

AN INFINITE SERIES OF KRONECKER CONJUGATE POLYNOMIALS

PETER MÜLLER

(Communicated by William W. Adams)

ABSTRACT. Let K be a field of characteristic 0, t a transcendental over K , and Γ be the absolute Galois group of $K(t)$. Then two non-constant polynomials $f, g \in K[X]$ are said to be Kronecker conjugate if an element of Γ fixes a root of $f(X) - t$ if and only if it fixes a root of $g(X) - t$. If K is a number field, and $f, g \in \mathcal{O}_K[X]$ where \mathcal{O}_K is the ring of integers of K , then f and g are Kronecker conjugate if and only if the value set $f(\mathcal{O}_K)$ equals $g(\mathcal{O}_K)$ modulo all but finitely many non-zero prime ideals of \mathcal{O}_K . In 1968 H. Davenport suggested the study of this latter arithmetic property. The main progress is due to M. Fried, who showed that under certain assumptions the polynomials f and g differ by a linear substitution. Further, he found non-trivial examples where Kronecker conjugacy holds. Until now there were only finitely many known such examples. This paper provides the first infinite series. The main part of the construction is group theoretic.

1. INTRODUCTION

Let K be a field of characteristic 0, and $f, g \in K[X]$ be two non-constant polynomials. Fix a transcendental t over K , and let L be a Galois extension 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 $L|K(t)$, and let U and V be the stabilizers of x and y in G respectively. Then f and g are said to be *Kronecker conjugate over K* if $\bigcup_{h \in G} U^h = \bigcup_{h \in H} V^h$. (This definition of course is equivalent to the one in the abstract, but more convenient to use.) The arithmetical interest in Kronecker conjugacy of polynomials comes from a Galois theoretic translation by M. Fried (see [1, 19.27], or [7, Theorem 2.3] for a stronger version) of a question by H. Davenport.

Theorem 1.1 (Fried). *Let K be a number field and \mathcal{O}_K its ring of integers. Let $f, g \in \mathcal{O}_K[X]$ be non-constant polynomials. Then the following are equivalent.*

- (i) *f and g are Kronecker conjugate over K .*
- (ii) *The value sets $f(\mathcal{O}_K)$ and $g(\mathcal{O}_K)$ are the same modulo all but finitely many non-zero prime ideals of \mathcal{O}_K .*

Davenport posed the problem to classify polynomials such that (ii) holds for $K = \mathbb{Q}$. See [7] for a survey of results known to date and some new results. It is

Received by the editors January 18, 1996.

1991 *Mathematics Subject Classification*. Primary 11C08, 11R09, 20B05; Secondary 11R32, 12E05, 12F10.

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

quite easy to see that f and g are Kronecker conjugate if they are linearly related over K , that is, $f(X) = g(rX + v)$ for some $0 \neq r \in K$, $s \in K$. Linear relatedness of f and g over K is easily seen ([7, Lemma 2.10]) to be equivalent to conjugacy of U and V in G . We say that a pair f, g with (i) is *properly Kronecker conjugate* over K if f and g are not linearly related over K . An example is $f(X) = X^8$, $g(X) = 16X^8$ for $K = \mathbb{Q}$. However, f and g are linearly related over the algebraic closure \bar{K} . We say that a Kronecker conjugate pair is *strongly Kronecker conjugate* over K , if it stays properly Kronecker conjugate over \bar{K} . The first such examples were given by M. Fried. They satisfy $\deg f = \deg g \in \{7, 11, 13, 15, 21, 31\}$. As a result of a certain classification, we [7] obtained six more examples of strongly 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 will say that a properly Kronecker conjugate pair f, g is *newly Kronecker conjugate* over K if it has not this form. To date, there were only finitely many known degrees for which there are newly Kronecker conjugate polynomials. In this paper we present the first infinite series. The pairs in this series are even strongly Kronecker conjugate.

Theorem 1.2. *Let $m \geq 3$ be an integer, and ζ be a primitive $4m$ -th root of unity. Set*

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

Then f and g are strongly and newly Kronecker conjugate over any field K which contains $\mathbb{Q}(\zeta)$.

