



Contents lists available at ScienceDirect

Journal of Number Theory

[www.elsevier.com/locate/jnt](http://www.elsevier.com/locate/jnt)



# The Galois theory of the lemniscate

David A. Cox<sup>a,\*</sup>, Trevor Hyde<sup>b</sup>

<sup>a</sup> Department of Mathematics, Amherst College, Amherst, MA 01002-5000, USA

<sup>b</sup> Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, USA

## ARTICLE INFO

### Article history:

Received 13 August 2012

Received in revised form 18 April 2013

Accepted 17 August 2013

Available online 11 October 2013

Communicated by David Goss

### MSC:

primary 11G15

secondary 11R37, 14K22, 33E05

### Keywords:

Lemniscate

Galois group

Chebyshev polynomial

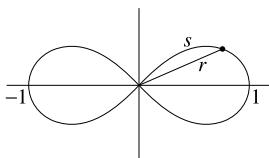
## ABSTRACT

This article studies the Galois groups that arise from division points of the lemniscate. We compute these Galois groups two ways: first, by class field theory, and second, by proving the irreducibility of lemnatonic polynomials, which are analogs of cyclotomic polynomials. We also discuss Abel's theorem on the lemniscate and explain how lemnatonic polynomials relate to Chebyshev polynomials.

© 2013 Elsevier Inc. All rights reserved.

## 1. Introduction

The lemniscate is the curve defined by the polar equation  $r^2 = \cos(2\theta)$ :



\* Corresponding author.

E-mail addresses: [dac@math.amherst.edu](mailto:dac@math.amherst.edu) (D.A. Cox), [tghyde@umich.edu](mailto:tghyde@umich.edu) (T. Hyde).

In the first quadrant, the arc length  $s$  is related to the radial distance  $r$  by the elliptic integral

$$s = \int_0^r \frac{dt}{\sqrt{1-t^4}}. \quad (1)$$

The arc length of the first-quadrant portion is  $\int_0^1 \frac{dt}{\sqrt{1-t^4}}$ , denoted by  $\varpi/2$  in analogy with  $\pi/2 = \int_0^1 \frac{dt}{\sqrt{1-t^2}}$ . Following Abel, the inverse function of (1) is denoted  $\varphi(s) = r$ . The goal of this paper is to compute the Galois group

$$\text{Gal}\left(K\left(\varphi\left(\frac{2\varpi}{n}\right)\right)/K\right), \quad (2)$$

where  $K = \mathbb{Q}(i)$  and  $n$  is a positive odd integer. Geometrically,  $\varphi(\frac{2\varpi}{n})$  tells us how to find the first  $n$ -division point of the lemniscate, and the size of the Galois group (2) determines whether or not we can divide the lemniscate into  $n$  pieces by ruler and compass. This will lead to a quick proof of Abel's theorem on the lemniscate, which characterizes those  $n$ 's for which this can be done (see Section 5 for a precise statement).

Our main result is an isomorphism

$$\text{Gal}\left(K\left(\varphi\left(\frac{2\varpi}{n}\right)\right)/K\right) \simeq (\mathbb{Z}[i]/n\mathbb{Z}[i])^\times \quad (3)$$

when  $n > 0$  is odd. We will prove this two ways, first using class field theory and complex multiplication in the spirit of [9], and second using *lemnatomic polynomials*, which are analogs of cyclotomic polynomials. The key step will be to prove that lemnatomic polynomials are irreducible.

Here is a brief summary of the paper. Section 2 explains how  $\varphi(s)$  extends to an elliptic function  $\varphi(z)$  and describes the period lattice  $L$  and associated elliptic curve  $E$ . We also recall how complex multiplication by  $\mathbb{Z}[i]$  gives explicit formulas for  $\varphi(\beta z)$  when  $\beta \in \mathbb{Z}[i]$ . Section 3 introduces the field  $K_\beta = K(\varphi(\frac{2\varpi}{\beta}))$  for  $\beta \in \mathbb{Z}[i]$  relatively prime to  $1+i$  (we say that  $\beta$  is *odd*) and constructs an injection

$$\text{Gal}(K_\beta/K) \hookrightarrow (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times. \quad (4)$$

We also give some alternate descriptions of  $K_\beta$  that clarify its relation to the elliptic curve  $E$ . We conclude by identifying  $K_\beta$  as the ray class field of  $K$  for the modulus  $2(1+i)\beta$  when  $\beta \in \mathbb{Z}[i]$  is odd and use class field theory and complex multiplication to prove that (4) is an isomorphism. Section 4 defines the lemnatomic polynomial  $\Lambda_\beta$  and proves its irreducibility over  $K$  by an elementary argument, leading to an elementary proof of (3). We also determine the degree and constant term of  $\Lambda_\beta$ . Section 5 shows how Abel's theorem on the lemniscate follows from the irreducibility of lemnatomic

polynomials, and the final Section 6 explores a surprisingly strong analogy between lemnatomic polynomials and irreducible factors of Chebyshev polynomials.

## 2. The complex lemniscatic function

As explained in [3, Chapter 15], the function  $\varphi(s)$  from the Introduction extends to a function of period  $2\varpi$  on  $\mathbb{R}$  and satisfies the addition law

$$\varphi(x + y) = \frac{\varphi(x)\varphi'(y) + \varphi(y)\varphi'(x)}{1 + \varphi(x)^2\varphi(y)^2} \tag{5}$$

and the differential equation

$$\varphi'(s)^2 = 1 - \varphi(s)^4. \tag{6}$$

As is well known, we extend  $\varphi$  to a meromorphic function on  $\mathbb{C}$  via

$$\varphi(z) = \varphi(x + iy) = \frac{\varphi(x)\varphi'(y) + i\varphi(y)\varphi'(x)}{1 - \varphi(x)^2\varphi(y)^2}.$$

By [3, Section 15.3],  $\varphi$  is an elliptic function for the lattice

$$L = \mathbb{Z}(1 + i)\varpi + \mathbb{Z}(1 - i)\varpi \tag{7}$$

whose zeros (all simple) are at points  $\equiv 0, \varpi \pmod L$  and whose poles (also simple) are at points  $\equiv (1 \pm i)\varpi/2 \pmod L$ . Also,  $\varphi$  is an odd function and

$$\varphi(z) = \varphi(w) \iff z = (-1)^{m+n}w + (m + in)\varpi, \quad m, n \in \mathbb{Z}. \tag{8}$$

For the rest of the paper, we will use the notation

$$K = \mathbb{Q}(i), \quad \mathcal{O} = \mathbb{Z}[i].$$

In the introduction we defined  $\beta \in \mathcal{O}$  to be odd if it is relatively prime to  $1 + i$ . Note that

$$\begin{aligned} \beta \in \mathcal{O} \text{ is odd} &\iff \beta = m + in, \quad m, n \in \mathbb{Z}, \quad m + n \text{ odd} \\ &\iff \beta \equiv i^\varepsilon \pmod{2(1 + i)} \text{ for some } \varepsilon \in \{0, 1, 2, 3\}. \end{aligned}$$

We say that  $\beta \in \mathcal{O}$  is *even* if it is not odd, i.e., if  $1 + i$  divides  $\beta$ .

