International Journal of Number Theory
Vol. 15, No. 6 (2019) 1127–1141

DOI: 10.1142/S1793042119500623

World Scientific
www.worldscientific.com

Galois groups of Taylor polynomials of some elementary functions

Khosro Monsef Shokri*, Jafar Shaffaf† and Reza Taleb‡

Department of Mathematical Sciences
Shahid Beheshti University
P. O. Box 19839-63113, Tehran, Iran
**k_shokri@sbu.ac.ir*
†*shaffaf@gmail.com*
‡*r_taleb@sbu.ac.ir*

Received 19 August 2018
Revised 11 December 2018
Accepted 18 December 2018
Published 23 January 2019

Motivated by Schur's result on computing the Galois groups of the exponential Taylor polynomials, this paper aims to compute the Galois groups of the Taylor polynomials of the elementary functions $1 + \log(1 - x)$ and $\cos x$. We first show that the Galois groups of the nth Taylor polynomials of $1 + \log(1 - x)$ are as large as possible, namely, S_n (full symmetric group) or A_n (alternating group), depending on the residue of the integer number n modulo 4. We then compute the Galois groups of the nth Taylor polynomials of $\cos(x)$ and show that these Galois groups essentially coincide with the Coexter groups of type B_n (or an index 2 subgroup of the corresponding Coexter group).

Keywords: Galois theory; Newton polygon; p-adic theory; discriminants.

Mathematics Subject Classification 2010: 11R32, 11F85, 11R29

1. Introduction

A famous result of David Hilbert asserts that there exist irreducible polynomials of every degree n over $\mathbb{Q}$ having the largest possible Galois group S_n. However, Hilbert's proof, based on his irreducibility theorem, is non-constructive. Schur [9] proved a constructive (and explicit) version of this result in 1930. He proved that the Galois group of the splitting field of the exponential Taylor polynomials

$$f_n(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!},$$

over $\mathbb{Q}$, is the alternating group A_n if n is a multiple of 4, and the full symmetric group S_n otherwise. Coleman [2] gave a different proof for this theorem in 1987

‡Corresponding author.

using the p-adic Newton polygon of the polynomial f_n, Bertrand's postulate and Jordan's theorem.

As a result, for any positive integer n with $4 \nmid n$, Schur constructed a polynomial of degree n with $n+1$ terms so that its Galois group is S_n. Here it is worth mentioning that in [5] for any n and s with $\gcd(n,(s-1)(s-2))=1$, a polynomial of degree n with s terms was constructed so that the corresponding Galois group is S_n (see, [5, Theorem 4.3]).

A natural question is that how the Galois groups of the Taylor polynomials of other elementary functions are similar to logarithm and trigonometric functions? The study of the corresponding Galois groups of these polynomials seems to be more complicated than the Taylor exponential polynomials for at least two reasons: first, unlike the exponential Taylor polynomials, there is no explicit formula for the discriminant of logarithm and trigonometric Taylor polynomials, and second, the p-adic Newton polygon of logarithm and trigonometric functions are not as easy as the exponential Taylor polynomials to study.

In this paper, we first focus on the Taylor polynomials of the logarithm function $1+\log(1-x)$, i.e.

$$f_n(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n},$$

and after showing the irreducibility, we prove that the Galois group of the splitting fields of $f_n(x)$ is either S_n or A_n. We then, working on the discriminants of the polynomials, we show that the corresponding Galois groups are exactly the full symmetric group S_n in the case n is of the form $4k, 4k+2, 4k+3$, and of the form $4k+1$, provided n is prime. The same method can compute the Galois groups of the Taylor polynomials of $1+\sin(x)$, i.e.

$$f_n(x) = 1 + x - \frac{x^3}{3!} + \cdots \pm \frac{x^{2n-1}}{(2n-1)!}.$$

Finally, we use a different argument to study the Galois groups G_n of the Taylor polynomials of the elementary function $\cos(x)$, i.e.

$$f_n(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots + (-1)^n \frac{x^{2n}}{(2n)!}.$$

In this case, we first compute the Galois groups $\tilde{G}_n$ of the polynomials

$$g_n(x) = 1 - \frac{x}{2!} + \frac{x^2}{4!} + \cdots + (-1)^n \frac{x^n}{(2n)!}$$

as S_n or A_n. Although we are not able to give an explicit formula for the discriminant of $g_n(x)$, we provide some sufficient conditions so that $\tilde{G}_n \simeq S_n$. We then prove that G_n is isomorphic to the semi-direct product $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$. In the end of this paper, we give a geometric picture of the Galois group G_n of the Taylor polynomial $f_n(x)$. After recalling the concept of special regular polytopes and their corresponding

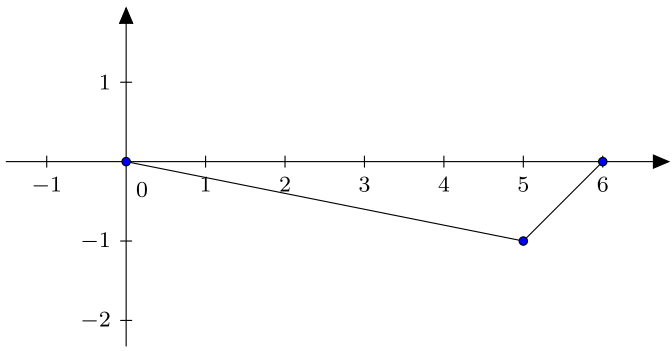


Fig. 1. The Newton polygon of $1 + x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \frac{x^5}{5} + \frac{x^6}{6} \in \mathbb{Q}_5[x]$.

Coexter groups, it is shown that G_n is indeed isomorphic to the symmetry group of a regular polytope, namely, cross-polytope which is a Coexter group of type B_n (or an index 2 subgroup).

