On the ring of integers of real cyclotomic fields

By Koji YAMAGATA*) and Masakazu YAMAGISHI**)

(Communicated by Shigefumi MORI, M.J.A., May 12, 2016)

Abstract: Let ζ_n be a primitive nth root of unity. As is well known, $\mathbf{Z}[\zeta_n+\zeta_n^{-1}]$ is the ring of integers of $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$. We give an alternative proof of this fact by using the resultants of modified cyclotomic polynomials.

Key words: Cyclotomic field; ring of integers; Chebyshev polynomials.

1. Introduction. Let ζ_n be a primitive nth root of unity. It is well known that $\mathbf{Z}[\zeta_n]$ is the ring of integers of the nth cyclotomic field $\mathbf{Q}(\zeta_n)$. Generally this is proved by reducing the case of general n to the prime-power case (cf. [5]). On the other hand, Lüneburg [4] directly proved the case of general n by showing that $\mathbf{Z}[\zeta_n]$ is a Dedekind domain.

It is also well known that $\mathbf{Z}[\zeta_n+\zeta_n^{-1}]$ is the ring of integers of the nth real cyclotomic field $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$. This fact easily follows from the corresponding fact for $\mathbf{Q}(\zeta_n)$ (cf. [5]). Another proof by use of the ramification groups is found in [3]. The purpose of this note is to give yet another proof of this fact, applying the method of [4] to $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$. A key ingredient in the proof is the computation of the resultants of modified cyclotomic polynomials by the second named author in [8]. We also compute the discriminants of modified cyclotomic polynomials. We remark that analogous results have been obtained for cyclotomic function fields in [1].

2. Chebyshev polynomials and modified cyclotomic polynomials. We recall the definition of Chebyshev polynomials and modified cyclotomic polynomials, and quote some of their properties.

Definition 2.1. The Chebyshev polynomials T_n, U_n, V_n, and W_n of the first, second, third, and fourth kind, respectively, are characterized by

$$T_n(\cos\theta)=\cos n\theta,\quad U_n(\cos\theta)=\frac{\sin(n+1)\theta}{\sin\theta},$$

$$V_n(\cos\theta)=\frac{\cos(n+1/2)\theta}{\cos\theta/2},$$

$$W_n(\cos\theta)=\frac{\sin(n+1/2)\theta}{\sin\theta/2},$$

where n is a nonnegative integer. The normalized Chebyshev polynomials of the first and second kind are defined by $C_n(x)=2T_n(x/2)$, $S_n(x)=U_n(x/2)$. We adopt Schur's notation $\mathscr{S}_n=S_{n-1}$. For odd n we define $\mathscr{V}_n(x)=V_{(n-1)/2}(x/2)$, $\mathscr{W}_n(x)=W_{(n-1)/2}(x/2)$.

Note that these polynomials all have integral coefficients.

Lemma 2.2.

$$C_n'(x)=n\mathscr{S}_n(x), \tag{2.1}$$

$$\mathscr{V}_n'(x)=\frac{n\mathscr{W}_n(x)-\mathscr{V}_n(x)}{2(x+2)}\ (n:odd)\ \text{and} \tag{2.2}$$

$$\mathscr{W}_n'(x)=\frac{n\mathscr{V}_n(x)-\mathscr{W}_n(x)}{2(x-2)}\ (n:odd). \tag{2.3}$$

We define the modified cyclotomic polynomials Ψ_n. For $n\geq 3$ let Ψ_n be the minimal polynomial of $2\cos(2\pi/n)$ over $\mathbf{Q}$. Then $\Psi_n(x)\in\mathbf{Z}[x]$ and $\deg(\Psi_n)=\varphi(n)/2$. We do not define Ψ_1,Ψ_2 themselves, but instead we define their squares by

$$\Psi_1(x)^2=x-2,\quad \Psi_2(x)^2=x+2.$$

Proposition 2.3 ([6, Proposition 2.4])**.**

(a) *For $n\geq 3$, we have*

$$C_n(x)=\prod_{d|n,\ \frac{n}{d}:odd}\Psi_{4d}(x),$$

$$\mathscr{S}_n(x)=\prod_{2<d|2n}\Psi_d(x).$$

(b) *For odd $n\geq 3$, we have*

$$\mathscr{V}_n(x)=\prod_{1<d|n}\Psi_{2d}(x), \tag{2.4}$$

2010 Mathematics Subject Classification. Primary 11E09; Secondary 11R18.

*) Field of Mathematics and Mathematical Science, Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan.