If  $\beta \in \mathcal{O}$  is nonzero and  $L$  is the period lattice (7), then note that

$$\frac{1}{\beta}L/L \simeq \mathcal{O}/\beta\mathcal{O}$$

as  $\mathcal{O}$ -modules. We say that  $\delta \in \frac{1}{\beta}L$  is a  $\beta$ -torsion generator if  $[\delta] \in \frac{1}{\beta}L/L$  generates  $\frac{1}{\beta}L/L$  as an  $\mathcal{O}$ -module. Any two  $\beta$ -torsion generators  $\delta, \delta'$  satisfy  $\delta \equiv \alpha\delta' \pmod L$  for some  $[\alpha] \in (\mathcal{O}/\beta\mathcal{O})^\times$ . We will use the  $\beta$ -torsion generator  $\delta_\beta = \frac{(1+i)\varpi}{\beta}$  frequently.

The elliptic function  $\varphi$  also has complex multiplication by  $\mathcal{O}$ .

**Theorem 2.1.** *Let  $\beta \in \mathcal{O}$  be odd. Then there exist coprime polynomials  $P_\beta(x), Q_\beta(x) \in \mathcal{O}[x]$  and  $\varepsilon \in \{0, 1, 2, 3\}$  such that*

1. For all  $z \in \mathbb{C}$ ,  $\varphi(\beta z) = M_\beta(\varphi(z))$ , where

$$M_\beta(x) = i^\varepsilon x \frac{P_\beta(x^4)}{Q_\beta(x^4)}.$$

2.  $\beta \equiv i^\varepsilon \pmod{2(1+i)}$ .
3.  $P_\beta(x)$  and  $Q_\beta(x)$  have degree  $(N(\beta) - 1)/4$ , where  $N(\beta) = \beta\bar{\beta}$  is the norm of  $\beta$ .
4. The  $\beta$ -division polynomial  $xP_\beta(x^4)$  has  $N(\beta)$  distinct roots given by  $\varphi(\alpha\delta)$  for  $[\alpha] \in \mathcal{O}/\beta\mathcal{O}$  and  $\delta \in \frac{1}{\beta}L$  a fixed  $\beta$ -torsion generator.
5.  $P_\beta(x)$  is monic and  $Q_\beta(x) = x^{(N(\beta)-1)/4} P_\beta(1/x)$ .
6. Suppose  $\pi$  is an odd prime in  $\mathcal{O}$  and let  $d = (N(\pi) - 1)/4$ . Then

$$P_\pi(x) = x^d + a_1x^{d-1} + \dots + a_d,$$

such that each  $a_j$  is divisible by  $\pi$  and  $a_d = i^{-\varepsilon}\pi$ .

**Proof.** See [3, Theorem 15.4.8] for (1), (2), (3), (5) and (6). Note that (6) is due to Eisenstein. As for part (4), let  $\delta_\beta = \frac{(1+i)\varpi}{\beta}$ . For any  $\alpha \in \mathcal{O}$ ,  $\varphi(\alpha\delta_\beta)$  is a root of  $xP_\beta(x^4)$  since  $\varphi$  vanishes at  $\beta\alpha\delta_\beta \in L$ . Now suppose that  $\alpha, \alpha' \in \mathcal{O}$  satisfy  $\varphi(\alpha\delta_\beta) = \varphi(\alpha'\delta_\beta)$ . By (8), we have

$$\alpha\delta_\beta = (-1)^{m+n}\alpha'\delta_\beta + (m+in)\varpi, \quad m, n \in \mathbb{Z}.$$

This implies  $\alpha(1+i) = (-1)^{m+n}\alpha'(1+i) + (m+in)\beta$ , so that  $m+in$  is even. It follows easily that  $\alpha \equiv \alpha' \pmod \beta$ . Thus  $xP_\beta(x^4)$  has at least  $N(\beta) = |\mathcal{O}/\beta\mathcal{O}|$  distinct roots, namely  $\varphi(\alpha\delta_\beta)$  for  $[\alpha] \in \mathcal{O}/\beta\mathcal{O}$ . Since this polynomial has degree  $N(\beta)$ , these are all of its roots. Then the same holds for any other  $\beta$ -torsion generator  $\delta$  since  $\delta \equiv \alpha\delta_\beta \pmod L$  for some  $[\alpha] \in (\mathcal{O}/\beta\mathcal{O})^\times$ .  $\square$

We conclude this section with a few words about the elliptic curve  $E = \mathbb{C}/L$  associated to the period lattice  $L = \mathbb{Z}(1+i)\varpi + \mathbb{Z}(1-i)\varpi$  from (7).

**Lemma 2.2.** *The Weierstrass equation of  $E$  is  $Y^2 = 4X^3 + X$ .*

**Proof.** The Weierstrass equation of  $E = \mathbb{C}/L$  is  $Y^2 = 4X^3 - g_2(L)X - g_3(L)$ , and  $g_3(L) = 0$  since  $E$  has complex multiplication by  $\mathcal{O} = \mathbb{Z}[i]$ . As for  $g_2(L)$ , we know from [9] that the lattice  $L' = \mathbb{Z}2\varpi + \mathbb{Z}2\varpi i$  has  $g_2(L') = \frac{1}{4}$ . Since  $L' = (1 + i)L$ , we obtain

$$\frac{1}{4} = g_2(L') = g_2((1 + i)L) = (1 + i)^{-4}g_2(L) = -\frac{1}{4}g_2(L). \quad \square$$

Let  $\wp(z) = \wp(z; L)$  be the Weierstrass  $\wp$ -function for  $L$ . The elliptic functions  $\wp$  and  $\wp'$  have period lattice  $L$  and hence are rational functions of  $\wp$  and  $\wp'$ . By analyzing the behavior at zeros and poles, one can show that

$$\wp(z) = -2\frac{\wp'(z)}{\wp'(z)}, \quad \wp'(z) = \frac{4\wp(z)^2 - 1}{4\wp(z)^2 + 1}. \tag{9}$$

Note that by (6),  $\wp$  and  $\wp'$  parametrize the curve

$$y^2 = 1 - x^4, \tag{10}$$

while  $\wp$  and  $\wp'$  parametrize the curve of Lemma 2.2. Then (9) tells us that the curves of Lemma 2.2 and (10) are related by the birational transformation

$$x = -2\frac{X}{Y}, \quad y = \frac{4X^2 - 1}{4X^2 + 1}.$$

### 3. Preliminary analysis of the Galois group

We begin with the field  $K_\beta = K(\wp(\frac{2\varpi}{\beta}))$  defined in the Introduction.

**Proposition 3.1.** *If  $\beta \in \mathcal{O}$  is odd and  $\delta$  is any  $\beta$ -torsion generator, then*

$$K_\beta = K(\wp(\delta)) = K(\wp(\delta), \wp'(\delta)) = K(\wp(\delta), \wp'(\delta)) = K(E[\beta]),$$

where  $K(E[\beta])$  is the field obtained from  $K$  by adjoining the coordinates of the  $\beta$ -torsion points of  $E$ .