For subgroups U and V of a group G , we say that U and V are *Kronecker conjugate in G* if $\bigcup_{h \in G} U^h = \bigcup_{h \in H} V^h$ holds. This notion has been studied by various authors either in different contexts or purely from the group theoretic point of view; see [4], [3], [1, Section 19.5], [2], [8], [10]. In section 2.1 we construct a finite group G with two non-conjugate subgroups U and V which are Kronecker conjugate. Further, we show that G has a generating system which fulfills a certain combinatorial condition with respect to the action on the coset spaces G/U and G/V , which guarantees that there are (by Riemann's Existence Theorem) polynomials f and g over some number field which have the properties we are looking for. In section 2.2 we use valuation theory and an irreducibility argument relying on Bézout's Theorem to actually compute the polynomials associated to our group theoretic configuration.

2. PROOF OF THEOREM 1.2.

2.1. Group theoretic preparation. Let the dihedral group D of order 8, acting on the letters 1, 2, 3 and 4, be generated by $a = (2\ 3)$ and $b = (1\ 3)(2\ 4)$.

$$\begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline \end{array} \quad \begin{aligned} D &= \langle a, b \rangle, \\ a &= (2\ 3), \quad b = (1\ 3)(2\ 4). \end{aligned}$$

For $k = 1, 2, \dots, m$, let ϕ_k be the homomorphism of D into the symmetric group on the letters $1, 2, \dots, 4m$ given as follows: For $d \in D$ let $\phi_k(d)$ fix all the letters except $4k - 3, 4k - 2, 4k - 1, 4k$. On these letters the action is given by

$r^{\phi_k(d)} = (r - 4k + 4)^d + 4k - 4$. Partition the numbers $1, 2, \dots, 4m$ in groups of size 4 as below.

1	3	5	7	9	11	...	$4m - 3$	$4m - 1$
2	4	6	8	10	12	...	$4m - 2$	$4m$

Then for each $d \in D$, $\phi_k(d)$ acts on the k -th square, and for each k the action of $\phi_k(d)$ on the k -th square is the same.

Now let C be a cyclic group of order $m \geq 3$. For c a generator of C , define an action ϕ of C on $1, 2, \dots, 4m$ by $i^{\phi(c)} \equiv i + 4 \pmod{4m}$. $\phi(C)$ acts by cyclically permuting the squares. So the wreath product $D \wr C = C \ltimes D^m$ acts on the numbers $1, 2, \dots, 4m$ in the obvious way.

Note that the squares do not provide a minimal system of imprimitivity; such a system is rather given by the the diagonals of the squares.

Let τ be the involutory outer automorphism of D which interchanges a and b . Let K be the normal Klein 4-subgroup of D generated by b and b^a . So $\phi_k(K)$ acts regularly on the k -th square.

Now let N be the subgroup of D^m given by

$$N = \{(d_1, d_2, d_3, \dots, d_m) \in D^m \mid d_i \tau(d_{i+1}) \in K \text{ for } i = 1, 2, \dots, m\},$$

where the indices are taken modulo m .

Obviously N is a group (a sort of generalization of a subdirect product), which is invariant under cyclically permuting its components. Thus we form the semi-direct product $G := C \ltimes N$. Besides this abstract description, we also regard G as a permutation group on $\{1, 2, \dots, 4m\}$.

Lemma 2.1. $|N| = 4^m$, and N acts as D on the k -th square for $k = 1, 2, \dots, m$.

Proof. We have 8 choices to choose $d_1 \in D$. Suppose we have chosen already d_i for $i = 1, 2, \dots, k$ with $k \leq m - 2$. Then the condition $d_k \tau(d_{k+1}) \in K$ leaves 4 possibilities to choose d_{k+1} . So there are $8 \cdot 4^{m-2}$ choices for taking d_1, d_2, \dots, d_{m-1} . The last component must meet the conditions $d_{m-1} \tau(d_m) \in K$ and $d_m \tau(d_1) \in K$, that is, $d_m \in \tau(K) d_{m-1}^{-1} \cap K \tau(d_1)^{-1}$. The assertion follows, as one easily checks $|\tau(K)r \cap Ks| = 2$ for all $r, s \in D$.

