eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
FACULTY OF SCIENCE AND TECHNOLOGY
UNIVERSITY OF THE BASQUE COUNTRY

The Galois Theory of The Lemniscate

Final Degree Dissertation
Degree in Mathematics

Josu Pérez Zarraonandia

Supervisor:
Josu Sangroniz Gómez

Leioa, June 21, 2022

Contents

Introduction

Geometric constructions with straightedge and compass go as far back as to the time of the ancient Greeks and Egyptians. In fact, there are three classical problems in Greek mathematics related to straightedge and compass constructions which were extremely important in the development of geometry, which are the squaring of a circle, the duplication of a cube, and the trisection of an angle. These three problems are impossible to solve with straightedge and compass, but the Greeks lacked the mathematical development needed to prove this.

The proof of the impossibility of these problems had to await the mathematics of the 19-th century, in particular to the development of Galois theory. In 1837 Pierre Wantzel published a paper in which he proved that duplication of a cube and the trisection of an angle are impossible to solve with straightedge and compass. The imposibility of the squaring of the circle will have to await until 1882 when Ferdinand von Lindemann proved that π is trascendental.

In his paper of 1837, Pierre Wantzel also characterized which regular polygons are constructible with straightedge and compass. Sufficiency was proved by Gauss in 1796, but Wantzel was the first to prove the characterization, in a theorem now known as the Gauss-Wantzel Theorem.

Theorem 0.1 (Gauss-Wantzel Theorem)**.** *A regular polygon with n sides is constructible if and only if $n = 2^m p_1 \dots p_r$ where $m \geq 0$ and p_i are Fermat primes.*

It is remarkable that in 1827, in his *Recherches sur les fonctions elliptiques*, Abel proved a similar sufficient condition for the constructibility of points that divide the lemniscate curve into arcs of equal lengths. However, it was not until the modern development of Class Field Theory that in 1981 Michael Rosen proved the complete characterization, which is known as Abel's Theorem on the lemniscate.

Theorem 0.2 (Abel's Theorem)**.** *The lemniscate can be divided into n equal parts with ruler and compass if and only if $n = 2^m p_1 \dots p_r$ where $m \geq 0$ and p_i are Fermat primes.*

It turns out that it is not required to use the full power of Class Field Theory to prove this result. In fact, one can define the lemniscate sine function similarly as one defines the sine function with respect to the circle, and then, consider the field extensions that arise when adjoining to $\mathbb{Q}(i)$ particular values of this function, as it is done when studying cyclotomic fields. It turns out that studying this extensions is enough to prove Abel's Theorem.

The similarities between the cyclotomic fields and the lemniscatic extensions go further than one can initially expect. The cyclotomic fields are abelian extensions of $\mathbb{Q}$, and there is also a partial converse to this, known as the Kronecker-Weber Theorem.

Theorem 0.3 (Kronecker-Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained within some cyclotomic field.*

Similarly, it turns out that the lemniscatic extensions are also abelian extensions but of $\mathbb{Q}(i)$, and every other abelian extension of $\mathbb{Q}(i)$ is contained in some lemniscatic extension. This is covered in the following theorem, due to Takagi (1903).

Theorem 0.4 (Takagi)**.** *Every finite abelian extension of $\mathbb{Q}(i)$ is contained within some lemniscatic extension.*

In general, given a number field K, the problem of knowing what algebraic numbers are necessary to construct all abelian extensions of K is known as Kronecker's Jugendtraum or Hilbert's twelfth problem, and it remains unsolved in this generality. However, the result is known for example when K is a quadratic imaginary field. The study of the abelian extensions of $\mathbb{Q}(i)$, the lemniscatic case, is interesting because it points towards the direction that one needs to go in order to prove Kronecker's Jugendtraum when K is a quadratic imaginary field.

In Chapter 1 we start with the definition of the lemniscate curve and the lemniscate sine function sl. The function sl is defined initially in a small interval of $\mathbb{R}$, and we work our way on extending the function to $\mathbb{C}$. Also, we study the most important properties of this function, which are the addition formula and the formulas for the multiplication by Gaussian integers. Our main reference for this chapter is the book [Cox12] by David A. Cox.

Once we have studied the function sl, we proceed to study the lemniscatic extensions in Chapter 2, which are the extensions that arise when adjoining special values of sl to $\mathbb{Q}(i)$. After studying their main properties and characterizing their Galois groups, we will be able to prove Abel's Theorem. Here we will still follow [Cox12] mostly, but also [CH14] and [Ros13].

It turns out that sl is an elliptic function, and this lets us use the powerful theory of elliptic functions to study the lemniscatic extensions. Chapter 3 is all about elliptic curves and elliptic functions, and our main reference for this topic has been the book [Kob84] by Neal Koblitz. However, we have also made use of the standard references in this topic, which are the books [Sil86], [Sil94] and [ST15] by Joseph Silverman and John Tate.

Straightedge and compass constructions have not been covered in the four year degree, and Appendix A is written with the aim to fill this lack of content and ensure the work is self-contained. This appendix is interesting on its own, because we give proofs for the three classical Greek problems mentioned previously and the Gauss-Wantzel Theorem.

Appendix B contains a set of solved problems about the lemniscate and the lemniscate sine function. Some of these problems are also about using the tehniques learnt in Chapter 1 to study the regular sin function and deduce some of its properties, which are similar to the ones proved in that chapter for sl.

Notation is standard and we assume the results studied in the mathematics degree, specially those concerning Linear Algebra, Commutative Algebra, Galois Theory and Number Theory.

Chapter 1

The Lemniscate

In this chapter we introduce the curve known as lemniscate and the lemniscate functions. The lemniscate functions play a role similar to that played by the sine and cosine functions in the study of the circle, but in the study of the lemniscate.

1.1 Definition and arc length

Definition 1.1. The *lemniscate* is the locus of all the points whose product of distances to two given points, the *focuses*, is constant.

If the focuses of the lemniscate are $(\pm a, 0)$ and the product of the distances is b^2, its cartesian equation is

$$(x^2 + y^2)^2 = b^4 - a^4 + 2a^2(x^2 - y^2).$$

From now on, we will only consider the lemniscate given by the constants $b = a = 1/\sqrt{2}$. The cartesian equation for this lemniscate simplifies to

$$(x^2 + y^2)^2 = x^2 - y^2,$$

which in polar coordinates is written as

$$r^2 = \cos 2\theta.$$

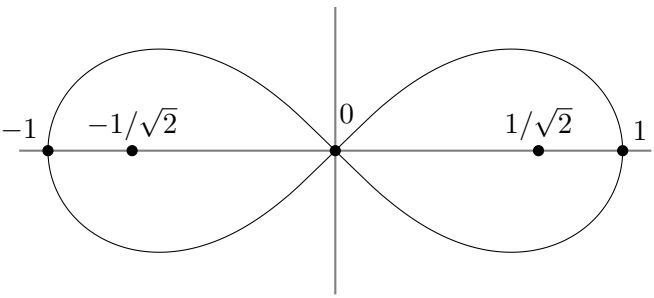

Figure 1.1: Lemniscate for $a = b = 1/\sqrt{2}$.

Notice that for $\cos 2\theta$ to be positive, we need $\theta \in [-\pi/4, \pi/4]$. To set the points in the lemniscate for negative $\cos 2\theta$, we allow $r < 0$ in this convention of polar coordinates. This means that any $(r, \theta) \in \mathbb{R}^2$ will be the polar coordinates of (x, y) if $x = r\cos\theta$ and $y = r\sin\theta$. Notice that with this agreement, (r, θ) and $(-r, \theta + \pi)$ are the polar coordinates of the same point.

Theorem 1.1. *The length L of the lemniscate is given by*

$$L = 4\int_0^1 \frac{dt}{\sqrt{1-t^4}}. \tag{1.1}$$

Proof. Using the standard formula for the arc length of a curve given in polar coordinates and the fact that the lemniscate is symmetric we get

$$L = 4\int_0^{\pi/4} \frac{d\theta}{\sqrt{\cos 2\theta}}.$$

The result is achieved after the change $t = \sqrt{\cos 2\theta}$. □

Let us define the constant $\varpi = L/2$, similarly as π is half the circumference of a circle with radius 1. This constant will play an important role in the following chapters.

Definition 1.2. The *lemniscatic constant* ϖ is $\varpi = L/2$.

Observe that ϖ is defined in terms of the integral in (1.1), and notice that π can be defined by a similar integral too:

$$\varpi = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}}, \quad \pi = 2\int_0^1 \frac{dt}{\sqrt{1-t^2}}.$$

In fact, both of these integrals are convergent since $t \in [0, 1)$ implies that

$$\int_0^1 \frac{dt}{\sqrt{1-t^4}} \leq \int_0^1 \frac{dt}{\sqrt{1-t^2}} \leq \int_0^1 \frac{dt}{\sqrt{1-t}} = 2.$$

There are other interesting facts about the lemniscate which are left as problems (see Problems 1 and 2) because they are not strictly necessary for our purposes.

1.2 The lemniscate sine function

We now proceed to define the lemniscate sine function. The regular sine function can be defined as the inverse function of the arcsin function, and similarly, we will define the lemniscate sine function as the inverse function of some integral function measuring the arc length.

Definition 1.3. Define the function arcsl: $[-1,1] \to [-\varpi/2, \varpi/2]$ by

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

By the fundamental theorem of calculus arcsl is continuous on $[-1,1]$ and differentiable in $(-1,1)$. In particular, for $r \in (-1,1)$

$$\operatorname{arcsl}'(r) = \frac{1}{\sqrt{1-r^4}} > 0,$$

and as a consequence arcsl is invertible in $(-1,1)$, with continuous and differentiable inverse.

Definition 1.4. Define the lemniscate sine function as the inverse of arcsl, that is, sl: $[-\varpi/2, \varpi/2] \to [-1,1]$ given by $\operatorname{sl}(u) = \operatorname{arcsl}^{-1}(u)$.

The next figure shows a geometric interpretation of arcsl and sl, and the similarities they present with arcsin and sin respectively.

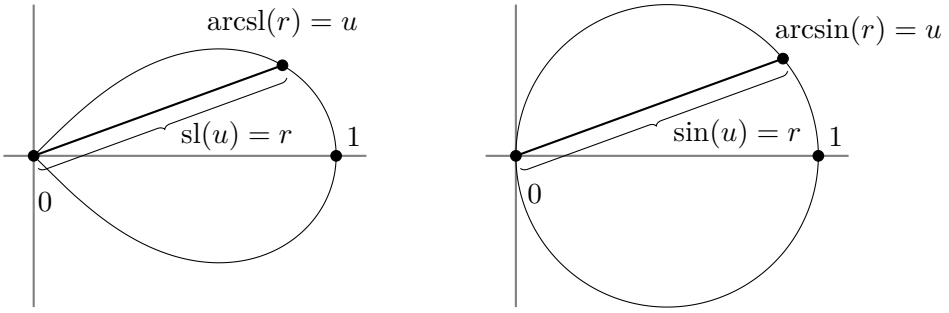

Figure 1.2: Geometric interpretation of the lemniscate sinus.

Proposition 1.2. $\operatorname{sl}'(u) = \sqrt{1-\operatorname{sl}^4(u)}$ *for* $u \in (-\varpi/2, \varpi/2)$. *Furthermore,* $\operatorname{sl}'_-(\varpi/2) = \operatorname{sl}'_+(-\varpi/2) = 0$.

Proof. The first part is obtained by applying the inverse function theorem. Observe that if $h > 0$ is small, then

$$h = \int_{\operatorname{sl}(\varpi/2-h)}^{\operatorname{sl}(\varpi/2)} \frac{dt}{\sqrt{1-t^4}}.$$

Take $c \in [\operatorname{sl}(\varpi/2-h), \operatorname{sl}(\varpi/2)]$, given by the mean value theorem, such that

$$h = \frac{\operatorname{sl}(\varpi/2) - \operatorname{sl}(\varpi/2-h)}{\sqrt{1-c^4}}.$$

Then,

$$\operatorname{sl}_-(\varpi/2) = \lim_{h\to 0^+} \frac{\operatorname{sl}(\varpi/2-h) - \operatorname{sl}(\varpi/2)}{-h} = \lim_{h\to 0^+} \sqrt{1-c^4},$$

and the result follows since $c \to 1$ as $h \to 0$. The other case is similar. □

Proposition 1.3. $\mathrm{sl}''(u) = -2\mathrm{sl}^3(u)$ *for* $u \in (-\varpi/2, \varpi/2)$. *Furthermore,* $\mathrm{sl}''_-(\varpi/2) = -2$ *and* $\mathrm{sl}''_+(-\varpi/2) = 2$.

Proof. Differentiating $(\mathrm{sl}'(u))^2 = 1 - \mathrm{sl}^4(u)$ and using that $\mathrm{sl}'(u) \neq 0$ in $(-\varpi/2, \varpi/2)$ we obtain the first result. When $h > 0$ is small, there exists some $c \in (\varpi/2 - h, \varpi/2)$ given by the mean value theorem such that

$$\frac{\mathrm{sl}'_-(\varpi/2) - \mathrm{sl}'(\varpi/2 - h)}{h} = \mathrm{sl}''(c) = -2\mathrm{sl}^3(c).$$

Then

$$\mathrm{sl}''_-(\varpi/2) = \lim_{h\to 0^+} \frac{\mathrm{sl}'(\varpi/2 - h) - \mathrm{sl}'_-(\varpi/2)}{-h} = \lim_{h\to 0^+} -2\mathrm{sl}^3(c),$$

and the result follows since $c \to \varpi/2$ as $h \to 0$. The other case is similar. □

Now we want to extend sl to the whole $\mathbb{R}$ in such a way that sl is differentiable and periodic in $\mathbb{R}$. In order to do that, we use the following fact about functions defined by reflections.

Lemma 1.4. *Let* φ *be a twice differentiable function defined to the left of a point* a *that has zero left derivative and second left derivate at that point. Then, the extension of* φ *obtained by reflection with respect to* $x = a$ *is twice differentiable at* a.

Proof. Extend φ to the right of a by $\varphi(a + x) = \varphi(a - x)$ for $x \in [0, \epsilon)$ with $\epsilon > 0$ sufficiently small. Then,

$$\varphi'_+(a) = \lim_{h\to 0^+} \frac{\varphi(a + h) - \varphi(a)}{h} = \lim_{h\to 0^+} \frac{\varphi(a - h) - \varphi(a)}{h} = -\varphi'_-(a) = 0,$$

so φ is differentiable at a and $\varphi'(a) = 0$. Similarly, for the second derivative of φ at a,

$$\varphi''_+(a) = \lim_{h\to 0^+} \frac{\varphi'(a + h) - \varphi'(a)}{h} = \lim_{h\to 0^+} \frac{\varphi'(a - h)}{-h} = \varphi''_-(a),$$

so φ' is differentiable at a. □

Theorem 1.5. sl *can be extended to a twice differentiable periodic function on* $\mathbb{R}$ *with period* 2ϖ.

