HOMOGENEOUS POLYNOMIALS AND THE MINIMAL POLYNOMIAL OF COS(2π/n)

David Surowski and Paul McCombs

Abstract. It is well known that if $\Phi_n(x)$ is the nth cyclotomic polynomial, then there is a factorization $x^n - 1 = \prod \Phi_d(x)$, where the product is taken over the divisors d of n. Thus, one can obtain, by Möbius inversion, a product formula for each $\Phi_n(x)$ in terms of the various factors $x^d - 1$. The purpose of this note is two–fold. First, we show that the above factorization implies a similar factorization for the minimal polynomials of the algebraic numbers $\cos(2\pi/n)$, where n is a positive integer. Secondly, we give an explicit formula for the minimal polynomials of $\cos(2\pi/p)$, where p is prime.

Introduction. If $\zeta \in \mathbb{C}$ is the primitive nth root of unity $\zeta = e^{2\pi i/n}$, and if $\Phi_n(x)$ is the minimal polynomial of ζ, then it is well known that $\Phi_n(x)$ is a monic polynomial with integer coefficients, has degree $\phi(n)$ (Euler ϕ–function), and satisfies the identity

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{1}$$

From this, the cyclotomic polynomials can be computed via Möbius inversion:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}, \tag{2}$$

where for any integer k,

$$\mu(k) = \begin{cases} (-1)^l & \text{if } k \text{ factors into } l \text{ distinct primes,} \\ 0 & \text{if not.} \end{cases}$$

In [3], W. Watkins and J. Zeitlin show that if $\Psi_n(x)$ is the minimal polynomial of $\cos(2\pi/n)$, then in analogy with equation (1) one has identities of the form

$$T_{s+1}(x) - T_s(x) = 2^s \prod_{d|n} \Psi_d(x) \quad \text{if } n = 2s+1 \text{ is odd,} \tag{3}$$

$$T_{s+1}(x) - T_{s-1}(x) = 2^s \prod_{d|n} \Psi_d(x) \quad \text{if } n = 2s \text{ is even.} \tag{4}$$

In the above expressions, $T_s(x)$ is the sth Chebyshev polynomial, defined by setting $T_s(\cos\theta) = \cos s\theta$. Thus, one can, in principle, compute the polynomials $\Psi_n(x)$ using the Chebyshev polynomials and Möbius inversion.

In this note, we shall show first that equations (3) and (4) are not merely analogs of equation (1), they are consequences of it. In the last section, we shall give an explicit formula for the minimal polynomial of $\cos(2\pi/p)$, where p is prime. This seems not to have been given in the literature.

1. Homogeneous Polynomials and Specialization. If D is an integral domain and $f(x) \in D[x]$ is a polynomial of degree k, we shall denote by $f(x,y) \in D[x,y]$ the corresponding homogeneous polynomial, also of degree k. Thus, if $f(x) = \sum a_i x^i$, then $f(x,y) = \sum a_i x^i y^{k-i}$. Clearly, if $f(x), g(x) \in D[x]$, and if $h(x) = f(x)g(x)$, then $h(x,y) = f(x,y)g(x,y)$. This allows us to consider the homogeneous version of equation (1):

$$x^n - y^n = \prod_{d|n} \Phi_d(x,y). \tag{5}$$

Next, as the roots of $\Phi_n(x)$ consist of all of the primitive nth roots of unity, and since these are closed under taking inverses, we see that if $n > 1$, the polynomial is "palindromic" in the sense that if $k = \phi(n)$ and $\Phi_n(x) = \sum_{i=0}^{k} a_i x^i$, then $a_i = a_{k-i}$, $i = 0, 1, \ldots, k$. If $n > 2$, then $\phi(n)$ is even: $\phi(n) = 2s$, for some integer s. In this case we set

$$L_n(x,y) = \sum_{i=0}^{s} a_i(x^i + y^i)(\sqrt{xy})^{s-i} \in \mathbb{Z}[x, y, \sqrt{xy}].$$

Note that since the polynomials $x^i + y^i$ are symmetric in x and y, then by the Fundamental Theorem on Symmetric Polynomials (FTSP) [1], $x^i + y^i$ can be expressed as a polynomial in the "elementary symmetric polynomials" $\sigma_1 = x + y$ and $\sigma_2 = xy$. Therefore, each $L_n(x,y) \in \mathbb{Z}[\sigma_1, \sqrt{\sigma_2}]$, $L_n(x,y) = \Lambda_n(\sigma_1, \sqrt{\sigma_2})$, where $\Lambda_n(x,y) \in \mathbb{Z}[x,y]$.

