J. KÖNIG
KODAI MATH. J.
41 (2018), 456–464

A NOTE ON FAMILIES OF MONOGENIC NUMBER FIELDS

Joachim König

Abstract

We give a sufficient criterion for specializations of certain families of polynomials to yield monogenic number fields. This generalizes constructions in several earlier papers. As applications we give new infinite families of monogenic number fields for several prescribed Galois groups.

1. Introduction

A number field $K|\mathbf{Q}$ is called monogenic if its ring of integers has a power basis, i.e. is of the form $\mathbf{Z} + \alpha\mathbf{Z} + \cdots + \alpha^n\mathbf{Z}$ for some $\alpha \in K$. An easy criterion for a field to be monogenic is the following: Let $f \in \mathbf{Z}[x]$ be monic irreducible, and $K = \mathbf{Q}[x]/(f)$. If the discriminant of f equals the field discriminant of K, then K is monogenic, and a power basis is obtained via powers of a root α of f. While quadratic fields are always monogenic, this is not the case any more for cubic fields.

It is unclear for which finite groups there are infinitely many monogenic number fields with Galois group (of the Galois closure) isomorphic to G. While there are infinitely many examples for the symmetric group S_n, it has been shown for cyclic groups G of prime order > 5 that there is at most one monogenic G-number field ([8]).

Several recent works have obtained infinite families of monogenic fields for prescribed Galois groups, including quintic D_5-fields ([10]), sextic A_4- ([5]) and $PSL_2(5)$-fields ([16]) and septimic $PSL_2(7)$-fields ([11]).

In this work, we prove a general criterion which not only subsumes most of the above existence results, but also makes verification of new results (under certain conditions) very easy and comfortable. We demonstrate this with several new infinite families of monogenic number fields.

2010 *Mathematics Subject Classification*. 11R32; 11R21; 11R04.

Key words and phrases. Monogenic number fields; Galois theory; specialization.
Received June 6, 2017; revised September 25, 2017.

2. Prerequisites

2.1. Some basics on number fields and function fields. We will later use the following well-known statement about exponents of ramified primes in discriminants, which holds in number fields as well as in function fields (cf. e.g. [9], p. 100 and Prop. 6.3.1).

Lemma 1. *Let $L|K$ be a finite separable extension of number fields or function fields, $M|K$ be its Galois closure, and $\Delta = \prod_{i=1}^{r} p_i^{e_i}$ the factorization of the discriminant of $L|K$ into prime ideals of K. If p_i is tamely ramified in $L|K$, then $e_i = ind(\sigma_i)$, where $\sigma_i \in Gal(M|K)$ is a generator of the inertia group at p_i, acting naturally on the cosets of $Gal(M|L)$, and the index $ind(x)$ of a permutation $x \in S_n$ is defined as n minus the number of cycles of x.*

Now, let K be a field of characteristic 0, $\overline{K}$ be its algebraic closure, t be a transcendental over K, and $N|K(t)$ be a Galois extension. A value $t_i \in \overline{K} \cup \infty$ is called a branch point of $N|K(t)$ if the ideal $(t - t_i)$ (or $(1/t)$ in the special case $t_i = \infty$) is ramified in $N\overline{K}|\overline{K}(t)$. Let $G := Gal(N\overline{K}|\overline{K}(t))$. Due to tame ramification, the inertia subgroup at a branch point t_i in $N|K(t)$ is cyclic, generated by some $\sigma_i \in G$.

We are particularly interested in the case that $N|K(t)$ is the Galois closure of an extension $K(y)|K(t)$ of rational function fields, i.e. the splitting field of some irreducible polynomial $f(t,x) := f_1(x) - tf_2(x)$. In this case, information about ramification is particularly easy to obtain.

In particular, the discriminant $\Delta(f) \in K[t]$ factors in $\overline{K}[t]$ as $C \cdot \prod_{i=1}^{r} (t - \alpha_i)^{e_i}$, where the α_i are exactly the finite branch points of $N|K(t)$ and $e_i = ind(\sigma_i)$, where σ_i is an inertia group generator at $t \mapsto \alpha_i$ in $N|K(t)$, in the permutation action on the roots of f.