2. Review of the Newton Polygons Over Local Fields

In this section, we briefly recall the main theorem on the Newton polygons of a polynomial $f(x)$ over the local fields, e.g., the p-adic field $\mathbb{Q}_p$ for a prime number p. For more details, one can consult [1, Chap. 4].

Theorem 2.1. *Let L be a local field with discrete valuation v_L, and let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in L[x]$ be a polynomial with $a_0a_n \neq 0$ whose Newton polygon is defined as the convex hull in $\mathbb{R}^2$ of the points*

$$(0, v_L(a_0)), \quad (1, v_L(a_1)), \ldots, (n, v_L(a_n)).$$

If one denotes the vertices of this polygon by the points $(x_0, y_0), (x_1, y_1), \ldots, (x_\ell, y_\ell)$, then $f(x)$ factors over L as

$$f(x) = f_1(x) \cdots f_\ell(x),$$

in which for any $1 \leq i \leq n$, the degree of $f_i(x)$ is $x_i - x_{i-1}$ and all roots of $f_i(x)$ in $\bar{L}$ have valuations $-\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$.

Corollary 2.2. *With the above notations, assume that $f_i(x) \in \mathbb{Q}_p[x]$ is irreducible. If d divides $x_i - x_{i-1}$ for some $1 \leq i \leq \ell$, then the order of the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$ is a multiple of d.*

Proof. Take a root $\alpha \in \bar{\mathbb{Q}}_p$ of the irreducible polynomial $f_i(x) \in \mathbb{Q}_p[x]$. Then

$$[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \deg(f_i(x)) = x_i - x_{i-1}$$

(see Theorem 2.1 for the second equality) divides the order of the Galois group of the splitting field of $f_i(x)$ (and hence $f(x)$) over $\mathbb{Q}_p$. To complete the proof, it is

enough to note that the Galois group of the splitting field of $f(x) \in \mathbb{Q}_p[x]$ over $\mathbb{Q}_p$ is embedded in the Galois group of the splitting field of $f(x) \in \mathbb{Q}[x]$ over $\mathbb{Q}$. □

3. Galois Groups of the Taylor Polynomials of $1 + \log(1 - x)$

In this section, we study the Galois groups G_n of the splitting fields of the Taylor polynomials

$$f_n(x) := 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n}$$

of the function $1 + \log(1 - x)$ for integers $n \geq 12$ over $\mathbb{Q}$. We first show that f_n is irreducible for any integer $n \geq 12$.

To show the irreducibility of $f_n(x) \in \mathbb{Q}[x]$ for any $n \geq 12$, we first choose a prime number p strictly between $n/2$ and n using Chebyshev theorem, and consider the polynomial f_n in $\mathbb{Q}_p[x]$. Then the Newton polygon of $f_n(x)$ has only three vertices $(0, 0), (p, -1), (n, 0)$ and therefore using Theorem 2.1, f_n factors in $\mathbb{Q}_p[x]$ as

$$f_n(x) = g_n(x)h_n(x),$$

in which g_n is a polynomial of degree p with roots of valuations $1/p$. As a result, $g_n(x) \in \mathbb{Q}_p[x]$ is an irreducible factor of $f_n(x) \in \mathbb{Q}_p[x]$. Repeating the same argument for another prime $q \neq p$ between $n/2$ and n, the polynomial $f_n(x) \in \mathbb{Q}_q[x]$ has an irreducible factor of degree q. We note that since $n \geq 12$, there are at least two primes between n and $n/2$. Now assuming that the degree n polynomial $f_n(x) \in \mathbb{Q}[x]$ is reducible, it must have two irreducible factors of degree $p > n/2$ and $q > n/2$ which is a contradiction.

Irreducibility of $f_n(x)$ implies that G_n is a transitive subgroup of S_n. On the other hand, using Corollary 2.2, p divides the order of the group G_n and so G_n has a p-cycle for the prime p between $n/2$ and n. Hence by Jordan's Theorem (see [4, Theorem 3.3]), G_n contains the alternating group A_n.

In the rest of this section, we show that in the case $n \not\equiv 1 \pmod 4$ and also in the case $n \equiv 1 \pmod 4$ provided that n is prime, the discriminant of $f_n(x)$ is not a perfect square and hence G_n is the full symmetric group S_n. We recall that if the Galois group of a polynomial of degree n is contained in the alternating group A_n if and only if the discriminant of that polynomial is a perfect square (see [6, Corollary 12.4]).

Observing that derivative function of $f_n(x)$ is $f_n'(x) = \frac{x^n - 1}{x - 1}$, the minimum of $f_n(x)$ occurs at $x = -1$ with a positive value for any even integer n. Thus $f_n(x)$ has no real roots for even integers n. Therefore in the case $n = 4k + 2$, the sign of the discriminant of $f_n(x)$ is $(-1)^t = (-1)^{2k+1} = -1$. For odd integers n, the derivative $f_n'(x)$ is always strictly greater than 1, and hence it has exactly one real root. Therefore in the case $n = 4k + 3$, the sign of the discriminant of $f_n'(x)$ is again $(-1)^t = (-1)^{2k+1} = -1$. From this, we conclude that the discriminant of the polynomial $f_n(x)$ is not a perfect square for any positive integer n of the form $n = 4k + 2, 4k + 3$, and the Galois group G_n is the full symmetric group S_n.