Proof. First, extend sl to $(\varpi/2, 3\varpi/2]$ by reflecting with respect to $\varpi/2$, so that $\mathrm{sl}(\varpi/2 + x) = \mathrm{sl}(\varpi/2 - x)$ for $x \in [0, \varpi]$. By the previous lemma, this extension is twice differentiable in $(-\varpi/2, 3\varpi/2)$. Observe that since $\mathrm{sl}'(\varpi/2 + x) = \mathrm{sl}'(\varpi/2 - x)$ for $x \in (0, \varpi)$, $\mathrm{sl}'_+(-\varpi/2) = \mathrm{sl}'_-(3\varpi/2) = 0$, and similarly we deduce $\mathrm{sl}''_+(-\varpi/2) = \mathrm{sl}''_-(3\varpi/2) = 0$.

Then, define $\mathrm{sl}(x + 2k\varpi) = \mathrm{sl}(x)$ for any $k \in \mathbb{Z}$ and $x \in [-\varpi/2, 3\varpi/2]$. By construction, it is clear that sl is twice differentiable in any interval of

the form $(-\varpi/2 + 2k\varpi, 3\varpi/2 + 2k\varpi)$ for $k \in \mathbb{Z}$, so it remains to show that sl is twice differentiable at the points $\varpi/2 + 2k\varpi$.

Notice that by periodicity it suffices to check double differentiability at $-\varpi/2$. Now, this follows by periodicity too, since $\mathrm{sl}'_-(-\varpi/2) = \mathrm{sl}'_-(3\varpi/2)$ and $\mathrm{sl}''_-(-\varpi/2) = \mathrm{sl}''_-(3\varpi/2)$. □

Observe that by construction $\mathrm{sl}(-x) = -\mathrm{sl}(x)$ for $x \in [-\varpi/2, 3\varpi/2]$, so by periodicity this property holds for all $x \in \mathbb{R}$. In particular, this implies that $\mathrm{sl}(0) = \mathrm{sl}(\varpi) = 0$, so by periodicity $\mathrm{sl}(k\varpi) = 0$ for $k \in \mathbb{Z}$. Analogously, one deduces that $\mathrm{sl}'(k\varpi/2) = 0$ for k odd.

Similarly, this construction implies that the formulas given in Propositions 1.2 and 1.3 for the first and second derivatives of sl and sl″ are valid for all $x \in \mathbb{R}$.

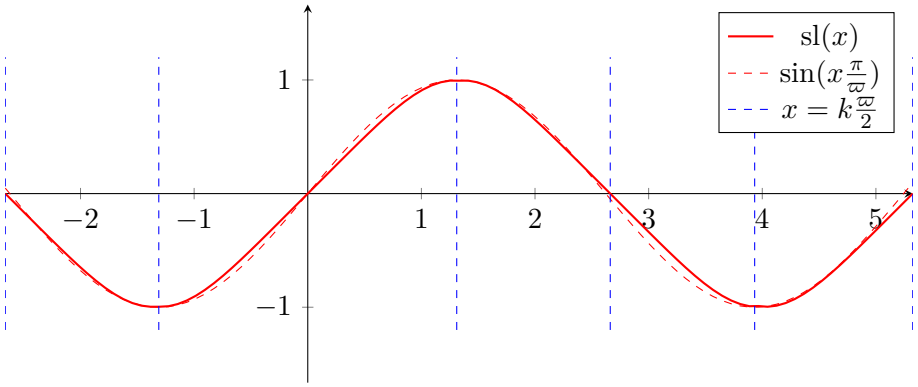

Figure 1.3: Plot of $\mathrm{sl}(x)$ in the interval $[-\varpi, 2\varpi]$ in comparison with the plot of $\sin(x\frac{\pi}{\varpi})$.

Our next goal is to prove the addition formula for sl, which relates the values of $\mathrm{sl}(x + y)$, $\mathrm{sl}(x)$ and $\mathrm{sl}(y)$. In order to do that, we will use the following lemma.

Lemma 1.6. *Let g be a twice differentiable function defined on $\mathbb{R}^2$. Then $g(x, y) = g(x + y, 0)$ if and only if $\partial g/\partial x = \partial g/\partial y$.*

Proof. The first condition is equivalent to $h(x) = g(x, a - x)$ being constant for any fixed a. Indeed, if $g(x, y) = g(x + y, 0)$, then $g(x, a - x) = g(a, 0)$, and so, $h(x) = g(a, 0)$ is constant for any fixed a.

Conversely, assume $h(x) = g(x, a - x)$ is constant for each fixed a. Then, $h(x) = h(a)$ implies $g(x, a - x) = g(a, 0)$, so by taking $a = x + y$ we obtain $g(x, y) = g(x + y, 0)$. Finally, since

$$h'(x) = \frac{\partial g}{\partial x}(x, a - x) - \frac{\partial g}{\partial y}(x, a - x),$$

it is clear that h is constant (for any a) if and only if $\partial g/\partial x = \partial g/\partial y$. □

Theorem 1.7 (Addition formula for sl)**.** *For any $x, y \in \mathbb{R}$,*

$$\mathrm{sl}(x+y) = \frac{\mathrm{sl}(x)\mathrm{sl}'(y) + \mathrm{sl}'(x)\mathrm{sl}(y)}{1 + \mathrm{sl}^2(x)\mathrm{sl}^2(y)}.$$

Proof. Consider the twice differentiable function in $\mathbb{R}^2$ given by

$$g(x,y) = \frac{\mathrm{sl}(x)\mathrm{sl}'(y) + \mathrm{sl}'(x)\mathrm{sl}(y)}{1 + \mathrm{sl}^2(x)\mathrm{sl}^2(y)}.$$

It is routine to check that $\partial g/\partial x = \partial g/\partial y$ using the formulas for sl' and sl''. As $g(x+y,0) = \mathrm{sl}(x+y)$, the result now follows by applying the previous lemma. □

Theorem 1.8. $\mathrm{sl}(u)$ *can be obtained from* $\mathrm{sl}(2u)$ *by extractions of square roots and arithmetic operations. In fact, if* $A = 4/\mathrm{sl}^2(2u)$*, then*

$$\mathrm{sl}(u) = \pm\sqrt{\frac{-A \mp \sqrt{A^2-16} \pm \sqrt{\left(-A \pm \sqrt{A^2-16}\right)^2 + 16}}{4}}.$$

Proof. Using the addition formula for $x = y = u$, we obtain a quartic equation $x^4 + Ax^3 + 2x^2 - Ax + 1 = 0$, where $x = \mathrm{sl}^2(u)$ and $A = 4/\mathrm{sl}^2(2u)$. The change $y = x - 1/x$ transforms this equation into $y^2 + Ay + 4 = 0$, which is then easily solved. □

Remark 1.1. Observe that the last theorem implies that the midpoint of an arc of the lemniscate with constructible endpoints is also constructible. Indeed, by the addition formula, if $\mathrm{sl}(x)$ and $\mathrm{sl}(y)$ are constructible, then so is $\mathrm{sl}(x+y)$, and by applying the last theorem, $\mathrm{sl}((x+y)/2)$ is also constructible (see Appendix A).

Notice also that if (r,θ) is a point in polar coordinates of the lemniscate and r is constructible, then the point is constructible too. Indeed, since r is constructible, so is $r^2 = \cos 2\theta = 2\cos^2\theta - 1$. Hence, $\cos\theta = \sqrt{(r^2+1)/2}$ and $\sin\theta = \sqrt{1-\cos^2\theta}$ are constructible, from which follows that both $x = r\cos\theta$ and $y = r\sin\theta$ are constructible.

Thanks to the previous remark, we are able to divide the lemniscate into 2^n equal points for any n. For example, for $n = 3$ this is equivalent to computing $\mathrm{sl}(2\varpi/8) = \mathrm{sl}(\varpi/4)$, which can be obtained from $\mathrm{sl}(\varpi/2) = 1$ by applying the previous formula with $A = 4$. Taking into account that $\mathrm{sl}(\varpi/4)$ is a positive real number, we get

$$\mathrm{sl}(\varpi/4) = \sqrt{\sqrt{2}-1}.$$

1.3 Multiplication by Integers.

As it can be seen in Problem 6, there exist some recurrence formulas to compute $\sin(mx)$ for $m \in \mathbb{Z}$, which depend on some polynomials $P_m(x)$. In this section, we aim to show that similar recurrence formulas and polynomials exist for $\mathrm{sl}(mx)$.

Lemma 1.9. *For any $x, y \in \mathbb{R}$,*

$$\mathrm{sl}(x+y) + \mathrm{sl}(x-y) = \frac{2\mathrm{sl}(x)\mathrm{sl}'(y)}{1+\mathrm{sl}^2(x)\mathrm{sl}^2(y)}.$$

Proof. It follows directly from applying the addition formula to compute $\mathrm{sl}(x+y)$ and $\mathrm{sl}(x-y)$, and summing the results afterwards. □

Proposition 1.10. *There exist rational functions $R_m \in \mathbb{Q}[x]$, with $m \in \mathbb{N}$, such that*

$$\mathrm{sl}(mx) = \begin{cases} \mathrm{sl}(x)R_m(\mathrm{sl}(x^4)), & \text{if } m \text{ is odd;} \\ \mathrm{sl}(x)\mathrm{sl}'(x)R_m(\mathrm{sl}(x^4)), & \text{if } m \text{ is even.} \end{cases}$$

Proof. By induction. The cases $m = 0$ and $m = 1$ trivially hold by considering the polynomials $R_0(x) = 0$ and $R_1(x) = 1$. Now let $m \geq 1$ and assume the result is true for $n \leq m$. Applying the previous lemma, we get

$$\mathrm{sl}((m+1)x) + \mathrm{sl}((m-1)x) = \frac{2\mathrm{sl}(mx)\mathrm{sl}'(x)}{1+\mathrm{sl}^2(mx)\mathrm{sl}^2(x)}.$$

Then, if $m+1$ is odd, applying the induction hypothesis (using that m is even and $m-1$ is odd) and using the formula for $\mathrm{sl}'(x)$, we obtain

$$\mathrm{sl}((m+1)x) = \mathrm{sl}(x)R_{m+1}(\mathrm{sl}^4(x)),$$

where

$$R_{m+1}(x) = \frac{2(1-x)R_m(x)}{1+x(1-x)R_m^2(x)} - R_{m-1}(x). \tag{1.2}$$

Similarly, when $m+1$ is even, we obtain

$$\mathrm{sl}((m+1)x) = \mathrm{sl}(x)\mathrm{sl}'(x)R_{m+1}(\mathrm{sl}^4(x)),$$

where

$$R_{m+1}(x) = \frac{2R_m(x)}{1+xR_m^2(x)} - R_{m-1}(x). \tag{1.3}$$

□

Note that formulas (1.2) and (1.3) define recurrence relations to compute these functions.

Proposition 1.11. *There exist coprime polynomials $P_m, Q_m \in \mathbb{Z}[x]$ such that $R_m = P_m/Q_m$ and $Q_m(0) = 1$. Moreover, these polynomials are unique.*

Proof. Uniqueness is clear since $\mathbb{Z}[x]$ is a UFD with only two units, ± 1. Since $R_m \in \mathbb{Q}[x]$, it is clear that we can write it as p_m/q_m where $p_m, q_m \in \mathbb{Z}[x]$. Formulas (1.2) and (1.3) define recurrence relations for the polynomials p_m and q_m, in fact,

$$q_{m+1}(x) = \begin{cases} q_{m-1}(x)(q_m^2(x) + x\ (1-x)p_m^2(x)), & \text{if } m+1 \text{ is odd;} \\ q_{m-1}(x)(q_m^2(x) + x\ p_m^2(x)), & \text{if } m+1 \text{ is even.} \end{cases}$$

In both cases, $q_{m+1}(0) = q_{m-1}(0)q_m^2(0)$, and so, it is clear by induction that $q_m(0) = 1$. After removing common factors, we can write $R_m = P_m/Q_m$ where $P_m, Q_m \in \mathbb{Z}[x]$ are coprime. Since $Q_m(0)|q_m(0)$, we can take P_m and Q_m so that $Q_m(0) = 1$. □

Since P_m and Q_m are uniquely determined, we are able to make the following definition.

Definition 1.5. The polynomials $xP_n(x^4)$, for n odd, and $x(1-x^2)P_n(x^4)$, for n even, are called the nth *division polynomials* of the lemniscate.

As it is shown in Problem 7, the real roots of these polynomials (with modulus smaller than or equal to 1) are $\mathrm{sl}(m\frac{2\varpi}{n})$, with $m \in \mathbb{Z}$ and $|m| \leq n/4$. Division polynomials also have complex roots, and in order to understand them we need to extend sl to the complex plane.

1.4 The Complex Lemniscate Function.

Before extending sl to $\mathbb{C}$, we study the extension of arcsl to the complex plane. In order to do that, we compute its Taylor series.

Proposition 1.12. *The Taylor series of* arcsl *for $x \in (-1, 1)$ is*

$$\mathrm{arcsl}(x) = \sum_{n=0}^{\infty} \frac{(-1)^n(2n-1)!!}{(4n+1)2^n n!} x^{4n+1}.$$

Proof. Recall that

$$\mathrm{arcsl}(x) = \int_0^x \frac{dt}{\sqrt{1-t^4}}.$$

Consider the function $f(x) = (1-x)^{-1/2}$, so that $\mathrm{arcsl}'(x) = f(x^4)$. For $x \in (-1, 1)$ its Taylor series is the following binomial series

$$f(x) = \sum_{n=0}^{\infty} \binom{-1/2}{n} (-x)^n = \sum_{n=0}^{\infty} \frac{(-1)^n(2n-1)!!}{2^n n!} x^n.$$

Then, since $\operatorname{arcsl}'(x) = f(x^4)$, it follows that

$$\operatorname{arcsl}(x) = \int_0^x f(t^4)dt = \sum_{n=0}^{\infty} \frac{(-1)^n(2n-1)!!}{(4n+1)2^n n!} x^{4n+1}.$$

□

Corollary 1.13. *The function* arcsl *can be extended to the disk* $|z| < 1$ *by means of the Taylor series*

$$\operatorname{arcsl}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n(2n-1)!!}{(4n+1)2^n n!} z^{4n+1}. \tag{1.4}$$

Proof. Clearly this Taylor series defines an analytic function in the disk $|z| < 1$, and it is clear by the previous proposition that it extends the real function arcsl. □

Lemma 1.14. $\operatorname{arcsl}(iz) = i \cdot \operatorname{arcsl}(z)$ *for* z *in the disk* $|z| < 1$.