This can be seen as a "polynomial version" of the Riemann-Hurwitz formula, and is essentially due to the fact that the extension $K(y)|K(t)$ is monogenic, in the sense that $\{y^i \mid i \in \{0, \dots, \deg(f) - 1\}\}$ is a power basis over $K[t]$.

2.2. Ramification in specializations. Let $E|k(t)$ be a Galois extension of function fields. For $t_0 \in k$, the specialization $E_{t_0}|k$ is defined as the residue field in E of any place extending the place $t \mapsto t_0$ of $k(t)$ (this is independent of the choice of place over $t \mapsto t_0$, since $E|k(t)$ is Galois). If $E|k(t)$ is the splitting field of a polynomial $f(t,x) \in k[t,x]$, then for all but finitely many $t_0 \in k$, this is simply the splitting field of $f(t_0, x)$.

Now let k be a number field, let a_0 be an algebraic number, $f \in k[X]$ be its minimal polynomial, and $\mathfrak{p}$ be a finite prime of k. Assume that a_0 is $\mathfrak{p}$-integral.[1] For $a \in k$, define $I_{\mathfrak{p}}(a, a_0)$ as the multiplicity of $\mathfrak{p}$ in the fractional ideal generated

[1] What follows is defined in the non-$\mathfrak{p}$-integral case as well. We keep the integrality assumption to avoid a distinction into cases which is not necessary for the purpose of this paper.

by $f(a)$. Obviously, we have $I_{\mathfrak{p}}(a, a_0) \neq 0$ only for finitely many prime ideals $\mathfrak{p}$ of k. With this notation, we can state an important criterion, relating ramification regular Galois extensions to ramification in specializations. It can be found in [1], Thm. 1.2 and Prop. 4.2; see also Theorem I.10.10 in [13] for a version close in wording to the one below.

Proposition 2. *Let k be a number field and $N|k(t)$ be a Galois extension with Galois group G. Then there is a finite set S of primes of k (depending on $N|k(t)$) such that for all primes $\mathfrak{p} \notin S$, the following holds:*

If $a \in k$ is not a branch point of $N|k(t)$ then the following condition is necessary for $\mathfrak{p}$ to be ramified in the specialization $N_a|k$:

$$e_i := I_{\mathfrak{p}}(a, a_i) > 0 \quad \textit{for some (automatically unique) branch point } a_i.$$

Furthermore, the inertia group of a prime extending $\mathfrak{p}$ in the specialization $N_a|k$ is then conjugate in G to $\langle \tau^{e_i} \rangle$, where τ is a generator of an inertia subgroup over the branch point $t \mapsto a_i$ of $k(t)$.

The finite set S of exceptional ("bad") primes in the above statement can also be described explicitly. For sake of simplicity, we do this under a few extra assumptions, all of which are fulfilled in our later examples.

Proposition 3. *Assume in Prop. 2 that $N|k(t)$ is k-regular, i.e. $N \cap \bar{k} = k$, and that $Z(G) = 1$. Then it suffices to take the set S of "bad" primes as the union of the following sets:*

i) *The set of primes dividing $|G|$,*
ii) *the set of primes $\mathfrak{p}$ at which two branch points t_1, t_2 of $N|k(t)$ meet (i.e. $I_{\mathfrak{p}}(t_1, t_2) > 0$),*
iii) *the set of primes dividing the discriminant of the minimal polynomial of some branch point.*

Proof. See Theorem 1.2 and Prop. 4.2 in [1]. □

3. A general criterion

Let $f(t, x) := f_1(x) - tf_2(x) \in \mathbf{Z}[t, x]$ be monic in x, with coprime $f_1, f_2 \in \mathbf{Z}[x]$. Let $\Delta(t) \in \mathbf{Z}[t]$ be the discriminant of f with respect to x. Write $\Delta(t) = \prod_{i=1}^{r} p_i(t)^{e_i}$ with pairwise distinct irreducible elements $p_i(t)$ in $\mathbf{Z}[t]$ (including constants $p_i(t) \equiv p_i \in \mathbf{P}$) and $e_i \in \mathbf{N}$. Then we denote by $\Delta^{red}(t) := \prod_{i=1}^{r} p_i(t)$ the reduced discriminant of f.

