# LIGHTLY RAMIFIED NUMBER FIELDS WITH GALOIS GROUP $S.M_{12}.A$

DAVID P. ROBERTS

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 [12, 14, 15]. 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 draws the dessins associated to these covers so that the presence of $M_{12}$ and its relation to $M_{12}.2$ can be seen very clearly. Section 5 describes the specialization procedure. Section 6 focuses on $M_{12}$ and $M_{12}.2$ and presents number fields with small root discriminant, small Galois root discriminant, and small number of ramifying primes, These last three notions are related but inequivalent interpretations of "lightly ramified." Finally Section 7 presents some explicit lifts to $\tilde{M}_{12}$ and $\tilde{M}_{12}.2$.

We thank the Simons Foundation for partially supporting this work through grant #209472.

## 2. General background

This section provides general background information to provide some context for the rest of this paper.

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 $\Delta$ of $K$, meaning the root discriminant of $K^g$. One has $\delta \leq \Delta$. To fully compute $\Delta$, one needs to identify the inertia subgroups $I_p \subseteq G$ and their filtration by higher ramification groups.

Online tables associated to [8] and [9] provide a large amount of information on low degree number fields. The tables for [8] 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 [9] 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 $\delta$ 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 non-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. [13] 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 producing complete non-empty lists for a given $G$ 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 smallest root discriminant $\delta$, smallest Galois root discriminant $\Delta$, and smallest $p$ among fields ramifying at a single prime $p$.

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 [12]. 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 [9], the current records for smallest root discriminant are give by the polynomials

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

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

The respective root discriminants are

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

Galois root discriminants are much harder to compute in general, with the general method being sketched in [7]. The interactive website [6] greatly facilitates GRD computations, as indeed in favorable cases it computes GRDs automatically. In the two current cases the GRDs are respectively

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

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 $M_{22}$ [10] and $M_{24}$ [5, 17]. 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. Generators of $M_{12}$ and $M_{12}.2$ are given pictorially in Section 4 and lifts of these generators to $\tilde{M}_{12}$ and $\tilde{M}_{12}.2$ are discussed in Section 7. The Atlas [3] as always provides a concise reference for group-theoretic facts. Several sections of [4] provide further useful background information, making the very beautiful nature of $M_{12}$ clear. To get a first sense

| $C$ | $\lvert C\rvert$ | freq | $\lambda_{12}$ | $\lambda_{12}^t$ | $\lambda_{24}$ | $\lambda_{24}^t$ | §7.3 | §7.4 |
|---|---|---|---|---|---|---|---|---|
| $1A$ | 1 | 1/190080 | $1^{12}$ | $1^{12}$ | $1^{24}$ | $1^{24}$ | 1 | 0 |
| $1A$ | 1 | 1/190080 | $1^{12}$ | $1^{12}$ | $2^{12}$ | $2^{12}$ | 0 | 1 |
| $2A$ | 792 | 1/240 | $2^6$ | $2^6$ | $4^6$ | $4^6$ | 768 | 789 |
| $2B$ | 495 | 1/384 | $2^41^4$ | $2^41^4$ | $2^{12}$ | $2^{12}$ | 470 | 503 |
| $2B$ | 495 | 1/384 | $2^41^4$ | $2^41^4$ | $2^81^8$ | $2^81^8$ | 521 | 515 |
| $3A$ | 1760 | 1/108 | $3^31^3$ | $3^31^3$ | $3^61^6$ | $3^61^6$ | 1735 | 1776 |
| $3A$ | 1760 | 1/108 | $3^31^3$ | $3^31^3$ | $6^32^3$ | $6^32^3$ | 1823 | 1781 |
| $3B$ | 2640 | 1/72 | $3^4$ | $3^4$ | $3^8$ | $3^8$ | 2702 | 2578 |
| $3B$ | 2640 | 1/72 | $3^4$ | $3^4$ | $6^4$ | $6^4$ | 2649 | 2510 |
| $4A$ | 5940 | 1/32 | $4^22^2$ | $4^21^4$ | $4^42^4$ | $4^42^21^4$ | 6002 | 11992 |
| $4B$ | 5940 | 1/32 | $4^21^4$ | $4^22^2$ | $4^42^21^4$ | $4^42^4$ | 5993 | |
| $5A$ | 9504 | 1/20 | $5^21^2$ | $5^21^2$ | $5^41^4$ | $5^41^4$ | 9329 | 9415 |
| $5A$ | 9504 | 1/20 | $5^21^2$ | $5^21^2$ | $10^22^2$ | $10^22^2$ | 9405 | 9613 |
| $6A$ | 15840 | 1/12 | $6^2$ | $6^2$ | $12^2$ | $12^2$ | 15798 | 15819 |
| $6B$ | 15840 | 1/12 | 6321 | 6321 | $6^23^22^21^2$ | $6^23^22^21^2$ | 15863 | 15590 |
| $6B$ | 15840 | 1/12 | 6321 | 6321 | $6^32^3$ | $6^32^3$ | 15881 | 15828 |
| $8A$ | 23760 | 1/8 | 84 | $821^2$ | $8^24^2$ | $8^24\ 21^2$ | 23613 | 47707 |
| $8B$ | 23760 | 1/8 | $821^2$ | 84 | $8^24\ 21^2$ | $8^24^2$ | 24022 | |
| $10A$ | 19008 | 1/10 | (10)2 | 102 | (20)4 | (20)4 | 19048 | 18965 |
| $11AB$ | 17280 | 1/11 | (11)1 | (11)1 | $11^21^2$ | $11^21^2$ | 17031 | 17308 |
| $11AB$ | 17280 | 1/11 | (11)1 | (11)1 | (22)2 | (22)2 | 17425 | 17194 |
| $2C$ | 1584 | 1/120 | $2^{12}$ | | $2^{24}$ | | | 1650 |
| $4C$ | 7920 | 1/24 | $4^42^4$ | | $4^82^8$ | | | 7964 |
| $4D$ | 15840 | 1/12 | $4^6$ | | $8^6$ | | | 15688 |
| $6C$ | 31680 | 1/6 | $6^4$ | | $6^8$ | | | 31651 |
| $10BC$ | 38016 | 1/5 | $10^22^2$ | | $10^42^4$ | | | 38245 |
| $12A$ | 31680 | 1/6 | $12^2$ | | $24^2$ | | | 31577 |
| $12BC$ | 63360 | 1/3 | 12 6 4 2 | | $12^26^24^22^2$ | | | 63493 |

TABLE 2.1. First seven 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 §7.3; distribution of factorization partitions $(\lambda_{12}\lambda_{12}^t, \lambda_{24}\lambda_{24}^t)$ of polynomials $(f_{D2}, \tilde{f}_{D2})$ from §7.4

of $M_{12}$ and its extensions, a understanding of conjugacy classes and their sizes is particularly useful, and information is given in Table 2.1.

