^2 1^4$	1/32	5940	6002	11992
$4B$	$4^2 1^4$	$4^2 2^2$	$4B4$	$4^4 2^2 1^4$	$4^4 2^4$	1/32	5940	5993	
$5A$	$5^2 1^2$	$5^2 1^2$	$5A5$	$5^4 1^4$	$5^4 1^4$	1/20	9504	9329	9415
			$5A10$	$10^2 2^2$	$10^2 2^2$	1/20	9504	9405	9613
$6A$	6^2	6^2	$6A12$	12^2	12^2	1/12	15840	15798	15819
$6B$	6321	6321	$6B6'$	$6^2 3^2 2^2 1^2$	$6^2 3^2 2^2 1^2$	1/12	15840	15863	15590
			$6B6''$	$6^3 2^3$	$6^3 2^3$	1/12	15840	15881	15828
$8A$	84	821^2	$8A8$	$8^2 4^2$	$8^2 4\,2\,1^2$	1/8	23760	23613	47707
$8B$	821^2	84	$8B8$	$8^2 4\,2\,1^2$	$8^2 4^2$	1/8	23760	24022	
$10A$	(10)2	(10)2	$10A20$	(20)4	(20)4	1/10	19008	19048	18965
$11AB$	(11)1	(11)1	$11AB11$	$11^2 1^2$	$11^2 1^2$	1/11	17280	17031	17308
			$11AB22$	(22)2	(22)2	1/11	17280	17425	17194
$2C$	2^{12}		$2C2$	2^{24}		1/120	1584		1650
$4C$	$4^4 2^4$		$4C4$	$4^8 2^8$		1/24	7920		7964
$4D$	4^6		$4D8$	8^6		1/12	15840		15688
$6C$	6^4		$6C6$	6^8		1/6	31680		31651
$10BC$	$10^2 2^2$		$10BC10$	$10^4 2^4$		1/5	38016		38245
$12A$	12^2		$12A24$	24^2		1/6	31680		31577
$12BC$	12 6 4 2		$12BC12$	$12^2 6^2 4^2 2^2$		1/3	63360		63493

TABLE 2.1. First eight columns: information on conjugacy classes of $S.M_{12}.A$ and their sizes. Last two columns: distribution of factorization partitions $(\lambda_{12}, \lambda_{12}^t, \lambda_{24}, \lambda_{24}^t)$ of polynomials $(f_B, f_{B^t}, \tilde{f}_B, \tilde{f}_{B^t})$ from §6.3; distribution of factorization partitions $(\lambda_{12}\lambda_{12}^t, \lambda_{24}\lambda_{24}^t)$ of polynomials $(f_{D2}, \tilde{f}_{D2})$ from §6.4

in §2.4 below. Similarly for $\tilde{M}_{12}$, one has λ_{24} corresponding to the given permutation representation and λ_{24}^t corresponding to its twin. For $M_{12}.2$ one has only the partition $\lambda_{12}\lambda_{12}^t$ of 24. For $\tilde{M}_{12}.2$, one likewise has only the partition $\lambda_{24}\lambda_{24}^t$ of 48.

On Table 2.1, classes which are not distinguished by cycle partitions are put on the same line. In more detail, treating each group separately:

M_{12}: The group M_{12} has fifteen conjugacy classes, $1A$, ..., $10A$, $11A$, $11B$ in Atlas notation. All conjugacy classes are rational except for $11A$ and $11B$ which are conjugate over $\mathbb{Q}(\sqrt{-11})$. The table presents these two classes together as $11AB$.

$M_{12}.2$: Three pairs of conjugacy classes in M_{12} each become one class in $M_{12}.2$, the new merged classes being $4AB$, $8AB$, and $11AB$. Also there are nine entirely new classes in $M_{12}.2$, all rational except for the Galois orbits $\{10B, 10C\}$ and $\{12B, 12C\}$.

$\tilde{M}_{12}$: The cover $\tilde{M}_{12}$ has 26 conjugacy classes, with all classes being rational except for the five Galois orbits $\{8A8', 8A8''\}$, $\{8B8', 8B8''\}$, $\{10A20', 10A20''\}$, $\{11A11, 11B11\}$, $\{11A22, 11B22\}$. The 21 Galois orbits correspond to the 21 lines of Table 2.1 above the dividing line.

$\tilde{M}_{12}.2$: Finally, $\tilde{M}_{12}.2$ has 34 conjugacy classes, 20 coming from the 26 conjugacy classes of $\tilde{M}_{12}$ and fourteen new ones. The seven lines below the divider give a quotient set of these new fourteen classes; the lines respectively correspond to 1, 2, 2, 1, 2, 2, and 4 classes.

The frequency column and the $|\tilde{C}|$ column give the same information, as they differ by a factor of $|\tilde{M}_{12}| = 190,080$.

The existence of the biextension $2.M_{12}.2$ is part of the exceptional nature of M_{12}. In fact, the outer automorphism group of M_n has order 2 for $n \in \{12, 22\}$ and has order 1 for the other possibililities, $n \in \{11, 23, 24\}$. Similarly, the Schur multiplier of M_{12} and M_{22} has order 2 and 12 respectively, and order 1 for the other M_n. The next two subsections consist of general facts about extensions of permutation groups, illustrated by contrasting $2.M_{12}.2$ with $2.M_{22}.2$.

2.4. G compared with $G.2$. For a group $G \subseteq S_n$ and a larger group $G.2$, there are two possibilities: either the inclusion can be extended to $G.2$ or it can not. In the latter case, certainly $G.2$ embeds in S_{2n}, although it might also embed in a smaller S_m, as is the case for e.g. $S_6.2 \subset S_{10}$.

The extension $M_{22}.2$ embeds in S_{22} while $M_{12}.2$ only first embeds in S_{24}. The fact that $M_{12}.2$ does not have a smaller permutation representation perhaps is a reason for its relative lack of presence in the explicit literature on the inverse Galois problem.

When $G.2$ does not embed in S_n, there is an associated twinning phenomenon: fields in $\mathcal{K}(G)$ come in twin pairs, with two twins K_1 and K_2 sharing a common splitting field K^g. When the outer automorphism group acts non-trivially on the set of conjugacy classes of G, then twin fields K_1 and K_2 do not necessarily have the same discriminant; this is the case for M_{12}.

2.5. G compared with $\tilde{G}$. For a group $G \subseteq S_n$ and a double cover $\tilde{G}$, finding the smallest N for which $\tilde{G}$ embeds in S_N can require an exhaustive analysis of subgroups. One needs to find a subgroup H of G of smallest possible index N which splits in $\tilde{G}$ in the sense that there is a group $\hat{H}$ in $\tilde{G}$ which maps bijectively to H. The subgroup H also needs to satisfy the condition that its intersection with all its conjugates in G is trivial.

In the case of $G = A_n$ and $\tilde{G} = \tilde{A}_n$, the Schur double cover, the desired N is typically much larger than n. Similarly $\tilde{M}_{22}$ first embeds in S_{352} and $\tilde{M}_{22}.2$ first embeds in S_{660}. The fact that one has the low degree embeddings $\tilde{M}_{12} \subset S_{24}$ and $\tilde{M}_{12}.2 \subset S_{48}$ greatly facilitates the study of $\mathcal{K}(\tilde{M}_{12})$ and $\mathcal{K}(\tilde{M}_{12}.2)$ via explicit polynomials. These embeddings arise from the fact that M_{11} splits in $\tilde{M}_{12}$.

2.6. The nonstandard double extension $(2.M_{12}.2)^*$. There is a second non-split double cover $(2.M_{12}.2)^*$ of $M_{12}.2$. We refer to the group $2.M_{12}.2$ we are working with throughout this paper as the standard double cover, since the Atlas [5] prints its character table. The isoclinic [5, §6.7] variant $(2.M_{12}.2)^*$ is considered briefly in [3], where the embedding $(2.M_{12}.2)^* \subset S_{48}$ is also discussed.

Elements of $2.M_{12}.2$ above elements in the class $2C \subset M_{12}.2$ have cycle type 2^{24}, as stated on Table 2.1. In contrast, elements in $(2.M_{12}.2)^*$ above elements in $2C$ have cycle type 4^{12}. This different behavior plays an important role in §6.1.

3. Three-point covers

In this section we give explicit equations for six three-point covers of the projective line. The covers, labeled by A, B, B^t, C, D, and E, all have degree twelve and monodromy group M_{12}. We "double" four of the covers in very simple ways to obtain covers labeled by $A2$, $C2$, $D2$, and $E2$ of degree twenty-four. All these covers will play a central role in the sequel.

3.1. Six partition triples. Suppose given three conjugacy classes C_0, C_1, C_∞ in a centerless group $M \subseteq S_n$. Suppose each of the C_t is *rational* in the sense that whenever $g \in C_t$ and g^k has the same order as g, then $g^k \in C_t$ too. Suppose that the triple (C_0, C_1, C_∞) is *rigid* in the sense that there exists a unique-up-to-simultaneous-conjugation triple (g_0, g_1, g_∞) with $g_t \in C_t$, $g_0 g_1 g_\infty = e$, and $\langle g_0, g_1, g_\infty \rangle = M$. Then the theory of three-point covers applies in its simplest form: there exists a canonically defined degree n cover X of $\mathbb{P}^1$, ramified only above the three points 0, 1, and ∞, with local monodromy class C_t about $t \in \{0, 1, \infty\}$ and global monodromy M. Moreover, this cover is defined over $\mathbb{Q}$ and the set S at which it has bad reduction satisfies

$$S_{\text{loc}} \subseteq S \subseteq S_{\text{glob}}.$$

Here S_{loc} is the set of primes dividing the order of one of the elements in a C_t, while S_{glob} is the set of primes dividing $|M|$.