The following is a sufficient criterion for f to possess specializations yielding monogenic number fields. We use without further mention the well-known fact that if $p \in \mathbf{Z}[x]$ is monic irreducible with a root $\alpha \in \bar{\mathbf{Q}}$, such that the polynomial discriminant of p equals the field discriminant of $\mathbf{Q}(\alpha)$, then $\mathbf{Q}(\alpha)$ is monogenic, with $\{\alpha^i \mid i \in \{0, \ldots, \deg(p) - 1\}\}$ forming a power basis of the ring of integers.

Theorem 4. *Let $f(t,x) := f_1(x) - tf_2(x) \in \mathbf{Z}[t,x]$ be as above, with Galois group G over $\mathbf{Q}(t)$, and let $\Delta^{red}(t) \in \mathbf{Z}[t]$ be its reduced discriminant (with respect to x). Assume that the following hold:*

i) $\Delta^{red}(t)$ has no irreducible factor of degree ≥ 4.[2]

ii) $\Delta^{red}(t)$ has no fixed prime divisor, i.e. there exists no prime $p \in \mathbf{P}$ dividing all integer values of Δ^{red}.

Then there are infinitely many $t_0 \in \mathbf{Z}$ such that $\mathbf{Q}(\alpha)|\mathbf{Q}$ is a monogenic number field with Galois group G, where α denotes a root of $f(t_0,x) = 0$. More precisely, $\{\alpha^i \mid i \in \{0,\dots,\deg(f)-1\}\}$ is a power basis of the ring of integers of $\mathbf{Q}(\alpha)$.

Proof. Let $F|\mathbf{Q}(t)$ be a splitting field of f and let $S = \{p_1,\dots,p_n\}$ be the set of bad primes for $F|\mathbf{Q}(t)$, in the sense of Prop. 2. By condition ii), for each $i \in \{1,\dots,n\}$, there exists an integer t_i such that $\Delta^{red}(t_i) \neq 0 \bmod p_i$. By the Chinese remainder theorem, there then exists $a \in \mathbf{Z}$ such that $\Delta^{red}(a)$ is coprime to all of $p_1,\dots,p_n$ (for short, say that it is coprime to S). The same then of course holds for all $\Delta^{red}(a+t_0b)$ with $t_0 \in \mathbf{Z}$ and $b := p_1 \cdots p_n$.

Let $g(t) := \Delta^{red}(a+tb)$. Note that g cannot have a fixed prime divisor p. For $p \in \{p_1,\dots,p_n\}$, this is clear from the definition of g. For any other p, the set $a + b\mathbf{Z}$ of course intersects every mod-p residue class, and the assertion follows from condition ii).

Now for $N \in \mathbf{N}$, let $M(g,N) := \{t_0 \in \{1,\dots,N\} \mid g(t_0) \text{ is squarefree}\}$. Then by Theorem 1.1 in [2], there exists $k \in \mathbf{N}$ such that $|M(g,N)| \gg N/\log(N)^k$ (this generalizes a classical result by Erdös ([6]), proving infinity of squarefree values for cubic polynomials). We claim that all $t_0 \in M(g,N)$ lead to monogenic number fields $\mathbf{Q}(\alpha)|\mathbf{Q}$, where α denotes a root of $f(a+t_0b,x)$.

This is because for all those t_0, the polynomial discriminant $\Delta^{red}(a+t_0b)$ (and then a fortiori the field discriminant of $\mathbf{Q}(\alpha)|\mathbf{Q}$) is not divisible by any bad primes of $F|\mathbf{Q}(t)$. Now let $\Delta^{red}(t) = \pm\prod_{i=1}^m h_i(t)$ be the factorization into irreducibles over $\mathbf{Z}$ (note that the leading coefficient has to be ± 1 by ii)). Let p be a prime divisor of $\Delta^{red}(a+t_0b)$, then p divides a unique h_i, and exactly once. Therefore $I_p(a+t_0b,t_i) = 1$, where t_i is a root of h_i. Prop. 2 then implies that an inertia group generator at p in $Gal(f(a+t_0b,x)|\mathbf{Q})$ equals an inertia group generator σ_i at $t \mapsto t_i$ in $F|\mathbf{Q}(t)$. So the exponent of p in the field discriminant of $\mathbf{Q}(\alpha)|\mathbf{Q}$ equals $\deg_x(f)$ minus number of cycles of σ_i. From Section 2.1, this is however exactly the exponent of p in $\Delta(a+t_0b)$. So the two discriminants are equal. This shows the claim.

