Bulletin of the Iranian Mathematical Society (2022) 48:1919–1926
https://doi.org/10.1007/s41980-021-00635-2

ORIGINAL PAPER

On the Galois Groups of Some Recursive Polynomials

Khosro Monsef-Shokri[1]

Received: 6 April 2021 / Revised: 21 July 2021 / Accepted: 16 August 2021 /
Published online: 27 August 2021

Abstract

We show that for some recursive sequence $(c_m)_{m\geq 1}$ of integers and for sufficiently large n, the Galois group of polynomial $f_n(x)=\frac{x^n}{n!}+c_{n-1}\frac{x^{n-1}}{(n-1)!}+\cdots+c_1\frac{x}{1!}+1$, contains the alternating group A_n. In case n is a prime number, this group is the full symmetric group S_n.

Keywords Galois groups · Recursive sequences · Permutation groups · Newton polygon

Mathematics Subject Classification 12F12 · 11B37

1 Introduction

In [10] Schur by taking the truncated Taylor series of e^x, gave an explicit answer to the question of finding a polynomial of arbitrary degree with rational coefficients whose Galois group is full symmetric group. Since then many explicit examples have been constructed (see for example [8]). Coleman [3] with the idea of Newton polygon gave an elegant proof for the theorem of Schur. This idea can be generalized to many examples which is the motivation for this article. Indeed the following theorem which is not mentioned in Colemann's paper but it is the core of that article is our key theorem.

Theorem 1.1 *Let*

$$f_n(x)=\frac{x^n}{n!}+c_{n-1}\frac{x^{n-1}}{(n-1)!}+\cdots+c_1\frac{x}{1!}+1,$$

Communicated by Rahim Zaare-Nahandi.

✉ Khosro Monsef-Shokri
k_shokri@sbu.ac.ir

[1] Faculty of Mathematical Sciences, Department of Mathematics, Shahid Beheshti University, Tehran, Iran

where $(c_m)_{m\geq 1}$ is an integer sequence such that for some prime p in the interval $(\frac{n}{2}, n-2)$, the term c_p is not divisible by p. Then the Galois group of $f_n(x)$ is either the alternating group A_n or the full symmetric group S_n.

In order to assure Theorem 1.1 for concrete examples, we search in two kinds of recursive sequences.

Theorem 1.2 *Let $f_n(x)$ be as in Theorem 1.1, where either*

- *the sequence $(c_m)_{m\geq 1}$ is an infinite integer sequence, defined recursively by*

$$c_1 = 1, \quad c_2 = r, \quad \text{and} \quad c_m = r\, c_{m-1} + s\, c_{m-2}, \qquad m \geq 3 \tag{1.1}$$

  for some $r, s \in \mathbb{Z}$, such that $r^2 + 4s \neq 0$, or
- *$(c_m)_{m\geq 0}$ is an infinite integer sequence, defined recursively by*

$$c_0 = 1, \quad c_1 = c, \quad \text{and} \quad c_m = r\, c_{m-1} + s\, c_{m-2}, \qquad m \geq 2 \tag{1.2}$$

  where c is an arbitrary integer and r, s as before.

Then for sufficiently large n, the Galois group of $f_n(x)$ is either A_n or S_n.

For non-linear recurrence of order one, we have a similar result as follows.

Theorem 1.3 *Let $f_n(x)$ be as in Theorem 1.1, such that $c_m = \phi(c_{m-1})$, with initial value $c_{-1} = 0$, where ϕ is a polynomial of degree $d \geq 2$, defined over $\mathbb{Z}$ with nonzero constant term. Then for sufficiently large n, the Galois group of $f_n(x)$ is either A_n or S_n.*

For an arbitrary orbit $c_m = \phi^m(a)$ we have a weaker result as follows.

Theorem 1.4 *Let $f_n(x)$ as before and $\phi \in \mathbb{Z}[x]$ is an irreducible polynomial of degree $d \geq 2$. For a nonzero integer a we consider the sequence $c_m = \phi^m(a)$, $m \geq 1$. Then for infinitely many n the Galois group of f_n is either A_n or S_n.*

The dichotomy expressed in all theorems is related to the value of discriminant. If the discriminant of the concerning polynomial is square then it is well-known that the corresponding Galois group is contained in A_n. This situation for example occurs in the Schur's example, when n is divisible by 4. In fact in this case there exists a simple formula for the discriminant, namely $D_n = (-1)^{\binom{n}{2}}(n!)^{2-n}$. Besides this example it seems hopeless to determine a situation in which the discriminant is square. However there are some criteria to decide the opposite side. Here we provide two cases:

Corollary 1.5 *Let f_n be as in the preceding theorems with $c_1 \neq 0$. If n is a sufficiently large prime number, then the Galois group of f_n is S_n.*

Corollary 1.6 *Let f_n and $(c_m)_{m\geq 1}$ be as in the first part of Theorem 1.2, such that $3 \nmid r(r^2+s)$, then there exists an arithmetic progression such that for each n in this sequence, the Galois group of f_n is S_n.*

The article organized as follows. In the following section we review some essential facts about Newton polygon and we give a proof of Theorem 1.1. Then in Sect. 3 we prove the main theorems and corollaries.