An interesting fact about the M_n is that they contain no rational rigid triples (C_0, C_1, C_∞). Accordingly, we will not be using the theory of three-point covers in its very simplest form. Instead, for each of our M_{12} covers there is a complication, always involving the number 2, but in different ways. We will not be formal about how the general theory needs to be modified, as our computations are standard, and all we need is the explicit equations that we display below to proceed with our construction of number fields.

We use the language of partition triples rather than class triples. The only essential difference is that the two conjugacy classes $11A$ and $11B$ give rise to the same partition of twelve, namely (11)1. The six partition triples we use are listed in Table 3.1. As we will see by direct computation, the sets S of bad reduction are always of the form $\{2, 3, q\}$, thus strictly smaller than $S_{\mathrm{glob}} = \{2, 3, 5, 11\}$. The extra prime q is 5 for Covers A, B, and B^t, while it is 11 for Covers C, D, and E.

Name	λ_0	λ_1	λ_∞	M_{12}	$M_{12}.2$	$\tilde{M}_{12}$	$\tilde{M}_{12}.2$	2	3	5	11
A	3333	22221111	(10)2		$\surd$			W	U	T	
B	441111	441111	(10)2	$\surd$		$\surd$		U	U	T	
B^t	4422	4422	(10)2	$\surd$		$\surd$		U	U	T	
C	333111	222222	(11)1		$\surd$		$\surd$	U	U		T
D	3333	22221111	(11)1		$\surd$		$\surd$	U	U		T
E	333111	333111	66	$\surd$	$\surd$			W	T		U

TABLE 3.1. Left: The six dodecic partition triples pursued in this paper. Middle: The Galois groups G they give rise to. Right: The primes of bad reduction and their least ramified behavior (Unramified, Tame, Wild) in specializations, according to Tables 4.2 and 4.3.

3.2. Cover *A*. Cover A was studied by Matzat [15] in one of the first computational successes of the theory of three-point covers. The complication here is that there are two conjugacy classes of (g_0, g_1, g_∞). It turns out that they are conjugate to each other over $\mathbb{Q}(\sqrt{-5})$. Abbreviating $a = \sqrt{-5}$, one finds an equation for this cover to be

$$f_A(t,x) = 5^3\Big(24ax^2 + 16ax - 648a - x^4 - 60x^3 - 870x^2 - 220x + 6399\Big)^3 \\ -2^{12}3^{15}(118a - 475)tx^2.$$

To remove irrationalities, we define

$$f_{A2}(t,x) \;=\; f_A(t,x)\overline{f}_A(t,x),$$

where $\bar{\cdot}$ indicates conjugation on coefficients. Because all cuspidal partitions involved are stable under twinning, the generic Galois group of $f_{A2}(t,x)$ is $M_{12}.2$, not the $M_{12}^2.2$ one might expect from similar situations in which quadratic irrationalities are removed in the same fashion.

3.3. Covers B and B^t. Cover B is the most well-known of the covers in this paper, having been introduced by Matzat and Zeh-Marschke [16] and studied further in the context of lifting by Bayer, Llorente, and Vila [1] and Mestre [17]. The complication from Cover A of there being two classes of (g_0, g_1, g_∞) is present here too. However, in this case, the complication can be addressed without introducing irrationalities. Instead one uses $\lambda_0 = \lambda_1$ and twists accordingly. An equation is then

$$\begin{aligned} f_B(s,x) = {} & 3x^{12} + 100x^{11} + 1350x^{10} + 9300x^9 + 32925x^8 \\ & + 45000x^7 - 43500x^6 - 147000x^5 + 46125x^4 \\ & + 172500x^3 - 16250x^2 + 22500x + 1875 \\ & - s2^{11}5^2x^2. \end{aligned}$$

The twisting is seen in the polynomial discriminant, which is

$$D_B(s) = 2^{144}3^{120}5^{38}(s^2-5)^6.$$

So here and for B^t below, the three critical values of the cover are $-\sqrt{5}$, $\sqrt{5}$, and ∞. The three critical values of Covers A, C, D, and E are all at their standard positions 0, 1, and ∞.

While the outer automorphism of M_{12} fixes the conjugacy class $10A = (10)2$, it switches the classes $4B = 441111$ and $4A = 4422$. Therefore Cover B^t, the twin of Cover B, has ramification triple $(4422, 4422, (10)2)$ and hence genus two. While the other five covers have genus zero and were easy to compute directly, it would be difficult to compute Cover B^t directly. Instead we started from B and applied resolvent constructions, eventually ending at the following polynomial:

$$\begin{aligned} f_{B^t}(s,x) = {} & 5^2\Big(2500x^{12} - 45000x^{10} + 310500x^8 - 1001700x^6 + \\ & \qquad +1433700x^4 - 641520x^2 + 174960x + 88209\Big) \\ & - 270s(12x+25)\Big(50x^6 - 450x^4 + 1080x^2 - 297\Big) \\ & + 3^6s^2(12x-25)^2. \end{aligned}$$

Unlike in our equations for Covers A, B, C, and D, here x is not a coordinate on the covering curve. Instead the covering curve is a desingularization of the plane curve given by $f_{B^t}(s,x) = 0$. The function x has degree two and

there is a degree 5 function y so that the curve can be presented in the more standard form $y^2 = 15x\left(5x^4 + 30x^3 + 51x^2 - 45\right)$.

3.4. Covers *C* and *D*. The next two covers are remarkably similar to each other and we treat them simultaneously. In these cases, the underlying permutation triple is rigid. However it is not rational, since $11A$ and $11B$ are conjugates to one another over $\mathbb{Q}(\sqrt{-11})$. So as for Cover A, there is an irrationality in our final polynomials, although this time one knows before computing that the field of definition is $\mathbb{Q}(\sqrt{-11})$. Abbreviating $u = \sqrt{-11}$, our polynomials are

$$\begin{aligned} f_C(t,x) = &\Big(21ux + 13u - 2x^3 - 54x^2 - 321x - 83\Big)^3 \\ &\cdot \Big(69ux + 1573u - 2x^3 - 102x^2 - 1713x - 10043\Big) \\ &+ 2^9 3^{12}(253u + 67)tx, \\ f_D(t,x) = &-11^2 u\Big(1188ux^3 + 198ux^2 - 1346ux - 27u + 594x^4 \\ &\qquad - 7920x^2 - 1474x + 135\Big)^3 \\ &- 2^8 3^{13}(253u - 67)tx. \end{aligned}$$

As with Cover A, we remove irrationalities by forming the products $f_{C2}(t,x) = f_C(t,x)\overline{f}_C(t,x)$ and $f_{D2}(t,x) = f_D(t,x)\overline{f}_D(t,x)$. As for $f_{A2}(t,x)$, the Galois group of these new polynomials is $M_{12}.2$.

3.5. Cover *E*. One complication for Cover E is the same as for Covers A, B, and B^t: there are two classes of underlying (g_0, g_1, g_∞). As for B and B^t, the classes C_0 and C_1 agree, which can be exploited by twisting to obtain rationality. But now, unlike for B and B^t, this class, namely $3A$, is stable under twinning. So now, replacing the twin pair (X_B, X_{B^t}), there is a single curve X_E with a self-twinning involution. Like X_B, this curve has genus zero and is defined over $\mathbb{Q}$. However, a substantial complication arises only here: the curve X_E does not have a rational point and is hence not parametrizable.

We have computed a corresponding degree twelve polynomial $f_E(s,x)$ and used it to determine a degree twenty-four polynomial

$$\begin{aligned} f_{E2}(t,x) = &\\ &(1-t)\Big(x^6+60x^5+2406x^4+56114x^3+1941921x^2 \\ &\qquad +55625130x+996578748\Big) \\ &\cdot \Big(x^6-20x^5+262x^4-15286x^3+477665x^2-10170814x+96944940\Big)^3 \end{aligned}$$

$$+t\Big(x^{12}+396x^{10}-27192x^9+933174x^8-20101752x^7+169737744x^6$$
$$-16330240872x^5+538400028969x^4-8234002812376x^3$$
$$+195276967064388x^2-3991355037576144x+30911476378259268\Big)^2$$
$$+2^4 3^{12} 11^{22} t(t-1).$$

One recovers $f_E(s,x)$ via $f_{E2}(1+s^2/11,x) = f_E(s,x)f_E(-s,x)$. The discriminants of $f_E(s,x)$ and $f_{E2}(t,x)$ are respectively

$$D_E(s) = 2^{64}3^{48}11^{60}(s^2+11)^6 c_4(s)^2,$$
$$D_{E2}(t) = 2^{224}3^{168}11^{264}t^{12}(t-1)^{12}c_{10}(t)^2.$$

The last factors in each case have the indicated degree and do not contribute to field discriminants. The Galois group of $f_E(s,x)$ over $\mathbb{Q}(s)$ is M_{12} and $f_E(-s,x)$ gives the twin M_{12} extension. The Galois group of $f_{E2}(t,x)$ over $\mathbb{Q}(t)$ is $M_{12}.2$. The .2 corresponds to the double cover of the t-line given by $z^2 = 11(t-1)$.