Proof. It follows directly by plugging iz into the Taylor series (1.4). □

Since arcsl is holomorphic in the disk $|z| < 1$ and $\operatorname{arcsl}'(0) \neq 0$, there is a holomorphic function g defined on a disk $|z| < \epsilon$ which is the local inverse of arcsl.

Recall that the local inverse of arcsl in the interval $(-\epsilon, \epsilon) \subset \mathbb{R}$ is sl, so g and sl coincide in this interval by uniqueness of the inverse function. Thus, we consider g to be the extension of sl to the disk $|z| < \epsilon$, which we also denote sl.

Since $\operatorname{arcsl}(\operatorname{sl}(z)) = z$ for $|z| < \epsilon$, then $\operatorname{arcsl}(i \cdot \operatorname{sl}(z)) = i \cdot \operatorname{arcsl}(\operatorname{sl}(z)) = iz$. Consequently, $\operatorname{sl}(iz) = \operatorname{sl}(\operatorname{arcsl}(i \cdot \operatorname{sl}(z))) = i \cdot \operatorname{sl}(z)$ for $|z| < \epsilon$. This suggests that the extension of $\operatorname{sl}(z)$ satisfies $\operatorname{sl}(iz) = i \cdot \operatorname{sl}(z)$ in the extended domain of sl.

In order to extend sl to the largest possible domain in $\mathbb{C}$ we will take a different approach. The previous paragraph suggests that we should have $\operatorname{sl}(iy) = i \cdot \operatorname{sl}(y)$ for any real y, and since we also want the addition law to hold for complex numbers, there is only one possible definition for $\operatorname{sl}(x+iy)$ that satisfies these conditions.

Definition 1.6. Define the complex lemniscate sin function by

$$\operatorname{sl}(z) = \operatorname{sl}(x+iy) = \frac{\operatorname{sl}(x)\operatorname{sl}'(y) + i \cdot \operatorname{sl}(x)\operatorname{sl}'(y)}{1 - \operatorname{sl}^2(x)\operatorname{sl}^2(y)}. \tag{1.5}$$

Notice that this function indeed extends sl, since by plugging $y = 0$ in the previous formula we recover the real lemniscate sinus.

The idea behind formula (1.5) is that we are applying the complex addition formula to x and iy, taking into account that $\operatorname{sl}(iy) = i \cdot \operatorname{sl}(y)$ and $\operatorname{sl}'(iy) = \operatorname{sl}'(y)$.

Proposition 1.15. $\mathrm{sl}(iz) = i \cdot \mathrm{sl}(z)$ *for any complex* $z \in \mathbb{C}$.

Proof. Applying formula (1.5) to $iz = -y + ix$, one can check that indeed $\mathrm{sl}(iz) = i \cdot \mathrm{sl}(z)$. □

In what follows, we study the properties of sl as a complex function.

Theorem 1.16. *The function* sl *is holomorphic for all* $z \neq (m+in)\frac{\varpi}{2}$, *were* $m, n \in \mathbb{Z}$ *are odd.*

Proof. sl is not defined when the denominator of (1.5) vanishes, that is, when $\mathrm{sl}^2(x) = \mathrm{sl}^2(y) = 1$. In this case, $x = m\frac{\varpi}{2}$ and $y = n\frac{\varpi}{2}$, for some odd integers m and n. Now assume $z \neq (m+in)\frac{\varpi}{2}$ and write $\mathrm{sl}(z) = u(x,y) + i \cdot v(x,y)$ where

$$u(x,y) = \frac{\mathrm{sl}(x)\mathrm{sl}'(y)}{1 - \mathrm{sl}^2(x)\mathrm{sl}^2(y)}, \quad v(x,y) = \frac{\mathrm{sl}(y)\mathrm{sl}'(x)}{1 - \mathrm{sl}^2(x)\mathrm{sl}^2(y)}.$$

In order to prove that sl is analytic at z, it suffices to show that $u(x,y)$ and $v(x,y)$ satisfy the Cauchy-Riemman equations. After some standard manipulations and using the real formulas for $\mathrm{sl}'(x)$ and $\mathrm{sl}''(x)$, one can check that indeed $\partial u/\partial x = \partial v/\partial y$ and $\partial u/\partial y = -\partial v/\partial x$. □

Theorem 1.17. *The addition formula holds for complex numbers: for all* $z, w \in \mathbb{C}$ *for which both sides of the equation are defined,*

$$\mathrm{sl}(z+w) = \frac{\mathrm{sl}(z)\mathrm{sl}'(w) + \mathrm{sl}(w)\mathrm{sl}'(z)}{1 + \mathrm{sl}^2(z)\mathrm{sl}^2(w)}.$$

Proof. Define the complex function

$$g(z,w) = \frac{\mathrm{sl}(z)\mathrm{sl}'(w) + \mathrm{sl}(w)\mathrm{sl}'(z)}{1 + \mathrm{sl}^2(z)\mathrm{sl}^2(w)}.$$

Consider $g(z, w_0)$ for any fixed $w_0 \in \mathbb{R}$. By the addition formula for real numbers, $g(z, w_0) = \mathrm{sl}(z + w_0)$ for any $z \in \mathbb{R}$. Then, by the identity theorem for complex functions, $g(z, w_0) = \mathrm{sl}(z + w_0)$ holds for any $z \in \mathbb{C}$ for which both functions are defined.

Now consider $g(z_0, w)$ for any fixed $z_0 \in \mathbb{C}$. By the previous paragraph, $g(z_0, w) = \mathrm{sl}(z_0 + w)$ for any $w \in \mathbb{R}$ where both functions are analytic. Then, by the identity theorem, $g(z_0, w) = \mathrm{sl}(z_0 + w)$ holds for any $w \in \mathbb{C}$ for which both functions are defined. As a consequence, $g(z, w) = \mathrm{sl}(z + w)$ for all $z, w \in \mathbb{C}$ for which both functions are defined. □

In the next two theorems we show that the relations satisfied by $\mathrm{sl}, \mathrm{sl}'$ and sl'' in the real case are also satisfied in the complex case.

Theorem 1.18. *For any* $z \in \mathbb{C}$ *such that* $z \neq (m+in)\frac{\varpi}{2}$, *where* $m, n \in \mathbb{Z}$ *are odd, we have* $(\mathrm{sl}'(z))^2 = 1 - \mathrm{sl}^4(z)$.

Proof. Define the function $g(z) = 1 - \mathrm{sl}^4(z)$. Since $\mathrm{sl}(z)$ is analytic, both $\mathrm{sl}'(z)$ and $\mathrm{sl}^4(z)$ are analytic, so in particular $g(z)$ is analytic too. Now, since $g(z) = (\mathrm{sl}'(z))^2$ for all $z \in \mathbb{R}$, it follows by the identity theorem that $g(z) = (\mathrm{sl}'(z))^2$ for all $z \in \mathbb{C}$ where the functions are defined. □

Theorem 1.19. *For any $z \in \mathbb{C}$ such that $z \neq (m + in)\frac{\varpi}{2}$, where $m, n \in \mathbb{Z}$ are odd, we have $\mathrm{sl}''(z) = -2 \cdot \mathrm{sl}^4(z)$.*

Proof. The proof is completely analogous to the one done in Theorem 1.18 □

The following theorem reveals that sl has some kind of periodicity over the Gaussian integers, and now we proceed to study it.

Theorem 1.20. *For any $m, n \in \mathbb{Z}$ we have that*

$$\mathrm{sl}(z + m\varpi + in\varpi) = (-1)^{n+m}\mathrm{sl}(z).$$

Proof. By the addition formula, we have that $\mathrm{sl}(z + \varpi) = -\mathrm{sl}(z)$ and $\mathrm{sl}(z + i\varpi) = -\mathrm{sl}(z)$. Then, by induction, $\mathrm{sl}(z + m\varpi) = (-1)^m\mathrm{sl}(z)$ and $\mathrm{sl}(z + in\varpi) = (-1)^n\mathrm{sl}(z)$, and consequently

$$\mathrm{sl}(z + m\varpi + in\varpi) = (-1)^m\mathrm{sl}(z + in\varpi) = (-1)^{n+m}\mathrm{sl}(z).$$

□

Definition 1.7. A Gaussian integer $\beta = a + bi \in \mathbb{Z}[i]$ is said to be *even* if $a \equiv b \pmod 2$, otherwise it is *odd*. Define the lattice $\mathcal{L}$ of even Gaussian integers by $\mathcal{L} = \{\beta \in \mathbb{Z}[i] \text{ such that } \beta \text{ is even}\}$.

Theorem 1.21. *$\mathcal{L} = \langle 1 \pm i \rangle$ as an additive subgroup of $\mathbb{Z}[i]$.*

Proof. Since the addition and substraction of even Gaussian integers is again even, it follows that $\mathcal{L}$ is an additive subgroup of $\mathbb{Z}[i]$. Thus, since $1 + i$ and $1 - i$ are even, it is clear that $\langle 1 \pm i \rangle \subseteq \mathcal{L}$.

To show that the converse, let $a + bi \in \mathcal{L}$. Since $a \equiv b \pmod 2$, there exists some $k \in \mathbb{Z}$ for which $a = b + 2k$. Then,

$$a + bi = (b + k)(1 + i) + k(1 - i) \in \langle 1 \pm i \rangle.$$

□

Theorem 1.22. *$\mathrm{sl}(z + \beta\varpi) = \mathrm{sl}(z)$ for all $\beta \in \mathcal{L}$.*

Proof. Let $\beta = a + bi \in \mathcal{L}$. Since $a \equiv b \pmod 2$, then $(-1)^{a+b} = 1$. The result follows by applying Theorem 1.20. □

The last theorem implies that sl is a meromorphic and double periodic function, with periods $1 \pm i$. This fact will be very important to relate the lemniscate to the theory of elliptic curves in Chapter 3, since it implies that sl is an elliptic function.

To end this chapter, we study the zeros and poles of sl.

Theorem 1.23. sl *is a meromorphic function on* $\mathbb{C}$ *with*

(i) *Simple zeros occurring at* $z = (m + in)\varpi$, *with* $m, n \in \mathbb{Z}$ *and*

(ii) *Simple poles occurring at* $z = (m + in)\frac{\varpi}{2}$, *with* $m, n \in \mathbb{Z}$ *odd.*

Proof. (i) If $\mathrm{sl}(z) = 0$, then by Theorem 1.18 $\mathrm{sl}'(z) \neq 0$ and thus the zeros are simple.

Let $z = x + iy$ be a zero of sl. By (1.5), $\mathrm{sl}(x)\mathrm{sl}'(y) = \mathrm{sl}(y)\mathrm{sl}'(x) = 0$. Assume $\mathrm{sl}(x) = 0$. Since $x \in \mathbb{R}$, then $x = m\varpi$ for some $m \in \mathbb{Z}$ and so $\mathrm{sl}'(x) \neq 0$. Thus, $\mathrm{sl}(y) = 0$, and so, $y = n\varpi$ for some $n \in \mathbb{Z}$, which implies that $z = (m + in)\varpi$.

On the other hand, if $\mathrm{sl}'(y) = 0$, since $y \in \mathbb{R}$ then $\mathrm{sl}(y) = \pm 1 \neq 0$ and so $\mathrm{sl}'(x) = 0$. This implies $\mathrm{sl}(x) = \pm 1$, and consequently, $1 - \mathrm{sl}^2(x)\mathrm{sl}^2(y) = 0$ and $\mathrm{sl}(z)$ is not defined, so this case doesn't occur.

(ii) By Theorem 1.16 we know that the poles are at $z = (m+in)\frac{\varpi}{2}$, with $m, n \in \mathbb{Z}$ odd, so it suffices to show that these poles are simple. To prove this, we will show that $1/\mathrm{sl}(z)$ has simple zeros at these points. Indeed, let z_0 be any of these points. Then, since

$$\left(\frac{d}{dz}\left(\frac{1}{\mathrm{sl}(z)}\right)\right)^2 = \left(\frac{\mathrm{sl}'(z)}{\mathrm{sl}^2(z)}\right)^2 = \frac{1 - \mathrm{sl}^4(z)}{\mathrm{sl}^4(z)} = \frac{1}{\mathrm{sl}^4(z)} - 1,$$

it folllows that the derivative at z_0 of $1/\mathrm{sl}(z)$ is different from zero, and thus they are simple zeros. □

1.5 Multiplication by Gaussian Integers.

Similarly as done in Section 1.3, we develop formulas to compute $\mathrm{sl}(\beta z)$, with $\beta \in \mathbb{Z}[i]$, in terms of some rational functions $R_\beta \in \mathbb{Q}(i)[z]$.

Lemma 1.24. *For any* $z, w \in \mathbb{C}$ *such that both sides of the equation are defined,*

$$\mathrm{sl}(z + w) + \mathrm{sl}(z - w) = \frac{2\mathrm{sl}(z)\mathrm{sl}'(w)}{1 + \mathrm{sl}^2(z)\mathrm{sl}^2(w)}.$$

Proof. It follows directly from applying the addition formula to compute $\mathrm{sl}(z + w)$ and $\mathrm{sl}(z - w)$, and summing the result afterwards. □

Proposition 1.25. *There exists a rational function $R_\beta \in \mathbb{Q}(i)[x]$, for each $\beta \in \mathbb{Z}[i]$, such that*

$$\mathrm{sl}(\beta z) = \begin{cases} \mathrm{sl}(z)R_\beta(\mathrm{sl}(z^4)), & \text{if } \beta \text{ is odd;} \\ \mathrm{sl}(z)\mathrm{sl}'(z)R_\beta(\mathrm{sl}(z^4)), & \text{if } \beta \text{ is even.} \end{cases}$$

Proof. Since $\mathrm{sl}(i^\epsilon \beta z) = i^\epsilon \mathrm{sl}(\beta z)$ for any $0 \leq \epsilon \leq 3$, it suffices to define R_β for one β among its associates, and then set $R_{i^\epsilon\beta} = i^\epsilon R_\beta$. Now we proceed by induction on $\mathrm{N}(\beta)$, the norm of β.

