Applied Mathematics and Computation 218 (2012) 7014–7022

Contents lists available at SciVerse ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

The minimal polynomial of $2\cos(\pi/q)$ and Dickson polynomials ☆

Abdelmejid Bayad [a], Ismail Naci Cangul [b,*]

[a] Université d'Evry Val d'Essonne, Département de Mathématiques, Bâtiment I.B.G.B.I., 3éme étage, 23 Bd. de France, 91037 Evry Cedex, France
[b] Uludag University, Faculty of Arts and Science, Department of Mathematics, Gorukle, 16059 Bursa, Turkey

ARTICLE INFO

Keywords:
Hecke groups
Minimal polynomials
Cyclotomic polynomials
Chebychev polynomials
Dickson polynomials
Möbius inversion

ABSTRACT

The number $\lambda_q = 2\cos(\pi/q),\ q \in \mathbb{N},\ q \geqslant 3$, appears in the study of Hecke groups which are Fuchsian groups, and in the study of regular polyhedra. There are many partial results about the minimal polynomial of this algebraic number. Here we obtain the general formula and it is Möbius inversion for this minimal polynomial by means of the Dickson polynomials and the Möbius inversion theory. Moreover, we investigate the homogeneous cyclotomic, Chebychev and Dickson polynomials in two variables and we show that our main results in one variable case nicely extend to this situation. In this paper, the deep results concerning these polynomials are proved by elementary arguments.

1. Introduction and motivation

Let $\zeta_q = e^{2\pi i/q}$ be a primitive qth root of unity. Then $\frac{\zeta_q+\zeta_q^{-1}}{2} = \cos\left(\frac{2\pi}{q}\right)$. Throughout this paper we denote the minimal polynomial of $\cos\left(\frac{2\pi}{q}\right)$ over $\mathbb{Q}$ by $\psi_q(x)$. Let $T_n(x)$ denote the nth Chebychev polynomial defined through the identity

$$T_n(\cos\theta) = \cos(n\theta).$$

The first few $T_n(x)$ polynomials are $T_0(x) = 1,\ T_1(x) = x,\ T_2(x) = 2x^2 - 1,\ T_3(x) = 4x^3 - 3x,\ T_4(x) = 8x^4 - 8x^2 + 1,\ T_5(x) = 16x^5 - 20x^3 + 5x$. It is well-known that $T_n(x)$ has degree n and the leading coefficient is 2^{n-1}. As $T_n(x)$ is not monic, we use the normalisation of it denoted by $D_n(x)$ called as the Dickson polynomial: $D_n(x) = 2T_n(x/2)$. Dickson polynomials are explicitly given in [9] by

$$D_n(x) = \sum_{i=0}^{[n/2]} (-1)^i \frac{n}{n-i} \binom{n-i}{i} x^{n-2i},$$

where $[n/2]$ denotes the greatest integer $\leqslant n/2$. Therefore the degree of $D_n(x)$ is n. The first few D_ns are $D_0(x) = 2$, $D_1(x) = x$, $D_2(x) = x^2 - 2$, $D_3(x) = x^3 - 3x$, $D_4(x) = x^4 - 4x^2 + 2$ and $D_5(x) = x^5 - 5x^3 + 5x$.

From the well-known decomposition identity

$$\cos(n\theta) = 2^{n-1} \prod_{k=1}^{n} (\cos(\theta) - \cos((k-1/2)\pi/n))$$

we have the factorisation of Dickson polynomials

☆ The second author is supported by the Commission of Scientific Research Projects of Uludag University, Project Nos. 2006/40, 2008/31 and 2008/54.
* Corresponding author.
E-mail addresses: abayad@maths.univ-evry.fr (A. Bayad), cangul@uludag.edu.tr (I.N. Cangul).

0096-3003/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.amc.2011.12.044

$$D_n(x) = \prod_{k=1}^{n}(x - 2\cos((k-1/2)\pi/n))$$

and these polynomials are a special case of the hypergeometric function ${}_2F_1(a,b;c;z)$ as

$$\frac{D_n(x)}{2} = {}_2F_1(-n, n; 1/2; 1/4(2-x)),$$

where ${}_2F_1(a,b;c;z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)}\int_0^1 \frac{t^{b-1}(1-t)^{c-b-1}}{(1-tz)^a}dt$, see [1].