The equation $f_{E2}(t,x) = 0$ gives the genus zero degree twenty-four cover X_{E2} of the t-line known to exist by [13, Prop. 9.1a]. The curve X_{E2} is just another name for the curve X_E discussed above. It does not have any points over $\mathbb{R}$ or over $\mathbb{Q}_2$. The function x has degree 2, and there is a second function y so that $X_{E2} = X_E$ is given by $y^2 = -x^2 + 40x - 404$.

4. Specialization

This section still focuses on covers, but begins the process of passing from covers to number fields. The next two sections are also focused on specialization, but with the emphasis shifted to the number fields produced.

4.1. Keeping ramification within $\{2,3,q\}$. Let $f(t,x) \in \mathbb{Z}[t,x]$ define a cover ramified only above the points 0, 1, and ∞ on the t-line. Then for each $\tau \in T(\mathbb{Q}) = \mathbb{Q} - \{0,1\}$, one has an associated number algebra K_τ. When $f(\tau,x)$ is separable, which it is for all our covers and all τ, this number algebra is simply $K_\tau = \mathbb{Q}[x]/f(\tau,x)$. Thus "specialization" in our context refers essentially to plugging in the constant τ for the variable t.

Local behavior. To analyze ramification in $\mathbb{Q}[x]/f(\tau,x)$, one works prime-by-prime. The procedure is described methodically in [20, §3,4] and we review it in briefer and more informal language here. For a given prime p, one puts $T(\mathbb{Q})$ in the larger set $T(\mathbb{Q}_p) = \mathbb{Q}_p - \{0,1\}$. One thinks of $T(\mathbb{Q}_p)$ as consisting of a generic "center" and three "arms," one extending to each of the cusps 0, 1, and ∞. A point τ is in arm $k \in \{0,1,\infty\}$ if τ reduces to k modulo p. Otherwise, τ is generic. If τ is in arm k, then one has its extremality index $j \in \mathbb{Z}_{\geq 1}$, defined by $j = \operatorname{ord}_p(\tau)$, $j = \operatorname{ord}_p(\tau-1)$, and $j = -\operatorname{ord}_p(\tau)$ for $k = 0$, 1, and ∞ respectively.

Suppose a prime p is not in the bad reduction set of $f(t,x)$. Then the analysis of p-adic ramification in any K_τ is very simple. First, if τ is generic, then p is unramified in K_τ. Second, suppose τ is in arm k with extremality index j; then the p-inertial subgroup of the Galois group of K_τ is conjugate to $\langle g_k^j \rangle$, where $g_k \in C_k$ is the local monodromy transformation about the cusp k. In particular, suppose g_k has order m_k; then a point τ on the arm k yields a K_τ unramified at p if and only if its extremality index is a multiple of m_k.

Global specialization sets. Let S be the set of bad reduction primes of $f(t,x)$, thus $\{2,3,q\}$ for us with $q=5$ for Covers A, B, and B^t and $q=11$ for Covers C, D, and E. Then the subset of $T(\mathbb{Q})$ consisting of τ giving K_τ ramified entirely within S depends only on S and the monodromy orders m_0, m_1, and m_∞. Following [20] still, we denote it $T_{m_0,m_1,m_\infty}(\mathbb{Z}^S)$. This set can be simply described without reference to p-adic numbers as follows. It consists of all $\tau = -ax^{m_0}/cz^{m_\infty}$ where (a,b,c,x,y,z) are integers satisfying the ABC equation $ax^{m_0} + by^{m_1} + cz^{m_\infty} = 0$ with a, b, and c divisible only by primes in S. After suitable simple normalization conditions are imposed, the integers a, b, c, x, y, and z are all completely determined by τ.

To find elements in some $T_{m_0,m_1,m_\infty}(\mathbb{Z}^S)$, one can carry out a computer search, restricting to $|ax^{m_0}|$ and $|cz^{m_\infty}|$ less than a certain height cutoff, say of the form 10^u. As one increases u, the new τ found rapidly become more sparse. Many of the new τ are not entirely new, as they are often base-changes of lower-height τ as described in [20, §4]. A typical situation, present for us here, is that one can be confident that one has found at least most of $T_{m_0,m_1,m_\infty}(\mathbb{Z}^S)$ by a short implementation of this process.

$A2$:	$\lvert T^5_{3,2,10}\rvert$	$=$	447,	158470321^3	$-$	1994904202391^2	$+$	$2^{10}3^4 5^1 19^{10}$	$=$	0,
B,B^t:	$\lvert T^5_{(4,4),10}\rvert$	$=$	27,	79^4	$-$	6881^2	$+$	$2^8 3^8 5$	$=$	0,
$C2$,$D2$:	$\lvert T^{11}_{3,2,11}\rvert$	$=$	394,	2540833^3	$-$	4050085583^2	$+$	$2^{18}3^1 11^6$	$=$	0,
$E2$:	$\lvert T^{11}_{3,2,12}\rvert$	$=$	395,	796531585^3	$-$	22481204531903^2	$+$	$2^{11}3^5 11^2 17^{12}$	$=$	0.

TABLE 4.1. Sizes and largest height elements of specialization sets

The sizes of our specialization sets $T^q_{m_0,m_1,m_\infty} \subseteq T_{m_0,m_1,m_\infty}(\mathbb{Z}^{\{2,3,q\}})$ are given by the left columns of Table 4.1. The right columns give the ABC triple corresponding to the element τ of largest height in these sets. The set $T^5_{(4,4),10}$ is not in our standard form. We obtain it by considering a set $T^5_{4,2,10}$ of 237 points. We select from this set the τ for which $5(1-\tau)$ is a perfect square. Each of these gives two specialization points $\sigma = \pm\sqrt{5(1-\tau)}$ in $T^5_{(4,4),10}$ and then we consider $\sigma = 0$ as in $T^5_{(4,4),10}$ as well. The displayed ABC triple yields $\sigma = \pm 6881/2^4 3^4$.

gen	τ	1	2	3	4	5	6	7	8	9	10
2	0	(68)			**Cover** $A2$						
	1	62	(50)								
	∞	72	$\{46,52\}$	66	$\{46,48\}$	64	42	60	$\{40,42\}$	52	42
		54	(36	52	40	52	40	48	40	52	40
		52)									
3	0	52	$\{40,48\}$	(36	48	48)					
	1	$\{40,44\}$	36	24	(20)						
	∞	52	48	24	42	38	22	32	34	22	30
		24	22	22	22	(0	20	16	20	16	12
		16	20	16	20)						
5	0	34	26	(20	12	20)					
	1	34	26	(18)							
26, 18	∞	(42	42	42	42	26)					

2	0	$(\{18,20,24\})$			**Cover** B						
	1	(34)									
	∞	$\{16,22\}$	30	$\{16,22\}$	30	$\{12,18\}$	28	$\{12,16\}$	24	$\{12,18\}$	24
		$(\{0,12\}$	22	$\{8,16\}$	22	$\{8,16\}$	18	$\{8,16\}$	22	$\{8,16\}$	22)
3	∞	16	16	10	14	12	10	10	(10	0	10
8, 10		8	10	8	6	8	10	8)			
5	0	14	(8)								
18	∞	(10	$\{6,10\}$	20	18	20	18	$\{8,12\}$	18	20	18)

TABLE 4.2. Specialization tables for Covers $A2$ and B, with entries as discussed in §4.2

4.2. Analyzing 2-, 3-, and q-adic ramification. Let $p \in \{2,3,q\}$. Then the quantity $\mathrm{ord}_p(\mathrm{disc}(K_\tau))$ is a locally constant function on $T(\mathbb{Q}_p)$. It shares some basic structural properities with the much simpler tame case of $\mathrm{ord}_p(\mathrm{disc}(K_\tau))$ for $p \notin \{2,3,q\}$. For example, it is ultimately periodic near each of the cusps. However there are no strong general theorems to apply in this situation, and the current best way to proceed is computationally.

Each entry on Tables 4.2 and 4.3 gives a value of $\mathrm{ord}_p(K_\tau)$ for the indicated cover and for τ in the indicated region. The entries in the far left column correspond to the generic region. The entries in the main part of the table correspond to the regions of the arms.

