Arithmetically exceptional functions and elliptic curves

Peter Müller *

August 16, 1999

Abstract

Let $f(X) \in \mathbb{Q}(X)$ be a rational function. For almost all primes p we can reduce the coefficients of f and consider $f_p := f \mod p$ as a function on the projective line $\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$. Here we continue the arithmetic aspects of joint work with Guralnick and Saxl, and classify the functions f such that f_p is a bijection for infinitely many primes p. This is the rational function analog of the classical conjecture of Schur (1923), solved by Fried (1970), which considered the case that f is a polynomial.

Thereby we also answer a question of J. G. Thompson about the minimal field of definition of a certain rational function of degree 25.

1 Introduction

A classical problem going back to Schur [Sch23] is the following: Let $f(X) \in \mathbb{Z}[X]$ be a polynomial, which induces a permutation of the residue fields $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes. Then Schur conjectured (and proved this for prime degree polynomials) that f is a composition of linear polynomials and Dickson polynomials $D_k(a, X)$, which are best defined implicitly by $D_k(a, Z + a/Z) = Z^k + (a/Z)^k$ for $a \in \mathbb{Q}$. Schur's conjecture has been proved by M. Fried in [Fri70], see also [Tur95] and [Mül97]. The obvious generalization of this question to number fields poses no difficulties, result and proof are the same.

*Supported by the DFG.

In recent joint work [GMS97] with R. Guralnick and J. Saxl we investigated the rational function analog of this question over number fields K. Let $f(X) \in K(X)$ be a rational function, and $\mathcal{O}_k$ be the ring of integers of K. Fix coprime polynomials $r, s \in \mathcal{O}_k[X]$ with $f = r/s$. The coefficients of $f = r/s$ can be reduced modulo all but finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$ without making s trivial. Such a reduced function induces a map on the projective line $\mathbb{P}^1(\mathcal{O}_k/\mathfrak{p})$. We say that f is *arithmetically exceptional* if this induced map is bijective for infinitely many prime ideals $\mathfrak{p}$.

It follows from this definition that if an arithmetically exceptional function is a composition $a(b(X))$ of two rational functions $a, b \in K(X)$, then a, b are also arithmetically exceptional. (In contrast to the polynomial case, the converse does not hold even over $\mathbb{Q}$, see [GMS97, Corollary 7.4].) So we can and do restrict to indecomposable functions. Define the degree of $f \in K(X)$ to be the maximum of the degrees of numerator and denominator in a reduced fraction. The degree is the same as the degree of the field extension $K(X)/K(f(X))$.

The aim of this paper is to classify the arithmetically exceptional functions over $\mathbb{Q}$. This also answers a question of J. Thompson [Tho90] raised in a different context.

The classification is in terms of the geometric monodromy group and the branching type. Let f be such a function, then $\mathrm{Gal}(f(X) - t/\mathbb{C}(t))$ is the geometric monodromy group of f, where $\mathrm{Gal}(f(X) - t/\mathbb{C}(t))$ denotes the Galois group of $R(X) - tS(X)$ over $\mathbb{C}(t)$, when $f = R/S$ is a reduced fraction of polynomials. Further, for the finitely many points $b_1, \ldots, b_r \in \mathbb{C} \cup \{\infty\}$ with $|f^{-1}(b)| < n = \deg f$ let m_i be the least common multiple of the multiplicities of the points in the fiber $f^{-1}(b_i)$. Then $(m_1, \ldots, m_r)$ is the branching type of f. The type, together with the geometric monodromy group, usually gives precise information about the function f. See Section 3 for more details; in particular the numbers m_i will be seen as the orders of the elements of a very specific generating system of $\mathrm{Gal}(f(X) - t/\mathbb{C}(t))$. The result, which completes work from [GMS97], is

Theorem 1.1. *Let $f \in \mathbb{Q}(X)$ be an indecomposable rational function of degree n which is arithmetically exceptional over $\mathbb{Q}$. Set $G := \mathrm{Gal}(f(X) - t/\mathbb{C}(t))$. Then one of the following holds, where p is an odd prime and C_m denotes a cyclic group of order m.*

(a) $n = p$, G is cyclic of type (p, p);

(b) $n = p \geq 5$, *G is dihedral of type* $(2, 2, p)$;

(c) $n = 4$, $G = C_2 \times C_2$ *of type* $(2, 2, 2)$;

(d) $n = p \in \{5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$, *$G$ is dihedral of type* $(2, 2, 2, 2)$;

(e) $n = p^2$, $G = (C_p \times C_p) \rtimes C_2$ *of type* $(2, 2, 2, 2)$;

(f) $n = 5^2$, $G = (C_5 \times C_5) \rtimes S_3$ *of type* $(2, 3, 10)$;

(g) $n = 5^2$, $G = (C_5 \times C_5) \rtimes (C_6 \rtimes C_2)$ *of type* $(2, 2, 2, 3)$;

(h) $n = 3^2$, $G = (C_3 \times C_3) \rtimes (C_4 \rtimes C_2)$ *of types* $(2, 2, 2, 4)$ *and* $(2, 2, 2, 2, 2)$;

(i) $n = 28$, $G = \mathrm{PSL}_2(8)$ *of types* $(2, 3, 7)$, $(2, 3, 9)$, *and* $(2, 2, 2, 3)$;

(j) $n = 45$, $G = \mathrm{PSL}_2(9)$ *of type* $(2, 4, 5)$;

While dealing with the arithmetic of case (g) above, we solve a question raised by John G. Thompson [Tho90] about the minimal field of definition of a certain rational function of degree 25.

Acknowledgment. I thank G. Malle and B. H. Matzat for a careful reading of the manuscript.

2 Arithmetically exceptional rational functions

Let B be a finite permutation group on Ω, and $G \trianglelefteq B$ be a transitive, normal subgroup. We say that the pair (B, G) is exceptional, if none of the orbits $\neq \{\omega\}$ of a point stabilizer G_ω is fixed by B_ω. (This is of course independent of the chosen point $\omega \in \Omega$.) This notion of exceptionality has first appeared in arithmetic questions of finite fields, see [FGS93] and the literature given there.

If the finite group A is acting on Ω, and $G \trianglelefteq A$ is transitive, then we say that (A, G) is *arithmetically exceptional*, if there is a group B with $G \leq B \leq A$, such that (B, G) is exceptional and B/G is cyclic.

Now fix a number field K, and let $f \in K(X)$ be a non–constant rational function. Let t be a transcendental over K, and let L be a splitting field of

$f(X)-t$ over the rational function field $K(t)$. Denote by $\hat{K}$ the algebraic closure of K in L. Then $A := \mathrm{Gal}(L/K(t))$ is called the *arithmetic monodromy group* of f, and $G := \mathrm{Gal}(L/\hat{K}(t))$ is called the *geometric monodromy group* of f. Except otherwise said, we regard A and G as permutation groups on the roots of $f(X) - t$. We call $\hat{K}$ the *field of constants* of f. Note that $A/G = \mathrm{Gal}(\hat{K}/K)$.

The following group–theoretic characterization of arithmetically exceptional functions is due to Fried [Fri78], see [GMS97, Theorem 2.1] for a short proof.