In the case $n = 4k$, we first note that the discriminant of $f_n(x)$ is

$$\begin{aligned}\operatorname{disc}(f_n) &= n^n(1/n)^{n-1}\prod_{i=1}^{n} f(\zeta_i)\\ &= n^n(1/n)^{n-1}\prod_{i=1}^{n}\left(1+\frac{\zeta_i}{1}+\frac{\zeta_i^2}{2}+\cdots+\frac{\zeta_i^n}{n}\right)\\ &= n\left(1+\sum_{1\le r_1,\ldots,r_{n-1}\le n-1}\frac{\zeta_1^{r_1}\cdots\zeta_{n-1}^{r_{n-1}}}{r_1\cdots r_{n-1}}\right),\end{aligned}$$

where the $(n-1)$th roots of unities $\zeta_i \neq 1$ are the roots of the derivative $f_n'(x)$. We now separate this summation into two parts: let the terms for which $r_1 = r_2 = \cdots = r_{n-1}$, i.e.

$$n\cdot\left(\frac{1}{n^{n-1}}+\frac{1}{(n-1)^{n-1}}+\cdots+\frac{1}{2^{n-1}}\right),$$

in one part, and the terms

$$n\left(1+\sum_{\substack{1\le r_1,\ldots,r_{n-1}\le n-1\\ \text{not all the same}}}\frac{\zeta_1^{r_1}\cdots\zeta_{n-1}^{r_{n-1}}}{r_1\cdots r_{n-1}}\right)$$

in the second part. Here we note that in

$$\sum_{\substack{1\le r_1,\ldots,r_{n-1}\le n-1\\ \text{not all the same}}}\frac{\zeta_1^{r_1}\cdots\zeta_{n-1}^{r_{n-1}}}{r_1\cdots r_{n-1}} = \sum_{\substack{1\le r_1,\ldots,r_{n-1}\le n-1\\ \text{not all the same}}}\frac{1}{r_1r_2\cdots r_{n-1}}\sum_{\sigma\in S_{n-1}}\zeta_{\sigma(1)}^{r_1}\cdots\zeta_{\sigma(n-1)}^{r_{n-1}},$$

the expression $\sum_{\sigma\in S_{n-1}}\zeta_{\sigma(1)}^{r_1}\cdots\zeta_{\sigma(n-1)}^{n-1}$ is symmetric, and thus is a rational number. Moreover, the p-valuations of all fractions in this summation are at most $n-2$.

Now taking the common denominator of all terms in these two parts leads to the fraction

$$n\cdot\frac{a+pb}{(\text{l.c.m.}(1,2,\ldots,n))^{n-1}},$$

in which $p \nmid a$. Hence the exact power of the prime p in this fraction is the odd number $n-1$, and so $\operatorname{disc}(f_n)$ is not a perfect square.

Finally, we show that if n is a prime number of the form $4k+1$, the discriminant of the polynomial $f_n(x)$ is not again a perfect square. By multiplying to n, we first make the polynomial f_n monic as

$$\tilde{f}_n(x) = n + nx + \frac{n}{2}x^2 + \cdots + \frac{n}{n-1}x^{n-1} + x^n$$

with derivative

$$\tilde{f}_n'(x) = n + nx + \cdots + nx^{n-1} + nx^n.$$

Therefore, we obtain the corresponding resultant as

$$\operatorname{Res}(\tilde{f}_n, \tilde{f}_n') = \det \begin{bmatrix} n & n & \frac{n}{2} & \dots & \frac{n}{n-1} & \boxed{1} & 0 & \cdots & 0 & 0 \\ 0 & n & n & \frac{n}{2} & \dots & \frac{n}{n-1} & \boxed{1} & 0 & \cdots & 0 \\ \vdots & & & & \vdots & & & & & \\ 0 & 0 & \cdots 0 & 0 & n & n & \frac{n}{2} & \cdots & \frac{n}{n-1} & \boxed{1} \\ \boxed{n} & n & \cdots & n & n & 0 & 0 & \cdots & 0 & 0 \\ 0 & \boxed{n} & \cdots & n & n & n & 0 & 0 & \cdots & 0 \\ \vdots & & & & \vdots & & & & & \\ 0 & 0 & \cdots & 0 & \boxed{n} & n & n & n & \cdots & n \end{bmatrix}$$

whose n-valuation is exactly equal to n. Here we note that determinant of this $(2n-1)\times(2n-1)$ is the product of the diagonal entries. All entries are multiples of n except the entries one in the partial diagonal. Hence in the product of the diagonal entries, all terms are multiples of n^{n+1} except one term, obtained from the diagonal including entries one, of n-valuation equal to n. Hence $\operatorname{val}_n(\operatorname{Res}(\tilde{f}_n, \tilde{f}_n')) = n$ which is an odd number. Since the $\tilde{f}_n$ is monic, we have the equality

$$\operatorname{disc}(\tilde{f}_n) = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(\tilde{f}_n, \tilde{f}_n'),$$

and the n-valuation of the discriminant of $\tilde{f}_n$ is the odd integer n. This implies that the discriminant of f_n, whose valuation is the same as $\tilde{f}_n$ up to a square, is not again a perfect square.

We summarize these results in the following theorem.

Theorem 3.1. *The Galois group of the splitting field of the polynomial*

$$f_n(x) := 1 + x + \frac{x}{2} + \cdots + \frac{x^n}{n}$$

is the full symmetric group S_n for any positive integer $n \geq 12$ with $n \not\equiv 1 \pmod 4$ and for any positive prime number $n \geq 12$ with $n \equiv 1 \pmod 4$.

4. Galois Groups of the Taylor Polynomials of cos(x)

In this section, we study the Galois groups G_n of the polynomials

$$f_n(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots + (-1)^n \frac{x^{2n}}{(2n)!}$$

for all $n \in \mathbb{Z} > 0$. To do that, we first compute the Galois groups $\tilde{G}_n$ of the polynomials

$$g_n(x) = 1 - \frac{x}{2!} + \frac{x^2}{4!} + \cdots + (-1)^n \frac{x^n}{(2n)!}$$

for all $n \in \mathbb{Z} > 0$, and then the Galois group G_n in the first part. In the second part, we provide a geometric interpretation of the Galois group G_n as the symmetry group of a regular polytope.