To assist in reading Table 2.1, note that $M_{12}$ has fifteen conjugacy classes, $1A$, ..., $10A$, $11A$, $11B$ in Atlas notation. All classes are rational except for $11A$ and $11B$ which are conjugate over $\mathbb{Q}(\sqrt{-11})$. Three pairs of these classes 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 $\{12B, 12C\}$. The cover $\tilde{M}_{12}$ has 26 conjugacy classes, with all classes rational except for the Galois orbits $\{8A1', 8A1''\}$, $\{8B1', 8B1''\}$, $\{10A2', 10A2''\}$, $\{11A1, 11B1\}$, $\{11A2, 11B2\}$. The 21 Galois orbits correspond to the 21 lines of Table 2.1 above the dividing line. 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 columns $\lambda_{12}$, $\lambda_{12}^t$, $\lambda_{24}$, $\lambda_{24}^t$ 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 $\lambda_{12}$ corresponds to the given permutation representation while $\lambda_{12}^t$ corresponds to the twin degree twelve permutation as explained in §2.4 below. Similarly for $\tilde{M}_{12}$, one has $\lambda_{24}$ corresponding to the given permutation representation and $\lambda_{24}^t$ corresponding to its twin. For $M_{12}.2$ one has only the partition $\lambda_{12}\lambda_{12}^t$ of 24, For $\tilde{M}_{24}.2$, one likewise has only the partition $\lambda_{24}\lambda_{24}^t$ of 48.

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 rest of this section consists of general comments, 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 extened 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 to 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 nonsplit 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 [3] prints its character table. The isoclinic [3, §6.7] variant $(2.M_{12}.2)^*$ is considered briefly in [2], 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 §7.1.

## 3. Three-point covers

3.1. **Six partition triples.** Suppose given three conjugacy classes $C_0$, $C_1$, $C_\infty$ 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 $(C_0, C_1, C_\infty)$ is *rigid* in the sense that there exists a unique-up-to-simultaneous-conjugation triple $(g_0, g_1, g_\infty)$ 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 cover degree $n$ cover $X$ of $\mathbb{P}^1$, ramified only above the three points 0, 1, and $\infty$, 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 $S_{\text{loc}}$ is the set of primes dividing the order of one of the elements in a $C_t$, while $S_{\text{glob}}$ is the set of primes dividing $|M|$.

An interesting fact about the $M_n$ is that they contain no rational rigid triples $(C_0, C_1, C_\infty)$. 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 $S_{\text{glob}} = \{2, 3, 5, 11\}$. The extra prime $q$ is 5 for Covers $A$, $B$, and $B^t$, while it is 11 for Covers $C$, $D$, and $E$.

| Name | $\lambda_0$ | $\lambda_1$ | $\lambda_\infty$ | $M_{12}$ | $M_{12}.2$ | $\tilde{M}_{12}$ | $\tilde{M}_{12}.2$ | 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) for specializations, according to Tables 5.2 and 5.3.

3.2. **Cover $A$.** Cover $A$ was studied by Matzat [14] 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 $(g_0, g_1, g_\infty)$. 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

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

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 [15] and studied further in the context of lifting by Bayer, Llorente, and Vila [1] and Mestre [16]. The complication from Cover $A$ of there being two classes of $(g_0, g_1, g_\infty)$ 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

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

The twisting is seen in the polynomial discriminant, which is

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

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

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:

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

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 are one another over $\mathbb{Q}(\sqrt{-11})$. So as for Cover $A$, there is an irrationality in our final polynomials, although this time we knew before computing that the field of definition would be $\mathbb{Q}(\sqrt{-11})$. Abbreviating $u = \sqrt{-11}$, our polynomials are

$$\begin{aligned} f_C(t,x) &= \left(21ux + 13u - 2x^3 - 54x^2 - 321x - 83\right)^3 \\ &\quad \cdot \left(69ux + 1573u - 2x^3 - 102x^2 - 1713x - 10043\right) \\ &\quad + t2^9 3^{12}(253u + 67)tx, \\ f_D(t,x) &= -11^2 u \left(1188ux^3 + 198ux^2 - 1346ux - 27u + 594x^4 \right. \\ &\qquad \left. -7920x^2 - 1474x + 135\right)^3 \\ &\quad -2^8 3^{13}(253u - 67)tx. \end{aligned}$$

As with Cover $A$, we remove irrationalities by forming $f_{C2}(t,x) = f_C(t,x)\overline{f}_C(t,x)$ 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 $(g_0, g_1, g_\infty)$. 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

$$\begin{aligned} &f_{E2}(t,x) = \\ &\quad (1-t)\left(x^6 - 20x^5 + 262x^4 - 15286x^3 + 477665x^2 - 10170814x + 96944940\right)^3 \\ &\quad \left(x^6 + 60x^5 + 2406x^4 + 56114x^3 + 1941921x^2 + 55625130x + 996578748\right) \\ &\quad + t\left(x^{12} + 396x^{10} - 27192x^9 + 933174x^8 - 20101752x^7 + 169737744x^6 \right. \\ &\qquad -16330240872x^5 + 538400028969x^4 - 8234002812376x^3 \\ &\qquad \left. +195276967064388x^2 - 3991355037576144x + 30911476378259268\right)^2 \\ &\quad + 2^4 3^{12} 11^{22} t(t-1). \end{aligned}$$

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

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

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 [12, 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. Dessins and generators

Figure 4.1 draws pictures corresponding to Covers $A$, $B$, and $B^t$ while Figure 4.2 draws pictures corresponding to Covers $C$, $D$, and $E$. In this section, we describe the figures and how they give rise to generators of $M_{12}$ and $M_{12}.2$. To avoid clutter, the twelve edges are not labeled in the figures. To follow the discussion, the reader needs to label the edges by 1, ..., 12, in a way consistent with the text.

### 4.1. Covers $A$, $C$, and $D$.

For $L = A$, $C$, or $D$, the corresponding figure draws the roots of $f_L(0,x)$ as black dots and the roots of $f_L(1,x)$ as white dots. As $t$ moves from 0 to 1, the roots of $f_L(t,x)$ sweep out the twelve edges of the figure. All together, the drawn bipartite graph, viewed as a subset of the Riemann sphere $X_L(\mathbb{C})$, is the dessin of Cover $L$.