Next, FTSP also says [1] that the polynomials are algebraically independent over $\mathbb{Z}$, from which it follows easily that σ_1 and $\sqrt{\sigma_2}$ are also algebraically independent. Therefore, if $R \supseteq \mathbb{Z}$ is any integral domain containing $\mathbb{Z}$, and if $r_1, r_2 \in R$ are arbitrary elements, then the evaluation $\sigma_1 \mapsto r_1$, $\sqrt{\sigma_2} \mapsto r_2$ determines a unique homomorphism $\mathbb{Z}[\sigma_1, \sqrt{\sigma_2}] \to R$, $f(\sigma_1, \sqrt{\sigma_2}) \mapsto f(r_1, r_2)$. Notice that if $n > 2$, and

$\phi(n) = 2s$, then $x^{-s}\Phi_n(x) = L_n(x, x^{-1}) = \Lambda_n(x + x^{-1}, 1)$. We now define the polynomials $\Theta_n(x) = \Lambda_n(x, 1)$. Clearly, $\Theta_n(x)$ is a monic polynomial of degree s having $2\cos(2\pi/n)$ as a root. Since it is a simple matter to show that the minimal polynomial of $2\cos(2\pi/n)$ must have degree s [2,3], one concludes that $\Theta_n(x)$ is the minimal polynomial of $2\cos(2\pi/n)$. From this, we see easily that if $\Psi_n(x)$ is the minimal polynomial of $\cos(2\pi/n)$, then we must have $\Psi_n(x) = 2^{-s}\Theta_n(2x)$.

Lemma 1.1. For each $n > 2$, $L_n(x, y) = \Phi_n(\sqrt{x}, \sqrt{y})$.

Proof. As $\Phi_n(\sqrt{x}, \sqrt{y}) = \prod(\sqrt{x} - \omega\sqrt{y})$, where the product is taken over the primitive nth roots of unity, and since $L_n(x, y)$, $\Phi_n(\sqrt{x}, \sqrt{y})$ have the same degree as polynomials in $\sqrt{x}$, $\sqrt{y}$, it suffices to prove that $L_n(\omega^2 y, y) = 0$ for any primitive nth root of unity. We have

$$L_n(\omega^2 y, y) = \sum_{i=0}^{s} a_i(\omega^{2i}y^i + y^i)(\omega y)^{s-i}$$

$$= y^s\omega^{-s}\sum_{i=0}^{s} a_i(\omega^i + \omega^{-i}) = 0.$$

Next, we set $L_1(x, y) = x + y - 2\sqrt{xy}$, $L_2(x, y) = x + y + 2\sqrt{xy}$. Thus, $L_1(x, y) = \Lambda_1(\sigma_1, \sqrt{\sigma_2}) := \sigma_1 - 2\sqrt{\sigma_2}$, $L_2(x, y) = \Lambda_2(\sigma_1, \sqrt{\sigma_2}) := \sigma_1 + 2\sqrt{\sigma_2}$, and $\Lambda_i(x, 1) = \Theta_i(x)$, $i = 1, 2$. Note also that $L_1(x, y)L_2(x, y) = (x - y)^2$.

Proposition 1.2. For any integer $n \geq 1$,

$$(x - y)(x^n - y^n) = \prod_{d|2n} L_d(x, y).$$

Proof. We have

$$x^n - y^n = \prod_{d|2n} \Phi_d(\sqrt{x}, \sqrt{y});$$

as $(x - y)\Phi_1(\sqrt{x}, \sqrt{y})\Phi_2(\sqrt{x}, \sqrt{y}) = (x - y)^2 = L_1(x, y)L_2(x, y)$, we may multiply both sides of the above equation by $(x - y)$ and apply Lemma 1.1 to obtain the result.