Lastly, $|M(g,N)| \gg N/\log(N)^k$, but by Hilbert's irreducibility theorem (see e.g. [3] for a very general version) the set of values $t_0 \in \{1,\dots,N\}$ such that $f(a+t_0b,x)$ is reducible has cardinality $\ll N^{1/2+\varepsilon}$. Therefore, infinitely many $t_0 \in \bigcup_{N\in\mathbf{N}} M(g,N)$ (and in fact almost all, in a density sense) also lead to extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ with Galois group G. The fact that this creates infinitely many distinct number fields follows immediately from the fact that the corresponding field discriminants are unbounded from above. □

[2] In other words, the splitting field of f over $\mathbf{Q}(t)$ has no branch point of degree ≥ 4 over $\mathbf{Q}$.

Remark 1. A few remarks on the conditions in Theorem 4:

- Condition i) can be dropped, conditional on the abc-conjecture. Namely, it was only used in the above proof to ensure the existence of sufficienty large sets of squarefree specializations. As shown by Granville ([7]), the abc-conjecture implies that for every integer polynomial $g(t) \in \mathbf{Z}[t]$ which does not have a fixed prime divisor, the set of $t_0 \in \mathbf{N}$ such that $g(t_0)$ is squarefree has positive density.
- Condition ii) is obviously somewhat restrictive, since Δ^{red} is in particular required to be a primitive polynomial (otherwise, every value would be divisible by the gcd of the coefficients).

  However, even in the case that Δ^{red} has a constant prime factor, the conclusions of the theorem may still be obtained in certain cases; see Section 4.3 for an example.
- The condition that f is of t-degree 1 is of course not strictly necessary either to obtain the conclusion. It is however the most convenient assumption to ensure that every root of the discriminant of f is in fact a branch point.

It should also be noted that the assertion of Theorem 4 can be combined with local conditions imposed on the monogenic number fields. In particular, the proof shows that the discriminants obtained can be chosen coprime to any given finite set of primes. Under modest extra assumptions, we can show more.

Corollary 5. *In the setting of Theorem* 4, *assume additionally that the splitting field L of f is a $\mathbf{Q}$-regular extension of $\mathbf{Q}(t)$ (i.e. $L \cap \bar{\mathbf{Q}} = \mathbf{Q}$). Let P be a finite set of sufficiently large prime numbers (with the bound only depending on f), and for each $p \in P$ let C_p be a conjugacy class of G. Then the monogenic number fields $\mathbf{Q}(\alpha)$ can additionally be required to fulfill the following*:

For each $p \in P$, the extension $\mathbf{Q}(\alpha)|\mathbf{Q}$ is unramified at p, with Frobenius class C_p.[3]

Proof. Let $p \in P$. By Prop. 5.1 in [4], we can assume (for p sufficiently large) the existence of a residue class $a_p + p\mathbf{Z}$ such that for all integers t_0 in this class, the splitting field of $f(t_0, x)$ has Frobenius C_p at p, and additionally $\Delta^{red}(t_0) \neq 0 \bmod p$. By the Chinese remainder theorem, there is then a residue class $c + N\mathbf{Z}$, with $N := \prod_{p \in S} p$, such that for all $t_0 \in a + N\mathbf{Z}$, the above requirements are fulfilled for all $p \in S$. Now simply repeat the proof of Theorem 4, replacing the residue class $a + b\mathbf{Z}$ occurring there by $(a + b\mathbf{Z}) \cap (c + N\mathbf{Z})$, which is non-empty under the assumption that no $p \in P$ is a bad prime. All one needs to note is that the polynomial $g(t)$ arising in the proof still has no fixed prime divisor, which is guaranteed by the above requirement $\Delta^{red}(t_0) \neq 0 \bmod p$ for $p \in P$. □

[3] Of course, by the Frobenius of a number field extension, we mean the Frobenius of its Galois closure.

