Hilbert's Irreducibility Theorem for prime degree and general polynomials

Peter Müller *

May 26, 1998

Abstract

Let $f(X,t) \in \mathbb{Q}[X,t]$ be an irreducible polynomial. Hilbert's irreducibility theorem asserts that there are infinitely many $t_0 \in \mathbb{Z}$ such that $f(X,t_0)$ is still irreducible. We say that $f(X,t)$ is *general* if the Galois group of $f(X,t)$ over $\mathbb{Q}(t)$ is the symmetric group in its natural action. We show that if the degree of f with respect to X is a prime $\neq 5$ or if f is general of degree $\neq 5$, then $f(X,t_0)$ is irreducible for all but finitely many $t_0 \in \mathbb{Z}$ unless the curve given by $f(X,t)=0$ has infinitely many points (x_0,t_0) with $x_0 \in \mathbb{Q}$, $t_0 \in \mathbb{Z}$. The proof makes use of Siegel's theorem about integral points on algebraic curves, and classical results about finite groups, going back to Burnside, Schur, Wielandt, and others.

1 Introduction

If $f(X,t) \in \mathbb{Q}[X,t]$ is an irreducible polynomial, then there are various assertions about densities of the set $\mathcal{R}$ of integers t_0 such that $f(X,t_0)$ becomes reducible. For instance it is well known that $|\mathcal{R} \cap [-n,n]| = O(n^{1/2})$, and this is best possible in view of $f(X,t) = X^2 - t$. A recent trend is the explicit construction of universal Hilbert sets $\mathcal{H}$, so that for any f as above, $f(X,t_0)$ is reducible only for finitely many $t_0 \in \mathcal{H}$, see [Zan96], [DZ98], [Bil96].

Here we go a different direction. We show finiteness of $\mathcal{R}$ under rather general conditions.

*Supported by the DFG.

Recall that an irreducible polynomial $f(X,t) \in \mathbb{Q}[X,t]$ is called *general* if the Galois group of $f(X,t)$ over $\mathbb{Q}(t)$ is the symmetric group in its natural action on the roots of $f(X,t)$.

Theorem 1.1. *Let $f(X,t) \in \mathbb{Q}[X,t]$ be an irreducible polynomial. Suppose that $\deg_X f$ is a prime number, or f is general. Suppose there are infinitely many $t_0 \in \mathbb{Z}$, such that $f(X,t_0) \in \mathbb{Q}[X]$ is reducible without linear factor. Then $\deg_X f = 5$, f is general, and there are actually such examples of degree 5.*

As a consequence we will obtain

Theorem 1.2. *Let $f(X,t) \in \mathbb{Q}[X,t]$ be an irreducible polynomial which is general or has prime degree in X, such that the curve given by $f(X,t) = 0$ has positive genus. Then $f(X,t_0) \in \mathbb{Q}[X]$ is reducible for only finitely many $t_0 \in \mathbb{Z}$.*

The proof proceeds roughly as follows. We use a representation of $\mathcal{R}$ as a union of the value sets of finitely many rational functions $g(Z)$. This representation comes from the classical reduction argument in the proof of Hilbert's irreducibility theorem combined with Siegel's classification of curves with infinitely many rational points with bounded denominator. This approach has also been used for the construction of explicit universal Hilbert sets as mentioned above, and is due to M. Fried [Fri74], who investigated the special case $f(X,t) = h(X) - t$ for a functionally indecomposable polynomial h. The group which encodes the properties for proving the above theorems is the Galois group of $f(X,t)(g(X) - t)$ over the rational function field $\mathbb{Q}(t)$, regarded as a permutation group on the roots of $f(X,t)$ on the one hand, and on the roots of $g(X) - t$ on the other hand. The interplay between these two permutation representations is the main theme of the paper. Information about the first representation comes from the hypotheses of the theorems, whereas information about the second representation comes from using specific properties of g, and some arithmetic considerations coming from Puiseux expansions of the roots of $g(Z) - t$ at infinity.

Despite the group theoretic nature of our treatment we do not need the classification of the finite simple groups. We do however, especially in the prime degree case, use classical non–trivial results of Schur, Burnside, Wielandt and Neumann, which miraculously fit our needs.

In Section 9 we discuss various extensions and their limitations of the above theorems. For this work, which is in progress right now, we do however employ the classification theorem.

It is interesting that the prime degree 5 plays an exceptional role in Theorem 1.1. A recent preprint of Dèbes and Fried [DF99] analyzes this in the special case $f(X,t) = h(X) - t$ for a polynomial h.

Acknowledgment. I thank Moshe Jarden for carefully reading previous versions and his valuable comments.

2 A description of Hilbert sets

Let $f(X,t) \in \mathbb{Q}[X,t]$ be an irreducible polynomial. Let $\mathcal{R} \subseteq \mathbb{Z}$ be the set of those integers $t_0 \in \mathbb{Z}$, such that $f(X,t_0)$ is reducible over $\mathbb{Q}$. So $\mathbb{Z} \setminus \mathcal{R}$ is the (integral) Hilbert set of f. Using a well known reduction argument in the proof of Hilbert's irreducibility theorem (see e.g. [Lan83, Chapter 9]) and Siegel's classification of algebraic curves with infinitely many rational points with bounded denominator [Sie29], [Lan83, Chapter 8], one obtains (confer also [Fri74, Theorem 1], [Zan96, page 705]) the following

Proposition 2.1. *There exist finitely many non–constant functions $g_i(Z) \in \mathbb{Q}(Z)$ and a finite set W such that*

$$\mathcal{R} = W \cup \bigcup (g_i(\mathbb{Q}) \cap \mathbb{Z})$$

and $f(X, g_i(Z))$ is reducible over $\mathbb{Q}(Z)$.

The degree $\deg g$ of a rational function $g(Z) \in \mathbb{Q}(Z)$ is the maximum of the degrees of the numerator and denominator in reduced representation. Note that $\deg g$ equals the degree of the field extension $\mathbb{Q}(Z)|\mathbb{Q}(g(Z))$. In particular, the degree is an invariant under composing rational functions with linear fractional functions. Also, if $g(Z) = a(b(Z))$, with $a(Z), b(Z) \in \mathbb{Q}(Z)$, then $\deg g = \deg a \cdot \deg b$.

We use the usual conventions when regarding g as a map of the projective line $\mathbb{C} \cup \{\infty\}$ to itself.

The following is a tightening of the representation of $\mathcal{R}$ from above.

