TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 350, Number 5, May 1998, Pages 1823–1850
S 0002-9947(98)02123-0

KRONECKER CONJUGACY OF POLYNOMIALS

PETER MÜLLER

ABSTRACT. Let $f, g \in \mathbb{Z}[X]$ be non-constant polynomials with integral coefficients. In 1968 H. Davenport raised the question as to when the value sets $f(\mathbb{Z})$ and $g(\mathbb{Z})$ are the same modulo all but finitely many primes. The main progress until now is M. Fried's result that f and g then differ by a linear substitution, provided that f is functionally indecomposable. We extend this result to polynomials f of composition length 2. Also, we study the analog when $\mathbb{Z}$ is replaced by the integers of a number field. The above number theoretic property translates to an equivalent property of subgroups of a finite group, known as Kronecker conjugacy, a weakening of conjugacy which has been studied by various authors under different assumptions and in other contexts.

We also give a simplified and strengthened version of the Galois theoretic translation to finite groups.

1. INTRODUCTION

Let $f \in \mathbb{Z}[X]$ be a polynomial with integral coefficients. For a prime $p \in \mathbb{P}$ denote by $\mathcal{V}_p(f)$ the value set $f(\mathbb{Z})$ modulo p. Suppose there is another polynomial $g \in \mathbb{Z}[X]$ such that

$$\mathcal{V}_p(f) = \mathcal{V}_p(g) \text{ for all but finitely many } p \in \mathbb{P}.$$

We call the pair f, g *Kronecker conjugate over* $\mathbb{Q}$, a notion which will be justified later. We say 'over $\mathbb{Q}$', as we will use this term for other base fields as well.

An obvious instance for this to happen is that $g(X) = f(uX + v)$ for some $u \in \mathbb{Q} \setminus \{0\}$, $v \in \mathbb{Q}$ — then $\mathcal{V}_p(f) = \mathcal{V}_p(g)$ for all p which do not divide the denominator or numerator of u. In such a case, we say that f and g are *linearly related over* $\mathbb{Q}$. If however g is not linearly related over $\mathbb{Q}$ to f, then we say that f and g are *properly Kronecker conjugate over* $\mathbb{Q}$.

H. Davenport posed the problem of determining properly Kronecker conjugate pairs of polynomials over $\mathbb{Q}$.

This problem can be seen as a far-reaching generalization of another question from algebraic number theory that has already been treated several times. Namely for $n \in \mathbb{N}$, determine those integers $u \in \mathbb{Z}$ which are an n-th power modulo all but finitely many primes. If we set $f(X) = uX^n$, $g(X) = X^n$, then the hypothesis is equivalent to the one in Davenport's question. In this special case, one can prove that u is an n-th power, except for the cases that n is divisible by 8 and

Received by the editors January 16, 1996.

1991 *Mathematics Subject Classification.* Primary 11C08, 20B10; Secondary 11R09, 12E05, 12F10, 20B20, 20D05.

The author thanks the Deutsche Forschungsgemeinschaft (DFG) for its support in the form of a postdoctoral fellowship.

$u = w^n 2^{n/2}$ for a non-zero integer w (see [32], [1], [17]). Thus if $h \in \mathbb{Z}[X]$ is an arbitrary polynomial of positive degree, then $f(X) = h(X^8)$ and $g(X) = h(16X^8)$ are properly Kronecker conjugate over $\mathbb{Q}$. To date, no other examples are known (up to trivial modifications).

A non–existence result has been given by M. Fried. To state it we need to introduce some more terminology. Let K be a field of characteristic 0. We call a polynomial $h \in K[X]$ of degree ≥ 2 *indecomposable*, if it cannot be written as a composition of polynomials of lower degree over K. For any polynomial $f \in K[X]$ of degree ≥ 2 write $f(X) = f_1(f_2(\dots f_l(X)\dots))$ with indecomposable polynomials $f_i \in K[X]$. By a classical result of Ritt (see [27], [21]), the number l is independent of the decomposition. We say that f has *composition length* l. It is known (see [13, 3.5]) that the polynomials f_i are indecomposable over any field extension of K. Thus the composition length of a polynomial is independent of the base field.

Now we can state Fried's result. Putting [9, Section 2] and [8, Section 3] together, one obtains

Theorem 1.1 (Fried)**.** *There is no pair $f, g \in \mathbb{Z}[X]$ of properly Kronecker conjugate polynomials over $\mathbb{Q}$ with f being indecomposable.*

One of the aims in this paper is to obtain the same result for composition length 2.

Theorem 1.2. *There is no pair $f, g \in \mathbb{Z}[X]$ of properly Kronecker conjugate polynomials over $\mathbb{Q}$ with f having composition length 2.*

As remarked already, $f(X) = X^8$, $g(X) = 16X^8$ is a pair of properly Kronecker conjugate polynomials with f having composition length 3. So Theorem 1.2 does not extend to higher composition lengths without change.

There is an obvious generalization of Davenport's original question. Let K be a number field, and denote by $\mathcal{O}_K$ its ring of integers. Now, replace the condition of Kronecker conjugacy for $f, g \in \mathcal{O}_K[X]$ by

$$\mathcal{V}_\mathfrak{p}(f) = \mathcal{V}_\mathfrak{p}(g) \text{ for all but finitely many non-zero prime ideals } \mathfrak{p} \text{ of } \mathcal{O}_K.$$

The picture changes if we allow K to be bigger than $\mathbb{Q}$. New examples occur, which even share a strong property. Let $f, g \in K[X]$ be properly Kronecker conjugate over K, and suppose that f and g are even not linearly related over the algebraic closure $\overline{K}$ of K. Then we say that f and g are *strongly Kronecker conjugate over* K. For instance, our previous example $f(X) = h(X^8)$, $g(X) = h(16X^8)$ is not strongly Kronecker conjugate over $\mathbb{Q}$, as f and g are linearly related over $\mathbb{Q}(\sqrt{2})$.

The number field version of Theorem 1.1, obtained by M. Fried [10] together with Feit [5], is

Theorem 1.3 (Fried, Feit)**.** *Let K be a number field, and $f, g \in \mathcal{O}_K[X]$ be properly Kronecker conjugate over K with f being indecomposable. Then f and g are even strongly Kronecker conjugate, and the degree of f is* 7*,* 11*,* 13*,* 15*,* 21*, or* 31*. For each of these degrees and suitably big K, there indeed exist examples.*

Remark. We will see in section 2.3 that the degrees of f and g are the same if f and g are Kronecker conjugate.

Again, we extend this theorem to

Theorem 1.4. *Let K be a number field, and $f, g \in \mathcal{O}_K[X]$ be properly Kronecker conjugate over K. Suppose that $f(X) = a(b(X))$ with indecomposable $a, b \in K[X]$,*

such that neither a nor b is strongly Kronecker conjugate over K to another polynomial. Then f and g are strongly Kronecker conjugate, and

$$(\deg a, \deg b) \in \{(4,2),(6,2),(8,2),(10,2),(5,3),(8,3)\}.$$

For each of these cases there exist examples f and g over a suitably big K; they are explicitly given in section 4.

So far, we have seen only finitely many possible degrees of properly Kronecker conjugate polynomials. Of course, there is a trivial source for producing more such pairs. Let d and d' be properly Kronecker conjugate polynomials, and h be an arbitrary non-constant polynomial. Then also $f(X) = h(d(X))$, $g(X) = h(d'(X))$ are Kronecker conjugate, and in general even properly. Adopting a term used by Fried in a similar context, we say that a Kronecker conjugate pair f, g is *newly Kronecker conjugate* if it does not have this form. In view of the results, one might wonder if there are strongly and newly Kronecker conjugate polynomials of arbitrary high degree. In [23] we give the first infinite series.

Theorem 1.5. *Let $m \geq 3$ be an integer, and ζ be a primitive $4m$-th root of unity. Set*

$$f(X) = ((X^2 + (\zeta^4 - 1))^2 + \zeta^4 - 1)^m,$$
$$g(X) = ((X^2 + \zeta^{m-2}(\zeta^4 - 1))^2 + \zeta^4 - 1)^m.$$

Then f and g are strongly and newly Kronecker conjugate over any number field K which contains ζ.

There is another non-existence result [24] which would require some more definitions to state. It allows arbitrary composition lengths, but imposes restrictions on the polynomials f_i in a maximal decomposition $f(X) = f_1(f_2(\dots f_l(X)\dots))$ of f.

None of these results seems to be deducible from the very definition of Kronecker conjugacy. Rather, they depend on an equivalent group theoretic translation of Kronecker conjugacy. Let $f, g \in \mathcal{O}_K[X]$. Fix a transcendental t over K. Fix a Galois extension Π of $K(t)$ which contains elements x and y such that $f(x) - t = 0$ and $g(y) - t = 0$. Denote by G the Galois group of $\Pi | K(t)$, and let U and V be the stabilizers of x and y in G respectively. Fried's basic theorem (see [12, 19.27]) is

Theorem 1.6 (Fried)**.** *Let K be a number field, and $f, g \in \mathcal{O}_K[X]$ be non-constant polynomials. Then the following are equivalent.*

(i) *f and g are Kronecker conjugate over K.*
(ii) $\bigcup_{g \in G} U^g = \bigcup_{g \in G} V^g$.

Note that condition (ii) is easily seen to be independent of the chosen Galois extension Π of $K(t)$. In section 2.1 we will give a simple proof of Theorem 1.6. Actually, our approach allows us to give more information, namely to determine the prime ideals where $\mathcal{V}_\mathfrak{p}(f) = \mathcal{V}_\mathfrak{p}(g)$ might fail to hold.

The group theoretic condition (ii) first appeared in the work of Kronecker on characterizing finite extension of number fields by the splitting behavior of prime ideals. See [19], [17], [12, Section 19.5]. This condition has also been investigated (independently of its number theoretical context) by various group theorists. See [15], [26], [29]. We call two subgroups U and V of an abstract finite group G *Kronecker conjugate* if (ii) holds.

We want to give one example to show that Kronecker conjugacy in finite groups gives rise to tough questions. Suppose that (ii) holds and U has index 2 in G. Then clearly $V \le U \lhd G$, and the question is whether $U = \bigcup_{g\in G} V^g$ forces $U = V$. (This is a generalization of the easy fact that a finite group cannot be the union of the conjugates of a proper subgroup.) Yet, this question is distinctly non-trivial and has been answered in the affirmative by Saxl [29] (and generalized by Guralnick [15]). Note that if we assume $U \lhd G$ of index 3, then (ii) does not force $U = V$ any more. An example is the alternating groups $G = \mathrm{A}_4$, U the Sylow 2-subgroup of G, and V a subgroup of order 2 in U.

In our context of polynomials, we gain additional group theoretic information, which makes some questions more tractable. The next section is devoted to providing all this information needed to prove Theorems 1.2 and 1.4 in section 3. We compute the polynomials whose existence is claimed in Theorem 1.4 in section 4. We finish by stating two conjectures in section 5.

Finally, we note that there is another classical question which has the same arithmetic flavor as Davenport's problem. In 1923 I. Schur [31] investigated the question of when the value set of $f \in \mathbb{Z}[X]$ is the full residue system modulo p for infinitely many primes p. This problem has been solved by M. Fried in [7]. For more literature and related results, see the recent exposition in [33].

2. Kronecker conjugacy and monodromy groups

This section is devoted to the passage from the original question to an equivalent question about finite groups, first giving consequences from Kronecker conjugacy, and providing results about monodromy groups of polynomials to be used later. We keep the notation from the Introduction.

2.1. **Translation to finite groups.** We give a short proof of Theorem 1.6 different from the original proof of Fried (which uses Čebotarev's density theorem for function fields over finite fields; see [9, Section 2]) and the model theoretic proof in [12], which gives a far more general principle for characteristic transfer. Actually, our argument allows for a stronger statement, namely the implication (i) $\Rightarrow$ (iii) in Theorem 2.3 below.

The argument is based on

Theorem 2.1 (Frobenius)**.** *Let $h \in \mathcal{O}_K[X]$ be monic and separable, and assume that $h(X) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in $\mathcal{O}_K$ for almost all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Then every element of the Galois group of $h(X)$ over K fixes at least one root of h.*

A proof of this theorem, which follows from Frobenius' density theorem (a weaker form of Čebotarev's density theorem) can be found in [12].

We need a converse of Frobenius' theorem. As we could not find it in the literature, we supply a proof.

Proposition 2.2. *Let $h \in \mathcal{O}_K[X]$ be monic and separable, and assume that every element of the Galois group of $h(X)$ over K fixes at least one root of h. Then $h(X) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in $\mathcal{O}_K$ for every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.*

Proof. Let L be a splitting field of $h(X)$ over K. Let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L, and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. The roots of $h(X) = 0$ lie in $\mathcal{O}_L$ by the assumption about h. Let D and I be the decomposition and inertia

group of $\mathfrak{P}$ respectively. Then D/I is cyclic, and maps isomorphically to the Galois group of the extension $\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p}$ of residue fields. Pick $d \in D$ such that the coset dI generates D/I. By the assumption, d fixes a root α of $h(X) = 0$. Thus dI fixes the image of α in $\mathcal{O}_L/\mathfrak{P}$. But dI generates the full Galois group of $\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p}$, so there is $\beta \in \mathcal{O}_K$ which is congruent to α modulo $\mathfrak{P}$. This gives $h(\beta) \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, and the assertion follows. □

A refinement of Theorem 1.6 is

Theorem 2.3. *Let K be a number field, and $f, g \in \mathcal{O}_K[X]$ be non-constant polynomials. Let d be the product of the leading coefficients of f and g. Then the following are equivalent.*

(i) $\mathcal{V}_\mathfrak{p}(f) = \mathcal{V}_\mathfrak{p}(g)$ *for all but finitely many non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$; that is, f and g are Kronecker conjugate over K.*
(ii) $\bigcup_{g\in G} U^g = \bigcup_{g\in G} V^g$.
(iii) $\mathcal{V}_\mathfrak{p}(f) = \mathcal{V}_\mathfrak{p}(g)$ *for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which do not divide d.*

Proof. Suppose that (i) holds. We show (ii). Let n be the degree of f, and u be the coefficient of X^n in f. Note that Kronecker conjugacy is preserved when we replace $f(X)$ and $g(X)$ by $u^{n-1}f(X/u)$ and $u^{n-1}g(X)$ respectively. Thus we may assume that f is monic. Now, for $a \in \mathcal{O}_K$, the hypothesis says that $f(X) - g(a) \equiv 0 \pmod{\mathfrak{p}}$ has a root for almost all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. It is clear that there are only finitely many $a \in \mathcal{O}_K$ such that $f(X) - g(a)$ is not separable, as those a are the roots of the discriminant of $f(X) - g(Y)$ taken with respect to X, which is a polynomial of positive degree in Y.