4. New examples

In the following, we apply Theorem 4 to some families of polynomials $f(t,x)$ with prescribed Galois groups. In particular, we show:

THEOREM 6. *Let G be one of $PGL_2(7)$, $AGL_3(2)$ or $PSL_2(11)$. Then there are infinitely many monogenic number fields with Galois group* (*of the Galois closure*) *isomorphic to G.*

For those examples, we will also make the results of Theorem 4 more explicit. It should be understood that using Theorem 4, many more examples can be produced, using polynomials from the literature. Also, several existing results, such as those of [10], [11] or [16], can be regained as immediate corollaries of Theorem 4.

4.1. The group $AGL_3(2)$. Let $AGL_3(2) = (\mathbf{F}_2)^3 \rtimes GL_3(2)$ be the affine linear group, in its natural transitive degree-8 action.

The following example is a special case of a multi-parameter family computed by Malle in [12]. However, computation of the individual example below is standard nowadays, e.g. using Gröbner basis methods.

PROPOSITION 7. *Let $f(t,x) := x^6(x-2)^2 - t(5x^2+5x+2)(x-1)^2$. Then f has Galois group $AGL_3(2)$ over $\mathbf{Q}(t)$.*

One computes, e.g. with Magma, that the discriminant of f with respect to t equals $\Delta(t) = t^6(288000t^2 + 40747t + 221184)^2$. This has no fixed prime divisor, since e.g. $t(288000t^2 + 40747t + 221184)$, evaluated at -1, equals $-29^2 \cdot 557$, and evaluated at 1 equals $37 \cdot 89 \cdot 167$. The monogeneity result now follows readily from Theorem 4.

To be more explicit, note that bad primes for the splitting field of f over $\mathbf{Q}(t)$ are only 2, 3, 7 (prime divisors of the group order), 5 (modulo which the degree-3 branch points are not integral, hence they meet the branch point at infinity) and 29, 71 (modulo which $disc(t \cdot (288000t^2 + 40747t + 221184)) = 0$, hence two finite branch points meet).

Let $N := 2 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot 71$. Since $\Delta(1)$ is coprime to N, the same holds for all $\Delta(t_0)$ with $t_0 \equiv 1 \bmod N$. Furthermore $\Delta(Nt+1)$ is a primitive polynomial, so the proof of Theorem 4 shows that all $t_0 \equiv 1 \bmod N$ such that $Gal(f(t_0,x)|\mathbf{Q}) = AGL_3(2)$ and $\Delta^{red}(t_0)$ is squarefree yield monogenic octic $AGL_3(2)$-number fields.

Furthermore, $f(t_0,x)$ factors mod 2 into irreducible polynomials of degree 7 and 1, mod 3 into irreducible polynomials of degree 6 and 2, and mod 5 into two irreducible polynomials of degree 4. By Dedekind's reduction theorem, the Galois group of $f(t_0,x)$ over $\mathbf{Q}$ then contains elements of cycle structures (7.1), (6.2) and (4.4). One verifies that no proper subgroup of $AGL_3(2)$ has this property, hence the result follows for all $t_0 \equiv 1 \bmod N$ such that $\Delta^{red}(t_0)$ is squarefree.

4.2. The group $PSL_2(11)$. Let G be the projective special linear group $PSL_2(11)$, in its (exceptional) transitive permutation action on 11 points. We use the following family of polynomials, given e.g. in the appendix of [13].

Proposition 8. *The polynomial* $f(t,x) := x^{11} - 3x^{10} + 7x^9 - 25x^8 + 46x^7 - 36x^6 + 60x^4 - 121x^3 + 140x^2 - 95x + 27 + tx^2(x-1)^3 \in \mathbf{Z}[t,x]$ *has Galois group* $PSL_2(11)$ *over* $\mathbf{Q}(t)$.

One computes that the discriminant $\Delta(t) \in \mathbf{Z}[t]$ of $f \in \mathbf{Z}[t,x]$ (as a polynomial in x) equals $(108t^3 - 7472t^2 + 267408t + 7987117)^4$, which again can easily be seen to have no fixed prime divisor. Again, the monogeneity result follows directly from Theorem 4.