For example, consider Cover $A2$ for $p = 2$ and focus on the ∞-arm. This case is relatively complicated, as the table has three lines giving entries corresponding to extremalities 1-10 on the first line, 11-20 on the second, and 21 on the third. A sample entry is $\{46,52\}$, corresponding to extremality $j = 2$. This means first of all that $\mathrm{ord}_2(K_\tau)$ can be both 46 and 52 in this region. It means moreover that our computations strongly suggest that no other values of $\mathrm{ord}_2(K_\tau)$ can occur. The parentheses indicate the experimentally-determined periodicity. Thus from the table, $\mathrm{ord}_2(K_\tau) = 36$

gen	τ	1	2	3	4	5	6	7	8	9	10
					Cover $C2$						
2	0	48	$\{12,24\}$	36	24	24	(0	20	20)		
	1	36	(36	48)							
	∞	48	$\{12,24\}$	36	24	24	(0	20	20	20	20
		20	20	20	20	20	20)				
3	0	$\{32,36\}$	(36	$\{20,24\}$	36)						
	1	34	22	(20	16)						
24	∞	42	38	$\{18,22\}$	32	34	22	30	24	(22	22
		22	0	22	22	22	22	22	22	22)	
11	0	36	28	(20	20	16)					
	1	32	(22)								
24	∞	(44	44	44	44	44	44	44	44	44	44
		24)									

					Cover $D2$						
2	0	40	$\{16,24\}$	24	24	24	(0	20	20)		
	1	24	(24	32)							
	∞	40	$\{16,24\}$	24	24	24	(0	20	20	20	20
		20	20	20	20	20	20)				
3	0	52	$\{40,48\}$	(36	48	48)					
	1	$\{40,44\}$	36	24	(20)						
36, 20	∞	52	48	24	42	38	22	32	34	22	30
		24	22	22	22	(0	20	20	20	20	20
		20	20	20	20	20)					
11	0	36	28	(22	22	18)					
	1	32	(20)								
24	∞	(44	44	44	44	44	44	44	44	44	44
		24)									

2	0	66	40	52	$\{24,32\}$	36	32	32	(16	24	24)
	1	66	$(\{44,48\})$		**Cover** $E2$						
	∞	70	(a	74	b	72	b	74	a	74	b
		72	b	74)							
3	0	48	$\{32,40\}$	32	(40	40	32)				
	1	48	$\{32,36\}$	32	(24	28)					
24, 20	∞	56	52	32	48	48	(24, 8	46	44	30	40
		46	28	46	40	30	44	46)			
11	0	36	28	(20	20	16)					
	1	32	24	(16	20)						
36, 24	∞	40	40	36	36	32	32	28	28	24	24
		(0	22	20	18	16	22	12	22	16	18
		20	22)								

TABLE 4.3. Specialization tables for Covers $C2$, $D2$ and $E2$, with entries as discussed in §4.2 using abbreviations $a = \{24, 36, 48\}$ and $b = \{32, 40, 52\}$

is the only possibility for extremality 12, and it is likewise the only possibility for extremalities $12 + 10k$. We have no need of rigorously confirming

the correctness of these tables, as they serve only as a guide for us in our search for lightly ramified number fields. Rigorous confirmations would involve computations which can be highly detailed for some regions. Examples of interesting such computations are in [19].

4.3. Field equivalence. A typical situation is that $f(\tau, x)$ is irreducible but has large coefficients. Starting in the next subsection, we apply *Pari*'s command *polredabs* [22] or some other procedure to obtain a polynomial $\phi(x)$ with smaller coefficients defining the same field. In general we say that two polynomials f and ϕ in $\mathbb{Q}[x]$ are *field equivalent*, and write $f \approx \phi$, if $\mathbb{Q}[x]/f(x)$ and $\mathbb{Q}[x]/\phi(x)$ are isomorphic.

4.4. Specialization points with a Galois group drop. We now shift to explicitly indicating the source cover in the notation, writing $K(L, \tau)$ rather than K_τ, as we will be often be considering various covers at once. Only a few of our algebras $K(L, \tau)$ have Galois group different from M_{12} or $M_{12}.2$. We present these degenerate cases here, before moving on to our main topic of non-degenerate specialization in the next section.

Cover	τ	Fact	G	Basic p-adic invariants 2	3	5	Slope Content 2	3	5	RD	GRD
B, B^t	-5/2	12	$L_2(11)$	6_8^2	$11_{10}1$	$10_{13}2$	$[2]_3^2$	$[\,]_{11}^5$	$[\frac{3}{2}]_2$	41.2	55.4
B	1	11 1	M_{11}	$6_{10}4_8 1\ 1$	$8_7 2_1\ 1\ 1$	$5_9\ 5_9\ 1\ 1$	$[\frac{8}{3}, \frac{8}{3}]_3^2$	$[\,]_8^2$	$[\frac{9}{4}]_4$	96.2	270.8
B^t		12	M_{11}^t	$6_{10}\,4_8\,2$	$8_7\ 4_3$	$10_{19}\,2_1$				103.3	
B	-11/5	12	M_{11}^t	$6_{10}\,4_8\,2$	$11_{10}1$	$10_{19}\,2$	$[\frac{8}{3}, \frac{8}{3}]_3^2$	$[\,]_{11}^5$	$[\frac{9}{4}]_4$	103.3	281.2
B^t		11 1	M_{11}	$6_{10}\,4_8\,1\ 1$	$11_{10}\,1$	$9_5\ 9_5\ 1\ 1$				117.5	

TABLE 4.4. Description of K_τ and K_τ^t for the three τ in $X^5_{(4,4),10}$ for which the Galois group is smaller than M_{12}

For B and B^t, our specialization set $T^5_{(4,4),10}$ has twenty-seven points. Three of them yield a group drop as in Table 4.4. In this table, and also Tables 4.5, 5.1, 5.2, we present an analysis of ramification using the notation of [8] and making use of the associated website repeatedly in the calculations. A p-adic field with degree $n = fe$, residual degree f, ramification index e, and discriminant p^{fc} is presented as e_c^f. Superscripts $f = 1$ are omitted. Likewise subscripts $c = e - 1$, corresponding to tame ramification, are omitted. Slope contents, as in $[2]_3^2$, $[\,]_{11}^5$, and $[3/2]_2$ on the first line, indicate the numerics of decomposition groups D_p and their natural filtration $D_p \supseteq I_p \supseteq P_p \cdots$. Here the superscript is the size $|D_p/I_p|$ of the unramified quotient, the subscript is the size $|I_p/P_p|$ of the tame inertia group, and the k numbers in brackets give the slopes associated to the p^k-element wild inertia group P_p. Thus the first field is tame at 3 with inertia

group of size 11. It is wild at 2 and 5 with inertia groups of sizes 6 and 10. The Galois root discriminant is computed prime-by-prime from the slope contents, following [8, Eq. 7], and works out to $2^{4/3}3^{10/11}5^{13/10} \approx 55.4$, as printed in the table.

Continuing to discuss Table 4.4, the specialization point $\tau = -5/2$ yields the same field in both B and B^t, with group $L_2(11) = PSL_2(\mathbb{F}_{11})$ of order 660. A defining equation is

$$f_B(-5/2, x) \approx x^{12} - 2x^{11} - 9x^{10} + 60x^8 + 42x^7 + 141x^6 + 162x^5 + 150x^4 + 60x^3 + 141x^2 + 18x + 21.$$

The field $K(B, -5/2)$ is very lightly ramified, comparable with the remarkable dodecic $L_2(11)$ field on [11] with RD = GRD = $\sqrt{1831} \approx 42.8$. For the specialization point $\tau = 1$, Cover B yields a polynomial factorizing as $11+1$ while B^t yields an irreducible polynomial. For the point $\tau = -11/5$ the situation is reversed. Again these fields are among the very lightest ramified of known fields with their Galois groups, the first having been highlighted as the M_{11} example of §2.2.

For covers $A2$, $C2$, $D2$, and $E2$, there are all together 1630 specialization points τ. Three of them yield group drops as in Table 4.5.

Cover	τ	Fact	G	Basic p-adic invariants 2	3	11	Slope Content 2	3	11	RD	GRD
$C2$	$-\frac{239^3}{3^{13}}$	24	G_t	$2_3^6 2_3^6$	$11_{10}11_{10}1\,1$	12_{11}^2	$[2]_3^2$	$[\,]_{11}^{10}$	$[\,]_{12}^2$	63.6	87.1
		12	$L_2(11).2$	2_3^6	$11_{10}1$	12_{11}				63.6	
$C2$	$\frac{311^5}{2^7}$	22 2	G_i	11_{10}^2	$6_{11}6_{10}3_5 3_5 2_1 2$	$4_3^2 4_3 4_3 2_1^2 2_1$	$[\,]_{11}^{10}$	$[\frac{5}{2}]_2^2$	$[\,]_4^2$	47.6	85.0
		12	$L_2(11).2$	$11_{10}1$	6_{11}^2	$4_3^2 4_3$				80.7	
$D2$	$\frac{-17^3}{2^7}$	22 2	G_i	11_{10}^2	$6_7 6_6 3_3 3_3 2_1 2$	$10_9 10_9 2_1$	$[\,]_{11}^{10}$	$[\frac{3}{2}]_2^2$	$[\,]_{10}$	40.4	58.6
		12	$L_2(11).2$	$11_{10}1$	6_7^2	$10_9 1\,1$				38.8	

TABLE 4.5. Description of $K(L, \tau)$ for the only three instances where the Galois group is smaller than M_{12} in Cases $A2$, $C2$, $D2$, and $E2$

In all three cases, the Galois group is $PGL_2(11) = L_2(11).2$, in either a transitive or an intransitive degree twenty-four representation. The least ramified case is the last one, for which a degree twelve polynomial is

$$x^{12} - 6x^{10} - 6x^9 - 6x^8 + 126x^7 + 104x^6 - 468x^5 + 258x^4 + 456x^3 - 1062x^2 + 774x - 380.$$

The GRD here is small, but still substantially larger than the smallest known GRD for a $PGL_2(11)$ number field of $3^{10/11}227^{1/2} \approx 40.90$. This field comes from a modular form of weight one and conductor $3 \cdot 227$ in

characteristic 11 [21, App. A]. The examples of this section serve to calibrate expectations for the proximity to minima of the M_{12} and $M_{12}.2$ number fields in the next section.