Hilbert's irreducibility theorem (see [34] or [12]) tells us that the Galois groups $\mathrm{Gal}(f(X) - g(y)|K(y))$ and $\mathrm{Gal}(f(X) - g(a)|K)$ are isomorphic as permutation groups on the roots of $f(X) - g(y)$ and $f(X) - g(a)$ respectively for infinitely many $a \in \mathcal{O}_K$. Recall that $g(y) = t$. Thus every element of the Galois group $\mathrm{Gal}(f(X) - t|K(y))$ fixes at least one root. This Galois group is just the induced action of V on the roots of $f(X) - t$. (V need not act faithfully on these roots.) Hence every element in V fixes a root. But these roots are the conjugates of x, and the stabilizer of x is U. So every element of V lies in some conjugate of U. Now (ii) follows from symmetry.

Of course, (iii) implies (i), so we are left to show the implication (ii) ⇒ (iii). Again, let u be the coefficient of X^n of the degree n polynomial f. We are going to show that $\mathcal{V}_\mathfrak{p}(f) \supseteq \mathcal{V}_\mathfrak{p}(g)$ for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which do not divide u. The assertion then follows from symmetry. So fix a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ which does not divide u. Again, replace $f(X)$ by $u^{n-1}f(X/u)$ and $g(X)$ by $u^{n-1}g(X)$. This does not affect (ii) and (iii). Let $a \in \mathcal{O}_K$ be arbitrary. We want to show that $f(X) - g(a) \equiv 0 \pmod{\mathfrak{p}}$ has a solution. By adding some element from $\mathfrak{p}$ to a, we assume that $f(X) - g(a)$ is separable. So the Galois group of $f(X) - g(a)$ over K is a subgroup of the Galois group of $f(X) - t = f(X) - g(y)$ over $K(y)$. Every element of the latter Galois group fixes a root of $f(X) - t$, so this is even more true for the former Galois group acting on the roots of $f(X) - g(a)$. Now Proposition 2.2 yields the assertion. □

For future use we draw the following conclusion.

Corollary 2.4. *Let K be a number field, and $f, g \in \mathcal{O}_K[X]$ be non-constant and monic polynomials which are Kronecker conjugate over K. Then $\mathcal{V}_\mathfrak{p}(f) = \mathcal{V}_\mathfrak{p}(g)$ for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$.*

2.2. **Monodromy groups of polynomials.** Here we record some properties of monodromy groups of polynomials which are independent of the setup of Kronecker conjugacy. For a similar exposition see also [11]. Let K be a field of characteristic 0, and $f \in K[X]$ a polynomial of degree $n \geq 1$. Throughout this section, we can assume without loss of generality that f is monic. We denote by $\overline{K}$ an algebraic closure of K, and let t be a transcendental over K. We say that the Galois group G of $f(X) - t$ over $K(t)$ is the *arithmetic monodromy group* of f, and call the Galois group $\dot{G}$ of $f(X) - t$ over $\overline{K}(t)$ the *geometric monodromy group* of f. Both groups are regarded as permutation groups on the roots of $f(X) - t$, and under this identification as permutation groups, $\dot{G}$ is a normal subgroup of G. The factor group $G/\dot{G}$ has a natural interpretation. Let Π be a splitting field of $f(X) - t$ over $K(t)$; thus $G = \mathrm{Gal}(\Pi|K(t))$. Let $\hat{K}$ be the algebraic closure of K in Π. As $\overline{K}(t) \cap \Pi = \hat{K}(t)$ (see [3, Corollary 2, V, §4]), we have $\dot{G} = \mathrm{Gal}(\Pi|\hat{K}(t))$; thus $G/\dot{G}$ can be identified with the Galois group $\mathrm{Gal}(\hat{K}|K)$.

We are now going to define two important subgroups of G, which also give us a hold on the extension $\hat{K}|K$. For this we make the change of variables $Y = 1/X$ and $z = 1/t$. Then the equation $f(X) - t = 0$ can be written as

$$Y^n - z\tilde{f}(Y) = 0,$$

where $\tilde{f}$ is the reciprocal polynomial of f. Note that $\tilde{f}$ has constant term 1. The Eisenstein criterion shows that the left hand side is irreducible even over the power series field $\overline{K}((z))$. In particular, G and its normal subgroup $\dot{G}$ are transitive. A splitting field of $Y^n - z\tilde{f}(Y)$ over $K((z))$ has the form $\Pi K((z))$. We can describe this splitting field explicitly. For this let $z^{1/n}$ be an n-th root of z, and set $W = Y/z^{1/n}$. Then the above equation becomes

$$W^n - \tilde{f}(Wz^{1/n}) = 0.$$

Hensel's lemma tells us that this equation has a solution in $K[[z^{1/n}]]$. Thus, there is

$$y_0 = z^{1/n} + a_2 z^{2/n} + a_3 z^{3/n} + \ldots \in K[[z^{1/n}]]$$

with

$$y_0^n - z\tilde{f}(y_0) = 0.$$

The other solutions y_i are given by replacing $z^{1/n}$ by $\zeta^i z^{1/n}$, where ζ is a fixed primitive n-th root of unity. We get that $K(\zeta)((z^{1/n}))$ is a splitting field of $Y^n - z\tilde{f}(Y)$ over $K((z))$. Hence the field $\hat{K}$ is a subfield of $K(\zeta)$. Set

$$D = \mathrm{Gal}(K(\zeta)((z^{1/n}))|K((z))),$$

and

$$Z = \mathrm{Gal}(K(\zeta)((z^{1/n}))|K(\zeta)((z))).$$

The group Z is cyclic of order n, and permutes the elements y_i cyclically. Also, the structure of D is clear. It is the semidirect product of Z with $\mathrm{Gal}(K(\zeta)|K)$, where

the action is given by identifying Z with $\mathbb{Z}/n\mathbb{Z}$ and $\mathrm{Gal}(K(\zeta)|K)$ with a subgroup of the group of units of $\mathbb{Z}/n\mathbb{Z}$ in its action by multiplication on $\mathbb{Z}/n\mathbb{Z}$.

It is clear that D and Z are naturally identified as subgroups of G. As the group D induces $\mathrm{Gal}(K(\zeta)|K)$ on $K(\zeta)$, it also induces $\mathrm{Gal}(\hat{K}|K)$ on $\hat{K}$. Hence $G = \dot{G}D$. Further, $Z \leq \dot{G}$, as Z is trivial on $\hat{K} \leq K(\zeta)$. Therefore D/Z maps surjectively on $G/\dot{G}$. A particular case of interest is $K = \mathbb{Q}$. Then D/Z is the full group of units of $\mathbb{Z}/n\mathbb{Z}$.

We summarize:

Proposition 2.5. *With the above notation, let G and $\dot{G}$ act on the n roots of $f(X) - t$. Then $\dot{G}$ contains a regular cyclic subgroup Z of order n. Further, there is a subgroup D of G with $Z \leq D$, such that Z has a complement in D which is isomorphic to a subgroup of the group $Z_n^\star$ of units of $\mathbb{Z}/n\mathbb{Z}$. If $K = \mathbb{Q}$, then this complement is isomorphic to $Z_n^\star$. Furthermore, $|G/\dot{G}|$ divides $|Z_n^\star|$.*

The presence of the cyclic regular subgroup Z of G has an interesting consequence, which we state in a slightly more general form. For a subgroup M of a finite group H, denote by $\mathrm{core}_H(M)$ the group $\bigcap_{h\in H} M^h$. Thus $\mathrm{core}_H(M)$ is the biggest subgroup of M which is normal in H.

Lemma 2.6. *Let U be a subgroup of a finite group H, such that $H = ZU$ with an abelian subgroup Z of H. If $U < M \leq H$, then $M \cap Z \leq \mathrm{core}_G(M)$, and $M \cap Z$ is not contained in U.*

Proof. As $H = ZU$, we have $M = U(M \cap Z)$, so $M \cap Z$ is not contained in U. Further, the set of H-conjugates of M coincides with the set of Z-conjugates of M. Hence $M \cap Z = \bigcap_{z\in Z}(M \cap Z)^z \leq \bigcup_{z\in Z} M^z = \mathrm{core}_H(M)$. □

Let U be the stabilizer in G of the root x of $f(X)-t$. There is a good correspondence between the maximal chains of subgroups from U to G and decompositions of f into indecomposable polynomials over K. The proof of the following lemma follows readily from Lüroth's theorem (see also [13]).

Lemma 2.7. *Let $f(X) = f_1(f_2(\dots(f_l(X))\dots))$ be a decomposition of f into indecomposable polynomials f_i. Denote by U_i the stabilizer of $f_i(f_{i+1}(\dots(f_l(x))\dots))$ in G for $1 \leq i \leq l$. Then $G = U_1 > U_2 > \dots > U_l > U$ is a maximal chain of subgroups.*

Conversely, if such a chain of subgroups is given, then there is a corresponding decomposition of f.

In particular, G is a primitive permutation group if and only if f is indecomposable.

Therefore the knowledge of the monodromy groups of indecomposable polynomials is of basic importance. In order to formulate a classification result, we need to introduce some terminology.

A_n, S_n	Alternating or symmetric group of degree n;
C_n	Cyclic group of degree n;
D_n	Dihedral group of degree n (and size $2n$ if $n > 2$, and size 2 if $n = 2$);
M_n	Mathieu group of degree n;
$\mathrm{PGL}_m(q)$	Projective linear group over the field with q elements, acting on the points of the $(m-1)$-dimensional projective space;
$\mathrm{PSL}_m(q)$	Projective special linear subgroup of $\mathrm{PGL}_m(q)$;
$\mathrm{P\Gamma L}_m(q)$	Projective semi-linear group. This group is generated by $\mathrm{PGL}_m(q)$ and the action of $\mathrm{Aut}(\mathbb{F}_q)$ on the projective space, where $\mathbb{F}_q$ is the finite field with q elements;
$\mathrm{AGL}_1(n)$	Affine group $C_n \rtimes \mathrm{Aut}(C_n)$. We regard it as the group of mappings on $\mathbb{Z}/n\mathbb{Z}$ given by $r \mapsto ar + b$ for $b \in \mathbb{Z}/n\mathbb{Z}$ and a a unit of $\mathbb{Z}/n\mathbb{Z}$.

The following result is basic for the rest of the paper.

Proposition 2.8. *Let K be a number field, and $f \in K[X]$ an indecomposable polynomial of degree n which is not strongly Kronecker conjugate to another polynomial. Then, with the previous notation, one of the following holds.*

(1) $n \in \mathbb{P}$, $\dot{G} = C_n$, $C_n \le G \le \mathrm{AGL}_1(n)$;
(2) $n \in \mathbb{P}$, $\dot{G} = D_n$, $D_n \le G \le \mathrm{AGL}_1(n)$;
(3) n *odd*, $\dot{G} = \mathrm{A}_n$, $\mathrm{A}_n \le G \le \mathrm{S}_n$;
(4) $\dot{G} = G = \mathrm{S}_n$;
(5) $n = 6$, $\dot{G} = G = \mathrm{PGL}_2(5)$;
(6) $n = 8$, $\dot{G} = G = \mathrm{PGL}_2(7)$;
(7) $n = 9$, $\dot{G} = G = \mathrm{P\Gamma L}_2(8)$;
(8) $n = 10$, $\dot{G} = G = \mathrm{P\Gamma L}_2(9)$;
(9) $n = 11$, $\dot{G} = G = \mathrm{M}_{11}$, *or* $n = 23$, $\dot{G} = G = \mathrm{M}_{23}$.

Proof. The group $\dot{G}$ equals the Galois group of $f(X) - t$ over $\mathbb{C}(t)$. These Galois groups have been classified when f is indecomposable by Feit ([5]; see [21] for a correction) for the case that f has a strongly Kronecker conjugate partner, and in [21] for the other cases. So [21] gives us the possibilities for $\dot{G}$. The statement about G follows from $\dot{G} \trianglelefteq G$ and considering the normalizer of $\dot{G}$ in S_n, where $\dot{G}$ has degree n. □

Remark. Though we won't need the result, we want to give the complementary list of monodromy groups of indecomposable polynomials. Suppose that f is indecomposable and has a strongly Kronecker conjugate partner. Then $\dot{G} = G$, and G is one of the following groups of degree n: $\mathrm{PSL}_2(11)$ ($n = 11$), $\mathrm{PGL}_3(2)$ ($n = 7$), $\mathrm{PGL}_3(3)$ ($n = 13$), $\mathrm{PGL}_4(2)$ ($n = 15$), $\mathrm{P\Gamma L}_3(4)$ ($n = 21$), and $\mathrm{PGL}_5(2)$ ($n = 31$).