Take $R_0(x) = 0$, $R_1(x) = 1$ and $R_{1+i}(x) = (1+i)/(1-x)$ for the basis of the induction. Then, let $\beta \in \mathbb{Z}[i]$ and assume the result is true for $\alpha \in \mathbb{Z}[i]$ with $\mathrm{N}(\alpha) < \mathrm{N}\beta)$. Notice that if $\mathrm{N}\beta) > 2$ there exists some $0 \leq \epsilon \leq 3$ such that $\mathrm{N}i^\epsilon\beta - 2) < \mathrm{N}i^\epsilon\beta - 1) < \mathrm{N}\beta)$ (it suffices to take ϵ so that $\mathrm{Re}(i^\epsilon\beta) \geq 2$).

In a similar fashion to Proposition 1.10, apply Lemma 1.24 with $w = 1$ and $z = i^\epsilon\beta - 1$ to write $\mathrm{sl}(i^\epsilon\beta z)$ in terms of $\mathrm{sl}(i^\epsilon\beta z - 1)$ and $\mathrm{sl}(i^\epsilon\beta z - 2)$. Then, applying the induction hypothesis, taking into account that if $i^\epsilon\beta$ is odd (even) then $i^\epsilon\beta - 1$ is even (odd) and $i^\epsilon\beta - 2$ is odd (even), we obtain the following recurrence formulas (note that ϵ may vary for each β)

$$R_{i^\epsilon\beta}(x) = \begin{cases} \dfrac{2(1-x)R_{i^\epsilon\beta-1}(x)}{1 + x(1-x)R^2_{i^\epsilon\beta-1}(x)} - R_{i^\epsilon\beta-2}(x), & \text{if } \beta \text{ odd;} \\ \dfrac{2R_{i^\epsilon\beta-1}(x)}{1 + zR^2_{i^\epsilon\beta-1}(x)} - R_{i^\epsilon\beta-2}(x), & \text{if } \beta \text{ even.} \end{cases} \tag{1.6}$$

□

Proposition 1.26. *There exist coprime polynomials $P_\beta, Q_\beta \in \mathbb{Z}[i][x]$ such that $R_\beta = P_\beta/Q_\beta$ and $Q_\beta(0) = 1$.*

Proof. As in the previous proposition, it suffices to prove the result for one β among its associates, so given β, take $0 \leq \epsilon \leq 3$ so that one of the previous recurrence formulas applies.

Since $R_\beta \in \mathbb{Q}(i)[x]$, write it as p_β/q_β where $p_\beta, q_\beta \in \mathbb{Z}[i][x]$. The formulas given in (1.6) define recurrence relations for these polynomials, in fact, by taking $q_0(x) = 1$, $q_1(x) = 1$ and $q_{1+i}(x) = 1 - x$ we get

$$q_{i^\epsilon\beta}(x) = \begin{cases} q_{i^\epsilon\beta-2}(x)(q^2_{i^\epsilon\beta-1}(x) + x(1-x)p^2_{i^\epsilon\beta-1}(x)), & \text{if } \beta \text{ is odd;} \\ q_{i^\epsilon\beta-2}(x)(q^2_{i^\epsilon\beta-1}(x) + xp^2_{i^\epsilon\beta-1}(x)), & \text{if } \beta \text{ is even.} \end{cases}$$

So by induction we can assume $q_{i^\epsilon\beta}(0) = 1$. Since $\mathbb{Z}[i]$ is a UFD, then $\mathbb{Z}[i][x]$ is also a UFD, and so, we can remove common factors and write $R_{i^\epsilon\beta} = P_{i^\epsilon\beta}/Q_{i^\epsilon\beta}$ where $P_{i^\epsilon\beta}, Q_{i^\epsilon\beta} \in \mathbb{Z}[i][x]$ are coprime. Since $Q_{i^\epsilon\beta}(0)$ divides $q_{i^\epsilon\beta}(0)$, we can take these polynomials so that $Q_{i^\epsilon\beta}(0) = 1$. □

In what follows we assume β to be odd. Luckily, this assumption will be enough for our purposes, but this means that some interesting theorems in Chapter 2 will be only available for β odd. Fortunately, we recover full generality in Chapter 3.

Proposition 1.27. *Let $\beta \in \mathbb{Z}[i]$ be odd. There exists a unique $0 \leq \epsilon \leq 3$ such that $\beta \equiv i^\epsilon \pmod{2(1+i)}$, and for this ϵ, the expression $R_\beta = i^\epsilon P_\beta/Q_\beta$ in lowest terms with $Q_\beta(0) = 1$ is unique.*

Proof. Uniqueness of ϵ is clear because if $i^\epsilon \equiv 1 \pmod{2(1+i)}$, then $\epsilon = 0$. Without loss of generality, assume $\beta = n + mi$ with n odd and m even. Observe that $n + m \pm 1$ is a multiple of 4 for an appropiate sign, and so $n - m \pm 1 = n + m \pm 1 - 2m$ is also a multiple of 4. Thus, for some $z \in \mathbb{Z}[i]$,

$$(\beta \pm 1)(1 - i) = n + m \pm 1 - (n - m \pm 1)i = 4z = 2(1 + i)(1 - i)z,$$

and consequently $\beta \equiv \pm 1 \pmod{2(1+i)}$ and the existence of ϵ is proven.

For this ϵ, since the expression of $R_\beta = P_\beta/Q_\beta$, $Q_\beta(0) = 1$, in lowest terms is unique, by replacing $P_\beta(x)$ with $i^{-\epsilon}P_\beta(x)$, we can write $R_\beta = i^\epsilon P_\beta/Q_\beta$ in a unique way. □

Our next goal is to prove that P_β is monic. In order to do that, we need the following lemma.

Lemma 1.28. *Let $\beta \in \mathbb{Z}[i]$ be odd and take ϵ given by Proposition 1.27. Then*

$$\mathrm{sl}(\beta z) \cdot \mathrm{sl}\left(\beta z + \beta(1+i)\frac{\varpi}{2}\right) = i^{3+2\epsilon}.$$

Proof. Using the addition formula and the formula for sl', we get

$$\mathrm{sl}\left(z + \frac{\varpi}{2}\right)\mathrm{sl}\left(z + \frac{\varpi}{2}i\right) = i.$$

By replacing z with $z + \varpi/2$, and afterwards z with $i^{-\epsilon}\beta z$, we obtain

$$\mathrm{sl}(\beta z) \cdot \mathrm{sl}\left(\beta z + i^\epsilon(1+i)\frac{\varpi}{2}\right) = i^{3+2\epsilon}.$$

Finally, since $\beta \equiv i^\epsilon \pmod{2(1+i)}$ and $2(1+i)^2\varpi/2 = 2\varpi i$ is an even multiple of ϖ, we can replace i^ϵ by β in the last expression to obtain

$$\mathrm{sl}(\beta z) \cdot \mathrm{sl}\left(\beta z + \beta(1+i)\frac{\varpi}{2}\right) = i^{3+2\epsilon}.$$

□

This lemma is interesting on its own, since for $\beta = 1$, $\epsilon = 0$ and we get $\mathrm{sl}(z)\cdot\mathrm{sl}(z+(1+i)\varpi/2) = -i$, from where we can deduce the value of $1/\mathrm{sl}(z)$.

Theorem 1.29. *P_β is monic for $\beta \in \mathbb{Z}[i]$ odd.*

Proof. Let $w = z + (1+i)\varpi/2$. By the previous lemma, $\mathrm{sl}(z)\cdot\mathrm{sl}(w) = i^3$ and $\mathrm{sl}(\beta z)\cdot\mathrm{sl}(\beta w) = i^{3+2\epsilon}$, with ϵ given by Proposition 1.27. Then,

$$\frac{P_\beta(\mathrm{sl}^4(z))}{Q_\beta(\mathrm{sl}^4(z))} = \frac{\mathrm{sl}(\beta z)}{i^\epsilon \mathrm{sl}(z)} = \frac{i^\epsilon \mathrm{sl}(w)}{\mathrm{sl}(\beta w)} = \frac{Q_\beta(1/\mathrm{sl}^4(z))}{P_\beta(1/\mathrm{sl}^4(z))}.$$

Since P_β and Q_β are polynomials, the formula $P_\beta(x)P_\beta(1/x) = Q_\beta(x)Q_\beta(1/x)$ holds for every $x \in \mathbb{C}$, since it holds for infinitely many values of x. Now let $\deg(P_\beta) = d$ and $\deg(Q_\beta) = e$. Then,

$$x^e P_\beta(x)(x^d P_\beta(1/x)) = x^d Q_\beta(x)(x^e Q_\beta(1/x)),$$

so by taking degrees $d = e$. Furthermore, since $P_\beta(x)$ and $Q_\beta(x)$ are coprime, it follows that $x^d Q_\beta(1/x)$ divides $P_\beta(x)$, so we can write $P_\beta(x) = \lambda x^d Q_\beta(1/x)$ for some $\lambda \in \mathbb{Z}[i]$. Evaluating at $x = 1$ we obtain

$$\lambda = \frac{P_\beta(1)}{Q_\beta(1)} = \frac{P_\beta(\mathrm{sl}^4(\varpi/2))}{Q_\beta(\mathrm{sl}^4(\varpi/2))} = \frac{\mathrm{sl}(\beta\varpi/2)}{i^\epsilon \mathrm{sl}(\varpi/2)} = \frac{\mathrm{sl}(\beta\varpi/2)}{i^\epsilon}.$$

Since $\beta \equiv i^\epsilon \pmod{2(1+i)}$, then $\mathrm{sl}(\beta\varpi/2) = i^\epsilon$, so $\lambda = 1$ and thus $P_\beta(x) = x^d Q_\beta(1/x)$. Since $Q_\beta(0) = 1$, it follows that P_β is monic. □

Recall that if $\beta \in \mathbb{Z}[i]$ is odd then $\mathrm{sl}(\beta z) = \mathrm{sl}(z)R_\beta(\mathrm{sl}(z^4))$. In particular, $\mathrm{sl}(\beta z) = 0$ if and only if $\mathrm{sl}(z)P_\beta(\mathrm{sl}^4(z)) = 0$, so in order to study these roots we will study the polynomials $xP_\beta(x^4)$.

The last goal of this chapter will be to compute the degree of $xP_\beta(x^4)$ for β odd.

Definition 1.8. For any $\beta \in \mathbb{Z}[i]$ odd, the monic polynomial given by $D_\beta(x) = xP_\beta(x^4)$ is called the *β-division polynomial* of the lemniscate.

Proposition 1.30. *Let $\beta \in \mathbb{Z}[i]$ be odd. Then the set of roots of D_β is $Z_\beta = \{\mathrm{sl}(z) \mid \mathrm{sl}(\beta z) = 0\}$, which is also given by*

$$Z_\beta = \left\{\mathrm{sl}\left(\frac{\gamma}{\beta}\varpi\right) \mid \gamma \in \mathbb{Z}[i]\right\} = \left\{\mathrm{sl}\left(\frac{\gamma}{\beta}\varpi\right) \mid \gamma \in \mathbb{Z}[i] \text{ is odd}\right\}. \tag{1.7}$$

Furthermore, the roots of D_β are simple, and so $\deg(D_\beta) = |Z_\beta|$.

Proof. Let $B_\beta(x) = Q_\beta(x^4)$. Since P_β and Q_β are coprime, so are D_β and B_β. Therefore, since $\mathrm{sl}(\beta z) = i^\epsilon D_\beta(\mathrm{sl}(z))/B_\beta(\mathrm{sl}(z))$ and sl is surjective (this is proven in Corollary 3.4 of Chapter 3), it is clear that the roots of D_β are Z_β.

Furthermore, since the zeros of sl are $\gamma\varpi$ for $\gamma \in \mathbb{Z}[i]$, it is clear that the first equality in (1.7) holds.

Finally, observe that if $\gamma \in \mathbb{Z}[i]$ is even, then $-\gamma+\beta$ is odd, and so we can write $\mathrm{sl}(\frac{\gamma}{\beta}\varpi) = \mathrm{sl}(\frac{-\gamma+\beta}{\beta}\varpi)$ in terms of odd Gaussian integers, proving the last equality.

Since $\mathrm{sl}(\beta z) = i^{\epsilon} D_\beta(\mathrm{sl}(z))/B_\beta(\mathrm{sl}(z))$ and all roots of sl are simple, we conclude that all roots of D_β are simple too. □

Lemma 1.31. $\mathrm{sl}(z) = \mathrm{sl}(z')$ *if and only if* $z' = (-1)^{n+m}z + (n+mi)\varpi$.

Proof. If $z' = (-1)^{n+m}z + (n+mi)\varpi$ then it is clear that $\mathrm{sl}(z) = \mathrm{sl}(z')$. Conversly, assume $\mathrm{sl}(z) = \mathrm{sl}(z')$, in which case $\mathrm{sl}'(z') = \pm\mathrm{sl}'(z)$. Depending on the sign of the last equality, it follows by the addition law that one of $\mathrm{sl}(z+z')$ or $\mathrm{sl}(z-z')$ is zero, so $z' = \pm z + (n+mi)\varpi$, with $n, m \in \mathbb{Z}$. Using that $\mathrm{sl}(z) = \mathrm{sl}(z')$, we deduce that the sign is given by $(-1)^{n+m}$. □

Proposition 1.32. *Let* $\gamma, \gamma' \in \mathbb{Z}[i]$ *be odd. Then* $\mathrm{sl}(\frac{\gamma}{\beta}\varpi) = \mathrm{sl}(\frac{\gamma'}{\beta}\varpi)$ *if and only if* $\gamma \equiv \gamma' \pmod{\beta}$. *In particular,* $|Z_\beta| = |\mathbb{Z}[i]/(\beta)|$.

Proof. Assume $\mathrm{sl}(\frac{\gamma}{\beta}\varpi) = \mathrm{sl}(\frac{\gamma'}{\beta}\varpi)$. Then, by the previous lemma, $\gamma' - (-1)^{n+m}\gamma = \beta(n+mi)$, and by studying the parity at both sides, it follows that $(-1)^{n+m} = 1$, and so, $\gamma \equiv \gamma' \pmod{\beta}$.

Conversely, if $\gamma \equiv \gamma' \pmod{\beta}$ then $\gamma' = \gamma + \beta(n+mi)$. Again, by studying parity $n+m$ is even, so $\gamma' = (-1)^{n+m}\gamma + \beta(n+mi)$ and applying the previous lemma we get the desired result.