Theorem 1.3. With the notation as above, we have

$$x^{s+1}+y^{s+1}-\sqrt{xy}(x^s+y^s)=\prod_{d|n}L_d(x,y), \quad \text{if } n=2s+1 \text{ is odd},$$

$$x^{s+1}+y^{s+1}-\sqrt{xy}(x^{s-1}+y^{s-1})=\prod_{d|n}L_d(x,y), \quad \text{if } n=2s \text{ is even}.$$

Proof. Assume first that $n=2s+1$ is odd. Then

$$(x^{s+1}+y^{s+1}-\sqrt{xy}(x^s+y^s))(x^{s+1}+y^{s+1}+\sqrt{xy}(x^s+y^s))=(x-y)(x^n+y^n)$$

$$=\prod_{d|2n}L_d(x,y)$$

$$=\prod_{d|n}L_d(x,y)\prod_{d|n}L_{2d}(x,y).$$

Since the polynomials $L_d(x,y)$ are pairwise relatively prime in $\mathbb{Z}[\sqrt{x},\sqrt{y}]$, it suffices to show that $L_d(x,y)|(x^{s+1}+y^{s+1}-\sqrt{xy}(x^s+y^s))$ in $\mathbb{Z}[\sqrt{x},\sqrt{y}]$, whenever $d|n$. If $d|n$, $d\neq 1,2$, then $L_d(x,y)=\Phi_d(\sqrt{x},\sqrt{y})$ which has factors of the form $(\sqrt{x}-\omega\sqrt{y})$ where ω is a primitive dth root of unity. On the other hand, if we set $\sqrt{x}=\omega\sqrt{y}$ in $x^{s+1}+y^{s+1}-\sqrt{xy}(x^s+y^s)$, we obtain

$$\begin{aligned}\omega^{2s+2}y^{s+1}+y^{s+1}-\omega y(\omega^{2s}y^s+y^s)&=y^{s+1}(\omega^{2s+2}+1-\omega^{2s+1}-\omega)\\&=y^{s+1}(\omega^{n+1}+1-\omega^n-\omega)\\&=0;\end{aligned}$$

since $d|n$ implies that $\omega^n=1$. Finally, note that

$$x^{s+1}+y^{s+1}-\sqrt{xy}(x^s+y^s)=(\sqrt{x}-\sqrt{y})((\sqrt{x})^{2s+1}-(\sqrt{y})^{2s+1})$$

and so $L_1(x,y)=x+y-2\sqrt{xy}=(\sqrt{x}-\sqrt{y})^2$ divides $x^{s+1}+y^{s+1}-\sqrt{xy}(x^s+y^s)$, as well.

Next, assume that $n = 2s$ is even. As above, we assume that $d|n$ and that ω is a primitive dth root of unity. Setting $\sqrt{x} = \omega\sqrt{y}$ yields

$$x^{s+1} + y^{s+1} - \sqrt{xy}(x^{s-1} + y^{s-1}) = y^{s+1}(\omega^{2s+2} + 1 - \omega^{2s} - \omega^2) = 0.$$

This proves that if $d|n$, $L_d(x,y)|(x^{s+1} + y^{s+1} - \sqrt{xy}(x^{s-1} + y^{s-1}))$. Also, $L_1(x,y)L_2(x,y) = (x + y - 2\sqrt{xy})(x + y + 2\sqrt{xy}) = (x+y)^2 - 4xy = (x-y)^2$ and $x^{s+1} + y^{s+1} - \sqrt{xy}(x^{s-1} + y^{s-1}) = (x-y)(x^s - y^s)$ and hence, is divisible by $(x-y)^2$. Finally, the argument is concluded in both cases by observing that as a polynomial in $\mathbb{Z}[\sqrt{x}, \sqrt{y}]$, $\prod_{d|n} L_d(x,y)$ has degree $n+2$.

2. The Minimal Polynomial of $\mathbf{cos(2\pi/n)}$. To relate the work of Section 1 with that of Watkins and Zeitlin [3], we recall the definition of the Chebyshev polynomial $T_n(\cos\theta) = \cos n\theta$. Equivalently, if $\zeta = e^{2\pi i\theta}$, then $\cos\theta = \frac{1}{2}(\zeta + \zeta^{-1})$, $\cos n\theta = \frac{1}{2}(\zeta^n + \zeta^{-n})$ and so the coefficients of $T_s(x)$ are obtained by writing $\frac{1}{2}(\zeta^n + \zeta^{-n})$ as a polynomial in $\frac{1}{2}(\zeta + \zeta^{-1})$. That this can be done is an easy inductive argument. On the other hand, using FTSP one writes $x^n + y^n$ as a polynomial in $\sigma_1 = x + y$ and $\sigma_2 = xy$. For example, we have

$$x^3 + y^3 = (x+y)^3 - 3xy(x+y) = \sigma_1^3 - 3\sigma_2\sigma_1.$$

Thus, if $x^n + y^n = S_n(\sigma_1, \sigma_2)$ then one sees easily that $T_n(x) = \frac{1}{2}S_n(2x, 1)$. Next, the polynomials occurring in Theorem 1.3 are all in $\mathbb{Z}[\sigma_1, \sqrt{\sigma_2}]$; we may then specialize $\sigma_1 \mapsto x$, $\sqrt{\sigma_2} \mapsto 1$. We have already observed that the polynomials $L_d(x,y)$ specialize to $\Theta_d(x)$, the minimal polynomial of $2\cos(2\pi/d)$. The following is immediate from which equations (3) and (4) follow easily.