2.2.1. *The geometric interpretation of $\dot{G}$.* As a preparation for the explicit computations in section 4 and some arguments needed in section 3.3, we say something about the geometric interpretation of $\dot{G}$ as a monodromy group of a branched cover. This, by the way, is also the tool to prove the above proposition.

Let f have degree n. Then f defines a branched covering of Riemann spheres $\mathbb{P}^1 \to \mathbb{P}^1$ by sending z to $f(z)$. We call this cover f also.

Let $\mathcal{B} = \{b_1, b_2, \dots, b_r\}$ be the set of branch points of f. These are the points b with $|f^{-1}(b)| < n$. Without loss, let b_r be the branch point ∞. The branch points different from ∞ will be called finite branch points. Fix $p \in \mathbb{P}^1 \setminus \mathcal{B}$, and denote by π_1 the fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathcal{B}, p)$. Then π_1 acts transitively on the points of the fiber $f^{-1}(p)$ by lifting of paths. We fix a numbering $1, 2, \dots, n$ of this fiber. So we get a homomorphism $\pi_1 \to \mathrm{S}_n$. By standard arguments (see [22, Section 2] for a self-contained presentation), the image of π_1 can be identified with the geometric monodromy group $\dot{G}$; thus we write $\dot{G}$ for this group too.

We choose a standard homotopy basis for $\pi_1 = \pi_1(\mathbb{P}^1 \setminus \mathcal{B}, p)$ as follows. Let γ_i be represented by paths which start and end in p and wind once around b_i counterclockwise, and around no other branch point, such that $\gamma_1\gamma_2\cdots\gamma_r = 1$. Then $\gamma_1, \gamma_2, \dots, \gamma_{r-1}$ freely generate π_1.

Definition. For $\sigma \in \mathrm{S}_n$, let $e_1, \dots, e_m$ be the cycle lengths of σ. Define the index of σ by $\operatorname{ind}\sigma = \sum_{j=1}^{m}(e_j - 1)$.

Let σ_i be the image of γ_i in S_n. If the points $s_1, \dots, s_m$ in the fiber of b_i have multiplicities $e_1, \dots, e_m$, respectively, then σ_i has cycle lengths $e_1, \dots, e_m$. In particular, $\operatorname{ind}\sigma_i = n - |\pi^{-1}(b_i)|$. Further, σ_r is an n-cycle, because $b_r = \infty$ has only one preimage under f. As $\mathbb{P}^1$ has genus 0, and σ_r has index $n-1$, the Riemann-Hurwitz genus formula gives (setting $R = r - 1$).

$\dot{G}$ is generated by $\sigma_1, \dots, \sigma_R$, and the following holds:

$$(\star) \qquad \begin{cases} \sigma_1\sigma_2\cdots\sigma_R \text{ is an } n\text{–cycle;} \\ \displaystyle\sum_{i=1}^{R} \operatorname{ind}\sigma_i = n - 1. \end{cases}$$

The tuple $(\sigma_1, \sigma_2, \dots, \sigma_R)$ will be called a *genus* 0 *system* of the cover f, or of the group $\dot{G}$. Conversely, the hypothesis about a finite permutation group of degree n having a generating system as above will be called the *genus* 0 *condition*.

We may reorder the conjugacy classes in $\dot{G}$ that the σ_i belong to. Namely, if we replace the i-th and $(i+1)$-st position in $(\sigma_1, \sigma_2, \dots, \sigma_r)$ by σ_{i+1} and $\sigma_i^{\sigma_{i+1}}$ respectively, then the above properties are preserved. (Geometrically, that amounts of giving the branch points a different order before choosing the standard generators of π_1.)

From Riemann's existence theorem, we get a converse to this procedure. Let a finite permutation group of degree n be generated by $\sigma_1, \sigma_2, \dots, \sigma_R$ such that $(\star)$ holds. Then there is a polynomial over some number field, such that $\dot{G}$ is just the group we started with, and the genus 0 system is given by $(\sigma_1, \sigma_2, \dots, \sigma_R)$.

We say that a polynomial f equals $\tilde{f}$ *up to linear changes* if there are linear polynomials L_1, L_2 over $\mathbb{C}$ such that $f(X) = L_1(\tilde{f}(L_2(X)))$. The Chebyshev polynomial $T_n(X) \in \mathbb{Q}[X]$ of degree n is defined by the relation $T_n(Z + 1/Z) = Z^n + 1/Z^n$. Note that $T_{mn}(X) = T_m(T_n(X))$, hence the indecomposable Chebyshev polynomials have prime degree. The following lemma follows mostly from [21] and some easy computations.

Lemma 2.9. *Let $f \in K[X]$ be indecomposable of degree n.*

(i) *If $\dot{G} = C_n$, then f equals X^n up to linear changes, and n is a prime.*

(ii) *If $\dot{G} = D_n$, then f equals T_n up to linear changes, and n is a prime. If $n > 2$, then the branch points of T_n are -2 and 2. The elements σ_1 and σ_2 associated to these branch points are both involutions with exactly one fixed point.*

(iii) *If $\dot{G} = \mathrm{S}_4$, then either there are three finite branch points, and the associated σ_i are transpositions, or there are two finite branch points, and the associated σ_i are one transposition and one 3-cycle.*

2.3. **Group theoretic consequences from Kronecker conjugacy.** The notion of Kronecker conjugacy as in Theorem 1.6(ii) makes sense over any field K of characteristic 0. Thus assume that f, g are non-constant polynomials in $K[X]$. Again, use the setup preceding Theorem 1.6. We begin with an easy lemma.

Lemma 2.10. *The polynomials f and g are linearly related over K if and only if U and V are conjugate in G.*

Proof. Suppose that $f(X) = g(uX + v)$. Then $g(ux + v) = t = g(y)$; thus $ux + v$ and y are conjugate elements, so their respective stabilizers U and V are conjugate. For the converse, assume $U = V^h$ for some $h \in G$. Then $t = g(y) = g(y^h)$ and y^h is fixed by U, so it lies in $K(x)$. Thus $f(x) = g(R(x))$ for some rational function $R \in K(X)$. On the other hand, the degrees of f and g are the same (both equal the index $[G : U]$), so R has degree 1. Looking at the denominator shows that R is a polynomial, and the claim follows. □

Lemma 2.11. *G contains a cyclic subgroup Z such that $G = UZ = VZ$.*

Proof. This follows either from a slight extension of the argument yielding Proposition 2.5, or from the geometric description of geometric monodromy groups as in section 2.2. Or see the proof of [12, 19.29]. □

Lemma 2.12. *If f, g are Kronecker conjugate over K, then f and g are Kronecker conjugate over any finite extension of K.*

Proof. Galois theoretically, this translates to the condition that for a subgroup H of G which still acts transitively on the coset spaces G/U and G/V, the subgroups $U \cap H$ and $V \cap H$ are Kronecker conjugate in H, which is obvious. □

Lemma 2.13. *Let A and B be Kronecker conjugate subgroups of a finite group H. Suppose there is an abelian subgroup Z of H with $H = AZ = BZ$. Then $A \cap Z = B \cap Z$. Thus $|A| = |B|$. Furthermore,* $\mathrm{core}_H(A) = \mathrm{core}_H(B)$.

Proof. By the argument from the previous proof, $A \cap Z$ and $B \cap Z$ are Kronecker conjugate in Z; hence they are equal. Let N be the core of A in H. Then $A = AN$ and BN are Kronecker conjugate in H. Thus $A \cap Z = B \cap Z = BN \cap Z$ by the first part of the lemma. The modular law yields $BN = BN \cap BZ = B(BN \cap Z) = B(B \cap Z) = B$, so $N \leq B$. From symmetry we get the assertion. □

For the following development, we assume that the Galois extension of $K(t)$ which contains x and y is taken to be minimal. The preceding lemma shows that if f and g are Kronecker conjugate over K, then U and V have trivial core in G; that is, G acts faithfully on the conjugates of x as well as on the conjugates of y. This also has an implication for the geometric consideration in section 2.2.

Lemma 2.14. *If f and g are Kronecker conjugate over K, then the branch points of f and g coincide.*

Proof. This follows from the preceding remark. Namely let $\mathcal{B}_f$ and $\mathcal{B}_g$ be the branch points of f and g respectively. For $p \in \mathbb{P}^1 \setminus (\mathcal{B}_f \cup \mathcal{B}_g)$ choose generators σ_i of $\pi_1(\mathbb{P}^1 \setminus (\mathcal{B}_f \cup \mathcal{B}_g), p)$ similarly as in section 2.2. If b is a branch point of f, then the associated σ_i is not trivial on the coset space G/U, so it is also not trivial on the coset space G/V. That means b is a branch point of g as well. From symmetry we get the claim. □

2.4. **Cases of Kronecker conjugacy.** Here we present the general type of the new cases of Kronecker conjugacy which belong to Theorem 1.4. In section 3 we will be able to identify G and a subgroup M such that subgroups U and V of M are Kronecker conjugate in G. While we will exactly determine G and M, we still have to determine what U and V really look like. The technical Proposition 2.16 will take care of that.

Let $\mathbb{F}_q$ be a finite field with q elements, and let $\Gamma\mathrm{L}_2(q)$ be the semilinear group over $\mathbb{F}_q$. Write $\Gamma\mathrm{L} = \mathrm{Aut}(\mathbb{F}_q) \ltimes \mathrm{GL}_2(q)$, and view this group as acting from the right on $\mathbb{F}_q^2$. Choose $\mathrm{GL}_2(q) \leq \hat{G} \leq \Gamma\mathrm{L}_2(q)$. Write $\hat{G} = \Gamma \ltimes \mathrm{GL}_2(q)$ with $\Gamma \leq \mathrm{Aut}(\mathbb{F}_q)$. Let S be a proper subgroup of $\mathbb{F}_q^\star$. Set

$$\begin{aligned}
\Delta &= \{\left(\begin{smallmatrix} s & 0 \\ 0 & s \end{smallmatrix}\right) |\ s \in S\},\\
\hat{U} &= \Gamma \ltimes \{\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right) |\ a \in S,\ b \in \mathbb{F}_q^\star,\ c \in \mathbb{F}_q\},\\
\hat{V} &= \Gamma \ltimes \{\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right) |\ a \in \mathbb{F}_q^\star,\ b \in S,\ c \in \mathbb{F}_q\},\\
G &= \hat{G}/\Delta,\\
U &= \hat{U}/\Delta,\\
V &= \hat{V}/\Delta.
\end{aligned}$$

Lemma 2.15. *U and V are Kronecker conjugate in G, but not conjugate in G.*

Proof. For $v \in \hat{V}$ write $v = \gamma m$ with $\gamma \in \Gamma$. Then m has eigenvalue $b \in S$. So m, and therefore v as well, is conjugate to an element in $\hat{U}$. Conversely, every element in $\hat{U}$ is conjugate to some element in $\hat{V}$. From this the Kronecker conjugacy of U and V in G follows.

Now suppose that U and V are even conjugate in G. Then, also the subgroups $\{\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right) |\ a \in S,\ b \in \mathbb{F}_q^\star,\ c \in \mathbb{F}_q\}$ and $\{\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right) |\ a \in \mathbb{F}_q^\star,\ b \in S,\ c \in \mathbb{F}_q\}$ are conjugate in $\mathrm{GL}_2(q)$. But this is easily seen to be not the case. □

For the group G as defined above we will use the notation $G = \hat{G}/C_s$, where s is the order of S.

Proposition 2.16. *Suppose $\mathrm{GL}_2(q) \leq \hat{G} \leq \Gamma\mathrm{L}_2(q)$, and set $G = \hat{G}/C_s$ for some proper subgroup S of $\mathbb{F}_q^\star$ of order s. Suppose there are subgroups U, V, M, N of G as follows. N is the core of M in G, and U, V are subgroups of prime index p of M such that $M = UN = VN$ and $U \cap N = V \cap N = 1$. Further, assume that U and V are Kronecker conjugate in G and that the action of G/N on the cosets of M in G is the natural action of the corresponding group between $\mathrm{PGL}_2(q)$ and $\mathrm{P\Gamma L}_2(q)$.*

Let Δ be as above, and for $(\lambda, \mu) \in \{(1, i), 0 \leq i \leq p-1\} \cup \{(0, 1)\}$ set

$$\hat{W}_{(\lambda,\mu)} = \Gamma \ltimes \{\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right) | a^\lambda b^\mu \in S\}.$$

Then one of the following holds.

(i) *U is conjugate to $\hat{W}_{(1,0)}/\Delta$ and V is conjugate to $\hat{W}_{(0,1)}/\Delta$, or vice versa.*

(ii) *U is conjugate to $\hat{W}_{(1,\mu)}/\Delta$ and V is conjugate to $\hat{W}_{(1,\mu')}/\Delta$ with $\mu\mu' \equiv 1 \pmod{p}$.*

In particular, if $p \in \{2,3\}$, then U and V are (up to interchanging) as in Lemma 2.15.

Proof. First one proves that a subgroup W of index p in M such that $M = NW$ and $W \cap N = 1$ has the form (up to conjugacy) of $W_{(\lambda,\mu)}$ as above. It remains to check Kronecker conjugacy of these subgroups. This is done by comparing the eigenvalues of the elements in $\hat{W}_{(\lambda,\mu)}$, where the Γ-part is omitted. The procedure is straightforward. □

3. Proof of Theorems 1.2 and 1.4.

Throughout this section we use standard notation from finite group theory (see [14] and [35]) and notation which has been defined in the previous sections.