5. Lightly ramified M_{12} and $M_{12}.2$ number fields

This section reports on ramification of specializations to number fields ramified within $\{2, 3, q\}$, with $q = 5$ for covers $A2$, B, B^t and $q = 11$ for covers $C2$, $D2$, $E2$. Our presentation continues to use the conventions of §4.3 on field equivalence and of §4.4 on p-adic ramification.

According to Tables 4.2 and 4.3 the maximal root discriminants our covers can give for these fields are

$$\delta_{A2}^{\max} = (2^{72}3^{52}5^{42})^{1/24} \approx 1445, \qquad \delta_{C2}^{\max} = (2^{48}3^{42}11^{44})^{1/24} \approx 2219,$$
$$\delta_{B}^{\max} = (2^{34}3^{16}5^{18})^{1/12} \approx \ \ 344, \qquad \delta_{D2}^{\max} = (2^{40}3^{52}11^{44})^{1/24} \approx 2784,$$
$$\delta_{E2}^{\max} = (2^{74}3^{56}11^{40})^{1/24} \approx 5985.$$

The fields highlighted below all have substantially smaller root discriminant. Subsections §5.1, §5.2, and §5.3 focus respectively on fields with small root discriminant, small Galois root discriminant, and at most two ramifying primes.

5.1. Small root discriminant. The smallest root discriminant appearing for our M_{12} specializations is approximately 46.2, as reported on the first line of Table 5.1 below. This is substantially above the smallest known root discriminant $2^2 3^1 29^{1/3} \approx 36.9$ from [11], discussed above in §2.2. For the larger group $M_{12}.2$, the two smallest root discriminants appearing in our list are $(2^{12}3^{24}11^{22})^{1/24} \approx 38.2$ and $(2^{20}3^{24}11^{20})^{1/24} \approx 39.4$. The smallest root discriminant comes from Cover $C2$ at $\tau = 5^3/2^2$ and the field can be given by the polynomial

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

The second smallest root discriminant also comes from Cover $C2$. It arises from two specialization points defining the same field, the points being $-17^3/2^7$ and $7^3/2^9$. There are seven more $M_{12}.2$ fields with root discriminant under 50, each arising exactly once. In order, they come from the covers $D2$, $A2$, $D2$, $C2$, $A2$, $A2$, and $D2$.

Cover	τ	Basic p-adic invariants 2	3	q	Slope Content 2	3	q	RD	GRD
B	5	$8_{16}3_21$	11_{10}	$10_{13}2_1$	$[\frac{4}{3},\frac{4}{3},3]_3^2$	$[\,]_{11}^5$	$[\frac{3}{2}]_2$	46.2	93.2
B^t		$8_{16}4_4$	11_{10}	$10_{13}2_1$				51.6	
B	0	12_{34}	9_92_11	$3_2^23_2^2$	$[\frac{23}{6},\frac{23}{6},3,\frac{8}{3},\frac{8}{3}]_3^2$	$[\frac{9}{8},\frac{9}{8}]_8^2$	$[\,]_3^2$	52.1	112.0
B^t		12_{34}	12_{12}	$3_2^23_2^2$				62.5	
B	5/2	12_{12}	9_92_11	$10_{13}2_1$	$[\frac{8}{3},\frac{8}{3},\frac{4}{3},\frac{4}{3}]_3^2$	$[\frac{9}{8},\frac{9}{8}]_8^2$	$[\frac{3}{2}]_2$	58.2	132.4
B^t		12_{12}	12_{12}	$10_{13}2_1$				69.9	
B	-5	4_8^3	9_92_11	$10_{13}2_1$	$[3,\frac{5}{2},2,2]^6$	$[\frac{9}{8},\frac{9}{8}]_8^2$	$[\frac{3}{2}]_2$	65.3	153.0
B^t		4_8^3	12_{12}	$10_{13}2_1$				78.5	
B	-3	$8_{16}4_4$	$8_72_11\,1$	$5_9^21^2$	$[3,\frac{4}{3},\frac{4}{3}]_3^2$	$[\,]_8^2$	$[\frac{9}{4}]_4^2$	73.8	255.6
B^t		$8_{16}3_21$	8_74_3	$10_{19}2_1$				103.3	
E	$-319/54$	$2_2^32_2^3$	$3_3^33_3$	$11_{16}1$	$[2]^3$	$[\frac{3}{2}]^3$	$[\frac{8}{5}]_5$	146.8	280.6
E	319/54	$2_2^32_2^3$	$3_3^33_3$	$11_{16}1$				146.8	
B	$-5/3$	$6_{10}4_82_2$	$9_{16}1^21$	$10_{13}2_1$	$[\frac{8}{3},\frac{8}{3},2]_3^2$	$[2,2]^2$	$[\frac{3}{2}]_2$	89.8	287.9
B^t		$6_{10}4_82_2$	$9_{16}1^21$	$10_{13}2_1$				89.8	

TABLE 5.1. The fourteen M_{12} fields from our list with Galois root discriminant ≤ 300, grouped in twin pairs. The two τ's for E both come from $\sigma = 23^3/2^23^6$.

5.2. Small Galois root discriminant. For M_{12}, the smallest known Galois root discriminant appears in [11] and also on the first line of Table 5.1. The fact that E appears only once in Table 5.1 is just a reflection of the simple fact that $q = 5$ contributes for B and B^t while the larger prime $q = 11$ contributes for E.

For $M_{12}.2$, Galois root discriminants can be substantially smaller than the minimum known for M_{12}, as illustrated by Table 5.2. In this case, in contrast to M_{12}, the field giving the smallest known root discriminant also gives the smallest known Galois root discriminant.

5.3. At most two ramifying primes. Let $d_L(\tau)$ be the field discriminant of $K(L,\tau)$. Then, generically for our specializations, $d_L(\tau)$ has the form $\pm 2^a3^bq^c$ with all three exponents positive. The few cases where at least one of the exponents is zero are as follows. For Cover $A2$, from Table 4.2 the prime 3 drops out from the discriminant exactly if $\mathrm{ord}_3(\tau) \in \{-15,-25,-35,\ldots\}$. This drop occurs in 2 of our 447 specializations:

$$d_{A2}(71^3/2^33^{15}5^2) \;=\; 2^{66}5^{42},$$
$$d_{A2}(3289^3/2^73^{15}5) \;=\; 2^{60}5^{42}.$$

For Covers $C2$ and $D2$, from Table 4.3 the prime 2 drops out exactly if $\mathrm{ord}_2(\tau) \in \{6,9,12,\ldots\} \cup \{6,17,28,\ldots\}$. This much less demanding condition is met by 24 of our 394 specialization points, as listed in Table 5.3.

Cover	τ	Basic p-adic invariants 2	3	q	Slope Content 2	3	q	RD	GRD
$C2$	$5^3/2^2$	$3_2^6 1^6$	$9_{12}3_3^2 3_3^2 1\,1\,1$	12_{11}^2	$[\,]_3^6$	$[\frac{3}{2},\frac{3}{2}]_2^2$	$[\,]_{12}^2$	38.2	65.8
$C2$	$11^3/2^3$	4_6^6	$10_0 10_9 2_1 2_1$	$12_{11}6_5 4_3 2_1$	$[2,2]^4$	$[\,]_{10}^4$	$[\,]_{12}^2$	52.1	68.5
$C2$	$-11^2/2^6 3^3$		$12_{12}9_9 2_1 1$	$22_{27}2_1$		$[\frac{9}{8},\frac{9}{8}]_8^2$	$[\frac{13}{10}]_{10}$	63.3	69.1
$A2$	$-2^3 5^4 11^3/3^8$	$8_{18}4_8^4$	$12_{18}9_{15}2_1 1$	$4_2 4_2 4_2 4_2 4_2 4_2$	$[3,2,2]^4$	$[\frac{15}{8},\frac{15}{8}]_8^2$	$[\,]_2^2$	44.9	73.9
$C2$	$\begin{cases} -17^3/2^7 \\ 7^3/2^9 \end{cases}$	$11_{10}^2 1^2$	$9_{12}3_3^2 3_3^2 1\,1\,1$	$11_{10}11_{10}2_1 2_1$	$[\,]_{11}^2$	$[\frac{3}{2},\frac{3}{2}]_2^2$	$[\,]_{10}$	39.4	74.7
$A2$	$-5^4/2^3 3^3$	$8_{22}^2 8_{22}$	$9_{12}9_9 3_3 3$	$4_2 4_2 4_2 4_2 4_2 4_2$	$[\frac{7}{2},3,2,2]^2$	$[\frac{3}{2},\frac{3}{2}]_2^3$	$[\,]_2^2$	45.1	75.4
$C2$	$5^3/3^3$	$2_3^6 2_3^6$	$12_{12}9_9 2_1 1$	$10_9 10_9 2_1 2_1$	$[3]^6$	$[\frac{9}{8},\frac{9}{8}]_8^2$	$[\,]_2$	57.1	81.7
$C2$	$-2^9 5^3/3^2$		$9_{18}6_{10}6_{10}1^2$	12_{11}^2		$[\frac{9}{4},\frac{9}{4}]_4^2$	$[\,]_{12}^2$	51.3	88.8
$D2$	$5^3/2^2$	$3_2^4 3_2^4$	$9_{15}6_9 3_4 3_3 2_1 1$	$12_{11}6_5 4_3 2_1$	$[\,]_3^4$	$[2,\frac{3}{2}]_2^2$	$[\,]_{12}^2$	50.7	94.8
$D2$	$-11^2/2^6 3^3$		$12_{12}9_{12}1^2 1$	$22_{27}2_1$		$[\frac{3}{2},\frac{3}{2}]_2^4$	$[\frac{13}{10}]_{10}$	49.2	95.2

TABLE 5.2. The ten $M_{12}.2$ fields from our list with Galois root discriminant ≤ 100.

