(A_n, S_n) Realizations by Polynomials – on a Question of Fried

Peter Müller *

October 10, 2000

Abstract

While disproving a conjecture of Cohen about monodromy groups of polynomials and applying this to give new counter–examples to a question of Chowla and Zassenhaus in [Fri95], Fried asked whether there are polynomials over $\mathbb{Q}$ of odd square degree n with geometric and arithmetic monodromy group the alternating group A_n and symmetric group S_n, respectively. In this note we give two different proofs that such polynomials do not exist.

1 Introduction

Let K be a field of characteristic 0, and $f(X) \in K[X]$ be a polynomial of positive degree n. With t a transcendental, denote by L a splitting field of $f(X) - t$ over $K(t)$, and let $\hat{K}$ be the algebraic closure of K in L. Then $A := \mathrm{Gal}(L/K(t))$ and $G := \mathrm{Gal}(L/\hat{K}(t))$ are the arithmetic and geometric monodromy group of f, respectively. These two groups are considered as permutation groups on the roots of $f(X) - t$. Note that $\mathrm{Gal}(\hat{K}/K) = A/G$. A subgroup of the symmetric group S_n is called even, if it is contained in the alternating group A_n, otherwise it is called odd.

Suppose that $G = A_n$ and $K = \mathbb{Q}$. As G contains a cyclic transitive group (see below), n must be odd. Using the branch cycle argument, Fried showed that $A = S_n$ provided that n is not a square. It is easy to give

*Supported by the DFG.

polynomials over $\mathbb{Q}$ with $G = A_n$. Such polynomials disprove a conjecture of Cohen about possible pairs (A, G) and give new types of counter–examples to a conjecture of Chowla and Zassenhaus. For all of this see [Fri95].

A question which was investigated but left open in [Fri95] is whether such polynomials exist also for square n, see [Fri95, Synopsis of unsolved problems 4.9]. Fried gives several approaches, and shows that some cannot work. In this note we show that such examples do not exist. Actually, we prove the more general

Theorem. *Let K be a field of characteristic 0, $f \in K[X]$ be a polynomial of degree $n > 0$, with A and G the arithmetic and geometric monodromy group of f, respectively.*

Suppose that G is even. Then n is odd, and A is even if and only if $(-1)^{(n-1)/2}n$ is a square in K. In particular, if $K = \mathbb{Q}$, then A is even if and only if n is a square.

2 Proof of the Theorem

Let $x_1, x_2, \ldots, x_n$ be the roots of $f(X) - t$, and $y_1, y_2, \ldots, y_{n-1}$ be the roots of the derivative $f'(X)$. Without loss assume that f is monic, hence $f'(X) = n\prod(X - y_k)$. From $f'(X) = \sum_j \prod_{i,i\neq j}(X - x_i)$ one obtains $f'(x_j) = \prod_{i,i\neq j}(x_j - x_i)$. Using this, we get the following expression for the discriminant of $f(X) - t$ with respect to X

$$
\begin{aligned}
(\mathrm{dis}_X(f(X) - t))^2 &= (\prod_{i,j,i<j}(x_i - x_j))^2 \\
&= (-1)^{n(n-1)/2}\prod_j \prod_{i,i\neq j}(x_j - x_i) \\
&= (-1)^{n(n-1)/2}\prod_j f'(x_j) \\
&= (-1)^{n(n-1)/2} n^n \prod_j \prod_k (x_j - y_k) \\
&= (-1)^{n(n-1)/2} n^n \prod_k \prod_j (y_k - x_j) \\
&= (-1)^{n(n-1)/2} n^n \prod_{k=1}^{n-1} (f(y_k) - t).
\end{aligned}
$$