3.1. **Group theoretic preparation.** Suppose that f, g are polynomials as in Theorem 1.2 or 1.4. Write $f(X) = a(b(X))$ with indecomposable polynomials $a, b \in K[X]$. Let t be a transcendental number. Denote by Π a minimal Galois extension of $K(T)$ which contains x and y with $f(x) = g(y) = t$. Set $G = \mathrm{Gal}(\Pi|K(t))$. Denote by U the stabilizer of x in G, by V the stabilizer of y, and by M the stabilizer of $b(x)$. Then $U < M < G$, and G acts faithfully on the coset spaces G/U and G/V (see section 2.3). Set $N = \mathrm{core}_G(M) > 1$ (see Lemma 2.6 and 2.7). The faithful action of G/N on the coset space G/M gives the arithmetic monodromy group of the polynomial a, and the induced action of M on M/U is the arithmetic monodromy group of b. Further, U is maximal in M, and M is maximal in G.

Now NU and NV are also Kronecker conjugate in G, and $NU = M$ as U is maximal in M and $N \not\leq U$. We have $V < NV < G$. Let $g(X) = c(d(X))$ be a corresponding decomposition (Lemma 2.7). Now a and c are Kronecker conjugate. If we are in the situation of Theorem 1.2, then a and c are linearly related over K by Theorem 1.1, and in the situation of Theorem 1.4 again a and c are linearly related over K by the assumption and Theorem 1.3. Thus NV and $NU = M$ are conjugate by Lemma 2.10. So from now on we assume without loss that $V < M$.

Lemma 3.1. *V is maximal in M.*

Proof. Let $V < W < M$. Then $C = \mathrm{core}_G(W) > 1$, and $V < CV \leq W < M$. Now $CU = M$ and CV are Kronecker conjugate in G. Thus, by Lemma 2.13, $|M| = |CU| = |CV| < |M|$, a contradiction. □

In the following we will consider G as a permutation group on the right coset space G/U. This action is imprimitive; a block system is provided by the right cosets G/M. Then N is the kernel of the action of G on G/M. Note that $M \cap Z \leq N$ (with Z from Lemma 2.11). Let $N_0 \leq N$ be a minimal normal subgroup of G. Set

$$N_U = \mathrm{core}_M(U), \quad N_V = \mathrm{core}_M(V).$$

Further, denote by $\widetilde{Y}$ the image of $Y \leq M$ in M/N_U. Thus $\widetilde{M}$ acts faithfully and primitively on M/U.

Lemma 3.2. *N_0 is an elementary abelian p–group.*

Proof. The configuration is similar to that studied in [24]; thus we use some arguments from the proof of [24, Lemma 5.1]. Suppose the assertion is wrong. Then, as N_0 is a minimal normal subgroup of G, it can be written as $N_0 = S_1 S_2 \cdots S_t$, the direct product of simple non–abelian groups S_i. These S_i's are permuted transitively by G. First we contend

> *Exactly one of the S_i's, say S_1, is not contained in N_U. Further, $M \leq \mathbf{N}_G(S_1)$.*

Since $M = (M \cap Z)U$, the group $\widetilde{M \cap Z}$ is a cyclic transitive subgroup of the primitive permutation group $\widetilde{M}$. Moreover, $\widetilde{M}$ is not solvable, as N_0 has a nontrivial image in $\widetilde{M}$; hence $\widetilde{M}$ is 2-transitive on M/U by theorems of Schur and Burnside [35, Theorems 25.3 and 11.7]. Because $\widetilde{M}$ is a 2-transitive permutation group, it has a unique minimal normal subgroup $\widetilde{S}$ which is either elementary abelian or simple non-abelian (see [35, Exercise 12.4]). As $\widetilde{N_0} \trianglelefteq \widetilde{M}$ is a nontrivial product of groups isomorphic to S_1, exactly one of the S_i's is not contained in N_U. The latter assertion follows from the former, as M permutes the S_i's.

$N_U = \mathbf{C}_M(S_1)$.

$\mathbf{C}_{\widetilde{M}}(\widetilde{S_1})$ is normal in $\widetilde{M}$, but does not contain $\widetilde{S_1}$, as $\widetilde{S_1}$ is not abelian. Thus $\mathbf{C}_{\widetilde{M}}(\widetilde{S_1})$ is trivial. In particular, $\mathbf{C}_M(S_1) \leq N_U$. We get the other inclusion as follows: S_1 is simple and normal in M by the previous assertion. Thus $S_1 \cap N_U = 1$ and therefore $N_U \leq \mathbf{C}_M(S_1)$.

By symmetry we also get

> *There is an index i such that all the S_j except for $j = i$ are contained in N_V, $M \leq \mathbf{N}_G(S_i)$, and $N_V = \mathbf{C}_M(S_i)$.*

Assume for a moment that $i = 1$. We then get that $\widetilde{M}$ acts faithfully and 2–transitively on the coset spaces M/U and M/V, and in both actions $\widetilde{M \cap Z}$ is a transitive cyclic subgroup. But this forces U and V to be Kronecker conjugate; see [6, 4.1]. But then U and V are even conjugate in M, by an argument similar to the one at the beginning of this section, a contradiction.

Observe that Z permutes the S_i's transitively, because G does so, M fixes S_1, and $G = MZ$. Therefore $\mathbf{N}_G(S_j) \cap Z$ is independent of j. By the previous steps we know that M is contained in $\mathbf{N}_G(S_1)$ and $\mathbf{N}_G(S_i)$; hence

$$\mathbf{N}_G(S_1) = (\mathbf{N}_G(S_1) \cap Z)M = (\mathbf{N}_G(S_i) \cap Z)M = \mathbf{N}_G(S_i) \ .$$

Pick $g \in G$ with $S_i = S_1^g$. Then

$$\mathbf{N}_G(S_1) = \mathbf{N}_G(S_i) = \mathbf{N}_G(S_1)^g \ .$$

Now, as M is a maximal subgroup of G, the group $\mathbf{N}_G(S_1)$ is either M or G. If the latter happens, then $N_0 = S_1$; hence of course $i = 1$, and we are done. Thus, assume $\mathbf{N}_G(S_1) = M$. If $\mathbf{N}_G(M) = M$, then g normalizes S_1; therefore $S_i = S_1^g = S_1$, and hence again $i = 1$. So it remains to check the case $M \lhd G$. As the normalizer of S_1 in G is M, we get $N_U = \mathbf{C}_G(S_1)$ and $N_V = \mathbf{C}_G(S_i)$. So $N_U^g = N_V$, and both N_U^g and N_V are contained in M. As in the case $N_U = N_V$, we get that U^g and V are conjugate in M, a contradiction. □

In virtue of the previous lemma, we now suppose that N_0 is elementary abelian of exponent p for some prime p.

Lemma 3.3. *One of the following holds.*

(a) $[M:U] = [M:V] = p$ *and* $C_p \le M/N_U, M/N_V \le \mathrm{AGL}_1(p)$.
(b) $[M:U] = [M:V] = 4$ *and* $M/N_U = M/N_V = \mathrm{S}_4$.

Proof. The group $\widetilde{N_0}$ is an elementary abelian normal and transitive p–subgroup of $\widetilde{M}$. Set $|N_0| = p^k$. Then $\widetilde{M}$ imbeds into $\mathrm{AGL}_k(p)$, with the latter group acting naturally on $\mathbb{F}_p^k$. Now $\mathrm{AGL}_k(p)$ is a subgroup of $\mathrm{GL}_{k+1}(p)$, and as $\widetilde{M}$ contains the cyclic subgroup $\widetilde{M \cap Z}$ of order p^k, we infer that $\mathrm{GL}_{k+1}(p)$ contains an element of order p^k. This easily forces $k = 1$ or $p^k = 4$. From this the assertion follows quickly. □

Note that in case (a) nothing guarantees that M/N_U and M/N_V are isomorphic.

Lemma 3.4. *Neither* $N_U \le N_V$, *nor* $N_V \le N_U$.

Proof. In a group between C_p and $\mathrm{AGL}_1(p)$, any two subgroups of index p are conjugate (for instance by Schur–Zassenhaus). Also, in S_4 any two subgroups of index 4 are conjugate. □

We need some more notation. Let Ω be the coset space G/U. If not otherwise said, G is considered as a permutation group on Ω. The cosets of M in G provide a system of imprimitivity for the action of G. Denote these blocks by $\Omega_1, \Omega_2, \dots, \Omega_m$, where Ω_1 should be the coset M. That is, M fixes Ω_1. Let $\overline{\Omega}$ be the set $\{\Omega_1, \Omega_2, \dots, \Omega_m\}$. For a subgroup Y of G, set $\overline{Y} = YN/N$. Then $\overline{G}$ acts faithfully on $\overline{\Omega}$. Set $\overline{\Omega}^* = \overline{\Omega} \setminus \Omega_1$. So $\overline{M}$ acts faithfully on $\overline{\Omega}^*$.

Further, we set $Z_p = M \cap Z$. Note that $|Z_p| = p$, and that Z_p acts regularly on each Ω_i.

Lemma 3.5. *Every element of* $N_U \setminus N_V$ *fixes an element of* $\overline{\Omega}^*$.

Proof. Let $u \in N_U$. Pick an arbitrary $m \in Z_p$. From $M = VZ_p$ we get $M = V^m Z_p$. Thus $u = v^m z$ for some $v \in V$, $z \in Z_p$. By Kronecker conjugacy, v fixes some element in Ω, so in particular it fixes some element in $\overline{\Omega}$. As $m, z \in Z_p \subseteq N$, the elements $v^m z$ and v fix the same elements in $\overline{\Omega}$. Now suppose that $u = v^m z$ fixes only the set Ω_1. Then v, and then also v^m, fixes an element in Ω_1. But $v^m z = u$ is trivial on Ω_1 (as $u \in N_U$); therefore $z = 1$. Thus $v^m = u$. As m was arbitrarily chosen, we get $u \in \bigcap_{m \in Z_p} V^m = \bigcap_{m \in M} V^m = N_V$, and the assertion follows. □

Lemma 3.6. *If* $M/N_U = \mathrm{S}_4$, *then* N *acts as* S_4 *on each block* Ω_i.

Proof. The group $N_U N/N_U$ is normal in $M/N_U = \mathrm{S}_4$ and contains the cyclic group $Z_4 N_U/N_U$ of order 4. The only normal subgroup of S_4 containing such a group is S_4 itself. Thus $N_U N/N_U = \mathrm{S}_4$. □

The list in 2.8 tells us that either $\overline{G}$ is 3–transitive and distinct from S_3, or $C_r \le \overline{G} \le \mathrm{AGL}_1(r)$ for some prime r. These two cases require totally different arguments, so we treat them in separate subsections.

3.2. **The case when $\overline{G} \ne \mathrm{S}_3$ is 3–transitive.** We assume throughout this subsection that $\overline{G}$ is 3–transitive and different from S_3. Then $\overline{M}$ is 2–transitive on $\overline{\Omega}^*$, so every normal subgroup of $\overline{M}$ is either trivial or transitive on $\overline{\Omega}^*$.

Lemma 3.7. $N_U \cap N_V \not\le N$.

Proof. Suppose not; then $\overline{N_U \cap N_V} = 1$. So $\overline{N_U}$ is intransitive on $\overline{\Omega}^*$ by 3.5 (as every transitive permutation group has fixed point free elements); thus even $N_U \leq N$. By symmetry we also get $N_V \leq N$. Thus $N_U N_V \leq N$. Therefore $\overline{M}$ is a homomorphic image of $M/N_U N_V$. We get the sequence of surjections

$$U/N_U \twoheadrightarrow UN_V/N_U N_V = M/N_U N_V \twoheadrightarrow \overline{M}.$$

If we are in case (a) of Lemma 3.3, then U/N_U is a subgroup of the cyclic group of order $p-1$, so 2–transitivity of $\overline{M}$ forces $\overline{M} = C_2$, and so $\overline{G} = \mathrm{S}_3$, a case ruled out from consideration here.

Now suppose that we are in case (b) of Lemma 3.3. Then $M = N_U N$ by 3.6. But we got $N_U \leq N$, so $M = N$, and thus $\overline{M} = 1$, a contradiction. □

Lemma 3.8. *$U \cap N = V \cap N \leq N_U \cap N_V$.*

Proof. By 3.7 the group $\overline{N_U \cap N_V}$ is transitive on $\overline{\Omega}^*$. Thus there is $x \in N_U \cap N_V$ such that x has no fixed point on $\overline{\Omega}^*$. Each element in $x \cdot (V \cap N) \subseteq V$ has, by Kronecker conjugacy, a fixed point in Ω, and this point therefore has to lie in Ω_1, because all the other blocks Ω_i are moved. As x is trivial on Ω_1, every element in $V \cap N$ has a fixed point on Ω_1. But $\widetilde{V \cap N}$ is normal in the primitive (on Ω_1) group $\widetilde{V}$, so is must be trivial. So $V \cap N \leq N_U$, in particular $V \cap N \leq U \cap N$, and the rest follows by symmetry. □

The next assertion rids us of the case $M/N_U = \mathrm{S}_4$.

Lemma 3.9. *$[M : U] = [M : V] = p$ and $C_p \leq M/N_U, M/N_V \leq \mathrm{AGL}_1(p)$.*

Proof. Suppose $M/N_U = \mathrm{S}_4$. Then $M = N_U N$ by 3.6. Thus $U = N_U(U \cap N)$. From 3.8 we further get $U \leq N_U$, which of course is nonsense. □

So from now on $p \in \mathbb{P}$. We introduce some more notation. Set

$$A = N_U \cap N_V Z_p,$$
$$B = N_U \cap N_V.$$

Note that A and B are normal subgroups of M.

