2004

An ABC Construction of Number Fields

David P. Roberts
University of Minnesota - Morris, roberts@morris.umn.edu

An ABC construction of number fields

David P. Roberts

Abstract. We describe a general three step method for constructing number fields with Lie-type Galois groups and discriminants factoring into powers of specified primes. The first step involves extremal solutions of the matrix equation $ABC = I$. The second step involves extremal polynomial solutions of the equation $A(x) + B(x) + C(x) = 0$. The third step involves integer solutions of the generalized Fermat equation $ax^p + by^q + cz^r = 0$. We concentrate here on details associated to the third step and give examples where the field discriminants have the form $\pm 2^a 3^b$.

Contents

1. Introduction

Let S be a finite set of primes and let G be a finite group. Let $NF(S, G)$ be the set of Galois number fields $K \subset \mathbb{C}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ and discriminant divisible only by primes in S. The sets $NF(S, G)$ are finite, by a classical theorem of Hermite.

We are interested in the following inverse Galois problem. *For given S and G, find defining polynomials $f(x) \in \mathbb{Q}[x]$ for as many fields in $NF(S, G)$ as possible.* This problem is most interesting when $|NF(S, G)|$ can be expected to be small, so that one can reasonably aim for complete lists. Thus we are interested in "collecting

number fields," the most valuable specimens being those which are least ramified, for a given Galois group G.

In this paper we consider only cases with $S = \{2, 3\}$. If G has a faithful permutation representation of degree ≤ 7, we have completely identified $NF(S, G)$ previously with Jones [**JR1**], [**JR3**]. Here we supplement these complete lists with lists of fields with larger groups G, involving the simple groups $PSL_2(9)$, $SL_2(8)$, $SL_3(3)$, $SU_3(3)$, A_8, $W(E_6)'$, A_9, $W(E_7)'$, and A_{32}.

We construct all our fields by specializing three point covers. Our requirement that the field discriminant be of the form $\pm 2^a 3^b$ is extremely restrictive. In the main, it restricts consideration to three point covers with bad reduction at 2 and 3 only. To keep ramification within $\{2, 3\}$, the specialization point has to be chosen judiciously as well. Throughout, our computations are done in *Mathematica*, supplemented by the *nfdisc*, *factorpadic*, *polredabs*, and *nfisisom* commands of *Pari*.

Our title refers to the three step procedure we go through in order to produce our final polynomials $f(x)$. Each step centers on an ABC-equation, these equations being (1.1), (1.4), and (1.5).

First, the general ABC construction makes use of Katz's theory of rigid local systems [**Kat**]. This theory associates a rigid local system to a rigid solution of the matrix equation

$$ABC = 1. \tag{1.1}$$

There are motivic aspects to Katz's theory which arise when one works with characteristic zero coefficients, as we will briefly discuss at the end of this introduction. But for the ABC construction itself, we take A, B, C in some $GL_n(\bar{\mathbb{F}}_\ell)$. Rigid means that the group $\tilde{M}$ generated by A, B and C acts irreducibly on $\bar{\mathbb{F}}_\ell^n$ and that the centralizer dimensions of A, B, and C sum to the largest possible number compatible with irreducibility, namely $n^2 + 2$. Katz's theory says that if the primes dividing the orders of A, B, and C are all in S, and also the coefficient characteristic ℓ is in S, then the associated local system is guaranteed to have its bad reduction entirely in S too. So the role of this first step is to point us to three point covers guaranteed to be ramified within S. The hypergeometric family of solutions to (1.1) given in (1.6)-(1.8) suffices to cover all our examples in this paper, and so we will not be making much explicit reference to this first step.

Second, the three point covers we present in Sections 5-12 are mostly of the form $F : \mathbb{P}^1_x \to \mathbb{P}^1_t$. Here the subscripts distinguish different copies of the projective line by the coordinate we are using. So $\mathbb{P}^1_x$ has function field $\mathbb{Q}(x)$ while $\mathbb{P}^1_t$ has function field $\mathbb{Q}(t)$. We give F by an equation $t = -A(x)/C(x)$ with $A(x) \in \mathbb{Z}[x]$ of degree N and $C(x) \in \mathbb{Z}[x]$ of degree $\leq N$. If we write

$$f(t, x) = A(x) + tC(x) \tag{1.2}$$

then the discriminant with respect to x has the form

$$D(t) = \pm 2^A 3^B t^{e_0} (t - 1)^{e_1}. \tag{1.3}$$

The simple way that t appears here reflects the fact that F ramifies only over 0, 1, and ∞, i.e. F is a three point cover. The form of the numerical coefficient reflects the fact that the bad reduction set of the cover is exactly $\{2, 3\}$. These covers are calculated from extremal relatively prime solutions to the polynomial equation

$$A(x) + B(x) + C(x) = 0. \tag{1.4}$$

Here extremal means that the total number of roots of $A(x)$, $B(x)$, and $C(x)$ in $\mathbb{P}^1_x$, not counting multiplicities, is as small as possible, namely $N+2$. In contrast, the total number of roots, counting multiplicities, is $3N$. The nature of the multiplicities is determined in a group-theoretic way from the given solution to (1.1). If the group generated by A, B, C is $\tilde{M}$ with center Z, the cover we seek has monodromy group $M = \tilde{M}/Z$. Here we are modding out by centers because the essence of the situation is maintained in a computationally simpler context: once one has a cover $X = \mathbb{P}^1_x$ corresponding to M, it is typically easy to take the appropriate abelian cover $\tilde{X}$ of X corresponding to $\tilde{M}$. For roughly half of our examples, the instance of (1.4) we need to solve has already been solved in the literature. For the other half, we find the solution by standard techniques. So we will not say too much more about this second step either.

Third, we specialize the three point covers. We view (1.2) as a family of separable polynomials $f(\tau, x) \in \mathbb{Q}[x]$ indexed by $\tau \in \mathbb{Q} - \{0, 1\}$. Let K_τ be the splitting field of $f(\tau, x)$ in $\mathbb{C}$. To keep the discriminant of K_τ divisible by 2 and 3 only, we consider the generalized Fermat equation

$$ax^p + by^q + cz^r = 0. \tag{1.5}$$

Here p, q, and r are given positive integers, giving the order of local monodromy about the cusps 0, 1, and ∞ respectively in (1.2). We look for integer solutions of (1.5) with relatively prime terms and with a, b, and c divisible by 2 and 3 only. From each solution, we take $\tau = -ax^p/cz^r$ as our specialization point. It is this third step, and various issues associated with it, that we will concentrate on in this paper. It is the most purely number-theoretical of the three steps.

Of course, there are very substantial differences between the three steps, despite the formal similarity between the central ABC equations. Of the three equations, the matrix equation (1.1) has the most powerful theory associated to it. There is a hypergeometric family of solutions, treated in depth in [**BH**]. There are also infinitely many other non-classical but similar families, introduced in [**Kat**] and discussed further in [**Rob2**]. The hypergeometric family of solutions goes as follows. Let $u(x)$ and $w(x)$ be relatively prime degree n polynomials in $\bar{\mathbb{F}}_\ell[x]$ with non-zero constant terms. Put

$$A = m_u \tag{1.6}$$

$$B = m_u^{-1} m_w \tag{1.7}$$

$$C = m_w^{-1}, \tag{1.8}$$

where m_p indicates the companion matrix of p, as illustrated by (8.1). Then (A, B, C) is a rigid solution of (1.1), as one has irreducibility and A, B, and C have centralizer dimension dimension n, $n^2 - 2n + 2$, and n respectively. More precisely with respect to B, one has

$$\det(B) = \det(A)^{-1} \det(C)^{-1} = u(0)^{-1} w(0).$$

If $\det(B) \neq 1$, then B is conjugate to a diagonal matrix with diagonal entries 1, $\ldots$, 1, $\det(B)$. If $\det(B) = 1$, then B is conjugate to a matrix with diagonal entries 1, the 1-2 entry also 1, and all other entries zero.

From a practical point of view, the polynomial equation (1.4) is the most problematic. We have formulated things so far in terms of $F : \mathbb{P}^1_x \to \mathbb{P}^1_t$, but the general situation is $F : X \to \mathbb{P}^1_t$ with X a curve of arbitrary genus. In fact, consider a rigid

solution (A, B, C) to (1.1) generating $\tilde{M} \subset GL_n(\bar{\mathbb{F}}_\ell)$ with center Z. Choose a faithful transitive permutation representation of $M = \tilde{M}/Z$ into some symmetric group S_N. Then A, B, and C each determine a partition of N. Write the total number of parts as $N + 2 - 2g$. Then g is a nonnegative integer. The general polynomial ABC equation then takes place in the function field $\mathbb{Q}(X)$ of an unspecified curve of genus g, as one looks for three divisors of degree N, supported at altogether $N + 2 - 2g$ points, and a function $F \in \mathbb{Q}(X)$, with the three divisors being the zero locus of F, the zero locus of $F - 1$, and the polar locus of F. This positive genus case, in other words the great mass of the cases, presents computational problems which at present are usually insurmountable.

While we do not apply any theory to the integer equation (1.5), from our point of view it presents no problem at all. We simply carry out a computer search to find some solutions of the sort we need. Finding all the solutions, and proving that there are no more, are entirely other issues, both wrapped up with the ABC conjecture.

Section 2 provides an overview of the fields constructed in this paper. Our main theorem is stated there; it says how many fields in $NF(\{2, 3\}, G)$ we construct in this paper for the various G we consider. Sections 3 and 4 discuss three point covers and especially specialization. Sections 5-12 discuss the individual constructions, sorted approximately by $|G|$. In each case, we describe in some detail what happens in the specialization step, i.e. Step 3 of the ABC construction. Each of these sections also discusses a more theoretical issue, as indicated by the section titles.

As stated above, we will be saying very little about Steps 1 and 2 of the ABC construction. As to Step 1, our covers 6, $9a$, $10a$, $13a$, $13b$, $27a$, $27b$, $27c$, N_m, and $28b$ all come directly from a hypergeometric solution to (1.1). We will just write down a $(u(x), w(x))$ giving this connection via (1.6)-(1.8); there are sometimes quite different pairs $(u(x), w(x))$ which would also work. Our covers $10b$, $9b$, $26c$, $28a$, and $27d$ come indirectly from a hypergeometric solution to (1.1), via a base change. We display equations indicating how these base changes go, and describe in §8 the case of $28a$ in more detail as an example, the other cases being similar. Some of our covers also come from non-hypergeometric solutions to (1.1), but we will not enter into these connections at all, save for some comments on $27d$. The coefficient characteristic is $\ell = 3$ in Sections 5, 7, 8 and we use $\mathbb{F}_9 = \mathbb{F}_3[i]$ with $i^2 = -1$, taking $\rho = 1 + i$ as our standard generator of $\mathbb{F}_9^\times$. The coefficient characteristic is $\ell = 2$ in Section 6 and we use models of $\mathbb{F}_8$ and $\mathbb{F}_{64}$ introduced there. In Sections 9-12 the coefficient characteristic can be generally taken to be either $\ell = 2$ or $\ell = 3$, as A, B, and C defined by (1.6)-(1.8) generate a finite group even when one takes $\mathbb{Q}$ as the coefficient field. This finiteness even in characteristic zero is a very unusual situation, and in this sense Sections 5-8 represent the general case better than Sections 9-12 do. As to Step 2, we will limit ourselves to a brief general discussion in §5, and a few comments about the new covers.

Throughout this paper, we work as much as possible in the setting of algebraic number theory. However the reader should realize that a systematic study of the sets $NF(S, G)$ would fundamentally involve both the theory of motives and the theory of automorphic representations. Our ABC construction is on the motivic side, as Katz's theory from which we begin is motivic in nature, as mentioned before. In fact, via rigid characteristic zero solutions to (1.1), all our $f(t, x)$ can be thought of as generalizations of classical division polynomials $f_m(t, x)$ associated

to the m-torsion points of the elliptic curve

$$y^2 = (t-1)x^3 - 3tx + 2t$$

with J-invariant $1728t$. A great advance would be to bypass the computational techniques from general three point covers and somehow use the motivic theory to directly calculate $f(t,x)$, just as the classical division polynomials $f_m(t,x)$ can be calculated for all m by explicit recursion relations [**McK**].

On the automorphic side, when G is solvable, the sets $NF(S,G)$ are in principle accessible by abelian class field theory. For groups embeddable into some $GL_2(\overline{\mathbb{F}}_\ell)$, Serre's conjecture applies [**Ser2**]. Extending Serre's conjecture, Ash and Gross both have conjectural Langlands-type non-abelian class field theory for quite general groups [**Ash**], [**Gro**]. Gross's theory predicts in particular that for a given prime p, $NF(\{p\},G)$ is non-empty for suitable non-solvable G. For example, it is predicted that $NF(\{5\},G_2(5))$ is non-empty. The fields we produce in this paper seem good candidates for comparison with automorphic forms.

2. Summary of fields constructed

To keep our investigation of manageable size, we focus attention on groups G of the form $H.A$, where H is non-abelian simple and the natural map $A \to \mathrm{Out}(H)$ is injective. In passing, however, we construct interesting fields for G not in this class. For example, in Sections 5-9, some interesting solvable fields appear. Also, in Section 6 some G involving two copies of $SL_2(8)$ appear, and many other such $H^n.A$ could be constructed just by specializing at non-rational points τ. Also, related to the distinction between $\tilde{M}$ and M, many of our covers have natural lifts; for example, Cover $27d$ in Section 9 with Galois group $W(E_6)$ has a natural lift to a cover with Galois group $2.W(E_6)$.

Table 2.1 lists some groups G of the form $H.A$. Groups G are placed in the same block iff they have the same H. We give a characteristic 0 description, a characteristic 2 description, and/or a characteristic 3 description. The Atlas [**Atlas**] sometimes gives even more descriptions, e.g. $SL_3(2).2 \cong PGL_2(7)$. The column N gives the degree of a minimal faithful permutation representation.

An entry under $\#_G$ of the form $\bullet x$ summarizes results from [**JR1**] and [**JR3**]. In this case, $|NF(\{2,3\},G)| = x$. The complete search for $GL_3(2)/A_7/S_7$ fields took thirteen hours, but we estimate an analogous complete search for $GL_3(2).2/A_8/S_8$ fields would take somewhere around ten thousand years [**JR2**]. This is why we are shifting attention to non-exhaustive but still systematic ways of constructing fields in a given $NF(S,G)$.

The main focus of the present paper is the following theorem.