The latter assertion follows, as the proof shows that d_i can be every element in D . □

Now set

$$\begin{aligned} U &:= \{(d_1, d_2, \dots, d_m) \in N \mid d_1 \in \langle a \rangle\}, \\ V &:= \{(d_1, d_2, \dots, d_m) \in N \mid d_m \in \langle b \rangle\}, \\ W &:= \{(d_1, d_2, \dots, d_m) \in N \mid d_1 \in \tau(K) = \langle a, a^b \rangle\}. \end{aligned}$$

Lemma 2.2. *The following holds.*

- (i) U and V are subgroups of W . Furthermore, $[W : U] = [W : V] = [N : W] = 2$.
- (ii) *The groups U and V are not conjugate in G .*
- (iii) *Let M be a group with $N \leq M < G$. Then U and V are in M not Kronecker conjugate.*

Proof. (i) $U \leq W$ follows from the definitions. Now let $(d_1, d_2, \dots, d_m) \in V$, hence $d_m \tau(d_1) \in K$ and $d_m \in \langle b \rangle < K$, so $\tau(d_1) \in K$. Therefore $d_1 \in \tau(K)$, and the claim follows.

(ii) The first part follows from the definition of G and U . Now suppose that V is conjugate to U . Then V fixes some point. Set $z = (ab)^2$; then $v = (z, z, \dots, z, a, b) \in V$ and $v' = (z, z, \dots, z, a^b, b) \in V$, as $z\tau(z) = 1$, $z\tau(a) = abab \cdot b = b^a \in K$, $a\tau(b) = 1$, and so on. Apparently v and v' do not have a common fixed point, so V has no fixed point.

(iii) Suppose wrong. Let $v = (z, z, z, \dots, z, 1) \in V$ with z from (ii). Then there is some $w \in M$ such that $v^w \in U$. But v has a fixed point only on the m -th square, so w moves the m -th square to the first one. Thus the coset wN generates G/N , contrary to $w \in M < G$. \square

We aim of course to prove Kronecker conjugacy of U and V in G . Actually, it turns out to be convenient to prove an even stronger relation. As a preparation, we need some simple properties of the elements in N . Let \mathcal{C}_i be the conjugacy classes of D labelled as follows.

$$\begin{aligned} \mathcal{C}_1 &= \{()\}, \\ \mathcal{C}_2 &= \{(1\ 2)(3\ 4), (1\ 3)(2\ 4)\}, \\ \mathcal{C}_3 &= \{(1\ 4), (2\ 3)\}, \\ \mathcal{C}_4 &= \{(1\ 4)(2\ 3)\}, \\ \mathcal{C}_5 &= \{(1\ 2\ 4\ 3), (1\ 3\ 4\ 2)\}. \end{aligned}$$

Let $(d_1, d_2, \dots, d_m) \in N$. Then one immediately verifies

$$\begin{aligned} d_i \in \mathcal{C}_1 &\implies d_{i+1} \in \mathcal{C}_1 \cup \mathcal{C}_3 \cup \mathcal{C}_4, \\ d_i \in \mathcal{C}_2 &\implies d_{i+1} \in \mathcal{C}_1 \cup \mathcal{C}_3 \cup \mathcal{C}_4, \\ d_i \in \mathcal{C}_3 &\implies d_{i+1} \in \mathcal{C}_2 \cup \mathcal{C}_5, \\ d_i \in \mathcal{C}_4 &\implies d_{i+1} \in \mathcal{C}_1 \cup \mathcal{C}_3 \cup \mathcal{C}_4, \\ d_i \in \mathcal{C}_5 &\implies d_{i+1} \in \mathcal{C}_2 \cup \mathcal{C}_5. \end{aligned}$$

Lemma 2.3. For $(d_1, d_2, \dots, d_m) \in N$ and $i \in \{1, 2, 3, 4, 5\}$ let N_i be the number of d_j 's in the class \mathcal{C}_i . Then $N_2 = N_3$.

Proof. Go cyclically through the positions $1, 2, \dots, m$. Then the above observation shows that the occurrences of elements in \mathcal{C}_2 and \mathcal{C}_3 alternate. For instance if $d_i \in \mathcal{C}_3$, then if $d_{i+1} \notin \mathcal{C}_2$, then $d_{i+1} \in \mathcal{C}_5$. But a successor of an element in \mathcal{C}_5 also is either in \mathcal{C}_2 or in \mathcal{C}_5 . So after an element in \mathcal{C}_3 an element in \mathcal{C}_2 has to show up, before an element in \mathcal{C}_3 can appear. Similarly we see that between two consecutive occurrences of elements in \mathcal{C}_2 , an element from \mathcal{C}_3 must lie in between. This proves the assertion. \square

For the action of G on the right cosets G/U , let $F_U(g)$ be the number of fixed points of $g \in G$. Analogously define $F_V(g)$.