Proposition 2.2. *Choose the functions g_i in Proposition 2.1 with $\sum \deg g_i$ minimal. Then $|g_i(\mathbb{Q}) \cap \mathbb{Z}| = \infty$, and the following holds: If $g_i(Z) = a(b(Z))$*

with $a, b \in \mathbb{Q}(Z)$ *and* $\deg b > 1$*, then* $f(X, a(b(Z)))$ *is irreducible over* $\mathbb{Q}(b(Z))$*.*

Proof. Of course $|g_i(\mathbb{Q}) \cap \mathbb{Z}| = \infty$, for otherwise we could enlarge W. Suppose that $f(X, a(b(Z)))$ is reducible over $\mathbb{Q}(b(Z))$. Upon replacing $b(Z)$ by the variable Y, this means that $f(X, a(Y))$ is reducible over $\mathbb{Q}(Y)$. In particular, $f(X, u)$ is reducible for each $u \in a(\mathbb{Q}) \cap \mathbb{Z}$, so $a(\mathbb{Q}) \cap \mathbb{Z} \subseteq \mathcal{R}$. Clearly $g_i(\mathbb{Q}) \cap \mathbb{Z} \subseteq a(\mathbb{Q} \cup \{\infty\}) \cap \mathbb{Z} = (a(\mathbb{Q}) \cup \{a(\infty)\}) \cap \mathbb{Z}$. So we could replace g_i by a and enlarge W by $a(\infty)$ (if this element is an integer), contrary to our minimality assumption. □

3 Rational functions g with $|g(\mathbb{Q}) \cap \mathbb{Z}| = \infty$

Throughout this section let $g \in \mathbb{Q}(Z)$ be a rational function. Assuming infinitely many integral values on $\mathbb{Q}$ is quite a restrictive condition on g, by the following result of Siegel, see [Lan83, Chapter 8, §5], [Sie29].

Proposition 3.1. *Let* $g \in \mathbb{Q}(Z)$ *with* $|g(\mathbb{Q}) \cap \mathbb{Z}| = \infty$*. Then one of the following holds.*

(a) g *is a polynomial.*

(b) $g^{-1}(\infty)$ *consists of two real, algebraically conjugate elements.*

Let t be a transcendental over $\mathbb{Q}$. Write $g(Z) = r(Z)/s(Z)$ with relatively prime polynomials $r, s \in \mathbb{Q}[Z]$. The *monodromy group* G of g is the Galois group of $r(Z) - ts(Z)$ over $\mathbb{Q}(t)$. If n is the degree of g, then we consider G as a permutation group on the n roots of $r(Z) - ts(Z)$. Note that the monodromy group of g does not change if we compose g with linear fractional functions over $\mathbb{Q}$.

The next result is about decompositions of functions as in Proposition 3.1.

Lemma 3.2. *Let* $g(Z) = a(b(Z))$ *with* $a, b \in \mathbb{Q}(Z)$*. Suppose that* $|g^{-1}(\infty)| = 2$*. Then one of the following holds.*

(a) There is $\gamma \in \mathbb{Q} \cup \{\infty\}$ *with* $b^{-1}(\gamma) = g^{-1}(\infty)$*.*

(b) The monodromy group of $b(Z)$ *is solvable.*

Proof. We have

$$g^{-1}(\infty) = b^{-1}(a^{-1}(\infty)),$$

so $|a^{-1}(\infty)| = 1$ or 2. First suppose that $a^{-1}(\infty) = \{\gamma\}$. Clearly $\gamma \in \mathbb{Q} \cup \{\infty\}$, as every algebraic conjugate of γ is also mapped to ∞ under a. So (a) holds.

Now suppose that $a^{-1}(\infty) = \{\gamma_1, \gamma_2\}$ for $\gamma_i \in \overline{\mathbb{Q}} \cup \{\infty\}$ and $\gamma_1 \neq \gamma_2$. Then $b^{-1}(\gamma_1) = \{\delta_1\}$ and $b^{-1}(\gamma_2) = \{\delta_2\}$ for certain $\delta_i \in \overline{\mathbb{Q}} \cup \{\infty\}$. Set $\tilde{b}(Z) := \lambda(b(\mu(Z)))$ with suitable linear fractional functions $\lambda, \mu \in \overline{\mathbb{Q}}(Z)$, such that $\tilde{b}^{-1}(\infty) = \{\infty\}$ and $\tilde{b}^{-1}(0) = \{0\}$. Then $\tilde{b}(Z) = \kappa Z^r$, for some $\kappa \in \overline{\mathbb{Q}}$. So the Galois group C of $b(Z) - t$ over $\overline{\mathbb{Q}}(t)$, which is the same one as that of $\tilde{b}(Z) - t$, is cyclic of degree r. Hence $\mathrm{Aut}(C)$ is abelian. But the monodromy group G of $b(Z)$, which is the Galois group of $b(Z) - t$ over $\mathbb{Q}(t)$, normalizes C. (The quotient G/C is the Galois group over $\mathbb{Q}$ of the algebraic closure of $\mathbb{Q}$ in a splitting field of $b(Z) - t$ over $\mathbb{Q}(t)$.) As C is abelian and transitive, C equals its centralizer in G (e. g. [Hup67, II.3.1]), hence G/C embeds into the abelian group $\mathrm{Aut}(C)$, so G is solvable. □

We need more precise information about monodromy groups of functions as in Proposition 3.1. The following proposition is a well–known application of the branch cycle argument, see e. g. [Shi74, Section 3], [Fri94, §3], [Völ96, 2.8]), or [Fri95, page 330]. Note that C is the inertia group of some place of a splitting field of $g(Z) - t$ over the place $t \mapsto \infty$, and the generators of C are conjugate already inside the decomposition group associated to this place. A proof of this proposition can also easily be obtained using Puiseux series expansions of the roots of $g(Z) - t$ in $1/t^{1/n}$, where $n = \deg g$, as in the proof of Lemma 3.4.

Proposition 3.3. *Let $g(Z) \in \mathbb{Q}[Z]$ be a non–constant polynomial. Then the monodromy group G of g contains a cyclic transitive group C, such that the generators of C are conjugate in G.*

Lemma 3.4. *Let $m \in \mathbb{N}$, $\gamma \in \mathbb{Q} \cup \{\infty\}$, and $b(Z) \in \mathbb{Q}(Z)$, such that $b^{-1}(\gamma)$ consists of two algebraically conjugate elements, each assumed with multiplicity m. (So b has degree $2m$.) Let B be the monodromy group of b. Then the following holds*

(a) B contains an element σ, which is the product of two m–cycles.

(b) B contains an element which switches the two orbits of $<\sigma>$.

(c) *If $m = p$ is an odd prime, then B contains an element which has two fixed points and four cycles of length $(p-1)/2$.*

Proof. There is no loss in assuming $\gamma = \infty$, and that the sum (which is in $\mathbb{Q} \cup \{\infty\}$) of the two elements in $b^{-1}(\infty)$ vanishes. Then $b(Z) = h(Z)/(Z^2 - d)^m$ with a non–square $d \in \mathbb{Q}$, where $h(Z) \in \mathbb{Q}[Z]$ is a polynomial of degree at most $2m$ which is relatively prime to $Z^2 - d$.