Let $T(\mathbb{C}) = \mathbb{C} - \{0,1\}$. Let $\star = 1/2 \in T$. Then the fundamental group $\pi_1(T(\mathbb{C}),\star)$ is the free group $\langle \gamma_0, \gamma_1 \rangle$ where $\gamma_k$ is the counterclockwise circle of radius $1/2$ about $k$. One has a natural extension $\pi_1(T(\mathbb{C})_{\mathbb{R}},\star)$ obtained from $\pi_1(T(\mathbb{C}),\star)$ by adjoining a complex conjugation operator $\sigma$ satisfying the involutory relation $\sigma^2 = 1$ and the intertwining relations $\sigma m_0 = m_0^{-1}\sigma$, and $\sigma m_1 = m_1^{-1}\sigma$.

For each $L$, in conformity with the general theory of dessins, we have a homomorphism $\rho_L$ from $\pi_1(T(\mathbb{C}),\star)$ into the group of permutations of the twelve edges. Always the image is $M_{12}$. Again in conformity with the general theory, $\rho_L(\gamma_0)$ is the minimal counterclockwise rotation about the black dots while $\rho_L(\gamma_1)$ is the minimal counterclockwise rotation about the white dots.

Covers $A$, $C$, and $D$ behave very similarly. Taking Cover $D$ as an example, and indexing edges in the figure roughly from left to right, one has

$$\rho_D(\gamma_0) = (1,2,3)(4,5,6)(7,8,9)(10,11,12),$$
$$\rho_D(\gamma_1) = (3,4)(5,7)(8,10)(11,12).$$

In the cases of $A$, $C$, and $D$, the twin permutation is easily visualized as follows. Consider the complex conjugates of the dessins, obtained by flipping the drawn pictures upside down. In the new pictures, the image of edge $e$ is denoted $\overline{e}$. Then we can apply the general theory again. In the case of Cover $D$ the result is

$$\rho_D^t(\gamma_0) = (\overline{3},\overline{2},\overline{1})(\overline{6},\overline{5},\overline{4})(\overline{9},\overline{7},\overline{6})(\overline{12},\overline{11},\overline{10}),$$
$$\rho_D^t(\gamma_1) = (\overline{3},\overline{4})(\overline{5},\overline{7})(\overline{8},\overline{10})(\overline{11},\overline{12}).$$

In other words, if one identifies the twelve $e$ with their corresponding $\overline{e}$, one has $\rho_D(\gamma_0) = \rho_D^t(\gamma_0)^{-1}$ and $\rho_D(\gamma_1) = \rho_D^t(\gamma_1)$. The same relations hold with $D$ replaced by $A$ or $C$.

The permutation representations $\rho_L$ and $\rho_L^t$ are extraordinarily similar to each other in our three cases $L = A$, $C$, and $D$. Continuing with our example of Case $D$, considers words $w$ of length $\leq 14$ in $\gamma_0$ and $\gamma_1$. Then 339 different permutations arise as $\rho_D(w)$. For each one of them, the cycle type of $\rho_D(w)$ and the cycle type

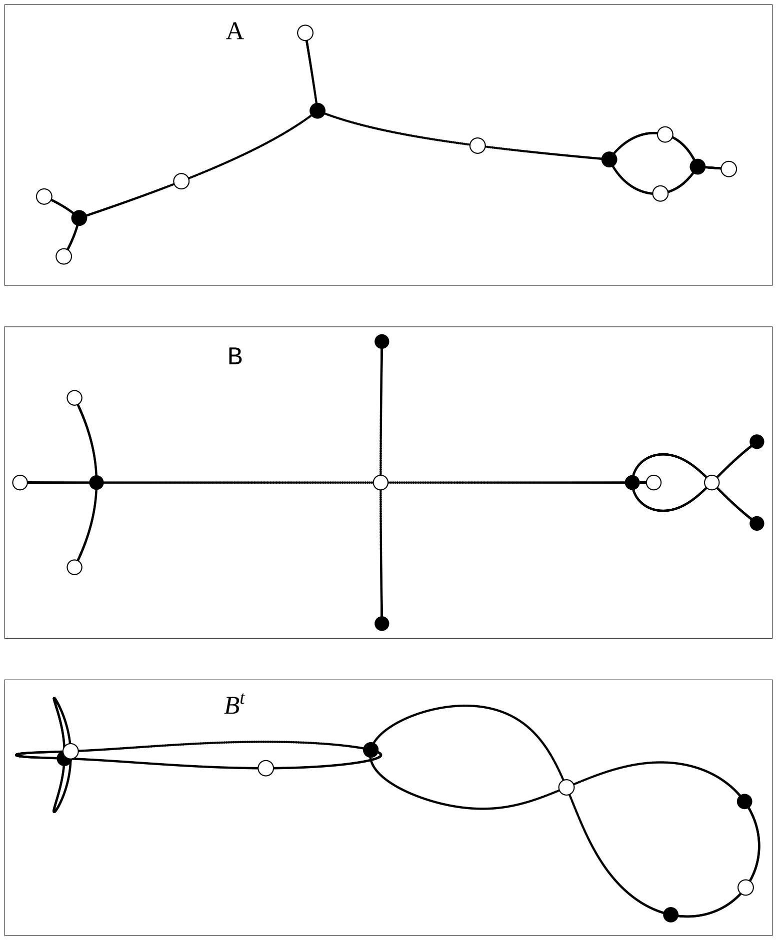


FIGURE 4.1. Dessins for Covers $A$, $B$, and $B^t$. For Covers $A$ and $B$, the ambient surface is the plane of the page; for Cover $B^t$ it is a genus two double cover of the plane of the page.

of $\rho_D^t(w)$ agree. Only for words of length 15 does one first get a disagreement:

$$\rho_D(\gamma_0^2\gamma_1\gamma_0\gamma_1\gamma_0\gamma_1\gamma_0^2\gamma_1\gamma_0\gamma_1\gamma_0^2\gamma_1) = (1,8,6,5)(4,9,7,11)(2)(3)(10)(12),$$
$$\rho_D^t(\gamma_0^2\gamma_1\gamma_0\gamma_1\gamma_0\gamma_1\gamma_0^2\gamma_1\gamma_0\gamma_1\gamma_0^2\gamma_1) = (\overline{2},\overline{11},\overline{10},\overline{6})(\overline{3},\overline{4},\overline{8},\overline{9})(\overline{1},\overline{5})(\overline{7},\overline{12}).$$

Only for words of length 18 does one first get the other possible disagreement with $\rho_D(w)$ and $\rho_D^t(w)$ having different cycle types, one 84 and the other $821^2$.