For more explicit results, note that the bad primes (in the sense of Prop. 2) are exactly 2, 3, 5, 11, 19 and 101, and $\Delta(1)$ is coprime to all of them. In fact Δ has no roots at all modulo 2, 3, 5 and 11, so here it suffices e.g. to set $N = 19 \cdot 101$ and $t_0 \equiv 1 \bmod N$.

The mod-19 reduction of $f(t_0, x)$ is irreducible, while the one mod 101 factors into irreducible polynomials of degree 6, 3 and 2. So $Gal(f(t_0,x)|\mathbf{Q})$ is a subgroup of $PSL_2(11)$ containing elements of order 11 and 6, and in particular is of order divisible by 66. However, the largest proper subgroup of $PSL_2(11)$ is of order 60. Therefore $Gal(f(t_0,x)|\mathbf{Q}) \cong PSL_2(11)$ for all $t_0 \equiv 1 \bmod 19 \cdot 101$. We therefore obtain monogenic number fields of degree 11 with group $PSL_2(11)$ for all $t_0 \equiv 1 \bmod 19 \cdot 101$ such that $\Delta^{red}(t_0)$ is squarefree.

Remark 2. So far we have used the elementary Dedekind criterion to ensure arithmetic progressions of specializations with the correct Galois group. Stronger results could be obtained using Siegel's finiteness theorem about integral points on curves. We only sketch this approach very briefly. See [15] for a much deeper introduction into the connection between Siegel's theorem and Hilbert's irreducibility theorem. Siegel's theorem ensures that a curve covering $X \to \mathbf{P}^1$ over $\mathbf{Q}$ (corresponding to a function field extension $K|\mathbf{Q}(t)$) with infinitely many integral points has to have genus zero and an inertia group generator with at most two orbits (and of equal length) at $t \mapsto \infty$. This translates to the assertion that a polynomial $f(t,x)$ with Galois group G over $\mathbf{Q}(t)$ can only have a strictly smaller Galois group $U < G$ for infinitely many specializations $t \mapsto t_0 \in \mathbf{Z}$ if G has a genus zero tuple including an element with at most two orbits in the coset action on G/U. Since $PSL_2(11)$ has no genus zero action fulfilling these requirements, we conclude that $f(t_0,x)$ remains irreducible for all but finitely many $t_0 \in \mathbf{Z}$ (this is a very special case of a general theorem by Müller ([14])). We then obtain the above result on monogenic $PSL_2(11)$-extensions for all but finitely many $t_0 \in \mathbf{Z}$ such that $\Delta^{red}(t_0)$ is squarefree and coprime to $19 \cdot 101$.

4.3. The group $PGL_2(7)$. Here we give an example that demonstrates how the restrictive condition ii) in Theorem 4 may be softened. Many more similar examples can be found. Again the polynomial below is a special case of a family computed in [12].

Proposition 9. *Let* $f(t,x) := x^7(x+1) + t(7x^2+x+1)$. *Then* f *has Galois group* $PGL_2(7)$ *over* $\mathbf{Q}(t)$.

The discriminant of f with respect to x equals $\Delta(t) = 7^7t^6(108t-1)^3$. This shows that the bad primes for the splitting field of f over $\mathbf{Q}(t)$ are only 2, 3 and 7. Ignoring the constant factor 7^7 of $\Delta(t)$, one verifies, just as in the proof of Theorem 4, that there are infinitely many $t_0 \in \mathbf{Z}$ such that the root field of $f(t_0,x)$ is a $PGL_2(7)$ number field whose discriminant differs from the discriminant of $f(t_0,x)$ at most by a 7-power $\leq 7^7$. Now let $t_0 := 1$. The discriminant of a root field of $f(1,x)$ equals $7^7 \cdot 107^3$. More precisely, this extension is totally tamely ramified at 7, which can be seen easily from the fact that $f(1,x-1)$ is a 7-Eisenstein polynomial. Now by Krasner's lemma, every $t_0 \in \mathbf{Z}$ which is 7-adically sufficiently close to 1 leads to the same behaviour at the prime 7 (in fact, $t_0 \equiv 1 \bmod 7$ is sufficient here due to Eisenstein, since $f(t,x-1)$ has constant coeficient $7t$). We therefore obtain a whole arithmetic progression of integers t_0 such that a root field of $f(t_0,x)$ has discriminant divisible by 7^7. But now it follows exactly as in the proof of Theorem 4 that infinitely many of those fields are monogenic $PGL_2(7)$-fields (by looking at suqarefree specializations of the reduced discriminant $t(108t-1)$).