**) Department of Mathematics, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan.

doi: 10.3792/pjaa.92.73

$$\mathscr{W}_n(x) = \prod_{1<d|n} \Psi_d(x). \tag{2.5}$$

Lemma 2.4. *Let $n \not\equiv 2 \pmod 4$. Let p be a prime and e,m positive integers such that $n = p^e m$, $p \nmid m$. Then,*

$$\Psi_n(x) \equiv \Psi_m(x)^{\varphi(p^e)} \pmod p.$$

Note that the right side makes sense even if $m = 1$ since $\varphi(p^e)$ is even by our assumption.

Proof. In the case where $m \geq 3$, this follows from [8, (3.4)].

In the case where $m = 1$, we are reduced to the case where $n = p \geq 3$ or $n = 4$, $p = 2$, by [8, (3.4)]. Suppose $n = p \geq 3$. By (2.5) and [7, Lemma 2.1 (ix)], we have

$$\Psi_p(x) = \mathscr{W}_p(x) \equiv (x-2)^{\frac{p-1}{2}} = \Psi_1(x)^{\varphi(p)} \pmod p.$$

For $n = 4$, $p = 2$, we have

$$\Psi_4(x) = x \equiv \Psi_1(x)^{\varphi(4)} \pmod 2.$$

Since $m \neq 2$, we complete the proof. □

For a positive integer n let $L(n) = p$ if n is a power of some prime p, and $L(n) = 1$ otherwise.

Lemma 2.5 ([8, Lemma 3.1])**.** *Let $n \geq 3$.*

(a) $\Psi_n(2) = L(n)$.

(b) $|\Psi_n(-2)| = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ L(n/2) & \text{if } n \text{ is even.} \end{cases}$

Let $\mathrm{res}(f,g)$ denote the resultant of two polynomials f and g.

Theorem 2.6 ([8, Theorem 3.2])**.** *Let $3 \leq m < n$.*

$$|\mathrm{res}(\Psi_n, \Psi_m)| = \begin{cases} L(n/m)^{\frac{\varphi(m)}{2}} & \text{if } m \mid n, \\ 1 & \text{otherwise.} \end{cases}$$

3. The discriminant of $\Psi_n(x)$. We give an alternative proof of the following well known result. Let $\Delta(f)$ denote the discriminant of a polynomial f.

Proposition 3.1 ([2, Theorem 3.8])**.** *Let $n \geq 3$. If $n = 2^e$, $e > 1$, then*

$$\Delta(\Psi_n) = 2^{(e-1)2^{e-2}-1}.$$

If $n = p^e$ or $n = 2p^e$, p is an odd prime, then

$$\Delta(\Psi_n) = p^{\frac{ep^e-(e+1)p^{e-1}-1}{2}}.$$

Otherwise,

$$\Delta(\Psi_n) = \frac{n^{\frac{\varphi(n)}{2}}}{\prod_{p|n} p^{\frac{\varphi(n)}{2(p-1)}}}.$$

Proof. Since all roots of Ψ_n are real, $\Delta(\Psi_n)$ is positive. So we ignore the signs in the computation of $\Delta(\Psi_n)$ throughout this proof.

Case n : odd If $\Psi_n(\lambda) = 0$, by (2.3) and (2.5), we have

$$\begin{aligned} \frac{n\mathscr{V}_n(\lambda)}{2(\lambda-2)} &= \mathscr{W}'_n(\lambda) \\ &= \Psi'_n(\lambda) \prod_{1<d|n,\ d\neq n} \Psi_d(\lambda). \end{aligned}$$