Let y be a transcendental over $\mathbb{Q}$, and Ω be a splitting field of $b(Z) - y$ over $\mathbb{Q}(y)$. We use Puiseux series in order to embed Ω into a power series field and explicitly write down the elements of B whose existence we claim.

We seek to solve

$$h(Z) - y(Z^2 - d)^m = 0. \tag{1}$$

Set $y = 1/\tilde{y}^m$ and $Z = \sqrt{d} + \tilde{y}\tilde{Z}$. Then this equation becomes

$$h(\sqrt{d} + \tilde{y}\tilde{Z}) - \tilde{Z}^m(2\sqrt{d} + \tilde{y}\tilde{Z})^m = 0.$$

Hensel's Lemma gives a solution for $\tilde{Z}$ in the power series ring $\overline{\mathbb{Q}}[[\tilde{y}]]$. Substituting back, and doing the same for $-\sqrt{d}$ instead of $\sqrt{d}$, shows that

$$\varepsilon\sqrt{d} + a_{1,\varepsilon}\tilde{y} + a_{2,\varepsilon}\tilde{y}^2 + \cdots \in \overline{\mathbb{Q}}[[\tilde{y}]]$$

are solutions of (1), where $\varepsilon \in \{-1, 1\}$ and $a_{i,\varepsilon} \in \overline{\mathbb{Q}}$. Let ζ be a primitive m–th root of unity. Note that (1) remains unchanged when we replace $\tilde{y}$ by $\zeta^i\tilde{y}$. Hence all the solutions of $b(Z) - y = 0$ have the form

$$z_{i,\varepsilon} = \varepsilon\sqrt{d} + a_{1,\varepsilon}\zeta^i\tilde{y} + a_{2,\varepsilon}\zeta^{2i}\tilde{y}^2 + \cdots \in \overline{\mathbb{Q}}[[\tilde{y}]],$$

where $i \in \{0, 1, \ldots, m-1\}$. This embeds Ω into $\overline{\mathbb{Q}}((\tilde{y}))$, which is an infinite Galois extension of $\mathbb{Q}((1/y))$. The restriction of $\Gamma := \mathrm{Gal}(\overline{\mathbb{Q}}((\tilde{y}))|\mathbb{Q}((1/y)))$ to Ω induces a subgroup of B.

To (a). Let $\sigma \in \Gamma$ be trivial on $\overline{\mathbb{Q}}$, and map $\tilde{y}$ to $\zeta\tilde{y}$. Note that $a_{1,\varepsilon} \neq 0$ (substitute the Puiseux series into $\tilde{y}^m h(Z) = (Z^2 - d)^m$ and check the lower degree in $\tilde{y}$ of both sides), so we can see the effect of σ on the roots $z_{i,\varepsilon}$ by looking at the term $a_{1,\varepsilon}\zeta^i\tilde{y}$. The restriction of σ to Ω induces the requested action on the $z_{i,\varepsilon}$.

To (b). Choose $\beta \in \Gamma$, such that $(\tilde{y})^\beta = \tilde{y}$, and $(\sqrt{d})^\beta = -\sqrt{d}$. Then β interchanges the set of the $z_{i,-1}$ with the set of the $z_{i,1}$.

To (c). Let H be the subgroup of index 2 of $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. If $\sqrt{d} \in \mathbb{Q}(\zeta)$, then H fixes $\sqrt{d}$. If however $\sqrt{d} \notin \mathbb{Q}(\zeta)$, then we can extend H to $\overline{\mathbb{Q}}$, such

that $\sqrt{d}$ is fixed. At any rate, we can extend H to $\overline{\mathbb{Q}}$ fixing $\sqrt{d}$. Let α be a generator of the cyclic group H of order $(p-1)/2$. Extend α to an element in Γ by requiring that α fixes $\tilde{y}$. Let $\zeta^\alpha = \zeta^w$ for an integer w. We must have $a_{1,\varepsilon}^\alpha = a_{1,\varepsilon}\zeta^{e_\varepsilon}$ for some integer e_ε. Taking indices modulo p, we set $v_{i,\varepsilon} := z_{i+e_\varepsilon/(1-w),\varepsilon}$. From

$$(a_{1,\varepsilon}\zeta^{i+e_\varepsilon/(1-w)})^\alpha = a_{1,\varepsilon}\zeta^{iw+e_\varepsilon/(1-w)}$$

we obtain

$$v_{i,\varepsilon}^\alpha = v_{iw,\varepsilon},$$

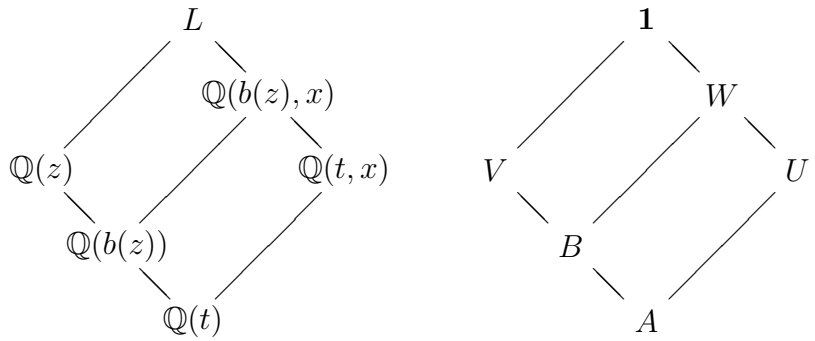
hence the element α of order $(p-1)/2$ permutes the p–th roots of unity in the same way as the roots $v_{i,\varepsilon}$ for fixed ε. Therefore α has two fixed points, and the remaining elements are permuted in cycles of length $(p-1)/2$. The claim follows. □

4 Galoistheoretic consequences from Proposition 2.2

Let $f(X,t) \in \mathbb{Q}[X,t]$ be irreducible, and $g(Z)$ be one of the rational functions g_i of Proposition 2.2. Write $g = r/s$ with relatively prime polynomials $r, s \in \mathbb{Q}[Z]$. Let t be a transcendental over $\mathbb{Q}$. Let x be a root of $f(X,t)$, and z be a root of $r(Z) - ts(Z)$, where x and z are chosen in some algebraic closure of $\mathbb{Q}(t)$. Denote by L the Galois closure of $\mathbb{Q}(x,z)|\mathbb{Q}(t)$, and let $A := \mathrm{Gal}(L|\mathbb{Q}(t))$ be the Galois group of this extension. Set $U := \mathrm{Gal}(L|\mathbb{Q}(t,x))$ and $V := \mathrm{Gal}(L|\mathbb{Q}(z))$. As $f(X,t)$ and $r(Z) - ts(Z)$ are irreducible over $\mathbb{Q}(t)$, the permutation action of A on the roots of $f(X,t)$ (or the roots of $r(Z) - ts(Z)$) is equivalent to the action on the coset spaces A/U (or A/V).