This shows that the map from Z_β to $\mathbb{Z}[i]/(\beta)$ sending $\mathrm{sl}(\frac{\gamma}{\beta}\varpi)$ to $\overline{\gamma}$ is injective. But, since β is odd, any element in $\mathbb{Z}[i]/(\beta)$ can be represented by an odd Gaussian integer, so the map is bijective and $|Z_\beta| = |\mathbb{Z}[i]/(\beta)|$. □

Although the next result is a particular case of a well-known result in number theory, we include a proof for completeness.

Proposition 1.33. *Let* $\beta \in \mathbb{Z}[i]$ *be odd, then* $|\mathbb{Z}[i]/(\beta)| = \mathrm{N}(\beta)$. *In particular,* $\deg(P_\beta) = (\mathrm{N}(\beta)-1)/4$.

Proof. Let $\alpha \in \mathbb{Z}[i]$ be nonzero and write $\alpha = m(a+bi)$ with $\gcd(a,b) = 1$. By Bezout's identity, take $c, d \in \mathbb{Z}$ such that $ad - bc = 1$. Then, consider the map $\varphi\colon \mathbb{Z}[i] \to \mathbb{Z} \oplus \mathbb{Z}$ given by

$$\mu + \gamma i \mapsto (\mu, \gamma) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Clearly it is a group homomorphism, and it is bijective because the matrix is invertible over $\mathbb{Z}$ (its determinant is $ad - bc = 1$), so φ is an isomorphism.

One can check that $\varphi(\alpha) = (m, 0)$ and $\varphi(\alpha i) = (-m(ac+bd), m(a^2+b^2))$. Consequently, the image of the ideal (α) is

$$\begin{aligned}\varphi((\alpha)) &= \varphi(\langle \alpha, \alpha i\rangle) = \langle \varphi(\alpha), \varphi(\alpha i)\rangle = \\ &= \langle (m,0), (-m(ac+bd), m(a^2+b^2))\rangle = \langle (m,0), (0, m(a^2+b^2))\rangle,\end{aligned}$$

and since φ is an isomorphism, it follows that

$$\frac{\mathbb{Z}[i]}{(\alpha)} \simeq \frac{\mathbb{Z} \oplus \mathbb{Z}}{\langle (m,0), (0, m(a^2+b^2)) \rangle} \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m(a^2+b^2)}.$$

In particular, by taking cardinals we get

$$\left| \frac{\mathbb{Z}[i]}{(\alpha)} \right| = \left| \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m(a^2+b^2)} \right| = m^2(a^2+b^2) = \mathrm{N}(\alpha).$$

As a consequence, $\deg(D_\beta) = \mathrm{N}(\beta)$ by the previous proposition, and since $\deg(D_\beta) = 1 + 4\deg(P_\beta)$, we get that $\deg(P_\beta) = (\mathrm{N}(\beta) - 1)/4$. □

Chapter 2

Lemniscatic Extensions

In this chapter we study the extensions $\mathbb{Q}(i, \mathrm{sl}(2\varpi/\beta))/\mathbb{Q}(i)$ for $\beta \in \mathbb{Z}[i]$ odd. As an important application, we prove Abel's theorem on the lemniscate, which is the analogue of Theorem A.12 for the lemniscate.

2.1 Lemniscatic Extensions

In this section we study the extensions $\mathbb{Q}(i, \mathrm{sl}(2\varpi/\beta))/\mathbb{Q}(i)$ for $\beta \in \mathbb{Z}[i]$ odd, similarly as done in Problem 8 for the extensions $\mathbb{Q}(i, \sin(2\pi/n))/\mathbb{Q}(i)$ with n odd. As a consequence, we will prove sufficiency in Abel's theorem.

Definition 2.1. Let $\beta \in \mathbb{Z}[i]$ be odd. The *β-th lemniscatic extension* is $L_\beta/\mathbb{Q}(i)$ where $L_\beta = \mathbb{Q}(i, \mathrm{sl}(2\varpi/\beta))$.

Theorem 2.1. *$L_\beta/\mathbb{Q}(i)$ is a Galois extension.*

Proof. We aim to show that L_β is the splitting field of $D_\beta \in \mathbb{Q}(i)[x]$ over $\mathbb{Q}(i)$. Recall that the roots of D_β are Z_β, given by

$$Z_\beta = \{\mathrm{sl}(\frac{\gamma}{\beta}\varpi) | \gamma \in \mathbb{Z}[i] \text{ is odd}\}. \tag{2.1}$$

Then, $Z_\beta = \{\mathrm{sl}(\frac{2\gamma}{\beta}\varpi) | \gamma \in \mathbb{Z}[i]\} = \{\mathrm{sl}(\frac{2\gamma}{\beta}\varpi) | \gamma \in \mathbb{Z}[i] \text{ is odd}\}$. For the first equality, replace γ by $\beta - \gamma$ in (2.1), and then, replace γ by $\gamma + \beta$ when γ is even. Then, for any odd $\gamma \in \mathbb{Z}[i]$, we have that

$$\mathrm{sl}\left(\frac{2\gamma}{\beta}\varpi\right) = \mathrm{sl}\left(\frac{2\varpi}{\beta}\right) R_\gamma\left(\mathrm{sl}\left(\frac{2\varpi}{\beta}\right)^4\right) \in L_\beta,$$

so L_β is the splitting field of D_β and consequently Galois over $\mathbb{Q}(i)$. □

Theorem 2.2. *$\mathrm{Gal}(L_\beta/\mathbb{Q}(i))$ is abelian. Furthermore, it is isomorphic to a subgroup of $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$.*

Proof. Let $G = \mathrm{Gal}(L_\beta/\mathbb{Q}(i))$ and $\sigma \in G$. Since σ permutes the roots of D_β, $\sigma(\mathrm{sl}(2\varpi/\beta)) = \mathrm{sl}(2\gamma\varpi/\beta)$ for some odd $\gamma \in \mathbb{Z}[i]$. Then, if $\mathrm{sl}(2\gamma\varpi/\beta) = \mathrm{sl}(2\alpha\varpi/\beta)$ for some $\alpha \in \mathbb{Z}[i]$ odd, by applying Proposition 1.32, it follows that $\gamma \equiv \alpha \pmod{\beta}$, so γ is well defined mod β. We denote σ by σ_γ. Using that σ is an automorphism, we get

$$\begin{aligned}(\sigma_\gamma \circ \sigma_\alpha)(\mathrm{sl}(2\varpi/\beta)) &= \sigma_\gamma(\sigma_\alpha(\mathrm{sl}(2\varpi/\beta))) = \sigma_\gamma(\sin(2\alpha\varpi/\beta)) = \\ &= \sigma_\gamma(\mathrm{sl}(2\varpi/\beta)R_\alpha(\mathrm{sl}^4(2\varpi/\beta))) = \\ &= \mathrm{sl}(2\gamma\varpi/\beta)R_\alpha(\mathrm{sl}^4(2\gamma\varpi/\beta)) = \mathrm{sl}(2\gamma\alpha\varpi/\beta),\end{aligned}$$

that is, $\sigma_\gamma \circ \sigma_\alpha = \sigma_{\alpha\gamma}$. The inverse of σ_γ is of the form σ_α, and since $\sigma_\gamma \circ \sigma_\alpha = \sigma_{\gamma\alpha} = \sigma_1$, it follows that $\gamma\alpha \equiv 1 \pmod{\beta}$, and in particular $\gamma \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$. Putting it all together, we conclude that the map $\rho\colon G \to (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ given by $\sigma_\gamma \mapsto \overline{\gamma}$ is a monomorphism. □

In fact, the homomorphism ρ given in the previous proof is an isomorphism, but we still need some work to prove this result. However, knowing that ρ is an injective homomorphism is enough to prove sufficiency in Abel's theorem. In order to do this, we need to know the order of the group $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$.

Lemma 2.3. *Let $\beta \in \mathbb{Z}[i]$ and assume $\beta = \pi_1^{e_1} \dots \pi_r^{e_r}$ is the factorization of β as a product of prime elements in $\mathbb{Z}[i]$. Then $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ is isomorphic to the direct product $\otimes_j(\mathbb{Z}[i]/\pi_j^{e_j}\mathbb{Z}[i])^\times$.*

Proof. It is a direct application of the Chinese Reminder Theorem. □

Theorem 2.4. *Let $\beta \in \mathbb{Z}[i]$. Then*

$$|(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times| = N(\beta)\prod_{\pi|\beta}\left(1 - \frac{1}{N(\pi)}\right),$$

where π runs over the irreducible factors of β.

Proof. Let $\pi \in \mathbb{Z}[i]$ be prime. Since $\mathbb{Z}[i]$ is a principal ideal domain, we have Bezout's identity, and as a consequence,

$$(\mathbb{Z}[i]/\pi^e\mathbb{Z}[i])^\times = (\mathbb{Z}[i]/\pi^e\mathbb{Z}[i])\backslash(\pi\mathbb{Z}[i]/\pi^e\mathbb{Z}[i]).$$

But, as a group, $\pi\mathbb{Z}[i]/\pi^e\mathbb{Z}[i] \simeq \mathbb{Z}[i]/\pi^{e-1}\mathbb{Z}[i]$, thus $|(\mathbb{Z}[i]/\pi^e\mathbb{Z}[i])^\times| = \mathrm{N}(\pi^e) - \mathrm{N}(\pi^{e-1}) = \mathrm{N}(\pi^e)(1 - 1/\mathrm{N}(\pi))$. Consequently, if $\beta = \pi_1^{e_1} \dots \pi_r^{e_r}$ is the factorization of β as a product of prime elements in $\mathbb{Z}[i]$, then, by applying the previous lemma we get that

$$\begin{aligned}|(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times| &= \prod_{j=1}^r |(\mathbb{Z}[i]/\pi_j^{e_j}\mathbb{Z}[i])^\times| = \prod_{j=1}^r \mathrm{N}(\pi_j^{e_j})\left(1 - \frac{1}{\mathrm{N}(\pi_j)}\right) = \\ &= \mathrm{N}(\beta)\prod_{j=1}^r\left(1 - \frac{1}{\mathrm{N}(\pi_j)}\right).\end{aligned}$$

□

Proposition 2.5. *Let $n \in \mathbb{N}$ be odd. Then*

$$|(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times| = \varphi(n)n \prod_{p\equiv 3}\left(1+\frac{1}{p}\right)\prod_{p\equiv 1}\left(1-\frac{1}{p}\right),$$

where p runs over the prime factors of n and the congruences are mod 4.

Proof. Recall that the odd primes in $\mathbb{Z}[i]$ are the rational primes $p \equiv 3 \pmod 4$ and $a+bi$ with $a^2+b^2 \equiv 1 \pmod 4$ a rational prime. Assume $n = p_1^{e_1}\dots p_r^{e_r}\alpha_1^{t_1}\dots\alpha_s^{t_s}$, where p_i are primes of the first kind and $\alpha_j = a_j + b_j i$ primes of the second kind. Notice that if $a+bi$ divides n, then $a-bi$ divides n too, so $p = a^2+b^2$ divides n and the factor $(1-1/(a^2+b^2))$ appears twice in the product of the previous theorem. Applying this theorem,

$$\begin{aligned}|(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times| &= \mathrm{N}(n)\prod_{i=1}^{r}\left(1-\frac{1}{p_i^2}\right)\prod_{j=1}^{s}\left(1-\frac{1}{a_j^2+b_j^2}\right)^2 = \\ &= n^2\prod_{p\equiv 3}\left(1-\frac{1}{p^2}\right)\prod_{p\equiv 1}\left(1-\frac{1}{p}\right)^2 = \\ &= \varphi(n)n\prod_{p\equiv 3}\left(1+\frac{1}{p}\right)\prod_{p\equiv 1}\left(1-\frac{1}{p}\right),\end{aligned}$$

where we have used that

$$\varphi(n) = n\prod_{p\mid n}\left(1-\frac{1}{p}\right).$$

□

Corollary 2.6. *Let $n \in \mathbb{N}$ be odd. Then $(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times$ is a 2-group if and only if n is a product of different Fermat primes.*

Proof. By the previous proposition, $\varphi(n)$ divides $|(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times|$, so if this number is a power of 2, then $\varphi(n) = 2^m$ and as in Theorem A.5, it follows that n is product of different Fermat primes. Conversely, assume $n = p_1\dots p_r$ with p_i Fermat primes. By the previous proposition,

$$\begin{aligned}|(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times| &= \varphi(n)n\prod_{p\equiv 3}\frac{p+1}{p}\prod_{p\equiv 1}\frac{p-1}{p} = \\ &= \varphi(n)\prod_{p\equiv 3}(p+1)\prod_{p\equiv 1}(p-1).\end{aligned}$$

Since n is the product of different Fermat primes, $\varphi(n) = 2^m$. Clearly, $p = 2^{2^k}+1 \equiv 1 \pmod 4$ unless $p = 3$, but in this case, $p+1$ is a power of 2 too, so we conclude that $(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times$ is a 2-group. □

We now prove sufficiency in Abel's theorem.

Theorem 2.7. *Let $n = 2^s p_1 \dots p_r$ with p_i different Fermat primes. Then the lemniscate can be divided into n equal arcs using straightedge and compass.*

Proof. By the previous corollary, $|(\mathbb{Z}[i]/p_1 \dots p_r\mathbb{Z}[i])^\times|$ is a power of 2, and since $|(\mathbb{Z}[i]/2^s\mathbb{Z}[i])^\times| = \mathrm{N}(2^s) = 2^{2s}$, it follows by the Chinese Reminder Theorem that $|(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times$ is a power of 2. Consequently, the degree of the extension $L_n/\mathbb{Q}$ is a power of 2, and by Theorem A.9, the elements in L_n are constructible. □

2.2 Lemniscatic Extensions: Odd Prime Case

In this section we consider the lemniscatic extension $L_\beta/\mathbb{Q}(i)$ for $\beta \in \mathbb{Z}[i]$ an odd Gaussian prime and show that the Galois group is isomorphic to $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$ in this case. For this we need to prove that the polynomial $P_\beta(x^4) \in \mathbb{Q}(i)[x]$ is irreducible and, as in the case of the cyclotomic polynomials, we'll achieve this goal by applying Eisenstein's irreducibility criterion. Notice that Eisenstein's criterion, usually proved in $\mathbb{Z}[x]$, works aswell for polynomials with coefficients in any unique factorization domain R.

In the sequel, let $\varphi(z) = \sum_{i=1}^\infty c_i z^i, c_i \in \mathbb{Q}, c_1 = 1$, be a formal power series and $R \subseteq \mathbb{C}$ a unique factorization domain with field of fractions K.