THEOREM 2.1. *For $G = M_{10}$, $PGL_2(9)$, $P\Gamma L_2(9)$, $SL_2(8)$, $\Sigma L_2(8)$, $SL_3(3)$, $SL_3(3).2$, $G_2(2)'$, $G_2(2)$, S_8, $PSp_4(3)$, $SO_5(3)$, A_9, S_9, $Sp_6(2)$, and S_{32}, the polynomials presented in Section 5-12 give $\#_G$ elements of $NF(\{2,3\},G)$, with $\#_G$ as on Table 2.1.*

In general, suppose given separable polynomials $f_i \in \mathbb{Q}[x]$, which one expects have distinct splitting fields K_i in some $NF(S,G)$. After a variable change, one can assume all the f_i are monic polynomials in $\mathbb{Z}[x]$. To prove that the K_i are in $NF(S,G)$ and distinct one has to do three things:

1. Verify that the ramification set S_i of K_i is really in S. Let $L_i = \mathbb{Q}[x]/f_i(x)$. Let D_i be the polynomial discriminant f_i and let d_i be the field discriminant of L_i.

TABLE 2.1. Lower bounds for $|NF(\{2,3\},G)|$.

$\lvert G\rvert$	0	2	3	N	$\#_G$	§
$60 = 2^2 3\,5$	A_5	$SL_2(4)$		5	•0	
$120 = 2^3 3\,5$	S_5	$\Sigma L_2(4)$		5	•5	
$168 = 2^3 3\,7$		$SL_3(2)$		7	•0	
$336 = 2^4 3\,7$		$SL_3(2).2$		8		
$360 = 2^3 3^2 5$	A_6	$Sp_4(2)'$	$PSL_2(9)$	6	•4	
$720 = 2^4 3^2 5$	S_6	$Sp_4(2)$	$PGO_4^-(3)$	6	•27	
$720 = 2^4 3^2 5$			$PGL_2(9)$	10	4	5
$720 = 2^4 3^2 5$	M_{10}			10	15	5
$1,440 = 2^5 3^2 5$			$P\Gamma L_2(9)$	10	79	5
$504 = 2^6 3^2 7$		$SL_2(8)$		9	3	6
$1,512 = 2^6 3^3 7$		$\Sigma L_2(8)$		9	64	6
$2,520 = 2^3 3^2 5\,7$	A_7			7	•0	
$5,040 = 2^4 3^2 5\,7$	S_7			7	•10	
$5,616 = 2^4 3^3 13$			$SL_3(3)$	13	6	7
$11,232 = 2^5 3^3 13$			$SL_3(3).2$	26	85	7
$6,048 = 2^5 3^3 7$		$G_2(2)'$	$SU_3(3)$	28	1	8
$12,096 = 2^6 3^3 7$		$G_2(2)$	$SU_3(3).2$	28	41	8
$20,160 = 2^6 3^2 5\,7$	A_8	$GL_4(2)$		8		
$40,320 = 2^7 3^2 5\,7$	S_8	$SO_6^+(2)$		8	2	11, 12
$25,920 = 2^6 3^4 5$	$W(E_6)'$	$SU_4(2)$	$PSp_4(3)$	27	21	9
$51,840 = 2^7 3^4 5$	$W(E_6)$	$SO_6^-(2)$	$SO_5(3)$	27	124	9
$181,440 = 2^6 3^4 5\,7$	A_9			9	10	10
$362,880 = 2^7 3^4 5\,7$	S_9			9	26	10, 12
$1,451,520 = 2^9 3^4 5\,7$	$W(E_7)'$	$Sp_6(2)$		28	34	11
$2.63\times 10^{35} \approx 32!$	S_{32}			32	1	12

One has to show that the $p \notin S$ dividing D_i do not divide d_i. This may require substantial computation in general, but in the setting of three point covers we do it uniformly without computation by (3.4).

2. Verify that the Galois group $G_i := \mathrm{Gal}(K_i/\mathbb{Q})$ is indeed isomorphic to G. One can very easily compute lower bounds by means of Frobenius elements; we briefly indicate how this goes in Section 5, and then give no more details. On a heuristic level, one can expect that the lower bound obtained after moderate computation is always exact. On a rigorous level, to get upper bounds may require very substantial computation, like those we carry out for related purposes in Sections 9 and 11. In the setting of three point covers, we get the needed upper bounds uniformly without computation from (3.2).

3. Verify that the K_i are distinct. Often the group G has up to isomorphism exactly one faithful permutation representation of a given degree N, and all given defining polynomials f_i have degree N. In this case, for each pair $i \neq i'$ one needs to find a prime p, not dividing $D_i D_{i'}$, for which the factorization partitions of f_i and $f_{i'}$ over $\mathbb{F}_p$ are distinct. In general the situation may be very slightly more complicated, for example by sextic twinning in Section 5 and projective twinning

in Section 7. But even here, one needs to just find p such that the factorization partitions come from elements of different orders in the symmetric group S_N. We have done this, but do not present any details here.

In the rest of the paper we complete the statement of Theorem 2.1 by presenting the defining equations. The proof of Theorem 2.1 is completed simultaneously, since, as we have just explained, the theorem is essentially self-proving from its full statement. Of course, it would be pointless to restrict ourselves only to establishing those facts literally contributing to Theorem 2.1. Rather, we present a fuller picture of both our particular examples and the general technique of constructing fields in a given $NF(S, G)$ by means of specializing three point covers.

Jones has run modest computer searches which have found an A_8 field and some more S_8 fields ramified at 2 and 3 only. From looking at mod ℓ Galois representations of various curves, we know also that there are more fields for $PGL_2(9)$, $SL_2(8)$, $SU_3(3).2$ and $SO_5(3)$ than listed here.

In [**JR1**], we analyzed the local behavior at 2 and 3 of low degree fields in complete detail. In particular, all $5 + 4 + 27$ fields on the top lines of Table 2.1 are wildly ramified at both 2 and 3, mostly very wildly ramified, as explained in Section 3.3 there. Similarly, all 10 S_7 fields are wildly ramified at both 2 and 3, as explained in [**JR3**]. In contrast, four of the fields here are wildly ramified at only one of these two primes; see (5.1), (6.1), (6.2) and (9.5). One can't have tame ramification at both primes, as a Galois field K with discriminant $\pm 2^a 3^b$ and tame ramification only has root discriminant < 6. Odlyzko's bounds [**Odl**], even the unconditional ones, then force $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{-3})$.

3. Three point covers and specialization

Let F be a field and work with smooth projective curves over the fixed projective line $\mathbb{P}^1_F = \mathrm{Spec}(F[t]) \cup \{\infty\}$. A three point cover over F is a finite separable cover $X \to \mathbb{P}^1_F$, ramified only above the three points 0, 1, and ∞. A defining polynomial for X is a polynomial $f(t, x)$ with $F(X) = F(t)[x]/f(t, x)$. An important issue extensively addressed in the literature is how one explicitly constructs defining polynomials; throughout this paper, we mainly take the defining polynomials simply as given, and the bulk of this section is devoted to setting up notation. Standard references for three point covers include the books [**Mat**], [**MM**], [**Ser1**], [**Sch**], and [**Völ**].

We need first some notation with respect to the universal base curve. Let $T = \mathrm{Spec}(\mathbb{Z}[t, 1/t, 1/(t-1)])$ be the thrice-punctured projective line, so that for any field F, $T(F) = F - \{0, 1\}$. The topological space $T(\mathbb{C})$ plays a central role. We work with the fundamental group

$$\pi_1 := \pi_1(T(\mathbb{C}), 1/2) = \langle \gamma_0, \gamma_1, \gamma_\infty | \gamma_0\gamma_1\gamma_\infty = 1 \rangle.$$

Here γ_0 and γ_1 come from the counterclockwise circle with radius $1/2$ centered at 0 and 1 respectively. The group π_1 is free on the two generators γ_0 and γ_1. The third element $\gamma_\infty := (\gamma_0\gamma_1)^{-1}$ is introduced so as to treat the three cusps in the same way.

To keep control of Galois groups even when specializing, it is convenient to "remove from $T(\mathbb{C})$ the segments $(-\infty, 0) - i\epsilon$ and $(1, \infty) - i\epsilon$ with ϵ a positive infinitesimal." What this really means is that we define $T(\mathbb{C})^{\mathrm{cut}}$ to be the point set $T(\mathbb{C}) = \mathbb{C} - \{0, 1\}$ with a stronger topology. The open sets are generated by

finite intersections and arbitrary unions from the standard ones together with the new open set consisting of $\{t \in \mathbb{C} : \mathrm{Im}(t) \geq 0\} - [0,1]$. So $T(\mathbb{C})^{\mathrm{cut}}$, unlike $T(\mathbb{C})$, is simply connected; one can think of it as a spread out version of the base point $1/2$.

A simple partition of $T(\mathbb{Q}_p)$ into subregions plays a fundamental role in the analysis of ramification. For $\tau \in T(\mathbb{Q}_p)$, write $\tau = -A/C$ with $A, C \in \mathbb{Z}_p$ not both divisible by p. Define $B \in \mathbb{Z}_p$ by $A + B + C = 0$. Define

$$\begin{aligned} \mathrm{ord}_0(\tau) &:= \mathrm{ord}_p(A) \\ \mathrm{ord}_1(\tau) &:= \mathrm{ord}_p(B) \\ \mathrm{ord}_\infty(\tau) &:= \mathrm{ord}_p(C). \end{aligned}$$

The partition is

$$T(\mathbb{Q}_p) = T(\mathbb{Q}_p)^{\mathrm{gen}} \coprod \left(\coprod_{i=1}^{\infty} T(\mathbb{Q}_p)^{0,i} \right) \coprod \left(\coprod_{i=1}^{\infty} T(\mathbb{Q}_p)^{1,i} \right) \coprod \left(\coprod_{i=1}^{\infty} T(\mathbb{Q}_p)^{\infty,i} \right).$$

Here ord_c takes the value i exactly on $T(\mathbb{Q}_p)^{c,i}$; so for c fixed and i increasing, the $T(\mathbb{Q}_p)^{c,i}$ are smaller and smaller annuli, all centered at the cusp c. The generic piece, empty for $p = 2$, is where all three ord_c take the value 0.

For the rest of this section, a degree N three point cover $X \to \mathbb{P}^1_F$ is fixed. A particular defining polynomial $f(t,x)$ is fixed too. Objects Δ, a, b, $c(t)$, and Σ below depend on f. Otherwise the objects M, G, ... depend only on X. We will use this notation systematically in the sequel, with indices when discussing particular examples. For example, once we have denoted a particular cover X_{27d}, automatically M_{27d} denotes its monodromy group.

The polynomial discriminant of $f(t,x)$, with respect to the variable x, factors uniquely as

$$D(t) = \Delta t^a (t-1)^b c(t)^2, \tag{3.1}$$

with $c(t) \in F[t]$ monic and prime to $t(t-1)$. Here $\Delta \in F^\times$ and a and b are integers. Let Σ be the subvariety of $\mathbb{P}^1_F$ corresponding to the roots of $c(t)$. Switching to a different defining polynomial $f^*(t,x)$ typically makes the corresponding $c^*(t)$ relatively prime to $c(t)$. So the factor $c(t)^2$ plays essentially no role in our situation; actually $c(t)$ is identically 1 in most of our examples.

For τ in $F - \{0,1\}$, let $X_\tau = \mathrm{Spec}(L_\tau)$ be the corresponding fiber. So $L_\tau = F(X_\tau)$ is a finite separable algebra over F. For $\tau \notin \Sigma(F)$, $L_\tau = F[x]/f(\tau,x)$; so in this case, L_τ is a field iff $f(\tau,x)$ is irreducible.

Suppose henceforth that $F \subseteq \mathbb{C}$. Let $X(\mathbb{C})^{\mathrm{cut}}$ be the inverse image of $T(\mathbb{C})^{\mathrm{cut}}$ in $X(\mathbb{C})$. Let C be set of components of $X(\mathbb{C})^{\mathrm{cut}}$, i.e. $C = \pi_0(X(\mathbb{C})^{\mathrm{cut}})$. So C has N components and the group π_1 acts naturally on C. The image of π_1 in the symmetric group $\mathrm{Sym}(C)$ is called the monodromy group M. For $c \in \{0, 1, \infty\}$, the image of γ_c in M is denoted m_c; its order is denoted e_c.

Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Suppose henceforth that $F \subseteq \bar{\mathbb{Q}}$; this is the essential case anyway. For $\tau \in F - \{0,1\}$, the branch cuts let us canonically identify the fiber $X_\tau(\mathbb{C})$ with the component set C; we use this identification without comment in the sequel. But also $X_\tau(\mathbb{C})$ is identified with the set of homomorphisms $\mathrm{Hom}(L_\tau, \bar{\mathbb{Q}})$; for $\tau \notin \Sigma(F)$, $X_\tau(\mathbb{C})$ is identified with the set of roots $X_\tau(\mathbb{C}) \subset \bar{\mathbb{Q}}$ of $f(\tau,x)$. Either way, one sees a natural action of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ on $X_\tau(\mathbb{C}) = X_\tau(\bar{\mathbb{Q}})$. The image of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ in the symmetric group $\mathrm{Sym}(C)$ is the Galois group G_τ.

Let M^* be the normalizer of M in the symmetric group $\mathrm{Sym}(C)$. A basic fact is that

$$\text{each } G_\tau \text{ is contained in } M^*. \tag{3.2}$$

Another basic fact is that all the biggest G_τ coincide, and we call this common group the Galois group G.

Suppose now that $F \subset \bar{\mathbb{Q}}$ is a number field of degree d. Then one has d conjugate covers $X^\delta \to F^\delta$. Restricting scalars, one gets a single cover of degree dN over the field $\mathbb{Q}$. On the level of defining polynomials, this operation of restricting scalars is the passage from $f(t,x) \in F[t,x]$ to $\prod f^\delta(t,x) \in \mathbb{Q}[t,x]$. Since our object is to construct Galois extensions of $\mathbb{Q}$, this is a natural thing for us to do; in the rest of this section, we take $F = \mathbb{Q}$.

Let K_τ be the splitting field in $\mathbb{C}$ of L_τ. So if $\tau \notin \Sigma(\mathbb{Q})$, K_τ is the field generated by the roots of $f(\tau, x)$ in $\mathbb{C}$. The fields K_τ are the fields which we emphasized in Sections 1 and 2; we have set things up so that $G_\tau = \mathrm{Gal}(K_\tau/\mathbb{Q})$. On the other hand, for most of this paper we focus on the degree N algebras L_τ which arise naturally and are computationally more accessible. Thus, for example, we sometimes give the algebra discriminant of L_τ, as computed by *nfdisc*. Determining the discriminant of K_τ would be much harder.

Let S be the set of primes at which the cover $X \to \mathbb{P}^1_{\mathbb{Q}}$ has bad reduction. Always S contains all primes dividing $e_0 e_1 e_\infty$. Always S is contained in the primes dividing numerator or denominator of Δ. By adjusting the defining equation, one can always make S exactly the primes dividing numerator or denominator of Δ.