We fix some more notation. Let B be any subgroup of A which properly contains V (possibly $B = A$). From Lüroth's theorem we obtain a decomposition $g(Z) = a(b(Z))$, where $B = \mathrm{Gal}(L|\mathbb{Q}(b(z)))$. Set $W := B \cap U = \mathrm{Gal}(L|\mathbb{Q}(b(z),x))$.

The following diagram illustrates the fields and their associated fix groups.



If H, I are subgroups of A, then set $HI := \{hi |\ h \in H, i \in I\}$. (In general, HI is not a group, but it is if H or I is normal in A.)

Lemma 4.1. *With the notation from above, assume that U is a maximal subgroup of A. Then the following holds.*

(a) V is intransitive on the coset spaces A/U and B/W, whereas B is transitive on A/U.

(b) A acts faithfully on the coset spaces A/U and A/V.

(c) If W is a maximal subgroup of B, then B acts faithfully on the coset spaces B/W and B/V.

Proof. To (a). $f(X,t)$ is reducible over $\mathbb{Q}(z)$ by Proposition 2.1. This means that V, the stabilizer of z in A, acts intransitively on the conjugates of x. This action is equivalent to the action on the coset space A/U. Similarly, by Proposition 2.2, $f(X, b(z))$ is irreducible over $\mathbb{Q}(b(z))$, so B acts transitively on the conjugates of x. Now suppose that V is transitive on B/W. This implies $WV = B$. Transitivity of B on A/U means $UB = A$. These two equations together give $UV = UWV = UB = A$, so V is transitive on A/U, a contradiction.

To (b). Let N_U and N_V be the kernels of the actions of A on A/U and A/V, respectively. So N_U is the maximal normal subgroup of A which is contained in U, and likewise for V. From (a) we get

$$(UN_V)(VN_U) = UVN_U = N_UUV = UV \subsetneqq A.$$

Note that $N_U \cap N_V = \mathbf{1}$, as L is the compositum of the fixed fields of N_U and N_V. Now $N_V \leq U$, as U is maximal in A by assumption. So $N_V \leq N_U$,

hence $N_V = \mathbf{1}$. Also, $N_U \leq V$, for otherwise $B := N_U V > V$, hence $UB = A$ by (a). But then $UV = UN_U V = UB = A$, contrary to (a). So $N_U = \mathbf{1}$, and the claim follows.

To (c). Suppose that $b \in B$ lies in the kernel of the action of B on B/W. Then b is contained in the B–conjugates of W, so b is contained in the B conjugates of $U \geq W$ as well. By (a), $UB = A$, so the set of the B–conjugates of U is the same as the set of the A–conjugates of U. But the A–conjugates of U intersect trivially by (b), so $b = 1$. Now let N be the kernel of the action of B on B/V. By (a), we know $(NW)V \subsetneqq B$, so $NW = W$ by maximality of W in B, hence $N \leq W$ and therefore $N = \mathbf{1}$ by the first part. □

5 Some group theoretic results

The following proposition is due to Burnside [HB82, XII.10.8] for n a prime. The more difficult case where n is not a prime is due to Schur [Wie64, 25.3], see also [DM96, 3.5]. Note that primitivity and the existence of the transitive cyclic subgroup is automatically guaranteed in the prime degree case.

Proposition 5.1. *Let G be a primitive permutation group of degree n which contains a cyclic transitive subgroup C. Then either G is doubly transitive, or n is prime and G is solvable.*

P. M. Neumann [Neu72, page 203] (see also [HB82, XII.10.10]) has given an elegant proof using simple facts about symmetric block designs for the following theorem of Wielandt.

Proposition 5.2. *Let G be a permutation group of prime degree p. Suppose that the normalizer of a Sylow p–subgroup has even order. Then G contains only one conjugacy class of subgroups of index p.*

The primitive groups of degree $2p$ (p a prime) are known by the classification of the finite simple groups. The following result of Wielandt [Wie64, 31.1, 31.2] is a tight statement about such groups which can be obtained without the classification (the main tools being character theory and Proposition 5.1).

Proposition 5.3. *Let p be a prime, and G be a primitive permutation group of degree $2p$. Then either G is doubly transitive, or the following holds: A pointstabilizer of G has three orbits of lengths 1, $u(2u+1)$ and $(u+1)(2u+1)$ for some $u \in \mathbb{N}$.*

We also need the following easy

Lemma 5.4. *Let G be a finite group with subgroups H_1 and H_2, such that $H_1H_2 \subsetneqq G$, and the actions of G on the coset spaces G/H_1 and G/H_2 are doubly transitive. Then $|H_1| = |H_2|$.*

Proof. If G acts on a set Ω, let $\chi(g)$ be the number of fixed points of $g \in G$. It is well known (see [Gor68, 2.7.4(i)]) that $\sum_{g\in G} \chi(g) = r|G|$, where r is the number of orbits of G. Apply this to the action on $\Omega \times \Omega$ to see that G is doubly transitive on Ω (which is equivalent to G having exactly two orbits on $\Omega \times \Omega$, namely the set of all (α, β) with $\alpha \neq \beta$, and the set of all (α, α)) if and only if $\sum_{g\in G} \chi(g)^2 = 2|G|$. Now let χ_1, χ_2 and χ correspond to the actions of G on G/H_1, G/H_2 and $G/H_1 \times G/H_2$, respectively. For $y \in G \setminus H_1H_2$ the pairs (H_1, H_2) and (H_1y, H_2) lie in distinct G–orbits. Thus G has at least two orbits on $G/H_1 \times G/H_2$. Taking these things together gives $\sum_{g\in G} \chi_i(g)^2 = 2|G|$ for $i = 1, 2$, and $\sum_{g\in G} \chi_1(g)\chi_2(g) \geq 2|G|$. As equality holds in the Cauchy–Schwarz inequality

$$4|G|^2 \leq (\sum_{g\in G} \chi_1(g)\chi_2(g))^2 \leq \sum_{g\in G} \chi_1(g)^2 \sum_{g\in G} \chi_2(g)^2 = 4|G|^2,$$

there is a constant s such that $\chi_1(g) = s\chi_2(g)$ for all $g \in G$. But

$$\sum_{g\in G} \chi_1(g) = \sum_{g\in G} \chi_2(g) = |G|,$$

so $s = 1$. In particular $[G : H_1] = \chi_1(1) = \chi_2(1) = [G : H_2]$. Conclude that $|H_1| = |H_2|$. □

Lemma 5.5. *Let G be a transitive, solvable permutation group of prime degree p. Then G is permutation equivalent to a subgroup of the affine group $\mathrm{AGL}_1(p)$, which is defined by the permutations $x \mapsto ax + b$ of the elements of the finite field $\mathbb{F}_p$, with $a, b \in \mathbb{F}_p$, $a \neq 0$.*

Furthermore, if $U < G$ is intransitive, then U fixes a point.