Note that n is odd, because G contains an n–cycle (a generator of an inertia group of a place of L lying above the infinite place of $K(t)$). Therefore $(\mathrm{dis}_X(f(X)-t))^2$ is a polynomial in t of degree $n-1$ and highest coefficient $a_{n-1} := (-1)^{n(n-1)/2}n^n$. As n is odd, $a_{n-1} = [(-1)^{(n-1)/2}n]^n$ is a square in K if and only if $(-1)^{(n-1)/2}n$ is a square in K. As G is even, $(\mathrm{dis}_X(f(X)-t))^2$ is a square in $\hat{K}(t)$. Accordingly write

$$(\mathrm{dis}_X(f(X)-t))^2 = a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = (b_m t^m + \cdots + b_1 t + b_0)^2$$

with $m = (n-1)/2$ and $b_i \in \hat{K}$. If A is even, then we can assume $b_i \in K$, hence $a_{n-1} = b_m^2$ is a square in K. Conversely, if a_{n-1} is a square in K, then we can successively solve for $b_m, b_{m-1}, \ldots, b_1, b_0$ and see that we get $b_i \in K$ for $i < m$ if we start with $b_m \in K$. This proves the claim.

3 Another proof for $K = \mathbb{Q}$

If $K = \mathbb{Q}$, then the case of non–square degree n is covered by [Fri95], so we assume that n is a square in the previous theorem. Note that $(-1)^{(n-1)/2} = 1$, as n is an odd square. So we need to show that A is even. For that we may assume that K is any field of characteristic 0.

Let P be a place of L lying above the infinite place of $K(t)$. Denote by D and I the decomposition and inertia group of P, respectively. Now D/I induces the full Galois group of the residue field extension L_P/K of the place P, but $\hat{K}$ embeds into L_P, so D/I surjects to $A/G = \mathrm{Gal}(\hat{K}/K)$. That is $A = GD$, so in particular $A = GN_A(I)$, where $N_A(I)$ denotes the normalizer of I in A. However, if n is a square, then the generators of I are already conjugate inside the alternating group A_n (e. g. by the the irrational cycle lemma [Fri95, page 332]), and this easily implies that $N_A(I) \le N_{A_n}(I)$ is even, so $A = GN_A(I)$ is even as well.

4 Remark on explicit (A_n, S_n)–realizations

Let $f \in \mathbb{Q}[X]$ be a polynomial which gives an (A_n, S_n)–realization. Then, as Fried showed in [Fri95], there are infinitely many primes p such that $f(X)-b$ is reducible modulo p for all integers b – contrary to a conjecture of Chowla–Zassenhaus.

In order to apply this result, one has to prove that there are polynomials $f \in \mathbb{Q}[X]$ with geometric monodromy group A_n for odd non–square degree n. Fried [Fri95] gives several constructions.

The simplest is the following: Let f be an antiderivative of $(X-1)^2 X^{n-3}$. The corresponding inertia generators (see [Fri95] for this concept) are an $(n-2)$–cycle, a 3–cycle, and the n–cycle at infinity.

A slight modification of this construction would replace the 3–cycle by a double–transposition. Fried investigates the arithmetic of this in [Fri95, Example 4.5]. The only odd $n \geq 5$ where he is able to show that there is a realization over $\mathbb{Q}$ is for $n = 5$. He derives an explicit polynomial $g_n(X)$ (of degree $n-3$) with the property that factors over $\mathbb{Q}$ of degree at most 2 would give such realizations of degree n, and vice versa. However, these polynomials seem to be irreducible for all n, though a proof is still missing. (Fried checked this for $n \leq 31$.)

[Fri95, Example] gives a well–known construction, where all inertia generators of the finite places are 3–cycles. Namely let $g \in \mathbb{Q}[X]$ be any separable polynomial of degree $(n-1)/2$, and f an antiderivative of g. Then f is such an example, provided that the roots of g are mapped to distinct points under f.

Again, as above, one might ask the analogous question if we replace the 3–cycles by double–transpositions. [Fri95] contains much about this question, but leaves the case $n > 7$ open.

References

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

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