**Proof.** We first show that  $\frac{2\varpi}{\beta}$  is a  $\beta$ -torsion generator. Since  $\beta$  is odd, we have  $u\beta + v(1 - i) = 1$  for some  $u, v \in \mathcal{O}$ . Multiplying this by  $\delta_\beta = \frac{(1+i)\varpi}{\beta}$  gives  $v\frac{2\varpi}{\beta} \equiv \delta_\beta \pmod L$ , and our claim follows.

Let  $\delta, \delta'$  be  $\beta$ -torsion generators. As noted above,  $\delta \equiv \alpha\delta' \pmod L$  for some  $[\alpha] \in (\mathcal{O}/\beta\mathcal{O})^\times$ , where we may assume that  $\alpha$  is odd since  $\beta$  is (if  $\alpha$  is even, replace it with  $\alpha + \beta$ .) Then  $\wp(\delta) = \wp(\alpha\delta')$  and the latter is in  $K(\wp(\delta'))$  by part (1) of Theorem 2.1. This implies  $K(\wp(\delta)) = K(\wp(\delta'))$ , and then  $K_\beta = K(\wp(\delta))$  follows using  $\delta' = \frac{2\varpi}{\beta}$ .

For the second equality of the proposition, we use (5) to obtain

$$\varphi\left(\frac{2\varpi}{\beta}\right) = \varphi\left(\frac{(1-i)(1+i)\varpi}{\beta}\right) = \varphi((1-i)\delta_\beta) = \frac{(1-i)\varphi(\delta_\beta)\varphi'(\delta_\beta)}{1 + \varphi(\delta_\beta)^4}.$$

This implies  $\varphi'(\delta_\beta) \in K(\varphi(\frac{2\varpi}{\beta}), \varphi(\delta_\beta)) = K(\varphi(\delta_\beta))$ , which shows that the second equality holds for  $\delta_\beta$ . Then the addition laws for  $\varphi$  and  $\varphi'$  show that it also holds for any  $\beta$ -torsion generator  $\delta$ .

The third equality follows since (9) is birational, and the final equality follows since  $(\wp(\delta), \wp'(\delta)) \in E[\beta]$  generates  $E[\beta]$  as an  $\mathcal{O}$ -module.  $\square$

**Proposition 3.1** shows that  $K_\beta$  is a Galois extension of  $K$  (this also follows from **Theorem 2.1**). We compute the Galois group of  $K_\beta/K$  as follows.

**Proposition 3.2.** *Let  $\beta \in \mathcal{O}$  be odd. Then for any  $\sigma \in \text{Gal}(K_\beta/K)$ , there is a unique  $[\alpha] \in (\mathcal{O}/\beta\mathcal{O})^\times$  such that  $\sigma(\varphi(\delta)) = \varphi(\alpha\delta)$  for any  $\beta$ -torsion generator  $\delta$ . Furthermore, the map  $\sigma \mapsto [\alpha]$  defines an isomorphism*

$$\text{Gal}(K_\beta/K) \simeq (\mathcal{O}/\beta\mathcal{O})^\times.$$

**Proof.** For later purposes, we separate the argument into two parts. First, the elementary methods used in [3, **Theorem 15.5.1**] give an injection

$$\text{Gal}(K_\beta/K) \hookrightarrow (\mathcal{O}/\beta\mathcal{O})^\times. \tag{11}$$

We prove surjectivity using class field theory, similar to what Rosen does in [9]. By [13, **Theorem 5.6**], the ray class field of  $K$  for the modulus  $2(1+i)\beta$  is

$$L = K(\wp(\delta_{2(1+i)\beta})^2).$$

Since  $\mathcal{O}$  is a PID with  $\mathcal{O}^\times = \{\pm 1, \pm i\}$  and  $\beta$  is odd, the Artin map and the Chinese Remainder Theorem give isomorphisms

$$\text{Gal}(L/K) \simeq (\mathcal{O}/2(1+i)\beta\mathcal{O})^\times / \mathcal{O}^\times \simeq (\mathcal{O}/\beta\mathcal{O})^\times.$$

Using (9), we also have

$$L = K(\varphi'(\delta_{2(1+i)\beta})) = K\left(\varphi'\left(\frac{\varpi}{2\beta}\right)\right).$$

Differentiating the addition law for  $\varphi(z - \frac{\varpi}{2})$  gives the identity

$$\varphi'\left(z - \frac{\varpi}{2}\right) = 2\frac{\varphi(z)}{1 + \varphi(z)^2}. \tag{12}$$

Since  $\beta$  is odd, there exists  $\gamma \in \mathcal{O}$  such that  $2(1+i)\gamma - \beta = i^\varepsilon$ . Then  $\gamma\delta_\beta - \frac{\varpi}{2} = i^\varepsilon \frac{\varpi}{2\beta}$ . Using  $\varphi'(iz) = \varphi'(z)$  and (12), we obtain

$$\varphi'\left(\frac{\varpi}{2\beta}\right) = \varphi'\left(i^\varepsilon \frac{\varpi}{2\beta}\right) = \varphi'\left(\gamma\delta_\beta - \frac{\varpi}{2}\right) = 2 \frac{\varphi(\gamma\delta_\beta)}{1 + \varphi(\gamma\delta_\beta)^2} \in K(\varphi(\delta_\beta)) = K_\beta.$$

Thus  $K \subseteq L \subseteq K_\beta$ , so that  $|\text{Gal}(K_\beta/K)| \geq |\text{Gal}(L/K)| = |(\mathcal{O}/\beta\mathcal{O})^\times|$ . Since (11) is an injection, we see that  $L = K_\beta$  and (11) is an isomorphism.  $\square$

In Section 4 we use elementary methods to prove that the map (11) is an isomorphism.

In 1980, Rosen [9] applied class field theory to the lemniscate, though his approach was slightly different. He used the lattice  $L' = \mathbb{Z}2\varpi + \mathbb{Z}2\varpi i$ , which corresponds to the elliptic curve  $E' = \mathbb{C}/L'$  defined by  $Y^2 = 4X^3 - \frac{1}{4}X$ . In order to prove Abel’s theorem on the lemniscate (see Theorem 5.1 below), he used the isomorphism

$$\text{Gal}\left(K\left(\wp\left(\frac{2\varpi}{n}; L'\right)^2\right)/K\right) \simeq (\mathcal{O}/n\mathcal{O})^\times / \mathcal{O}^\times$$

since  $K(\wp(\frac{2\varpi}{n}; L')^2)$  is the ray class field of  $K$  for the modulus  $n$ . The first person to apply class field theory to the lemniscate was Takagi in his 1903 thesis, where he showed that all abelian extensions of  $K = \mathbb{Q}(i)$  are generated by division values of the lemniscatic elliptic function (see Schappacher [10, p. 259] for precise references).