Then it follows that

$$\begin{aligned} \Delta(\Psi_n) &= \prod_\lambda \Psi'_n(\lambda) \\ &= \frac{n^{\frac{\varphi(n)}{2}} \prod_\lambda \mathscr{V}_n(\lambda)}{2^{\frac{\varphi(n)}{2}} (\prod_\lambda (\lambda-2)) (\prod_\lambda \prod_{1<d|n,\ d\neq n} \Psi_d(\lambda))} \end{aligned} \tag{3.1}$$

where λ ranges over the roots of Ψ_n. By (2.4) and Theorem 2.6 we have

$$\begin{aligned} \prod_\lambda \mathscr{V}_n(\lambda) &= \prod_{1<d|n} \mathrm{res}(\Psi_n, \Psi_{2d}) \\ &= \mathrm{res}(\Psi_n, \Psi_{2n}) \\ &= 2^{\frac{\varphi(n)}{2}}. \end{aligned} \tag{3.2}$$

Lemma 2.5 (a) gives

$$\prod_\lambda (\lambda - 2) = \Psi_n(2) = L(n). \tag{3.3}$$

Finally we compute

$$\prod_\lambda \prod_{1<d|n,\ d\neq n} \Psi_d(\lambda) = \prod_{1<d|n,\ d\neq n} \mathrm{res}(\Psi_n, \Psi_d) \tag{3.4}$$

as follows: If $n = p^e$, then, by Theorem 2.6 we have

$$\prod_{1<d|n,\ d\neq n} \mathrm{res}(\Psi_n, \Psi_d) = \prod_{i=1}^{e-1} p^{\frac{\varphi(p^i)}{2}} = p^{\frac{p^{e-1}-1}{2}}. \tag{3.5}$$

If $n = \prod_{i=1}^t p_i^{e_i}$, $t \geq 2$, $e_i \geq 1$, then, by Theorem 2.6, we have

$$\begin{aligned} \prod_{1<d|n,\ d\neq n} \mathrm{res}(\Psi_n, \Psi_d) &= \prod_{i=1}^t \prod_{j=1}^{e_i} p_i^{\frac{\varphi(n/p_i^j)}{2}} \\ &= \prod_{i=1}^t p_i^{\frac{\varphi(n)}{2(p_i-1)}}, \end{aligned} \tag{3.6}$$

since

$$\sum_{j=1}^{e_i}\varphi(n/p_i^j)=\varphi(n/p_i^{e_i})\sum_{j=0}^{e_i-1}\varphi(p_i^j)$$
$$=\varphi(n/p_i^{e_i})p^{e_i-1}$$
$$=\frac{\varphi(n)}{p_i-1}.$$

Substituting (3.2)–(3.6) into (3.1), the desired identity follows.

The argument is similar in the remaining cases, so we just provide some key identities:

Case $n\equiv 2 \pmod 4$

$$\frac{(n/2)\mathscr{W}_{n/2}(\lambda)}{2(\lambda+2)}=\mathscr{V}'_{n/2}(\lambda)$$
$$=\Psi'_n(\lambda)\prod_{1<d|\frac{n}{2},\ d\neq\frac{n}{2}}\Psi_{2d}(\lambda).$$

$$\Delta(\Psi_n)=\left(\frac{n}{4}\right)^{\frac{\varphi(n/2)}{2}}\times\frac{\prod_\lambda\mathscr{W}_{\frac{n}{2}}(\lambda)}{(\prod_\lambda(\lambda+2))(\prod_\lambda\prod_{1<d|\frac{n}{2},\ d\neq\frac{n}{2}}\Psi_{2d}(\lambda))},$$

$$\prod_\lambda\mathscr{W}_{\frac{n}{2}}(\lambda)=\prod_{1<d|\frac{n}{2}}\operatorname{res}(\Psi_n,\Psi_d)$$
$$=\operatorname{res}(\Psi_n,\Psi_{\frac{n}{2}})$$
$$=2^{\frac{\varphi(n/2)}{2}},$$

$$\prod_\lambda(\lambda+2)=\Psi_n(-2)=L(n/2).$$

If $n=2p^e$, then

$$\prod_\lambda\prod_{1<d|\frac{n}{2},\ d\neq\frac{n}{2}}\Psi_{2d}(\lambda)=p^{\frac{p^{e-1}-1}{2}}.$$