The computation of the Galois groups of the cosine Taylor polynomials, using the corresponding Newton polygon, is quite different from the exponential and the logarithm Taylor polynomials. The reason is as follows: unlike the exponential and logarithm cases, the first place that any prime p between $n/2$ and n appears in the coefficients of the cosine Taylor polynomials $f_n(x)$ is the term $\frac{x^{p+1}}{(p+1)!}$ which gives the slope $\frac{1}{p+1}$. So, we cannot conclude that p divides the denominator of the slope, and that the Galois group has a cycle of length p. Therefore, we have to use a different argument in this section.

4.1. *Computing the Galois groups $\tilde{G}_n$ and G_n*

By a classical result of Schur [8] in 1929, any polynomial of the form

$$1 + c_1 x + c_2 \frac{x^2}{2!} + \cdots + c_{\ell-1} \frac{x^{\ell-1}}{(\ell-1)!} \pm \frac{x^\ell}{\ell!} \in \mathbb{Q}[x]$$

with $c_i \in \mathbb{Z}$ is irreducible. Hence, as a corollary, the polynomial $f_n(x)$ and so the polynomial $g_n(x)$ are irreducible in $\mathbb{Q}[x]$.

Let $n \neq 3, 5, 11$ be a positive integer, and choose a prime p with $2n/3 < p < n$ (by consequence of prime number theorem). Then all places that p appears in the coefficients of the polynomial $f_n(x)$ are the coefficients $\pm\frac{1}{(p+j)!}$ for $0 < j < p$ with valuations -1, and in $\pm\frac{1}{(2p+j)!}$ for $0 \leq j \leq 2n-2p$ with valuations -2. Here we note that $2p < 2n$ and $2n < 3p$. Comparing the slopes of lines from $(0, 0)$ to $(\frac{p+1}{2}, -1)$

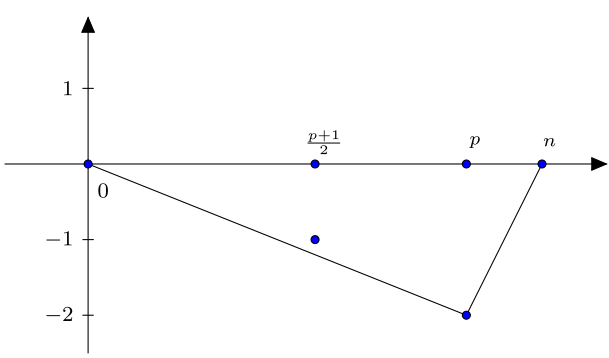


Fig. 2. The Newton polygon of $g_n(x) \in \mathbb{Q}_p[x]$.

and to $(p,-2)$, the slope of the first segment of the Newton polygon of $f_n(x)$ is obtained as $\frac{-2}{p}$ by connecting $(0,0)$ to $(p,-2)$. Therefore using Corollary 2.2 and again Jordan's theorem, the Galois group of the splitting field of $g_n(x)$ over $\mathbb{Q}$ is of order divisible by p and, since $n/2 < p$, has a cycle of length p. On the other hand, by irreducibility of $g_n(x)$, the corresponding Galois group is transitive. Hence assuming $n \neq 3, 5, 11$, the Galois group $\tilde{G}_n$ is the full symmetric group S_n or the alternating group A_n.

In exceptional cases $n = 3, 5, 11$, the Galois group $\tilde{G}_n$ is also isomorphic to either S_n or A_n. For $n = 11$, in the polynomial $g_{11}(x)$, the prime 7 appears only in the terms $\frac{x^4}{8!}$, $\frac{x^7}{14!}$ and $\frac{x^{11}}{22!}$. So the first segment in the 7-adic Newton polygon of $g_{11}(x)$ is $\frac{-2}{7}$. Again, since 7 divides the denominator of this slope, the order of the Galois group $\tilde{G}_7$ is divisible by 7, and consequently $\tilde{G}_n$ has a cycle of length 7 by Corollary 2.2. Therefore, since $7 > 11/2$ by Jordan's theorem, $\tilde{G}_n$ is isomorphic to S_n or A_n. In the cases $n = 3$ and $n = 5$, using the software PARI/GP, the discriminants have the prime factors 7 and 37 with exponents one, respectively. Moreover, $g_3(x)$ and $g_5(x)$ have the double roots 2 modulo 7 and 12 modulo 37, respectively. Therefore, by [7, Lemma 1], the groups $\tilde{G}_3$ and $\tilde{G}_7$ are generated by transpositions, and since these groups are transitive, they are isomorphic to S_3 and S_5, respectively. Consequently, $\tilde{G}_n$ is isomorphic to S_n or A_n for any positive integer n. At the end of this section, we give some sufficient conditions so that $\tilde{G}_n \simeq S_n$.

Now to relate the Galois group $\tilde{G}_n$ to G_n, let $\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2$ be the roots of $f_n(x)$. So $\mathbb{Q}(\alpha_1^2, \ldots, \alpha_n^2)$ is the splitting field of the polynomial $f_n(x)$, and $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is the splitting field of the polynomial $g_n(x)$. Let us consider the following Galois extensions:

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2) \subseteq \mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2) \subseteq \cdots \subseteq \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2) \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_n).$$

For simplicity, we use the following notations:

$$F := \mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2), \quad E := \mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2).$$

The strategy is as follows: we first show that the Galois group $\mathrm{Gal}(E/F)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and then similarly

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)) \simeq \mathbb{Z}/2\mathbb{Z},$$

and so on. As a result, the Galois group of the extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)$, which is indeed a 2-group, is obtained as follows:

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)) \simeq (\mathbb{Z}/2\mathbb{Z})^n.$$

We then conclude that $G_n \simeq (\mathbb{Z}/2\mathbb{Z})^n \rtimes \tilde{G}_n$, in which G_n is either the full symmetric group S_n or the alternating group A_n.