Reinterpreting, one immediately gets homomorphisms $\rho_{L2} : \pi_1(T(\mathbb{C})_\mathbb{R}, \star) \to S_{24}$ with image $M_{12}.2$. Namely the twenty-four element set is $\{1, \ldots, 12\} \cup \{\overline{1}, \ldots, \overline{12}\}$. The element $\rho_{L2}(\sigma)$ acts by interchanging each $e$ with its $\overline{e}$. For $k \in \{0, 1\}$ one has $\rho_{L2}(\gamma_k) = \rho_L(\gamma_k)\rho_L^t(\gamma_k)$.

4.2. **Covers $B$ and $B^t$.** Inside the Riemann sphere $X_B(\mathbb{C})$, we use black dots to represent roots of $f_B(-\sqrt{5}, x)$ and white dots to represent roots of $f_B(\sqrt{5}, x)$. The twelve edges then correspond to the twelve preimages in the $x$-line of the interval

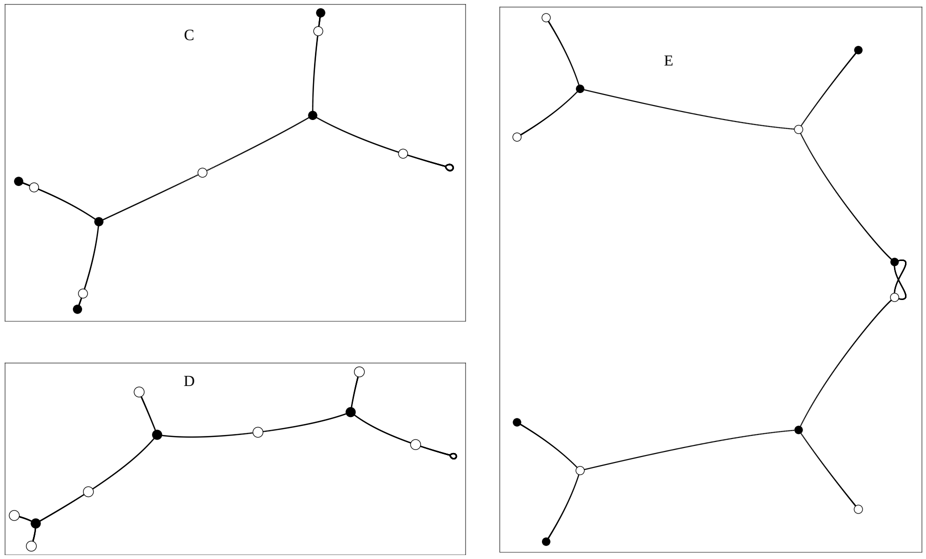


FIGURE 4.2. Dessins for Covers $C$, $D$, and $E$. For $C$ and $D$, the rightmost black and white vertices, of valence 3 and 2 respectively, are not drawn, so as not to obscure the small loop to the right. For Covers $C$ and $D$, the ambient surface is the plane of the page; for Cover $E$ it is a genus zero double cover of the plane of the page.

$(-\sqrt{5}, \sqrt{5})$. Now we have monodromy operators $m_\pm = m_{\pm\sqrt{5}}$ and a complex conjugation $\sigma$ as before. From the picture, indexing edges roughly from left to right again, one immediately has

$$\rho_B(m_-) = (1,2,4,3)(7,9,8,10)(5)(6)(11)(12),$$
$$\rho_B(m_+) = (4,5,7,6)(9,11,12,10)(1)(2)(3)(8),$$
$$\rho_B(\sigma) = (2,3)(5,6)(9,10)(11,12)(1)(4)(7)(8).$$

The fact that Cover $B$ is defined over $\mathbb{R}$ corresponds to $\rho_B(\sigma)$ already being in $M_{12}$.

There are complications with presenting the twin case $B^t$ visually, since $X_{B^t}$ has genus two. If we drew things using the $x$-variable, we would have four black dots and four white dots, all distinct in the $x$-plane. An advantage of this presentation would be that complex conjugation would be represented by the standard flip; this flip would fix exactly two of the black dots and all four of the white dots. A disadvantage would be that some edges would be right on top of other edges, and some edges would fold back on themselves.

Instead, we perturb things slightly, using the $y$-variable of §3.3, introducing the new variable $z = x + iy/200$, and drawing the dessin instead in the $z$ plane. Now monodromy operators $\rho_{B^t}(m_-)$ and $\rho_{B^t}(m_+)$ can be easily read off the picture. Even $\rho_{B^t}(\sigma) = (2,3)(7,8)(9,10)(11,12)$ can be clearly read off, the deformed version of the real axis through all four white dots being easily imagined.

4.3. **Cover $E$.** Inside the sphere $X_E(\mathbb{C})$, we draw the roots of $f_E(-\sqrt{-11}, x)$ as black dots and the roots of $f_E(\sqrt{-11}, x)$ as white dots. As $s$ moves upward from

$-\sqrt{-11}$ to $\sqrt{-11}$, the twelve roots of $f_E(s,x)$ sweep out the twelve drawn edges. We work now with monodromy operators $m_\pm = m_{\pm\sqrt{-11}}$. Because the ramification points $\pm\sqrt{-11}$ are no longer real, complex conjugation now satisfies $\sigma m_- = m_+^{-1}\sigma$ and $\sigma m_+ = m_-^{-1}\sigma$.

The changes do not obstruct our basic procedure. From the picture we have

$$\rho_E(m_+) = \rho_E^t(m_-) = (3,4,5)(6,7,8)(10,11,12),$$
$$\rho_E(m_-) = \rho_E^t(m_+) = (10,9,8)(5,6,7)(1,2,3).$$

In this case, as just indicated, the twin representation is obtained by reversing the roles of the black and white dots. For the monodromy representation and its twin, complex conjugation acts by subtraction from 13 on indices: $\rho_E(\sigma) = \rho_E^t(\sigma) = (1,12)(2,11)(3,10)(4,9)(5,8)(6,7)$.

The degree 24 dessin corresponding to $f_{E2}(t,x)$ can be easily imagined from our drawn degree 12 dessin corresponding to $f_E(s,x)$. Namely, one first views both white dots and black dots as associated to the number $t=0$. Then one adds say a cross at the appropriate midpoint $\epsilon$ of each edge $e$, viewing these twelve crosses as associated to the number $t=1$. Any old edge $e$ now splits into two edges $\epsilon b$ and $\epsilon w$, with $\epsilon b$ incident on a black vertex and $\epsilon w$ incident on a white vertex. The monodromy operator about zero is then

$$\rho_{E2}(m_0)=(3b,4b,5b)(6b,7b,8b)(10b,11b,12b)(10w,9w,8w)(5w,6w,7w)(1w,2w,3w).$$

The operator $\rho_{E2}(m_1)$ acts by switching each $\epsilon b$ and $\epsilon w$ while the complex conjugation operator $\rho_{E2}(\sigma)$ acts by switching $\epsilon c$ and $(13-\epsilon)c$ for either color $c$.