A basic fact is that all the fields K_τ are tamely ramified outside S. To be more precise, recall that for a Galois number field $K \subset \mathbb{C}$, tamely ramified at p, one has a conjugacy class r_p in $\mathrm{Gal}(K/\mathbb{Q})$, measuring the ramification at p. In our case, for $p \notin S$, one has an explicit formula for the ramification class $r_{\tau,p}$ as a conjugacy class in $G \supseteq G_\tau$:

$$r_{\tau,p} = \begin{cases} [1] & \text{if } \tau \in T(\mathbb{Q}_p)^{\mathrm{gen}} \\ [m_c^i] & \text{if } \tau \in T(\mathbb{Q}_p)^{c,i}. \end{cases} \tag{3.3}$$

Thus L_τ is unramified at p iff $\tau \in T(\mathbb{Q}_p)^{\mathrm{gen}}$ or $\tau \in T(\mathbb{Q}_p)^{c,i}$ with $m_c^i = 1$. Also

$$\text{if } \tau \in T(\mathbb{Q}_p)^{c,i} \text{ then } \mathrm{ord}_p(\mathrm{disc}(L_\tau)) = N - |C/m_c^i|, \tag{3.4}$$

the last term being the number of orbits of m_c^i on the component set C.

4. Specialization lists for $S = \{2, 3\}$

Let p, q, and r be positive integers or ∞. Let S be a finite set of primes. Define $T_{p,q,r}(\mathbb{Z}^S)$ to be the set of those rational numbers $\tau \in \mathbb{Q} - \{0, 1\}$ such that

$$\tau \in T(\mathbb{Q}_p)^{\mathrm{gen}} \coprod \left(\coprod_{i=1}^{\infty} T(\mathbb{Q}_p)^{0,pi} \right) \coprod \left(\coprod_{i=1}^{\infty} T(\mathbb{Q}_p)^{1,qi} \right) \coprod \left(\coprod_{i=1}^{\infty} T(\mathbb{Q}_p)^{\infty,ri} \right)$$

for all p not in S. Here if an index is ∞, then the corresponding cuspidal summand is by definition empty.

Explicitly, and without reference to p-adic numbers, a rational number τ is in $T_{p,q,r}(\mathbb{Z}^S)$ iff there exist integers a, b, c, x, y, z as follows: a, b, and c are divisible

only by primes in S;

$$\begin{aligned} \tau &= -\frac{ax^p}{cz^r}\ ; \\ ax^p + by^q + cz^r &= 0. \end{aligned}$$

The six-tuple (a, b, c, x, y, z) is then uniquely determined under the following auxiliary normalization conditions: x, y, and z are divisible only by primes not in S; $A = ax^p$, $B = by^q$, and $C = cz^r$ are relatively prime; x, y, and z are positive; two of A, B, and C are positive. In short, identifying $T_{p,q,r}(\mathbb{Z}^S)$ requires finding the solutions of the generalized Fermat equation.

TABLE 4.2. The 56 S_3-orbits of $T_h(\mathbb{Z}^{\{2,3\}})$ needed for $T_{2,3,\infty}(\mathbb{Z}^{\{2,3\}})$

$a{\cdot}x^p$	$b{\cdot}y^q$	$c{\cdot}1$
1	1	$-2{\cdot}1$
$2{\cdot}1$	1	$-3{\cdot}1$
$3{\cdot}1$	1	$-2^2{\cdot}1$
$2^3{\cdot}1$	1	$-3^2{\cdot}1$
$3{\cdot}1$	5^3	$-2^7{\cdot}1$
-5^2	$2^4{\cdot}1$	$3^2{\cdot}1$
-5^2	$2^3 3{\cdot}1$	1
5^2	$2{\cdot}1$	$-3^3{\cdot}1$
-7^2	$2^4 3{\cdot}1$	1
7^2	$2^5{\cdot}1$	$-3^4{\cdot}1$
$2{\cdot}11^2$	1	$-3^5{\cdot}1$
-17^2	$2^5 3^2{\cdot}1$	1
-131^2	5^6	$2^9 3{\cdot}1$
$2{\cdot}5^4$	-11^3	$3^4{\cdot}1$
$2{\cdot}7^2$	-5^3	$3^3{\cdot}1$
11^2	-5^3	$2^2{\cdot}1$
13^2	$-2{\cdot}5^3$	$3^4{\cdot}1$
$2^2{\cdot}5^2$	-7^3	$3^5{\cdot}1$
17^2	-7^3	$2\cdot 3^3{\cdot}1$
-19^2	7^3	$2\cdot 3^2{\cdot}1$
19^2	5^3	$-2\cdot 3^5{\cdot}1$
13^2	7^3	$-2^9{\cdot}1$
$3^3{\cdot}7^2$	-11^3	$2^3{\cdot}1$
37^2	$-2^2{\cdot}7^3$	$3{\cdot}1$
$-3{\cdot}23^2$	11^3	$2^8{\cdot}1$
35^2	-13^3	$2^2 3^5{\cdot}1$
$2^2{\cdot}23^2$	-13^3	$3^4{\cdot}1$
-47^2	13^3	$2^2 3{\cdot}1$

$a{\cdot}x^2$	$b{\cdot}y^3$	$c{\cdot}1$
$-2^3{\cdot}17^2$	5^3	$3^7{\cdot}1$
59^2	$-3{\cdot}11^3$	$2^9{\cdot}1$
61^2	$3{\cdot}5^3$	$-2^{12}{\cdot}1$
-71^2	17^3	$2^7{\cdot}1$
$-2^3 3^2{\cdot}13^2$	23^3	1
11^2	23^3	$-2^{12}3{\cdot}1$
73^2	23^3	$-2^3 3^7{\cdot}1$
143^2	$-3{\cdot}19^3$	$2^7{\cdot}1$
$2^3{\cdot}73^2$	-35^3	$3^5{\cdot}1$
107^2	$-3^2{\cdot}17^3$	$2^{15}{\cdot}1$
-215^2	19^3	$2\cdot 3^9{\cdot}1$
-253^2	$2^9{\cdot}5^3$	$3^2{\cdot}1$
-359^2	$3{\cdot}35^3$	$2^8{\cdot}1$
545^2	$-2{\cdot}53^3$	$3^6{\cdot}1$
595^2	-73^3	$2^4 3^7{\cdot}1$
$-3{\cdot}389^2$	$2{\cdot}61^3$	1
-827^2	73^3	$2^{15}3^2{\cdot}1$
955^2	-97^3	$2^3 3^4{\cdot}1$
1871^2	$-3^2{\cdot}73^3$	$2^9{\cdot}1$
2359^2	47^3	$-2^5 3^{11}{\cdot}1$
2681^2	-193^3	$2^4 3^4{\cdot}1$
$-2{\cdot}2761^2$	239^3	$3^{13}{\cdot}1$
8549^2	$-3^5{\cdot}67^3$	$2^3{\cdot}1$
-23053^2	505^3	$2^{27}3{\cdot}1$
$2{\cdot}21395^2$	-971^3	$3^8{\cdot}1$
39151^2	-1153^3	$2^5 3^5{\cdot}1$
$-3{\cdot}48383^2$	1915^3	$2^{13}{\cdot}1$
$-2{\cdot}184211^2$	4079^3	$3{\cdot}1$

The discussion at the end of Section 3 makes clear why we are interested in the sets $T_{p,q,r}(\mathbb{Z}^S)$. Namely, let $X \to \mathbb{P}^1_{\mathbb{Q}}$ be a three point cover with bad reduction set within S and local monodromy orders $p = e_0$, $q = e_1$, $r = e_\infty$. Then the specialized fields K_τ have bad reduction within S exactly if $\tau \in T_{p,q,r}(\mathbb{Z}^S)$. This important statement is called the Chevalley-Weil theorem for M-curves in [**Dar**].

If $X \to \mathbb{P}^1_{\mathbb{Q}}$ yields $\{p,q,r\}$ with $1/p+1/q+1/r \geq 1$, then the monodromy group M is solvable, except perhaps for some composition factors isomorphic to A_5. Thus we are interested here exclusively in the hyperbolic case

$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1. \tag{4.1}$$

Here the sets $T_{p,q,r}(\mathbb{Z}^S)$ are known to be finite [**DG**], the proof appealing to Faltings' general finiteness theorem for curves.

TABLE 4.3. 45 more S_3-orbits in $T_h(\mathbb{Z}^{\{2,3\}})$

$a{\cdot}x^p$	$b{\cdot}y^q$	$c{\cdot}z^r$
$2^5{\cdot}1$	$-3{\cdot}5^3$	7^3
23^2	-5^4	$2^5 3{\cdot}1$
7^2	-5^4	$2^6 3^2{\cdot}1$
-29^2	5^4	$2^3 3^3{\cdot}1$
47^2	-7^4	$2^6 3{\cdot}1$
$2^5 3{\cdot}5^2$	-7^4	1
-113^2	7^4	$2^7 3^4{\cdot}1$
$-2^2{\cdot}61^2$	11^4	$3^5{\cdot}1$
239^2	$-2{\cdot}13^4$	1
287^2	-17^4	$2^7 3^2{\cdot}1$
$2{\cdot}5861^2$	$-3^2{\cdot}59^4$	7^9
$3^2{\cdot}5^3$	$2^2{\cdot}19^3$	-13^4
-37^3	$2{\cdot}29^3$	$3{\cdot}5^4$
$-2^8{\cdot}7^3$	$3{\cdot}29^3$	11^4
-71^3	23^3	$2^4 3^2{\cdot}7^4$
$-2{\cdot}203^3$	$3^3{\cdot}79^3$	43^4
2293^2	$2{\cdot}67^3$	$-3{\cdot}5^9$
1079^2	$-2^{10}{\cdot}19^3$	$3{\cdot}5^9$
$-3{\cdot}36553^2$	203^3	$2^{11}{\cdot}5^9$
-138743^2	$3{\cdot}1027^3$	$2^{13}{\cdot}5^9$
$2^3 3^2{\cdot}12515^2$	-2797^3	13^9
107567^2	$-3{\cdot}3155^3$	$2^{11}{\cdot}7^9$

$a{\cdot}x^2$	$b{\cdot}y^q$	$c{\cdot}z^8$
$-2{\cdot}3{\cdot}263^2$	29^3	5^8
$-2^2{\cdot}353^2$	$3^4{\cdot}11^3$	5^8
5239^2	$-3^2{\cdot}163^3$	$2{\cdot}7^8$
$-2^5{\cdot}4015^2$	799^3	7^8
26311^2	$2^4 3^2{\cdot}95^3$	-13^8
-32039^2	241^3	$2^5 3^4{\cdot}5^8$
-39313^2	$2{\cdot}767^3$	$3{\cdot}11^8$
31987^2	-1489^3	$2^3 3^6{\cdot}5^8$
36631^2	1679^3	$-2^6 3^5{\cdot}5^8$
-99431^2	$2^3{\cdot}1073^3$	$3^2{\cdot}5^8$
-160975^2	$2^{10}3{\cdot}203^3$	11^8
-185039^2	1633^3	$2^6 3^4{\cdot}7^8$
$2^2{\cdot}774517^2$	-15613^3	$3^8{\cdot}11^8$
-6827035^2	$2{\cdot}28559^3$	$3^3{\cdot}13^8$
9101359^2	-43873^3	$2^7 3^7{\cdot}7^8$
-26615519^2	78913^3	$2^7 3^5{\cdot}17^8$
-30042907^2	$2^3 3^3{\cdot}16037^3$	43^8
$2{\cdot}45707519^2$	1171537^3	$-3^5{\cdot}95^8$
$2{\cdot}13^2$	$-3{\cdot}19^4$	5^8
437147^2	-21769^3	$2^9 3^4{\cdot}5^{12}$
1169^2	$2^3 3^4{\cdot}5^4$	-11^6
2591^2	$-3{\cdot}43^4$	$2{\cdot}11^6$
14089^2	-131^4	$2^{11}3{\cdot}5^6$

In the application to specializing three point covers, only cases satisfying the condition

$$\text{all primes dividing } pqr \text{ are in } S \tag{4.2}$$

arise. Accordingly, put

$$T_h(\mathbb{Z}^S) = \bigcup_{(p,q,r)} T_{p,q,r}(\mathbb{Z}^S) \tag{4.3}$$

the union being over (p,q,r) satisfying (4.1) and (4.2). Write $(p,q,r)|(p',q',r')$ iff $p|p'$, $q|q'$, and $r|r'$, with the convention that (any positive integer)$|\infty$. Then

$$T_{p,q,r}(\mathbb{Z}^S) \supseteq T_{p',q',r'}(\mathbb{Z}^S)$$

if $(p,q,r)|(p',q',r')$. Thus (4.3) can be written as a finite union over (p,q,r) minimal with respect to divisibility, and so $T_h(\mathbb{Z}^S)$ is also finite. To avoid confusion, we should mention that it is natural in other contexts to consider a larger set $T_H(\mathbb{Z}^S)$ by letting (p,q,r) on the right side of (4.3) run over triples satisfying (4.1) but not necessarily (4.2). The ABC conjecture would say that each $T_H(\mathbb{Z}^S)$ is finite, but this finiteness is not known. The group $S_3 = \mathrm{Sym}(\{0,1,\infty\})$ acts naturally on the sets $T_h(\mathbb{Z}^S)$ and $T_H(\mathbb{Z}^S)$. If $2 \in S$, one has the three-element orbit $\{-1, 1/2, 2\}$; otherwise all orbits have six elements. A case which has received a lot of attention recently is the case $S = \emptyset$. The corresponding set $T_H(\mathbb{Z})$ is known to contain ten S_3-orbits [**Beu**], and conjectured not to contain any more [**DG**], [**Dar**].

The set $T_{2,3,\infty}(\mathbb{Z}^{\{2,3\}})$ has been completely identified [**Cog**]; it has 81 elements giving rise to 56 S_3-orbits. We have carried out a several-day computer search for more elements of $T_h(\mathbb{Z}^{\{2,3\}})$, with the expectation that each τ found will be involved in the construction of infinitely many essentially distinct number fields K_τ, via our ABC construction. We have found 45 more orbits. Representatives of these 101 orbits are given in Table 4.2 and Table 4.3. The representatives τ on these tables are grouped according to their corresponding $\{p,q,r\}$. Each S_3-orbit is given in terms of a solution to a generalized Fermat equation. For example, the fifth line in the left column of Table 4.2 corresponds to $3 + 5^3 - 2^7 = 0$. The members of the corresponding S_3-orbit are all possible negative quotients of the three terms, i.e. $3/2^7$, $2^7/3$, $5^3/2^7$, $2^7/5^3$, $-3/5^3$, $-5^3/3$.