Lemma 3.10. *$|A/B| = p$.*

Proof. $N_V Z_p/N_V$ is the unique minimal normal subgroup of M/N_V; thus

$$N_V Z_p \leq N_U N_V.$$

Therefore the natural map

$$A \longrightarrow N_V Z_p/N_V$$

is surjective with kernel B, and the assertion follows. □

Here, and in the following, we need the easy

Proposition 3.11. *Let X be a (not necessarily faithful) transitive permutation group with a subgroup Y, such that every element in $X \setminus Y$ has a fixed point. Then every element in $X \setminus Y$ has exactly one fixed point.*

Proof. Let o be the number of orbits of Y. Denote by $F(x)$ the number of fixed points of x. The orbit formula yields

$$\begin{aligned} 1 &= \frac{1}{|X|}\left(\sum_{x\in X\setminus Y} F(x) + \sum_{y\in Y} F(y)\right) \\ &\geq \frac{1}{|X|}\big((|X|-|Y|)+|Y|o\big), \end{aligned}$$

and hence $o \leq 1$. Thus $o = 1$, and equality holds everywhere. □

Lemma 3.12. *$U \cap N = V \cap N = 1$, and $N = Z_p$.*

Proof. From 3.7 we know that B is not contained in N. Thus A is transitive on $\overline{\Omega}^*$. Choose $a \in A \setminus B$. By 3.5 and 3.11 we get that a fixes exactly one element in $\overline{\Omega}^*$. Write $a = zv$ with $z \in Z_p$ and $v \in N_V$. Then $z \neq 1$, because $a \notin N_V$. As a, and hence v, fixes exactly one element Ω_i in $\overline{\Omega}^*$, and v has order p on Ω_1, v fixes a point in Ω_i. Set $w = v^{p-1}$. By 3.10, a^{p-1} is still in $A \setminus B$, so a^{p-1} and thus also w fixes exactly one element in $\overline{\Omega}^*$. As v has order p on M, and order a divisor of $p-1$ on Ω_i, we conclude that w is trivial on Ω_i, non–trivial on Ω_1, and moves all the blocks Ω_j except for Ω_1 and Ω_i. By 3.8 we have $V \cap N \leq N_U$, so every element in $w(V \cap N)$ has fixed points only on Ω_i, and the same holds for $V \cap N$. But $V \cap N$ acts as a subgroup of $\mathrm{AGL}_1(p)$ on Ω_i, so it fixes a point in Ω_i. Thus $V \cap N \leq U^t \cap N = (U \cap N)^t$ for some $t \in G \setminus M$. Again using 3.8 we get $V \cap N \leq N_U^t$. The Ω_i we got could have been any Ω_j different from Ω_1 (by transitivity of A on $\overline{\Omega}^*$), so there is a set of coset representatives $\{t_1, t_2, \ldots, t_m\}$ of M in G such that $V \cap N \leq N_U^{t_i}$ for all i. As $N_U \trianglelefteq M$, we get $V \cap N \leq \mathrm{core}_G(N_U) = 1$. The latter assertion is obvious, as $Z_p \leq N$ has regular orbits on each Ω_i. □

Lemma 3.13. *M/N_U is a homomorphic image of $\overline{M} = M/N$.*

Proof. By 3.12 we get

$$M/N = VN/N \cong V \twoheadrightarrow VN_U/N_U = M/N_U.$$

□

The next proposition collects the information to be used most frequently in the following.

Proposition 3.14. *The following hold.*

(a) $[M : U] = [M : V] = p$ *and* $C_p \leq M/N_U, M/N_V \leq \mathrm{AGL}_1(p)$ *for some prime* p.
(b) $|\overline{A}/\overline{B}| = p$.
(c) $|\overline{M}/\overline{N_U}|$ *divides* $p-1$.
(d) $|\overline{N_U}/\overline{B}|$ *divides* $p(p-1)$.
(e) *Every element of* $\overline{A} \setminus \overline{B}$ *fixes an element in* $\overline{\Omega}^*$.
(f) $N = Z_p$.
(g) M/N_U *is a homomorphic image of* $M/N = \overline{M}$.

Proof. (a) is just 3.9.

(b) follows from 3.12, as A has trivial intersection with N.

As for (c), we have (as $N = Z_p$ by 3.12) $\overline{M}/\overline{N_U} = MZ_p/N_UZ_p = M/N_UZ_p$, and the assertion follows from (a).

(d) follows from $N_U \cap N = 1$ (3.12) and $N_U/B = N_U/N_U \cap N_V = N_U N_V/N_V \leq M/N_V$.

(e) follows from 3.5, (f) is 3.12, and (g) is 3.13. □

The strategy now is the following. The list in 2.8 tells us that $\overline{G}$ is one of the following groups:

> A_m ($m \geq 5$ odd), S_m ($m \geq 4$), M_{11}, M_{23}, $\mathrm{PGL}_2(5)$, $\mathrm{PGL}_2(7)$, $\mathrm{P\Gamma L}_2(8)$, and $\mathrm{P\Gamma L}_2(9)$.

In $\overline{M}$ we find the normal subgroups $\overline{B} \lhd \overline{A} \trianglelefteq \overline{N_U}$, and use the information provided in Proposition 3.14 to determine the possibilities for G/N and N and the action of G/N on N. If N has a complement in G, we can immediately write down G. In the other cases, we prefer to use the classification of transitive groups of small degrees, or in two instances the computer algebra system GAP (see [30]) to determine the possibilities.

Lemma 3.15. *The extension*

$$1 \to N \to M \to M/N \to 1$$

splits. Let $m = [G : M]$ be the degree of $\overline{G}$. If $(m, p) = 1$, then also

$$1 \to N \to G \to G/N \to 1$$

splits.

Proof. The first part follows from 3.12, as U is a complement of N in M.

Let $f \in \mathrm{H}^2(G/N, N)$ describe the extension $1 \to N \to G \to G/N \to 1$. Then, by the first part,

$$\mathrm{res}_{G/N \to M/N}(f) = 0.$$

On the other hand, we have the well–known relation between restriction and corestriction of cohomology groups

$$\mathrm{cor}_{M/N \to G/N}(\mathrm{res}_{M/N \to G/N}(x)) = x^m$$

for all $x \in \mathrm{H}^2(G/N, N)$. As $(m, |N|) = 1$, the restriction is injective, so $f = 0$ and the assertion follows. □

Lemma 3.16. *If $\overline{G} = \mathrm{A}_m$, then $m = 5$, $p = 3$, and $G = \mathrm{GL}_2(4)$.*

Proof. By 3.14 $\overline{M}$ has normal subgroups $\overline{A}$ and $\overline{B}$ with $|\overline{A}/\overline{B}| = p$. If $m \geq 6$, then $\overline{M} = \mathrm{A}_{m-1}$ is simple, so this cannot occur at all. If $m = 5$, then $\overline{M} = \overline{N_U} = \overline{A} = \mathrm{A}_4$, $\overline{B} = C_2 \times C_2$ is the only configuration such that each element in $\overline{A} \setminus \overline{B}$ has a fixed point.

Now $N = C_3$ (by 3.14(f)), and $\overline{G} = \mathrm{A}_5$ can act only trivially on C_3. From 3.15 we gets $G = \mathrm{GL}_2(4)$. □

Lemma 3.17. *If $\overline{G} = \mathrm{S}_m$, then either $m = 5$, $p = 3$, and $G = \Gamma\mathrm{L}_2(4)$, or $m = 4$, $p = 2$, and $G = \mathrm{GL}_2(3)$.*

Proof. If $m \geq 6$, then the only possibility could be $\overline{A} = \mathrm{S}_{m-1}$, $\overline{B} = \mathrm{A}_{m-1}$. But it is immediate that for $m \geq 6$ there are fixed-point-free elements in $\mathrm{S}_{m-1} \setminus \mathrm{A}_{m-1}$; for instance if $m - 1$ is odd, then choose an $(m-1)$–cycle, and if $m - 1$ is even, then take the product of an $(m-3)$–cycle with a disjoint transposition.

Thus $m \leq 5$. If $m = 5$, then as in 3.16 we get $\overline{N_U} = \overline{A} = \mathrm{A}_4$, $\overline{B} = C_2 \times C_2$; thus $p = 3$. By 3.14(g) we get that M/N_U is a homomorphic image of S_4. On the other

hand, $C_3 \le M/N_U \le D_3$. That is only possible if $M/N_U = D_3$. Thus N is not central in G. There is a unique nontrivial action of S_4 on C_3, so from 3.15 we get $G = \Gamma L(2,4)$.

If $m = 4$, then $\overline{M} = \overline{N_U} = \overline{A} = S_3$ and $\overline{B} = C_3$, hence $p = 2$. Here $H^2(G/N, N) = C_2 \times C_2$, so rather than considering the 4 cases we use the classification of transitive groups of small degree [2]: There are just two groups of degree 8 and size 48. One is $GL_2(3)$ and the other one is $S_2 \times S_4$, acting on a 2×4 array with S_2 switching the rows, and S_4 permuting the columns. This group, however, does not contain a cyclic subgroup Z of order 8. Thus $G = GL_2(3)$. □

Lemma 3.18. *$\overline{G}$ is different from M_{11} and M_{23}.*

Proof. The case $\overline{G} = M_{23}$ dies immediately, as $\overline{M} = M_{22}$ is simple, and so the required normal subgroup $\overline{B}$ does not exist.

Now suppose $\overline{G} = M_{11}$. Then the simple group $PSL_2(9)$ has index 2 in $\overline{M}$. Thus $\overline{A} = \overline{M}$ and $\overline{B} = PSL_2(9)$. As M_{11} is sharply 4–transitive, $\overline{A}$ is sharply 3–transitive. By 3.11 every element of $\overline{A}$ with exactly two fixed points lies in $\overline{B}$. The permutation group $PGL_2(9)$ is also sharply 3–transitive, so it must have the same number of elements with exactly two fixed points as $\overline{A}$ has, so all these elements are lying in $PSL_2(9)$. However, that is not the case. Let α be a generator of the multiplicative group of the finite field $\mathbb{F}_9$. Then the image in $PGL_2(9)$ of the diagonal matrix with entries 1 and α fixes two points, but does not lie in $PSL_2(9)$. □

Lemma 3.19. *If $\overline{G} = PGL_2(5)$, then $p = 2$ and $G = GL_2(5)/C_2$ (see section 2.4 for this notation).*

Proof. We have $C_5 \le \overline{B} < \overline{A} \le \overline{N_U} \le \overline{M} = AGL_1(5)$. Thus $p = 2$ by 3.14(g). A look at [28] shows that $GL_2(5)/C_2$ and $S_2 \times PGL_2(5)$ are the only transitive groups of degree 12 and size 240. As G contains an element of order 12, only $G = GL_2(5)/C_2$ is possible. □

Lemma 3.20. *If $\overline{G} = PGL_2(7)$, then $p = 2$, $G = GL_2(7)/C_3$, or $p = 3$, $G = GL_2(7)/C_2$.*

Proof. As in the previous case we get $p = 2$ or 3. First consider $p = 3$. As $AGL_1(7) \twoheadrightarrow M/N_U$ (3.14(f)), we have $M/N_U \le C_6$, so $M/N_U = C_3$. Therefore G is a subgroup of the wreath product $C_3 \wr PGL_2(7)$; in particular, N is central in G. From 3.15 we get $G = GL_2(7)/C_2$.

The case $p = 2$ is more elaborate. The second cohomology $H^2(G/N, N)$ has size four; also there is no list of the transitive groups of degree 16. So we prefer to make an exhaustive search as follows. $PGL_2(7)$ is generated by the 8–cycle $(1\ 2\ 3 \cdots 8)$ and $(1\ 7)(2\ 8)(3\ 4)$. Set $a_i = (i\ i+8)$ for $i = 1, 2, \dots, 8$ and $W := \langle a_1, a_2, \dots, a_8 \rangle$. Set $\sigma_1 = (1\ 2\ 3 \cdots 8)(9\ 10\ 11 \cdots 16)$, $\sigma_2 := (1\ 7)(2\ 8)(3\ 4)(9\ 15)(10\ 16)(11\ 12)$.

Then $G \le C_2 \wr PGL_2(7) = \langle W, \sigma_1, \sigma_2 \rangle$. Then N is generated by $\sigma_3 := a_1 a_2 \cdots a_8$. There are $w_1, w_2 \in W$ with $G = \langle w_1\sigma_1, w_2\sigma_2, \sigma_3 \rangle$.

To find the possibilities for w_1, w_2, first note that we may replace $w_1\sigma_1$ by the conjugate $(w_1\sigma_1)^w$ for $w \in W$; this amounts of switching the labellings of certain pairs $i, i+8$. As σ_1 is an 8–cycle, a moment's thought shows that there are just two orbits under the action of W on $W\sigma_1$ by conjugation; they are given by $(1\ 9)\sigma_1$ and σ_1. For w_2 we have to consider all the 2^8 possibilities, though, and to check when $|\langle w_1\sigma_1, w_2\sigma_2, \sigma_3 \rangle| = 2 \cdot |PGL_2(7)|$. Then we check the surviving groups for conjugacy in the full wreath product $C_2 \wr PGL_2(7)$, and find that there are just the

two cases, $\mathrm{GL}_2(7)/C_3$ and $\mathrm{S}_2 \times \mathrm{PGL}_2(7)$. As in the former cases, we conclude that $G = \mathrm{GL}_2(7)/C_3$. The implementation of the procedure just described in GAP is straightforward, and so we omit it here. □

Lemma 3.21. *$\overline{G}$ is different from $\mathrm{P\Gamma L}_2(8)$.*

Proof. The argument as given in 3.19 shows that $p = 3$ or $p = 7$. Suppose $p = 3$. Then $|\overline{M}/\overline{N_U}|$ divides $p - 1 = 2$ (by 3.14(c)), and it also divides $[\mathrm{A\Gamma L}_1(8) : C_8] = 3 \cdot 7$, so $\overline{M} = \overline{N_U}$.