Theorem 2.1. *Let f, A, and G be as above. Then f is arithmetically exceptional if and only if the pair (A, G) is arithmetically exceptional.*

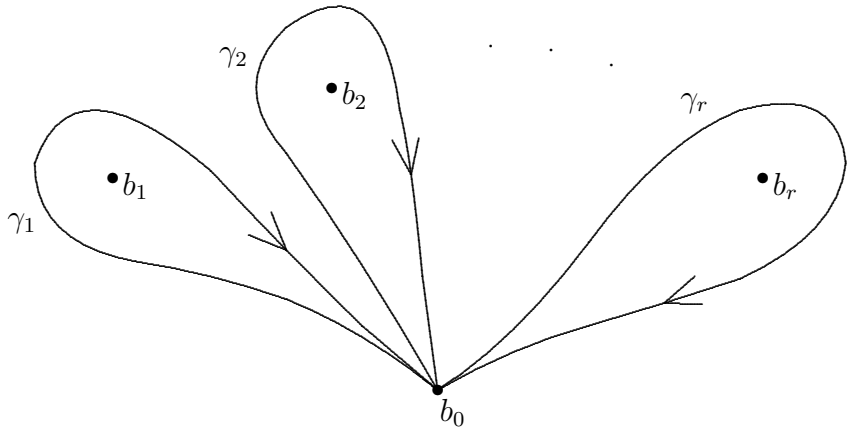
Remark 2.2. The proof of this theorem in [GMS97] also characterizes the prime ideals $\mathfrak{p}$ modulo which the function f is bijective if it is arithmetically exceptional. Namely there is a bound C such that if $|\mathcal{O}_k/\mathfrak{p}| > C$, then such an f is bijective modulo $\mathfrak{p}$ if and only if (B, G) is exceptional, where B/G is the decomposition group of a prime of $\hat{K}$ lying above $\mathfrak{p}$.

3 Branch cycle descriptions in geometric monodromy groups

Let $\mathbb{P}^1 = \mathbb{P}^1(\mathbb{C})$ be the Riemann sphere over the complex numbers. We keep the notation from the previous subsection, and regard now f as a covering map from $\mathbb{P}^1$ to $\mathbb{P}^1$. Let n be the degree of f. There is a finite set $\mathcal{B} := \{b_1, b_2, \ldots, b_r\} \subset \mathbb{P}^1$ of elements with less than n preimages. We call these elements the *branch points* of f.

Fix a base point $b_0 \in \mathbb{P}^1 \setminus \mathcal{B}$, and denote by π the fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathcal{B}, b_0)$. Then π acts transitively on the points of the fiber $f^{-1}(b_0)$ by lifting of paths. Fix a numbering $1, 2, \ldots, n$ of this fiber. Thus we get a homomorphism $\pi \to \mathrm{Sym}_n$. By standard arguments (see [MM] or [Völ96]), the image of π can be identified with the geometric monodromy group G defined above, thus we write G for this group too.

This identification has a combinatorial consequence. Choose a standard homotopy basis of $\mathbb{P}^1 \setminus \mathcal{B}$ as follows. Let γ_i be represented by paths which wind once around b_i clockwise, and around no other branch point, such that $\gamma_1\gamma_2\cdots\gamma_r = 1$. Then $\gamma_1, \gamma_2, \ldots, \gamma_{r-1}$ freely generate π.



Definition 3.1. Let $\sigma \in \mathrm{Sym}_n$. Then the index $\mathrm{ind}(\sigma)$ is defined to be n minus the number of cycles in σ (where fixed points count as cycles too).

Let σ_i be the image of γ_i in Sym_n. If the points $s_1, \ldots, s_m$ in the fiber of b_i have multiplicities $e_1, \ldots, e_m$, respectively, then σ_i has cycle lengths $e_1, \ldots, e_m$. We say that σ_i has *cycle type* $1^{a_1}2^{a_2}\cdots$, where a_i is the number of cycle lengths i. Note that $\mathrm{ind}(\sigma_i) = n - |f^{-1}(b_i)| = n - m$.

The Riemann–Hurwitz genus formula (or a more elementary argument using the derivative of f) gives the following basic relation:

$$\sum_i \mathrm{ind}(\sigma_i) = 2(n-1) \tag{1}$$

We call the r–tuple $(\sigma_1, \sigma_2, \ldots, \sigma_r)$ a *branch cycle description* of G, and the unordered tuple $(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_r|)$ the *branching type* of the branch cycle description. Of course the orders of the σ_i do not specify the σ_i, but in most cases where G is fixed the branching types distinguish between the various possibilities for f.

Note that one can arbitrarily order the conjugacy classes of the σ_i using an iteration of the elementary braiding operations Q_i, $i = 1, \ldots, r-1$, which send the tuple $(g_1, g_2, \ldots, g_r)$ to $(g_1, \ldots, g_{i-1}, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, g_{i+2}, \ldots, g_r)$.

The elements σ_i can also be seen as inertia group generators in a slightly more general context. Let K be a field of characteristic 0, and $L/K(t)$ be a regular (i.e. K is algebraically closed in L) finite Galois extension with group

G. For each ramified place $P_i : t \mapsto b_i$ (or $1/t \mapsto 0$ if $b_i = \infty$) let σ_i be a generator of an inertia group of a place of L lying above P_i. There is a natural choice of σ_i up to conjugacy. Namely set $y := t - b_i$ (or $y := 1/t$ if $b_i = \infty$). There is a minimal integer e such that L embeds into the power series field $\overline{\mathbb{Q}}((y^{1/e}))$. For such an embedding, let σ_i be the restriction to L of the automorphism of $\overline{\mathbb{Q}}((y^{1/e}))$ which is the identity on the coefficients and maps $y^{1/e}$ to $y^{1/e}\exp(2\pi\sqrt{-1}/e)$. The non–uniqueness of the embedding of L accounts for the fact that such σ_i are well–defined only up to conjugacy. We call the conjugacy class of σ_i the *distinguished conjugacy class* associated to b_i.

Let E be a field between $K(t)$ and L, and let $\mathrm{ind}(\sigma_i)$ refer to the permutation action of G on the conjugates of a primitive element of $E/K(t)$. Then the genus g of E is given by

$$\sum_i \mathrm{ind}(\sigma_i) = 2([E : K(t)] - 1 + g). \tag{2}$$

The well–known deficiency of this purely algebraic setup is the following: Even for $K = \mathbb{C}$ there is no known algebraic proof that the σ_i can be chosen with $\sigma_1\sigma_2\cdots\sigma_r = 1$ and $G = <\sigma_1, \sigma_2, \ldots, \sigma_r>$.

Subsequently, we will call a place (or branch point) K–rational (or simply rational if $K = \mathbb{Q}$) if $b_i \in K \cup \{\infty\}$.

Sometimes one can read off from the branch cycle description whether the function f is defined over certain fields using the so called branch cycle argument, see [Völ96, 2.8] for a fuller version. Let G be a subgroup of A. We call an element $x \in G$ rational in A, if all powers σ^m with m prime to $|G|$ are conjugate to σ in A. Also, we call a conjugacy class of G rational in A, if it consists of elements rational in A.

Theorem 3.2. *Let K be a field of characteristic 0, and $L/K(t)$ be a finite Galois extension with group A. Set $n = [L\bar{K} : \bar{K}(t)]$. Then $\alpha \in \mathrm{Gal}(L\bar{K}/K(t))$ permutes the branch points of $L\bar{K}/\bar{K}(t)$ among themselves. Let ζ_n be a primitive n–th root of 1, and m be an integer with $\alpha^{-1}(\zeta) = \zeta^m$. Let $\mathcal{C}_b$ be the distinguished conjugacy class of inertia generators associated to the place b of $\bar{K}(t)$. Then $\mathcal{C}_{\alpha(b)} = \alpha^\star(\mathcal{C}_b)^m$, where $\alpha^\star$ is the conjugation map $g \mapsto \alpha g \alpha^{-1}$ on G.*

In particular, if b is K–rational, then the class $\mathcal{C}_b$ is rational in A.

A typical application is the following. Suppose $f \in \mathbb{Q}(X)$. Then the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ permutes the branch points, but also preserves

their cycle types. So if there is a branch point whose cycle type appears only once, then it must be rational. If the associated element σ_i is not rational in G, then necessarily $A > G$.