Our computer search shows that Table 4.3 is complete with respect to solutions with $|ax^p|$, $|bx^q|$, and $|cz^r|$ all $\leq 10^9$. To get larger solutions, we permuted cusps and applied the following base change maps iteratively.

$$\begin{aligned} f_2 : T_{m,m,n}(\mathbb{Z}^S) &\to T_{m,2,2n}(\mathbb{Z}^{S\cup\{2\}}) \\ \tau &\mapsto 4\tau(1-\tau) \\ (A,B,C) &\mapsto (4AB, (2A+C)^2, -C^2) \end{aligned}$$

$$\begin{aligned} f_3 : T_{2n,2,n}(\mathbb{Z}^S) &\to T_{3,2,2n}(\mathbb{Z}^{S\cup\{3\}}) \\ \tau &\mapsto \frac{(4\tau-1)^3}{27\,\tau} \\ (A,B,C) &\mapsto ((4A+C)^3, (8A-C)^2B, -27AC^2) \end{aligned}$$

$$\begin{aligned} f_4 : T_{3n,3,n}(\mathbb{Z}^S) &\to T_{3,2,3n}(\mathbb{Z}^{S\cup\{2\}}) \\ \tau &\mapsto \frac{(9\tau-1)^3(1-\tau)}{64\,\tau} \\ (A,B,C) &\mapsto (B(9A+C)^3, (27A^2+18AC-C^2)^2, 64AC^3). \end{aligned}$$

These maps themselves are three point covers. In fact, f_3 and f_4 describe how the modular curve $X_0(N)$ covers the j-line $X_0(1)$ for $N = 2, 3$.

The base change operations are quite efficient. For example, not using [**Cog**], but rather starting from just $\tau = -2$ corresponding to $2 - 3 + 1 = 0$, one gets 73 of the 101 orbits. Two more examples of low height solutions being transformed to larger height solutions are

$$f_3(3^5,\ -2^2 61^2,\ 11^4) = (-15613^3,\ 2^2 774517^2,\ 3^8 11^8) \tag{4.4}$$

$$f_2(3^3 79^3,\ -2^1 203^3,\ 43^4) = (-2^3 3^3 16037^3,\ 30043907^2,\ -43^8). \tag{4.5}$$

Note that the orbits appearing in (4.4) and the right side of (4.5) are three of the 10 known orbits of $T_H(\mathbb{Z})$. Our list contains four more of these orbits; the remaining three are excluded from our consideration, as they involve the exponent 7 on primes other than 2 and 3.

In the rest of this paper, we abbreviate the part of $T_{p,q,r}(\mathbb{Z}^{\{2,3\}})$ appearing on Tables 4.2 and 4.3 by $T^*_{p,q,r}$. Table 4.4 gives the cardinality of $T^*_{p,q,r}$ in all cases, under the normalization hypothesis $p \le q \le r$. The block on the right illustrates that we are using the bulk of Tables 4.2 and 4.3 in Sections 5-11.

TABLE 4.4. Order of the specialization sets $T^*_{p,q,r}$

		Section:	5	6	7	8	9	10	11
p	q $\quad r$	$\lvert T^*_{p,q,r}\rvert$	A_6	$SL_2(8)$	$SL_3(3)$	$SU_3(3)$	$W(E_6)'$	A_9	$W(E_7)'$
2	3 8	99	f_{10a}						
2	3 9	87		f_{9a}					
2	3 12	82							
2	3 ≥ 16	81		f_{18}					
2	4 6	48							
2	4 8	45			f_{26c}				
2	4 9	45					f_{27d}		
2	4 ≥ 12	44				f_{28a}			
2	6 ≥ 8	36							
2	≥ 8 ≥ 8	35	f_{10b}				f_{27abc}	$f_{9,1}$	f_{28b}
3	3 4	39	f_6						
3	3 ≥ 6	27			f_{13a}				
3	4 ≥ 6	24			f_{13b}				
3	≥ 6 ≥ 6	23							
≥ 4	≥ 4 ≥ 4	21							

5. A_6, S_6, $PGL_2(9)$, M_{10} and $P\Gamma L_2(9)$; basics of computations

In this section, we work with the following three covers, with $\rho = 1 + i \in \mathbb{F}_9$, as explained towards the end of §1.

$$\begin{aligned} u_6 &= (x-1)^2 \\ w_6 &= (x-\rho)(x-\rho^7) = x^2 + ix + 1 \\ \Lambda_6 &= (3A,\ 3B,\ 4A) \to (33,\ 3111,\ 42) \\ f_6(t,x) &= (x^2-2)^3 + t(3x-4)^2 \\ D_6(t) &= 2^{13}3^6t^4(t-1)^2 \end{aligned}$$

$$\begin{aligned} u_{10a} &= (x-1)^3 \\ w_{10a} &= (x+1)(x-\rho)(x-\rho^7) = x^3 + \rho x^2 + \rho x + 1 \\ \Lambda_{10a} &= (3AB,\ 2D,\ 8A) \to (3331, 22222, 811) \\ f_{10a}(t,x) &= (x^3+12x^2+60x+96)^3x + 1728t(3x^2+28x+108) \\ D_{10a}(t) &= -2^{99}3^{42}t^6(t-1)^5 \end{aligned}$$

$$\begin{aligned}
u^s_{10b} &= (x-1)(x-\rho)\\
w^s_{10b} &= (x-\rho^3)(x-\rho^6)\\
\Lambda^s_{10b} &= (8A,4A,8B) \to (811,411,811) \text{ (genus one)}\\
t &= -(s-1)^2/4s\\
\Lambda_{10b} &= (8CD,\ 2BC,\ 8AB) \to (82,22211,811)\\
f_{10b}(t,x) &= x^8(x-3)^2 - 27t(3x^2-2x+3)\\
D_{10b}(t,x) &= 2^{29}3^{42}(t-1)^3t^8.
\end{aligned}$$

The covers in the later sections will be presented in the same format. First, if the cover comes directly from a hypergeometric solution (1.6)-(1.8) to (1.1), we simply give such a solution by giving $u_N(x)$ and $w_N(x)$, as we have done for $N = 6$ and $N = 10a$. There are more lines if the cover comes only indirectly from a hypergeometric solution to (1.1). In the case of $10b$, the hypergeometric solution gives a cover $X^s_{10b} \to \mathbb{P}^1_s$ where X^s_{10b} has genus one. However there is an involution on X^s_{10b} over the involution $s \leftrightarrow 1/s$ on $\mathbb{P}^1_s$. We mod out by these involutions to obtain our cover $X_{10b} = \mathbb{P}^1_x \to \mathbb{P}^1_t$. We consistently reserve the variable t for the base variable in the final three point cover; s and/or u enter as base variables in intermediate three point covers. The intermediate covers, such as $X^s_{10b} \to \mathbb{P}^1_s$ here, drop from consideration as the final covers, such as $X_{10b} \to \mathbb{P}^1_t$, specialize to give more fields. The bulk of a given section discusses specialization, and the connection with the matrix ABC equation (1.1) no longer plays a role; in these discussions, only the last three lines corresponding to each cover enter.

The line beginning Λ_N gives first the conjugacy class $[m_c]$ of m_c in M, in Atlas notation, for $c = 0,\ 1,\ \infty$. When M has non-trivial outer automorphisms, like in cases 6 and $10a$, there may be some ambiguity in how Atlas notation is used; in case $10a$, for example, we could just as well write $8B$ rather than $8A$. The Λ_N line gives next the orbit-partition λ_c of m_c acting on the component set C. All the covers in this paper are rigid, meaning that they are completely determined by the group-theoretical data $([m_0]; [m_1], [m_\infty]; M \subseteq \mathrm{Sym}(C))$. The computation of the defining equation starts from this group-theoretical information.

The component set $C_6 = \pi_0(X_6(\mathbb{C})^{\mathrm{cut}})$ of the cover $X_6 \to \mathbb{P}^1_{\mathbb{Q}}$ has six elements. The monodromy transformations $m_{6,0}$, $m_{6,1}$, and $m_{6,\infty}$ generate the alternating group $M_6 = \mathrm{Alt}(C_6)$. The Galois group G_6 is all of $\mathrm{Sym}(C_6)$. The constant field extension with Galois group G_6/M_6 is $\mathbb{Q}(\sqrt{2})$, as can be seen from considering $D_6(t)$ modulo squares. Similarly, C_{10a} can be identified with a projective line over $\mathbb{F}_9$ so that the monodromy group M_{10a} is $PGL_2(9)$ and the Galois group G_{10a} is $P\Gamma L_2(9)$; the constant field extension is again $\mathbb{Q}(\sqrt{2})$, although this can no longer be seen from $D_{10a}(t)$. In contrast, Cover $10b$ has $M_{10b} = G_{10b} = P\Gamma L_2(9)$.

Except for f_{9a} in Section 6 and the $f^*_{N,m}$ in Section 10, the equations for all our covers have the simple form $f(t,x) = A(x)+tC(x)$. In these cases, x is a coordinate on the covering curve X, identifying it with $\mathbb{P}^1_x$. The cover $X \to \mathbb{P}^1_t$ is given by the rational function $x \mapsto -A(x)/C(x)$. Define $B(x)$ by requiring that the polynomial ABC equation (1.4) hold, i.e. $B(x) = -A(x) - C(x)$. Then the polynomials $A(x)$, $B(x)$, and $C(x)$ factor over $\mathbb{Q}$ according to λ_0, λ_1, and λ_∞. Thus, for example, $f_{10a}(1,x)$ factors as a quintic squared, according to $\lambda_{10a,1} = 22222$. In brief, one determines the coefficients of A and C by imposing some normalization conditions and demanding that B factor in the proper way. For very simple computations of

this form see [**Bir**]; to make the computations feasible in our range of degrees, one has to use the "differentiation trick" described there systematically.

We specialize the cover X_6 at the 39-element set $T^*_{3,3,4}$. The 39 algebras $L_{6,\tau}$ are all of degree six, thus the factor fields all appear in [**JR1**]. The algebra $L_{6,\tau}$ is the twin [**Rob1**] of the algebra $L_{6,1-\tau}$, so that their splitting fields in $\mathbb{C}$ are identical: $K_{6,\tau} = K_{6,1-\tau}$. Since $L_{6,1/2}$ is self-twin, it is forced to be a non-field; in fact, $L_{6,1/2}$ factors as a quintic field L_5 times $\mathbb{Q}$, with L_5 the unique quintic $\{2,3\}$-field with Galois group the Frobenius group F_5.

The 39 specialization points yield 37 isomorphism classes of algebras, the repetitions being $L_{6,2^2 19^3/13^4} \cong L_{6,2^2}$ and $L_{6,3^2 5^3/13^4} \cong L_{6,-3}$. Excluding $L_5 \times \mathbb{Q}$ and counting the repeated fields once, one has 10 S_6 twin pairs and 2 $C_3^2.D_4$ twin pairs. The remaining 6 twin pairs consist of a field and a non-field. Two of these have Galois group S_5, three have Galois group $S_4 \times S_2$, and one has Galois group $S_3 \times S_3$.

In [**JR1**], we found a rather mysterious lack of balance in the 27-element set $NF(\{2,3\}, S_6)$. Namely, if we group these fields, and also those in $NF(\{2,3\}, S_5)$, by their unique quadratic subfields $\mathbb{Q}(\sqrt{d})$, the decomposition is as follows:

$d:$	-6	-3	-2	-1	2	3	6
$NF(\{2,3\}, S_5)$	1	0	0	0	2	1	1
$NF(\{2,3\}, S_6)$	1	1	0	2	13	4	6

In each case, just under half of the fields have discriminant class $d = 2$. So one can view the existence of the cover f_6 as explaining this imbalance; it accounts for both S_5's and 10 of the 13 S_6's.

Next, we specialize the cover X_{10a} at the 99-element set $T^*_{3,2,8}$. There is a tight relation between the covers X_6 and X_{10a}. Namely $f_6(s,x)$, $f_6(1-s,x)$ and $f_{10a}(1-(2s-1)^2,x)$ have the same splitting field over $\mathbb{Q}(s)$. This accounts for the behavior of the nineteen specialization points with $1-\tau \in \mathbb{Q}^{\times 2}$.

Twelve of the elements $\tau \in T^*_{3,2,8}$ satisfy $2(1-\tau) \in \mathbb{Q}^{\times 2}$. By the form of $D_{10a}(t)$, the corresponding G_τ are in the index two subgroup M_{10} of $P\Gamma L_2(9)$. The polynomials $f_{10a}(-23^3,x)$ and $f_{10a}(-799^3/7^8,x)$ each factor as $f_9 f_1$. The field $K_{10a,-23^3}$ is one member of the two-element set $NF(\{2,3\}, C_3^2.C_4)$. The field $K_{10a,-731^3/7^8}$ has Galois group $C_3^2.Q$, with Q being the quaternion group. One knows that $NF(\{2,3\}, Q)$ also has two elements, with defining equations

$$g_\pm(x) = x^8 \pm 12x^6 + 36x^4 \pm 36x^2 + 9.$$

The field K_- is totally real while K_+ is totally imaginary; the quaternionic subfield of $K_{10a,-731^3/7^8}$ is K_+. The remaining ten fields are all distinct, with Galois group M_{10}, and discriminants $2^a 3^b$, $24 \le a \le 34$, $10 \le b \le 18$.

For eight of the remaining sixty-eight τ, the polynomial $f_{10a}(\tau,x)$ factors as $9+1$, namely $\tau = -2^1 61^3$, $-2^1 28559^3/3^3 13^8$, $-239^3/3^{13}$, $-212567^3/3^1 11^8$, $-29^3/5^8$, $2/3^3$, $1171537^3/3^5 95^8$, and $-4079^3/3$. The splitting fields $K_{10a,\tau}$ all have Galois group of the form $C_3^2.B$, with B the Sylow 2 subgroup of $GL_2(3)$; these eight fields are all distinct. The remaining sixty specialization points give 59 fields in $NF(\{2,3\}, P\Gamma L_2(9))$, the unique duplication being $K_{10a,15613^3/3^8 11^8} = K_{10a,5^3/2^2}$, verified by *polredabs*. Note that none of the 59 algebras $L_{10a,\tau}$ are tame at 2, because all of them have $\mathbb{Q}(\sqrt{2})$ in their splitting field. However exactly one is tame at 3, namely

$$L_{10a,11^3/2^3} : x^{10} - 4x^9 + 6x^8 + 24x^2 + 32x + 16, \tag{5.1}$$

with discriminant $-2^{34}3^9$. Note that $f(11^3/2^3, x)$ has relatively large coefficients. The displayed polynomial is obtained from $f(11^3/2^3, x)$ by *polredabs*. We have used *polredabs* analogously below, so as to always display only polynomials with relatively small coefficients.

Next, we specialize X_{10b} at the 35-element set $T^*_{8,2,8} = T^*_{\infty,2,\infty}$. The polynomial $f_{10b}(3^5, x)$ factors into an irreducible nonic and a linear, the nonic defining the same nonic field as the nonic factor of $f_{10a}(-23^3, x)$. Otherwise the Galois fields produced from X_{10b} are distinct from those produced from X_{10a}. The polynomial $f_{10b}(2/3^3, x)$ also factors in the form $9 + 1$; it has splitting field of degree 72 and is tame at 3. The remaining 33 elements of $T^*_{8,2,8}$ give irreducible degree 10 polynomials. The polynomial $f_{10b}(4, x)$ has splitting field the unique field in $NF(\{2, 3\}, S_5)$ containing $\mathbb{Q}(\sqrt{6})$. The remaining thirty-two specialization points give thirty-two distinct fields containing A_6 in their Galois group, one with Galois group A_6, four with Galois group $PGL_2(9)$, five with Galois group M_{10}, two with Galois group S_6, and twenty with Galois group $P\Gamma L_2(9)$. The four with Galois group $PGL_2(9)$ come from $\tau = -8$, -288, -1, and 2. Their corresponding field discriminants are $-2^{33}3^{10}$, $-2^{33}3^{16}$, $-2^{26}3^{12}$, and $2^{33}3^{12}$.