τ	$d_{C2}(\tau)$	$d_{D2}(\tau)$
$-2^9 5^3/3^2$	$3^{38}11^{22}$	$3^{48}11^{20}$
$-11^2/2^6 3^3$	$3^{22}11^{28}$	$3^{24}11^{28}$
$-2^9/3^3$	$3^{22}11^{32}$	$3^{24}11^{32}$
$-11\cdot 131^3/2^6 3^3$	$3^{18}11^{36}$	$3^{24}11^{36}$
$-3^3 11/2^6$	$3^{20}11^{36}$	$3^{36}11^{36}$
$-11/2^6$	$3^{34}11^{36}$	$3^{44}11^{36}$
$2^6 11/3^6$	$3^{22}11^{36}$	$3^{22}11^{36}$
$11\cdot 59^3/2^{17}3^2$	$3^{38}11^{36}$	$3^{48}11^{36}$
$-67^3/2^6 11$	$3^{34}11^{44}$	$3^{40}11^{44}$
$-2^{12}/11$	$3^{34}11^{44}$	$3^{40}11^{44}$
$-2^6 3^3/11^2$	$3^{20}11^{44}$	$3^{36}11^{44}$
$-2^6/11$	$3^{34}11^{44}$	$3^{40}11^{44}$

τ	$d_{C2}(\tau)$	$d_{D2}(\tau)$
$-2^6 31^3/3^3 11^5$	$3^{22}11^{44}$	$3^{20}11^{44}$
$-2^6/3^3 11$	$3^{18}11^{44}$	$3^{24}11^{44}$
$173^3/2^6 11^7$	$3^{34}11^{44}$	$3^{40}11^{44}$
$2^9/3\cdot 11^3$	$3^{42}11^{44}$	$3^{52}11^{44}$
$13^3/2^6 11^2$	$3^{34}11^{44}$	$3^{44}11^{44}$
$7^3/2^6 11$	$3^{24}11^{44}$	$3^{20}11^{44}$
$2087^3/2^6 3^{15}11$	$3^{20}11^{44}$	11^{44}
$3^6/2^6 11$	$3^{24}11^{44}$	$3^{28}11^{44}$
$553^3/2^6 3^9 11^2$	$3^{22}11^{44}$	$3^{22}11^{44}$
$313^3/2^6 3^6 11$	$3^{22}11^{44}$	$3^{22}11^{44}$
$89^3/2^6 11^2$	$3^{24}11^{44}$	$3^{32}11^{44}$
$7033^3/2^6 3^6 11^4$	$3^{22}11^{44}$	$3^{22}11^{44}$

TABLE 5.3. The 24 specialization points of $T_{3,2,11}^{11}$ at which 2 drops out from discriminants of specializations in the $C2$ and $D2$ families

Also for Covers $C2$ and $D2$ it is possible for the prime 3 to drop out. From Table 4.3 this occurs if $\mathrm{ord}_3(\tau)$ is in $\{-12,-23,-34,\ldots\}$ for $C2$ or in $\{-15,-26,-37,\ldots\}$ for $D2$. This stringent condition is met once in each case. For $C2$, this one 3-drop gives $d_{C2}(-55177^3/2^3 3^{23}11^2) = 2^{36}11^{44}$. For $D2$, the one 3-drop occurs is where there is also a 2-drop, giving the $M_{12}.2$ field contained in the $\tilde{M}_{12}.2$ field highlighted in our abstract and introduction. An equation for this $\tilde{M}_{12}.2$ field is given at the end of §6.4.

6. Lifts to the double covers $\tilde{M}_{12}$ and $\tilde{M}_{12}.2$

In this final section, we discuss lifts to $\tilde{M}_{12}$ and $\tilde{M}_{12}.2$. Interestingly, our six cases behave quite differently from each other.

6.1. Lack of lifts to $(2.M_{12}.2)^*$. The .2 for the geometrically disconnected degree twenty-four covers $A2$, $C2$, and $D2$ corresponds to the constant imaginary quadratic fields $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-11})$, and $\mathbb{Q}(\sqrt{-11})$ respectively. Accordingly all specializations have complex conjugation in the class $2C$ on Table 2.1. Elements of $2C$ lift to elements of order 4 in the nonstandard $(2.M_{12}.2)^*$ as reviewed in §2.6. Thus $M_{12}.2$ fields of the form $K(L2,\tau)$ with $L \in \{A, C, D\}$ do not embed in $(2.M_{12}.2)^*$ fields.

The B families do not even give $M_{12}.2$ fields. Also $M_{12}.2$ fields of the form $K(E2,\tau)$ do not embed in $(2.M_{12}.2)^*$ fields, as explained at the end of §6.3 below. For these reasons, we have deemphasized $(2.M_{12}.2)^*$ in this paper, despite the fact that it fits into the framework of our title. An open problem which we do not pursue here is to explicitly write down a degree forty-eight polynomial with Galois group $(2.M_{12}.2)^*$.

6.2. Geometric lifts to $\tilde{M}_{12}$. In this subsection, we work over $\mathbb{C}$ so that symbols such as X_L should be understood as complex algebraic curves. Table 6.1 reprints the six partition triples belonging to M_{12} of Table 3.1. In each case on the next line it then gives a lift to a partition triple in $\tilde{M}_{12}$. Each of these new partition triples is represented by a permutation triple $(\tilde{g}_0, \tilde{g}_1, \tilde{g}_\infty)$ generating $\tilde{M}_{12}$ and satisfying $\tilde{g}_0\tilde{g}_1\tilde{g}_\infty = 1$. Accordingly, one gets a double cover $\tilde{X}_L$ of X_L. The degree 24 map $\tilde{X}_L \to \mathbb{P}^1$ by design has monodromy group $\tilde{M}_{12}$.

The class of $-\tilde{g}_k$ is indicated on Table 6.1 right below the class of $\tilde{g}_k$. Note that $\pm\tilde{g}_0$, $\pm\tilde{g}_1$, and $\pm\tilde{g}_\infty$ multiply either to 1 or -1 in $\tilde{M}_{12}$, according to whether the number of minus signs is even or odd. Thus our choice of $(\tilde{g}_0, \tilde{g}_1, \tilde{g}_\infty)$ could equally well be replaced by $(\tilde{g}_0, -\tilde{g}_1, -\tilde{g}_\infty)$, $(-\tilde{g}_0, \tilde{g}_1, -\tilde{g}_\infty)$, or $(-\tilde{g}_0, -\tilde{g}_1, \tilde{g}_\infty)$. The choice we make always minimizes the genus of $\tilde{X}_L$.

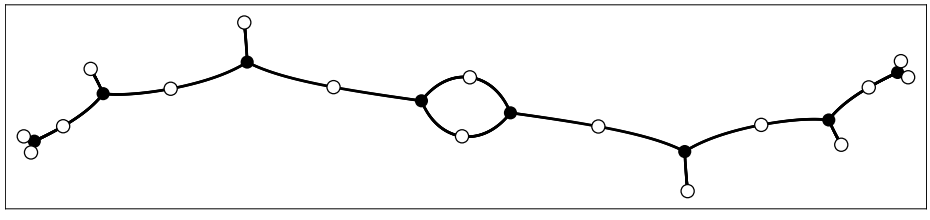

FIGURE 6.1. The dessin of $\tilde{f}_D(t, y)$ in the complex y-line

To understand Table 6.1 in diagrammatic terms, consider Cover D as an example. The curve X_D is just the complex x-line $\mathbb{P}^1_x$. Its cover $\tilde{X}_D$ is just

Cover	0	1	∞	g
A	3^4	$2^4 1^4$	(10)2	0
$\tilde{A}$	3^8	$2^8 1^8$	(20)4	0
	6^4	2^{12}	(20)4	

Cover	0	1	∞	g
C	$3^3 1^3$	2^6	(11)1	0
$\tilde{C}$	$3^6 1^6$	4^6	$11^2 1^2$	2
	$6^3 2^3$	4^6	(22)2	

Cover	0	1	∞	g
B	$4^2 1^4$	$4^2 1^4$	(10)2	0
$\tilde{B}$	$4^4 2^2 1^4$	$4^4 2^2 1^4$	(20)4	2
	$4^4 2^2 1^4$	$4^4 2^2 1^4$	(20)4	