Proposition 3.2 for the case when  $\beta$  is an odd prime power was first proved by Lemmermeyer in [6, Theorem 8.19].

### 4. Lemnatomic polynomials

In this section we present an elementary proof of our main result. Pursuing the analogy between the roots of unity and the division points of the lemniscate leads to an algebraic theory for the lemniscate akin to the circle’s cyclotomy. We introduce the *lemnatomic polynomials* and prove their irreducibility over  $K$ . Our main result (3) follows as a corollary.

**Definition 4.1.** Let  $\beta \in \mathcal{O}$  be odd and set  $\delta_\beta = \frac{(1+i)\varpi}{\beta}$ . We call

$$A_\beta(x) = \prod_{[\alpha] \in (\mathcal{O}/\beta\mathcal{O})^\times} (x - \varphi(\alpha\delta_\beta))$$

the  $\beta^{\text{th}}$  *lemnatomic polynomial*.

In this definition, we can replace  $\delta_\beta$  with any  $\beta$ -torsion generator  $\delta$ . Furthermore, the roots of  $A_\beta$  are  $\varphi(\delta)$  as  $\delta$  ranges over all lattice-inequivalent  $\beta$ -torsion generators.

Note also that  $\Lambda_\beta = \Lambda_{\beta'}$  when  $\beta$  and  $\beta'$  are associates in  $\mathcal{O}$  since  $\Lambda_\beta$  depends only on the ideal generated by  $\beta$ . It will often be convenient to specify an associate. Recall that an odd  $\beta \in \mathcal{O}$  satisfies  $\beta \equiv i^\varepsilon \pmod{2(1+i)}$  for  $\varepsilon \in \{0, 1, 2, 3\}$ .

**Definition 4.2.** An odd element  $\beta \in \mathcal{O}$  is *normalized* if  $\beta \equiv 1 \pmod{2(1+i)}$ .

**Lemma 4.3.** Let  $\Lambda_\beta$  be as above. Then  $\Lambda_\beta \in \mathcal{O}[x]$  is monic of degree  $|(\mathcal{O}/\beta\mathcal{O})^\times|$ .

**Proof.** All that requires demonstration is  $\Lambda_\beta \in \mathcal{O}[x]$ . By [Proposition 3.2](#), the roots of  $\Lambda_\beta$  are permuted under the action of  $\text{Gal}(K_\beta/K)$  and hence the coefficients lie in the fixed field  $K$  of the Galois group. The roots of  $\Lambda_\beta$  are algebraic integers since they are also roots of the monic polynomial  $xP_\beta(x^4) \in \mathcal{O}[x]$ . It follows that  $\Lambda_\beta(x) \in \mathcal{O}[x]$ .  $\square$

As cyclotomic polynomials provide a factorization of  $x^n - 1$  over  $\mathbb{Q}$ , the lemnatomic polynomials provide a factorization of  $xP_\beta(x^4)$  over  $K$ .

**Proposition 4.4.** Let  $\beta \in \mathcal{O}$  be odd and let  $xP_\beta(x^4)$  be the  $\beta$ -division polynomial from [Theorem 2.1](#). Then

$$xP_\beta(x^4) = \prod_{\gamma|\beta} \Lambda_\gamma(x),$$

where the product is over all normalized divisors  $\gamma$  of  $\beta$ .

**Proof.** From [Theorem 2.1](#), the roots of  $xP_\beta(x^4)$  are  $\varphi(\alpha\delta_\beta)$  for  $[\alpha] \in \mathcal{O}/\beta\mathcal{O}$ . The proof consists of using gcd's to reorganize the roots as in the analogous cyclotomic result. We refer the reader to [\[3, Proposition 9.1.5\]](#).  $\square$

We can also determine the constant term of  $\Lambda_\beta$ .

**Proposition 4.5.** Let  $\beta \in \mathcal{O}$  be odd and a nonunit. If  $\beta = u\pi^k$  where  $u \in \mathcal{O}^\times$ ,  $\pi$  is a normalized prime, and  $k \geq 1$ , then  $\Lambda_\beta(0) = \pi$ . In all other cases,  $\Lambda_\beta(0) = 1$ .

**Proof.** We may assume that  $\beta$  is odd and normalized (this implies  $i^\varepsilon = 1$  in part (1) of [Theorem 2.1](#)). Using  $\varphi'(0) = 1$  and L'Hôpital's rule, we have

$$\beta = \lim_{x \rightarrow 0} \frac{\varphi(\beta x)}{\varphi(x)} = \lim_{x \rightarrow 0} \frac{P_\beta(\varphi(x)^4)}{Q_\beta(\varphi(x)^4)} = \frac{P_\beta(0)}{Q_\beta(0)} = P_\beta(0) \tag{13}$$

since  $Q_\beta(0) = 1$  by part (5) of [Theorem 2.1](#).

Now let  $\pi$  be a normalized odd prime. If  $\beta = \pi$ , then [Proposition 4.4](#) tells us that  $\Lambda_\pi(x) = P_\pi(x^4)$ . Therefore,  $\Lambda_\pi(0) = P_\pi(0) = \pi$  by (13).

Next, if  $\beta = \pi^k$ , then we proceed by strong induction. Suppose that for all  $1 \leq k \leq n$ , we have  $\Lambda_{\pi^k}(0) = \pi$ . From [Proposition 4.4](#) and our induction hypothesis we obtain



$$\pi^{n+1} = P_{\pi^{n+1}}(0) = \prod_{k=1}^{n+1} A_{\pi^k}(0) = \pi^n A_{\pi^{n+1}}(0).$$

We conclude that  $A_{\pi^{n+1}}(0) = \pi$ , completing our induction.

Finally, suppose  $\beta$  is not a prime power. Again, Proposition 4.4 tells us that

$$\beta = P_\beta(0) = \prod_{\substack{\gamma|\beta, \gamma \neq 1 \\ \gamma \text{ normalized}}} A_\gamma(0). \tag{14}$$

Each prime power  $\pi^k$  dividing  $\beta$ , where  $\pi$  is a normalized prime, contributes  $\pi$  to the product (14). Thus the normalized prime power divisors of  $\beta$  contribute a factor of  $\beta$  to (14). Therefore

$$\prod_{\substack{\gamma|\beta, \gamma \neq 1, \gamma \text{ normalized} \\ \gamma \text{ not a prime power}}} A_\gamma(0) = 1.$$

Using this and strong induction on the number of prime factors of  $\beta$  (counted with multiplicity), it is now easy to prove that  $A_\beta(0) = 1$  when  $\beta$  is not a prime power. We leave the details to the reader.  $\square$

**Remark 4.6.** The inspiration for Proposition 4.5 derives from a similar result for irreducible factors of Chebyshev polynomials proved in [5, Proposition 2]. We will explore the analogy between lemnatomic polynomials and Chebyshev polynomials in Section 6.

We now come to the main result of this section.