## 5. 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.

5.1. **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 $\infty$ on the $t$-line. Then for each $\tau \in T(\mathbb{Q}) = \mathbb{Q} - \{0,1\}$, one has an associated number algebra $K_\tau$. When $f(\tau,x)$ is separable, which it is for all our covers and all $\tau$, 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 $\tau$ 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 $\infty$. A point $\tau$ is in arm $k \in \{0,1,\infty\}$ if $\tau$ reduces to $k$ modulo $p$. Otherwise, $\tau$ is generic. If $\tau$ is in arm $k$, then one has its extremality index $j \in \mathbb{Z}_{\geq 1}$, defined by $j = \mathrm{ord}_p(\tau)$, $j = \mathrm{ord}_p(\tau - 1)$, and $j = -\mathrm{ord}_p(\tau)$ for $k = 0$, 1, and $\infty$ 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 $K_\tau$ is very simple. First, if $\tau$ is generic, then $p$ is unramified in $K_\tau$. Second, suppose $\tau$ is in arm $k$ with extremality index $j$; then the $p$-inertial subgroup of the Galois group of $K_\tau$ is conjugate to $g_k^j$, 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 $\tau$ on the arm $k$ yields a $K_\tau$ 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 $\tau$ giving $K_\tau$ ramified only within $S$ depends only on $S$ and the monodromy orders $m_0$, $m_1$, and $m_\infty$. 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 $\tau = -ax^p/cz^r$ where $(a,b,c,x,y,z)$ are integers satisfying the $ABC$ equation $ax^p + by^q + cz^r = 0$ 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 $\tau$.

To find elements in some $T_{m_0,m_1,m_\infty}(\mathbb{Z}^S)$ one can carry out a computer search, restricting to $|ax^p|$ and $|cz^r|$ less than a certain height cutoff, say of the form $10^u$. As one increases $u$, the new $\tau$ found rapidly become more sparse. Many of the new $\tau$ are not entirely new, as they are often base-changes of lower-height $\tau$ 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, | $158470321^3$ | $-\ 1994904202391^2$ | $+\ 2^{10}3^45^119^{10}$ | $=0$ |
| $B$,$B^t$: $\lvert T^5_{(4,4),10}\rvert$ | $=$ 27, | $79^4$ | $-\ 6881^2$ | $+\ 2^83^85$ | $=0$ |
| $C2$,$D2$: $\lvert T^{11}_{3,2,11}\rvert$ | $=$ 394, | $2540833^3$ | $-\ 4050085583^2$ | $+\ 2^{18}3^111^6$ | $=0$ |
| $E2$: $\lvert T^{11}_{3,2,12}\rvert$ | $=$ 395, | $796531585^3$ | $-\ 22481204531903^2$ | $+\ 2^{11}3^511^217^{12}$ | $=0$ |

Table 5.1. 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 5.1. The right columns give the ABC triple corresponding to the element $\tau$ 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 $\tau$ for which $5(1-\tau)$ is a perfect square. Each of these gives two specialization points $\sigma = \pm\sqrt{5(1-\tau)}$ in $T_{(4,4),10}$ and then we consider $\sigma = 0$ as in $T^5_{(4,4),10}$ as well. The displayed ABC triple yields $\sigma = \pm 6881/2^43^4$.

5.2. **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 features 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 5.2 and 5.3 gives a value of $\mathrm{ord}_p(K_\tau)$ for the indicated cover and for $\tau$ 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 $\infty$-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

| gen | $\tau$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 0 | (68) | | | **Cover** $A2$ | | | | | | |
| | 1 | 62 | (50) | | | | | | | | |
| | $\infty$ | 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) | | | | | | |
| | $\infty$ | 52 | 48 | 24 | 42 | 38 | 22 | 32 | 34 | 22 | 30 |
| | | 24 | 22 | 22 | 22 | (0 | 20 | 16 | 20 | 16 | 12 |
| 5 | 0 | 34 | 26 | (20 | 12 | 20) | | | | | |
| | 1 | 34 | 26 | (18) | | | | | | | |
| $26, 18$ | $\infty$ | (42 | 42 | 42 | 42 | 26) | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 0 | ($\{18, 20, 24\}$) | | | **Cover** $B$ | | | | | | |
| | 1 | (34) | | | | | | | | | |
| | $\infty$ | $\{16, 22\}$ | 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 | $\infty$ | 16 | 16 | 10 | 14 | 12 | 10 | 10 | (10 | 0 | 10 |
| $8, 10$ | | 8 | 10 | 8 | 6 | 8 | 10 | 8) | | | |
| 5 | 0 | 14 | (8) | | | | | | | | |
| 18 | $\infty$ | (10 | $\{6, 10\}$ | 20 | 18 | 20 | 18 | $\{8, 12\}$ | 18 | 20 | 18) |

TABLE 5.2. Specialization tables for Covers $A2$ and $B$.

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, $\mathrm{ord}_2(K_\tau) = 36$ is the only possibility for extremality 12, and it is likewise the only possibility for extremalities $12 + 11k$. 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].

5.3. **Field equivalence.** A typical situation is that $f(\tau, x)$ is ireducible but has large coefficients. Starting in the next subsection, we apply *Pari*'s command *polredabs* [18] 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 $\phi$ 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.

5.4. **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 $K_\tau$, 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.

| gen | $\tau$ | 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) | | | | | | | |
| | $\infty$ | 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 | $\infty$ | 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 | $\infty$ | (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) | | | | | | | |
| | $\infty$ | 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 | $\infty$ | 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 | $\infty$ | (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 $E2$** | | | | | | | |
| | $\infty$ | 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 | $\infty$ | 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 | $\infty$ | 40 | 40 | 36 | 36 | 32 | 32 | 28 | 28 | 24 | 24 |
| | | (0 | 22 | 20 | 18 | 16 | 22 | 12 | 22 | 16 | 18 |
| | | 20 | 22) | | | | | | | | |

TABLE 5.3. Specialization tables for Covers $C2$, $D2$ and $E2$, with $a = \{24, 36, 48\}$ and $b = \{32, 40, 52\}$ in the case of Cover $E2$.