Corollary 2.1 [Watkins–Zeitlin]. The following are polynomial identities.

$$S_{s+1}(x) - S_s(x) = \prod_{d|n} \Theta_d(x) \quad \text{if } n = 2s+1 \text{ is odd;}$$

$$S_{s+1}(x) - S_{s-1}(x) = \prod_{d|n} \Theta_d(x) \quad \text{if } n = 2s \text{ is even.}$$

3. The Minimal Polynomial of $\mathbf{cos(2\pi/p)}$, Where p is Prime. In this section, we assume that p is prime, and that $\zeta = e^{2\pi i/p}$. As in the earlier sections, we shall continue to focus on $2\cos(2\pi/p) = \zeta + \zeta^{-1}$ and its minimal polynomial $\Theta_p(x)$, and derive information on $\Psi_p(x)$ as a consequence.

Naturally, one approach to this problem is to write $p = 2s + 1$ (the case $p = 2$ being trivial: $\Theta_2(x) = x + 2$) and use Corollary 2.1. This yields

$$(x-2)(S_{s+1}(x) - S_s(x)) = \Theta_p(x).$$

This will generate recurrence relations on the coefficients of $\Theta_p(x)$. However, we prefer a more direct approach.

Theorem 3.1. Let $p = 2s + 1$ be an odd prime. If $\Theta_p(x)$ is the minimal polynomial of $2\cos(2\pi/p)$, then

$$\Theta_p(x) = \sum_{i=0}^{s} (-1)^i \sigma_i x^{s-i},$$

where

$$\sigma_{2k} = (-1)^k \binom{s-k}{k}, \quad k = 0, 1, \dots, \left\lfloor \frac{s}{2} \right\rfloor;$$

$$\sigma_{2k+1} = (-1)^k \binom{s-k}{k-1}, \quad k = 1, \dots, \left\lfloor \frac{s+1}{2} \right\rfloor.$$

Proof. If

$$f(x) = \sum_{k=0}^{\lfloor \frac{s}{2} \rfloor} (-1)^k \binom{s-k}{k} x^{s-2k} - \sum_{k=1}^{\lfloor \frac{s+1}{2} \rfloor} (-1)^k \binom{s-k}{k-1} x^{s-(2k-1)},$$

then since $\deg f(x) = \deg \Theta_p(x)$, it suffices to show that $f(\zeta+\zeta^{-1}) = 0$. We have

$$f(\zeta+\zeta^{-1}) = \sum_{k=0}^{\lfloor \frac{s}{2} \rfloor} (-1)^k \binom{s-k}{k} (\zeta+\zeta^{-1})^{s-2k}$$

$$- \sum_{k=1}^{\lfloor \frac{s+1}{2} \rfloor} (-1)^k \binom{s-k}{k-1} (\zeta+\zeta^{-1})^{s-2k+1}$$

$$= \sum_{k=0}^{\lfloor \frac{s}{2} \rfloor} \sum_{l=0}^{s-2k} (-1)^k \binom{s-k}{k} \binom{s-2k}{l} \zeta^{-s+2k+2l}$$

$$- \sum_{k=1}^{\lfloor \frac{s+1}{2} \rfloor} \sum_{l=0}^{s-2k+1} (-1)^k \binom{s-k}{k-1} \binom{s-2k+1}{l} \zeta^{-s+2k+2l-1}.$$

In the sum,

$$\sum_{k=0}^{\lfloor \frac{s}{2} \rfloor} \sum_{l=0}^{s-2k} (-1)^k \binom{s-k}{k} \binom{s-2k}{l} \zeta^{-s+2k+2l},$$

the coefficient of ζ^{-s+2r}, $0 \le r \le \lfloor \frac{s}{2} \rfloor$ is given by

$$\binom{s}{0}\binom{s}{r} - \binom{s-1}{1}\binom{s-2}{r-1} + \cdots + (-1)^r \binom{s-r}{r}\binom{s-2r}{0}$$