Theorem 2.4. $F_U(g) = F_V(g)$ for all $g \in G$. In particular, U and V are Kronecker conjugate in G .

Proof. If $g \notin N$, then g fixes no coset of N in G . As $U, V \leq N$, we get $F_U(g) = F_V(g) = 0$. So assume now that $g = (d_1, d_2, \dots, d_m) \in N$. As the action on G/U is the natural action we started with, we get

$$F_U(g) = 4N_1 + 2N_3.$$

Now we are computing $F_V(g)$. A coset Vx is fixed by g if and only if $g \in V^x$. As each coset of V contains $|V|$ elements, we get

$$F_V(g) = \frac{1}{|V|} |\{x \in G \mid g \in V^x\}|.$$

Now write the elements $x \in G$ as $x = cn$ with $c \in C$, $n \in N$. Note that V^c consists of those elements in N which have the identity $()$ or $(1\ 3)(2\ 4)$ at the $c(1)$ -th position. Thus if $d_{c(1)} = ()$, then for all $n \in N$ we have $g \in V^{cn}$. If $d_{c(1)} \in \mathcal{C}_2$, then the number of elements $n \in N$ with $g \in V^{cn}$ has size $|N|/2$. If $d_{c(1)}$ is neither in \mathcal{C}_1 nor in \mathcal{C}_2 , then there is no element $n \in N$ with $g \in V^{cn}$. So we obtain further

$$\begin{aligned} F_V(g) &= \frac{1}{|V|} (N_1|N| + N_2|N|/2) \\ &= 4N_1 + 2N_2. \end{aligned}$$

So the assertion follows from 2.3. □

Recall that $a = (2\ 3)$ and $b = (1\ 3)(2\ 4)$. Set

$$n := (a, b, 1, 1, \dots, 1) \in N$$

and

$$c := (1, 2, 3, \dots, m) \in C.$$

Lemma 2.5. *G is generated by the elements n and c . Further, $c \cdot n$ acts as a $4m$ -cycle on the points $1, 2, \dots, 4m$.*

Proof. Set $z := c \cdot n$. Then z moves cyclically the m sets $\{1, 2, 3, 4\}, \{5, 6, 7, 8\}, \dots, \{4m - 3, 4m - 2, 4m - 1, 4m\}$. So the latter assertion follows once we know that z^m acts as a 4-cycle on one (and hence each) of these sets. We compute

$$\begin{aligned} z^m &= (cn)^m \\ &= c^m n^{c^{m-1}} n^{c^{m-2}} \dots n^c n \\ &= n^{c^{m-1}} n^{c^{m-2}} \dots n^c n \\ &= (b, 1, \dots, 1, a)(1, \dots, 1, a, b) \cdots (1, a, b, 1, \dots, 1)(a, b, 1, \dots, 1) \\ &= (ba, ba, ba, \dots, ba). \end{aligned}$$

But $ba = (1\ 2\ 4\ 3)$, and the latter assertion follows.

Now compute the commutator $[n, n^c] = (1, (ba)^2, 1, \dots, 1)$. As $(ba)^2$ is the central involution in D , we get (by cyclic shifts using c) that $Z(D)^m \leq N$. The 2^m elements $(n^{c^0})^{\epsilon_0} \cdot (n^{c^1})^{\epsilon_1} \dots (n^{c^{m-1}})^{\epsilon_{m-1}}$, for $\epsilon_i \in \{0, 1\}$, are all different modulo $Z(D)^m$, so the group generated by n and c has a least the size $m \cdot 2^m \cdot 2^m = m \cdot 4^m$, and the claim follows from Lemma 2.1. □

Summarizing, we get

Lemma 2.6. *Set σ_1 and σ_2 be the permutations which c and n induce on the elements $\{1, 2, \dots, 4m\}$ respectively. Then*

- (i) $\sigma_1 \sigma_2$ is a $4m$ -cycle.
- (ii) $\sigma_1 = (2\ 3)(5\ 7)(6\ 8)$,
 $\sigma_2 = (1\ 5 \dots 4m - 3)(2\ 6 \dots 4m - 2)(3\ 7 \dots 4m - 1)(4\ 8 \dots 4m)$.
- (iii) σ_1 and σ_2 generate G .