If $n=2\prod_{i=1}^t p_i^{e_i}$, $t\geq 2$, $e_i\geq 1$, then

$$\prod_\lambda\prod_{1<d|\frac{n}{2},\ d\neq\frac{n}{2}}\Psi_{2d}(\lambda)=\prod_{i=1}^t p_i^{\frac{\varphi(n)}{2(p_i-1)}}.$$

Case $n\equiv 0 \pmod 4$

$$\frac{n}{4}\mathscr{S}_{n/4}(\lambda)=C'_{n/4}(\lambda)=\Psi'_n(\lambda)\prod_d\Psi_{4d}(\lambda),$$

the product being taken over all d such that $d\mid\frac{n}{4}$, $d\neq\frac{n}{4}$, $\frac{n}{4d}$ is odd,

$$\Delta(\Psi_n)=\left(\frac{n}{4}\right)^{\frac{\varphi(n)}{2}}\frac{\prod_\lambda\mathscr{S}_{\frac{n}{4}}(\lambda)}{\prod_\lambda\prod_d\Psi_{4d}(\lambda)}.$$

If $n=2^e$, then

$$\prod_\lambda\prod_d\Psi_{4d}(\lambda)=\prod_d\operatorname{res}(\Psi_n,\Psi_{4d})=1,$$
$$\prod_\lambda\mathscr{S}_{n/4}(\lambda)=\prod_{2<d|\frac{n}{2}}\operatorname{res}(\Psi_n,\Psi_d)$$
$$=\prod_{j=2}^{e-1}\operatorname{res}(\Psi_n,\Psi_{2^j})$$
$$=2^{2^{e-2}-1}.$$

If $n=\prod_{i=1}^t p_i^{e_i}$, $t\geq 2$, $e_i\geq 1$, then

$$\prod_\lambda\prod_d\Psi_{4d}(\lambda)=\prod_d\operatorname{res}(\Psi_n,\Psi_{4d})=\prod_{i=1}^t p_i^{\frac{\varphi(n)}{2(p_i-1)}},$$

$$\prod_\lambda\mathscr{S}_{n/4}(\lambda)=\prod_{2<d|\frac{n}{2}}\operatorname{res}(\Psi_n,\Psi_d)$$
$$=\prod_{j=1}^{e}\operatorname{res}(\Psi_n,\Psi_{\frac{n}{2^j}})$$
$$=2^{\frac{\varphi(n)}{2}}.$$ □

4. The ring of integers of $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$. We need the following lemma to prove Theorem 4.2. Let $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$.

Lemma 4.1 ([4, Hilfssatz 4]). *Let θ be an algebraic integer, and $f(x)$ the minimal polynomial of θ over $\mathbf{Q}$. Let P be a maximal ideal of $\mathbf{Z}[\theta]$ and p the prime such that $p\mathbf{Z}=P\cap\mathbf{Z}$. Let $\mu(x)$ be a monic polynomial over $\mathbf{Z}$ of least degree such that $\mu(\theta)\in P$. Then, there exist polynomials $g(x),h(x)\in\mathbf{Z}[x]$ such that $f=\mu h+pg$. Suppose $\gcd(\mu,g,h)=1$ over $\mathbf{F}_p$. Then, the localization of $\mathbf{Z}[\theta]$ at P is a discrete valuation ring.*

The main result of this note is the following

Theorem 4.2. *Let $n\geq 3$. Then $\mathbf{Z}[\zeta_n+\zeta_n^{-1}]$ is a Dedekind domain. Therefore $\mathbf{Z}[\zeta_n+\zeta_n^{-1}]$ is the ring of algebraic integers in the field $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$.*

Proof. We may assume $n\not\equiv 2 \pmod 4$ since $\zeta_n=-\zeta_{n/2}$ if $n\equiv 2 \pmod 4$. Put $\theta=\zeta_n+\zeta_n^{-1}$, $R=\mathbf{Z}[\theta]$. We shall prove that R is a Dedekind domain by showing that the localization R_P is a discrete valuation ring for each maximal ideal $P\subset R$. Let p be the prime such that $p\mathbf{Z}=P\cap\mathbf{Z}$.