**Theorem 4.7.** *If  $\beta \in \mathcal{O}$  is odd, then the lemnatomic polynomial  $A_\beta$  is irreducible over  $K$ .*

**Proof.** We will follow the strategy used in [3, Theorem 9.1.9] to prove that the cyclotomic polynomial  $\Phi_n$  is irreducible over  $\mathbb{Q}$ .

Since  $A_\beta \in \mathcal{O}[x]$  is monic, Gauss’s lemma implies that an irreducible factor  $f$  of  $A_\beta$  in  $K[x]$  lies in  $\mathcal{O}[x]$ , and we can assume that  $f$  is also monic. The roots of  $f$  have the form  $\varphi(\alpha_i \delta_\beta)$  for  $\alpha_i \in \mathcal{O}$  with  $\gcd(\alpha_i, \beta) = 1$  and  $1 \leq i \leq r$  for some  $r$ . For  $\pi \in \mathcal{O}$  an odd prime, consider the polynomial

$$f_\pi(x) = \prod_{i=1}^r (x - \varphi(\pi \alpha_i \delta_\beta)).$$

Recall that  $xP_\beta(x^4)$  is separable by Theorem 2.1. It follows that  $A_\beta$  is separable over  $K$  and hence is separable modulo any prime of  $\mathcal{O}$  not dividing  $\text{disc}(A_\beta) \neq 0$ . For our purposes, we assume that the prime  $\pi \in \mathcal{O}$  satisfies

(A)  $\pi \equiv 1 \pmod{2(1+i)}$ .

- (B)  $\Lambda_\beta$  is separable modulo  $\pi$ .
- (C)  $\gcd(\pi, \beta) = 1$ .

First, we show that  $f_\pi \in \mathcal{O}[x]$ . Let  $\sigma \in \text{Gal}(K_\beta/K)$  and take a root  $\varphi(\pi\alpha_i\delta_\beta)$  of  $f_\pi$ . Since  $\alpha_i\delta_\beta$  and  $\pi\alpha_i\delta_\beta$  are  $\beta$ -torsion generators, Proposition 3.2 implies that there is  $\gamma \in \mathcal{O}$  relatively prime to  $\beta$  such that

$$\sigma(\varphi(\alpha_i\delta_\beta)) = \varphi(\gamma\alpha_i\delta_\beta), \quad \sigma(\varphi(\pi\alpha_i\delta_\beta)) = \varphi(\gamma\pi\alpha_i\delta_\beta) = \varphi(\pi\gamma\alpha_i\delta_\beta). \tag{15}$$

Since  $\varphi(\alpha_i\delta_\beta)$  is a root of  $f \in \mathcal{O}[x]$ , the left side of (15) implies that  $\varphi(\gamma\alpha_i\delta_\beta)$  is a root as well. Then  $\varphi(\pi\gamma\alpha_i\delta_\beta)$  is a root of  $f_\pi$  by definition. But this root is  $\sigma(\varphi(\pi\alpha_i\delta_\beta))$  by the right side of (15). It follows that  $\sigma$  permutes the roots of  $f_\pi$ , and then  $f_\pi(x) \in \mathcal{O}[x]$  follows easily.

We next prove the following claim:

$$f = f_\pi \quad \text{when } \pi \text{ satisfies (A), (B) and (C)}. \tag{16}$$

Suppose (16) is false. Since  $f$  and  $f_\pi$  are monic of the same degree and  $f$  is irreducible,  $f \neq f_\pi$  implies that  $f$  is coprime to  $f_\pi$ . The roots of  $f_\pi$  are also roots of  $\Lambda_\beta$ , so there exists a monic  $h \in \mathcal{O}[x]$  such that  $\Lambda_\beta = ff_\pi h$ . Let us analyze the roots of  $f_\pi \pmod{\pi}$ . From parts (5) and (6) of Theorem 2.1, we have

$$\begin{aligned} P_\pi(x^4) &= x^{N(\pi)-1} + a_1x^{N(\pi)-5} + \dots + a_{(N(\pi)-1)/4} \\ Q_\pi(x^4) &= a_{(N(\pi)-1)/4}x^{N(\pi)-1} + \dots + a_1x^4 + 1, \end{aligned} \tag{17}$$

where  $\pi$  divides all the coefficients  $a_j$ . Let  $\mathcal{O}_{K_\beta}$  be the ring of integers of  $K_\beta$  and let  $\mathfrak{P}$  be a prime ideal of  $\mathcal{O}_{K_\beta}$  dividing  $\pi\mathcal{O}_{K_\beta}$  and suppose that  $\varphi(\alpha_i\delta_\beta)$  is a root of  $f$ . Therefore

$$\varphi(\pi\alpha_i\delta_\beta) = \varphi(\alpha_i\delta_\beta) \frac{P_\pi(\varphi(\alpha_i\delta_\beta)^4)}{Q_\pi(\varphi(\alpha_i\delta_\beta)^4)}$$

in  $K_\beta$ . By (17), we may reduce this equality modulo  $\mathfrak{P}$  to get

$$\varphi(\pi\alpha_i\delta_\beta) \equiv \varphi(\alpha_i\delta_\beta)^{N(\pi)} \pmod{\mathfrak{P}}. \tag{18}$$

Let

$$\tilde{f}_\pi(x) = \prod_{i=1}^r (x - \varphi(\alpha_i\delta_\beta)^{N(\pi)}).$$

Then an argument similar to that given for  $f_\pi$  shows that  $\tilde{f}_\pi(x) \in \mathcal{O}[x]$ . By (18),  $f_\pi(x)$  and  $\tilde{f}_\pi(x)$  have the same roots in  $\mathcal{O}_{K_\beta}/\mathfrak{P}$  and hence

$$f_\pi \equiv \tilde{f}_\pi \pmod{\pi\mathcal{O}[x]}.$$

However,  $\tilde{f}_\pi$  is obtained from  $f$  by raising its roots to the  $N(\pi)^{\text{th}}$  power, and a standard argument implies that

$$\tilde{f}_\pi \equiv f \pmod{\pi\mathcal{O}[x]}.$$

(See [3, Lemma 9.1.8] for the case of a prime  $p \in \mathbb{Z}$ . The proof for a prime  $\pi \in \mathcal{O}$  is identical.) Combining these congruences shows that  $f_\pi \equiv f \pmod{\pi\mathcal{O}[x]}$ . Therefore,

$$A_\beta \equiv f f_\pi h \equiv f^2 h \pmod{\pi\mathcal{O}[x]},$$

which is to say that  $A_\beta$  is not separable modulo  $\pi$ . This contradicts our choice of  $\pi$  and allows us to conclude (16).