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 5.4. In this table, and also Tables 5.5, 6.1, 6.2, we present an analysis of ramification using the notation of [6] and making use

| | | | | Basic $p$-adic invariants | | | Slope Content | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Cover | $\tau$ | Fact | $G$ | 2 | 3 | 5 | 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 5.4. Description of $K_\tau$ and $K_\tau^t$ for the three $\tau$ in $X^5_{(4,4),10}$ for which the Galois group is smaller than $M_{12}$

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 decomposition groups and their natural filtration. This first field is tame at 3 with inertia group of size 11 and thus a contribution of $3^{10/11}$ to the GRD. It is wild at 2 and 5 with inertia groups of sizes 6 and 10 and contributions $2^{4/3}$ and $5^{13/10}$ to the GRD respectively. The Galois root discriminant, as printed, is $2^{4/3}3^{10/11}5^{13/10} \approx 55.4$.

Continuing to discuss Table 5.4, 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

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

The field $K(B, -5/2)$ is very lightly ramified, comparable with the remarkable dodecic $L_2(11)$ field on [9] with GRD = RD = $\sqrt{1831} \approx 42.8$. 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 in our Section 2.

For covers $A2$, $C2$, $D2$, and $E2$ there are all together 1630 specialization points $\tau$. Three of them yield group drops as in Table 5.5. In all three cases, the Galois group

| | | | | Basic $p$-adic invariants | | | Slope Content | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Cover | $\tau$ | Fact | $G$ | 2 | 3 | 11 | 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 5.5. 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 $E2$

is $PGL_2(11) = L_2(11)$, 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.

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

This section reports on ramification of specializations to 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 §5.3 on field equivalence and of §5.4 on $p$-adic ramification.

According to Tables 5.2 and 5.3 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 §6.1, §6.2, and §6.3 focus respectively on fields with small root discriminant, small Galois root discriminant, and at most two ramifying primes.

### 6.1. 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 6.1 below. This is substantially above the smallest known root discriminant $2^2 3^1 29^{1/3} \approx 36.9$ from [9], 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 twice, once from $-17^3/2^7$ and once from $7^3/2^9$. Both these specialization points define the same field. 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 $D2$.

6.2. **Small Galois root discriminant.** For $M_{12}$, the smallest known Galois root discriminant appears in [9] and also on the first line of Table 6.1. The fact that $E$ appears only once in Table 6.1 is just a reflection of the simple fact that $q = 5$ for $B$ and $B^t$ while $q = 11$ for $E$.

| Cover | $\tau$ | Basic $p$-adic invariants 2 | 3 | $q$ | Slope Content 2 | 3 | $q$ | RD | GRD |
|---|---|---|---|---|---|---|---|---|---|
| $B$ | $5$ | $8_{16}3_2 1$ | $11_{10}$ | $10_{13}2_1$ | $[\frac{4}{3}, \frac{4}{3}, 3]_3^2$ | $[\,]_{11}^5$ | $[\frac{3}{2}]_2$ | 46.2 | 93.2 |
| $B^t$ | | $8_{16}4_4$ | $11_{10}$ | $10_{13}2_1$ | | | | 51.6 | |
| $B$ | $0$ | $12_{34}$ | $9_9 2_1 1$ | $3_2^2 3_2^2$ | $[\frac{23}{6}, \frac{23}{6}, 3, \frac{8}{3}, \frac{8}{3}]_3^2$ | $[\frac{9}{8}, \frac{9}{8}]_8^2$ | $[\,]_3^2$ | 52.1 | 112.0 |
| $B^t$ | | $12_{34}$ | $12_{12}$ | $3_2^2 3_2^2$ | | | | 62.5 | |
| $B$ | $5/2$ | $12_{12}$ | $9_9 2_1 1$ | $10_{13}2_1$ | $[\frac{8}{3}, \frac{8}{3}, \frac{4}{3}, \frac{4}{3}]_3^2$ | $[\frac{9}{8}, \frac{9}{8}]_8^2$ | $[\frac{3}{2}]_2$ | 58.2 | 132.4 |
| $B^t$ | | $12_{12}$ | $12_{12}$ | $10_{13}2_1$ | | | | 69.9 | |
| $B$ | $-5$ | $4_8^3$ | $9_9 2_1 1$ | $10_{13}2_1$ | $[3, \frac{5}{2}, 2, 2]^6$ | $[\frac{9}{8}, \frac{9}{8}]_8^2$ | $[\frac{3}{2}]_2$ | 65.3 | 153.0 |
| $B^t$ | | $4_8^3$ | $12_{12}$ | $10_{13}2_1$ | | | | 78.5 | |
| $B$ | $-3$ | $8_{16}4_4$ | $8_7 2_1 1\,1$ | $5_9^2 1^2$ | $[3, \frac{4}{3}, \frac{4}{3}]_3^2$ | $[\,]_8^2$ | $[\frac{9}{4}]_4^2$ | 73.8 | 255.6 |
| $B^t$ | | $8_{16}3_2 1$ | $8_7 4_3$ | $10_{19}2_1$ | | | | 103.3 | |
| $E$ | $-319/54$ | $2_2^3 2_2^3$ | $3_3^3 3_3$ | $11_{16}1$ | $[2]^3$ | $[\frac{3}{2}]^3$ | $[\frac{8}{5}]_5$ | 146.8 | 280.6 |
| $E$ | $319/54$ | $2_2^3 2_2^3$ | $3_3^3 3_3$ | $11_{16}1$ | | | | 146.8 | |
| $B$ | $-5/3$ | $6_{10}4_8 2_2$ | $9_{16}1^2 1$ | $10_{13}2_1$ | $[\frac{8}{3}, \frac{8}{3}, 2]_3^2$ | $[2, 2]^2$ | $[\frac{3}{2}]_2$ | 89.8 | 287.9 |
| $B^t$ | | $6_{10}4_8 2_2$ | $9_{16}1^2 1$ | $10_{13}2_1$ | | | | 89.8 | |

TABLE 6.1. The fourteen $M_{12}$ fields from our list with Galois root discriminant $\leq 300$, grouped in twin pairs. The two $\tau$'s for $E$ both come from $\sigma = 23^3/2^2 3^6$.

For $M_{12}.2$, Galois root discriminants can be substantially smaller than the minimum known for $M_{12}$, as illustrated by Table 6.2. In this case, in contrast to $M_{12}$, the field giving the smallest known root discriminant also gives the smallest known Galois root discriminant.

| Cover | $\tau$ | 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 6.2. The ten $M_{12}.2$ fields from our list with the Galois root discriminant $\leq 100$.