4 Monodromy groups of arithmetically exceptional functions

The main group–theoretic result from [GMS97] is the following:

Theorem 4.1. *Let A be a primitive permutation group of degree n and G be a normal subgroup such that (A, G) is arithmetically exceptional. Further suppose that G has a generating system $\sigma_1, \sigma_2, \ldots, \sigma_r$ with $\sigma_1\sigma_2\cdots\sigma_r = 1$ and $\sum \mathrm{ind}(\sigma_i) = 2(n-1)$. Then one of the following holds, where type means the branching type of the generating system.*

(I) $n = p^e$ for a prime p, $A \leq N \rtimes \mathrm{GL}_e(p)$ with $N = \mathbb{F}_p^e$ is an affine group, and one of the following holds:

- *(a) (i) $n = p \geq 3$, G is cyclic of type (p, p); or*
  - *(ii) $n = p \geq 5$, G is dihedral of type $(2, 2, p)$; or*
  - *(iii) $n = 4$, $G = C_2 \times C_2$ of type $(2, 2, 2)$, $A = A_4$ or S_4.*
- *(b) $n = p$ or $n = p^2$ for p odd, and*
  - *(i) G is of type $(2, 2, 2, 2)$, $G = N \rtimes C_2$, and $n \geq 5$; or*
  - *(ii) G is of type $(2, 3, 6)$, $G = N \rtimes C_6$, and $n \equiv 1 \pmod 6$; or*
  - *(iii) G is of type $(3, 3, 3)$, $G = N \rtimes C_3$, and $n \equiv 1 \pmod 6$; or*
  - *(iv) G is of type $(2, 4, 4)$, $G = N \rtimes C_4$, and $n \equiv 1 \pmod 4$.*
- *(c) (i) $n = 11^2$, G is of type $(2, 3, 8)$, $G/N \cong \mathrm{GL}_2(3)$ and $A = \mathrm{A\Gamma L}_1(11^2)$; or*
  - *(ii) $n = 5^2$, G is of type $(2, 3, 10)$, $G/N = S_3$ and $A/N \cong S_3 \times C_4$; or*
  - *(iii) $n = 5^2$, G is of type $(2, 2, 2, 4)$, G/N is a Sylow 2-subgroup of the subgroup of index 2 in $\mathrm{GL}_2(5)$, and A/G has order 3 or 6; or*
  - *(iv) $n = 5^2$, G is of type $(2, 2, 2, 3)$, $G/N = C_6 \rtimes C_2$ and A/G is cyclic of order 2 or 4; or*

(v) $n = 3^2$, *G is of type* $(2,4,6)$, $(2,2,2,4)$, $(2,2,2,6)$, *or* $(2,2,2,2,2)$, $G/N = C_4 \rtimes C_2$ *and* A/G *has order* 2*; or*

(vi) $n = 2^4$, *G is of type* $(2,4,5)$ *or* $(2,2,2,4)$, $G/N = C_5 \rtimes C_2$, *and* A/G *has order* 3 *or* 6.

(II) *(a)* $n = 28$, $G = \mathrm{PSL}_2(8)$ *is of type* $(2,3,7)$, $(2,3,9)$, *or* $(2,2,2,3)$, *and* $A = \mathrm{P\Gamma L}_2(8)$.

(b) $n = 45$, $G = \mathrm{PSL}_2(9)$ *is of type* $(2,4,5)$, *and either* $A = \mathrm{M}_{10}$, *or* $A = \mathrm{P\Gamma L}_2(9)$.

If we take a group G and a branch cycle description from this theorem, then Riemann's existence theorem implies the existence of a rational function over some number field K with G as geometric monodromy group, and branching given by the branch cycle description. However, two difficult arithmetic problems are left. First, it is not clear how small we may take K, in particular whether we may take $K = \mathbb{Q}$. This is the descent problem encountered in the inverse Galois problem. Secondly, it is difficult to get a hold on the arithmetic monodromy group A once we have fixed K and $f(X) \in K(X)$. So after having done all the group–theoretic work yielding the above theorem, the question remains whether there are indeed arithmetically exceptional functions with the data in the theorem.

The cases in (II) have been dealt with in [GMS97, Section 6] using variants of the rational rigidity theorem, and they are shown to appear over $\mathbb{Q}$. The cases (I)(a)(i) and (I)(a)(ii) are very easy to deal with, and basically lead to cyclic polynomials X^p and the Rédei functions (see [GMS97, Section 7]) in the first case, and the Dickson polynomials in the second case. Case (I)(a)(iii) appears also over the rationals, with the added feature that if $A = \mathrm{Alt}_4$, then $\hat{\mathbb{Q}}$ can be any cyclic cubic extension of $\mathbb{Q}$.

The four infinite series in (I)(b) are intimately connected with isogenies of elliptic curves. A careful analysis is contained in [GMS97]. We want to remark that, as an alternative to the treatment in [GMS97], one can also use the branch cycle argument Theorem 3.2 to show that the cases (I)(b)(ii), (iii), and (iv) do not occur over the rationals. Section 5 contains information concerning the first of these series, as we will need this setup to decide a question of Thompson.

As to (I)(c): Only (vi) has been shown to not occur at all over any number field K. Case (iv), which is the hardest, will be dealt with in Section 6.

In the following we decide the existence over the rationals in all other cases.

Cases (I)(c)(i) and (I)(c)(iii). In the first case the element of order 8 is not rational in A, and in the second case the element of order 4 is not rational in A, so these cases do not occur by the branch cycle argument Theorem 3.2.

Case (I)(c)(ii). The given tuple $(\sigma_1, \sigma_2, \sigma_3)$ is rigid in G. The elements σ_1 and σ_2 are rational in G, and σ_3 is rational in A. The values of the irreducible characters of G at σ_3 generate the cyclotomic field $K = \mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive 5th root of unity. The rational rigidity criterion thus gives a regular Galois extension $L/K(t)$ with group G and branching data given by the σ_i. The four conjugacy classes in G of elements of order 10 are permuted transitively by $\mathrm{Aut}(G)$, because A already permutes them transitively. Thus L is Galois over $\mathbb{Q}(t)$, see [Völ96, Section 3.1.2]. One obtains that $A = \mathrm{Gal}(L/\mathbb{Q}(t))$. Let U be a subgroup of index 25 in A, and E the fixed field of U. Then $A = GU$, so $E/\mathbb{Q}(t)$ is regular. Further, the Riemann–Hurwitz formula (2) shows that E has genus 0, and is even rational because σ_2 has a unique fixed point, and so E has a rational place. Thus $E = \mathbb{Q}(x)$. Write $t = f(x)$, and f is the desired rational function.

Case (I)(c)(v). Here we have four different kinds of branching types. In the first one of type $(2, 4, 6)$, we obtain that the associated triple of the σ_i is rigid and consists of elements which are rational in G. So the usual rational rigidity criterion shows that we cannot have $A > G$.

Now suppose that we have branching type $(2, 2, 2, 4)$. Here indeed there are arithmetically exceptional functions with this data. It seems to be difficult to exactly write them all down. Instead we give just one example, and show in Appendix A how we got it (and how to possibly get others). Set

$$f(X) = \frac{X(X^4 - 8X^3 + 12X^2 - 48X - 28)^2}{(X^2 - 2)^4}$$

and let $F(X, Y) \in \mathbb{Q}[X, Y]$ be the numerator of $(f(X) - f(Y))/(X - Y)$ as a reduced fraction. One verifies easily that $f(X, 1)$ is irreducible over the rationals ($f(X, 1)$ is irreducible even modulo 3), so $F(X, Y)$ is irreducible over $\mathbb{Q}$, hence the arithmetic monodromy group A of f is doubly transitive. On the other hand, one easily checks that $F(X, Y)$ factors (into two factors of degree 4) over $K := \mathbb{Q}(\sqrt{2})$, so the geometric monodromy group G is

not doubly transitive. There are only 3 doubly transitive groups of degree 9 with a subgroup of index 2 which is not doubly transitive, namely $\mathrm{AGL}_1(9)$, M_9, and $\mathrm{A\Gamma L}_1(9)$. From the branching over ∞ and 0 we see already that G contains elements of cycle types $1^1 4^2$ and $1^1 2^4$. Now let β be a root of $2Z^2 + 88Z + 343$. The numerator of $f(X) - \beta$ factors as $(25X^3 + 16X^2 + 3\beta X^2 + 100X + 56 - 2\beta)(25X^3 - 208X^2 - 14\beta X^2 + 702X + 16\beta X + 112 - 4\beta)^2$, so f has two more branch points, and the inertia generators have cycle type $1^3 2^3$. None of the index 2 subgroups of $\mathrm{AGL}_1(9)$ and M_9 has elements of this type, so we have $A = \mathrm{A\Gamma L}_1(9)$, and the only not doubly transitive subgroup of A containing elements of the previous types is $G = \mathrm{A\Sigma L}_1(9)$.