Proof. For the first part (an easy theorem of Galois), see [Hup67, II.3.6]. As to the second part, let $u_i = (x \mapsto a_ix + b_i)$, $i = 1, 2$, be two nontrivial elements of U. Then $a_i \neq 1$ by intransitivity of U. (Otherwise u_i would generate a p–cycle.) Write the action of $\mathrm{AGL}_1(p)$ on $\mathbb{F}_p$ from the right. Then the commutator $u_1^{-1}u_2^{-1}u_1u_2$ is $x \mapsto x + (a_2 - 1)b_1 - (a_1 - 1)b_2$. We get $(a_2 - 1)b_1 - (a_1 - 1)b_2 = 0$ by intransitivity of U. So u_1 and u_2 have the common unique fixed point $b_i/(1 - a_i)$. The claim follows. □

Lemma 5.6. *Let B be the alternating group on 5 letters $M = \{1, 2, 3, 4, 5\}$, V be a subgroup of index 10, and $\sigma \in B$ be an element of order 5. Then σ has two 5–cycles on B/V, and B does not contain an element which switches the two orbits of $<\sigma>$ on B/V.*

Proof. V has order 6, so by divisibility reasons V has two orbits on M, one of length 2, the other one of length 3. If V, say, leaves $\{1, 2\}$ invariant, then, since the stabilizer in B of $\{1, 2\}$ has a faithful representation on $\{3, 4, 5\}$, it must coincide with V. Thus the action of B on B/V is equivalent to the action of B on the set M_2 of subsets of M of size 2. (Note that B is transitive on M_2.) Let $\tau \in B$ be an element which switches the two orbits of $<\sigma>$ on M_2. So τ has even order, hence $|\tau| = 2$ (because even order elements in B are necessarily involutions) and τ is a double transposition on M. In particular, τ has two fixed points on M_2, so τ cannot switch the two orbits of $<\sigma>$ on M_2, a contradiction. □

Lemma 5.7. *Let $2 \leq k \leq n-2$ be integers, and denote by M_k the collection of all subsets of $M = \{1, 2, \ldots, n\}$ of size k. Let σ be an element of the symmetric group on M. Then σ has at least two cycles on M_k, and if it has exactly two cycles, then either $n = 4$, $|\sigma| = 3$ or 4, or $n = 5$, $|\sigma| = 5$.*

Proof. First consider the case that σ is an n–cycle on M. Then $<\sigma>$ cannot be transitive on M_k, for then $n = |\sigma| = |M_k| = \binom{n}{k} \geq \binom{n}{2}$, so $n \leq 3$, but $n \geq 4$ by assumption. Now suppose that σ has exactly two orbits on M_k. Then one of the orbits has length at least $\binom{n}{k}/2$, so $n \geq \binom{n}{k}/2 \geq n(n-1)/4$, thus $n \leq 5$. These cases really occur.

Next suppose that σ is an $(n-1)$–cycle on M. As above, we now get $n = 4$. This case occurs too.

Now suppose that σ is neither an n–cycle nor an $(n-1)$–cycle on M. Then σ leaves on M a set S with $2 \leq |S| \leq n/2$ invariant. Without loss $k \leq n/2$ (as the action on M_k is the same as the action on M_{n-k}). For $i = 0, 1, 2$ choose sets S_i of size k, such that i points of S_i are in S, and the remaining $k - i$ points are in the complement of S. Then these three sets of course are not conjugate under $<\sigma>$. □

Lemma 5.8. *Let the symmetric group S_4 act on the set of subsets of size 2 of $\{1, 2, 3, 4\}$. Let σ be an element of order 3. Then no element of S_4 switches the two orbits of $<\sigma>$.*

Proof. Without loss assume σ is the permutation (1 2 3) on $\{1,2,3,4\}$. Then σ permutes cyclically the sets $\{1,4\}$, $\{2,4\}$, and $\{3,4\}$. Suppose that an element in S_4 switches these three sets with $\{1,2\}$, $\{2,3\}$, and $\{1,3\}$. Thus each of the latter three sets contains a number which is mapped to 4. This of course is nonsense. □

6 The prime degree case

We continue to use the setup from Section 4, but additionally assume throughout this section that $\deg_X f = p$, with p a prime number. Also, we assume that B is chosen such that V is a maximal subgroup of B. Recall that the possibility $B = A$ is not excluded. From Lemma 4.1(a) we obtain

$$[B : W] = [A : U] = \deg_X f = p.$$

In particular, W is a maximal subgroup of B, so 4.1(c) implies that B acts faithfully and of course transitively on the coset spaces B/V and B/W. The aim of this section is

Lemma 6.1. *With the assumptions from above, V and W are conjugate in B, or $p = 5$ and the action of A on A/U is the natural action of the symmetric group on 5 letters.*

For the sake of easier reading, we assume that V and W are not conjugate in B, and derive in a series of claims $p = 5$ and the identification of A.

Claim 6.2. *B is doubly transitive on B/W and not solvable.*

Proof. Suppose that B is solvable. Then the action of B on B/W is given as a transitive subgroup of the affine group $\mathrm{AGL}_1(p)$, see Lemma 5.5. But V is intransitive in this action by Lemma 4.1(a). Hence, by Lemma 5.5, V fixes a point in this representation. So V is contained in a B–conjugate of W. But V is maximal in B by assumption, so V and W are conjugate in B, contrary to the general hypothesis. This contradiction shows that B is not solvable. The first part of the claim then follows from the second one and Proposition 5.1. (Note that $p = [B : W]$ implies that B is primitive on B/W, and that the existence of a transitive cyclic subgroup follows from Sylow's theorem, just take the group generated by an element of order p.) □

Claim 6.3. *There is $\gamma \in \mathbb{Q} \cup \{\infty\}$ with $|b^{-1}(\gamma)| = 2$.*

Proof. We have $|g(\mathbb{Q}) \cap \mathbb{Z}| = \infty$, hence either g is a polynomial, or $|g^{-1}(\infty)| = 2$, by Proposition 3.1.

Assume first that g is a polynomial. Hence $g^{-1}(\infty) = \{\infty\}$. So $a^{-1}(\infty)$ consists of only one element. Use a linear fractional transformation to move this element to ∞. Thus we can assume without loss that $b^{-1}(\infty) = \{\infty\}$, so b is also a polynomial with coefficients in $\mathbb{Q}$. By faithful action, the monodromy group of b is B in the action on B/V. Use Propositions 3.3 and 5.1 and the non–solvability of B (Claim 6.2) to conclude that B is doubly transitive on B/V. Since B is doubly transitive on B/W (Claim 6.2), Lemma 5.4 implies that $[B : V] = [B : W] = p$. Let C be the cyclic transitive (on B/V) subgroup of B from Proposition 3.3. This proposition says that the generators of C are conjugate in B. In particular, a generator c of C is conjugate to its inverse, say $c^b = c^{-1}$ for some $b \in B$. So the order of b modulo the centralizer of C in B is 2, in particular b has even order. But C is a Sylow p–subgroup of B (as $p \mid |C|$, but $p^2 \not| |B| \mid p!$), with a normalizer of even order. Apply Proposition 5.2 to get the contradiction that W and V are conjugate in B.