6.3. **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 $\pm 2^a 3^b q^c$ 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 5.2 the prime 3 drops out from the discriminant exactly if $\text{ord}_3(\tau) \in \{-15, -25, -35, \ldots\}$. This drop occurs in 2 of our 447 specializations:

$$\begin{aligned} d_{A2}(71^3/2^3 3^{15} 5^2) &= 2^{66} 5^{42}, \\ d_{A2}(3289^3/2^7 3^{15} 5) &= 2^{60} 5^{42}. \end{aligned}$$

For Covers $C2$ and $D2$, from Table 5.3 the prime 2 drops out exactly if $\text{ord}_2(\tau) \in \{6, 9, 12, \ldots\} \cup \{6, 17, 28, \ldots\}$. This much less demanding condition is met by 24 of our 394 specialization points, as listed in Table 6.3.

| $\tau$ | $d_{C2}(\tau)$ | $d_{D2}(\tau)$ | $\tau$ | $d_{C2}(\tau)$ | $d_{D2}(\tau)$ |
|---|---|---|---|---|---|
| $-2^9 5^3/3^2$ | $3^{38}11^{22}$ | $3^{48}11^{20}$ | $-2^6 31^3/3^3 11^5$ | $3^{22}11^{44}$ | $3^{20}11^{44}$ |
| $-11^2/2^6 3^3$ | $3^{22}11^{28}$ | $3^{24}11^{28}$ | $-2^6/3^3 11$ | $3^{18}11^{44}$ | $3^{24}11^{44}$ |
| $-2^9/3^3$ | $3^{22}11^{32}$ | $3^{24}11^{32}$ | $173^3/2^6 11^7$ | $3^{34}11^{44}$ | $3^{40}11^{44}$ |
| $-11\cdot 131^3/2^6 3^3$ | $3^{18}11^{36}$ | $3^{24}11^{36}$ | $2^9/3\cdot 11^3$ | $3^{42}11^{44}$ | $3^{52}11^{44}$ |
| $-3^3 11/2^6$ | $3^{20}11^{36}$ | $3^{36}11^{36}$ | $13^3/2^6 11^2$ | $3^{34}11^{44}$ | $3^{44}11^{44}$ |
| $-11/2^6$ | $3^{34}11^{36}$ | $3^{44}11^{36}$ | $7^3/2^6 11$ | $3^{24}11^{44}$ | $3^{20}11^{44}$ |
| $2^6 11/3^6$ | $3^{22}11^{36}$ | $3^{22}11^{36}$ | $2087^3/2^6 3^{15} 11$ | $3^{20}11^{44}$ | $11^{44}$ |
| $11\cdot 59^3/2^{17} 3^2$ | $3^{38}11^{36}$ | $3^{48}11^{36}$ | $3^6/2^6 11$ | $3^{24}11^{44}$ | $3^{28}11^{44}$ |
| $-67^3/2^6 11$ | $3^{34}11^{44}$ | $3^{40}11^{44}$ | $553^3/2^6 3^9 11^2$ | $3^{22}11^{44}$ | $3^{22}11^{44}$ |
| $-2^{12}/11$ | $3^{34}11^{44}$ | $3^{40}11^{44}$ | $313^3/2^6 3^6 11$ | $3^{22}11^{44}$ | $3^{22}11^{44}$ |
| $-2^6 3^3/11^2$ | $3^{20}11^{44}$ | $3^{36}11^{44}$ | $89^3/2^6 11^2$ | $3^{24}11^{44}$ | $3^{32}11^{44}$ |
| $-2^6/11$ | $3^{34}11^{44}$ | $3^{40}11^{44}$ | $7033^3/2^6 3^6 11^4$ | $3^{22}11^{44}$ | $3^{22}11^{44}$ |

TABLE 6.3. The 24 specialization points of $T^{11}_{3,2,11}$ at which 2 does out from discriminants of specializations in the $C2$ and $D2$ families

Also for Covers $C2$ and $D2$ it is possible for 3 to drop out. From Table 5.3 this occurs if $\text{ord}_3(\tau)$ 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 $D$, the one 3-drop occurs where there is also a 2-drop. An equation for the corresponding number field is given at the end of §7.4.

## 7. 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.

7.1. **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 §7.3 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 in $\mathbb{Q}[y]$ with Galois group $(2.M_{12}.2)^*$.

7.2. **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 7.1 reprints the six partition triples belonging to $M_{12}$ of Table 3.1 and for each indicates lifts to partition triples in $\tilde{M}_{12}$. For a fixed label $L$ in $\{A, B, B^t, C, D, E\}$, let $(g_0, g_1, g_\infty)$ be the permutation triple in $M_{12}$ presented pictorially in Figure 4.1 or 4.2. Then our main focus is a permutation triple $(\tilde{g}_0, \tilde{g}_1, \tilde{g}_\infty)$. Here each $\tilde{g}_k$ is in the class indicated in row $\tilde{L}$ and column $k$ of Table 7.1. One has $\tilde{g}_0\tilde{g}_1\tilde{g}_\infty = 1$ and 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 7.1 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 $\tilde{X}_L$.

| Cover | 0 | 1 | $\infty$ | $g$ |
|---|---|---|---|---|
| $A$ | $3^4$ | $2^4 1^4$ | $(10)2$ | 0 |
| $\tilde{A}$ | $3^8$ | $2^8 1^8$ | $(20)4$ | 0 |
| | $6^4$ | $2^{12}$ | $(20)4$ | |
| $B$ | $4^2 1^4$ | $4^2 1^4$ | $(10)2$ | 0 |
| $\tilde{B}$ | $4^4 2^2 1^4$ | $4^4 2^2 1^4$ | $(20)4$ | 2 |
| | $4^4 2^2 1^4$ | $4^4 2^2 1^4$ | $(20)4$ | |
| $B^t$ | $4^2 2^2$ | $4^2 2^2$ | $(10)2$ | 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 | $\infty$ | $g$ |
|---|---|---|---|---|
| $C$ | $3^3 1^3$ | $2^6$ | $(11)1$ | 0 |
| $\tilde{C}$ | $3^6 1^6$ | $4^6$ | $11^2 1^2$ | 2 |
| | $6^3 2^3$ | $4^6$ | $(22)2$ | |
| $D$ | $3^4$ | $2^4 1^4$ | $(11)1$ | 0 |
| $\tilde{D}$ | $3^8$ | $2^8 1^8$ | $(22)2$ | 0 |
| | $6^4$ | $2^{12}$ | $11^2 1^2$ | |
| $E$ | $3^3 1^3$ | $3^3 1^3$ | 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 7.1. Lifts of partition triples in $M_{12}$ to partition triples in $\tilde{M}_{12}$.