From this function f we immediately get also a function corresponding to the branching type $(2, 2, 2, 2, 2)$. Namely note that $f(X^2) = g(X)^2$ for $g \in \mathbb{Q}(X)$. It is easy to verify that f and g have the same pairs of arithmetic and geometric monodromy group, and that the branching of g is as claimed.

Next suppose that we have branching type $(2, 2, 2, 6)$. We are going to show that this does not occur. To start with we need

Lemma 4.2. *Let K be a field of characteristic 0, $\mathcal{E}$ be an elliptic curve and $\varphi : \mathcal{C} \to \mathcal{E}$ be a K–rational morphism of finite degree of an algebraic curve $\mathcal{C}$ defined over K of genus 1 to $\mathcal{E}$. Then $\mathcal{C}$ is an elliptic curve.*

Proof. Let J be the jacobian of $\mathcal{C}$, and $\Phi : \mathcal{C} \to J$ be the map such that $\Phi^\gamma \circ \Phi^{-1}$ is the translation map T_γ on J by a point P_γ depending on $\gamma \in \mathrm{Gal}(\bar{K}/K)$. Set $\Psi := \varphi \circ \Phi^{-1} : \mathcal{C} \to \mathcal{E}$. Without loss assume that Ψ maps a fixed K–rational point 0_J to a K–rational point $0_\mathcal{E}$, and that 0_J and $0_\mathcal{E}$ are the zero elements of the respective additions on the elliptic curves. We get

$$\Psi^\gamma \circ T_\gamma = \Psi.$$

So for Q a point on J, we get

$$\Psi(Q) = \Psi^\gamma(Q + P_\gamma) = \Psi^\gamma(Q) + \Psi^\gamma(P_\gamma).$$

But $Q = 0_J$ shows $\Psi^\gamma(P_\gamma) = 0_\mathcal{E}$, hence $\Psi = \Psi^\gamma$ for all $\gamma \in \mathrm{Gal}(\bar{K}/K)$, so Ψ and therefore also Φ is defined over K. □

Now fix a branch cycle description $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ of type $(2, 2, 2, 6)$, and let K be the field of constants. Without loss let ∞ correspond to the element σ_4 of order 6. Two of the involutions, say σ_1 and σ_2, are conjugate in G, whereas σ_3 is not conjugate to them. So the branch point corresponding to

σ_3 first has to be K–rational, but it is even $\mathbb{Q}$–rational for otherwise (by the branch cycle argument) an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ would interchange both points corresponding to σ_1 and σ_2 with the one belonging to σ_3, because σ_1, σ_2, and σ_3 are conjugate in A.

The group A has a subgroup U of index 4 with $A = GU$, so the fixed field of U in L is a regular extension of $\mathbb{Q}(t)$. The action of A on A/U is the dihedral group action, so there is precisely one group W between U and A of index 2 in A. Using the Riemann–Hurwitz genus formula (2) we compute that the fixed fields L_U and L_W of U and W both have genus 1. As ∞ is ramified in $L_W/\mathbb{Q}(t)$, we get that $L_W = \mathbb{Q}(t, x)$, where $x^2 = q(t)$ for a cubic polynomial $q \in \mathbb{Q}[T]$. The zeros of q are the finite branch points of f, so in particular q has a rational root, so the elliptic curve $X^2 = q(T)$ has a rational point of order 2. The inclusion $L_W \subset L_U$ induces a rational morphism of a genus 1 curve with function field L_U to $X^2 = q(T)$ of degree 2. By the preceding lemma, L_U is thus the function field of an elliptic curve. Let (z, v) be a generic point on this curve with equation $z^2 = q'(v)$ for some cubic polynomial q'. Then $L_U = \mathbb{Q}(z, v)$. By the immediate part of [GMS97, Lemma 5.3], the isogeny of degree 2 gives $t = R(v)$, where $R \in \mathbb{Q}(V)$ has degree 2. But then we get the quadratic extension $\mathbb{Q}(v)$ of $\mathbb{Q}(t)$ inside L_U (and different from L_W, for instance because the genus is different), contrary to the fact that W is the unique group properly between U and A.

5 Rational functions with branching type $(2, 2, 2, 2)$

Throughout this section let K be a field of characteristic 0. We call a rational function a $(2, 2, 2, 2)$–function if it has exactly 4 branch points, and branching type $(2, 2, 2, 2)$. The following proposition gives a characterization of indecomposable $(2, 2, 2, 2)$–functions of odd degree. The easy extension to the decomposable case (which we don't need here) is left to the reader.

Proposition 5.1. *Let $f \in K(X)$ be a $(2, 2, 2, 2)$–function of odd degree n which is indecomposable over K. For a transcendental t let $A := \mathrm{Gal}(f(X) - t/K(t))$ and $G := \mathrm{Gal}(f(X) - t/\bar{K}(t))$ be the arithmetic and geometric monodromy group, respectively. Then f has degree p^m with a prime p and $m \in \{1, 2\}$, $A = \mathbb{F}_p^m \rtimes H$ with $H \leq \mathrm{GL}_m(p)$, and $G = \mathbb{F}_p^m \rtimes <-1>$.*

Proof. We have $G = <\sigma_1, \sigma_2, \sigma_3, \sigma_4>$ with inertia generators σ_i of order 2, and $\sigma_1\sigma_2\sigma_3\sigma_4 = 1$. From $\sigma_1\sigma_2 = \sigma_4^{-1}\sigma_3^{-1}$ we see that the σ_i act by inversion on $\sigma_1\sigma_2$. For $i \neq j$ set $T_{i,j} = <\sigma_i\sigma_j>$. We see as before that the σ_k act by inversion on $T_{i,j}$. Note that $T_{1,2} = T_{3,4}$, and so on. Also, $\sigma_1\sigma_2$ commutes with $\sigma_1\sigma_3$. From that we see that the normal subgroup N of G which is generated by the $T_{i,j}$ is abelian and actually generated by $\sigma_1\sigma_2$ and $\sigma_1\sigma_3$. Also, N has index 2 in G, and therefore is transitive (there are at most 2 orbits, they have the same lengths, but the degree is odd.) Note that f indecomposable implies that A is primitive, so every non–trivial normal subgroup of A is transitive. Hence N is even normal in A, for otherwise N would embed into the direct product of the groups G/N^a for a running through A, so N were a 2–group, contrary to odd degree. So N is a minimal and hence elementary abelian p–subgroup of A, which is generated by two elements. Thus A embeds naturally into the affine general linear group $\mathrm{AGL}_m(p)$ for $m = 1$ or 2, and the action of the σ_i on $\mathbb{F}_p^m$ is of the form $x \mapsto -x + t_i$ for $t_i \in \mathbb{F}_p^m$. (Note that by the Riemann–Hurwitz formula (1), each σ_i has exactly one fixed point.) In particular, $G = \mathbb{F}_p^m \rtimes <-1>$. □

Remark 5.2. (A, G) is arithmetically exceptional if and only if H contains an element which has neither 1 nor -1 as eigenvalue.