Dickson polynomials have various properties and applications in a variety of areas. In particular, Dickson polynomials play a fundamental role in the theory of permutation polynomials over finite fields. For a prime power q, let $\mathbb{F}_q$ denote the finite field containing q elements. It is known that the Dickson polynomial $D_n(x)$ is a permutation polynomial on $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$. The real importance of Dickson polynomials in the theory of permutations comes from the Schur conjecture. In 1923, Schur conjectured in [8] that there are no other integral polynomials that permute the field $\mathbb{F}_q$ for infinitely many prime numbers other than compositions of power polynomials x^n, Dickson polynomials, and rational linear polynomials. This conjecture was proved by Fried [6].

There are many reasons for being interested in the minimal polynomials of the numbers $\lambda_q = 2\cos(\pi/q)$ for $q \geqslant 3,\ q \in \mathbb{N}$. First for all, we are motivated by the following phenomenon. In the formula of Dickson polynomials, if we put $\theta = \pi/q$, then

$$D_n(2\cos\pi/q) = 2\cos(n\pi/q) = \zeta_q^n + \zeta_q^{-n}.$$

It is well-known that the number λ_q is very important in the theory of Hecke groups. The group generated by $R(z) = -\frac{1}{z}$ and $S(z) = -\frac{1}{z+\lambda_q}$ is denoted by $H(\lambda_q)$ and is called the Hecke group. For $\lambda_q = 2\cos(\pi/q)$, $H(\lambda_q)$ is a finitely generated discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$, (the group of isometries of the upper half plane). For $q \geqslant 3$, the fundamental region for $H(\lambda_q)$ is given by

$$F_q = \{z \in \mathbb{C} : \Im(z) > 0, |\Re(z)| < \lambda_q/2, |z| > 1\}.$$

On the other hand, the numbers $\lambda_q = 2\cos(\pi/q)$ and $\alpha_q = \cos(2\pi/q)$ are special Gaussian periods. In mathematics Gaussian periods permit explicit calculations in cyclotomic fields connected with Galois theory and with discrete Fourier transform. Indeed, Gaussian periods are closely related to Gauss sums which are linear combinations of Gauss periods. They have many applications in Number theory, for instance in primality testing [7] and in the theory of compass and straightedge constructions. For all these interactions and for their consequences which ensue from it, it seems necessary to have a more complete study of the minimal polynomial of λ_q and $\alpha_q = \cos(2\pi/q)$. In this paper, we shall deal with these minimal polynomials. We denote by $P_q^*(x)$ and $\psi_q(x)$, the minimal polynomials of λ_q and $\alpha_q = \cos(2\pi/q)$, respectively.

The main aim of this paper is to obtain explicit formulas for $P_q^*(x)$ and $\psi_q(x)$ by means of Möbious inversion formula. So far in the literature, there are only some partial results on $P_q^*(x)$ if q is odd, see [3,2,10]. Here we obtain this polynomial both for odd and even q cases, covering all situations. Another reason is that we generalised the following theorem and we investigated its analogue by replacing ψ_q by P_q^*. In [5,10], two relations between $\psi_n(x)$ and $T_n(x)$ are given as follows:

Theorem 1 ([5,10]).

(1) *If $n = 2s+1$ is odd, then*

$$T_{s+1}(x) - T_s(x) = 2^s \prod_{d|n} \psi_d(x).$$

(2) *If $n = 2s$ is even, then*

$$T_{s+1}(x) - T_{s-1}(x) = 2^s \prod_{d|n} \psi_d(x).$$

Here we will give two relations between $P_q^*(x)$ and Dickson polynomials.

Note that the degree of the extension $\mathbb{Q}(\cos 2\pi/n)$ over $\mathbb{Q}$ is equal to the degree of the minimal polynomial of $\cos 2\pi/n$ over $\mathbb{Q}$. Note that

$$\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}(\cos 2\pi/n) \supseteq \mathbb{Q}$$

and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Also as ζ_n is a root of the quadratic polynomial

$$x^2 - 2\cos(2\pi/n)x + 1,$$

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos 2\pi/n)] = 1$ or 2. If $n \geqslant 3$, ζ_n is not real, then

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos 2\pi/n)] = 2.$$

Therefore the following holds

$$\deg \psi_n(x) = \begin{cases} 1 & \text{if } n = 1, 2, \\ \varphi(n)/2 & \text{if } n \geqslant 3. \end{cases}$$