2 Newton Polygon and Its Applications

Let K be a local field with discrete valuation ν_K and let

$$f(x) = a_0 + a_1 x + \cdots a_{n-1} x^{n-1} + a_n x^n \in K[x]$$

be a polynomial with $a_0 a_n \neq 0$. Then the Newton polygon of f is defined to be the lower convex hull in $\mathbb{R}^2$ of the points

$$(0, \nu_K(a_0)), \ldots, (i, \nu_K(a_i), \ldots, (n, \nu_K(a_n)).$$

ignoring the points with $a_i = 0$. If we denote the vertices of this polygon by the points $(x_0, y_0), (x_1, y_1), \ldots, (x_s, y_s)$, then $f(x)$ factors over K as

$$f(x) = f_1(x) \cdots f_s(x),$$

in which for any $1 \leq i \leq s$ the degree of $f_i(x)$ is $x_i - x_{i-1}$ and all the roots of $f_i(x)$ in $\bar{K}$ have valuations $-\dfrac{y_i - y_{i-1}}{x_i - x_{i-1}}$ (see [1]).

Example 2.1 Let $e_4(x) = \frac{x^4}{4!} + \frac{x^3}{3!} + \frac{x^2}{2!} + x + 1$, be the 4-th Taylor polynomial of e^x. Its Newton polygon over $\mathbb{Q}_2$ has one side, joining $(0, 0)$ to $(4, -3)$. Hence all roots of $e_4(x)$ have valuation $\frac{3}{4}$ over $\mathbb{Q}_2$, while over $\mathbb{Q}_3$ it has two sides: one side joining $(0, 0)$ to $(3, -1)$, the other side joining $(3, -1)$ to $(4, -1)$ The corresponding polynomials have 3 roots of valuation $\frac{1}{3}$ and one root with zero valuation, respectively.

The advantage of having information about the roots of f over local fields leads to the following important lemma:

Lemma 2.2 (Coleman [3]) *Let $f(x)$ be a polynomial defined over $\mathbb{Q}$, such that*

$$f(x) = f_1(x) \cdots f_s(x) \in \mathbb{Q}_p[x]$$

where $f_i(x)$ corresponds to the i-th side of its Newton polygon. Let $f_k(x)$ for some $1 \leq k \leq s$, be irreducible over $\mathbb{Q}_p$. If d divides $x_k - x_{k-1}$, then the order of the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$ is a multiple of d.

Applying the above lemma to Example 2.1 we find that the order of its Galois group G, is divisible by 12. On the other hand $\mathrm{disc}(e_4) = 24^{-2}$, is square, so G must be the alternating group A_4.

The following theorem of Schur, guarantees that the family of polynomials $f_n(x)$ are irreducible, which is essential in the continuation.

Theorem 2.3 (Schur [9]) *Let $(c_n)_{\geq 1}$ be an integer sequence. Then the polynomial*

$$f_n(x) = \frac{x^n}{n!} + c_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + c_1 \frac{x}{1!} + 1,$$

is an irreducible polynomial over $\mathbb{Q}$.

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1 According to Theorem 2.3, $f_n(x)$ is irreducible, so the Galois group of f_n, G, is transitive. Now by the assumption there exists a prime number p between $n/2$ and n, such that $p \nmid c_p$, so the Newton polygon of $f_n(x)$ over $\mathbb{Q}_p$ has two sides: one side joining $(0, 0)$ to $(p, -1)$ and another one joining $(p, -1)$ to $(n, -1)$. Hence we have $f_n(x) = f_{n1}(x) f_{n2}(x)$ over $\mathbb{Q}_p$, where f_{n1} is a monic polynomial of degree p with roots of valuation $\frac{1}{p}$. We claim that $f_{n1}(x)$ is irreducible over $\mathbb{Q}_p$. Indeed if $f_{n_1}(x) = g(x)h(x)$ over $\mathbb{Q}_p$, with $1 \le \deg(h) \le p - 1$, then h_0, the constant term of h equals to the product over a proper subset of the roots of $f_{n_1}(x)$. So its valuation is not integral which is a contradiction with $h_0 \in \mathbb{Q}_p$. Now from Lemma 2.2, p divides the order of G, the Galois group of $f_n(x)$ and by Cauchy's theorem G has an element of order p. Since $\frac{n}{2} < p < n-2$, this element is a p-cycle. This implies that G is primitive. Indeed if G is imprimitive, then there exist nontrivial blocks X_i, $i = 1, \ldots, d$, for some $d \ge 2$, which are invariant under G. Since G is transitive, so for $i = 1, \ldots, d$, the cardinal of X_i, are equal. Therefore $|X_i| \le n/2$ and $d \le n/2$. Now let $\sigma = (a_1, a_2, \ldots, a_p) \in G$ be a p-cycle with $p > n/2$, then either each a_i belongs to distinct X_j or all of them belong to a single X_i. Both cases lead to a contradiction.