2.2. Existence and computation of f and g . Let t be a transcendental over the complex numbers \mathbb{C} . By a *place at $a \in \mathbb{C}$* we mean the place of $\mathbb{C}(t)$ that maps t to a . For $a = \infty$ the place at a is the place of $\mathbb{C}(t)$ which maps $1/t$ to 0. See [1] for more details. If L is a finite extension of $\mathbb{C}(t)$, then the *branch points* are the $a \in \mathbb{C} \cup \{\infty\}$ such that the place at a is ramified in L .

Riemann's Existence Theorem (see [11], [5]) guarantees the following. There exists a finite Galois extension Π of $\mathbb{C}(t)$ with Galois group (isomorphic to) G , and branch points $b_1 = 0$, $b_2 = 1$, and $b_3 = \infty$, such that σ_1 , σ_2 and $\sigma_3 = (\sigma_1\sigma_2)^{-1}$ are the generators of the inertia groups of places \mathfrak{P}_1 , \mathfrak{P}_2 , and \mathfrak{P}_3 of Π respectively, where \mathfrak{P}_1 , \mathfrak{P}_2 , and \mathfrak{P}_3 lie above 0, 1, and ∞ respectively. For a subgroup M in G , denote by Π_M the fixed field of M in Π . The ramification indices of the places of Π_M lying above b_i are just the orbit lengths of σ_i on the coset space G/M . Now, using Lemma 2.6, we get for the genus g of Π_U using the Riemann-Hurwitz genus formula

$$4(m-1) + 3(2-1) + (4m-1) = 2(4m-1+g),$$

hence $g = 0$. So Π_U is a rational field, and as the place at ∞ is totally ramified in Π_U , we even get that $\Pi_U = \mathbb{C}(x)$ with $f(x) = t$ for some polynomial f . As a consequence of Lemma 2.4, the elements σ_i have the same cycle decomposition with respect to the action on G/V as if acting on G/U . So, by the same argument as above, $\Pi_V = \mathbb{C}(y)$ with $g(y) = t$ for some polynomial g . The inclusions $U, V < W < N < G$ allow for writing $f(X) = a(b(c(X)))$, $g(X) = a(b(\bar{c}(X)))$ for polynomials a , b , c , and \bar{c} , such that $\Pi_W = \mathbb{C}(c(x)) = \mathbb{C}(\bar{c}(y))$ and $\Pi_N = \mathbb{C}(b(c(x)))$ (see e.g. [6, Appendix]).

The polynomials f and g we got are properly Kronecker conjugate over \mathbb{C} . Namely they are Kronecker conjugate by Theorem 2.4. If they were not properly Kronecker conjugate, then an easy argument (see [7, Lemma 2.10]) shows that U and V are conjugate in G , contrary to Lemma 2.2(ii).

For the actual computation of f and g , we are using the following easy fact. Let h be a non-constant polynomial over \mathbb{C} . Consider the field extension $\mathbb{C}(x)|\mathbb{C}(h(x))$. Then the ramification indices of the places above $b \in \mathbb{C}$ are the multiplicities of the zeroes of $h(X) - b$.

Now σ_1 acts as an m -cycle on G/N , so $a(X) - 0$ is the m -th power of a polynomial, which has to be linear as $\deg a = m$. Thus we assume without loss $a(X) = X^m$. The polynomial b has degree 2, so without loss assume $b(X) = X^2 + \delta$. If δ were 0, then σ_1 had to act as a $2m$ -cycle on G/W . But this is not the case. So we may assume $\delta = 1$. Finally, we may assume that $c(X) = X^2 + \kappa$ for some κ . The element σ_2 will help us to determine κ . Let θ be a primitive m -th root of 1, and write

$$\begin{aligned} f(X) - b_2 &= ((X^2 + \kappa)^2 + 1)^m - 1 \\ &= \prod_{i=1}^m ((X^2 + \kappa)^2 + 1 - \theta^i). \end{aligned}$$

For $i = m$ we have the double roots $\pm\sqrt{\kappa}$. So $\kappa \neq 0$ (otherwise σ_2 would contain a 4-cycle), and there is one more factor $((X^2 + \kappa)^2 + 1 - \theta^i)$ for $i \neq m$ which is inseparable. This quickly gives $\kappa^2 + 1 = \theta^k$ for some k . With the same argument, we get $\bar{c}(X) = X^2 + \lambda$ with $\lambda^2 + 1 = \theta^l$ for some l . We will later see that k is prime to m , that is θ^k is a primitive m -th root of unity.