By 3.14(b) and 3.14(d) we also get that $|\overline{N_U}/\overline{A}|$ divides $p - 1$ (and also $3 \cdot 7$); hence $\overline{A} = \overline{M} = \mathrm{A\Gamma L}_1(8)$, and therefore $\overline{B} = \mathrm{AGL}_1(8)$. It is easy to see that each element in $\mathrm{A\Gamma L}_1(8) \setminus \mathrm{AGL}_1(8)$ has no or exactly two fixed points; thus, by 3.11, each such element is contained in $\overline{B}$, a contradiction.

To rule out $p = 7$ we have to recall the polynomial context our groups came from, for otherwise $G = \Gamma\mathrm{L}_2(8)$, for instance, would be an example matching all the group theoretic requirements used so far.

Let $\dot{G}$ be the geometric monodromy group of the polynomial f; then $\dot{G}$ is a transitive normal subgroup of G (see section 2.2). For $X \leq G$ set $\dot{X} = \dot{G} \cap X$. We still have $N = Z_2 \leq \dot{G}$. As no nontrivial normal subgroup of $\mathrm{P\Gamma L}_2(8) = G/N$ is a monodromy group of a polynomial (see Proposition 2.8), we get $G = \dot{G}N$; thus $G = \dot{G}$. So we may assume that G is already a geometric monodromy group. From 3.14(g) we get $\mathrm{A\Gamma L}_1(8) \twoheadrightarrow M/N_U$; thus $M/N_U = C_7 \rtimes C_3$. So also $C_7 \rtimes C_3$ is a geometric monodromy group of a polynomial, contrary to Proposition 2.8. □

Lemma 3.22. *If $\overline{G} = \mathrm{P\Gamma L}_2(9)$, then $p = 2$ and $G = \Gamma\mathrm{L}_2(9)/C_4$.*

Proof. We have $[\mathrm{A\Gamma L}_1(9) : C_9] = 2^3 \cdot 2$; hence $p = 2$ as in 3.19. To exhibit the structure of G, we use the analogous procedure as in the case $\overline{G} = \mathrm{PGL}_2(7)$, $p = 2$. □

3.3. **The case $C_r \leq \overline{G} \leq \mathrm{AGL}_1(r)$.** We are left to consider the case that $C_r \leq \overline{G} \leq \mathrm{AGL}_1(r)$ for some prime r. In order to rule out many group theoretic configurations (which otherwise could occur), we will partially make use of the genus 0 condition (see section 2.2) or argue directly with the polynomials $f(X) = a(b(X))$, $g(X) = a(b'(X))$. As in the proof of Lemma 3.21, we will thus use the geometric monodromy group $\dot{G} \trianglelefteq G$. For $X \leq G$ set $\dot{X} := \dot{G} \cap X$. We use the information about the genus 0 generators of $\dot{G}$ as in 2.2 without further comment. The first lemma already shows that this case behaves completely different from the case that $\overline{G}$ is triply transitive (compare with Lemma 3.7).

Lemma 3.23. *$N_U N_V \leq N$.*

Proof. Choose $u \in N_U \setminus N_V$. Then, by Lemma 3.5, u has a fixed point on $\overline{\Omega}^*$. On the other hand, $\overline{M}$ acts fixed–point–freely on $\overline{\Omega}^*$; hence $u \in N$. Thus $N_U = \langle N_U \setminus N_V \rangle \leq N$. From symmetry we get $N_V \leq N$ as well. □

We call a polynomial *cyclic* or *dihedral*, if it equals X^n or $T_n(X)$ up to linear changes respectively. By Lemma 2.9 we know that the polynomial a corresponding to $\overline{G}$ is either a cyclic or a dihedral polynomial. Let $r \in \mathbb{P}$ be its degree. In the following we will encounter two cases where Z will happen to be normal in G. A short number theoretic argument rules this out.

Lemma 3.24. *Z is not normal in G.*

Proof. Suppose $Z \trianglelefteq G$. The case $M/N_U = \mathrm{S}_4$ does not occur, for otherwise also Z_4 would be normal in G; but $Z_4 N_U/N_U$ is not normal in M/N_U.

So $p \in \mathbb{P}$, and G is a subgroup of $\mathrm{AGL}_1(pr)$. Set $R = \mathbb{Z}/pr\mathbb{Z}$. We identify the action of G on Ω with the natural action of G on R, where G consists of permutations $x \mapsto \mu x + \theta$. For elements in R, a congruence modulo p or r has its obvious meaning.

The multiplicative group of R is generated by (at most) two elements, so also U is generated by two elements. As $V \cong U$ (from $V \cong VZ/Z = UZ/Z \cong U$), also V is generated by two elements. Without loss (and by Kronecker conjugacy), one of the generators fixes 0. Let γ be a fixed point of the other generator. Thus V is generated by elements

$$A:\ x \mapsto \alpha x,$$
$$B:\ x \mapsto \beta x + \gamma(1-\beta).$$

As V is abelian, we have $AB = BA$, which gives

$$(1-\alpha)(1-\beta)\gamma = 0.$$

As $\gamma \neq 0$ (for otherwise V fixes 0, and we are done), we assume without loss that

$$\alpha \equiv 1 \pmod{p}.$$

The fact that $A^e B^f \in V$ has a fixed point translates to the divisibility relation $(\alpha^e \beta^f - 1) \mid (\gamma(1-\beta^f))$. As β is a unit in R, we find an exponent f such that $\alpha\beta^f - 1 \equiv 0 \pmod{r}$. So (choosing $e = 1$) $\alpha\beta^f - 1$ is divisible by r, and divides $\gamma(1-\beta^f)$. But r does not divide $1-\beta^f$, for otherwise r would also divide $(\alpha\beta^f - 1) + (1-\beta^f) = (\alpha-1)\beta^f$, so even $\alpha \equiv 1 \pmod{r}$; hence $\alpha = 1$, a contradiction.

So r divides γ. But then γ is also a fixed point of A, as $\alpha \equiv 1 \pmod{r}$, so $\alpha\gamma = \gamma$. So V fixes γ; that is, U and V are conjugate in G. □

We are now going to rule out the case that a is a dihedral polynomial.

Lemma 3.25. *The polynomial a is cyclic.*

Proof. Suppose otherwise. Then a is a dihedral polynomial of degree $r \geq 3$. Let $\sigma_1, \sigma_1, \dots, \sigma_R$ be a genus 0 system of $\dot{G}$. Without loss (using braiding), we may assume that $\overline{\sigma_1}, \overline{\sigma_2}$ is a genus 0 system corresponding to a, thus generating $\overline{G}$. We know that $\overline{\sigma_1}$ and $\overline{\sigma_2}$ are involutions, each fixing exactly one block Ω_i. So suppose that σ_1 and σ_2 fix Ω_{i_1} and Ω_{i_2} setwise, respectively. Let b_1 and b_2 be the branch points of a corresponding to $\overline{\sigma_1}$ and $\overline{\sigma_2}$ respectively. The preimage $a^{-1}(b_i)$ contains $(r-1)/2$ double points and a single point c_i. The fiber $b^{-1}(c_1)$ tells us how σ_1 acts on Ω_{i_1}. If all the elements in $b^{-1}(c_1)$ are distinct, then σ_1 is trivial on Ω_{i_1}. But this cannot happen by Lemma 3.24, as then σ_1 is conjugate to an element in N_U, which acts as an involution on $\overline{\Omega}^*$, hence is not contained in N.

So c_1 is a branch point of the polynomial b, and with the same argument c_2 is too. So b has at least two finite branch points, so it either is dihedral or has monodromy group S_4. The latter cannot happen. Namely by Lemma 3.6 we find an $n \in N$ such that $\sigma_1 n$ is trivial on Ω_{i_1}, again contradicting Lemma 3.23.

So b is a dihedral polynomial. By linear changes we may assume that $f(X) = \rho_1 \dot{f}(\rho_3(X) + \rho_4) + \rho_2$ with $\dot{f}(X) = T_r(\gamma T_p(X) + \delta)$ with $\rho_i, \gamma, \delta \in \mathbb{C}$ and ρ_1, ρ_3, γ nonzero. The branch points of T_p and T_r are 2 and -2. So, by the above consideration, we must have $\{c_1, c_2\} = \{2, -2\}$. This shows that either $2\gamma + \delta = 2$ and

$-2\gamma+\delta=-2$, or $-2\gamma+\delta=2$ and $2\gamma+\delta=-2$. Thus $\delta=0$ and $\gamma=1$ or -1. As T_r is an odd polynomial, we have $\dot{f}(X)=\pm T_r(T_p(X))=\pm T_{rp}(X)$.

Thus $\dot{G}=D_{rp}$. But then G normalizes Z, for if some $g\in G$ did not, then g would map a generator of Z to an involution in $\dot{G}$, which of course is nonsense. We are done by Lemma 3.24. □

Lemma 3.26. *The polynomial f has at least 2 finite branch points.*

Proof. Suppose otherwise. Then f is a cyclic polynomial, so $C_{rp}\le G\le \mathrm{AGL}_1(rp)$. The claim follows from Lemma 3.24. □

Now again let $\sigma_1,\sigma_2,\dots,\sigma_R$ be a genus 0 system for $\dot{G}$, where $\overline{\sigma_1}$ should generate the cyclic group $\overline{\dot{G}}$. Thus $\sigma_2,\sigma_3,\dots,\sigma_R$ are in $\dot{N}$. We will use these elements to show that the group $\dot{N}$ is not too small.

Lemma 3.27. *If $p\neq 4$ (that is, $M/N_U\neq \mathrm{S}_4$), then $C_p^r\le\dot{N}$.*

Proof. We view G in the natural way as being a subgroup of the wreath product $\mathrm{AGL}_1(r)\ltimes\mathrm{AGL}_1(p)^r$. Write

$$\sigma_1=c\cdot(d_1,d_2,\dots,d_r),$$

where $c\in\mathrm{AGL}_1(r)$ induces the cyclic shift $(1,2,\dots,r)$ on the blocks Ω_i, and with $d_i\in\mathrm{AGL}_1(p)$. We have the genus 0 condition

$$\sum_{i=1}^{R}\operatorname{ind}\sigma_i=pr-1.$$

Next compute that

$$\sigma_1^r=(\delta_1,\delta_2,\dots,\delta_r)$$

with $\delta_1=d_1d_2\cdots d_r$ and δ_i conjugate to δ_1 in $\mathrm{AGL}_1(p)$. Suppose that δ_1 has k orbits on Ω_1. Then also σ_1 has k orbits on Ω. So $\operatorname{ind}\sigma_1=pr-k$. The above relation gives

$$\sum_{i=2}^{R}\operatorname{ind}\sigma_i=k-1\le p-1.$$

Suppose that one of the $\sigma_2,\dots,\sigma_R$, say σ_w, induces the action of an element in $\mathrm{AGL}_1(p)\setminus C_p$ on Ω_i for some i, but fixes all the other Ω_j's pointwise. Then the group generated by the commutators $[n,\sigma_w]$, $n\in\dot{N}$, induces a cyclic group of order p on Ω_i, and is trivial on all the other Ω_j's. Conjugating by powers of σ_1 then yields the assertion in this case.

Another case is that one of the elements $\sigma_2,\dots,\sigma_R$ is trivial on all but one Ω_i, and is a p-cycle on this block. Then again $C_p^r\le\dot{N}$ as above.

Any non–trivial element in $\mathrm{AGL}_1(p)$ is either a p-cycle, hence has index $p-1$, or is an involution, hence has index $(p-1)/2$, or has index $>(p-1)/2$. So the only case not covered yet and which is allowed by the above genus relation is $k=p$, $R=2$, and σ_2 induces an involution on two Ω_i's, and is trivial on all the other

Ω_j's. Then $\delta_1 = 1$. Set

$$\begin{aligned}\omega_1 &= d_2 d_3 \cdots d_r,\\ \omega_2 &= d_3 d_4 \cdots d_r,\\ &\cdots,\\ \omega_{r-1} &= d_r,\\ \omega_r &= 1.\end{aligned}$$

We replace σ_1 and σ_2 by their conjugates with $(\omega_1, \omega_2, \dots, \omega_r)$ and obtain $\sigma_1 = c$. So $\sigma_2 = (1, 1, \dots, 1, \tau_1, 1, \dots, 1, \tau_2, 1, \dots, 1)$, where τ_1, τ_2 are involutions in $\mathrm{AGL}_1(p)$. They are distinct, for otherwise σ_1 and σ_2 would generate a group containing no subgroup which is transitive on Ω_1. Now suppose $r \geq 3$ for a moment. Then there is a power c^e of c such that σ_2 and $\sigma_2^{c^e}$ have only one position in common, where both components are nontrivial. Thus the commutator $[\sigma_2, \sigma_2^{c^e}]$ has order p on the corresponding Ω_i, and is trivial on all the other Ω_j's. So in this case, again $C_p^r \leq \dot{N}$. Now if $r = 2$ and $C_p^2 \not\leq \dot{N}$, then p^2 does not divide the order of $\dot{N}$. By Proposition 2.5 we know that $|N/\dot{N}|$ divides $\varphi(2p)$. If $p = 2$, then G has degree 4, and there is nothing to do. If $p \neq 2$, then $\varphi(2p) = p - 1$, so p^2 does not divide $|N|$. Thus U and V are Hall subgroups of the solvable group $M = N$, and hence they are conjugate by P. Hall's theorem [14, 6.4.1], a contradiction. □

Lemma 3.28. *The case $p \neq 4$ does not occur.*

Proof. Let $C = C_p^r$ be the subgroup of N from the previous lemma. As $N \leq \mathrm{AGL}_1(p)^r$, we conclude that C is the normal Sylow p-subgroup of N. Thus $M = UC = VC$. Regard C as the $\mathbb{F}_p$-vector space $\mathbb{F}_p^r$. We get that $U \cap C$ and $V \cap C$ are subspaces of codimension 1. Then, by Kronecker conjugacy, each element in $V \cap C$ has a 0 in at least one component. Suppose $p > 2$ for a moment. This forces that there is an i such that all the elements in $V \cap C$ have a 0 in the i-th position. Suppose that there is an element $v \in V \cap N$ which has no fixed point on Ω_i. Then v^{p-1} lies in C. But then there is $c \in V \cap C$, so that cv has no fixed point at all, contrary to Kronecker conjugacy. Thus each element in $V \cap N$ has a fixed point on Ω_i. As this group induces a subgroup of $\mathrm{AGL}_1(p)$, it then even fixes a point on Ω_i. There are three subcases which require different arguments. If $i = 1$, then every element of V fixes a point in Ω_1 (as by Kronecker conjugacy each element in $V \setminus N$ must fix a point in Ω_1), so V is not transitive on Ω_1, contrary to Lemma 3.4. Now suppose $i > 1$. If $M = N$, then $V = V \cap N$, and we have just seen that then V is a point stabilizer, thus conjugate to U. Now assume that $M > N$, and choose an $m \in M$ which moves Ω_i. Further, as N_V fixes a point on Ω_i, but is also normal in M, it is trivial on Ω_i as well as on Ω_i^m. Therefore p^2 divides $[C : N_V \cap C]$. On the other hand, this index equals the size of CN_V/N_V, and the latter group is a subgroup of M/N_V with order dividing $p(p-1)$.