Now according to a Theorem of Jordan (see [4, Theorems 5.6.2 and 5.7.2]) a primitive group having such a p-cycle contains A_n. □

The following definition is suitable for our purpose.

Definition 2.4 For an integer sequence $(c_m)_{m \ge 1}$, a prime p is called favorite if $p \nmid c_p$, otherwise p is unfavorite.

It is worth mentioning that the index divisibility problem, namely the classification of those n such that $n \mid c_n$ is an interesting question in Arithmetic Dynamics and it has been the subject of several papers. For example see [2] and the references therein.

3 Proofs

In this section we prove main results. First we consider the linear case.

3.1 Linear Sequences

The main idea to prove Theorem 1.2 is to show that the set of favorite primes of the sequence $(c_m)_{m \ge 1}$ has not zero density, more precisely we have:

Lemma 3.1 *Let $(c_m)_{m \ge 0}$ be as in (1.2) and $\Delta = r^2 + 4s$ be the discriminant of its characteristic polynomial. If $p > 2$ is a prime number such that $p \nmid c$ and $(\frac{\Delta}{p}) = 1$, then p is favorite.*

Proof Let α and β be two distinct roots of $x^2 - rx - s = 0$, the characteristic polynomial of (c_m) modulo p. By the assumption Δ is a nonzero quadratic residue modulo p. Hence $\alpha, \beta \in \mathbb{F}_p$. The general term of the sequence is given by

$$c_m = \frac{c-\beta}{\alpha-\beta}\alpha^m - \frac{c-\alpha}{\alpha-\beta}\beta^m.$$

We have $\alpha^p \equiv \alpha \pmod p$ and $\beta^p \equiv \beta \pmod p$. Therefore

$$c_p \equiv \frac{c-\beta}{\alpha-\beta}\alpha - \frac{c-\alpha}{\alpha-\beta}\beta \equiv c \pmod p.$$

Since $p \nmid c$, so $p \nmid c_p$ and hence p is a favorite prime.

Now we are ready to prove Theorem 1.2.

Proof of Theorem 1.2 The first part is straightforward. We show that almost all primes are favorite with respect to the sequence $(c_m)_{m\geq 1}$. Since $\Delta \neq 0$, we can take a prime p which is not a divisor of Δ. Let $\alpha, \beta \in \mathbb{F}_{p^2}$ are the distinct roots of $x^2 - rx - s = 0$, then the general term of (c_m) can be written as

$$c_m = \frac{1}{\alpha-\beta}(\alpha^m - \beta^m).$$

Therefore $c_p = (\alpha-\beta)^{p-1} = \Delta^{\frac{p-1}{2}} \not\equiv 0 \pmod p$. Hence every prime $p > \Delta$, is favorite. Now we apply Theorem 1.1 and the proof of the first part is complete.

For the second part, from Lemma 3.1, if $(\frac{\Delta}{p}) = 1$, then p is favorite. According to the quadratic reciprocity law, those primes such that $(\frac{\Delta}{p}) = 1$, form some arithmetic progressions. Now Dirichlet's theorem implies that the density of such primes is at least $1/\varphi(\Delta)$, where φ is the Euler's totient function. Hence for large enough n always there exists such prime between $n/2$ and $n-2$. Once again we apply Theorem 1.1 and the result follows. □

3.2 Nonlinear Sequences

With the same strategy as in the proof of Theorem 1.2 we would like to show that the set of favorite primes for the sequence $(\phi^m(0))_{m\geq 1}$ has positive density. We need the following proposition. Although the statement of proposition was not conjectured by Schur, but it is known as Schur's conjecture in the literature. For a proof see [7].