Lemma 2.8. *There exist polynomials $S_i \in \mathbb{Q}[x]$ with $\deg S_i < i$ such that for any $\beta \in \mathbb{C}$,*

$$\varphi(\beta z) = \sum_{i=1}^\infty (\beta S_i(\beta))\varphi(z)^i.$$

Proof. We expand formally the series $\sum_{k=1}^\infty b_k \varphi(z)^k$.

$$\varphi(\beta z) = \sum_{k\geq 1} b_k \varphi(z)^k = \sum_{k\geq 1} b_k \left(\sum_{i\geq 1}^\infty c_i z^i\right)^k = \sum_{\substack{k\geq 1 \\ i_1,\dots,i_k\geq 1}} b_k c_{i_1} \dots c_{i_k} z^{i_1+\dots+i_k} =$$

$$= \sum_{l\geq 1} \sum_{\substack{k\leq i \\ i_1,\dots,i_k\geq 1 \\ i_1+\dots+i_k=i}} (b_k c_{i_1} \dots c_{i_k}) z^i$$

Use that $c_1 = 1$ and equate the coefficient of z^i with $c_i\beta^i$ to get for $i \geq 1$,

$$c_i\beta^i = \sum_{\substack{1\leq k\leq i \\ i_1,\dots,i_k\geq 1 \\ i_1+\dots+i_k=i}} b_k c_{i_1} \dots c_{i_k} = b_i + \sum_{\substack{1\leq k<i \\ i_1,\dots,i_k\geq 1 \\ i_1+\dots+i_k=i}} b_k c_{i_1} \dots c_{i_k}.$$

Now the proof follows defining inductively the polynomials S_i, by $S_1(x) = 1$ and for $s \geq 2$,

$$S_i(x) = c_i x^{i-1} - \sum_{\substack{k<i \\ i_1,\ldots,i_k \geq 1 \\ i_1+\cdots+i_k=i}} S_k(x) c_{i_1} \ldots c_{i_k}.$$

□

Lemma 2.9. *Assume S_i is nonzero and for $\beta \in R$ set $b_i(\beta) = \beta S_i(\beta)$, which we assume to be in R. Let $\beta \in R$ be prime and $i < |R/(\beta)|$. Then β divides $b_i(\beta)$ in R.*

Proof. Let $S_i = T_i/s_i$, with $T_i \in \mathbb{Z}[x]$ and $s_i \in \mathbb{Z}$ coprime with the greatest common divisor of the coefficients of T_i. Then, for any $\beta \in R$,

$$s_i b_i(\beta) = s_i \beta S_i(\beta) = \beta T_i(\beta).$$

Let $\alpha \in R$ be a prime dividing s_i. Since $\alpha \mid s_i$, and s_i is coprime with the greatest common divisor of the coefficients of T_i, it follows that $\alpha \nmid T_i$, so $\overline{T_i} \neq \overline{0}$ in $R/(\alpha)[x]$. Since $\alpha \mid s_i b_i(\beta) = \beta T_i(\beta)$, then $\overline{T_i(\beta)\beta} = \overline{0}$, and since $R/(\alpha)$ is an integral domain, then either $\overline{\beta} = \overline{0}$ or $\overline{T_i(\beta)} = \overline{0}$. In particular, for all $\beta \in R$ such that $\overline{\beta} \neq \overline{0}$, $\overline{T_i(\beta)} = \overline{0}$, so $\deg T_i \geq \deg \overline{T_i} \geq |R/(\alpha)| - 1$. Since $\deg T_i < i$, it follows that $i \geq |R/(\alpha)|$.

Now, since $\beta \in R$ is prime dividing $\beta T_i(\beta)$, it divides $s_i b_i(\beta)$ too. However, if $i < |R/(\alpha)|$, it cannot divide s_i, and since β is prime, it must divide $b_i(\beta)$ in R. □

Theorem 2.10. *Let $P, Q \in R[x]$ such that $Q(0) \in R^\times$, P is monic and $\deg P = |R/(\beta)| - 1$. If there is some prime $\beta \in R$ for which*

$$\varphi(\beta z) = \varphi(z) \frac{P(\varphi(z))}{Q(\varphi(z))},$$

then P is irreducible over K.

Proof. We have

$$\sum_{i=1}^{\infty} b_i \varphi(z)^i = \varphi(\beta z) = \varphi(z) \frac{P(\varphi(z))}{Q(\varphi(z))},$$

where $b_i = \beta S_i(\beta)$. Define $B(z) = \sum_{i=1}^{\infty} b_i z^i$ so that $B(z)Q(z) = zP(z)$. Since $Q(0)$ is a unit, $1/Q(z)$ can be expanded as geometric series with coefficients in R, and consequently, so can $B(z)$. Since β is a prime, by the previous lemma for any $i < |R/(\beta)|$, β divides b_i, so $z^{|R/(\beta)|-1}$ divides $B(z)Q(z) = zP(z)$ in $R/(\beta)[x]$. In particular, $z^{|R/(\beta)|-2}$ divides $P(z)$ in $R/(\beta)[x]$. Since P is monic with $\deg P = |R/(\beta)| - 1$, it follows that β divides all coeficients of P, except the leading coefficient. Furthermore, since the value of $B(z)/z$ at $z = 0$ is $b_1 = \beta S_1(\beta) = \beta$, then $P(0) = Q(0)\beta$ with $Q(0)$ a unit, so β^2 does not divide the independent term of P. Thus, applying Eisenstein's criterion, it follows that P is irreducible over K. □

Theorem 2.11. *Let $\beta \in \mathbb{Z}[i]$ be odd prime. Then* $\mathrm{Irr}(\mathrm{sl}(2\varpi/\beta), \mathbb{Q}) = P_\beta(x^4)$*, and so,* $\mathrm{Gal}(L_\beta/\mathbb{Q}(i)) \simeq (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$.

Proof. Observe that $P_\beta(x^4)$ is monic by Theorem 1.29 and that $\deg P_\beta(x^4) = |\mathbb{Z}[i]/\beta\mathbb{Z}[i]| - 1$ by Proposition 1.33. Then, by Proposition 1.25, it follows that for any $\beta \in \mathbb{Z}[i]$ odd prime

$$\mathrm{sl}(\beta z) = \mathrm{sl}(z)\frac{P_\beta(\mathrm{sl}^4(z))}{Q_\beta(\mathrm{sl}^4(z))},$$

where $P, Q \in \mathbb{Z}[i][x]$ with $Q(0) = 1$, and sl can be expanded as a formal power series around 0, $\mathrm{sl}(z) = z + \ldots$, with the coefficient of z being 1 since $\mathrm{sl}'(0) = 1$. Applying the previous theorem, $P_\beta(x^4)$ is irreducible over $\mathbb{Q}(i)$. Since $\mathrm{sl}(2\varpi/\beta)$ is one of the roots of $P_\beta(x^4)$, then $\mathrm{Irr}(\mathrm{sl}(2\varpi/\beta), \mathbb{Q}(i)) = P_\beta(x^4)$, and so, L_β is the splitting field of this polynomial. Consequently, $|\operatorname{Gal}(L_\beta/\mathbb{Q}(i))| = |\mathbb{Z}[i]/\beta\mathbb{Z}[i]| - 1 = |(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times|$, and the monomorphism of Theorem 2.2 is an isomorphism. □

The technique used to prove the irreducibility of $P_\beta(x^4)$ is useful in other scenarios too. In fact, in Problem 9, Theorem 2.10 is used to prove the irreducibility of $T_p(x)/x$ over $\mathbb{Q}$, where T_p is the p-th Chebyshev polynomial and p is a prime number.

2.3 Lemniscatic Extensions: General Case

In this section we prove that for any odd Gaussian integer β, the Galois group of the lemniscatic extension $L_\beta/\mathbb{Q}(i)$ is isomorphic to $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$. Furthermore, we will conclude Abel's theorem.

We know that L_β is the splitting field of $D_\beta(x) = \prod_\gamma (x - \mathrm{sl}(\frac{2\varpi}{\beta}\gamma))$, where (with some abuse of notation) γ runs over the elements in $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$. The elements in this ring can be enumerated according to their greatest common divisor with β. More precisely, for $\alpha \in \mathbb{Z}[i]$ odd, we say that α is *normalised* if $\alpha \equiv 1 \pmod{2(1+i)}$. Then $\mathbb{Z}[i]/\beta\mathbb{Z}[i]$ is the disjoint union of the sets $\{\gamma | (\gamma, \beta) = \alpha\}$, where α runs over the normalised divisors of β.

Definition 2.2. Let $\beta \in \mathbb{Z}[i]$ be odd and define the β-th *lemniscatic polynomial* as

$$\Lambda_\beta(x) = \prod_{\gamma \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times} (x - \mathrm{sl}(\frac{2\varpi}{\beta}\gamma)).$$

Proposition 2.12. *Let $\beta \in \mathbb{Z}[i]$ be odd. Then $\Lambda_\beta \in \mathbb{Z}[i][x]$ and*

$$D_\beta = \prod_{\alpha | \beta} \Lambda_\alpha,$$

where α runs over the normalised divisors of β.

Proof. $\sigma \in \mathrm{Gal}(L_\beta/\mathbb{Q}(i))$ permutes the elements $\mathrm{sl}(\frac{2\varpi}{\beta}\gamma)$, $\gamma \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$, so $\sigma(\Lambda_\beta(x)) = \Lambda_\beta(x)$, for all $\sigma \in \mathrm{Gal}(L_\beta/\mathbb{Q}(i))$, and thus $\Lambda_\beta(x) \in \mathbb{Q}(i)[x]$. Since the elements $\mathrm{sl}(\frac{2\varpi}{\beta}\gamma)$ are roots of the monic polynomial $D_\beta \in \mathbb{Z}[i][x]$, they are algebraic integers, and thus, so are the coefficients of Λ_β. Since the ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$, it follows that $\Lambda_\beta \in \mathbb{Z}[i][x]$.

For the second part we will show that both polynomials have the same roots. Since α is a divisor of β, it is clear that the roots of $\prod_{\alpha|\beta}\Lambda_\alpha$ are all roots of D_β. Now let $\mathrm{sl}(\frac{2\varpi}{\beta}\gamma)$, $\gamma \in (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$, be a root of D_β. By removing common factors, we can write $\mathrm{sl}(\frac{2\varpi}{\beta}\gamma) = \mathrm{sl}(\frac{2\varpi}{\alpha}\rho)$ with α a normalised divisor of β and $\rho \in (\mathbb{Z}[i]/\alpha\mathbb{Z}[i])^\times$, so this element is a root of Λ_α too. □

We now aim to show that the polynomials Λ_β are irreducible. In order to do that, let $f \in \mathbb{Q}(i)[x]$ be an irreducible monic factor of Λ_β in $\mathbb{Q}(i)[x]$. By Gauss's Lemma, $f \in \mathbb{Z}[i][x]$. Let $\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)$, $1 \le i \le r$ be the roots of f and for $\pi \in \mathbb{Z}[i]$ an odd prime define

$$f_\pi = \prod_{i=1}^{r}(x - \mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_i)).$$

Lemma 2.13. *Let $\beta \in \mathbb{Z}[i]$ be odd and f an irreducible factor of Λ_β. If $\pi \in \mathbb{Z}[i]$ is an odd prime, then $f_\pi \in \mathbb{Z}[i][x]$. Furthermore, if $\pi \nmid \beta$, then $f_\pi \mid \Lambda_\beta$.*

Proof. Since $\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)$ is a root of $f \in \mathbb{Z}[i][x]$, which is monic and irreducible, $f = \mathrm{Irr}(\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i), \mathbb{Q}(i))$. Thus, if $\sigma \in \mathrm{Gal}(L_\beta/\mathbb{Q}(i))$, then $\sigma(\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)) = \mathrm{sl}(\frac{2\varpi}{\beta}\gamma_j)$ for some j, and so,

$$\begin{aligned}\sigma\left(\mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_i)\right) &= \sigma\left(\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)R_\pi\left(\mathrm{sl}^4(\frac{2\varpi}{\beta}\gamma_i)\right)\right) = \\ &= \mathrm{sl}(\frac{2\varpi}{\beta}\gamma_j)R_\pi\left(\mathrm{sl}^4(\frac{2\varpi}{\beta}\gamma_j)\right) = \mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_j).\end{aligned}$$

Hence, $\sigma(f_\pi(x)) = f_\pi(x)$ for any $\sigma \in \mathrm{Gal}(L_\beta/\mathbb{Q}(i))$, and so $f_\pi \in \mathbb{Q}(i)[x]$. All $\mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_i)$ are roots of $D_\beta \in \mathbb{Z}[i][x]$, hence algebraic integers, so the coefficients of f_π are algebraic integers too. Since, the algebraic integers of $\mathbb{Q}(i)$ are $\mathbb{Z}[i]$, we conclude that $f_\pi \in \mathbb{Z}[i][x]$.

That f_π divides Λ_β if $\pi \nmid \beta$ follows from the fact that $\mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_i)$ are roots of Λ_β for all i, because $(\pi, \beta) = 1$. □

Lemma 2.14. *Let R be a unique factorization domain with a maximal ideal $\mathfrak{M}$ such that $R/\mathfrak{M}$ is a finite field with q elements. Consider $f \in R[x]$ monic with roots $u_1, \ldots, u_n$ and assume $\overline{f} \in R/\mathfrak{M}[x]$ is separable. Then, if $g(x) = \prod_{i=1}^{r}(x - u_i^q)$, it follows that $\overline{f} = \overline{g}$.*

Proof. Notice first that $g \in R[x]$. In fact, if F is the fraction field of R and L is the splitting field of f over F, then $g \in F[x]$ since it is fixed under $\mathrm{Gal}(L/F)$. Then, since all its roots are integral and the ring of integers of F is R, it follows that $g \in R[x]$. Since $(x-u) \mid (x^q - u^q)$, then $f(x) \mid g(x^q)$. Thus, $\overline{f(x)} \mid \overline{g(x)}^q$, since $R/\mathfrak{M}$ is a finite field of q elements and $\overline{a} = \overline{a}^q$ for any element in this field. Now, since $\overline{f}$ is separable, $\overline{f} = \overline{f_1 \dots f_n}$, with $\overline{f_i} \in R/\mathfrak{M}[x]$ irreducible and distinct. Then, for each i, $\overline{f_i} \mid \overline{g}$ implies that $\overline{f} \mid \overline{g}$ too. Both $\overline{g}$ and $\overline{f}$ are monic with the same degree, so $\overline{g} = \overline{f}$. □

Proposition 2.15. *Let $\beta \in \mathbb{Z}[i]$ be odd and f an irreducible factor of Λ_β. Let $\pi \in \mathbb{Z}[i]$ be an odd prime such that π does not divide the discriminant of Λ_β, $\Delta(\Lambda_\beta)$, and $\pi \nmid \beta$. Then, $f = f_\pi$.*

Proof. Assume $f \neq f_\pi$. Notice that they are both monic and have the same degree. Since f is irreducible, they are coprime, so $f f_\pi \mid \Lambda_\beta$.