As we discussed in §2, we carried out many computations with Frobenius elements to distinguish fields and get lower bounds on Galois groups. Here are some group-theoretical details for the situation of this section Let $G^\natural$ be the set of conjugacy classes in $G = P\Gamma L_2(9)$. For every $N \in \{10a, 10b\}$, $p \geq 5$ and $\tau \in \mathbb{F}_p - \{0, 1\}$, one has a Frobenius element $\mathrm{Fr}_{N,\tau,p}$ in $G^\natural$. As an element of the quotient group $C_2 \times C_2$, it is given by a pair of Jacobi symbols:

$$[\mathrm{Fr}_{10a,\tau,p}] = \left(\left(\frac{2}{p}\right), \left(\frac{-2(\tau-1)}{p}\right)\right) \tag{5.2}$$

$$[\mathrm{Fr}_{10b,\tau,p}] = \left(\left(\frac{2\tau(\tau-1)}{p}\right), \left(\frac{2(\tau-1)}{p}\right)\right). \tag{5.3}$$

The Frobenius class $\mathrm{Fr}_{N,\tau,p}$ itself is then completely determined by the factorization pattern $\lambda_{N,\tau,p}$ of $f_N(\tau, x)$ in $\mathbb{Q}_p$. The possibilities are

$[\mathrm{Fr}_{N,\tau,p}]$	$A_6 = PSL_2(9) = M'_{10}$ $(1,1)$					$S_6 - A_6$ $(-1,-1)$			$PGL_2(9) - PSL_2(9)$ $(1,-1)$			$M_{10} - M'_{10}$ $(-1,1)$	
Atlas	$1A$	$2A$	$3AB$	$4A$	$5AB$	$2BC$	$4B$	$6AB$	$2D$	$8AB$	$10AB$	$4C$	$8CD$
#	1	45	80	90	144	30	90	240	36	180	144	180	180
$\lambda_{N,\tau,p}$	1^{10}	$2^4 1^2$	$3^3 1$	$4^2 1^2$	5^2	$2^3 1^4$	$4^2 2$	631	2^5	81^2	10	$4^2 1^2$	82

The line # gives the number of elements of $P\Gamma L_2(9)$ belonging to each conjugacy class. We do not use this information to distinguish fields and get lower bounds on Galois groups. However this information is very orienting as one carries out Frobenius computations, because a field with Galois group H has its Frobenius elements distributed in $H^\natural$ in proportion to the analogous numbers, here tabulated for $H = P\Gamma L_2(9)$.

6. $SL_2(8)$ and $\Sigma L_2(8)$; Shimura curves

Here we specialize two covers. For the first, we work with $\mathbb{F}_8 = \mathbb{F}_2[a]/(a^3+a+1)$. For the second, we work with $\mathbb{F}_{64} = \mathbb{F}_2[b]/(b^6 + b^3 + 1)$. The field element a has multiplicative order 7, while b has multiplicative order 9. We regard $\mathbb{F}_{64}$ as containing $\mathbb{F}_8$ via $a = b + b^8$.

The first cover is

$$\begin{aligned}
u_{9a} &= x^2+x+1\\
w_{9a} &= x^2+ax+1\\
\Lambda_{9a} &= (333, 22221, 9)\\
f_{9a}(t,x) &= (x^3-9x^2-69x-123)^3 -\\
&\quad 2^{14}t(9x^4-42x^3-675x^2-1485x-441)-2^{28}t^2\\
D_{9a}(t) &= 2^{140}3^{18}t^6(t-1)^4\cdot\\
&\quad (4398046511104t^3-5421322469376t^2-7496810496t+513922401)^2.
\end{aligned}$$

The defining polynomial f_{9a} was sent to us by Elkies in 1995. This cover has genus one. This is the reason behind the extraneous cubic-squared factor in $D_{9a}(t)$, an example of a non-trivial $c(t)^2$ in (3.1). All the other covers in this paper, besides a few that we see briefly while carrying out a construction involving base change, have genus zero.

The construction of the second cover involves two base changes, the first a degree three base change $\mathbb{P}^1_s \to \mathbb{P}^1_u$, and the second a degree two base change $\mathbb{P}^1_u \to \mathbb{P}^1_t$.

$$\begin{aligned}
u^s_{9b} &= (x-b)(x-b^6)\\
w^s_{9b} &= (x-b^4)(x-b^6)\\
\Lambda^s_{9b} &= (9A, 9B, 9C) \to (9,9,9) \quad \text{(genus 4)}\\
u &= (s-2)(s+1)(2s-1)/3(s-1)s\\
\Lambda^u_{9b} &= (3B, 3B, 9ABC) \to (33111, 33111, 9) \quad \text{at } u=\sqrt{-3}, -\sqrt{-3}, \infty\\
f_{9b}(u,x) &= A(x)+u2^{13}3^4\\
A(x) &= x^9+108x^7+216x^6+4374x^5+\\
&\quad 13608x^4+99468x^3+215784x^2+998001x+810648\\
D_{9b}(u) &= 2^{104}3^{50}(u^2+3)^4\\
t &= -u^2/3\\
\Lambda_{18} &= (2^9,\ 3^4\,1^6,\ 18)\\
f_{18}(t,x) &= f_{9b}(u,x)f_{9b}(-u,x)\\
&= A(x)^2+2^{26}3^9t\\
D_{18}(t) &= -2^{460}3^{189}t^9(t-1)^8.
\end{aligned}$$

The formula $f_{9b}(u,x)$ for Cover 9*b* is from [**Mat**, page 193]. The monodromy and Galois group of this cover are both $\Sigma L_2(8) = SL_2(8).3$. Matzat's three point cover does not fit into our set-up because the ramification locus is $u = \sqrt{-3}$, $-\sqrt{-3}$, ∞. Our second base change is to place the ramification points at our standard locations, $t = 0$, 1, ∞. To do this without introducing irrationalities, we double the degree of the cover. The Galois group becomes $G_{18} = \Sigma L_2(8)^2.2$. The monodromy group is the unique index three normal subgroup. The constant field extension, with Galois group G_{18}/M_{18}, is $\mathbb{Q}(\cos(2\pi/9))$, with defining polynomial x^3-3x+1; this is the unique field in $NF(\{2,3\}, A_3)$.

We specialize f_{9a} at the 87-element set $T^*_{3,2,9}$. The polynomial $f_{9a}(-17^3/2^7, x)$ factors as f_8f_1, the degree eight factor having Galois group $A_4 \times C_2$. The polynomials $f_{9a}(-2^53^2, x)$ and $f_{9a}(3^217^3/2^{15}, x)$ define the same field, with defining

equation x^9+6x^3-2 and Galois group the 54-element affine group $(\mathbb{Z}/9).(\mathbb{Z}/9)^\times$. The remaining 84 specialization points give 55 fields, all with Galois group $\Sigma L_2(8)$. All these fields are wildly ramified at three. Exactly two of them are only tamely ramified at 2:

$$L_{9a,\tau} \quad : \quad x^9-36x^6-162x^4-54x^3-972x^2+486x-594 \tag{6.1}$$

$$L_{9a,4/3} \quad : \quad x^9-18x^3+27x-6. \tag{6.2}$$

The first field arises from five specialization points, namely $\tau = 2^5/3^4$, $-505^3/2^{27}3$, $2^{10}19^3/5^93$, $-2^95^3/3^2$, and $-73^3/2^{15}3^2$. The field discriminants are 2^83^{26} and 2^63^{26}, respectively.

We specialize f_{18} at the 81-element set $T^*_{2,3,18} = T^*_{2,3,\infty}$. When -3τ is not a square in $\mathbb{Q}$, we get fields which generically have Galois group containing two copies of $SL_2(8)$, thus interesting, but out of our self-imposed context. The six elements τ with -3τ a square are $\tau = -u^2/3$ with $u \in \{1, 10/9, 35/18, 3, 595/108, 37\}$. The twelve algebras $L_{9b,\pm u}$ are all fields, and so is $L_{9b,0}$; they are all pairwise non-isomorphic. Exactly one of these fields appeared already as a specialization of f_{9a}, namely $L_{9b,-5\cdot 7/2\cdot 3^2}$ which coincides with the tame-at-two field $L_{9a,4/3}$. Of the twelve remaining fields, nine have Galois group $\Sigma L_2(8)$, and three have Galois group $SL_2(8)$, these being

$$\begin{aligned} L_{9b,-3} \quad &: \quad x^9-12x^6-18x^5+36x^2-27x-128 \\ L_{9b,37} \quad &: \quad x^9-36x^6-54x^5-324x^4-216x^3-972x^2-243x-2124 \\ L_{9b,1} \quad &: \quad x^9-36x^6-54x^5+432x^3+324x^2-243x-1152. \end{aligned}$$

These fields have discriminants $2^{14}3^{22}$, $2^{14}3^{26}$, and $2^{14}3^{26}$, respectively.

In comparison with the other examples in this paper, the most remarkable phenomenon here is that often two or more $L_{9a,\tau}$ are isomorphic. This phenomenon can be partially explained as follows. The cuspidal data identifies the base $\mathbb{P}^1$ with a minimal-area Shimura curve $X_0(1)$ associated to the cubic field $\mathbb{Q}(\cos(2\pi/9))$ and no ramification at finite places. The cover $X_{9a} \to \mathbb{P}^1$ is identified with $X_0(2) \to X_0(1)$, the ideal (2) having residual cardinality 8. But now, one has also a degree four cover $\pi : X_0(P) \to X_0(1)$, where P is the unique prime above 3. The curve $X_0(P)$ has an Atkin-Lehner-type involution W_P, and hence a second natural map $\pi \circ W_P$ to the base curve $X_0(1)$. As in the classical case, one can think of $X_0(P) \subset X_0(1) \times X_0(1)$ as being a correspondence T_P from $X_0(1)$ to $X_0(1)$ of bidegree $(4,4)$. In terms of our fixed coordinate t on $X_0(1)$, and the same coordinate s on the second copy of $X_0(1)$, the defining equation for $X_0(P)$ is unique up to scalars:

$$\begin{aligned} h_P(s,t) = \\ & 2^{12}st\left(-3^{10}17^366383+2^{13}3^81054805(s+t)+2^{27}3^5211(s^2+t^2)+\right. \\ & \left. 2^{13}3^62486119st-2^{21}3^322267(s^2t+st^2)-2^{24}55s^2t^2+2^{30}(s^3t^2+s^2t^3)\right) \\ & -3^6(-3^217^3+2^{15}s)^3-3^6(-3^217^3+2^{15}t)^3-3^{12}17^9. \end{aligned}$$

The specialization points giving isomorphic algebras are exactly as follows. Here $\sigma \approx \tau$, rather than just $\sigma \sim \tau$, indicates that $h_P(\sigma,\tau) = 0$; so these isomorphisms

$L_{9a,\sigma} \cong L_{9a,\tau}$ are explained by the Hecke correspondence T_P.

$$\begin{array}{rcl} -1 & \sim & 2797^3/13^9 \\ 5^3 7^3/3^5 & \sim & -4079^3/3 \\ 3^2 & \sim & 5^3/3^3 \\ 3^5 & \sim & -23^3 \\ -2^5 3^2 & \sim & 3^2 17^3/2^{15} \\ -1/2^3 & \sim & 3^5 67^3/2^3 \end{array} \qquad \begin{array}{rcl} -2^4/3^2 & \sim & 2^2 7^3/3 \approx 23^3/2^{12}3 \\ 2^3/3^2 & \sim & -13^3/2^2 3 \approx -5^6/2^9 3 \\ -2^3 3 & \sim & 1/2^2 \approx 3^1 11^3/2^9 \\ -3 & \sim & 5^3/2^7 \approx 3^1 19^3/2^7 \end{array}$$

$$\begin{array}{rcccccccc} 2^5/3^4 & \sim & -505^3/2^{27}3 & \approx & 2^{10}19^3/5^9 3 & \sim & -2^9 5^3/3^2 & \approx & -73^3/2^{15}3^2 \\ -2^3 & \sim & -3^2/2^4 & \sim & 5^3/2^2 & \approx & 7^3/2^9 & \approx & 3^2 73^3/2^9 \\ 3/2^2 & \sim & -11^3/2^8 & \approx & -35^3 3/2^8 & \sim & -203^3/2^{11}5^9 & \approx & 3155^3 3/2^{11}7^9 \\ -2^4 3 & \sim & 2^2 & \approx & 3^1 5^3/2^{12} & \sim & -1915^3/2^{13} & \approx & -3^1 1027^3/2^{13}5^9 \end{array}$$

The Hecke correspondence T_P also explains two of the three cases mentioned above of unexpectedly small Galois group. First, the degree seven polynomial $h_P(t,t)$ factors as $f_3^2 f_1$, the root of the linear factor being $\tau = -17^3/2^7$. So this τ is a CM point, which forces $L_{9a,\tau}$ to be non-generic. Second, the degree three polynomial $h_P(0,t)$ factors as f_1^3, the root of the linear factor being $\tau = 3^2 17^3/2^{15}$. So this τ, like 0, is also a CM point, again forcing non-genericity in $L_{9a,\tau}$.

The cover X_{10a} from the previous section is also a minimal area Shimura curve, coming from the field $\mathbb{Q}(\sqrt{2})$. For more on Shimura curves as covers of the projective line, see [**Tak**], [**Elk**].