Proposition 3.2 *Let $\phi(x)$ be an integral polynomial, which is a permutation polynomial over $\mathbb{F}_p$ for infinitely many primes p. Then $\phi(x)$ is a composition of linear and Dickson polynomials.*

Proof of Theorem 1.3 If the set of unfavorite primes of the sequence $(c_m)_{m\geq 1}$ is finite, then the result follows from Theorem 1.1, otherwise for infinitely many primes p we have $\phi^p(0) \equiv 0 \pmod p$. For all but finitely many of such primes we have $p \nmid \phi(0)$. Therefore if for some k, we have $p \mid \phi^k(0)$, then $p \mid k$, so the set $\{\phi^i(0) \pmod p\}_{i=1}^{p}$ is a complete set of residue modulo p. This implies that for such primes, $\phi(x)$ is a permutation polynomial over $\mathbb{F}_p$. Hence by Proposition 3.2, $\phi(x)$ is a composition of Dickson and linear polynomials. Now we choose primes p in the arithmetic progressions $dk + 1$, where $d \geq 2$ is the degree of ϕ. Since $(d, p - 1) > 1$, so $\phi(x)$ can not be a composition of a linear polynomial and $D_d(0, x) = x^d$. On the other hand it is well-known that the Dickson polynomial $D_d(a, x)$ with $a \neq 0$ of degree d is a permutation polynomial in $\mathbb{F}_p$ if and only if $p^2 - 1$ and d are coprime (see [6], p.396). Therefore primes of the form $dk+1$ are favorite for the sequence $(\phi^m(0))_{m\geq 1}$. Now Dirichlet's theorem on arithmetic progression implies that for sufficiently large n, between $n/2$ and $n - 2$ always there exists a prime of the form $dk + 1$. □

For a nonzero orbit $(\phi^m(a))_{m\geq 1}$, if the set of unfavorite primes is finite then in a similar fashion one can deduce that for sufficiently large n the Galois group of $f_n(x)$ contains the alternating group A_n. However if the set of unfavorite primes is infinite, then unlike the zero orbit one can not deduce that $\phi(x)$ is a permutation polynomial. Instead we apply the Chebotarev density theorem.

Proof of Theorem 1.4 We show that the set of favorite primes for the sequence $(\phi^m(a))$ is infinite. Suppose in contrary all but finitely many primes are unfavorite. It means that $\phi^p(a) \equiv 0 \pmod p$ for almost all p. In particular $\phi(x)$ has a solution in $\mathbb{F}_p$ for almost all p. Since $\phi(x)$ is irreducible over $\mathbb{Z}$, so its Galois group G is a transitive group. Since $\deg(\phi) > 1$, hence by Jordan's theorem [5] there exists an element $\sigma \in G$ acting on the set of roots of ϕ without fixed point. We consider the conjugacy class C of σ in G. By Chebotarev density theorem the density of primes p, such that $\mathrm{Frob}_p \in C$ is $\frac{|C|}{|G|}$. For this set of primes of positive density the cycle structure of Frob_p has no fixed point. But by Dedekind's theorem the length of each cycle corresponds to the degree of factors of $\phi(x) \pmod p$. It means that for such primes p, the factorization of $\phi(x) \pmod p$ has no linear factors which contradicts our assumption on ϕ. Hence the set of favorite primes is infinite. Now from Theorem 1.1 for each favorite prime p and n in the interval $(p, 2p)$, the Galois group of $f_n(x)$, contains A_n. □

3.3 Corollaries

In this final subsection we determine some cases in which the Galois group of $f_n(x)$ is exactly S_n. As we have discussed in the Introduction, we need to show that the discriminant of $f_n(x)$ is not square. In order to obtain Corollary 1.5 we use the resultant matrix. For Corollary 1.6 we use the fact that if the discriminant of $f_n(x)$ is square then in any reduction modulo p it must be a quadratic residue.

Proof of Corollary 1.5 Let

$$g_n(x) = n! f_n(x) = x^n + nc_{n-1} x^{n-1} + \cdots + n!c_1 x + n!.$$

We show that if $n > c_1$ is an odd prime number then the exponent of n in $D = \mathrm{disc}(g_n)$ is an odd number, so D is not square and therefore the discriminant of f_n is not square as well.