First we consider the case where $p\nmid n$. By Proposition 3.1 we have $p\nmid\Delta(\Psi_n)$, so that $\Psi_n(x)$ is separable over $\mathbf{F}_p$. If we apply Lemma 4.1 to $f=\Psi_n$, then $\mu(x)$ and $h(x)$ have no common roots over the algebraic closure $\overline{\mathbf{F}_p}$, so R_P is a discrete valuation ring.

Suppose $p\mid n$ and write $n=p^em$, $e\geq 1$, $p\nmid m$.

By Lemma 2.4, there exists $g(x) \in \mathbf{Z}[x]$ such that

$$\Psi_n(x) = \Psi_m(x)^{\varphi(p^e)} + pg(x). \tag{4.1}$$

Note that $\varphi(p^e)$ is even by our assumption $n \not\equiv 2 \pmod 4$.

Lemma 4.3. *$g(\theta)$ is a unit in R.*

Proof. Suppose $m \geq 3$. By Theorem 2.6 we have

$$\begin{aligned} p^{\varphi(n)} &= p^{\varphi(m)\varphi(p^e)} \\ &= \operatorname{res}(\Psi_n, \Psi_m)^{2\varphi(p^e)} \\ &= \prod_\lambda (\Psi_m(\lambda)^{\varphi(p^e)})^2, \end{aligned}$$

the product being taken over the roots λ of Ψ_n. Since $\Psi_m(\lambda)^{\varphi(p^e)} = -pg(\lambda)$ by (4.1), we have

$$p^{\varphi(n)} = \left(p^{\frac{\varphi(n)}{2}} \prod_\lambda g(\lambda) \right)^2.$$

Hence $\prod_\lambda g(\lambda) = \pm 1$, from which we conclude that $g(\theta)$ is a unit in R.

Suppose $m = 1$. By Lemma 2.5 we have

$$\operatorname{res}(\Psi_{p^e}, \Psi_1^2) = \operatorname{res}(\Psi_{p^e}, x-2) = \pm \Psi_{p^e}(2) = \pm p,$$

so that

$$p^{\varphi(p^e)} = \operatorname{res}(\Psi_{p^e}, \Psi_1^2)^{\varphi(p^e)} = \left(p^{\frac{\varphi(p^e)}{2}} \prod_\lambda g(x) \right)^2.$$

Hence the claim follows similarly. □

We return to the proof of Theorem 4.2. One could proceed as in [4], but here we give a shorter proof which was suggested to us by the referee. In the notation of Lemma 4.1, we take f, μ, g such that $f(x) = \Psi_n(x)$ and $g(x)$ is defined by (4.1). Since every root of $\mu(x) \bmod P$ coincides with $\theta \bmod P$ for some choice of primitive nth root of unity ζ_n, we see, by Lemma 4.3, that $\mu(x)$ and $g(x)$ have no common roots over $\overline{\mathbf{F}_p}$. Hence R_P is a discrete valuation ring by Lemma 4.1. This completes the proof. □

Acknowledgment. The authors would like to thank an anonymous referee for pointing out the simplification of the proof of Theorem 4.2.

References

[1] S. Jeong, Resultants of cyclotomic polynomials over $\mathbf{F}_q[T]$ and applications, Commun. Korean Math. Soc. **28** (2013), no. 1, 25–38.

[2] D. H. Lehmer, An extended theory of Lucas' functions, Ann. of Math. (2) **31** (1930), no. 3, 419–448.

[3] J. J. Liang, On the integral basis of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math. **286/287** (1976), 223–226.

[4] H. Lüneburg, Resultanten von Kreisteilungspolynomen, Arch. Math. (Basel) **42** (1984), no. 2, 139–144.

[5] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, 83, Springer, New York, 1997.

[6] M. Yamagishi, A note on Chebyshev polynomials, cyclotomic polynomials and twin primes, J. Number Theory **133** (2013), no. 7, 2455–2463.

[7] M. Yamagishi, Periodic harmonic functions on lattices and Chebyshev polynomials, Linear Algebra Appl. **476** (2015), 1–15.

[8] M. Yamagishi, Resultants of Chebyshev polynomials: the first, second, third, and fourth kinds, Canad. Math. Bull. **58** (2015), no. 2, 423–431.