To complete the proof, by contrast, assume that $F = E$, and write α_1 as follows:

$$\alpha_1 = c_0(\alpha_2^2, \ldots, \alpha_n^2) + c_1(\alpha_2^2, \ldots, \alpha_n^2)\alpha_1^2 + \cdots + c_{n-1}(\alpha_2^2, \ldots, \alpha_n^2)\alpha_1^{2n-2}. \quad (4.1)$$

Here $c_i(\alpha_2^2, \ldots, \alpha_n^2) \in \mathbb{Q}(\alpha_2^2, \ldots, \alpha_n^2)$. For the rest of the proof, denote

$$T_{12} := \{\sigma \in \mathrm{Gal}(E/\mathbb{Q}); \sigma(\alpha_1^2) = \alpha_2^2\} \subseteq \mathrm{Gal}(E/\mathbb{Q}).$$

We take the action of all $\sigma \in T_{12}$ on both sides of the equality 4.1, and finally sum up both sides of equalities:

$$\sum_{\sigma \in T_{12}} \sigma(\alpha_1) = \sum_{\sigma \in T_{12}} c_0(\alpha_2^2, \ldots, \alpha_n^2) + \sum_{\sigma \in T_{12}} \sigma(c_1(\alpha_2^2, \ldots, \alpha_n^2))\alpha_2^2$$

$$+ \cdots + \sum_{\sigma \in T_{12}} \sigma(c_{n-1}(\alpha_2^2, \ldots, \alpha_n^2))\alpha_2^{2n-2}.$$

We note that $\sigma(\alpha_1) = \pm\alpha_2$, and therefore

$$\sum_{\sigma \in T_{12}} \sigma(\alpha_1) = m\alpha_2$$

for some integer m. On the other hand, we claim that the sum

$$\sum_{\sigma \in T_{12}} \sigma(c_i(\alpha_2^2, \ldots, \alpha_n^2))$$

is in the field $\mathbb{Q}(\alpha_2^2)$. To see this, we observe for any

$$\tau \in \mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_2^2))$$

that $\tau \circ \sigma(\alpha_1^2) = \alpha_2^2$, and so

$$\begin{aligned}\tau\left(\sum_{\sigma \in T_{12}} \sigma(c_i(\alpha_2^2, \ldots, \alpha_n^2))\right) &= \sum_{\sigma \in T_{12}} (\tau \circ \sigma)(c_i(\alpha_2^2, \ldots, \alpha_n^2)) \\ &= \sum_{\tau\circ\sigma \in T_{12}} \sigma(c_i(\alpha_2^2, \ldots, \alpha_n^2)) \\ &= \sum_{\sigma \in T_{12}} \sigma(c_i(\alpha_2^2, \ldots, \alpha_n^2)).\end{aligned}$$

Hence, $\sum_{\sigma \in T_{12}} \sigma(c_i(\alpha_2^2, \ldots, \alpha_n^2))$ is in the fixed field of the subgroup

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_2^2)) \leq \mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)/\mathbb{Q})$$

for any $0 \leq i \leq n-1$. Here we remark that the extension

$$\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2) = \mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)$$

is Galois over $\mathbb{Q}$. Thus we obtain the following equality:

$$m\alpha_2 = d_0 + d_1\alpha_2^2 + \cdots + d_{n-1}\alpha_2^{2n-2}$$

for $d_i \in \mathbb{Q}$. Since the polynomial $g_n(x) \in \mathbb{Q}(x)$ is irreducible and so the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)/\mathbb{Q})$$

is transitive, applying an element of this Galois group which maps 2 to j on the above equality, we obtain

$$m\alpha_j = d_0 + d_1\alpha_j^2 + \cdots + d_{n-1}\alpha_j^{2n-2}$$

for all $0 \leq j \leq n-1$. Then multiplying all these equalities for $0 \leq j \leq n-1$ leads to the following:

$$m^{n-1}\alpha_1 \cdots \alpha_n = \prod_{0\leq j\leq n-1} (d_0 + d_1\alpha_j^2 + \cdots + d_{n-1}\alpha_j^{2n-2}). \tag{4.2}$$

Now the right-hand side of equality 4.2 is a symmetric function in terms of the roots $\alpha_1^2, \ldots, \alpha_n^2$ of $g_n(x) \in \mathbb{Q}[x]$, and consequently is a rational number. This contradicts with the irrationality of the left-hand side of equality 4.2, i.e. the irrationality of $m^{n-1}\sqrt{(2n)!}$, unless $m = 0$. As a result, m should be zero, and so

$$\sum_{\sigma\in T_{12}} \sigma(\alpha_1) = 0.$$

This means that

$$\#\{\sigma \in T_{12}; \sigma(\alpha_1) = \alpha_2\} = \#\{\sigma \in T_{12}; \sigma(\alpha_1) = -\alpha_2\}. \tag{4.3}$$

Hence for any $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ which maps α_1^2 to α_2^2, there are two lifts τ_1 (sending α_1 to α_2) and τ_2 (sending α_1 to $-\alpha_2$) in $\mathrm{Gal}(E/\mathbb{Q})$. This is a contradiction with the equality $F = E$. Therefore

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)) \simeq \mathbb{Z}/2\mathbb{Z}. \tag{4.4}$$

In the next step, we claim that

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Otherwise, $\alpha_2 \in \mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)$ which implies the equality

$$\alpha_2 = c_0(\alpha_1^2, \ldots, \alpha_n^2) + c_1(\alpha_1^2, \ldots, \alpha_n^2)\alpha_1 \tag{4.5}$$

for some $c_i(\alpha_1^2, \ldots, \alpha_n^2) \in \mathbb{Q}(\alpha_1^2, \ldots, \alpha_n^2)$. The element

$$\tau = (\alpha_1^2, \alpha_2^2)(\alpha_3^2, \alpha_4^2) \in \mathrm{Gal}(F/\mathbb{Q})$$

has the following possible lifts in $\mathrm{Gal}(E/\mathbb{Q})$:

$$\begin{aligned} &(\alpha_1, \alpha_2)(\alpha_3^2, \alpha_4^2), \qquad (\alpha_1, \alpha_2, -\alpha_1, -\alpha_2)(\alpha_3^2, \alpha_4^2), \\ &(\alpha_1, -\alpha_2)(\alpha_3^2, \alpha_4^2), \quad (\alpha_1, -\alpha_2, -\alpha_1, \alpha_2)(\alpha_3^2, \alpha_4^2). \end{aligned} \tag{4.6}$$