We must now determine the pairs (k, l) . For this we use the factorization of $f(X) - g(y)$ over $\mathbb{C}(y)$ into irreducible factors. As $g(y) = t$, these irreducible factors correspond to the orbits of V on G/U , and the degrees of these factors are the lengths of the orbits. Now it is easy to see that V has 4 orbits each of length 2, and the remaining orbits have length 4. (The orbits of length 2 are on the first and the last square.) By switching the role of U and V , we see that these 4 factors of degree 2 in X also have degree 2 in Y . For better reading we now write Y for y . We have

$$\begin{aligned} f(X) - g(Y) &= ((X^2 + \kappa)^2 + 1)^m - ((Y^2 + \lambda)^2 + 1)^m \\ &= \prod_{i=1}^m ((X^2 + \kappa)^2 + 1 - \theta^i((Y^2 + \lambda)^2 + 1))^m. \end{aligned}$$

Set

$$\begin{aligned} f_0(X) &= (X^2 + \kappa)^2 + 1, \\ g_0(Y) &= (Y^2 + \lambda)^2 + 1. \end{aligned}$$

So for some $i \neq m$, the factor

$$\Delta_i = f_0(X) - \theta^i g_0(Y)$$

is a product of two factors of degree 2 in X and Y , hence also of total degree 2.

Lemma 2.7. $k + l = 0$, and $i = k$.

Proof. Write $\Delta_i = A(X, Y)B(X, Y)$, where A and B have total degree 2. It is immediate that the polynomials A and B are coprime, so they have finitely many common zeroes. These common zeroes (ξ, ϵ) with $A(\xi, \epsilon) = B(\xi, \epsilon) = 0$ then are singularities of the curve given by $\Delta_i = 0$. So $f'(\xi) = g'(\epsilon) = 0$. One verifies immediately that the projective completion of Δ_i has no singularities which do not lie in the affine plane. Next we show that the intersections of the curves $A = 0$ and $B = 0$ are transversal, so by Bézout's Theorem we will get 4 intersection points. So let (ξ, ϵ) be such an intersection point. Write $f_0(X + \xi) - \theta^i g_0(Y + \epsilon) = h_0 + h_1 + \dots$, where h_w is homogeneous in X and Y of degree w . Of course the terms h_0 and h_1 vanish. We compute

$$h_2(X, Y) = (6\xi^2 + 2\kappa)X^2 - \theta^i(6\epsilon^2 + 2\lambda)Y^2.$$

So if the intersection at (ξ, ϵ) is not transversal, then h_2 is a square (or even trivial). However, if for instance $6\xi^2 + 2\kappa = 0$, then one computes that $f'_0(\xi) \neq 0$, and the analog holds for ϵ . So we get only transversal intersections, and by the previous argument there are four of them.

Now if $f'_0(\xi) = 0$, then $\xi \in \{0, \pm\sqrt{-\kappa}\}$, and $f'_0(\xi) \in \{\theta^k, 1, 1\}$ (in multiset notation). Analogously, if $g'_0(\epsilon) = 0$, then $\epsilon \in \{0, \pm\sqrt{-\lambda}\}$, and $g'_0(\epsilon) \in \{\theta^l, 1, 1\}$. Further using that $f'_0(\xi) - \theta^i g'_0(\epsilon) = 0$ for an intersection point (ξ, ϵ) , we see that there is no other choice than the one claimed in the Lemma. An actual factorization will be given later. □

We now show that k is prime to m . First note that if ϕ is an automorphism of the complex numbers, then we may replace f by f^ϕ and g by g^ϕ , and the resulting pair is still Kronecker conjugate. (Group theoretically, this amounts of replacing U and V by their images under some automorphism of G .) Suppose that k is not prime to m , and that under all m where this happens we have chosen m minimal. Let s

be the order of θ^k . Then s is a proper divisor of m . Now, by assuming a minimal counter-example and by what we know so far, the pair $f_s(X) = ((X^2 + \kappa)^2 + 1)^s$, $g_s(X) = ((X^2 + \lambda)^2 + 1)^s$ is properly Kronecker conjugate over \mathbb{C} . Let G_s be the stabilizer of $f_s(x)$ in G . Then $N < G_s < G$, and the pair U, V is already Kronecker conjugate in G_s , contrary to Lemma 2.2(iii).