So we must have $p = 2$. Note that $\overline{\dot{G}} = C_r$, so certainly $C = \dot{N} = N$. In particular, $\dot{U}, \dot{V} \leq N$. We finish as above if $V \cap C$ stabilizes a point. Suppose that this is not the case. Also $\dot{U} \cap C$ and $\dot{V} \cap C$ have index p in C; therefore $\dot{U} \cap C = U \cap C$ and $\dot{V} \cap C = V \cap C$. So $\dot{U}$ and $\dot{V}$ are Kronecker conjugate in $\dot{G}$, but not conjugate. In terms of polynomials, we may assume after some linear changes over the complex numbers that $f(X) = (X^2 + 1)^r$ and $g(X) = (X^2 + \gamma)^r$ for some $\gamma \neq 0$. But f and g have the same branch points by Lemma 2.14. The branch

points of f are 0 and 1, and those of g are 0 and γ^r. Thus $\gamma^r = 1$. Let ζ satisfy $\zeta^2 = \gamma$. Then $g(\zeta X) = f(X)$, so f and g are linearly related; therefore $\dot{U}$ and $\dot{V}$ are conjugate by Lemma 2.10. □

Now we are going to rule out the case $M/N_U = \mathrm{S}_4$. The procedure is similar to the above, but even more complicated. The reader might wonder if there are no better arguments. Maybe there are, but on the other hand we are very close to the actual existence of strongly Kronecker conjugate polynomials. Indeed, if we replace S_4 by D_4, then a careful analysis of the type of difficulties encountered in the following led to an infinite series; see [23].

From now on we assume $M/N_U = \mathrm{S}_4$, and thus $p = 4$.

Lemma 3.29. *If $r > 3$, then $\mathrm{A}_4^r \le N$.*

Proof. Again let $\sigma_1, \sigma_2, \dots, \sigma_R$ be a genus 0 system for $\dot{G}$ with $\overline{\sigma_1}$ being an r-cycle, and $\sigma_i \in N$ for $i \ge 2$. Also, imbed G into $\mathrm{AGL}_1(r) \ltimes \mathrm{S}_4^r$, and write $\sigma_1 = c(d_1, d_2, \dots, d_r)$ with $d_i \in \mathrm{S}_4$ and c moving Ω_i to Ω_{i+1}. Write $\sigma_1^r = (\delta_1, \delta_2, \dots, \delta_r)$ with $\delta = d_1 d_2 \cdots d_r$. Note that δ_i is conjugate to δ_1 for all i. Let k be the number of orbits of δ_1 on Ω_1. Then (see the procedure above)

$$(\star) \qquad \sum_{i=2}^{R} \operatorname{ind} \sigma_i = k - 1 \le 3.$$

We use the fact from Lemma 3.6 that N induces the full S_4 on each Ω_i. So to start with the easiest case, suppose that there is a σ_w which is trivial on all blocks but Ω_i, and induces either a transposition, a 3-cycle, or a 4-cycle on Ω_i. Then the group generated by the commutators $[n, \sigma_w]$ with $n \in N$ induces A_4 on Ω_i, and acts trivially on all the other blocks. Conjugating by powers of σ_1 shows that $\mathrm{A}_4^r \le N$. Now assume that we cannot find such elements. Then $\operatorname{ind} \sigma_i \ge 2$ for $i \ge 2$; thus $R = 2$. We start with the case $k = 4$. We may assume (see the proof of 3.27) that $\sigma_1 = c$. Write $\sigma_2 = (e_1, e_2, \dots, e_r)$. We go through the different possibilities for σ_2. First assume that σ_2 is trivial on all but three Ω_i's. Then three of the e_i's are transpositions generating S_4, and the other entries are 1. Further, the support of any two of these transpositions has size 2, so their commutator is a 3-cycle. Now, as $r > 3$ is a prime, an easy argument shows that there is a power c^e of c such that σ_2 and $\sigma_2^{c^e}$ have only one position with nontrivial entries in common. So the commutator $[\sigma_2, \sigma_2^{c^e}]$ is a 3-cycle on some Ω_i, and trivial on all the other blocks. As above, we get the assertion. Now suppose that σ_2 is trivial on only two Ω_i's. As $\sigma_1\sigma_2$ is a $4r$-cycle, we get that $(\sigma_1\sigma_2)^r$ is a 4-cycle on each Ω_i. Thus the product of the two nontrivial components of σ_2 is a 4-cycle. Further, by $(\star)$ we get that these two elements are a transposition and a 3-cycle with exactly one point moved by both of them. Again, the commutator $[\sigma_2, \sigma_2^{c^e}]$ is a 3-cycle on some Ω_i and trivial on the others for a suitable e. The case that σ_2 is nontrivial on only one Ω_i cannot occur, as then $\operatorname{ind} \sigma_2 = 3$ implies that σ_2 is a 4-cycle on this Ω, a case we have already dealt with.

So $k \le 3$. The only two cases not covered yet and allowed by $(\star)$ are $k = 3$ and σ_2 is either a double–transposition on one Ω_i, or a product of two transpositions on two different Ω_i's. We first look at the latter case. Let i_1 and i_2 be the positions where σ_2 has a transposition. Let W be the group generated by the commutators $[\sigma_2, n]$, $n \in N$. Then W acts as A_4 on Ω_{i_1} and Ω_{i_2}, and is trivial on the other blocks. Now set $\tau = \sigma_2^{\sigma_1^{i_2 - i_1}}$. Then τ has a transposition at i_2, and (as r is odd)

is trivial at i_1. Thus the group generated by $[\tau, n]$, $n \in N$, acts as A_4 on Ω_{i_2}, and trivially on all the other blocks. Again, $\mathrm{A}_4^r \le N$.

So the remaining case is that σ_2 is a double transposition on one block. Geometrically, that means that the polynomial b has a genus 0 system containing a double transposition. But that does not happen—see Lemma 2.9. □

Lemma 3.30. *The case $M/N_U = \mathrm{S}_4$ does not occur.*

Proof. If $r = 2$ or 3, then this is easily checked using GAP. (One could also refine the above investigation and do this by hand.) Let us assume $r \ge 5$, so $A := \mathrm{A}_4^r \le N$. Of course A is normal in G. Therefore $A \not\le V$. Thus $M = VA$, hence $[A : V \cap A] = 4$. Thus $V \cap A$ contains a Sylow 3-subgroup S of A. Then $S \cong C_3^r$. We first show that for some $i \in \{1, 2, \dots, r\}$ each element of $V \cap N$ has a fixed point on Ω_i. Suppose that this is not the case for i. Then there is $v \in V \cap N$ which induces either a double transposition or a 4-cycle on Ω_i. Let S_i be the subgroup of $S \le V \cap N$, inducing a group of order 3 on Ω_i, and acting trivially on all the other blocks. Then $[S_i, \langle v \rangle]$ contains the Klein 4-group K_4 in its regular action. So we end up with $K_4^r \le V \cap N$, so there were fixed point free elements in $V \cap N$, contrary to Kronecker conjugacy. So, for some i, each element in $V \cap N$ has a fixed point on Ω_i. As $V \cap N$ contains S_i, this group even stabilizes a point in Ω_i. Now we finish similarly as in the proof of 3.28. If $i = 1$, then, as every element in $V \setminus N$ has a fixed point on Ω_1, we get that V is intransitive on Ω_1, contrary to Lemma 3.4. If $M = N$, then $V = V \cap N$ fixes a point, so V and U are conjugate. Finally, suppose $M > N$. Then there is $m \in M$ with $\Omega_i^m \ne \Omega_i$. As $N_V \trianglelefteq M$ has a fixed point on Ω_i, we conclude that N_V is trivial on Ω_i as well as on Ω_i^m. Thus 12^2 divides $[A : N_V \cap A]$. On the other hand, AN_V/N_V is a subgroup of $M/N_V = \mathrm{S}_4$, so $[A : N_V \cap A] = |AN_V/N_V|$ divides 12, a contradiction. □

3.4. **End of the proof.** We summarize the result about the groups which have survived. Using Proposition 2.16, we get

Theorem 3.31. *Let K be a field of characteristic 0, and $f, g \in K[X]$ be properly Kronecker conjugate over K. Suppose that $f(X) = a(b(X))$ with $a, b \in K[X]$, and that neither a nor b is strongly Kronecker conjugate over K to another polynomial. Then G is one of the following groups:* $\mathrm{GL}_2(3)$, $\mathrm{GL}_2(5)/C_2$, $\mathrm{GL}_2(7)/C_3$, $\Gamma\mathrm{L}_2(9)/C_4$, $\mathrm{GL}_2(4)$, $\Gamma\mathrm{L}_2(4)$, $\mathrm{GL}_2(7)/C_2$. *The subgroups U and V are (up to conjugation and interchanging) as in Lemma 2.15.*

This gives us the part about the degrees in Theorem 1.4. We show that f and g are indeed strongly Kronecker conjugate. An argument similar to the one in the proof of Lemma 3.21 shows that $G = \dot{G}$ except for the case $G = \Gamma\mathrm{L}_2(4)$. But in this case, $\mathrm{GL}_2(4) \le \dot{G}$. So $\dot{U}$ and $\dot{V}$ are not conjugate in $\dot{G}$ in all cases. The existence part of Theorem 1.4 is the subject of the next section.

So it remains to prove Theorem 1.2. Let G be one of the groups from subsection 3.2. Let m be the degree of $\overline{G}$, and p the degree of M/N_U. We identify Ω with the elements from $\mathbb{Z}/pm\mathbb{Z}$, and the blocks Ω_i with the residue classes modulo m. So the stabilizer of 0 in D (notation from Proposition 2.5) can be identified with the maps $x \mapsto \alpha x$ for units α in $\mathbb{Z}/pm\mathbb{Z}$. Let $d = (x \mapsto \alpha x)$ be in N. This translates to $\alpha \equiv 1 \pmod m$. Then, as d also fixes a point, we have $d = 1$ by 3.14(f). So even $\alpha \equiv 1 \pmod p$. Suppose $p > 2$. Then either $\alpha = 1 + m$ or $\alpha = 1 + 2m$ is prime to pm and violates the above conclusion, as $(x \mapsto \alpha x) \in D$ by Proposition

2.5. Thus $p = 2$ and m is odd (for otherwise $\alpha = 1 + m$ would work). But none of the constellations which appear in Theorem 1.4 has $p = 2$ and odd m.

4. Existence results

This section is devoted to the proof of the existence part of Theorem 1.4. We proceed as follows. Let G be one of the groups in Theorem 3.31 which survived section 3. Further, choose the subgroups U, V, and M according to section 2.4. Except for the case $G = \Gamma\mathrm{L}_2(4)$, we construct a genus 0 system in G of a polynomial. Then, as a consequence of Riemann's existence theorem, there are a number field E and a Galois extension Π of $E(t)$ (where t is transcendental) with $G = \mathrm{Gal}(\Pi|E(t))$, and rational fields $E(x)$, $E(y)$ and $E(z)$ between $E(t)$ and Π, such that $b(x) = z = b'(y)$ and $a(z) = t$ for polynomials $a, b, b' \in E[X]$. Then $f(X) = a(b(X))$ and $g(X) = a(b'(X))$ is a pair of strongly Kronecker conjugate polynomials.

We left the computation of the genus 0 systems to a GAP program. The following list gives the result. In all cases, there are only 2 finite branch points. We give the group G along with the elements $\sigma_1, \sigma_2, \overline{\sigma_1}$ and $\overline{\sigma_2}$, where $\overline{\sigma_i}$ denotes the action on the cosets of M in G, thus giving a genus 0 system of the polynomial a. We note that as a result of the computation, the cycle types of the σ's are uniquely given in all cases. This, together with the subsequent computation of explicit examples, gives a certain uniqueness result for pairs of Kronecker conjugate polynomials.

$G = \mathrm{GL}_2(3)$,
$\sigma_1 = (2\ 3)(4\ 8)(6\ 7)$, $\sigma_2 = (1\ 2\ 4)(5\ 6\ 8)$,
$\overline{\sigma_1} = (3\ 4)$, $\overline{\sigma_2} = (1\ 3\ 2)$.

$G = \mathrm{GL}_2(5)/C_2$,
$\sigma_1 = (2\ 3)(4\ 7\ 10\ 9)(5\ 6\ 11\ 8)$,
$\sigma_2 = (1\ 4)(2\ 7)(3\ 6)(5\ 12)$,
$\overline{\sigma_1} = (2\ 5\ 4\ 3)$, $\overline{\sigma_2} = (1\ 2)(5\ 6)$.