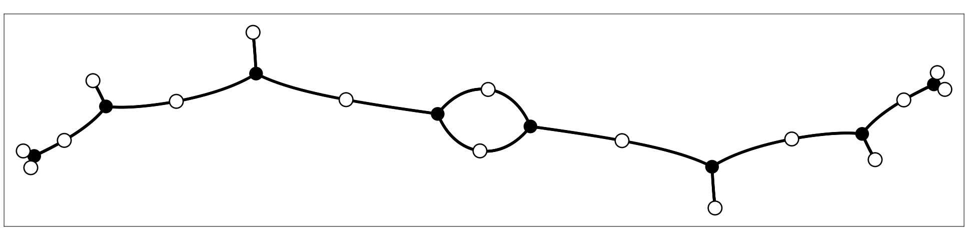

FIGURE 7.3. The dessin of $f_{\tilde{D}}(t, y)$ in the complex $y$-line

To understand Table 7.1 in diagrammatic terms, consider Cover $D$ as an example. The curve $X_D$ is just the complex $x$-line. Its cover $\tilde{X}_D$ is just the complex $y$-line, with relation given by $y = x^2$. The dessin drawn in $X_D$ in Figure 4.2 "unwinds" to a double cover dessin in $\tilde{X}_D$ drawn in Figure 7.3. The monodromy operators are

$$\begin{aligned}\tilde{g}_0 = \rho_{\tilde{D}}(\gamma_0) &= (1,2,3)(4,5,6)(7,8,9)(10,11,12)\\ &\qquad (-1,-2,-3)(-4,-5,-6)(-7,-8,-9)(-10,-11,-12)\\ \tilde{g}_1 = \rho_{\tilde{D}}(\gamma_1) &= (3,4)(5,7)(8,10)(11,-12)(-11,12)(-3,-4)(-5,-7)(-8,-10)\end{aligned}$$

Cover $A$ is extremely similar, with $\tilde{X}_A$ also covering $X_A$ via $y = x^2$.

At a geometric level, the six covers behave similarly, as just described. However 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.

7.3. **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 $\epsilon$ 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 [6, §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 [16], summarizing the approach of [1], we have the general formula

$$\epsilon(K(B,\tau)_v) = (25 - 5\tau^2, \tau)_v, \tag{7.1}$$

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 7.1, 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 (7.1) vanish. This motivates consideration of the following base-change diagram of smooth projective complex algebraic curves:

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

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 $\infty$. While $\tilde{X}_B$ is not realizable over $\mathbb{Q}$, Mestre proved that $\tilde{Z}_B$ is realizable [16].

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 6.1 is unobstructed. Corresponding equations are

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

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

Carefully taking square roots of the correct field elements, to avoid Galois groups such as the generically occuring $2^{12}.M_{12}$, we find covering $\tilde{M}_{12}$ fields to be given by

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

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

The $p$-adic factorization partitions of these 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 $\tilde{M}_{12}$ in 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 $\infty$, 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 $2A2$ of cycle type $4^6$, and so the complex conjugation element cannot lift.

7.4. **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 7.1, 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 7.1 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

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

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 $\tau = 5^3/2^2$ corresponding to the first line of Table 6.2. A corresponding polynomial is

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

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 $\tilde{K}(C,\tau)$ 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 $\tau = 5^3/2^2 \in T_{3,4,11}(\mathbb{Z}^{\{2,3,11\}})$, the other six specialization points for Cover $C2$ appearing in Table 6.2 are not.

*Cover D*. From Table 7.1 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 6.3, a defining polynomial with $e = 11$ is as follows:

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

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, 15359303. Two of these are still split at the $\tilde{M}_{12}.2$ level, namely 11291131 and 15061523.

The Klüners-Malle database [9] 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] Bayer, Pilar; Llorente, Pascual; Vila, Núria. $\tilde{M}_{12}$ comme groupe de Galois sur **Q**. C. R. Acad. Sci. Paris Sr. I Math. 303 (1986), no. 7, 277-280.

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

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

[4] Conway, J. H.; Sloane, N. J. A. Sphere packings, lattices and groups. Third edition. Grundlehren der Mathematischen Wissenschaften, 290. Springer-Verlag, New York, 1999. lxxiv+703 pp. ISBN: 0-387-98585-9

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

[6] Jones, John W.; Roberts, David P. A database of local fields. J. Symbolic Comput. 41 (2006), no. 1, 80-97. Database at `http://math.la.asu.edu/~jj/localfields/`

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

[8] ——— A database of number fields, submitted. Arxiv preprint 1404.0266. Database at `http://hobbes.la.asu.edu/NFDB/`

[9] Klüners, Jürgen; Malle, Gunter. A database for field extensions of the rationals. LMS J. Comput. Math. 4 (2001), 182-196. Database at `http://galoisdb.math.upb.de/`

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

[11] ——— Multi-parameter polynomials with given Galois group. Algorithmic methods in Galois theory. J. Symbolic Comput. 30 (2000), no. 6, 717-731.

[12] Malle, Gunter; Matzat, B. Heinrich. Inverse Galois theory. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999. xvi+436 pp.

[13] Martinet, Jacques. Petits discriminants des corps de nombres. Number theory days, 1980 (Exeter, 1980), London Math. Soc. Lecture Note Ser., 56 (1982), 151–193.

[14] Matzat, B. Heinrich. Konstruktion von Zahlkörpern mit der Galoisgruppe $M_{12}$ über $\mathbf{Q}(\sqrt{-5})$. Arch. Math. (Basel) 40 (1983), no. 3, 245254.
[15] Matzat, B. Heinrich; Zeh-Marschke, Andreas. Realisierung der Mathieugruppen $M_{11}$ und $M_{12}$ als Galoisgruppen über $\mathbf{Q}$. J. Number Theory 23 (1986), no. 2, 195-202.
[16] Mestre, Jean-François. 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 Sr. I Math. 319 (1994), no. 8, 781-782.
[17] Müller, Peter. A one-parameter family of polynomials with Galois group $M_{24}$ over $\mathbb{Q}(t)$. Arxiv preprint: 1204.1328v1.
[18] The PARI group, Bordeaux. PARI/GP. Version 2.3.4, 2009.
[19] Plans, Bernat; Vila, Núria. 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, 271-282.
[20] Roberts, David P. An *ABC* construction of number fields. Number theory, 237267, CRM Proc. Lecture Notes, 36, Amer. Math. Soc., Providence, RI, 2004.
[21] Schaeffer, George J. The Hecke stability method and ethereal modular forms. Berkeley Ph. D. thesis, 2012.

Division of Science and Mathematics, University of Minnesota Morris, Morris, MN 56267
*E-mail address*: roberts@morris.umn.edu