Now we know what $f = f_0^m$ and $g = g_0^m$ look like. Replacing $f_0(X)$ and $g_0(X)$ by $\kappa^2 f_0(X/\sqrt{\kappa})$ and $\kappa^2 g_0(X/\sqrt{\kappa})$ preserves strong Kronecker conjugacy. Let ζ be a primitive $4m$ -th root of unity. We eventually get

$$\begin{aligned} f_0(X) &= (X^2 + (\zeta^4 - 1))^2 + \zeta^4 - 1, \\ g_0(X) &= (X^2 + \zeta^{m-2}(\zeta^4 - 1))^2 + \zeta^4 - 1. \end{aligned}$$

As a confirmation of the previous Lemma, we compute

$$\begin{aligned} f_0(X) - \zeta^4 g_0(Y) &= (X^2 + \frac{2\zeta}{1 + \zeta^m} XY + \zeta^{2-m} Y^2 + \zeta^4 - 1) \\ &\quad \cdot (X^2 - \frac{2\zeta}{1 + \zeta^m} XY + \zeta^{2-m} Y^2 + \zeta^4 - 1). \end{aligned}$$

Let K be a field which contains the $4m$ -th roots of unity, and let L be a normal closure of $K(x, y)$ over $K(t)$. Then it is easy to see (cf. [7, Section 2.2]) that K is algebraically closed in L , so the Galois group of $L|K(t)$ is the same as G which we got for $K = \mathbb{C}$.

It remains to show that the pair f, g is newly Kronecker conjugate. Suppose it is not; then $f(X) = h(d(X))$, $g(X) = h(\bar{d}(X))$ such that h has degree ≥ 2 , and d, \bar{d} are Kronecker conjugate. Using a theorem of Ritt about maximal decompositions of a polynomial (see [9] or [6]), the reader might quickly verify that $d(X) = e(b(c(X)))$, $\bar{d}(X) = e(\bar{b}(\bar{c}(X)))$ for some polynomial e . Let G_e be the stabilizer of $e(b(c(x)))$ in G . Then it follows that $N < G_e < G$, and that the pair U, V is Kronecker conjugate in G_e , contrary to Lemma 2.2(iii).

REFERENCES

- [1] M. FRIED, M. JARDEN. *Field Arithmetic*. Springer, Berlin Heidelberg, 1986. MR **89b**:12010
- [2] R. GURALNICK. *Zeros of permutation characters with applications to prime splitting and Brauer groups*. J. Algebra 131 (1990), 294–302. MR **91j**:20038
- [3] W. JEHNE. *Kronecker classes of algebraic number fields*. J. Number Theory 9 (1977), 279–320. MR **56**:5499
- [4] L. KRONECKER. *Über die Irreduzibilität von Gleichungen*. Werke II, 85–93; Monatsberichte Deutsche Akademie für Wissenschaft (1880), 155–163.
- [5] G. MALLE, B. H. MATZAT. *Inverse Galois Theory*. Book manuscript.
- [6] P. MÜLLER. *Primitive monodromy groups of polynomials*. Contemp. Math. 186 (1995), 385–401. CMP 96:01
- [7] P. MÜLLER. *Kronecker conjugacy of polynomials*. Preprint (1995).
- [8] C. PRAEGER. *Kronecker classes of field extensions of small degree*. J. Austr. Math. Soc. (Series A) 50 (1991), 297–315. MR **92m**:12004
- [9] J. F. RITT. *Prime and composite polynomials*. Trans. Amer. Math. Soc. 23 (1922), 51–66.
- [10] 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
- [11] H. VÖLKLEIN. *Groups as Galois Groups – an Introduction*. Cambridge University Press, 1996.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, GAINESVILLE, FLORIDA 32611
E-mail address: pfm@math.ufl.edu