Among these lifts, two lifts certainly occur in $\mathrm{Gal}(E/\mathbb{Q})$ by isomorphism 4.4. But applying any two lifts among all possible cases in 4.6 on the both sides of equality 4.5 implies that $\alpha_1 = 0$, $\alpha_1 \in \mathbb{Q}(\alpha_1^2, \ldots, \alpha_n^2)$ or $c_0(\alpha_1^2, \ldots, \alpha_n^2) = 0$. The first two cases are obviously contradictions. In the latter case,

$$\alpha_2 = c_1(\alpha_1^2, \ldots, \alpha_n^2)\alpha_1$$

implies that $\alpha_1\alpha_2 \in \mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)$, and more generally by the transitivity of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$, $\alpha_i\alpha_j \in \mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)$ for any $1 \le i, j \le n$. As a result, the symmetric polynomial

$$\sum_{i,j} \alpha_i\alpha_j \in \mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)$$

in terms of α_i's is indeed a symmetric polynomial in terms of α_i^2's. Consequently, it is fixed by all elements of the Galois group of the Galois extension $\mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)/\mathbb{Q}$, and thus $\sum_{i,j} \alpha_i\alpha_j \in \mathbb{Q}$. Equivalently, since $\sum_i \alpha_i^2 \in \mathbb{Q}$, we obtain that $(\sum_i \alpha_i)^2 \in \mathbb{Q}$. One can extend this argument simply to obtain $(\sum_{i,j,k} \alpha_i\alpha_j\alpha_k)^2 \in \mathbb{Q}$, and so on. To summarize what we have obtained is that $(\sum_{i_1,\ldots,i_l} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_m})^2 \in \mathbb{Q}$ for any odd integer m, and $\sum_{i_1,\ldots,i_l} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_m} \in \mathbb{Q}$ for any even integer m. As a result, we have the decomposition

$$f(x) = \left(\prod_{1\le i\le n} (x - \alpha_i)\right)\left(\prod_{1\le i\le n} (x + \alpha_i)\right),$$

where $\prod_i (x - \alpha_i), \prod_i (x + \alpha_i) \in K[x]$, where $K := \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_s})$ for some $d_i \in \mathbb{Z}$ and $s \le n/2$. So to obtain a contradiction, it is enough to show that $f(x)$ is irreducible in the number field K. To show that, we look at this polynomial in the local field $K_{\mathfrak{P}}$ for a prime ideal $\mathfrak{P}$ in the ring of integers K above a prime number $2n/3 < p < n$. The first segment of the Newton polygon of $f(x) \in K_{\mathfrak{P}}[x]$ connects $(0, 0)$ to $(2p, -2^r)$ for certain positive integer $r \le s$. Here we note that $K/\mathbb{Q}$ is Galois, and so the ramification index is a divisor of $[K : \mathbb{Q}] = 2^s$. Thus $f(x) \in K_{\mathfrak{P}}[x]$ has a factor of degree $2p$ with roots of $\mathfrak{P}$-valuations $\frac{2^t}{2p}$. Therefore, this factor is either irreducible or the product of two irreducible factors of degrees p. By substituting a prime ideal $\mathfrak{P}'$ lying above another prime number $2n/3 < p' < n$ provided n is large enough, e.g., $n \ge 30$, the same argument says that $f(x) \in K_{\mathfrak{P}'}[x]$ has an irreducible factor of degree $2p'$ or decomposes to the product of two irreducible factors of degrees p'. In any case if one assumes that $f(x) \in K[x]$ is reducible, we have a contradiction. Therefore

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_1, \alpha_2^2, \ldots, \alpha_n^2)) \simeq \mathbb{Z}/2\mathbb{Z}.$$

In the third step to show that

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2))$$

is of order 2, we assume again the contrary. So one can write the equality

$$\alpha_3 = c_0(\alpha_1^2, \ldots, \alpha_n^2) + c_1(\alpha_1^2, \ldots, \alpha_n^2)\alpha_1 + c_2(\alpha_1^2, \ldots, \alpha_n^2)\alpha_2 + c_3(\alpha_1^2, \ldots, \alpha_n^2)\alpha_1\alpha_2.$$

Since so far we obtain that the Galois group of $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2)$ over $\mathbb{Q}(\alpha_1^2, \alpha_2^2, \alpha_3^2, \ldots, \alpha_n^2)$ is of order 4, the element

$$\tau = (\alpha_1^2, \alpha_2^2, \alpha_3^2) \in \mathrm{Gal}(\mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)/\mathbb{Q})$$

has four lifts among all possible cases — similar to 4.6 — in the Galois group of $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2)$ over $\mathbb{Q}(\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2)$. By applying any two lifts among them, we get a simple contradiction or we come up with the case

$$\alpha_1 = c_0(\alpha_1^2, \ldots, \alpha_n^2) + c_1(\alpha_1^2, \ldots, \alpha_n^2)\alpha_2 + c_2(\alpha_1^2, \ldots, \alpha_n^2)\alpha_3 + c_3(\alpha_1^2, \ldots, \alpha_n^2)\alpha_2\alpha_3,$$

$$-\alpha_1 = c_0(\alpha_1^2, \ldots, \alpha_n^2) + c_1(\alpha_1^2, \ldots, \alpha_n^2)\alpha_2 + c_2(\alpha_1^2, \ldots, \alpha_n^2)\alpha_3 + c_3(\alpha_1^2, \ldots, \alpha_n^2)\alpha_2\alpha_3,$$

which imply $\alpha_1 = 0$. This is again a contradiction. As a result, we have the following isomorphism:

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4^2, \ldots, \alpha_n^2)/\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3^2, \ldots, \alpha_n^2)) \simeq \mathbb{Z}/2\mathbb{Z}.$$

By induction and repeating the same argument as in the third step, we finally derive the structure of the 2-group $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}(\alpha_1^2, \ldots, \alpha_n^2))$ as follows:

$$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}(\alpha_1^2, \ldots, \alpha_n^2)) \simeq (\mathbb{Z}/2\mathbb{Z})^n.$$

Here we note that this group, as the Galois group of a Galois extension, is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q})$.