By Theorem 2.11, $P_\pi(x^4)$ is an Eisenstein monic polynomial of degree $\mathrm{N}\pi) - 1$, so $xP_\pi(x^4) \equiv x^{\mathrm{N}\pi)} \pmod{\pi}$. By (the proof of) Theorem 1.29, $P_\pi(x) = x^d Q_\pi(1/x)$ with $d = \deg(Q_\pi(x))$, so Q_π has the same coefficients as P_π but in reversed order. In particular, it follows that $Q_\pi(x^4) \equiv 1 \pmod{\pi}$. Consequently,

$$xR_\pi(x^4) = \frac{xP_\pi(x^4)}{Q_\pi(x^4)} \equiv x^{\mathrm{N}(\pi)} \pmod{\pi}.$$

Now let $\mathfrak{p} \subseteq \mathcal{O}_{L_\beta}$ be a prime ideal containing π. Then, since $\mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_i) = \mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)R_\pi(\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i))$, we have that $\mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_i) \equiv \mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)^{\mathrm{N}(\pi)} \pmod{\mathfrak{p}}$. Now define

$$\tilde{f}_\pi(x) = \prod_{i=1}^{r} \left(x - \mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)^{\mathrm{N}(\pi)} \right).$$

Similarly as in Lemma 2.13, $\sigma(\tilde{f}_\pi(x)) = \tilde{f}_\pi(x)$ for any $\sigma \in \mathrm{Gal}(L_\beta/\mathbb{Q}(i))$, since $\sigma(\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i) = \mathrm{sl}(\frac{2\varpi}{\beta}\gamma_j)$, so $\tilde{f}_\pi(x) \in \mathbb{Q}(i)[x]$. Furthermore, since its roots are algebraic integers, its coefficients are also algebraic integers, so $\tilde{f}_\pi(x) \in \mathbb{Z}[i][x]$. Now, since $\mathrm{sl}(\frac{2\varpi}{\beta}\pi\gamma_i) \equiv \mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)^{\mathrm{N}(\pi)} \pmod{\mathfrak{p}}$, it follows that $\tilde{f}_\pi \equiv f_\pi \pmod{\mathfrak{p}}$. But, since $\pi \in \mathfrak{p} \cap \mathbb{Z}[i]$ is prime, $\pi\mathbb{Z}[i] \subseteq \mathfrak{p} \cap \mathbb{Z}[i]$ is a maximal ideal, so $\pi\mathbb{Z}[i] = \mathfrak{p} \cap \mathbb{Z}[i]$, and, $\tilde{f}_\pi = f_\pi \pmod{\pi}$.

On the other hand, notice that $R = \mathbb{Z}[i]$ is a unique factorization domain with maximal ideal $\mathfrak{M} = \pi\mathbb{Z}[i]$ such that $R/\mathfrak{M}$ is a finite field with $q = \mathrm{N}(\pi)$ elements, and that f and $\tilde{f}_\pi$ satisfy the conditions of Lemma 2.14. Hence, $f \equiv \tilde{f}_\pi \pmod{\pi}$. Indeed, notice that $\overline{f}$ is separable in $R/\mathfrak{M}[x]$ because $\overline{\Lambda_\beta}$ is separable, as $\pi \nmid \Delta(f)$.

Combining both congruences, it follows that $f_\pi \equiv f \pmod{\pi}$. In particular, since $f f_\pi \mid \Lambda_\beta$, then $f^2 \mid \Lambda_\beta \pmod{\pi}$, and so, Λ_β is not separable mod π. However, since $\pi \nmid \Delta(\Lambda_\beta)$, Λ_β should be separable mod π. This way we reach a contradiction, so we conclude that it must be $f = f_\pi$. □

Theorem 2.16. *Let $\beta \in \mathbb{Z}[i]$ be odd. Then Λ_β is irreducible over $\mathbb{Q}(i)$.*

Proof. Consider $f \in \mathbb{Z}[i][x]$ an irreducible factor of Λ_β as before. Let $\mathrm{sl}(\frac{2\varpi}{\beta}\gamma_i)$ be any root of f. Define η to be the product of all primes in $\mathbb{Z}[i]$ dividing $\Delta(\Lambda_\beta)$ but not dividing β. Let $\mathrm{sl}(\frac{2\varpi}{\beta}\alpha)$ be any root of Λ_β. By the Chinese reminder theorem, there exists some $\omega \in \mathbb{Z}[i]$ such that

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

In particular, ω is odd, and $\omega = \pi_1 \dots \pi_k$, where $\pi_i \in \mathbb{Z}[i]$ are odd normalized primes coprime with $\beta\Delta(\Lambda_\beta)$. Then, iterating Proposition 2.15, it follows that $f = f_{\pi_1} = f_{\pi_1\pi_2} = \cdots = f_{\pi_1\pi_2\dots\pi_k}$. Thus,

$$\mathrm{sl}\left(\frac{2\varpi}{\beta}\alpha\right) = \mathrm{sl}\left(\frac{2\varpi}{\beta}\alpha\gamma_i^{-1}\gamma_i\right) = \mathrm{sl}\left(\frac{2\varpi}{\beta}\omega\gamma_i\right) = \mathrm{sl}\left(\frac{2\varpi}{\beta}\pi_1\dots\pi_k\gamma_i\right)$$

is a root of $f_{\pi_1\pi_2\dots\pi_k} = f$. Hence, f and Λ_β have the same roots, and since Λ_β is separable and monic, it follows that $f = \Lambda_\beta$. So in particular, Λ_β is irreducible over $\mathbb{Q}(i)$. □

Corollary 2.17. *Let $\beta \in \mathbb{Z}[i]$ be odd. Then* $\mathrm{Gal}(L_\beta/\mathbb{Q}(i)) \simeq (\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$.

Proof. Theorem 2.2 shows that $\mathrm{Gal}(L_\beta/\mathbb{Q}(i))$ is isomorphic to a subgroup of $(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times$, so it suffices to show that they have the same cardinal. Since $\mathrm{sl}(\frac{2\varpi}{\beta})$ is a root of the irreducible polynomial Λ_β, it follows that $\mathrm{Irr}(\mathrm{sl}(\frac{2\varpi}{\beta}), \mathbb{Q}(i)) = \Lambda_\beta$, so in particular,

$$|\operatorname{Gal}(L_\beta/\mathbb{Q}(i))| = [L_\beta \colon \mathbb{Q}(i)] = \deg(\Lambda_\beta) = |(\mathbb{Z}[i]/\beta\mathbb{Z}[i])^\times|.$$

□

This is the main result concerning this chapter, and it is analogue to the cyclotomic extensions having Galois grouop isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. With this result and thanks to the previous work we have done, we are able to finally prove Abel's theorem on the lemniscate.

Theorem 2.18 (Abel's theorem)**.** *Assume that the lemniscate can be divided into n equal arcs using straightedge and compass. Then, $n = 2^s p_1 \dots p_r$ with p_i different Fermat primes.*

Proof. In this case, the number $\mathrm{sl}(\frac{2\varpi}{n})$ is contructible, so $|\operatorname{Gal}(\mathbb{Q}(\mathrm{sl}(\frac{2\varpi}{n}))/\mathbb{Q})|$ is a power of 2 by Theorem A.10. Now, since

$$|\operatorname{Gal}(\mathbb{Q}(\mathrm{sl}(\frac{2\varpi}{n}))/\mathbb{Q})| = |\operatorname{Gal}(L_n/\mathbb{Q}(i))| = |(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times|,$$

it follows that $|(\mathbb{Z}[i]/n\mathbb{Z}[i])^\times|$ is a power of 2 too, and then, by Corollary 2.6, that $n = 2^s p_1 \dots p_r$ with p_i different Fermat primes. □

Theorems 2.7 and 2.18 together give a characterization of when the lemniscate can be divided into n equal arcs using straightedge and compass in terms of the factorization of n, which is the analogue of Theorem A.12 for the lemniscate.

Chapter 3

The lemniscate and Elliptic Curves

In this chapter we study the relationship of the lemniscate with the theory of elliptic curves. It happens that sl is an elliptic function with complex multiplication, which explains why lemniscatic extensions are abelian.

3.1 Introduction to Elliptic Curves

In this section we provide a brief introduction to the theory of elliptic curves. We start with some basic definitions.

Definition 3.1. Let $\omega_1, \omega_2 \in \mathbb{C}$ be such that $\{\omega_1, \omega_2\}$ is an $\mathbb{R}$-basis of $\mathbb{C}$. The *lattice* they generate is $\mathcal{L} = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$. The *fundamental parallelogram* associated to this lattice is $\mathcal{F} = \{a\omega_1 + b\omega_2 \mid 0 \leq a, b \leq 1\}$.

Definition 3.2. Given a lattice $\mathcal{L}$, a meromorphic function f on $\mathbb{C}$ is said to be an *elliptic function* relative to $\mathcal{L}$ if $f(z + \alpha) = f(z)$ for all $\alpha \in \mathcal{L}$. The set of elliptic functions relative to $\mathcal{L}$ is denoted $\mathscr{E}_{\mathcal{L}}$.

Example 3.1. sl is an elliptic function over the lattice $\mathcal{L}$ generated by $(1 \pm i)\varpi$. Indeed, it is double periodic by Theorem 1.22, and meromorphic by Theorem 1.23.

Observe that any $f \in \mathscr{E}_{\mathcal{L}}$ is determined by its values on $\mathcal{F}$, and that its values on opposite sides of $\mathcal{F}$ are equal. Thus, an elliptic function is a function on the set $\mathcal{F}$ with opposite sides glued together, that is, a torus which can be described as the quotient $\mathbb{C}/\mathcal{L}$.

The next proposition is extremely useful to show when two elliptic functions are equal.

Proposition 3.2. *Let $f \in \mathscr{E}_{\mathcal{L}}$ and assume f has no poles in $\mathcal{F}$. Then f is constant.*

Proof. Since f has no poles in $\mathcal{F}$, then by periodicity f is an entire function. Also, since $\mathcal{F} \subseteq \mathbb{C}$ is compact, f is bounded in $\mathcal{F}$, and by periodicity it follows that f is bounded in $\mathbb{C}$. The result now follows from Liouville's Theorem (every bounded entire function is constant). □

Obviously $\mathscr{E}_{\mathcal{L}}$ is a field. Furthermore, if $f \in \mathscr{E}_{\mathcal{L}}$, $f' \in \mathscr{E}_{\mathcal{L}}$. We have the following corollary.

Corollary 3.3. *If $f, g \in \mathscr{E}_{\mathcal{L}}$, $f, g \neq 0$, have the same zeros and poles (counting multiplicities), then $f = cg$ for some $c \in \mathbb{C}$.*

Proof. Notice that $f/g \in \mathscr{E}_{\mathcal{L}}$ has no poles in $\mathcal{F}$, so the result follows from the previous proposition. □

Corollary 3.4. *Elliptic functions are surjective.*

Proof. Let $f \in \mathscr{E}_{\mathcal{L}}$ be non-constant, and assume there exists some $z_0 \in \mathbb{C}$ for which $f(z) \neq z_0$ for all $z \in \mathbb{C}$. Then, the function $g(z) = 1/(f(z) - z_0)$ is non-constant and holomorphic in $\mathbb{C}$. Furthermore, $g \in \mathscr{E}_{\mathcal{L}}$ by the periodicity of f, so by Proposition 3.2 g is constant, reaching a contradiction. □

The following example of an elliptic function is the Weierstrass $\wp$-function relative to a lattice $\mathcal{L}$. As we will see, this function turns out to be very useful when studying elliptic curves.

Definition 3.3. Let $\mathcal{L}$ be any lattice. The Weierstrass $\wp$-function relative to $\mathcal{L}$, denoted $\wp(z; \mathcal{L})$ or simply $\wp$, is the function

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\alpha \in \mathcal{L} \\ \alpha \neq 0}} \left(\frac{1}{(z-\alpha)^2} - \frac{1}{\alpha^2} \right). \tag{3.1}$$

Theorem 3.5. *Let $\mathcal{L}$ be any lattice. Then $\wp \in \mathscr{E}_{\mathcal{L}}$, and its only poles are double poles at each lattice point.*

Proof. See Proposition 7 in page 17 of [Kob84]. □

It is not clear in general what are the zeros of $\wp$. However, it is a general result that an elliptic function $f \in \mathscr{E}_{\mathcal{L}}$ has the same number of zeros and poles in $\mathbb{C}/\mathcal{L}$ counting multiplicities (see Proposition 5 in page 16 of [Kob84]), so $\wp$ has two simple zeros in $\mathbb{C}/\mathcal{L}$ or a double zero.

The situation for $\wp'$ is more clear. In fact, notice that the only pole of $\wp'$ in $\mathbb{C}/\mathcal{L}$ is a triple pole at 0, so $\wp'$ must have three zeros counting multiplicities. Using the fact that $\wp$ is even, one checks that $\varpi_1/2, \varpi_2/2$ and $(\varpi_1 + \varpi_2)/2$ are the three (simple) zeros of $\wp'$ in $\mathbb{C}/\mathcal{L}$.

An important property of the Weierstrass $\wp$-function is that any elliptic function can be expressed as a rational expression in $\wp$ and $\wp'$, as it can be seen in Proposition 8 of [Kob84]. For example, we have the following expression for sl.

Example 3.6. If $\mathcal{L}$ be the lattice generated by $(1 \pm i)\varpi$, then

$$\mathrm{sl}(z) = -2\frac{\wp(z)}{\wp'(z)}.$$

To prove this it suffices to show that $\mathrm{sl} \cdot \wp'$ and $\wp$ have the same poles and zeros with same multiplicities in $\mathbb{C}/\mathcal{L}$, because then, by Corollary 3.3, it follows that $\mathrm{sl}(z)\wp'(z) = c\wp(z)$ for some $c \in \mathbb{C}$, which can be checked to be -2 by comparing the first term of the Laurent series of $\mathrm{sl} \cdot \wp'$ and $\wp$.