We now relate the arithmetic monodromy group A to the arithmetic of elliptic curves. For the applications in this paper we need only the case where one of the branch points is K–rational. A linear fractional change of f over K can move this point to infinity, but does not affect A. Thus suppose that ∞ is one of the branch points of f. Also, we may and do assume that the unique simple point in the fiber $f^{-1}(\infty)$ is also ∞. Accordingly, write

$$f(X) = \frac{R(X)}{S(X)^2}$$

with $R, S \in K(X)$, $\deg R = n$, $\deg S = (n-1)/2$. We may assume that R and S are monic. Let λ_i be the 3 finite branch points of f, and μ_i be the simple point in the fiber of λ_i. Set $q_\lambda(X) = (X-\lambda_1)(X-\lambda_2)(X-\lambda_3) \in K[X]$ and $q_\mu(X) = (X-\mu_1)(X-\mu_2)(X-\mu_3) \in K[X]$. We have

$$f(X) - \lambda_i = (X - \mu_i)\frac{Q_i(X)^2}{S(X)^2}$$

for $Q_i(X) \in \bar{K}[X]$. The roots of the monic polynomial $Q_1(X)Q_2(X)Q_3(X)$ are the roots of the monic numerator of the derivative of f, thus

$$Q_1(X)Q_2(X)Q_3(X) = f'(X)S(X)^3,$$

hence

$$q_\lambda(f(X)) = q_\mu(X)f'(X).$$

From that we see that the morphism

$$(x, y) \mapsto (f(x), yf'(x))$$

induces a K–rational isogeny of degree n of the elliptic curve $E_\mu : Y^2 = q_\mu(X)$ to $E_\lambda : Y^2 = q_\lambda(X)$.

The interesting question in this context is the structure of A, or more precisely, the field of constants of f. In [GMS97, Proposition 5.4] we prove that the field of constants is generated over K by the X–coordinates of the finite points in the kernel of ϕ, where $\phi : E_\mu \to E_\lambda$ is the associated isogeny. But these X–coordinates are just the roots of the polynomial S. Hence we get

Proposition 5.3. *Let f be a $(2, 2, 2, 2)$–function as above, and $\hat{K}$ be the algebraic closure of K in a normal closure of $K(x)/K(f(x))$. Then $\hat{K}$ is the splitting field of $S(X)$ over K.*

Note that A_1/G_1 can be naturally identified with $\mathrm{Gal}(\hat{K}/K)$. On the other hand $\mathrm{Gal}(\hat{K}/K)$ acts on the elements of the kernel of ϕ, which is an $\mathbb{F}_p$–space of dimension m, thus $\mathrm{Gal}(\hat{K}/K)$ maps into $\mathrm{GL}_m(p)$. The induced action on the X–coordinates of these kernel elements is just the action of A_1 on $\mathbb{F}_p^m/<-1>$ (this follows from the proof of [GMS97, Proposition 5.4]), so we get the following

Corollary 5.4. *Let f be a $(2, 2, 2, 2)$–function as above. Then f is arithmetically exceptional if and only if* $\mathrm{Gal}(S(X)/K)$ *contains an element which does not fix a root of $S(X)$.*

Remark 5.5. If the degree of f is a prime p (so $m = 1$ in our notation), then the condition on S is easily seen to be equivalent to $S(X)$ having no root in K. For $m = 2$, a typical situation where the condition holds is when $S(X)$ is irreducible over K. Using Hilbert's irreducibility theorem and a theorem of Weber, one can easily construct for each odd p a function f of degree p^2 such that S is irreducible over K, see [GMS97, Proposition 5.6].

Let K be a number field. It is amusing to give a direct proof of the permutation property of the functions f from the Corollary without going the detour over the group–theoretic equivalence of arithmetic exceptionality. Note that if the Galois group of $S(X)$ contains an element which fixes no root, then $S(X)$ has no root modulo infinitely many primes by Chebotarëv's density theorem. Thus we get a direct proof of the Corollary from

Proposition 5.6. *Let K be a number field, and $\mathfrak{p}$ be a prime of K, such that f, S, and the associated elliptic curves can be reduced modulo $\mathfrak{p}$. (That of course is possible for all but finitely many primes.) Let $K_\mathfrak{p}$ be the residue field of the prime $\mathfrak{p}$. If $S(x)$ modulo $\mathfrak{p}$ has no root in $K_\mathfrak{p}$, then f mod $\mathfrak{p}$ is bijective on $K_\mathfrak{p} \cup \{\infty\}$.*

Proof. We work over the field $K_\mathfrak{p}$, and understand the coefficients of f, S and so on being reduced modulo $\mathfrak{p}$, so as being in $K_\mathfrak{p}$. The hypothesis gives that $f(\infty) = \infty$, and $f(a) \neq \infty$ for $a \in K_\mathfrak{p}$. So we only need to show injectivity on $K_\mathfrak{p}$.

Let E_μ and E_λ be the elliptic curves $Y^2 = q_\mu(X)$ and $Y^2 = q_\lambda(X)$, respectively. Suppose there is $a, b \in K_\mathfrak{p}$, $a \neq b$, such that $f(a) = f(b)$. Then there are u, v in a quadratic extension of $K_\mathfrak{p}$ such that $P := (a, u)$ and $Q := (b, v)$ are in $E_\mu(K')$, where K' is the quadratic extension of $K_\mathfrak{p}$. Let $T \mapsto \bar{T}$ be the involutory automorphism on the K'–rational points on E_μ and E_λ induced by the Frobenius generator of $\mathrm{Gal}(K'/K_\mathfrak{p})$, respectively. This Galois action commutes with the isogeny ϕ. By the assumption, the points $\phi(P) = (f(a), uf'(a))$ and $\phi(Q) = (f(b), vf'(b))$ have the same X–coordinate, so their Y–coordinates differ by at most a sign, so may be assumed to be equal by possibly replacing v by $-v$. Thus there is $\epsilon = -1$ or 1, such that $\overline{\phi(P)} = \epsilon\phi(P)$ and $\overline{\phi(Q)} = \epsilon\phi(Q)$. Note that $P - Q$ is in the kernel of ϕ, and that $\overline{(P - Q)} = \epsilon(P - Q)$, thus $P - Q$ has X–coordinate in $K_\mathfrak{p}$, so is a root of S, contrary to the hypothesis. □

5.1 Rational isogenies of degree 5

If $f \in \mathbb{Q}(X)$ is a function of branching type $(2, 2, 2, 2)$, and $n = \deg f$ is a prime, then we get a rational isogeny of an elliptic curve over $\mathbb{Q}$ of degree n. According to a result of Mazur [Maz78, Theorem 1], this can happen only for a few values of n. This is the reason for the short list of primes in Theorem 1.1(e). In Section 6 we have to look closer at the case $n = 5$. There are infinitely many elliptic curves admitting an isogeny of degree 5, however

the possible j–invariants are restricted by the following: If $\phi : E \to E'$ is an isogeny of elliptic curves (everything defined over $\mathbb{Q}$), then there is an absolutely irreducible polynomial (modular equation) $F_n(J, J') \in \mathbb{Q}[J, J']$ of degree $n + 1$ in each variable, such that $F_n(j, j') = 0$, where j and j' is the j–invariant of E and E', respectively (see [Sil94, Chapter III,§6]). Now suppose that $n = 5$. Then F_5 admits a rational parametrization as follows, see [Fri22, Viertes Kapitel]:

$$J = \frac{(T^2 + 10T + 5)^3}{T}$$
$$J' = \frac{(T'^2 + 10T' + 5)^3}{T'} \text{ with } TT' = 125.$$

One can write $T = R(J, J')/S(J, J')$ with $R, S \in \mathbb{Q}[J, J']$. So, as we have to have rational values for j and j', the corresponding parameter is rational except for those pairs (j, j') for which R and S vanish. One computes that in these cases $j = j' \in \{1728, -32768, 287496, -884736\}$, and verifies directly (e.g. using the Maple package apecs for computations with elliptic curves [Con97]) that we cannot have rational isogenies of degree 5 in these cases. Conversely, if an elliptic curve has a j–invariant of the form $\frac{(\eta^2+10\eta+5)^3}{\eta}$ for some non–zero rational η, then one can compute that the 5th division polynomial has a factor of degree 2. So the curve has a 5–division point P whose X–coordinate has degree at most 2 over $\mathbb{Q}$. One easily checks that the group generated by P is Galois invariant, so dividing by this group gives a rational isogeny of degree 5.