Thus we have $|g^{-1}(\infty)| = 2$. As remarked above, B is the monodromy group of b. But B is not solvable by Claim 6.2, so Proposition 3.2(a) holds. Conclude that $|b^{-1}(\infty)| = 2$. □

We have seen that the rational function b fulfills the hypotheses of Lemma 3.4. Accordingly, let $2m = [B : V] = \deg b$ be the degree of b. Recall that B can be identified with the monodromy group of b (by faithful action of B on B/V, see Lemma 4.1(c)). Let $\sigma \in B$ be the element from Lemma 3.4(a), which acts as a product of two m–cycles on B/V.

Claim 6.4. *$m = p$ and B contains a subgroup H which has two fixed points and four orbits of lengths $(p-1)/2$ on B/V. (Note that $p > 2$ by Claim 6.2.)*

Proof. Recall that B acts faithfully on the coset spaces B/V and B/W by Lemma 4.1(c), and that $[B : W] = p$. So p divides $|B|$. On the other hand, p does not divide $|V|$, for otherwise V would contain an element of order p. But such an element acts as a p–cycle on B/W, in particular V were transitive on B/W, contrary to Lemma 4.1(a). Hence p divides $[B : V] = 2m$, so $p|m$ as p is odd. Thus a suitable power σ^c has order p. So σ^c is a p–cycle on B/W, but then σ has to be a p–cycle on B/W too. Since the action of σ on B/W is faithful, $|\sigma| = p$. Since σ acts on B/V as a product of two m–cycles and since this action is faithful too, $|\sigma| = m$. Conclude that $m = p$.

The existence of H follows from Lemma 3.4(c). $\square$

We are now ready to prove Lemma 6.1. By the previous claim, the action of B on B/V has degree $2p$. This action is primitive, as V is a maximal subgroup of B (see the beginning of this section). So we can apply Proposition 5.3. As $VW < B$ and the action of B on B/W is doubly transitive (by Claim 6.2), Proposition 5.4 implies that the action of B on B/V is not doubly transitive (for then $p = [B : W] = [B : V] = 2p$), so the alternative holds, that is a point stabilizer of B has orbit lengths 1, $u(2u+1)$, and $(u+1)(2u+1)$ for $u \in \mathbb{N}$. Each of these orbits is a disjoint union of orbits of the group H from the previous claim, whose lengths are 1 (2 times) and $(p-1)/2$ (4 times). Thus there are integers $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 4$ such that

$$\alpha + \beta\frac{p-1}{2} = u(2u+1)$$
$$1 - \alpha + (4-\beta)\frac{p-1}{2} = (u+1)(2u+1).$$

Eliminate $(p-1)/2$ to obtain $4\alpha - \beta = (2u+1)(4u - 2\beta u - \beta)$, so $2u+1$ divides $4\alpha - \beta$. Since $|4\alpha - \beta| \leq 4$, we get $u = 1$ and $\alpha + 2\beta = 3$. Conclude that $\alpha = \beta = 1$ and therefore $p = 5$.

The only non–solvable transitive groups of degree 5 are the alternating and symmetric group. The former case cannot hold, because the alternating group A_5, in its representation on 10 points, does not contain an element which switches the two 5–cycles of σ (see Lemma 5.6), contrary to Lemma 3.4(b).

7 The general case

Now suppose that $\deg_X f = n$, and that the Galois group of $f(X,t)$ over $\mathbb{Q}(t)$ is the symmetric group S_n in the natural action. Again we use the setup from Section 4. By Lemma 4.1(b), A acts faithfully as the symmetric group on A/U. The following lemma describes the faithful action of A on A/V.

Lemma 7.1. *There is an integer $1 \leq k \leq n-1$, such that the action of A on A/V is equivalent to the natural action of the symmetric group S_n on M_k, where M_k denotes the set of subsets of $M = \{1, 2, \ldots, n\}$ of size k.*

Proof. Identify A with S_n, and A/U with M. Then V is a subgroup of S_n, which by Lemma 4.1(a) is intransitive on M. Without loss, suppose that $\{1, 2, 3, \ldots, k\}$ is an orbit of V on M. Let $B \geq V$ be the full setwise stabilizer of this orbit in S_n. As the group B is still intransitive on M, it cannot properly contain V by Lemma 4.1(a). Therefore $V = B$, and as A is transitive on M_k, the action of A on A/V is equivalent to the action on M_k. □

Lemma 7.2. *If $n \neq 5$, then the groups U and V are conjugate in A.*

Proof. Suppose that U and V are not conjugate in A. Then $2 \leq k \leq n-2$ with k from the previous lemma. The rational function g fulfills $|g(\mathbb{Q}) \cap \mathbb{Z}| = \infty$, hence either g is a polynomial, or $|g^{-1}(\infty)| = 2$, by Proposition 3.1. So Proposition 3.3 or Lemma 3.4(a) gives an element $\sigma \in A$, such that σ has at most two cycles on A/V. Use Lemma 5.7 to conclude $n = 4$ or 5.

So we have to look at $n = 4$. Note that $k = 2$. As the symmetric group on 4 letters does not contain an element of order $6 = [A : V]$, we get from Proposition 3.3 that g is not a polynomial. Now Proposition 3.1 together with Lemma 3.4(a) allows us to assume that the σ from above has two cycles on A/V of equal length, hence $|\sigma| = 3$. Now use Lemma 5.8 to see that the two orbits of σ on A/V cannot be switched by an element in A, contrary to Lemma 3.4(b). □

8 Proof of Theorems 1.1 and 1.2

Assume in addition to the assumptions of Theorem 1.1 that $\deg_X f \neq 5$, or $\deg_X f = 5$ but f is not general. Let g be one of the functions g_i that occur in Proposition 2.2.

Lemma 6.1 and Lemma 7.2 prove in the setup of Section 4 that V is conjugate in A to a subgroup of U. Hence, V, which is the stabilizer in A of z, fixes one of the conjugates of x. This implies that $f(X, g(Z))$ has a factor of degree 1 in X over $\mathbb{Q}(Z)$. Since this holds for each i, the tightened presentation of $\mathcal{R}$ implies that for almost all $t_0 \in \mathbb{Q}$, $f(X, t_0)$ has a linear factor in $\mathbb{Q}[X]$. This contradicts the assumption of Theorem 1.1. Conclude from this contradiction that $\deg_X f = 5$ and f is general, as claimed.