Cover	0	1	∞	g
D	3^4	$2^4 1^4$	(11)1	0
$\tilde{D}$	3^8	$2^8 1^8$	(22)2	0
	6^4	2^{12}	$11^2 1^2$	

Cover	0	1	∞	g
B^t	$4^2 2^2$	$4^2 2^2$	(10)2	2
$\tilde{B}^t$	$4^4 2^4$	$4^4 2^4$	(20)4	4
	$4^4 2^4$	$4^4 2^4$	(20)4	

Cover	0	1	∞	g
E	$3^3 1^3$	$3^3 1^3$	66	0
$\tilde{E}$	$3^6 1^6$	$3^6 1^6$	12^2	0
	$6^3 2^3$	$6^3 2^3$	12^2	

TABLE 6.1. Lifts of partition triples in M_{12} to partition triples in $\tilde{M}_{12}$.

the complex y-line $\mathbb{P}^1_y$, with relation given by $y^2 = x$. The dessin of $\tilde{X}_D$, meaning the preimage of $[0,1] = \bullet\!\!-\!\!\circ \subset \mathbb{P}^1_t$ in $\tilde{X}_D$, is drawn in Figure 6.1. The action of $\tilde{g}_0$ and $\tilde{g}_1$ on edges, being minimal rotations about black and white endpoints respectively, can be algebraically confirmed to truly generate $\tilde{M}_{12}$, as asserted. The map $y \mapsto -y$ stabilizes the dessin and commutes with $\tilde{g}_0$ and $\tilde{g}_1$.

At a geometric level, the six cases $\tilde{X}_L \stackrel{2}{\to} X_L \stackrel{12}{\to} \mathbb{P}^1$ behave similarly. However, at an arithmetic level, the curves X_L are defined over $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}$, $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-11})$, and $\mathbb{Q}$, for $L = A$, B, B^t, C, D, and E, respectively. At issue is whether the cover $\tilde{X}_L$ can likewise be defined over this number field.

6.3. Lifts to $\tilde{M}_{12}$. *A lifting criterion.* A v-adic field K_v has a local root number $\epsilon(K_v) \in \{1, i, -1, -i\}$. For example, taking $v = \infty$, one has $\epsilon(\mathbb{C}) = -i$; also if $K_p/\mathbb{Q}_p$ is unramified then $\epsilon(K_p) = 1$. The invariant ϵ extends to algebras by multiplicativity: $\epsilon(K'_v \times K''_v) = \epsilon(K'_v)\epsilon(K''_v)$. For an algebra K_v, there is a close relation between the local root number $\epsilon(K_v)$ and the Hasse-Witt invariants $HW(K_v) \in \{-1, 1\}$. In fact if the discriminant of K_v is trivial as an element of $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$ then $\epsilon(K_v) = HW(K_v)$. In this case of trivial discriminant class, one has $\epsilon(K_v) = 1$ if and only if the homomorphism $h_v : \mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v) \to A_n$ corresponding to K_v can be lifted into a homomorphism into the Schur double cover, $\tilde{h}_v : \mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v) \to \tilde{A}_n$. If K is now a degree n number field then one has local root numbers $\epsilon(K_v)$ multiplying to 1. In the case when the discriminant class is trivial, then

all $\epsilon(K_v)$ are 1 if and only if the homomorphism $h : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to A_n$ corresponding to K can be lifted into a homomorphism $\tilde{h} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \tilde{A}_n$. The general theory of local root numbers is presented in more detail in [8, §3.3] and local root numbers are calculated automatically on the associated database.

Since the map $\tilde{M}_{12} \to M_{12}$ is induced from $\tilde{A}_{12} \to A_{12}$, one gets that an M_{12} number field embeds in an $\tilde{M}_{12}$ number field if and only if all $\epsilon(K_v)$ are trivial. Also it follows from the above theory that if K and K^t are twin M_{12} fields then $\epsilon(K_v) = \epsilon(K_v^t)$ for all v.

Covers B and B^t. From the very last part of [17], summarizing the approach of [1], we have the general formula

$$\epsilon(K(B,\tau)_v) = (25 - 5\tau^2, \tau)_v, \tag{6.1}$$

where the right side is a local Hilbert symbol. For example, one gets that $K(B,\tau)$ is obstructed at $v = \infty$ if and only if $\tau < -\sqrt{5}$. Similar explicit computations identify exactly the locus of obstruction for all primes p. This locus is empty if and only if $p \equiv 3, 7$ (20).

In particular, because one has obstructions even in specializations, $\tilde{X}_B$ cannot be defined over $\mathbb{Q}$. One can see this more naively as follows. By Table 6.1, one has eight points on X_B corresponding to the $1^4 1^4$. The cover $\tilde{X}_B$ is ramified at exactly four of these points, those which correspond to the $2^2 2^2$. But the eight points in X_B are the roots of

$$x^8 + 36x^7 + 462x^6 + 2228x^5 - 585x^4 - 30948x^3 - 22388x^2 + 215964x - 82539$$

and this polynomial is irreducible in $\mathbb{Z}[x]$.

If $\tau \in \mathbb{Q}$ is a square then of course all the local Hilbert symbols in (6.1) vanish. This motivates consideration of the following base-change diagram of smooth projective complex algebraic curves:

$$\begin{array}{ccc} \tilde{Z}_B & \to & \tilde{X}_B \\ \downarrow & & \downarrow \\ Z_B & \to & X_B \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \to & \mathbb{P}^1 \end{array} \qquad \begin{array}{lcc} & & \\ 7 & & 2 \\ & & \\ 0 & & 0 \\ & & \\ 0 & & 0 \end{array} \quad \text{(with genera)}.$$

Here the bottom map is the double cover $t \mapsto t^2$ and Z_B and $\tilde{Z}_B$ are the induced double covers of X_B and $\tilde{X}_B$ respectively. Thus the cover $Z_B \to \mathbb{P}^1$ is a five-point cover, with ramification invariants $2^4 1^4$ above the fourth roots of 5 and $5^2 1^2$ above ∞. While $\tilde{X}_B$ is not realizable over $\mathbb{Q}$, Mestre proved that $\tilde{Z}_B$ is realizable [17].

Rather than seek equations for a degree 24 polynomial giving the cover $\tilde{Z}_B$, we content ourselves with a single example in the context of number fields. Conveniently the first twin pair on Table 5.1 is unobstructed.

Corresponding equations are

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

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

Replacing x by y^2 in either of the last two displays gives a polynomial with Galois group $2^{12}.M_{12}$; that this generic behavior indeed occurs is quickly confirmed by *Magma*'s `GaloisGroup` [2].

To find the desired degree 24 polynomials, we need to carefully choose a different defining polynomial $f(x)$ for the original degree twelve field, and only then replace x by y^2. It is guaranteed that a correct $f(x)$ is among the characteristic polynomials of $\{2,3,11\}$-units, and more details of the general procedure for finding $f(x)$ are in [4, §5.2]. By eliminating all other possibilities, this procedure proves that the following polynomials and their quadratic twists are correct.

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

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

Magma's `GaloisGroup` double checks that the Galois group of the displayed polynomials is indeed the desired $\tilde{M}_{12} = 2.M_{12}$.

The p-adic factorization partitions of the displayed degree 24 polynomials for the first $|\tilde{M}_{12}| = 190080$ primes different from 2, 3, and 5 are summarized in Table 2.1. As expected from the Chebotarev density theorem, the distribution is quite similar to the distribution of elements of $\tilde{M}_{12}$ into classes. The one class not represented is the central non-identity class $1A2$. Calculating now with five times as many primes, exact equidistribution would give five classes each for $1A1$ and $1A2$. In fact, in this range there are eight primes splitting at the M_{12} level, *76493*, *2956199*, *5095927*, 7900033, *7927511*, *10653197*, 11258593, and *12420649*. Those in ordinary type correspond to $1A2$ while those in italics to $1A1$.

Cover E. For all $\tau \in \mathbb{Q}$, the algebra $K(E,\tau)$ is obstructed at ∞, since $K(E,\tau)_\infty \cong \mathbb{C}^6$ and $\epsilon(\mathbb{C}^6) = \epsilon(\mathbb{C})^6 = (-i)^6 = -1$. This obstruction can be

seen more directly from Table 2.1: a field in $K(E,\tau)$ has complex conjugation in class $2A$ of M_{12} of cycle type 2^6. The only class above $2A$ in $\tilde{M}_{12}$ is $2A4$ of cycle type 4^6, and so the complex conjugation element cannot lift.

6.4. Lifts to $\tilde{M}_{12}.2$. Lifting for the remaining cases behaves as follows.

Cover A. The polynomial $f_A(t,x)$ from §3.2 gives an equation for X_A. From Table 6.1, we see that $\tilde{f}_A(t,x) = f_A(t,y^2)$ gives an equation for $\tilde{X}_A$ with coefficients in $\mathbb{Q}(\sqrt{-5})$. The Galois group of $f_A(t,y^2)$ over $\mathbb{Q}(\sqrt{-5})(t)$ is $\tilde{M}_{12}$ by construction. However the Galois group of the rationalized polynomial $f_{A2}(t,y^2)$ over $\mathbb{Q}(t)$ is not $\tilde{M}_{12}.2 = 2.M_{12}.2$ but rather an overgroup of shape $2^2.M_{12}.2$, with the final .2 corresponding to $\mathbb{Q}(\sqrt{-5})$ present already in the splitting field of $f_{A2}(t,x)$.