Summarizing, we get

Proposition 5.7. *Let j be the j–invariant of an elliptic curve over $\mathbb{Q}$. Then the curve admits a rational isogeny of degree 5 if and only if $j = \frac{(\eta^2+10\eta+5)^3}{\eta}$ for some non–zero rational η.*

In order to determine the field of constants, we also need

Proposition 5.8. *Let $f(X) = R(X)/S(X)^2$ be a $(2, 2, 2, 2)$–function of degree 5 as above, $q_\lambda(X)$, $q_\mu(X)$ be the associated cubic polynomials. Let j be the j–invariant of $Y^2 = q_\lambda(X)$. Then $j = \frac{(\eta^2+10\eta+5)^3}{\eta}$ for some non–zero rational η, and the field of constants of f is $\mathbb{Q}(\sqrt{5(\eta^2 + 22\eta + 125)})$.*

Proof. f induces an isogeny ϕ from $Y^2 = q_\mu(X)$ to $Y^2 = q_\lambda(X)$. Let $\hat{\phi}$ be the dual isogeny. Then $\Phi := \hat{\phi} \circ \phi$ is the multiplication by 5 map on $Y^2 = q_\mu(X)$.

The kernel of ϕ of course is contained in the kernel of Φ, so $S(X)$ is a divisor of the 5–th division polynomial of $Y^2 = q_\mu(X)$. By the previous proposition, we may assume that $j = \frac{(\eta^2+10\eta+5)^3}{\eta}$. Let j' be the j–invariant of $Y^2 = q_\mu(X)$. Then $j' = \frac{(\eta'^2+10\eta'+5)^3}{\eta'}$ with $\eta' = 125/\eta$. Knowing j', we can compute the discriminant of $S(X)$. It is, up to a square factor, equal to $5(\eta^2+22\eta+125)$. The result follows. □

6 Application to a question of Thompson

As mentioned already in Section 4, it is usually a difficult problem to decide whether rational functions $f(Z) \in \mathbb{C}(Z)$ with specific geometric monodromy groups (and branching data) are defined over certain small fields. In [Tho90] Thompson proposes the project to determine the cases where f is already defined over the rationals, and adds "..., an analysis which may require several years of hard work." Specifically, he investigates the case of a certain degree 25 function, but has to leave undecided the question about small fields of definition. The purpose of this section is to give a different approach and to settle this question. We give the method in reasonably complete detail, as it works also in many other instances. As this function also appears in Theorem 4.1(I)(c)(iv) as a possible candidate of an arithmetically exceptional function, we give more details in order to also show existence of examples with the correct pair of arithmetic and geometric monodromy group.

6.1 Thompson's question, group–theoretic preparation

Let $W = \mathrm{A\Gamma L}(1, 25)$ be the affine semi–linear group acting on the elements of the finite field $\mathbb{F}_{25}$. Thus $W = T \rtimes (S \rtimes F)$, where T is the group of translations $x \mapsto x + t$, S is the group of scalar multiplications $x \mapsto ax$ for non–zero a, and the group F of order 2 is generated by the Frobenius map $x \mapsto x^5$.

For i a divisor of 24, denote by $S_{(i)}$ the subgroup of S of order i, and set $W_{(i)} := T \rtimes (S_{(i)} \rtimes F)$. So $W_{(24)} = W$. Set $G := W_{(6)}$, and note that W/G is cyclic of order 4.

Let β be an element of order 12 in $\mathbb{F}_{25}^*$, and define elements σ_1, σ_2, σ_3, $\sigma_4 \in G$ as follows:

$$\sigma_1 : x \mapsto \beta^{20} x$$
$$\sigma_2 : x \mapsto -x + \beta$$
$$\sigma_3 : x \mapsto -\beta^{20} x^5 + \beta$$
$$\sigma_4 : x \mapsto x^5$$

One immediately verifies that these σ_i generate G, and that $\sigma_1\sigma_2\sigma_3\sigma_4 = 1$. (Here we write the action on $\mathbb{F}_{25}$ from the right.) The following table gives the cycle type and index of these elements:

	σ_1	σ_2	σ_3	σ_4
Cycle type	$1^1 3^8$	$1^1 2^{12}$	$1^5 2^{10}$	$1^5 2^{10}$
Ind	16	12	10	10

For natural action

Thus, by (2) we see that $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ is a genus 0 system, so there is a rational function $f(Z) \in \mathbb{C}(Z)$ having G as geometric monodromy group and branch cycle description given by the σ_i. Thompson's question [Tho90] is whether we can have $f \in \mathbb{Q}(Z)$. We give an answer which also takes care of the different possibilities of the arithmetic monodromy group of f.

Definition 6.1. Let K be a field, and $f, \tilde{f} \in K(X)$ rational functions. We call f and $\tilde{f}$ *linearly equivalent over* K, if there are linear fractional functions $\ell_1, \ell_2 \in K(X)$ such that $f(X) = \ell_1(\tilde{f}(\ell_2(X)))$.

Theorem 6.2. *Let $f(Z) \in \mathbb{Q}(Z)$ be a rational function with geometric monodromy group G and branching data as above. Let $A := \mathrm{Gal}(f(Z) - t | \mathbb{Q}(t))$ be the arithmetic monodromy group. Then there are, up to linear equivalence, exactly one such functions with $A = G$, and exactly two with $A/G = C_2$.*

In the latter two cases, the field of constants is $\mathbb{Q}(\sqrt{5})$.

The proof of this theorem is the subject of the following subsections.

Remark 6.3. The normalizer of G in the symmetric group S_{25} is W. We have $W/G = C_4$. Grouptheoretically, there is the third possibility that $A/G = C_4$. We have not been able to prove existence in this case, though we have very strong evidence for that.

Corollary 6.4. *Up to linear equivalence, there are exactly two arithmetically exceptional functions belonging to Theorem 4.1(I)(c)(iv).*

6.2 Passing to a different rational function

Let f be as in Theorem 6.2, and L be a splitting field of $f(Z) - t$ over $\mathbb{Q}(t)$. Denote by $\hat{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in L. Then $G = \mathrm{Gal}(L|\hat{\mathbb{Q}}(t))$ and $A := \mathrm{Gal}(L|\mathbb{Q}(t))$, so $A/G = \mathrm{Gal}(\hat{\mathbb{Q}}|\mathbb{Q})$.

Thompson's idea [Tho90] was to look at the fixed field of T in $\mathbb{C}L$ over $\mathbb{C}(t)$. Then $\mathbb{C}L$ is an unramified Galois extension of this field (of genus 2) with Galois group $S_{(6)} \rtimes F$. Here we rather work with fixed fields which have genus 0, and involve rational functions of type $(2, 2, 2, 2)$.

Recall that A is one of the groups $W_{(6)}$, $W_{(12)}$, $W_{(24)}$. If $A = W_{(i)}$, then A has, up to conjugation, the unique subgroup $A^{(3)} := W_{(i/3)}$ of index 3. Set $G^{(3)} := A^{(3)} \cap G$. Let $L^{(3)}$ be the fixed field of $A^{(3)}$ in L. As $A = GA^{(3)}$, we get that $L^{(3)}$ is a regular extension of $\mathbb{Q}(t)$ of degree 3. The action of the σ_i on the coset space $G/G^{(3)}$ gives the following cycle types:

	σ_1	σ_2	σ_3	σ_4
Cycle type	3^1	1^3	$1^1 2^1$	$1^1 2^1$

For action on $G/G^{(3)}$

By the Riemann–Hurwitz genus formula (2), we see that $L^{(3)}$ has genus 0, furthermore $L^{(3)}$ is a rational field, because σ_3 has a unique fixed point on $G/G^{(3)}$.

Let H be an F–stable $\mathbb{F}_5$–subspace of $T = \mathbb{F}_{25}$. Then H is also stable under $S_{(2)}$ and $S_{(4)}$, so the semidirect product $H \rtimes (S_{(i/3)} \rtimes F)$ is a subgroup of index 15 of $W_{(i)}$ for $i = 6$ or $i = 12$.