As to the degree 5 case, the work of Dèbes and Fried [DF99] contains a thorough study of counterexamples, where f can be even chosen as simple as $f(X, t) = h(X) - t$, where $h \in \mathbb{Q}[X]$.

We now prove Theorem 1.2. If the curve $f(X,t)=0$ has infinitely many rational points (x_0,t_0) with $t_0 \in \mathbb{Z}$, then this curve has genus zero by Siegel, see [Lan83, Chapter 8], [Sie29]. So in order to prove Theorem 1.2, we only need to show that in an exceptional situation coming up in the proof of Theorem 1.1 for $p=5$, the genus of $f(X,t)=0$ is zero. So suppose that $A=S_5$ and $U=S_4$. Then the action of A on A/V is the action on the 2–sets, see Lemma 7.1. (Note that if $k=1$ in this Lemma, then U and V are conjugate, hence in particular the genera of the fixed fields of U and V are the same. But the genus of the fixed field $\mathbb{Q}(z)$ of V is zero.) For $\sigma \in A=S_5$, let $\mathrm{ind}_U(\sigma)$ (or $\mathrm{ind}_V(\sigma)$) be $5=[A:U]$ (or $10=[A:V]$) minus the number of orbits of $<\sigma>$ on A/U (or A/V). Let $\sigma_1,\sigma_2,\ldots,\sigma_r$ be a branch cycle description (see e.g. [Fri94] or [Mül96, Section 2] for definitions and results) of the extension $\mathbb{C}L|\mathbb{C}(t)$. The Riemann–Hurwitz genus formula gives $\sum \mathrm{ind}_V(\sigma_i)=2\cdot([A:V]-1)=18$, because the fixed field of V, which is $\mathbb{C}(z)$, has genus zero. The following table, which can easily be computed by hand, gives the index function for representatives σ of the conjugacy classes of S_5.

σ	**1**	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3)(4 5)	(1 2 3 4)	(1 2 3 4 5)
$\mathrm{ind}_U(\sigma)$	0	1	2	2	3	3	4
$\mathrm{ind}_V(\sigma)$	0	3	4	6	7	7	8

We notice that $\mathrm{ind}_U(\sigma) \leq \mathrm{ind}_V(\sigma)/2$ for all $\sigma \in S_5$. Let e be the genus of the fixed field of U. The genus formula then gives

$$(5-1+e)=\sum \mathrm{ind}_U(\sigma_i) \leq \frac{1}{2}\sum \mathrm{ind}_V(\sigma_i)=9,$$

hence $e=0$, which is the genus of the curve $f(X,t)=0$, and the claim follows.

9 Further directions

Theorems 1.1 and 1.2 still hold when we replace $\mathbb{Z}$ by a finitely generated $\mathbb{Z}$–algebra in $\mathbb{Q}$. The only essential change is that we need to replace the classical Siegel theorem by the more general theorem of Siegel–Mahler–Lang, which handles algebraic curves with infinitely many point with coordinates in such a $\mathbb{Z}$–algebra, see [Lan83, Chapter 8].

There are three obvious ways to lessen the assumptions in the Theorems 1.1 and 1.2. Namely

(a) Weakening the assumptions on the Galois group of $f(X,t)$ over $\mathbb{Q}(t)$.

(b) Replacing $\mathbb{Q}$ by a number field.

(c) Instead of specializing in $\mathbb{Z}$, consider specialization in $\mathbb{Q}$.

Of course, each of the points (a), (b), and (c) can be combined, yielding configurations of increasing difficulty to analyze. We shortly comment on these points.

To (a). Most of the group theoretic setup and immediate consequences still hold if we only assume that $\mathrm{Gal}(f(X,t)|\mathbb{Q}(t))$ is primitive, however the group theoretic analysis requires considerably more work. In particular, the classification of the finite simple groups proves indispensable for this analysis.

There are certain families of examples showing that we cannot simply replace the prime degree or generality assumption by primitivity. As a sample, we give the following construction.

Theorem 9.1. *Let $2 \leq k \leq n-2$ be integers with $2k \neq n$. Then there exists an irreducible polynomial $f(X,t)$ with $\deg_X f = \binom{n}{k}$ and primitive Galois group over $\mathbb{Q}(t)$, such that there are infinitely many $t_0 \in \mathbb{Z}$ such that $f(X,t_0)$ is reducible without a linear factor.*

Proof. The proof is a sort of inversion of the arguments in the general case, but with the special feature that U and V interchange their roles! Let A be the symmetric group on n letters $\{1,2,\ldots,n\}$, and $g(Z) \in \mathbb{Z}[Z]$ be a polynomial of degree n such that the Galois group of $g(Z)-t$ over $\mathbb{Q}(t)$ is A. (Such polynomials are very easy to construct – for instance the Morse polynomial $g(Z) = Z^n - Z$ will do it, see [Ser92, Theorem 4.4.1], or $g(Z) = Z^n - Z^{n-1}$, see [Ser92, page 42].) Let U be the setwise stabilizer in A of a subset of size k in $\{1,2,\ldots,n\}$. We first show that U is a maximal subgroup of A. Let M be a subgroup of $A = S_n$ which properly contains $U = S_k \times S_{n-k}$. So M is transitive on $\{1,2,\ldots,n\}$. As $2k \neq n$, we see that the group M is even primitive, as it does not admit a nontrivial system of imprimitivity. (For suppose that there is a non–trivial block system. Without loss there is a block Δ which contains at least two of the digits $1,2,\ldots,k$. Then each of these digits has to be contained in Δ, as S_k is doubly transitive on these

digits. The same reasoning then shows that the remaining digits $k+1, \ldots, n$ constitute a block Δ'. But there is an element in M which does not fix Δ, so it must interchange Δ and Δ'. Hence $k = |\Delta| = |\Delta'| = n - k$, a contradiction.) Also, M obviously contains a transposition (because even U does), so $M = S_n$ by [Wie64, 13.3]. Thus U is a maximal subgroup of A.

Let L be a splitting field of $g(Z) - t$ over $\mathbb{Q}(t)$ and let z be a root of $g(Z) - t$. Let $f(X, t)$ be a minimal polynomial of a generator x of the fixed field of U over $\mathbb{Q}(t)$. Then $\mathrm{Gal}(L/\mathbb{Q}(z))$ acts on the conjugates of x over $\mathbb{Q}(t)$ as S_{n-1} acts on $S_n/(S_k \times S_{n-k})$. The latter action is intransitive (with two orbits, one of length $\binom{n-1}{k}$, the other one of length $\binom{n-1}{k-1}$). Moreover, as $2 \leq k \leq n-2$, it has no fixed point. This means that $f(X, t)$ is reducible over $Q(z)$ but has no linear factor. Conclude that $f(X, g(Z))$ is reducible over $Q(Z)$ but has no linear factor.