7. $SL_3(3)$ and $SL_3(3).2$; projective twinning

Here we use two new covers $13a$, $13b$, and a cover $26c$, which is a doubled version of one of the covers in [**Mal1**]. The new covers are

$$\begin{array}{rcl} u_{13a} & = & (x-1)^3 \\ w_{13a} & = & (x-\rho)(x-\rho^3)(x+1) = x^3+2x^2+2 \\ \Lambda_{13a} & = & (3B,\ 3A,\ 8A) \to (33331,\ 3331111,\ 841) \\ f_{13a}(t,x) & = & (x^3-6x+6\sqrt{-2}x-4-8\sqrt{-2})^3(x-2-\sqrt{-2})^3(x-2+2\sqrt{-2}) - \\ & & t2^2 3^2(3x-4+\sqrt{-2})^4(3x-8+\sqrt{-2}) \\ D_{13a}(t) & = & 2^{112}3^{54}(1-\sqrt{-2})^{72}t^8(t-1)^6 \end{array}$$

$$\begin{array}{rcl} u_{13b} & = & (x-1)(x^2+1) \\ w_{13b} & = & w_{13a} \\ \Lambda_{13b} & = & (4A,\ 3A,\ 8A) \to (44221,\ 3331111,\ 841) \\ f_{13b}(t,x) & = & (x^2-3\sqrt{-2}x-3\sqrt{-2}-3)^4(x^2+6\sqrt{-2}-3)^2(x+3-3\sqrt{-2}) + \\ & & t2^2 3^3(1+\sqrt{-2})^8(x+1-\sqrt{-2})^4(3x+5-\sqrt{-2}) \\ D_{13b}(t) & = & 2^{92}3^{72}(1+\sqrt{-2})^{96}t^8(t-1)^6. \end{array}$$

These covers were first computed over $\mathbb{F}_{11}$, where each cover appeared with its projective twin, as described below; at this level, there is no evident relation between the equation for a cover ($\sqrt{-2} \mapsto 3 \in \mathbb{F}_{11}$) and the equation for its twin ($\sqrt{-2} \mapsto 8 \in \mathbb{F}_{11}$). We worked with the auxiliary prime 11 because it is the smallest prime besides 3 which is split in the field $\mathbb{Q}(\sqrt{-2})$. We then lifted via the 11-adics to solutions in $\mathbb{Q}(\sqrt{-2})$ as explained in [**Mal2**]. At this level, passing from a cover to its twin is induced by complex conjugation in the ground field $\mathbb{Q}(\sqrt{-2})$.

The third cover is

$$\begin{aligned}
u^u_{13c} &= (x-\rho^5)(x-\rho^7)(x-1) = x^3+x^2+1\\
w^u_{13c} &= w_{13a}\\
\Lambda^u_{13c} &= (8A, 8B, 2A) \to (841, 841, 222211111) \text{ at } u = -\sqrt{-8}, \sqrt{-8}, \infty\\
f_{13c}(u,x) &= A(x) - uB(x)\\
A(x) &= (x^3-12x^2-6x-64)(x^4+16x^3-36x^2+128x-28)\cdot\\
&\quad (x^6+12x^5+54x^4+176x^3+444x^2+624x+552)\\
B(x) &= (x^4+16x^3+72x^2+128x+188)(3x^4-4x^3+12x^2-24x-68)^2\\
D_{13c}(u) &= 2^{160}3^{114}(u^2+8)^{10}\\
t &= -u^2/8\\
\Lambda_{26c} &= (2B,\ 8AB,\ 4B) \to (2^{13},\ 8^2\,4^2\,1^2,\ 4^4\,2^5)\\
f_{26c}(t,x) &= f_{13a}(u,x)f_{13a}(-u,x)\\
&= A(x)^2 + 8tB(x)^2\\
D_{26c}(t) &= -2^{777}3^{452}t^{13}(t-1)^{20}.
\end{aligned}$$

One has $M_{13c} = G_{13c} = SL_3(3)$. Just as we doubled the Matzat cover in the previous section, we double the Malle cover to place the critical values at our standard positions 0, 1, and ∞ and remove irrationalities. In distinction to what happened when we doubled the Matzat cover, here the groups do not become much bigger: $M_{26c} = G_{26c} = SL_3(3).2$.

To facilitate comparison with f_{26c}, we consider the degree 26 polynomials $f_{26a} = f_{13a}\bar{f}_{13a}$ and $f_{26b} = f_{13b}\bar{f}_{13b}$ in $\mathbb{Q}[t,x]$. We specialize f_{26a} at the 27-element set $T^*_{3,3,8}$ and f_{26b} at the 24-element set $T^*_{4,3,8}$. The polynomials $f_{26a}(-8,x)$, $f_{26b}(4,x)$, $f_{26b}(3/4,x)$ each factor, and the corresponding splitting fields have Galois group $3^{1+2}_+.D_4$, $3^{1+2}_+.V$, and $3^{1+2}_+.C_2$ respectively. A Frobenius computation shows that the remaining 48 polynomials have Galois group all of $SL_3(3).2$. The Frobenius computation shows that these fields are all non-isomorphic except for perhaps $L_{26b,1/4}$ and $L_{26b,-8}$. We have verified that this last pair of fields is indeed isomorphic. We used the method described in Section 9, working only with the roots of $f_{13b,1/4}$ and $f_{13b,-8}$.

Now consider Cover 26*c*. In general, if -2τ is not a square in $\mathbb{Q}$, then $L_{26c,\tau}$ contains a subfield isomorphic to $\mathbb{Q}(\sqrt{-2\tau})$. If -2τ is a square, then one has the factorization $f_{26c}(\tau,x) = f_{13c}(u,x)f_{13c}(-u,x)$, with $u^2 = -8\tau$. Thirty-eight of the elements in the 45-element set $T^*_{2,8,4}$ are such that -2τ is a non-square. A Frobenius computation shows that all of these have Galois group all of $SL_3(3).2$ and are pairwise non-isomorphic. Moreover the fields $L_{26c,\tau}$ are not isomorphic with any of the 47 fields coming from 26*a* and 26*b*.

The seven elements τ with -2τ a square are $\tau = -u^2/8$ with $u = 1$, 2, 7/2, 4, 8, 44 and 10. A Frobenius computation shows generic behavior in the first six cases: the splitting field of $f_{13c}(u,x)$ has Galois group all of $SL_3(3)$, and these six splitting fields are non-isomorphic. Note that the degree thirteen fields $\mathbb{Q}[x]/f_{13c}(u,x)$ and $\mathbb{Q}[x]/f_{13c}(-u,x)$ are non-isomorphic, corresponding to different permutation representations of their common Galois group. This is seen clearly in the degenerate case $\tau = -5^2/2$. In this case, $f_{13c}(-10,x)$ factors as $9+4$ and $f_{13c}(10,x)$ factors as $12+1$; the common Galois group is $3^{1+2}_+.\tilde{S}_4$.

The twinning phenomenon here is quite general, deriving from the fact that the permutation representations of a group PGL_n on the projective space $\mathbb{P}^{n-1}$ and its dual $\check{\mathbb{P}}^{n-1}$ are not isomorphic, for $n \geq 3$. A prime ℓ and a degree $n \geq 3$ being fixed, say that a number field of degree $\ell^{n-1} + \ell^{n-2} + \cdots + \ell + 1$ is projective iff its Galois group can be identified with $PGL_n(\ell)$, as a permutation group. Then a projective field L has a non-isomorphic twin L^t, there being a canonical isomorphism $L = L^{tt}$.

This situation of twin projective fields contrasts in one important way with the situation of twin A_6 or S_6 sextic fields, which played a role in Section 5. Namely, the two different permutation representations induce the same linear representation only in the projective case. So twin fields have the same Dedekind zeta function only in the projective case. One can summarize by saying that A_6 and S_6 sextic fields come in fraternal twin pairs while projective fields come in identical twin pairs. In particular, twin projective fields have the same discriminant. In the cases here, one has discriminants $2^{28}3^{24}$, $2^{36}3^{26}$, $2^{28}3^{22}$, $2^{38}3^{26}$, $2^{32}3^{24}$, $2^{38}3^{20}$ for $|s| = 1$, 2, 7/2, 4, 8, 44.

8. $SU_3(3)$ and $SU_3(3).2$; connections with a base change

Here we work with a cover $X_{28a} \to \mathbb{P}^1_t$, which comes from a solution to the matrix ABC equation (1.1) as follows.

$$\begin{aligned}
u^s_{28a}(x) &= (x-1)^2(x-i) = x^3 + (1+2i)x^2 + (1+2i)x + 2i \\
w^s_{28a}(x) &= (x+1)^2(x+i) = x^3 + (2+i)x + (1+2i)x + i \\
\Lambda^s_{28a} &= (12A, 2A, 12B) \to (12^2 3\ 1,\ 2^{12}1^4,\ 12^2 3\ 1)\ \text{(genus three)} \\
t &= -(s-1)^2/4s \\
\Lambda_{28a} &= (4D, 2B, 12AB) \to (4^6 1^4,\ 2^{12}1^4,\ 12^2 3\ 1) \\
f_{28a}(t,x) &= (x^6 - 6x^5 - 435x^4 - 308x^3 + 15x^2 + 66x + 19)^4 \cdot \\
&\quad (x^4 + 20x^3 + 114x^2 + 68x + 13) - 2^2 3^9 t(x^2 + 4x + 1)^{12}(2x+1) \\
D_{28a}(t) &= 2^{576}3^{630}t^{18}(t-1)^{12}
\end{aligned}$$

The monodromy group of the genus three cover $X^s_{28a} \to \mathbb{P}^1_s$ is the simple group $SU_3(3)$. The Galois group is $SU_3(3).2$, the corresponding constant field extension being $\mathbb{Q}(i)$. The equation $f_{28a}(t,x)$ for Cover 28a appears in [**MM**, page 412]. Its monodromy and Galois groups are both $M_{28a} = G_{28a} = SU_3(3).2$.

Explicitly, the rigid solution to (1.1) we are using is

$$\begin{pmatrix} 0 & 0 & i \\ 1 & 0 & 2+i \\ 0 & 1 & 2+i \end{pmatrix} \begin{pmatrix} 1 & 0 & 1+2i \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1+i & 1 & 0 \\ 2+2i & 0 & 1 \\ i & 0 & 0 \end{pmatrix} = I. \tag{8.1}$$

The three displayed matrices generate $M = SU_3(3)$ inside $GL_3(9)$. In constrast, the faithful linear representations of the larger group $SU_3(3).2$ in characteristic two and three all have dimension ≥ 6. None of these representations gives rise to a rigid solution of the matrix equation (1.1). This is why our passage from (1.1) to Cover 28a involves an intermediate cover.

The intermediate cover $X^s_{28a} \to \mathbb{P}^1_s$ is a pullback via the base change $\mathbb{P}^1_s \to \mathbb{P}^1_t$, $s \mapsto -(s-1)^2/4s$ of the cover $X_{28a} = \mathbb{P}^1_x \to \mathbb{P}^1_t$. Some particular points that play

a special role in our discussion behave as follows.

$$1 \mapsto 0 \tag{8.2}$$

$$-1 \to 1 \tag{8.3}$$

$$0, \infty \mapsto \infty. \tag{8.4}$$

The points $s = -1, 1$ in $\mathbb{P}^1_s$ are the unique ramification points of this quadratic base change map. From (8.2), the ramification class $4D$ associated to $t = 0$ pulls back to its square $2A$, which is now associated to $s = 1$. From (8.3), the class $2B$ associated with $t = 1$ pulls back to its square, the identity class $1A$; so there is no ramification associated to $s = -1$ in $\mathbb{P}^1_s$. Finally, from (8.4), the ramification class $12AB$ associated to $t = \infty$ splits into two ramification classes, $12A$ at $s = 0$ and $12B$ at the $s = \infty$. This entire discussion explains on a conceptual level why Cover $28a$ is ramified only at 2 and 3; were it not for the connection via the base change to rigidity, one would have expected 7 to very likely ramify too.

Two of the specialization points τ in the 44-element set $T^*_{4,2,12}$ yield a factorizable polynomial. Namely $f_{28a}(2/3^3, x)$ factors as $27 + 1$ and $f_{28a}(-5^4/2^3 3^3, x)$ factors as $24 + 4$. The splitting fields of these polynomials have Galois groups $3^{1+2}_+.8.2$ and $4.S_4.2$ respectively, these being maximal subgroups of $U_3(3).2$. The specialization point $\tau = 1/2$ yields a polynomial with Galois group $SU_3(3)$; the remaining polynomals yield 41 distinct fields, all having Galois group all of $SU_3(3).2$.

9. $W(E_6)'$ and $W(E_6)$; exhibiting exceptional isomorphisms

Here we work with four degree twenty-seven covers, denoted $27a$, $27b$, $27c$, $27d$. Cover $27a$ is due to Häfner [**Häf**], while $27b$ and $27c$ are new here. These three covers are related to algebraic hypergeometric functions with finite monodromy, corresponding to the entries 47, 45, and 48 on the Beukers-Heckman list [**BH**]; they all have $M = G = W(E_6)$. Cover $27d$ is also new. It is directly related to hypergeometric-like functions with finite monodromy, namely functions corresponding to the families A and D of [**Rob2**], rather than to the family H corresponding to hypergeometric functions. Here, however we present $27d$ as related via a base change to hypergeometric functions with infinite monodromy. For this cover, $M = W(E_6)'$ and $G = W(E_6)$, the corresponding constant field extension being $\mathbb{Q}(\sqrt{-3})$.

$$\begin{aligned}
u_{27a} &= x^6 + x^3 + 1 \\
w_{27a} &= (x^2 + x + 1)(x^2 + 1)(x + 1)(x - 1) \\
\Lambda_{27a} &= (9AB,\ 2C,\ 12C) \to (9^3,\ 2^6\,1^{15},\ 12\,6\,4^2\,1) \\
f_{27a}(t, x) &= (x^3 + 6\,x^2 - 8)^9 - t2^4 3^{12} x^6 (x^2 + 5\,x + 4)^4 (x - 2) \\
D_{27a}(t) &= 2^{414} 3^{450} t^{24} (t - 1)^6
\end{aligned}$$

$$\begin{aligned}
u_{27b} &= (x^4 - x^2 + 1)(x^2 + x + 1) \\
w_{27b} &= (x^4 + 1)(x + 1)(x - 1) \\
\Lambda_{27b} &= (12AB,\ 2C,\ 8A) \to (12^2\,3, 2^6\,1^{15},\ 8^3\,2\,1) \\
f_{27b}(t, x) &= 2^4 x^3 (x^2 - 3)^{12} - t3^9 (x - 1)^8 (x - 2)(x^2 - 2x - 1)^8 \\
D_{27b}(t) &= 2^{542} 3^{270} t^{24} (t - 1)^6
\end{aligned}$$

$$\begin{aligned}
u_{27c} &= u_{27a}\\
w_{27c} &= w_{27b}\\
\Lambda_{27c} &= (9AB,\ 2C,\ 8A) \to (9^3,\ 2^6\,1^{15},\ 8^3\,2\,1)\\
f_{27c}(t,x) &= 2^{18}(x^3+9\,x^2+6\,x+1)^9 - 3^{15}\,t\,x\,(2\,x+1)^8(x^2-2\,x-1)^8\\
D_{27c}(t) &= 2^{522}3^{450}t^{24}(t-1)^6
\end{aligned}$$

$$\begin{aligned}
u^s_{27d} &= (x-1)^5 \in \mathbb{F}_3[x]\\
w^s_{27d} &= (x+1)^5 \in \mathbb{F}_3[x]\\
\Lambda^s_{27d} &= (9A,\ 2A,\ 9A) \to (9^3,\ 2^{12}1^3,\ 9^3)\ \text{(genus 4)}\\
t &= -4s/(s-1)^2\\
\Lambda_{27d} &= (9A,\ 2B,\ 4A) \to (9^3,\ 2^{10}\,1^7,\ 4^6\,1^3)\\
f_{27d}(t,x) &= 4(3x^3-12\,x-8)^9 - t(12\,x^3+54\,x^2+63\,x+22)\cdot\\
&\quad (9\,x^6+81\,x^5+135\,x^4+276\,x^3+432x^2+288\,x+64)^4\\
D_{27d}(t) &= 2^{518}3^{450}t^{24}(t-1)^{10}
\end{aligned}$$

The three new covers were all found first modulo 5, and then lifted via the 5-adics to rational solutions as explained in [**Mal2**]. The cover X_{28b} of Section 11 was also computed in this way. Of these four new covers, $27d$ was the hardest to obtain, since the $N+2$ parts of $3N$ are more evenly distributed among the cusps.