Suppose $|A/G| \leq 2$, so $A = W_{(i)}$ for $i = 6$ or 12. Then let $A^{(15)}$ be the subgroup of index 15 in A constructed above, which is also a subgroup of index 5 of $A^{(3)}$. As $A = GA^{(15)}$, the fixed field $L^{(15)}$ of this subgroup is a regular extension of $\mathbb{Q}(t)$. The action of the σ_i on $G/G^{(15)}$ gives the following cycle types:

	σ_1	σ_2	σ_3	σ_4
Cycle type	3^5	$1^3 2^6$	$1^1 2^7$	$1^5 2^5$
Ind	10	6	7	5

For action on $G/G^{(15)}$

For the genus $g_{L^{(15)}}$ of $L^{(15)}$ we obtain

$$2(15-1+g_{L^{(15)}}) = 10+6+7+5,$$

hence $g_{L^{(15)}} = 0$. As σ_3 has a unique fixed point on $G/G^{(15)}$, the field $L^{(15)}$ has a rational place, so this field is rational. As the cycle types of the σ_i in this action are all different, we get that the branch points of $L/\mathbb{Q}(t)$ are rational. Write $L^{(15)} = \mathbb{Q}(z)$, so $t = g(z)$ for a rational function $g(Z) \in \mathbb{Q}(Z)$. We get a decomposition $g(Z) = g_1(g_2(Z))$, with $g_i \in \mathbb{Q}(Z)$, $\deg g_1 = 3$, and $\deg g_2 = 5$, such that $L^{(3)} = \mathbb{Q}(g_2(z))$.

6.3 Rationality question for $|A/G| \leq 2$

We use the results from Section 5 to precisely pin down the function g_2 of degree 5. As the branch points of g are rational, we may make the following assumptions: ∞ corresponds to σ_1, and $0 = g_1^{-1}(\infty)$. Let 0 correspond to σ_3. The ramification information from above shows that the single point in the fiber $g_2^{-1}(0)$ is a branch point of g_2. Assume that this branch point is ∞. Without loss assume that $4/27$ is the branch point corresponding to σ_4, and that g_1 has monic numerator and denominator. This gives

$$g_1(X) = \frac{(X-1)^2}{X^3}.$$

Finally, let $1/\mu$ be the branch point corresponding to σ_2. The ramification information from above shows that $g_1^{-1}(1/\mu)$ consists of 3 different points, which are branch points of g_2. What we get is that g_2 is a $(2,2,2,2)$ function with branch points ∞ and the three roots of $X^3 - \mu(X-1)^2$. The elliptic curve associated to the branching data of g_2 thus is (see Section 5)

$$Y^2 = X^3 - \mu(X-1)^2. \tag{3}$$

The j–invariant of $\mathcal{E}$ is

$$j = 256\frac{\mu(\mu-6)^3}{4\mu-27}.$$

On the other hand, as $\mathcal{E}$ has a rational isogeny of degree 5, its j–invariant is of the form

$$j = \frac{(\eta^2+10\eta+5)^3}{\eta}$$

for some non–zero rational η, see Proposition 5.7. This gives the algebraic curve relation

$$\mathcal{C}: \ 256\mu(\mu-6)^3\eta = (4\mu-27)(\eta^2+10\eta+5)^3.$$

The curve $\mathcal{C}$ is birationally equivalent to the elliptic curve

$$\mathcal{E}: \ V^2 = U^3 - 7U^2 - 144U = U(U+9)(U-16).$$

Using the MAPLE package [Hoe95] and some adhoc tricks, we get the following birational correspondence, where $\zeta := (\eta^2+10\eta+5)/(\mu-6)$:

$$\begin{aligned}
\mu &= \frac{27(864V + U^4 - 36U^3 + 4320U)}{4(U-36)U^3} \\
\eta &= \frac{36V + VU - 13U^2 + 108U}{2U^2} \\
U &= \frac{9\zeta^2 - 36(\eta+1)\zeta + 144(\eta-1)}{4(\eta^2+4\eta-1)} \\
V &= \frac{9(2\eta+7)\zeta^2 - 36(\eta+9)\zeta - 144(3\eta+5)}{4(\eta^2+4\eta-1)}
\end{aligned}$$

Lemma 6.5. *The field of constants of f is the same one as the field of constants of g_2.*

Proof. Of course, the field of constants of g_2 is contained in the field of constants of f. One verifies that the index of the core of $A^{(15)}$ in $A^{(3)}$ is 10 if $A = W_{(6)}$, and 20 if $A = W_{(12)}$. So the degrees of the two fields of constants are the same. □

We are now going to study the rational points on $\mathcal{C}$ via the rational points on $\mathcal{E}$.

Lemma 6.6. *The finite rational points (u_0, v_0) on $\mathcal{E}$ are $(0,0)$, $(16,0)$, $(-9,0)$, $(-4, \pm 20)$, and $(36, \pm 180)$.*

Proof. As 7 does not divide the discriminant of $\mathcal{E}$, the rational torsion points of $\mathcal{E}$ map injectively to the $\mathbb{F}_7$–rational points of the reduction $\mathcal{E}$ modulo 7, see [Sil86, VII.3.1]. We compute that there are exactly 8 points modulo 7 (including the one at infinity), so we are done once we know that the

Mordell–Weil rank of $\mathcal{E}$ is 0. This however is well–known. Namely the linear transformation $X = U/4 - 1$, $Y = (V - U)/8$ maps $\mathcal{E}$ to the curve

$$Y^2 + XY + Y = X^3 + X^2 - 10X - 10,$$

which is C15 (one of the 8 curves with conductor 15) in the notation of [Cre97], and shown to have rank 0 there, confer [Cre97, page 110]. □

Lemma 6.7. *The rational points* (μ_0, η_0) *on* $\mathcal{C}$ *are* $(135/128, -25/8)$, $(-5/4, -25/2)$, $(-675/8, -40)$, *and* $(27/4, 0)$.

Proof. As $\eta^2 + 4\eta - 1$ has no root in $\mathbb{Q}$, the above transformation equations show that the only possible rational points (μ_0, η_0) which are not mapped to finite points on $\mathcal{E}$ have $\mu_0 = 6$. But that leads to $\eta^2 + 10\eta + 5 = 0$, which has no rational solution. The finite points (u_0, v_0) on $\mathcal{E}$ which give points on $\mathcal{C}$ are those with $u_0 \neq 0, 36$. (Those with $u_0 = 0$ or 36 give points on the projective completion of $\mathcal{C}$.) □

We summarize:

Proposition 6.8. *Let* C *be the set of linear equivalence classes of rational functions* $g \in \mathbb{Q}(X)$ *such that* $g(X) = g_1(g_2(X))$ *with* $g_1, g_2 \in \mathbb{Q}(X)$ *and the following holds:*

(a) $\deg g_1 = 3$, *and* g_1 *has three rational branch points of branching type* 3^1, $1^1 2^1$, *and* $1^1 2^1$.

(b) $\deg g_2 = 5$. *Furthermore,* g *has, besides the three branch points of* g_1, *also the different rational branch point* $1/\mu$, g_2 *is a* $(2, 2, 2, 2)$*–function with branch points* $g_1^{-1}(1/\mu)$ *and a simple point* $g_1^{-1}(b)$, *where* b *is a branch point of* g_1 *of type* $1^1 2^1$.

Let $\hat{\mathbb{Q}}$ *be the field of contants of* g_2. *Then* C *has size* 3, *with* g_1 *and* g_2 *as above, where* $\mu_0 = -675/8$ *gives* $\hat{\mathbb{Q}} = \mathbb{Q}$, *and* $\mu_0 = 135/128$ *or* $-5/4$ *gives* $\hat{\mathbb{Q}} = \mathbb{Q}(\sqrt{5})$.