$G = \mathrm{GL}_2(7)/C_3$,
$\sigma_1 = (5\ 9\ 14)(6\ 10\ 12)(7\ 11\ 16)(8\ 13\ 15)$,
$\sigma_2 = (1\ 5)(2\ 6)(3\ 10)(4\ 9)(7\ 12)(8\ 14)(15\ 16)$,
$\overline{\sigma_1} = (2\ 4\ 3)(5\ 8\ 7)$, $\overline{\sigma_2} = (1\ 2)(3\ 5)(4\ 6)$.

$G = \Gamma\mathrm{L}_2(9)/C_4$,
$\sigma_1 = (1\ 6\ 17\ 4)(2\ 14)(5\ 11\ 15\ 19)(7\ 8\ 13\ 16)(9\ 12\ 10\ 20)$,
$\sigma_2 = (2\ 5)(3\ 15)(7\ 10)(12\ 18)(14\ 20)(17\ 19)$,
$\overline{\sigma_1} = (1\ 4\ 3\ 2)(5\ 9\ 7\ 6)$, $\overline{\sigma_2} = (3\ 5)(6\ 8)(9\ 10)$.

$G = \mathrm{GL}_2(4)$,
$\sigma_1 = (2\ 3\ 15)(4\ 7\ 5)(9\ 11\ 10)(12\ 13\ 14)$,
$\sigma_2 = (1\ 4)(2\ 8)(3\ 12)(6\ 9)(7\ 13)(11\ 14)$,
$\overline{\sigma_1} = (2\ 4\ 3)$, $\overline{\sigma_2} = (1\ 2)(4\ 5)$.

$G = \mathrm{GL}_2(7)/C_2$,
$\sigma_1 = (1\ 2\ 4)(3\ 15\ 12)(5\ 18\ 14)(7\ 21\ 17)(9\ 19\ 23)$
$(11\ 22\ 24)(13\ 16\ 20)$,
$\sigma_2 = (1\ 5)(2\ 7)(3\ 4)(6\ 22)(8\ 16)(9\ 21)(10\ 19)(11\ 15)(13\ 18)$,

$$\overline{\sigma_1} = (2\ 4\ 3)(5\ 7\ 6),\ \overline{\sigma_2} = (1\ 2)(4\ 5)(7\ 8).$$

We treat these groups case by case. As we do not care about the base field, we are free to make several "without loss of generality" assumptions about the location of branch points and their preimages.

4.0.1. $G = \mathrm{GL}_2(3)$. The branching of a is given by $\overline{\sigma_1}$ and $\overline{\sigma_2}$. Without loss, let 0 be the branch point where the triple point lies above; furthermore, we may assume that this triple point is 0, and that the other preimage of 0 under a is 1. Thus $a(X) = X^3(X-1)$. We find the other finite branch point b_1 as follows. Compute the discriminant of $a(X) - t$ with respect to X; then the zero of that discriminant different from 0 is b_1. We get $b_1 = -27/256$ as the point corresponding to the transposition. The polynomials b and b' have, again without loss, the form $b(X) = X^2 + \beta$ and $b'(X) = X^2 + \beta'$. The branching data given by σ_1 and σ_2 tells us what β and β' look like. Let γ and γ' be the two simple points in the preimage under a of b_1. The finite branch point of $b(X)$ must be γ or γ_1. Now $a(X) - b_1 = \frac{1}{256}(16X^2 + 8X + 3)(4X - 3)^2$ tells us that γ and γ' are the zeros of $16X^2 + 8X + 3$. Thus $b(X) = X^2 + \frac{-1+\sqrt{-2}}{4}$ and $b'(X) = X^2 + \frac{-1-\sqrt{-2}}{4}$.

4.0.2. $G = \mathrm{GL}_2(5)/C_2$. To determine a, let $b_1 = 0$ correspond to $\overline{\sigma_1}$, and let 0 be the quadruple point above 0. Then $a(X) = X^4(X^2 + \eta X + \theta)$. As a is indecomposable, η must be nonzero; thus $\eta = 6$ without loss. There are two solutions for b_2 different from 0 of the discriminant of $a(X) - t$. To get the correct one, check the factorization of $a(X) - b_2$ for these two values. We must have two roots of order 2, and two simple roots. That is only the case if $\theta = 25$. Thus $a(X) = X^4(X^2 + 6X + 25)$. (For a different procedure to determine a, see [21].) Again set $b(X) = X^2 + \beta$, $b'(X) = X^2 + \beta'$. From σ_1 and σ_2 we see that β and β' must be one of the two simple points in the fiber $a^{-1}(0)$. So β and β' are the zeros of $X^2 + 6X + 25$. Thus $b(X) = X^2 - (3 - 4i)$ and $b'(X) = X^2 - (3 + 4i)$, where $i^2 = -1$.

4.0.3. $G = \mathrm{GL}_2(7)/C_3$ *and* $G = \mathrm{GL}_2(7)/C_2$. In both cases, we get the same cycle type for the branch cycle description of $a(X)$. The computation is similar as above. We get $a(X) = (343X^2 - 1600 + 1408\sqrt{2})^3(2401X^2 - 11200X + 9856\sqrt{2}X + 46656 - 27008\sqrt{2})$.

The branch point corresponding to σ_1 is 0. Let b_2 be the other branch point. We get that $a^{-1}(b_2)$ contains two points of multiplicity 1. In the case $G = \mathrm{GL}_2(7)/C_3$ these two points are the finite branch points of $b(X) = X^2 + \beta$ and $b'(X) = X^2 + \beta'$ respectively. Computing yields that β and β' are the different solutions of $16807X^2 + 58800X - 51744\sqrt{2}X + 150464 - 84992\sqrt{2} = 0$.

The case $G = \mathrm{GL}_2(7)/C_2$ is a little different, as now the two points of multiplicity 1 in $a^{-1}(0)$ happen to be the finite branch points $b(X) = X^3 + \beta$ and $b'(X) = X^3 + \beta'$. Thus β and β' are the distinct solutions of $2401X^2 - 11200X + 9856\sqrt{2}X + 46656 - 27008\sqrt{2} = 0$.

4.0.4. $G = \Gamma\mathrm{L}_2(9)/C_4$. The polynomial a has the geometric monodromy group $\mathrm{P}\Gamma\mathrm{L}_2(9)$; it has been computed with the given branching data by Matzat [20, 8.7]. The result is $a(X) = (X^2 - 405)^4(X^2 + 50X + 945)$. The two points of multiplicity 1 in $a^{-1}(0)$ are the branch points of $b(X)$ and $b'(X)$. Thus $b(X) = X^2 - (25 - 8\sqrt{-5})$ and $b'(X) = X^2 - (25 + 8\sqrt{-5})$.

4.0.5. $G = \mathrm{GL}_2(4)$. The last case is quite easy. We quickly get the equality $a(X) = X^3(X^2+X+\frac{8}{5})$, and the fact that the branch points of $b(X)$ and $b'(X)$ are the points of multiplicity 1 in $a^{-1}(0)$. From this we conclude that $b(X) = X^2 - (\frac{1}{2} - \frac{3}{10}\sqrt{-15})$ and $b'(X) = X^2 - (\frac{1}{2} + \frac{3}{10}\sqrt{-15})$.

5. Conjectures

We want to state two conjectures. The first one does not look quite hopeless. We have some evidence for it, but are still far away from a solution.

Conjecture 5.1. *Let $f, g \in \mathbb{Q}[X]$ be non-constant polynomials which are strongly Kronecker conjugate over $\mathbb{Q}$. Then, up to linear changes over $\mathbb{Q}$, we have $f(X) = h(X^8)$, $g(X) = h(16X^8)$ for some $h \in \mathbb{Q}[X]$.*

All examples of Kronecker conjugate polynomials we have met so far have the even stronger property of *arithmetical equivalence*. In terms of our groups this means that the permutation characters $\mathbf{1}_U^G$ and $\mathbf{1}_V^G$ are the same. This group theoretic property has been investigated by various authors in different contexts; see [16], [18], [25], and the literature given there. Of course, this property can again be translated back to an arithmetical property of the value sets of polynomials on residue fields.

Conjecture 5.2. *Let K be a field of characteristic 0. If $f, g \in K[X]$ are Kronecker conjugate, then they are arithmetically equivalent.*

We have examples of finite groups G with Kronecker conjugate subgroups U and V, such that G has a cyclic subgroup Z with $G = UZ = VZ$, but $\mathbf{1}_U^G \neq \mathbf{1}_V^G$. So if the conjecture should be true, then it is a fancy consequence of the genus 0 condition from subsection 2.2.

We have no idea how many more types of pairs of Kronecker conjugate polynomials exist. Their determination without further restrictions seems hopeless to us. Still, it would be interesting to exhibit further classes as in Theorem 1.5.

References

1. N. C. Ankeny, C. A. Rogers, *A conjecture of Chowla*, Ann. of Math. **53** (1951), 541–550; **58** (1953), 591. MR **12:**8042; MR **15:**210d
2. G. Butler, J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11**(8) (1983), 863–911. MR **84f:**20005
3. C. Chevalley, *Algebraic Functions of One Variable*, Mathematical Surveys VI, AMS, Providence, 1951. MR **13:**64a
4. J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Clarendon Press, Oxford, New York, 1985. MR **88g:**20025
5. W. Feit, *On symmetric balance incomplete block designs with doubly transitive automorphism groups*, J. Combin. Theory Ser. A, vol. 14 (1973), 221–247. MR **48:**5882
6. W. Feit, *Some consequences of the classification of finite simple groups*, The Santa Cruz conference on finite groups, Proc. Sympos. Pure Math., vol. 37, AMS, Providence, Rhode Island, 1980, 175–181. MR **82c:**20019
7. M. Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55. MR **41:**1688
8. M. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois Journal of Mathematics **17** (1973), 128–146. MR **50:**329
9. M. Fried, *On Hilbert's Irreducibility Theorem*, Journal of Number Theory **6** (1974), 211–231. MR **50:**2117
10. M. Fried, *Rigidity and applications of the classification of simple groups to monodromy, Part II – Applications of connectivity; Davenport and Hilbert-Siegel Problems*, preprint.

11. M. Fried, *Extension of constants, rigidity, and the Chowla-Zassenhaus conjecture*, Finite Fields and their Applications **1** (1995), 326–359. MR **96i:**11120
12. M. Fried, M. Jarden, *Field Arithmetic*, Springer, Berlin, Heidelberg, 1986. MR **89b:**12010
13. M. Fried, R. E. MacRae, *On the invariance of chains of fields*, Illinois Journal of Mathematics **13** (1969), 165–171. MR **39:**179
14. D. Gorenstein, *Finite Groups*, Harper and Row, New York–Evanston–London, 1968. MR **38:**229
15. R. Guralnick, *Zeroes of permutation characters with applications to prime splitting and Brauer groups*, J. Algebra **131** (1990), 294–302. MR **91j:**20038
16. R. Guralnick, *Subgroups inducing the same permutation representation*, J. Algebra **81** (1983), 312–319. MR **84j:**20010
17. W. Jehne, *Kronecker classes of algebraic number fields*, J. Number Theory **9** (1977), 279–320. MR **56:**5499
18. N. Klingen, *Zahlkörper mit gleicher Primzerlegung*, J. reine angew. Math. **299/300** (1978), 342–384. MR **58:**10817
19. L. Kronecker, *Über die Irreduzibilität von Gleichungen*, Werke II, 85–93; Monatsberichte Deutsche Akademie für Wissenschaft (1880), 155–163.
20. B. H. Matzat, *Konstruktion von Zahl– und Funktionenkörpern mit vorgegebener Galoisgruppe*, J. Reine Angew. Math. **349** (1984), 179–220. MR **85j:**11164
21. P. Müller, *Primitive monodromy groups of polynomials*. Contemp. Math. **186** (1995), 385–401. MR **96m:**20004
22. P. Müller, *Reducibility behavior of polynomials with varying coefficients*, Israel J. Math. **94** (1996), 59–91. CMP 96:14
23. P. Müller, *An infinite series of Kronecker conjugate polynomials*, Proc. Amer. Math. Soc. **125** (1997), 1933–1940. CMP 97:10
24. P. Müller, H. Völklein, *On a question of Davenport*, J. Number Theory **58** (1996), 46–54. MR **97h:**12012
25. R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), 342–360. MR **56:**5503
26. C. Praeger, *Kronecker classes of field extensions of small degree*, J. Austr. Math. Soc. (Series A) **50** (1991), 297–315. MR **92m:**12004
27. J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.
28. G. F. Royle, *The transitive groups of degree twelve*, J. Symb. Comp.**4** (1987), 255–268. MR **89b:**20010
29. J. Saxl, *On a question of W. Jehne concerning covering subgroups of groups and Kronecker classes of fields*, J. London. Math. Soc.(2) **38** (1988), 243–249. MR **90b:**11118
30. M. Schönert et. al., *GAP – Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Techn. Hochschule, Aachen, Germany, fourth edition, 1994.
31. 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), 123–134.
32. E. Trost, *Zur Theorie der Potenzreste*, Nieuw Arch. Wiskunde **18** (1934), 58–61.
33. G. Turnwald, *On Schur's conjecture*, J. Austr. Math. Soc. (Series A) **58** (1995), 312–357. MR **96a:**11135
34. H. Völklein. *Groups as Galois Groups – an Introduction*, Cambridge University Press, 1996. CMP 96:17
35. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London, 1964. MR **32:**1252

IWR, Universität Heidelberg, D-69120 Heidelberg, Germany
E-mail address: peter.mueller@iwr.uni-heidelberg.de