Now consider a root  $\varphi(\alpha_i \delta_\beta)$  of  $f$ . Let  $\eta$  be the product of all odd primes dividing  $\text{disc}(A_\beta)$  but not dividing  $\beta$ . If  $\varphi(\gamma \delta_\beta)$  is any root of  $A_\beta$ , then the Chinese remainder theorem implies that there is a Gaussian integer  $\omega$  such that

$$\omega \equiv \gamma \alpha_i^{-1} \pmod{\beta}, \quad \omega \equiv 1 \pmod{2(1+i)}, \quad \omega \equiv 1 \pmod{\eta}.$$

Therefore  $\omega$  is odd and we may factor  $\omega$  as  $\omega = \pi_1 \cdots \pi_k$  for odd, normalized primes  $\pi_j$  coprime to  $\beta \text{disc}(A_\beta)$ . Iterating (16) we have

$$f = f_{\pi_1} = f_{\pi_1 \pi_2} = \cdots = f_{\pi_1 \cdots \pi_k}.$$

Hence

$$\varphi(\gamma \delta_\beta) = \varphi(\gamma \alpha_i^{-1} \alpha_i \delta_\beta) = \varphi(\omega \alpha_i \delta_\beta) = \varphi(\pi_1 \cdots \pi_k \alpha_i \delta_\beta)$$

is a root of  $f_{\pi_1 \cdots \pi_k} = f$ . Thus  $A_\beta$  and  $f$  have the same roots; since both are monic and separable they must be equal. We conclude that  $A_\beta$  is irreducible over  $K$  as desired.  $\square$

**Corollary 4.8.** *Let  $\beta \in \mathcal{O}$  be odd. Then*

$$\text{Gal}(K_\beta/K) \simeq (\mathcal{O}/\beta\mathcal{O})^\times.$$

*In particular, if  $n$  is a positive, odd integer, then*

$$\text{Gal}\left(K\left(\varphi\left(\frac{2\varpi}{n}\right)\right)/K\right) \simeq (\mathcal{O}/n\mathcal{O})^\times.$$

**Proof.** The elementary part of Proposition 3.2 gives an injection

$$\text{Gal}(K_\beta/K) \hookrightarrow (\mathcal{O}/\beta\mathcal{O})^\times$$

(see (11)). Since  $K_\beta = K(\varphi(\delta_\beta))$ , Theorem 4.7 and Lemma 4.3 tell us that

$$|\text{Gal}(K_\beta/K)| = [K_\beta : K] = [K(\varphi(\delta_\beta)) : K] = \text{deg}(\Lambda_\beta(x)) = |(\mathcal{O}/\beta\mathcal{O})^\times|.$$

Therefore, our injection must be an isomorphism. The final assertion follows since  $K_n = K(\varphi(\frac{2\varpi}{n}))$  by definition.  $\square$

The final assertion of [Corollary 4.8](#) completes the elementary proof of the isomorphism [\(3\)](#) from the introduction.

**Remark 4.9.** Let  $\pi \in \mathcal{O}$  be an odd prime not dividing  $\beta$ , so that  $\pi$  is unramified in  $K_\beta$ . Under the isomorphism of [Corollary 4.8](#), some  $\sigma \in \text{Gal}(K_\beta/K)$  maps to  $[\pi] \in (\mathcal{O}/\beta\mathcal{O})^\times$ , where  $\sigma$  and  $\pi$  are linked via the equation

$$\sigma(\varphi(\delta_\beta)) = \varphi(\pi\delta_\beta).$$

If we assume in addition that  $N(\pi)$  is relatively prime to the index  $[\mathcal{O}_{K_\beta} : \mathcal{O}[\varphi(\delta_\beta)]]$ , then [\(18\)](#) easily implies that

$$\sigma(u) \equiv u^{N(\pi)} \pmod{\mathfrak{P}}$$

for any  $u \in \mathcal{O}_{K_\beta}$  and any prime  $\mathfrak{P}$  of  $\mathcal{O}_{K_\beta}$  dividing  $\pi\mathcal{O}_{K_\beta}$ . Since  $K_\beta/K$  is abelian, the Artin symbol  $((K_\beta/K)/\pi)$  is the unique element of  $\text{Gal}(K_\beta/K)$  with this property. Hence we have proved that

$$\left(\frac{K_\beta/K}{\pi}\right)(\varphi(\delta_\beta)) = \varphi(\pi\delta_\beta),$$

which shows that the isomorphism  $\text{Gal}(K_\beta/K) \simeq (\mathcal{O}/\beta\mathcal{O})^\times$  from [Corollary 4.8](#) can be identified with the Artin map.

Observe the key role played by [\(18\)](#) here and in the proof of [Theorem 4.7](#). If you look back at the proof, you will see that [\(18\)](#) follows from [\(17\)](#). Proving [\(17\)](#) is actually the hardest part of the proof of [Theorem 4.7](#). The proof of [\(17\)](#) given in [\[3, Theorem 15.4.8\]](#) follows Eisenstein’s original argument, which is both intricate and brilliant.

**Example 4.10.** Let us work out the case  $n = 5$ . The 5-division polynomial is

$$xP_5(x^4) = x^{25} + 50x^{21} - 125x^{17} + 300x^{13} - 105x^9 - 62x^5 + 5x.$$

We can factor 5 into normalized primes as  $5 = (-1 + 2i)(-1 - 2i)$ . Then

$$\begin{aligned} xP_5(x^4) &= A_1(x)A_{-1+2i}(x)A_{-1-2i}(x)A_5(x) \\ &= x(x^4 - 1 + 2i)(x^4 - 1 - 2i)(x^{16} + 52x^{12} - 26x^8 - 12x^4 + 1). \end{aligned}$$

Note that the constant terms of the factors are as predicted by [Proposition 4.5](#).

### 5. Abel’s theorem on the lemniscate

Our work in the previous section allows us to give a new, concise proof of Abel’s wonderful result about ruler and compass constructions on the lemniscate.

**Theorem 5.1** (Abel’s theorem on the lemniscate). *For a positive integer  $n$ , the  $n$ -division points of the lemniscate may be constructed using ruler and compass if and only if*

$$n = 2^k p_1 \cdots p_m,$$

where the  $p_i$  are distinct Fermat primes and  $k$  is a nonnegative integer.

**Proof.** We begin by reducing the equivalence. According to [3, Proposition 15.1.1], a point on the lemniscate is constructible if and only if its radial component is constructible. Therefore, constructing the  $n$ -division points is equivalent to constructing  $\varphi(\frac{2\varpi a}{n})$  for  $a = 1, \dots, n$ . We need not worry about all these points, as [3, Corollary 15.2.7] states that if  $\varphi(\frac{2\varpi}{n})$  is constructible, then  $\varphi(\frac{2\varpi a}{n})$  is constructible for all  $a \in \mathbb{Z}$ . Finally, [3, Proposition 15.2.3] allows us to conclude that  $\varphi(z)$  is constructible if and only if  $\varphi(z/2)$  is constructible. Hence we may assume  $n$  is odd.