In cases $27a$, $27b$, and $27c$, we specialize to τ in the 35-element set $T^*_{9,2,12} = T^*_{12,2,8} = T^*_{9,2,8} = T^*_{\infty,2,\infty}$. In case $27d$, we specialize to τ in the 45-element set $T^*_{9,2,4}$. All 150 defining polynomials $f_{27*}(\tau,x)$ are irreducible, so all the algebras $L_{27*,\tau}$ are fields. A Frobenius computation proves that at least 146 of these fields have Galois group all of G or G'. Using the monodromy technique described in Section 11, we have verified that each apparent group-drop indeed occurs, and computed degree nine resolvents as follows.

$$h_{27a,-1}(x) = x^9 - 3x^8 + 6x^7 - 3x^5 + 15x^4 + 6x^3 + 6x^2 + 6x + 2 \tag{9.1}$$

$$h_{27b,-1/48}(x) = x^9 - 12x^6 - 9x^5 + 54x^3 + 36x^2 + 18x - 56 \tag{9.2}$$

$$g_{27d,1/2}(x) = x^9 - 6x^7 + 27x^5 - 12x^4 - 174x^3 - 108x^2 + 183x + 124 \tag{9.3}$$

$$g_{27d,1/2\cdot 13^4}(x) = x^9 + 3x^8 - 16x^6 - 36x^5 + 36x^4 + 96x^3 - 108x - 36. \tag{9.4}$$

Here $h_{27a,-1}$ and $f_{27a,-1}$ have the same splitting field, and so too do $h_{27b,-1/48}$ and $f_{27b,-1/48}$; the Galois groups here have the form $3^3.(S_4 \times C_2)$ and $3^3.S_4$ respectively. On the other hand, the Galois groups $G_{27d,1/2}$ and $G_{27d,1/2\cdot 13^4}$ each have the form $3^{1+2}.\tilde{S}_4$; the corresponding degree nine resolvents have Galois group of the form $3^2.\tilde{S}_4$. The field discriminants of the four displayed nonic polynomials are $2^{13}3^{15}$, $2^{12}3^{18}$, $-2^{22}3^{13}$, and $-2^{22}3^{15}$ respectively.

All the 150 specializations are wild at both 2 and 3 except

$$L_{27d,-48} = \mathbb{Q}[x]/f_{27d}(-48,x), \tag{9.5}$$

which is tame at 2, with discriminant $2^{20}3^{84}$. The tameness at 2 can almost be seen from the Newton polygon at 2, which has slopes 1/5, 1, 8/5, and 5 with multiplicities 10, 1, 15, and 1 respectively. It can be seen from the full 2-adic factorization of $f_{27d}(-48,x)$ which has three factors of degree five and discriminant 2^4, one factor of degree ten and discriminant 2^8, and two linear factors.

The Frobenius computation proves that except for the possible isomorphism

$$L_{27b,-48} \cong L_{27d,32/81},$$

the 146 generic specializations are all distinct. To prove that $L_{27b,-48}$ and $L_{27d,32/81}$ are isomorphic one needs to exhibit the unique isomorphism; this is our topic for the rest of the section.

In numerical terms, one needs to find the unique bijection σ from the complex roots $A = \{\alpha_i\}$ of $f_{27b,-48}$ to the complex roots $B = \{\beta_j\}$ of $f_{27d,32/81}$ such that the the polynomial

$$\text{test}_{\sigma,r}(x) = \prod_i (x - \alpha_i - r\beta_{\sigma(i)}) \tag{9.6}$$

has rational coefficients for all $r \in \mathbb{Q}$; here we introduce r just to avoid possible inseparability problems; in practice one can simply fix r at 1.

The bijection σ must intertwine complex conjugation: $c_B \circ \sigma = \sigma \circ c_A$. Since the polynomials in question have exactly three real roots, there are $3!12!2^{12} \approx 1.177 \times 10^{13}$ such bijections. The sheer size of this number is why *Pari*'s *nfisisom*, which is designed to find isomorphisms between fields, does not work here. Indeed, if we were simply given the bare polynomials $f_{27b,-48}$ and $f_{27d,32/81}$, we would not know how to find the desired isomorphism.

But we are not given the polynomials in isolation. Rather we can figure out how the monodromy operators m_c act on the roots. In the case of $f_{27b,-48}$ this action is as follows.

$$\begin{aligned} m_{27b,0} &= (1a, 15a, 7a, 4a, 3a, 2a, 2b, 3b, 4b, 7b, 15b, 1b)(5a, 6, 5b) \cdot \\ &\quad (11, 12b, 13b, 14b, 8b, 9b, 10, 9a, 8a, 14a, 13a, 12a) \\ m_{27b,\infty} &= (1a, 1b)(2a, 3a, 4a, 5a, 5b, 4b, 3b, 2b)(6, 7a, 8a, 9a, 10, 9b, 8b, 7b) \cdot \\ &\quad (11)(12a, 13a, 14a, 15a, 15b, 14b, 13b, 12b). \end{aligned}$$

Here we have ordered the $\text{Gal}(\mathbb{C}/\mathbb{R})$-orbits from left to right, 1 through 15. If a root is in the lower half plane, we append "a"; if it is the upper half plane we append "b"; if it is on the real line we index the root simply by a number; thus $\alpha_{1a} = -(12.976\ldots) - (243.333\ldots)i$ and $\alpha_6 = .518\ldots$. The action of $m_{27b,0}$ is obtained by considering the inverse image of $[-48, 0]$ in the complex plane with coordinate x. It is the union of three "wheels," two with 12 spokes and one with 3. The action is obtained by "rotating the wheels one spoke counter-clockwise." All this can be done numerically, working visually with say the roots of $f_{27b}(-48u^{12}, x)$, with $u = 0, 1/100, 2/100, \ldots, 1$; restricting to $u \geq 20/100$ lets one work entirely in standard precision and still do the computation. The other monodromy action $m_{27b,\infty}$ is obtained similarly, i.e. again in the the spirit of Grothendieck's *dessins d'enfants* [**Sch**]. Repeating the procedure for the roots of $f_{27d,32/81}$ gives

$$\begin{aligned} m_{27d,0} &= (1a, 2a, 10a, 6a, 3, 6b, 10b, 2b, 1b)(9b, 8b, 7b, 5b, 4, 5a, 7a, 8a, 9a) \cdot \\ &\quad (11a, 13a, 14a, 12a, 15, 12b, 14b, 13b, 11b) \\ m_{27d,1} &= (5a)(5b)(13a)(13b)(14a)(14b)(15)(1a, 1b)(2a, 12a)(2b, 12b) \cdot \\ &\quad (3, 4)(6a, 9a)(6b, 9b)(7a, 8a)(7b, 8b)(10a, 11a)(10b, 11b). \end{aligned}$$

Let C be one of the two root sets A or B. We use the monodromy action to view the 27-element set C as a structured set. Namely consider the set $\text{Sub}_2(C)$

of two-element subsets. Under the action of the monodromy group one has a decomposition into two orbits

$$\mathrm{Sub}_2(C) \quad = \quad \mathrm{Sub}_2(C)' \coprod \mathrm{Sub}_2(C)''.$$

Here the first orbit has 135 elements and the second has 216. In other words, we can view C as the vertices of a graph Γ_C, with edge-set $\mathrm{Sub}_2(C)'$. The action of complex conjugation on C extends to Γ_C. The graph-with-involution (Γ_C, i_C) has only $2^7 3^2 = 1152$ automorphisms.

The bijection $\sigma : A \to B$ we seek respects not only complex conjugation but also the graph structure. To find it, we work purely group-theoretically to first find some isomorphism $s : (A, i_A) \to (B, i_B)$ respecting the graph structure; this is easy. Then we compose it with the 1152 elements of $\mathrm{Aut}(\Gamma_B, i_B)$ to get 1152 candidates for σ. For only one of them does (9.6) appear to have rational coefficients, and we have thereby numerically determined σ. It is as follows:

roots of $f_{27b,-48}$:	$1a$	$2a$	$3a$	$4a$	$5a$	6	$7a$	$8a$	$9a$	10	11	$12a$	$13a$	$14a$	$15a$
roots of $f_{27d,32/81}$:	$7b$	$1b$	$9a$	$5b$	$8a$	4	$6a$	$2b$	$11a$	15	3	$14b$	$13a$	$12b$	$10a$

Here, since $\sigma(\alpha_{1a}) = \beta_{7b}$, we must have $\sigma(\alpha_{1b}) = \beta_{7a}$ as well, and so too for the other complex conjugate pairs.

To check rigorously that indeed σ induces an isomorphism we proceed as follows. First, we numerically solve the 27-by-27 system $Tz = B$ with $T_{ik} = \alpha_i^k$ and $B_i = \beta_{\sigma(i)}$ for the vector z, rationalizing at the end. Then

$$y = \sum_{k=0}^{26} z_k x^k, \tag{9.7}$$

as an element of the ring $\mathbb{Q}[x]/f_{27b}(-48, x)$, should satisfy $f_{27d}(32/81, y) = 0$. In our case, (9.7) takes the explicit form $126414618624y =$

$$\begin{array}{rrr}
-778448003x^{26} & -981509289x^{25} & -45939794218464x^{24} \\
1137207587245554x^{23} & -12724591174373616x^{22} & 84720990963862440x^{21} \\
-370643301489686778x^{20} & 1104517184207752350x^{19} & -2221386267735948267x^{18} \\
2770729912599438087x^{17} & -1364804638977353670x^{16} & -1659195683617968252x^{15} \\
3294135546577106040x^{14} & -1424334213106643304x^{13} & -1494872066602993428x^{12} \\
1744593287940021708x^{11} & 58514783809113639x^{10} & -818860129717879323x^{9} \\
171625804007741892x^{8} & 237402868177405098x^{7} & -68548289134461768x^{6} \\
-50056832848713984x^{5} & 11561622988644846x^{4} & 7711324091701110x^{3} \\
-484480924209657x^{2} & -608102864271747x & -73397655884286.
\end{array}$$

This indeed satisfies $f_{27d}(32/81, y) = 0$. The case $L_{13c,1/4} \cong L_{13c,-8}$ from §8 is substantially easier, as the root sets to be identified have only 13 elements each.

10. A_9 and S_9; cuspidal specialization

Let (A, B, C) be a rigid solution to the matrix ABC equation (1.1) generating a subgroup $\tilde{M}$ of $GL_n(\overline{\mathbb{F}}_\ell)$ with center Z. Almost always, $\tilde{M}$ is closely related to a finite classical group, i.e. an orthogonal group, a symplectic group, a unitary group, or a general linear group. Our ABC construction requires us to choose a faithful permutation representation of $M = \tilde{M}/Z$, i.e. an overgroup $S_N \supseteq M$, and only then do we have a three point cover for which we seek an equation. The equations we have been finding are rather complicated, because they reflect not only the

fundamental datum (A, B, C), but also the choice of S_N. Accordingly, even though solutions to (1.1) come in very regularly behaving families, we have had to work one cover at a time.

In this section, we are in the very exceptional situation where the monodromy group is closely related to a symmetric group. We work with two positive integer parameters $N > m$, and the construction is uniform in these parameters. Throughout, we take $r = N - m$.

$$\begin{aligned} u_{N,m}(x) &= (x^N - 1)/(x - 1) \\ w_{N,m}(x) &= (x^m - 1)(x^r - 1)/(x - 1) \\ \Lambda_{N,m} &= (N,\ 2\,1^{N-2},\ mr) \\ f_{N,m}(t, x) &= m^m x^N - t(Nx - r)^m \\ D_{N,m}(t) &= (-1)^{(N+2m)(N+1)/2} N^N (mr)^{(N-1)m} t^{N-1}(t - 1). \end{aligned}$$

The cover $X_{N,m}$ is isomorphic to the cover $X_{N,r}$, an isomorphism being $x \mapsto mx/(Nx - r)$. So, without loss of generality, we restrict to the case $m \leq N/2$. We assume further that N and m are relatively prime, so as to make $u_{N,m}(x)$ and $w_{N,m}(x)$ relatively prime and hence (1.6)-(1.8) irreducible. In this case, the monodromy group $M_{N,m}$ and the Galois group $G_{N,m}$ are both the full symmetric group S_N.

For $m = 1$, the polynomial $f_{N,m}$ is a trinomial and these covers have been discussed in e.g. [**Mat**, Section II.3]. As we explain next, even the other covers $X_{N,m}$ can be given by trinomial equations, and in this guise they have appeared in many places. Define integers v and w by

$$\begin{aligned} v &\in \{0, 1, \ldots, r - 1\} \\ Nv &\equiv 1 \bmod (r) \\ w &= (Nv - 1)/r. \end{aligned}$$

Define

$$y = \left(\frac{m}{Nx - r}\right)^{w-v} x^w \in \mathbb{Q}(x).$$

One has

$$y^m = t^{w-v} x \in \mathbb{Q}(x)$$

and y is a root of

$$f^*_{N,m}(t, y) = my^N - Nt^v y^m + rt^w.$$

In summary, we have two defining polynomials for the same cover, the canonical one $f_{N,m}$ and a trinomial version $f^*_{N,m}$. We use $f^*_{N,m}$ exclusively in the sequel. We mention $f_{N,m}$ because this is the cover given by the standard three point cover algorithm sketched in Section 5: x is a coordinate on $X_{N,m}$ while y is a rational function in x, typically of degree > 1. The general trinomial $ax^N + bx^m + c$ fits in this situation via $t = (m/a)^m (b/N)^N (r/c)^r$. Thus we call the $X_{N,m}$ trinomial covers.

The bad reduction set $S_{N,m}$ is the set of primes dividing Nmr; in other words, $X_{N,m}$ has bad reduction within S iff $N/m \in T_{\infty,\infty,\infty}(\mathbb{Z}^S)$. In particular, $S_{N,m} \subseteq \{2, 3\}$ exactly for the four pairs $(N, m) = (2, 1)$, $(3, 1)$, $(4, 1)$, and $(9, 1)$. For comparison, we note that specializing $f_{3,1}$ just at $T^*_{\infty,2,\infty}$ already yields all 9 A_3/S_3 cubics. Similarly, specializing $f_{4,1}$ just at $T^*_{\infty,2,\infty}$ already yields all 23

A_4/S_4 quartics, except the unique totally real one; in fact, no specialization of $f_{4,1}$ is totally real.