We can now write the following exact sequence:

$$0 \to (\mathbb{Z}/2\mathbb{Z})^n \to G_n \to \tilde{G}_n \to 0$$

with the splitting map $\tilde{G}_n \to G_n$ sending any permutation $\alpha_i^2 \to \alpha_j^2$ simply to the permutation $\alpha_i \to \alpha_j$. On the other hand, we showed that the Galois group $\tilde{G}_n = \mathrm{Gal}(\mathbb{Q}(\alpha_1^2, \ldots, \alpha_n^2)/\mathbb{Q})$ is S_n or A_n. Therefore, we conclude that G_n is the semi-direct product of the normal subgroup $(\mathbb{Z}/2\mathbb{Z})^n$ and $\tilde{G}_n$, and the action of $\tilde{G}_n$ on $(\mathbb{Z}/2\mathbb{Z})^n$ is just permutations of direct factors. We summarize these results in the following theorem.

Theorem 4.1. *The Galois group of the splitting field of the polynomial*

$$f_n(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots + (-1)^n \frac{x^{2n}}{(2n)!}$$

over $\mathbb{Q}$ *is the group* $H \rtimes \tilde{G}_n$ *with the prescribed action for any* $n \in \mathbb{Z} > 0$ *in which* $H \simeq (\mathbb{Z}/2\mathbb{Z})^t$ *for* $t \leq n$*, and* $\tilde{G}_n$ *— the Galois group of the splitting field of the polynomial*

$$g_n(x) = 1 - \frac{x}{2!} + \frac{x^2}{4!} + \cdots + (-1)^n \frac{x^n}{(2n)!}$$

over $\mathbb{Q}$ *— is either the full symmetric group* S_n *or the alternating group* A_n*. For large enough positive integers* n*, e.g.,* $n \geq 30$*, we have* $H \simeq (\mathbb{Z}/2\mathbb{Z})^n$*.*

Although we are not able to give an explicit formula for $\mathrm{disc}(g_n)$, we provide some conditions so that $\tilde{G}_n$ is the full symmetric group S_n in the last part of this section. To do that, we remark that if $\mathrm{disc}(g_n)$ is a perfect square, then $\mathrm{disc}(g_n)$ is

a perfect square modulo any prime number p. Now choose a prime number $p \neq 3$ such that $p \,|\, 2n-4$, and multiply g_n by $(2n)!$ to obtain the monic polynomial

$$\frac{1}{(2n)!} + \frac{x}{(2n-2)!} + \frac{x^2}{(2n-1)!} + \cdots + x^n.$$

This polynomial is congruent to $1 + 12x + 24x^2$ modulo the prime p, and has the discriminant

$$\operatorname{disc}(g_n) \equiv 3 \pmod{p}$$

modulo p. This implies that the discriminant $\operatorname{disc}(g_n)$ is not a perfect square provided that the Legender symbol $(\frac{3}{p})$ is -1, equivalently $p \equiv \pm 5 \pmod{12}$. For example, we note that if $n \equiv 7, 9 \pmod{12}$, the number $2n-4$ has a prime factor p with $p \equiv \pm 5 \pmod{12}$.

Similarly, choosing a prime number $p \neq 2$ such that $p \,|\, 2n-5$, the polynomial $g_n(x)$ is of the form $1 - 20x + 120x^2$ modulo p with discriminant -20. Therefore, $\operatorname{disc}(g_n)$ is not again a perfect square provided that the Legender symbol $(\frac{-5}{p})$ is -1, equivalently $p \equiv 11, 13, 17, 19 \pmod{20}$. Thus we have the following proposition.

Proposition 4.2.

(1) *If n is a positive number of the form $12k+7$ or $12k+9$, then $\tilde{G}_n \simeq S_n$.*
(2) *If n is a positive integer which has a prime factor p with $p \equiv 11, 13, 17, 19 \pmod{20}$, then $\tilde{G}_n \simeq S_n$.*

Remark 4.3. The methods we used for computing the Galois groups of the logarithm and cosine Taylor polynomials apply to the Taylor polynomials of the function $1 + \sin(x)$. But these methods do not work for the Tangent and Cotangent Taylor polynomials whose coefficients are related to Bernoulli numbers. To explain it, we consider the Taylor polynomials

$$\sum_{k=0}^{n} (-1)^k \frac{B_{2k}}{(2k)!} (2x)^{2k}$$

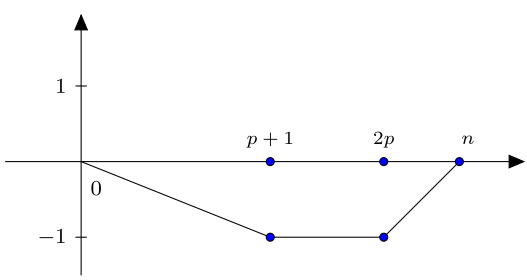


Fig. 3. The Newton polygon of the Taylor polynomials of $x \cdot \cot(x) \in \mathbb{Q}_p[x]$.

of the function $x \cdot \cot(x)$. Here we note that, since for any prime p

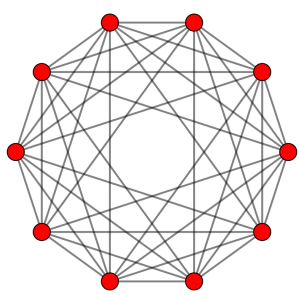
$$\frac{B_{2p}}{2p} \equiv \frac{B_{p+1}}{p+1} \equiv \frac{B_2}{2} \pmod{p},$$

according to the Kummer criterion for Bernouli numbers, the first vertices of the corresponding Newton polygon are $(0,0),(p+1,-1),(2p,-1)$. Since the prime p does not appear in the slopes of the connecting lines, the methods used in the previous sections do not work!