Next observe that  $\Lambda_n \in \mathbb{Z}[x]$ . This follows since lemniscatic polynomials satisfy  $\overline{\Lambda_\beta} = \Lambda_{\bar{\beta}}$  with respect to complex conjugation. Then  $\Lambda_n$  is irreducible over  $\mathbb{Q}$  since it is irreducible over  $K$  by Theorem 4.7. Furthermore,  $\varphi(\frac{2\varpi}{n})$  is a root of  $\Lambda_n$  since  $\frac{2\varpi}{n}$  is an  $n$ -torsion generator (see the proof of Proposition 3.1). It follows that

$$\left[ \mathbb{Q}\left(\varphi\left(\frac{2\varpi}{n}\right)\right) : \mathbb{Q} \right] = \deg(\Lambda_n) = |(\mathcal{O}/n\mathcal{O})^\times| = n^2 \prod_{p|n} \left(1 - \frac{1}{p}\right) \left(1 - \left(\frac{-1}{p}\right)\frac{1}{p}\right), \tag{19}$$

where the last equality follows from [4, Example 7.29].

Now assume that  $\varphi(\frac{2\varpi}{n})$  is constructible. Then  $[\mathbb{Q}(\varphi(\frac{2\varpi}{n})) : \mathbb{Q}]$  is a power of 2 by [3, Corollary 10.1.8], so that by (19), we have

$$2^m = n^2 \prod_{p|n} \left(1 - \frac{1}{p}\right) \left(1 - \left(\frac{-1}{p}\right)\frac{1}{p}\right).$$

Since  $n$  is odd, this implies that  $n$  is a product of distinct primes  $p$ . If  $(-1/p) = -1$ , then  $(p - 1)(p + 1)$  is a power of 2, which forces  $p = 3$ , and if  $(-1/p) = 1$ , then  $(p - 1)^2$  is a power of 2, which easily implies that  $p$  is a Fermat prime.

Conversely, assume that  $n$  is a product of distinct Fermat primes. Observe that  $\varphi(\frac{2\varpi}{n}) \in K(\varphi(\frac{2\varpi}{n})) = K_n$ , which is Galois over  $\mathbb{Q}$  since  $K_n/K$  is Galois and  $\varphi(\frac{2\varpi}{n})$  is real. Then (19) shows that

$$[K_n : \mathbb{Q}] = 2 \left[ \mathbb{Q} \left( \varphi \left( \frac{2\varpi}{n} \right) \right) : \mathbb{Q} \right]$$

is a power of 2. Hence  $\varphi\left(\frac{2\varpi}{n}\right)$  is constructible by [3, Theorem 10.1.12].  $\square$

Other proofs of this theorem are due to Abel, Eisenstein and Rosen, though Rosen was the first to prove the “only if” part of the theorem. Rosen’s proof [9] uses class field theory, while the above proof uses only the irreducibility of the lemnatomic polynomial  $A_n$ , which was proved without class field theory in Theorem 4.7. The proofs of Abel and Eisenstein are discussed in [3, Section 15.5], with references to the original papers. See also the book [7] by Prasolov and Solov’ev.

### 6. Chebyshev polynomials

The analogy between Abel’s function  $\varphi(z)$  and the sine function  $\sin(\theta)$  has been recognized since the time of Gauss and Abel. For example, in his unpublished work on elliptic functions, Gauss wrote  $\varphi(z)$  as  $\sin \text{lemn}z$  (see [2]). Thus the analogy between lemnatomic polynomials and cyclotomic polynomials made earlier in this paper needs to be reconsidered from the point of view of the sine function. As we now show, the analog of the division polynomial  $xP_\beta(x^4)$  is the well-known *Chebyshev polynomial*  $T_n \in \mathbb{Z}[x]$ , which is defined by the identity

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

for a positive integer  $n$ .

**Lemma 6.1.** *If  $n$  is odd, then*

$$\sin(n\theta) = (-1)^{(n-1)/2} T_n(\sin(\theta)).$$

*Furthermore, there is  $S_n \in \mathbb{Z}[x]$  such that*

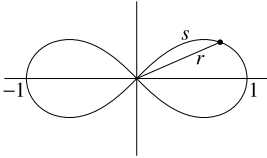
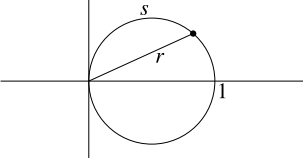
$$T_n(x) = xS_n(x^2),$$

*and the roots of  $T_n(x) = xS_n(x^2)$  are  $\sin(a\frac{2\pi}{n})$  for  $[a] \in \mathbb{Z}/n\mathbb{Z}$ .*

**Proof.** Since  $n$  is odd, the addition laws for  $\sin$  and  $\cos$  imply that

$$\begin{aligned} \sin(n\theta) &= \cos\left(n\theta - \frac{\pi}{2}\right) = \cos\left(n\left(\theta - \frac{\pi}{2}\right) + \frac{n-1}{2}\pi\right) = \cos\left(n\left(\theta - \frac{\pi}{2}\right)\right) (-1)^{(n-1)/2} \\ &= (-1)^{(n-1)/2} T_n\left(\cos\left(\theta - \frac{\pi}{2}\right)\right) = (-1)^{(n-1)/2} T_n(\sin(\theta)). \end{aligned}$$

**Table 1**  
The Lemniscate and the circle.

	Lemniscate	Circle
Polar equation	$r^2 = \cos(2\theta)$	$r = \cos(\theta)$
Graph		
Arc length	$s = \int_0^r \frac{dt}{\sqrt{1-t^4}}$	$s = \int_0^r \frac{dt}{\sqrt{1-t^2}}$
Inverse function	$r = \varphi(s)$	$r = \sin(s)$
Differential equation	$\varphi'(z)^2 + \varphi(z)^4 = 1$	$\cos(\theta)^2 + \sin(\theta)^2 = 1$
Multiplication map ( $\beta, n$ odd)	$\varphi(\beta z) = (-1)^\varepsilon \varphi(z) \frac{P_\beta(\varphi(z)^4)}{Q_\beta(\varphi(z)^4)}$	$\sin(n\theta) = (-1)^{(n-1)/2} \sin(\theta) S_n(\sin(\theta)^2)$
Galois group ( $\beta, n$ odd)	$\text{Gal}(K(\varphi(\frac{2\pi}{\beta}))/K) \simeq (\mathcal{O}/\beta\mathcal{O})^\times$	$\text{Gal}(\mathbb{Q}(\sin(\frac{2\pi}{n}))/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

The formula for  $\sin(n\theta)$  implies that 0 is a root of  $T_n$ . Since  $\sin(n\theta)/\sin(\theta)$  is an even function, it follows that  $T_n(x)/x$  is also even and hence is a polynomial in  $x^2$ . The assertion concerning the roots of  $T_n$  is equally easy and is omitted.  $\square$

Notice how  $\sin(n\theta) = (-1)^{(n-1)/2} \sin(\theta) S_n(\sin(\theta)^2)$ ,  $n$  odd, is analogous to the formula for  $\varphi(\beta z)$ ,  $\beta$  odd, from part (1) of [Theorem 2.1](#), where  $n \equiv (-1)^{(n-1)/2} \pmod 4$  corresponds to  $\beta \equiv i^\varepsilon \pmod{2(1+i)}$ . Also, the crucial identity (12) used in the proof of [Proposition 3.2](#) is the lemniscatic analog of the identity  $\cos(\theta - \frac{\pi}{2}) = \sin(\theta)$  used in the proof of [Lemma 6.1](#).