We are interested here in the case $(N, m) = (9, 1)$, coming from the Catalan equation $2^3+1 = 3^2$. Here a Frobenius computation shows that nothing unexpected happens when one specializes t to τ in the 35-element set $T^*_{8,2,9} = T^*_{\infty,2,\infty}$. One gets 10 fields with Galois group A_9 and 25 with Galois group S_9. The absolute field discriminants 2^a3^b are mostly near the maximum possible $2^{31}3^{26}$, with $12 \le a \le 31$ and $12 \le b \le 26$ being the exact ranges. [**LNV**] lets one understand a and b in terms of the 2-adic and 3-adic placement of τ, respectively.

In general, suppose $X \to \mathbb{P}^1_{\mathbb{Q}}$ is a three point cover with defining equation $f(t, x)$. It makes sense to specialize t to one of the cuspidal points $c = 0$, 1, and ∞ as well, to obtain a Galois field $K_c \subset \mathbb{C}$. Let Norm_c be the normalizer of the monodromy transformation m_c in G. Then $\mathrm{Gal}(K_c/\mathbb{Q})$ is contained in $\mathrm{Norm}_c/\langle m_c\rangle$.

For the covers $X_{N,m}$ of this section, the most interesting cusp to specialize at is $c = 1$. The Galois group $G_{N,m,1}$ is contained in a symmetric group S_{N-2}. These fields $K_{N,m,1} \subset \mathbb{C}$ have been studied in [**Bor**]. In our example, one has

$$f_{9,1}(1, x) = (x - 1)^2(x^7 + 2x^6 + 3x^5 + 4x^4 + 5x^3 + 6x^2 + 7x + 8).$$

The septic field defined by the degree seven factor has Galois group S_7 and discriminant $-2^{12}3^{10}$. In general, cuspidal specializations seem worthy of special attention. First, they depend only on the group-theoretic data defining the cover from which they come. Second, they serve as an aid in understanding non-cuspidal specializations which are p-adically near the cusp.

11. $W(E_7)'$; computing lower degree resolvents

Here we use the following new cover with $M = G = W(E_7)' = Sp_6(2)$:

$$\begin{aligned}
u_{28b} &= (x^6 - x^3 + 1)(x + 1)\\
w_{28b} &= (x^4 - x^2 + 1)(x^2 + x + 1)(x - 1)\\
\Lambda_{28b} &= (12C, 2A, 9A) \to (12^2\,3\,1,\ 2^6\,1^{16},\ 9^3\,1)\\
f_{28b}(t, x) &= 3^6\,(x^2 + 6\,x + 6)^{12}x^3(3\,x + 4) - t\,2^{18}\,(x^3 + 3\,x^2 - 3)^9\\
D_{28b}(t) &= 2^{540}3^{450}t^{24}(t - 1)^6.
\end{aligned}$$

Here x, as a multivalued function of t, can be expressed in terms of hypergeometric functions with finite monodromy, as this cover corresponds to Entry 58 of the Beukers-Heckman list [**BH**, page 353].

We specialize to τ in the 35-element set $T^*_{12,2,9} = T^*_{\infty,2,\infty}$. A Frobenius computation proves that for $\tau \ne -1$ the algebras $L_{28b,\tau}$ all have Galois group all of $Sp_6(2)$. At $\tau = -1$, there is an apparent group-drop to $S_8 \cong SO^+_6(2) \subset Sp_6(2)$. The rest of this section explains how we produce a degree eight polynomial with the same splitting field as $f_{28b}(-1, x)$, thereby proving that indeed $G_{28b,-1} \cong S_8$.

In general, suppose given an irreducible degree 28 polynomial f over $\mathbb{Q}$ with Galois group S_8 or $W(E_7)'$. For each bijection

$$\begin{aligned}
L = (\text{Two element subsets of } \{0,\dots,7\}) &\to \text{Complex roots of f}\\
\{i, j\} &\to \alpha_{L(i,j)},
\end{aligned}$$

one has an octic polynomial

$$g_L(x) = \prod_{i=1}^{8}(x - \sum_{j\neq i} \alpha_{L(i,j)}).$$

Assuming f is sufficiently generic, one gets $28!/8! \approx 7.5 \times 10^{24}$ distinct octic polynomials. If the Galois group is S_8, then exactly one of these has coefficients in $\mathbb{Q}$, it being the desired polynomial.

Suppose now that f has exactly four real roots so that the desired octic has two real roots. Then it suffices to consider bijections L where the involution -1 acting on $\mathbb{Z}/8$ goes over to complex conjugation. Then one gets $(4!24!!)/(2!3!2^3) \approx 4.9 \times 10^{11}$ octic polynomials. So still this method for finding a resolvent octic is impractical.

In our case, however, we have an action of $W(E_7)' \subset S_{28}$ on the roots of $f_{28b}(-1,x)$ and the desired g_L is among the thirty-six g_L coming from the thirty-six subgroups of $W(E_7)'$ isomorphic to S_8. Using monodromy techniques as described in Section 9, we can identify these 36 copies of S_8. Looking among only these, we find a labeling L giving a desired g with quite large coefficients. Applying *polredabs*, gives

$$g_8(x) = x^8 + 4x^7 + 8x^6 + 16x^5 + 22x^4 + 20x^3 + 10x^2 - 8x - 10, \tag{11.1}$$

with field discriminant $-2^{17}3^9$.

To prove rigorously that $f_{28b}(-1,x)$ and $g_8(x)$ have the same splitting field, we proceed again as in Section 9. Write

$$\begin{aligned} g_8(x) &= \prod_{\alpha\in A'}(x-\alpha) \\ g_{28}(x) &= \prod_{\{\alpha_1,\alpha_2\}\subset A'}(x-\alpha_1-\alpha_2) \\ f_{28b}(-1,x) &= 3^7\prod_{\beta\in B}(x-\beta). \end{aligned}$$

We need to numerically find the right bijection σ from $A = \mathrm{Sub}_2(A')$ to B, and then algebraically confirm that one indeed gets an isomorphism from $\mathbb{Q}[x]/g_{28}(x)$ to $\mathbb{Q}[y]/f_{28b}(-1,y)$. This unique correct bijection is indicated on the following chart, with the root-labeling convention of Section 9:

	1	2a	2b	3a	3b	4a	4b	5
1		11b	11a	13a	13b	10a	10b	2
2a			15	5b	14b	12b	7b	16a
2b				14a	5a	7a	12a	16b
3a					9	4a	8a	3b
3b						8b	4b	3a
4a							1	6a
4b								6b
5								

Thus, for example, $\{\alpha_1,\alpha_2\} = \{1, 2a\} \in A$ matches $11b \in B$. Our computation and confirmation of the resolvents (9.1), (9.2), (9.3), (9.4) were each of similar complexity.

12. S_{32}; prime-dropping specialization

Let $f(t,x) \in \mathbb{Q}[t,x]$ define a degree N three point cover, with bad reduction set S'. For $\tau \in \mathbb{Q} - \{0,1\}$ it may happen that the specialized algebra L_τ is ramified strictly within S'. Then we call τ a prime-dropping specialization point for f. Our experience suggests that such prime-dropping specialization points are quite rare. Here we report on three related instances of this phenomenon.

Consider again the trinomial covers $X_{N,m}$ of Section 10, with $r := N-m$. Recall that the specialized algebra is given by a trinomial equation: $L_\tau = \mathbb{Q}[x]/f^*_{N,m}(\tau,x)$. Recall also that the cover has bad reduction at all primes dividing Nmr. Nonetheless, one has the following fact, i being any positive integer:

$$\text{If } p^e || \begin{cases} N \\ m \\ r \end{cases} \text{ and } \tau \in \begin{cases} T(\mathbb{Q}_p)^{0,Nei} \\ T(\mathbb{Q}_p)^{\infty,mei} \\ T(\mathbb{Q}_p)^{\infty,rei} \end{cases} \text{ then } K_{N,m,\tau} \text{ is unramified at } p \tag{12.1}$$

This fact can be proved directly: for suitable rational numbers a and b, one has $af^*_{N,m}(\tau, bx) \in \mathbb{Z}[x]$, with polynomial discriminant prime to p, as in (12.2), (12.3), and (12.4) below. Alternatively, this fact is a special case of the main theorem of [**LNV**].

We found three new fields this way with $S = \{2,3\}$. All three fields come from the specialization point $\tau = 2 \cdot 5^5/3^2$, associated to the ABC triple

$$-2 \cdot 5^5 + 79^2 + 3^2 = 0.$$

The fields come from the covers

$$\begin{aligned} f^*_{8,3}(t,x) &= 3x^8 - 8t^2x^3 + 5t^3 \\ f^*_{9,4}(t,x) &= 4x^9 - 9t^4x^4 + 5t^7 \\ f^*_{32,5}(t,x) &= 5x^{32} - 32t^{11}x^5 + 27t^{13}. \end{aligned}$$

Nice defining polynomials for the number fields are as follows.

$$3^7 5^{-16} f^*_{8,3}(2 \cdot 5^5/3^2, -5^2x/3) = x^8 + 2^5x^3 + 2^3 3 \tag{12.2}$$

$$2^{-2} 3^{18} 5^{-36} f^*_{9,4}(2 \cdot 5^5/3^2, 5^4x/3^2) = x^9 - 2^2 3^4 x^4 + 2^5 3^4 \tag{12.3}$$

$$3^{32} 5^{65} f^*_{32,5}(2 \cdot 5^5/3^2, -5^2x/3) = x^{32} + 2^{16} 3^5 x^5 + 2^{13} 3^9. \tag{12.4}$$

The polynomial discriminants are $-2^{45}3^5 79^2$, $-2^{40}3^{48}79^2$, and $-2^{563}3^{277}79^2$, respectively. The field discriminants are $-2^{31}3^5$, $-2^{14}3^{24}$, and $-2^{191}3^{111}$, respectively. Here, in the degree 32 case, we used [**LNV**] to compute the exponents 191 and 111. Note that the maximal absolute discriminant allowed by local considerations in the last case is $2^{191}3^{112}$.

In all three cases, the fact that 79 does not divide the field discriminant d can be seen directly from the polynomial, rather than by our usual appeal to (3.4). Namely, each polynomial factors in the form $f_{N-2}f_1^2$ over $\mathbb{F}_{79}$, with f_{N-2} separable. This implies that $\mathrm{ord}_{79}(d) \in \{0,1\}$. However from the polynomial discriminant we know that $\mathrm{ord}_{79}(d) \in \{0,2\}$.

References

[Ash] A. Ash, Galois representations and cohomology of $GL(n,\mathbb{Z})$, Séminaire de Théorie des Nombres, Paris, 1989-90, Prog. Math, **102** (1992), 9–22.

[Atlas] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An atlas of finite groups.* Oxford University Press, (1985).

[BH] F. Beukers and G. Heckman, *Monodromy for the hypergeometric function* ${}_nF_{n-1}$. Inv. Math. **95** (1989) 325–354.
[Beu] F. Beukers, *The diophantine equation* $Ax^p + By^q = Cz^r$. Duke Math J., **91** (1998) 61–88.
[Bir] B. Birch, *Noncongruence subgroups, covers and drawings.* In [**Sch**], 25–46.
[Bor] A. Borisov, *On some polynomials allegedly related to the abc conjecture.* Acta Arith. **84** (1998), 109–128.
[Buh] J. P. Buhler, ed., *Algorithmic number theory (ANTS-III).* Springer Lect. Notes in Comp. Sci., **1423** (1998).
[Cog] F. B. Coghlan, *Elliptic curves with conductor* $N = 2^a3^b$. Ph. D. Thesis, Manchester University, 1967. Tables published in: Modular functions of one variable IV. Springer Lect. Notes in Math. **476** (1975), 123–134.
[Dar] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation.* C. R. Math. Rep. Acad. Sci. Canada **19** (1997), 3–14.
[DG] H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$. Bull. London Math Soc. **27** (1995), 513–543.
[Elk] N. D. Elkies, *Shimura curve computations.* In [**Buh**], 1–47.
[Gro] B. H. Gross, *Modular forms (mod p) and Galois representations.* Internat. Math. Res. Notices 1998, no. 16, 865–875.
[Häf] F. Häfner, *Einige orthogonale und symplektische Gruppen als Galoisgruppen über* $\mathbb{Q}$. Math. Ann. **292** (1992), no. 4, 587–618.
[JR1] J. W. Jones and D. P. Roberts, *Sextic number fields with discriminant* $-^j2^a3^b$. Number Theory (Ottawa, ON, 1996). CRM Proc. Lecture Notes **19** (1999) 141–172.
[JR2] ———, *Timing analysis of targeted Hunter searches.* In [**Buh**], 412-423.
[JR3] ———, *Septic number fields with discriminant* $\pm 2^a3^b$, Math. Comp. **72** (2003), no. 244, 1975–1985.
[Kat] N. M. Katz, *Rigid local systems.* Annals of Mathematics Study 138, Princeton University Press (1996).
[LNV] P. Llorente, E. Nart, and N. Vila, *Discriminants of number fields defined by trinomials.* Acta Arith. XLIII (1984), 367–373.
[Mal1] G. Malle, *Polynomials for primitive nonsolvable permutation groups of degree* $d \leq 15$. J. Symbolic Comput. **4** (1987), 83–92.
[Mal2] ———, *Polynomials with Galois groups* $\mathrm{Aut}(M_{22})$, M_{22}, *and* $PSL_3(\mathbb{F}_4).2_2$ *over* $\mathbb{Q}$. Math. Comp. **51** (1988), no. 184, 761–768.
[MM] G. Malle and B. H. Matzat, *Inverse Galois theory.* Springer Monographs in Mathematics, 1999.
[Mat] B. H. Matzat, *Konstructive Galoistheorie.* Springer Lect. Notes in Math. **1284** (1987).
[McK] J. McKee, *Computing division polynomials*, Math. Comp. **63** 208 (1994) 767–771.
[Odl] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators, and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux, **2** (1990), no. 1, 119–141
[Rob1] D. P. Roberts, *Twin sextic algebras.* Rocky Mountain J. Math **28** (1998), no. 1, 341–368.
[Rob2] ———, *Rigid Jordan tuples*, submitted.
[Sch] L. Schneps, ed., *The Grothendieck Theory of Dessins d'Enfants.* London Math. Soc. Lecture Notes **200** (1994).
[Ser1] J.-P. Serre with H. Darmon, *Topics in Galois theory.* Jones and Bartlett Publishers (1992).
[Ser2] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. **54** (1987), 179–230.
[Tak] K. Takeuchi, *Commensurability classes of arithmetic triangle groups.* J. Fac. Sci. Univ. Tokyo Sect. 1A Math. **24** (1977) 201–212.
[Völ] H. Völklein, *Groups as Galois groups, an introduction.* Cambridge Studies in Advanced Mathematics **53**, Cambridge University Press (1996).

Division of Science and Mathematics, University of Minnesota-Morris, Morris, Minnesota, 56267
URL: `http://cda.mrs.umn.edu/~roberts/`
E-mail address: `roberts@mrs.umn.edu`