The overgroup also has shape $2.M_{12}.2^2$. Here the quotient 2^2 corresponds to $\mathbb{Q}(\sqrt{3},\sqrt{-15})$. Over $\mathbb{Q}(\sqrt{3})$, the polynomial $f_{A2}(t,x^2)$ has Galois group $2.M_{12}.2$. Over $\mathbb{Q}(\sqrt{-15})$ it has Galois group the isoclinic variant $(2.M_{12}.2)^*$ discussed in §2.6.

Cover C. Here Table 6.1 says that $\tilde{X}_C$ is a double cover of X_C ramified at six points and hence of genus two. A defining polynomial is

$$\tilde{f}_C(t,y) = \text{Resultant}_x(y^2 - 2h(x), f_C(t,x))$$

where, writing $u = \mathbb{Q}(\sqrt{-11})$,

$$\begin{aligned} h(x) \;=\; & 2x^6 + 22x^5u - 22y^5 - 165x^4u - 957x^4 - 1804x^3z + 4664x^3 \\ & + 4884x^2u + 17754x^2 + 4686xu - 15114x + 385u + 1243. \end{aligned}$$

Here the Galois group of the rationalized polynomial $\tilde{f}_{C2}(t,y)$ is indeed the desired $\tilde{M}_{12}.2$. As an example of an interesting specialization, consider $\tau = 5^3/2^2$ from the first line of Table 5.2. A corresponding polynomial is

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

The fields $K(C2, 5^3/2^2)$ and $\tilde{K}(C2, 5^3/2^2)$ respectively have discriminant, root discriminant, and Galois root discriminant as follows:

$$\begin{aligned} d &= 2^{12}3^{24}11^{22}, & \tilde{d} &= 11^2 d^2, \\ \delta &= 2^{1/2}3^{1}11^{11/12} \approx 38.2, & \tilde{\delta} &= 11^{1/24}\delta \approx 42.2, \\ \Delta &= 2^{2/3}3^{25/18}11^{11/12} \approx 65.8, & \tilde{\Delta} &= 11^{1/24}\Delta \approx 72.7. \end{aligned}$$

The first two splitting primes for $\tilde{f}_{C2}(5^3/2^2, x)$ are 1270747 and 2131991.

The specialization point $\tau = 5^3/2^2$ just treated is well behaved as follows. In general, to keep ramification of $\tilde{K}(C2, \tau)$ within $\{2, 3, 11\}$, one must take specialization points in the subset $T_{3,4,11}(\mathbb{Z}^{\{2,3,11\}})$ of $T_{3,2,11}(\mathbb{Z}^{\{2,3,11\}})$. While the known part of $T_{3,2,11}(\mathbb{Z}^{\{2,3,11\}})$ has 394 points, the subset in $T_{3,4,11}(\mathbb{Z}^{\{2,3,11\}})$ has only 78 points. In particular, while $\tau = 5^3/2^2$ is in $T_{3,4,11}(\mathbb{Z}^{\{2,3,11\}})$, the other six specialization points for Cover $C2$ appearing in Table 5.2 are not.

Cover D. From Table 6.1, we see that $f_D(t, y^2) = 0$ is an equation for $\tilde{X}_D$ with $\mathbb{Q}(\sqrt{-11})$ coefficients. This equation combines the good features of the cases just treated. Like $\tilde{X}_A$ but unlike $\tilde{X}_C$, the cover $\tilde{X}_D$ has genus zero. Like Case C but unlike Case A, the Galois group of the rationalized polynomial $f_{D2}(t, y^2)$ over $\mathbb{Q}(t)$ is $\tilde{M}_{12}.2$.

At the 2-3-dropping specialization point $2087^3/2^6 3^{15} 11$ of Table 5.3, a defining polynomial with $e = 11$ is as follows:

$$\begin{aligned}\tilde{f}_{D2}(2087^3/2^6 3^{15} 11, y) \approx \\ y^{48} + 2e^3 y^{42} + 69e^5 y^{36} + 868e^7 y^{30} - 4174e^7 y^{26} + 11287e^9 y^{24} \\ - 4174e^{10} y^{20} + 5340e^{12} y^{18} + 131481e^{12} y^{14} + 17599e^{14} y^{12} \\ + 530098e^{14} y^8 + 3910e^{16} y^6 + 4355569e^{14} y^4 + 20870e^{16} y^2 + 729e^{18}.\end{aligned}$$

The p-adic factorization patterns for the first $|\tilde{M}_{12}.2| = 380160$ primes different from 11 are summarized in Table 2.1. Again one sees agreement with the Haar measure on conjugacy classes. In this case, the first primes split at the $M_{12}.2$ level are 3903881, 8453273, 11291131, 12153887, 15061523 and 15359303. Two of these are still split at the $\tilde{M}_{12}.2$ level, namely 11291131 and 15061523.

The Klüners-Malle database [11] contains an M_{11} field ramified at 661 only. The polynomial just displayed makes M_{12} the second sporadic group known to appear as a subquotient of the Galois group of a field ramified at one prime only. These two examples are quite different in nature, because 661 is much too big to divide $|M_{11}|$ while 11 divides $|M_{12}|$.

References

[1] P. Bayer, P. Llorente & N. Vila, "$\tilde{M}_{12}$ comme groupe de Galois sur $\mathbf{Q}$", *C. R. Acad. Sci. Paris Sér. I Math.* **303** (1986), no. 7, p. 277-280.

[2] W. Bosma, J. J. Cannon, C. Fieker & A. Steel (eds.), *Handbook of Magma functions*, 2.20 ed., University of Sydney Press, 2014.

[3] T. Breuer, "Multiplicity-Free Permutation Characters in GAP, part 2", Manuscript (2006), 43 pages.

[4] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000, xvi+578 pages.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker & R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985, Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray, xxxiv+252 pages.

[6] J. H. Conway & N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov, lxxiv+703 pages.

[7] L. Granboulan, "Construction d'une extension régulière de $\mathbf{Q}(T)$ de groupe de Galois M_{24}", *Experiment. Math.* **5** (1996), no. 1, p. 3-14.

[8] J. W. Jones & D. P. Roberts, "A database of local fields", *J. Symbolic Comput.* **41** (2006), no. 1, p. 80-97, Database at `http://math.la.asu.edu/~jj/localfields/`.

[9] ———, "Galois number fields with small root discriminant", *J. Number Theory* **122** (2007), no. 2, p. 379-407.

[10] ———, "A database of number fields", *LMS J. Comput. Math.* **17** (2014), no. 1, p. 595-618, Database at `http://hobbes.la.asu.edu/NFDB/`.

[11] J. Klüners & G. Malle, "A database for field extensions of the rationals", *LMS J. Comput. Math.* **4** (2001), p. 182-196 (electronic), Database at `http://galoisdb.math.upb.de/`.

[12] G. Malle, "Polynomials with Galois groups $\mathrm{Aut}(M_{22})$, M_{22}, and $\mathrm{PSL}_3(\mathbf{F}_4)\cdot 2_2$ over $\mathbf{Q}$", *Math. Comp.* **51** (1988), no. 184, p. 761-768.

[13] G. Malle & B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999, xvi+436 pages.

[14] J. Martinet, "Petits discriminants des corps de nombres", in *Number theory days, 1980 (Exeter, 1980)*, London Math. Soc. Lecture Note Ser., vol. 56, Cambridge Univ. Press, Cambridge-New York, 1982, p. 151-193.

[15] B. H. Matzat, "Konstruktion von Zahlkörpern mit der Galoisgruppe M_{12} über $\mathbf{Q}(\sqrt{-5})$", *Arch. Math. (Basel)* **40** (1983), no. 3, p. 245-254.

[16] B. H. Matzat & A. Zeh-Marschke, "Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbf{Q}$", *J. Number Theory* **23** (1986), no. 2, p. 195-202.

[17] J.-F. Mestre, "Construction d'extensions régulières de $\mathbf{Q}(t)$ à groupes de Galois $\mathrm{SL}_2(\mathbf{F}_7)$ et $\widetilde{M}_{12}$", *C. R. Acad. Sci. Paris Sér. I Math.* **319** (1994), no. 8, p. 781-782.

[18] P. Müller, "A one-parameter family of polynomials with Galois group M_{24} over $\mathbb{Q}(t)$", `http://arxiv.org/abs/1204.1328`, 2012.

[19] B. Plans & N. Vila, "Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization", *J. Théor. Nombres Bordeaux* **17** (2005), no. 1, p. 271-282.

[20] D. P. Roberts, "An *ABC* construction of number fields", in *Number theory*, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, p. 237-267.

[21] G. J. Schaeffer, "The Hecke stability method and ethereal modular forms", PhD Thesis, Berkeley (USA), 2012.

[22] The PARI group, Bordeaux, "PARI/GP", Version 2.3.4, 2009.

David P. Roberts
Division of Science and Mathematics
University of Minnesota Morris
Morris, MN 56267, USA
E-mail: `roberts@morris.umn.edu`
URL: `http://facultypages.morris.umn.edu/~roberts/`