The analogy between  $\varphi(z)$  and  $\sin(\theta)$  actually begins with the equations  $r^2 = \cos(2\theta)$  and  $r = \cos(\theta)$  that define the lemniscate and circle of radius  $1/2$  centered at  $(1/2, 0)$ . [Table 1](#) shows how these curves lead naturally to the functions  $\varphi(z)$  and  $\sin(\theta)$  and also records some of the similarities between their properties. (See also [\[6, 8.2\]](#) for another view of the analogy between  $\varphi(z)$  and  $\sin(\theta)$ .)

This analogy suggests in particular that the lemnatomic polynomials  $A_\beta$  should correspond to the irreducible factors of the Chebyshev polynomial  $T_n$  when  $n$  is odd. The factors of  $T_n$  were studied by Hsiao [\[5\]](#) in 1984. Since  $T_n$  is not monic, he used the monic polynomial

$$C_n(x) = 2T_n(x/2) \in \mathbb{Z}[x].$$

Hsiao determines the irreducible factorization of  $C_n$  over  $\mathbb{Q}$  [\[5, Proposition 1\]](#). When  $n$  is odd, his result may be restated as a factorization

$$C_n = \prod_{k|n} D_k, \tag{20}$$

where  $D_n$  has degree  $\phi(n)$  (the Euler  $\phi$ -function) and is given by

$$D_n(x) = \prod_{[a] \in (\mathbb{Z}/n\mathbb{Z})^\times} \left( x - 2 \sin \left( a \frac{2\pi}{n} \right) \right). \tag{21}$$

Note the analogy with [Definition 4.1](#). Thus, when  $n$  is odd, (20) is the analog of [Proposition 4.4](#), where the irreducibility of  $D_n$  corresponds to the irreducibility of  $\Lambda_\beta$  proved in [Theorem 4.7](#). Although Hsiao’s proof of irreducibility ultimately rests on the irreducibility of cyclotomic polynomials, we note that the polynomials  $D_n$  may be shown irreducible over  $\mathbb{Q}$  directly by adapting the proof of [Theorem 4.7](#). We also note that in one of his unpublished papers, Schur [[12](#), p. 423] mentions very briefly (without proof) the irreducible decomposition of Chebyshev polynomials

Hsiao also studied the constant term of the factors of  $C_n$ . When  $n$  is odd, his result can be stated as follows [[5](#), [Proposition 2](#)].

**Proposition 6.2.** *Let  $n \in \mathbb{Z}$  be odd and positive. If  $n = p^k$  for a prime  $p$ , then  $|D_n(0)| = p$ . Otherwise,  $D_n(0) = 1$ .*

By tweaking Hsiao’s proof, one can show that when  $p$  is an odd prime and  $k \geq 1$ , we have  $D_{p^k}(0) = (-1)^{(p-1)/2} p$ . Since  $(-1)^{(p-1)/2} p \equiv 1 \pmod 4$ , we see that  $(-1)^{(p-1)/2} p$  is the analog of a normalized prime  $\pi \in \mathcal{O}$ , so that [Proposition 6.2](#) is the analog of [Proposition 4.5](#). In fact, [Proposition 4.5](#) was inspired by Hsiao’s result.

[Proposition 6.2](#) and (21) imply that  $2 \sin(\frac{2\pi}{n})$  is a unit when  $n > 1$  is odd and not a prime power. This is closely related to the standard fact that  $1 - \zeta_n$  ( $\zeta_n = e^{2\pi i/n}$ ) is a unit when  $n > 1$  is not a prime power (see [[14](#), [Proposition 2.8](#)]). To see why, note that  $1 - \zeta_n = \zeta_{2n} \zeta_{2n}^{-1} - \zeta_{2n}^2 = -i \zeta_{2n} \cdot 2 \sin(\frac{\pi}{n})$ .

For further results on the factorization of Chebyshev polynomials, see [[8](#)]. There is also another interesting analogy to consider, this one involving the *Carlitz polynomials*  $[M](X)$  for  $M \in \mathbb{F}_p[T][X]$ . The irreducible factors of Carlitz polynomials have a lot in common with lemnatomic and cyclotomic polynomials. See [[1](#)] for more details.

For more on the history and number theory associated to the lemniscate, the reader should consult Schappacher’s article *Some Milestones of Lemniscatomy* [[11](#)].

**Acknowledgments**

The results of Section 4 are based on the Amherst College senior honors thesis of the second author, written under the direction of the first author. We are grateful to Amherst College for the Post-Baccalaureate Summer Research Fellowship that supported the writing of this paper. We would like to thank Rosario Clement and Keith Conrad for useful conversations. The comments by Keith Conrad, Franz Lemmermeyer and Michael Rosen on earlier versions of the paper are greatly appreciated. We are also grateful to the referee for helpful suggestions.



## References

- [1] K. Conrad, Carlitz extensions, available at <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/carlitz.pdf>.
- [2] D.A. Cox, The arithmetic-geometric mean of Gauss, *Enseign. Math.* 30 (1984) 275–330.
- [3] D.A. Cox, *Galois Theory*, 2nd edition, Wiley, Hoboken, 2012.
- [4] D.A. Cox, *Primes of the Form  $x^2 + ny^2$* , 2nd edition, Wiley, Hoboken, 2013.
- [5] H.-J. Hsiao, On factorization of Chebyshev’s polynomials of the first kind, *Bull. Inst. Math. Acad. Sin.* 12 (1984) 89–94.
- [6] F. Lemmermeyer, *Reciprocity Laws*, Springer-Verlag, New York, Berlin, Heidelberg, 2000.
- [7] V. Prasolov, Y. Solovyev, *Elliptic Functions and Elliptic Integrals*, AMS, Providence, RI, 1997.
- [8] M.O. Rayes, V. Trevisan, P.S. Wang, Factorization properties of Chebyshev polynomials, *Comput. Math. Appl.* 50 (2005) 1231–1240.
- [9] M. Rosen, Abel’s theorem on the lemniscate, *Amer. Math. Monthly* 88 (1981) 387–395.
- [10] N. Schappacher, On the history of Hilbert’s twelfth problem: a comedy of errors, in: *Matériaux pour l’histoire des mathématiques au XX<sup>e</sup> siècle*, Nice, 1996, in: *Sémin. Congr.*, vol. 3, Soc. Math. France, Paris, 1998, pp. 243–273.
- [11] N. Schappacher, Some milestones of lemniscatomy, in: *Algebraic Geometry: Proceedings of Bilkent Summer School*, in: *Lect. Notes Pure Appl. Math.*, vol. 193, Marcel Dekker, New York, 1997, pp. 257–290.
- [12] I. Schur, Arithmetisches über Tschebyscheffens Polynome, in: *Gesammelte Abhandlungen*, vol. III, Springer-Verlag, New York, Berlin, Heidelberg, 2000, pp. 422–453.
- [13] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, Berlin, Heidelberg, 1994.
- [14] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, Berlin, Heidelberg, 1982.