Remark 3. As in Remark 2, Siegel's theorem may be used to ensure the full Galois group $PGL_2(7)$. Firstly, note that for $t_0 \equiv 1 \bmod 7$, the decomposition group of $f(t_0,x)$ at the prime 7 is of order 16 (and equals the normalizer of a cyclic subgroup of order 8 in $PGL_2(7)$). This is because this decomposition group has to contain a cyclic normal subgroup of order 8 (the inertia subgroup), but cannot equal this subgroup, as $\mathbf{Q}_7$ has no totally ramified C_8-extension. Therefore $Gal(f(t_0,x)|\mathbf{Q})$ contains a subgroup of order 16 and can then only equal either this subgroup (which is maximal in $PGL_2(7)$) or $PGL_2(7)$. By simple order arguments, no element of $PGL_2(7)$ has two or less cycles in the (degree-21) action on the cosets of the order-16 subgroup. Therefore, Siegel's theorem yields that for all but finitely many $t_0 \equiv 1 \bmod 7$, $f(t_0,x)$ has Galois group $PGL_2(7)$.

Acknowledgment. This work was partially supported by the Israel Science Foundation (grant no. 577/15).

References

[1] S. Beckmann, On extensions of number fields obtained by specializing branched coverings, J. reine angew. Math. **419** (1991), 27–53.

[2] A. R. Booker and T. D. Browning, Squarefree values of reducible polynomials, Preprint (2015), https://arxiv.org/abs/1511.00601.

[3] S. D. Cohen, The distribution of Galois groups and Hilbert's irreducibility theorem, Proc. London Math. Soc. **43** (1981), 227–250.

[4] P. Dèbes, On the Malle conjecture and the self-twisted cover, Isr. J. Math. **218** (2017), 101–131.

[5] D. Eloff, B. K. Spearman and K. S. Williams, A_4 sextic fields with a power basis, Missouri J. Math. Sci. **19** (2007), 188–194.

[6] P. Erdös, Arithmetical properties of polynomials, J. London Math. Soc. **28** (1953), 416–425.

[7] A. Granville, ABC allows us to count square-frees, Internat. Math. Res. Notices **19** (1998), 991–1009.

[8] M.-N. Gras, Non monogénéité de l'anneau des entiers des extensions cycliques de Q de degrée premier $l > 5$, J. Number Theory **23** (1986), 347–353.

[9] H. Koch, Number theory – Algebraic numbers and functions, AMS, Providence, Rhode Island, 2000.

[10] M. J. Lavallee, B. K. Spearman, K. S. Williams and Q. Yang, Dihedral quintic fields with a power basis, Math. J. Okayama Univ. **47** (2005), 75–79.

[11] M. J. Lavallee, B. K. Spearman and Q. Yang, $PSL(2,7)$ septimic fields with a power basis, Journal de Théorie des Nombres de Bordeaux **24** (2012), 369–375.

[12] G. Malle, Multi-parameter polynomials with given Galois group, J. Symb. Comput. **21** (2000), 1–15.

[13] G. Malle and B. H. Matzat, Inverse Galois theory, Springer monographs in mathematics, Berlin-Heidelberg, 1999.

[14] P. Müller, Hilbert's irreduciblity theorem for prime degree and general polynomials., Isr. J. Math. **109** (1999), 319–337.

[15] P. Müller, Finiteness Results for Hilbert's Irreducibility Theorem, Ann. Inst. Fourier **52** (2002), 983–1015.

[16] B. K. Spearman, A. Watanabe and K. S. Williams, $PSL(2,5)$ sextic fields with a power basis, Kodai Mathematical Journal **29** (2006), 5–12.

Joachim König
University of Würzburg
Emil-Fischer-Str.30
97074 Würzburg
Germany
E-mail: joachim.koenig@mathematik.uni-wuerzburg.de