Proof. The case $(\mu_0, \eta_0) = (27/4, 0)$ is nonsense, whereas the other rational points on $\mathcal{C}$ give examples as stated. The claim about $\hat{\mathbb{Q}}$ follows from Proposition 5.8 □

6.4 Existence of f for $|A/G| \leq 2$

We now use the functions g_i from Proposition 6.8 in order to show that we get back the desired functions f whose existence we hypothetically assumed.

Let $\hat{\mathbb{Q}}$ be the field of constants of g_2. It is clear that the geometric monodromy group of g is a transitive subgroup of the wreath product $D_5 \wr D_3$, where D_5 denotes the dihedral group of degree 5, and that in the case $\hat{\mathbb{Q}} = \mathbb{Q}$ the arithmetic monodromy group is a subgroup of the same wreath product, whereas in the case $\hat{\mathbb{Q}} = \mathbb{Q}(\sqrt{5})$ it is a subgroup of $(C_5 \rtimes C_4) \wr D_3$. Also, we know the cycle types of the branch cycle description of g. Using the computer algebra system GAP [S$^+$95], one verifies that such a 4–tuple generates $W_{(6)}$ in its action on 15 points, and that this group G is selfnormalizing in $D_5 \wr D_3$, and that the normalizer of G in $(C_5 \rtimes C_4) \wr D_3$ is $W_{(12)}$. So the normalizers in these wreath products are just the expected arithmetic monodromy groups A. Now let L be a splitting field of $g(Z) - t$ over $\mathbb{Q}(t)$, and E be a fixed field of a subgroup U of A of index 25. One verifies that the σ_i induce the expected action on $G/(G \cap U)$, also $A = GU$, so E has genus 0 and is regular over $\mathbb{Q}(t)$. Also, $E = \mathbb{Q}(y)$ is rational, because σ_1 has a unique fixed point in this degree 25 action. Write $t = f(y)$ for $f(Y) \in \mathbb{Q}(Y)$, and f is the desired function.

A Computation of the $(2, 2, 2, 4)$–example

Let K be the proposed field of constants. In $G = \mathrm{Gal}(L/K(t))$ there is a subgroup U of index 6, such that the cycle types of σ_1, σ_2, σ_3, and σ_4 are $1^2 2^2$, $1^4 2^1$, 2^3, and $2^1 4^1$. Thus there is a rational function $r(X)$ of degree 6 over K such that the fixed field of U is $K(x)$ with $r(x) = t$. Let b_i be the branch point corresponding to σ_i. From the degree 9 action we see that b_1 and b_4 are rational. Without loss assume that $b_4 = \infty$, the 4–fold point over b_4 is ∞, and the other one is 0. A consideration similar to the one in the $(2, 2, 6)$–case, utilizing the regular degree 4–extension over $\mathbb{Q}(t)$, shows that b_2 and b_3 are algebraically conjugate and generate K over $\mathbb{Q}$. Without loss assume $b_2 = -\lambda$, $b_3 = \lambda$, with $\lambda^2 \in \mathbb{Q}$. If we make a further choice, namely assume that the double point above b_2 is 1, then r is given by

$$r(X) = -2\frac{\lambda(8X^3 + 8\beta X^2 + 12X + 8\beta X + \beta^2 X + 8\beta + 16)^2}{(36 + 24\beta + \beta^2)^2 X^2} + \lambda,$$

where $\beta \in K$. Furthermore, we compute

$$b_1 = -\frac{\lambda(\beta^4 - 80\beta^3 - 504\beta^2 - 1728\beta - 2160)}{\beta^4 + 48\beta^3 + 648\beta^2 + 1728\beta + 1296}.$$

If we write $\beta = u + v\lambda$ with $u, v \in \mathbb{Q}$, and use that b_1 has to be rational, we get a polynomial condition in u and v. This polynomial is the product of two genus 0 factors over $\mathbb{Q}$, and it is easy to find rational points on them. One of them gives $\lambda = \sqrt{2}$ and $b_1 = 44/25$. Of course, we have used only necessary conditions so far. Yet, nothing guarantees that the Galois closure of $K(x)/K(t)$ is Galois over $\mathbb{Q}(t)$. However, in the specific case one can use an "almost–argument" to verify that. Namely express the coefficients of r in terms of $\lambda = \sqrt{2}$, and denote by $\bar{r}$ the function where we replace λ by $-\lambda$. So the numerator of $(r(X) - t)(\bar{r}(X) - t)$ is in $\mathbb{Q}(t)[X]$ of degree 12, and the Galois group should have size $|A| = 144$. One now checks that using the computer algebra system KASH [DFK+96] for various specializations of t. So we have a good candidate for the location of the branch points in order to compute the function $f \in \mathbb{Q}(X)$ of degree 9. The branching data gives polynomial equations for the coefficients of f. The resulting system is too big to be handled and solved by the usual Groebner basis packages. Instead, we use a MAPLE package by Raphael Nauheim [Nau95], which computes the solutions modulo a fixed prime, and lift them to p–adic numbers for sufficiently many digits in order to see periodicities and then guess the rational numbers. Once one has such a function, it is routine to verify that it has the desired properties, as we did in Section 4.

References

[Con97] I. Connell, *Apecs (arithmetic of plane elliptic curves), a program written in maple*, available via anonymous ftp from math.mcgill.ca in /pub/apecs (1997).

[Cre97] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press (1997).

[DFK+96] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, S. M., K. Wildanger, *KANT V4*, J. Symb. Comput. (1996), **24**(3), 267–283, KASH software available from ftp.math.tu-berlin.de in /pub/algebra/Kant/Kash/Binaries.

[FGS93] M. Fried, R. Guralnick, J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. (1993), **82**, 157–225.

[Fri22] R. Fricke, *Die elliptischen Funktionen und ihre Anwendungen, Zweiter Teil*, B. G. Teubner, Leipzig, Berlin (1922).

[Fri70] M. Fried, *On a conjecture of Schur*, Michigan Math. J. (1970), **17**, 41–55.

[Fri78] M. Fried, *Galois groups and complex multiplication*, Trans. Amer. Math. Soc. (1978), **235**, 141–163.

[GMS97] R. Guralnick, P. Müller, J. Saxl, *The rational function analogue of a question of Schur and exceptionality of permutation representations*, preprint.

[Hoe95] M. v. Hoeij, *An algorithm for computing the Weierstraß normal form*, ISSAC '95 Proceedings (1995), Implementation to be found at http://klein.math.fsu.edu/~hoeij.

[Maz78] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. (1978), **44**, 129–162.

[MM] G. Malle, B. H. Matzat, *Inverse Galois Theory*, Book manuscript.

[Mül97] P. Müller, *A Weil–bound free proof of Schur's conjecture*, Finite Fields Appl. (1997), **3**, 25–32.

[Nau95] R. Nauheim, *Algebraische Gleichungssysteme bei schlechter Reduktion*, Ph.D. thesis, Universität Heidelberg (1995), Software available from ftp.iwr.uni-heidelberg.de in /pub/nauheim.

[S+95] M. Schönert, et al., *GAP – Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany (1995).

[Sch23] I. Schur, *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*, S.-B. Preuss. Akad. Wiss., Phys.–Math. Klasse (1923), pp. 123–134.

[Sil86] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer–Verlag, New York (1986).

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer–Verlag, New York (1994).

[Tho90] J. G. Thompson, *Groups of genus zero and certain rational functions*, in *Groups, Sel. Pap. Aust. Natl. Univ. Group Theory Program, 3rd Int. Conf. Theory Groups Rel. Top., Canberra/Aust. 1989*, vol. 1456 of *Lect. Notes Math.* (1990), 1990 pp. 185–190, Zbl. 749.12005.

[Tur95] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A (1995), **58**, 312–357.

[Völ96] H. Völklein, *Groups as Galois Groups – an Introduction*, Cambridge University Press, New York (1996).

IWR, Universität Heidelberg, Im Neuenheimer Feld 368,
D-69120 Heidelberg, Germany
E-mail: Peter.Mueller@iwr.uni-heidelberg.de