4.2. *Galois group G_n as the symmetry group of a regular polytope*

To understand the structure of the Galois group G_n of the nth Taylor polynomial of the elementary function $\cos x$, we try to relate it to a well-known symmetry group of a finite convex object in n-dimensional space called cross-polytope.

We recall that an n-simplex α_n (we use Coexter notation, see [3]) is defined as the convex hull of the origin $O = (0,\ldots,0)$ and all n points are fixed on the n coordinate axes in $\mathbb{R}^n$. If the n points on the coordinate axes are equidistant from the origin O, it is called a regular n-simplex. If we choose $2n$ points on the coordinate axes equidistant from the origin O in both directions, the convex hull of the origin O and these $2n$ points are another important figure, the cross-polytope β_n, whose facets consist of 2^n regular simplex α_{n-1}. To see it more visually, you can take $(\pm1,0,\ldots,0),\ldots,(0,\ldots,\pm1)$ in $\mathbb{R}^n$ as $2n$ vertices and the corresponding convex hull in $\mathbb{R}^n$ is the cross-polytope. The Schlafli symbol of this regular cross-polytope is $\{3,3,\ldots,3,4\}$, or say, $\beta_n = \{3^{n-2},4\}$, also $\alpha_n = \{3^{n-1}\}$ (for the definition of Schlafli symbol, see [3] or the references therein). For example, the cross-polytope in $\mathbb{R}^2$ is the square with vertices $(\pm1,0),(0,\pm1)$ with symbol $\{4\}$, and in $\mathbb{R}^3$, it is an octahedron with symbol $\beta_3 = \{3,4\}$, i.e. all faces are triangles and around each vertex, there are 4 triangles (it is in fact one of the Platonic solids). The corresponding cross-polytope in $\mathbb{R}^5$ has 10 vertices $(\pm1,0,\ldots,0),\ldots,(0,\ldots,\pm1)$ and 40 edges and 80 triangle faces and 80 tetrahedron cells with the symbol $\{3^3,4\}$, and also its orthogonal projection on the xy-plane is the following figure:



If we are given the position of one facet and one vertex of a regular polytope in n-dimensional space, we can build up the whole polytope in a unique manner, i.e. there is a symmetry group which is transitive on facets and likewise transitive

on the vertices. In particular, the symmetry group of the regular simplex α_{n-1} or $\{3^{n-1}\}$ is the full symmetric group S_n — group of all permutations of the n vertices of the simplex α_{n-1} — and the order of the symmetry group of a regular simplex is $N(\alpha_{n-1}) = n!$

Since the cross-polytope β_n or $\{3^{n-2}, 4\}$ has 2^n facets α_{n-1}, then one can show that the order of the symmetry group of the cross-polytope β_n is as follows:

$$N(\beta_n) = 2^n N(\alpha_{n-1}) = 2^n n! \tag{4.7}$$

In fact, it is known that the symmetry group of the cross-polytope β_n is just the symmetry group of the frame of the orthogonal Cartesian axes (see [3]). So, it consists of 2^n possible changes of signs of the n coordinate axes combined with the $n!$ permutations of the axes. As we observed before, we see that the Galois group of the nth Taylor polynomial g_n of the function $\cos x$ consists of possible changes of signs of the roots $\alpha_1, \ldots, \alpha_n$ and also it contains the permutations of these roots. Hence, we can clearly consider the Galois group G_n as a subgroup of the symmetry group $\mathrm{Sym}(\beta_n)$. By the above argument and also by the computation of the order of the Galois group of the Taylor polynomials of $\cos x$ (at least when this Galois group is as large as possible), both groups have the same order, and consequently,

$$G_n \simeq \mathrm{Sym}(\beta_n). \tag{4.8}$$

Finally, we note that the symmetry group of the cross-polytope β_n is a Coexter group of type B_n, and its structure is of the form $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$.

Acknowledgment

The authors would like to thank the referee for comments and corrections.

References

[1] J. W. S. Cassels, *Local Fields* (Cambridge University Press, 1986).
[2] R. Coleman, On the Galois groups of the exponential Taylor polynomials, *Enseign. Math.* **33** (1987) 183–189.
[3] H. S. M. Coxeter, *Regular Polytopes*, 3rd edition (Dover, New York, 1973).
[4] J. D. Dixon and B. Mortimer, *Permutation Groups* (Springer-Verlag, New York–Heidelberg–Berlin, 1996).
[5] K. Monsef Shokri, J. Shaffaf and R. Taleb, *Computing Galois groups of certain families of polynomials*, Acta Arith. **185** (2018) 357–365.
[6] P. Morandi, *Field and Galois Theory* (Springer, New York, 1996).
[7] H. Osada, The Galois groups of the polynomials $x^n + ax^s + b$, *J. Number Theory* **25** (1987) 230–238.
[8] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibiliätsfragen I, *Sitzungsberichte Preuss. Akad. Wiss. Phys.-Math. Klasse* **14** (1929) 125–136; *Gesammelte Abhandlungen, Band III*, 140151.
[9] I. Schur, Gleichungen ohne Affekt, *Gesammelte Abhandlungen, Band III* **67** (1929) 191–197.