Let $f_i(X, Z)$ be the irreducible factors of $f(X, g(Z))$. By Hilbert's irreducibility theorem, there are infinitely many $z_0 \in \mathbb{Z}$ such that all $f_i(X, z_0)$ are irreducible. For these z_0 set $t_0 = g(z_0) \in \mathbb{Z}$, and we have that $f(X, t_0)$ is reducible without a linear factor. □

Remark. There are other examples besides the given one. However, if we assume that $A = \mathrm{Gal}(f(X, t))|\mathbb{Q}(t)$ is primitive, then there are only very few possibilities for the composition factors of A. Work on this is in progress.

It can be shown that the genus of the curve $f(X, t) = 0$ in the example above can be made arbitrarily large (with growing n).

As to (b). If we assume $n \neq 4$, then in the general case actually we need not work over $\mathbb{Q}$. The only difference coming in is the structure of g. Again g has two poles (or is a polynomial), but they no longer need to have the same order. So we still get an inertia generator σ with at most 2 orbits on A/V. Lemma 5.7 handles this case. Also, the arguments go through without change if $\mathrm{Gal}(f(X, t)|K(t))$ is alternating rather than symmetric. So we indeed get the more general

Theorem 9.2. *Let K be a number field, and $f(X, t) \in K[X, t]$ be an irreducible polynomial of X–degree $\neq 4, 5$, such that $\mathrm{Gal}(f(X, t)|K(t))$ is the alternating or symmetric group in the natural representation. Let R be a finitely generated $\mathbb{Z}$–subalgebra of K. Then there are only finitely many $t_0 \in R$, such that $f(X, t_0) \in K[X]$ is reducible without a linear factor.*

The prime degree case is harder, and there are numerous examples which show that we indeed cannot simply replace $\mathbb{Q}$ by a number field. These examples can be classified, but require a considerable amount of work and the classification of the finite simple groups. Work on this is in progress too.

As to (c). Here the theorem of Siegel–Mahler–Lang has to be replaced by Falting's theorem, that there are only finitely many rational points on an algebraic curve of genus > 1. The Galois theoretic translation requires obvious modifications. In particular, instead of the field $\mathbb{Q}(z)$ we can have the function field of an elliptic curve of positive Mordell–Weil rank. But even if we still have rational fields, we of course do not have any information about the ramification of $\mathbb{Q}(z)$ over $\mathbb{Q}(b(z))$, there are no constraints. Still, we can use the Riemann–Hurwitz genus formula to analyze the configurations, and the branch cycle argument to eliminate many cases. We have just begun analyzing this configuration. The analysis is already very difficult if we assume only that A is a symmetric group in the natural action.

Remark 9.3. Let $f(X,t) \in \mathbb{Q}[X,t]$ be irreducible. Instead of looking for specializations $t_0 \in \mathbb{Z}$ with $f(X,t_0)$ still irreducible, one could also ask for the stronger property that $\mathrm{Gal}(f(X,t)|\mathbb{Q}(t)) = \mathrm{Gal}(f(X,t_0)|\mathbb{Q})$. Here, however, the analog of Theorem 1.1 is not true in the prime degree case, nor in the general case. For set $h_\theta(X) = X^{n-1}(X-1) - \theta$ for a variable θ. The ramification of $h_\theta(X)$ shows that $A := \mathrm{Gal}(h(X,\theta)|\mathbb{Q}(\theta))$ contains an n–cycle, an $(n-1)$–cycle, and a transposition, see [Ser92, page 42]. The first two elements force A to be doubly transitive, so A contains all transpositions of the roots of $h_\theta(X)$, hence $A = S_n$. One easily computes the X–discriminant of $h_\theta(X)$: $\mathrm{dis}_X\, h_\theta(X) = c\theta^{n-2}(\theta + d)$, for some $0 \neq c, d \in \mathbb{Q}$. (The actual values of c and d are easy to compute, but are irrelevant here.) Rewrite $\mathrm{dis}_X\, h_\theta(X) = c\theta^{n-1}(\theta + d)/\theta$ and set $t := d/\theta$, $f(X,t) := tX^{n-1}(X-1) - d$. So $\mathrm{Gal}(f(X,t_0)|\mathbb{Q}) \leq A_n$ if and only if $c(1+1/t_0)$ is a square in $\mathbb{Q}$. Of course, there are infinitely many such $t_0 \in \mathbb{Z}$, for instance $t_0 = c_1c_2k^2 - 1$, where c_1, c_2 are numerator and denominator of c respectively, and k runs through the integers. On the other hand, $f(X,t_0)$ is reducible only for finitely many integers t_0 by the results in this paper.

References

[Bil96] Y. Bilu, *A note on universal Hilbert sets*, J. Reine Angew. Math. (1996), **479**, 195–203.

[DF99] P. Dèbes, M. D. Fried, *Integral specialization of families of rational functions*, Pacific J. Math. (1999), **190**(1), 45–85.

[DM96] J. D. Dixon, B. Mortimer, *Permutation Groups*, Springer–Verlag, New York (1996).

[DZ98] P. Dèbes, U. Zannier, *Universal Hilbert subsets*, Math. Proc. Cambridge Philos. Soc. (1998), **124**, 127–134.

[Fri74] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory (1974), **6**, 211–231.

[Fri94] M. Fried, *Review of Serre's 'Topics in Galois Theory'*, Bull. Amer. Math. Soc. (N.S.) (1994), **30**(1), 124–135.

[Fri95] M. Fried, *Extension of constants, rigidity, and the Chowla–Zassenhaus conjecture*, Finite Fields Appl. (1995), **1**, 326–359.

[Gor68] D. Gorenstein, *Finite Groups*, Harper and Row, New York–Evanston–London (1968).

[HB82] B. Huppert, N. Blackburn, *Finite Groups III*, Springer–Verlag, Berlin Heidelberg (1982).

[Hup67] B. Huppert, *Endliche Gruppen I*, Springer–Verlag, Berlin Heidelberg (1967).

[Lan83] S. Lang, *Fundamentals of Diophantine Geometry*, Springer–Verlag, New York (1983).

[Mül96] P. Müller, *Reducibility behavior of polynomials with varying coefficients*, Israel J. Math. (1996), **94**, 59–91.

[Neu72] P. M. Neumann, *Transitive permutation groups of prime degree*, J. London Math. Soc. (2) (1972), **5**, 202–208.

[Ser92] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston (1992).

[Shi74] K. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. (1974), **207**, 99–120.

[Sie29] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Pr. Akad. Wiss. (1929), **1**, 41–69, (=Ges. Abh., I, 209–266).

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

[Wie64] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York London (1964).

[Zan96] U. Zannier, *Note on dense Hilbert sets*, C. R. Acad. Sci. Paris Sér. I Math. (1996), **322**, 703–706.

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