Since g_n is monic, so we have $D = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(g_n, g_n')$, where Res denotes the resultant:

$$\operatorname{Res}(g_n, g_n') = \det \begin{pmatrix} 1 & 0 & \cdots & 0 & n & 0 & \cdots & 0 \\ nc_{n-1} & 1 & \cdots & 0 & n(n-1)c_{n-1} & n & \cdots & 0 \\ \vdots & \vdots & \ddots & 1 & \vdots & \vdots & \ddots & n \\ n! & n!c_1 & \cdots & \vdots & n!c_1 & n!c_2 & \cdots & \vdots \\ 0 & n! & \ddots & \vdots & 0 & n!c_1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & n!c_1 & \vdots & \vdots & \ddots & n!c_2 \\ 0 & 0 & \cdots & n! & 0 & 0 & \cdots & n!c_1 \end{pmatrix}.$$

If we call the above matrix with $R = (r_{ij})_{m \times m}$, where $m = 2n - 1$. Then the entries of the first $n-1$ columns of R are the coefficients of g_n in the echelon form and the entries of the next n columns are the coefficients of g_n'. By definition we have

$$\begin{aligned} \det(R) &= \sum_{\pi \in S_m} \operatorname{sgn}(\pi) r_{1\pi(1)} \cdots r_{m\pi(m)} \\ &= r_{11} r_{22} \cdots r_{mm} + \sum_{\pi \in S_m \pi \neq id} \operatorname{sgn}(\pi) r_{1\pi(1)} \cdots r_{m\pi(m)} \\ &= c_1^n (n!)^n + \sum_{\pi \in S_m \pi \neq id} \operatorname{sgn}(\pi) r_{1\pi(1)} \cdots r_{m\pi(m)}. \end{aligned}$$

We note that $n \mid r_{ij}$, unless $i = j$, with $1 \leq i \leq n-1$, so the second term in above is divisible by n^{n+1}, while the exponent of n in the first term is n. Hence $\operatorname{ord}_n(\det(R)) = n$. and $\det(R)$ is not square.

Proof of Corollary 1.6 We reduce $g_n = n! f_n(x)$ modulo prime 3. For $n = 3k + 2$, we find that

$$g_n(x) \equiv x^{n-2}(x^2 + nc_{n-1}x + n(n-1)c_{n-2}) \equiv x^{n-2}(x^2 - c_{n-1}x - c_{n-2}) \pmod 3.$$

In order to show that the discriminant of f_n is not square it is enough to show that,

$$\operatorname{disc}(x^2 - c_{n-1}x - c_{n-2}) \equiv c_{n-1}^2 + c_{n-2} \pmod 3,$$

is not a quadratic residue in $\mathbb{F}_3$, namely $c_{n-1}^2 + c_{n-2} \equiv -1 \pmod 3$. We would like to show that this situation occurs when n belongs to some arithmetic progression.

By assumption $r^2 + s$, the characteristic polynomial, is not zero in $\mathbb{F}_3$. Thus as we have seen in the proof of Theorem 1.2, the general term of $c_m \pmod 3$ is given by $c_m = \frac{1}{\alpha - \beta}(\alpha^m - \beta^m)$, where $\alpha, \beta \in \mathbb{F}_9$. From this expression it is clear that $c_{8m+k} \equiv c_k \pmod 3$. Now if $r \equiv 1 \pmod 3$, then

$$c_{8m+2}^2 + c_{8m+1} \equiv -1 \pmod 3$$

and we are done. Otherwise we have the two following sequences according to $s \equiv 1, 0 \pmod 3$ respectively:

- $1, -1, \boxed{-1}, \boxed{0}, -1, \boxed{1}, \boxed{1}, 0 \cdots$
- $\boxed{1}, \boxed{-1}, 1, -1, \cdots$

Those consecutive terms in the boxes which satisfying the desired condition, make arithmetic progressions, and the proof is finished. □

References

1. Cassels, J.W.S.: Local Fields. Cambridge University Press, Cambridge (1986)
2. Chen, A.S., Alden Gassert, T., Stange, K.E.: Index divisibility in dynamical sequences and cyclic orbits modulo p. N. Y. J. Math. **23**, 1045–1063 (2017)
3. Coleman, R.: On the Galois groups of the exponential Taylor polynomials. Enseign. Math. **33**, 183–189 (1987)
4. Hall, M.: Theory of Groups. Macmillan, New York (1959)
5. Jordan, C.: Recherches sur les substitutions. J. Liouville **17**, 351–367 (1872)
6. Lidle, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
7. Muller, P.: A Weil-bound free proof of Schur's conjecture. Finite Fields Their Appl. **3**, 25–32 (1997)
8. Osada, H.: The Galois groups of the polynomials $x^n + ax^s + b$. J. Number Theory **25**, 230–238 (1987)
9. Schur, I.: Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibiliätsfragen I. Sitzungsberichte Preuss. Akad. Wiss. Phys. Math. Klasse **14**, 125–136 (1929)
10. Schur, I.: Gleichungen ohne Affekt. Gesammelte Abhandlungen **III**(67), 191–197 (1930)