$$= \sum_{m=0}^{r} (-1)^m \binom{s-m}{m} \binom{s-2m}{r-m}.$$

Next note that

$$\binom{s-m}{m}\binom{s-2m}{r-m} = \frac{(s-m)!}{m!(s-m-m)!}\frac{(s-2m)!}{(r-m)!(s-2m-r+m)!}$$

$$= \frac{(s-m)!(s-2m)!}{m!(s-2m)!(r-m)!(s-m-r)!} = \frac{r!(s-m)!}{m!(r-m)!r!(s-m-r)!}$$

$$= \frac{r!}{m!(r-m)!}\frac{(s-m)!}{r!(s-m-r)!} = \binom{r}{m}\binom{s-m}{r}.$$

In the sum

$$\sum_{k=1}^{\lfloor\frac{s+1}{2}\rfloor}\sum_{l=0}^{s-2k+1}(-1)^{k+1}\binom{s-k}{k-1}\binom{s-2k+1}{l}\zeta^{-s+2k+2l-1}$$

the coefficient of $\zeta^{-s+2r-1}$, $1 \leq r \leq \lfloor\frac{s+1}{2}\rfloor$ is given by

$$\binom{s-1}{0}\binom{s-1}{r-1} - \binom{s-2}{1}\binom{s-3}{r-2} + \cdots + (-1)^r\binom{s-r}{r-1}\binom{s-2r+1}{0}$$

$$= \sum_{m=0}^{r-1}(-1)^m\binom{s-m-1}{m}\binom{s-2m-1}{r-m-1}.$$

Now

$$\begin{aligned}
&\binom{s-m-1}{m}\binom{s-2m-1}{r-m-1} \\
&= \frac{(s-m-1)!}{m!(s-m-1-m)!}\frac{(s-2m-1)!}{(r-m-1)!(s-2m-1-r+m+1)!} \\
&= \frac{(s-m-1)!(s-2m-1)!}{m!(s-m-1)!(r-m-1)!(s-m-r)!} \\
&= \frac{(r-1)!(s-m-1)!}{m!(r-1-m)!(r-1)!(s-m-r)!} \\
&= \frac{(r-1)!}{m!(r-1-m)!}\frac{(s-m-1)!}{(r-1)!(s-m-1-r+1)!} \\
&= \binom{r-1}{m}\binom{s-m-1}{r-1}.
\end{aligned}$$

Therefore, since $\sum_{m=-s}^{s}\zeta^m = 0$, it suffices to prove that

$$\sum_{m=0}^{r}(-1)^m\binom{r}{m}\binom{s-m}{r} = 1,$$

and that

$$\sum_{m=0}^{r-1}(-1)^m\binom{r-1}{m}\binom{s-m-1}{r-1} = 1.$$

Thus, it suffices to prove the following.

<u>Lemma 3.2</u>. For any integer s, we have

$$\sum_{m=0}^{r}(-1)^m\binom{r}{m}\binom{s-m}{r} = 1.$$

Proof. We shall prove the stronger result that

$$\sum_{m=0}^{r} (-1)^m \binom{r}{m} \binom{s-m}{r'} = \begin{cases} 1, & \text{if } r = r'; \\ 0, & \text{if } r' < r. \end{cases}$$

We use induction on s.

$$\sum_{m=0}^{r} (-1)^m \binom{r}{m} \binom{s-m}{r} = \sum_{m=0}^{r} (-1)^m \binom{r}{m} \left[\binom{s-m-1}{r} + \binom{s-m-1}{r-1} \right]$$

$$= 1 + 0 = 1.$$

Now, if $r' < r$,

$$\sum_{m=0}^{r} (-1)^m \binom{r}{m} \binom{s-m}{r'} = \sum_{m=0}^{r} (-1)^m \binom{r}{m} \left[\binom{s-m-1}{r'} + \binom{s-m-1}{r'-1} \right]$$

$$= 0 + 0 = 0.$$

This concludes the proof of Theorem 3.1.

References

1. N. Jacobson, *Basic Algebra I*, W. H. Freeman and Company, New York, 1985.
2. D. H. Lehmer, "A Note on Trigonometric Algebraic Numbers," *American Mathematical Monthly*, 40 (1933), 165–166.
3. W. Watkins and J. Zeitlin, "The Minimal Polynomial of $\cos(2\pi/n)$," *American Mathematical Monthly*, 100 (1993), 471–474.

David Surowski
Department of Mathematics
Kansas State University
Manhattan, KS 66506–2602
email: dbski@math.ksu.edu

Paul McCombs
Department of Mathematics
Olney Central College
Olney, IL 62450
email: mccombsp@iecc.cc.il.us