Now, one can check that the only poles and zeros of $\mathrm{sl} \cdot \wp'$ in $\mathbb{C}/\mathcal{L}$ are a double pole at 0 and double zero at ϖ. Since the only pole of $\wp$ in $\mathbb{C}/\mathcal{L}$ is a double pole at 0, it only remains to show that $\wp$ has a double zero at ϖ. Indeed, since $\wp(iz) = -\wp(z)$ and $i\varpi \equiv \varpi$ in $\mathbb{C}/\mathcal{L}$, $\wp(\varpi) = 0$, and since $\wp'(\varpi) = 0$, we conclude the desired result.

As another example, notice that the elliptic functions $\wp'(z)^2$ and

$$(\wp(z) - \wp(\omega_1/2))(\wp(z) - \wp(\omega_2/2))(\wp(z) - \wp((\omega_1 + \omega_2)/2)$$

have the same poles and zeros in $\mathcal{F}$ counting multiplicities, so by Corollary 3.3 they are equal except for a constant. By comparing the first term of their Laurent series one checks that this constant is 1.

Thus, $(\wp')^2$ satisfies a cubic equation in $\wp$ with roots $\wp(\varpi_1/2), \wp(\varpi_2/2)$ and $\wp((\varpi_1 + \varpi_2)/2)$. Furthermore, one can check that these roots are different, see for example [Kob84], which will be important when defining the concept of an elliptic curve. Say this cubic equation is given by

$$\wp'(z)^2 = a\wp(z)^3 + b\wp(z)^2 + c\wp(z) + d.$$

Then, the coefficients can be computed by comparing the Laurent expansions of these two functions. In fact, as it is shown in [Kob84],

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\mathcal{L})\wp(z) - g_3(\mathcal{L}), \tag{3.2}$$

where

$$g_2(\mathcal{L}) = 60 \sum_{\substack{\alpha \in \mathcal{L} \\ \alpha \neq 0}} \frac{1}{\alpha^4}, \qquad g_3(\mathcal{L}) = 140 \sum_{\substack{\alpha \in \mathcal{L} \\ \alpha \neq 0}} \frac{1}{\alpha^6}. \tag{3.3}$$

Definition 3.4. Let K be any subfield of $\mathbb{C}$ and let $a, b \in K$. An *elliptic curve* over K is a projective curve E in $\mathbb{CP}^2$ given by an equation of the form $y^2 = f(x)$, where $f(x) = 4x^3 - ax - b$ is separable over K.

The points in E that have coordinates in some field extension L of K are the L-points of E, sometimes denoted $E(L)$.

The relationship between $\wp$ and $\wp'$ given by (3.2) tells us that these two functions parametrize the elliptic curve given by $y^2 = 4x^3 - g_2x - g_3$. In fact,

consider the following function, defined from the torus $\mathbb{C}/\mathcal{L}$ to the projective space $\mathbb{CP}^2$ and given by

$$z \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1), & \text{if } z \neq 0, \\ (0 : 1 : 0), & \text{if } z = 0, \end{cases} \tag{3.4}$$

Proposition 3.7. *The map* (3.4) *is a one-to-one correspondence between* $\mathbb{C}/\mathcal{L}$ *and the elliptic curve* $y^2 = 4x^3 - g_2x - g_3$ *in* $\mathbb{CP}^2$.

Proof. See Proposition 10 in page 24 of [Kob84]. □

In fact, this correspondence between $\mathbb{C}/\mathcal{L}$ and the elliptic curve E can be used to carry over the addition law in the torus to E. With some abuse of notation, let P_z denote the point $(\wp(z), \wp'(z))$ in E.

Definition 3.5. Let E be an elliptic curve over K and let P_{z_1} and P_{z_2} be two points in E. Define $P_{z_1} + P_{z_2} = P_{z_1+z_2}$.

Theorem 3.8. *Let* E *be an elliptic curve over* K*. Then, the addition law defined previously gives* E *a group structure.*

Proof. It follows from using correspondence (3.4) to translate the addition law in $\mathbb{C}/\mathcal{L}$ to E. □

The remarkable fact about this addition law is that if $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then, the coordinates of $P_1 + P_2$ can be expressed directly in terms of x_1, x_2, y_1, y_2 by rational functions, without the need of using the correspondence (3.4) to compute them. This gives a very nice geometric interpretation of this operation (the tangent-chord rule), which Kobltiz explains further in [Kob84]. This relation can also be thought of as an addition law for $\wp$, analog to the addition law for sl.

To end this section, we will study the torsion points of an elliptic curve. These points are the ones which have finite order with respect to the addition law in the elliptic curve.

Proposition 3.9. *Let* E *be an elliptic curve over* K*. Then a point* P_z *has finite order dividing* n *if and only if* $z = \alpha/n$*, for some* $\alpha \in \mathcal{L}$*. Furthermore,* $E[n]$*, the subgroup of* $E(\mathbb{C})$ *with points of order dividing* n*, is isomorphic to* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *and it has* n^2 *points.*

Proof. Clearly, a point P_z has finite order dividing n if and only if $nz \in \mathcal{L}$, that is, when $z = \alpha/n$, for some $\alpha \in \mathcal{L}$.

There is a natural isomorphism from $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ to $\mathbb{C}/\mathcal{L}$ induced by the map $(a, b) \mapsto a\omega_1 + b\omega_2$. Thus, we can see the correspondence (3.4) as a one-to-one correspondence between $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ and E. Under this correspondence, the torsion subgroup of the elliptic curve is the image of $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$. In particular, the subgroup of elements of order dividing n, is the image of $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \times \frac{1}{n}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and we conclude the result. □

This situation is the two-dimensional analog of the circle group, whose torsion subgroup is precisely the group of all roots of unity, that is, all $e^{2\pi iz}$ for $z \in \mathbb{Q}/\mathbb{Z}$.

Just as the cyclotomic fields are central to algebraic number theory, we would expect that the fields obtained by adjoining the coordinates of torsion points of elliptic curves should have a special significance, so we study them.

Let $K(E[n])$ denote the subfield of $\mathbb{C}$ obtained by adjoining to K the x- and y-coordinates of all points in $E[n]$.

Lemma 3.10. *Let L/K be any field extension, and $\sigma\colon L \to \mathbb{C}$ be a field embedding fixing K. Consider an elliptic curve E over K and let $P \in E[n]$ with coordinates on L. Then $\sigma(P) \in E[n]$.*

Proof. It follows from the fact that σ induces an automorphism of the group of L-points in the elliptic curve. □

Proposition 3.11. *Let E be an elliptic curve over K. Then, $K(E[n])/K$ is a (finite) Galois extension and its Galois group is isomorphic to a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.*

Proof. $K(E[n])$ is obtained by adjoining a finite set of complex numbers which are permuted by any automorphism of $\mathbb{C}$ fixing K, so $K(E[n])/K$ is a (finite) Galois extension.

Recall that $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ by Proposition 3.9. Since any $\sigma \in \mathrm{Gal}(K(E[n])/K)$ gives an automorphism of $E[n]$ by the previous lemma, σ can be viewed as an invertible linear map of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ to itself, so $\mathrm{Gal}(K(E[n])/K)$ is isomorphic to a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$. □

Notice that this is a generalization of the situation with the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$, with $\zeta_n = e^{2\pi i/n}$. Indeed, recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times \simeq GL_1(\mathbb{Z}/n\mathbb{Z})$. However, one major difference between both cases is that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq GL_1(\mathbb{Z}/n\mathbb{Z})$, while $\mathrm{Gal}(K(E[n])/K)$ is only isomorphic to a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.

3.2 The lemniscate elliptic curve

The lemniscate function sl is an elliptic function with period lattice $\mathcal{L}$ generated by $(1 \pm i)\varpi$. By the correspondence between lattices and elliptic curves, $\mathcal{L}$ defines an elliptic curve with Weierstrass equation $y^2 = 4x^3 - g_2(\mathcal{L})x - g_3(\mathcal{L})$, where $g_2(\mathcal{L})$ and $g_3(\mathcal{L})$ are given by (3.3).

The goal of this section is to compute this curve. In order to do that, we'll work out first the elliptic curve associated to the sublattice $\mathcal{L}' = \langle 2\varpi, 2\varpi i\rangle$ and then derive the elliptic curve associated to $\mathcal{L}$ from it.

Similarly as before, let $y^2 = 4x^3 - g_2(\mathcal{L}')x - g_3(\mathcal{L}')$ be the elliptic curve associated to the lattice $\mathcal{L}'$. Since $\mathcal{L}'$ is invariant under multiplication by i, $g_3(\mathcal{L}')$ is easy to compute.

Proposition 3.12. $g_3(\mathcal{L}') = 0$.

Proof. Since $i\mathcal{L}' = \mathcal{L}'$ we can replace α by $i\alpha$ in the series defining $g_3(\mathcal{L}')$, and this changes the sign of the sum but not its value, hence $g_3(\mathcal{L}') = 0$. □

The computation of $g_2(\mathcal{L}')$ requires more work. For the sake of convenience, let's define the sets

$$\mathcal{L}_0 = \langle \varpi, \varpi i \rangle;\ \mathcal{L}_1 = \{\frac{n+mi}{2}\varpi \mid n, m \text{ odd}\};\ \mathcal{L}_2 = \{\frac{n+mi}{2}\varpi \mid n \not\equiv m \pmod 2\}.$$

Proposition 3.13.

$$\frac{\mathrm{sl}'(z)}{\mathrm{sl}(z)} = \sum_{\alpha\in\mathcal{L}_0} \frac{z^3}{z^4-\alpha^4} - \sum_{\beta\in\mathcal{L}_1} \frac{z^3}{z^4-\beta^4}. \tag{3.5}$$

Proof. Notice that $\mathrm{sl}'(z)/\mathrm{sl}(z)$ is an elliptic function over $\mathcal{L}$ with only simple poles at each $\alpha \in \mathcal{L}_0$ and $\beta \in \mathcal{L}_1$. On the other hand, it is routine to check that the series on the right hand side define a holomorphic function $f(z)$ for z outside $\mathcal{L}_0$ and $\mathcal{L}_1$, where it has simple poles (see Lemmas 1 and 2 in page 17 of [Kob84]).

To show periodicity of f, consider f as the limit of the partial sums over the elements of $\mathcal{L}_0$ and $\mathcal{L}_1$ in the squares $B_n = [-n, n]\varpi \times [-n, n]\varpi i$. Then, $f(z+\varpi) - f(z)$ and $f(z+\varpi i) - f(z)$ can be expressed as the limit of the corresponding partial sums, which happen to converge to 0.

Applying Proposition 3.2 to the difference of the function sl'/sl and f, which have the same simple poles with same residues, this difference must be constant. One checks that this constant is 0 by comparing the first term of the Laurent expansions of both sides of the equation (see (3.6)). □

Corollary 3.14. *Let $|\mathcal{L}_i| = \sum \alpha^{-4}$, where the sum extends to the non-zero elements in $\mathcal{L}_i$. Then $|\mathcal{L}_1| - |\mathcal{L}_0| = -2/5$.*

Proof. Multiplying equation (3.5) by z and then expanding both sides as Taylor series, we obtain

$$1 - \frac{2}{5}z^4 + \ldots = 1 + (|\mathcal{L}_1| - |\mathcal{L}_0|)z^4 + \ldots, \tag{3.6}$$

from which the result follows. □

Proposition 3.15. $|\mathcal{L}_1| = -5|\mathcal{L}_0|$.

Proof. Notice that $\frac{1}{2}\mathcal{L}_0 = \mathcal{L}_0 \cup \mathcal{L}_1 \cup \mathcal{L}_2$, where the union is disjoint. Hence it is clear that $|\frac{1}{2}\mathcal{L}_0| = |\mathcal{L}_0| + |\mathcal{L}_1| + |\mathcal{L}_2|$. One can check that $\mathcal{L}_2 = \frac{(1+i)}{2}\mathcal{L}_1$, so we get $|\mathcal{L}_2| = -4|\mathcal{L}_1|$. Furthermore, one has $|\frac{1}{2}\mathcal{L}_0| = 16|\mathcal{L}_0|$. Combining all together, we get that $|\mathcal{L}_1| = -5|\mathcal{L}_0|$. □

Corollary 3.16. $|\mathcal{L}_0| = 1/15$. *Consequently,* $\sum z^{-4} = \varpi^4/15$, *where the sum extends to the non-zero Gaussian integers.*

Proof. It follows from combining Corollary 3.14 and Proposition 3.15. □

Notice the analogy with the Bassel problem, where $\sum z^{-2} = \pi^2/6$ and the sum extends to the positive integers.

Proposition 3.17. *The elliptic curve associated to* $\mathcal{L}'$ *is* $y^2 = 4x^3 - \frac{1}{4}x$.

Proof. Recall that $g_3(\mathcal{L}') = 0$ by Proposition 3.12. Now, notice $\mathcal{L}' = 2\mathcal{L}_0$, so $|\mathcal{L}_0| = 16|\mathcal{L}'|$. By the previous corollary $|\mathcal{L}_0| = 1/15$, so $|\mathcal{L}'| = 1/240$. Then, $g_2(\mathcal{L}') = 60|\mathcal{L}'| = 1/4$, and we conclude the result. □

Corollary 3.18. *The elliptic curve associated to* $\mathcal{L}$ *is* $y^2 = 4x^3 + x$.

Proof. Observe that $\mathcal{L}' = (1+i)\mathcal{L}$. Then, by replacing α by $(1+i)\alpha$ in the sums of $g_2(\mathcal{L}')$ and $g_3(\mathcal{L}')$, we obtain the relations $g_2(\mathcal{L}') = -1/4\, g_2(\mathcal{L})$ and $g_3(\mathcal{L}') = -i/8\, g_3(\mathcal{L})$. By the previous proposition $g_2(\mathcal{L}') = -1/4$ and $g_3(\mathcal{L}') = 0$, so $g_2(\mathcal{L}) = 1$ and $g_3(\mathcal{L}) = 0$, and we conclude the result. □

Corollary 3.19. $\mathrm{sl}(2\varpi/n) \in \mathbb{Q}(E[n])$, *where* $E[n]$ *denotes the* n*-torsion points of the elliptic curve* $y^2 = 4x^3 + x$.

Proof. Let $z = 2\varpi/n$ and $\wp$ be the Weierstrass function associated to the lattice $\mathcal{L}$. Since $nz \in \mathcal{L}$, it follows that $P_z = (\wp(z), \wp'(z)) \in E[n]$, by the discussion at the end of section 3.1. Then, since $\mathbb{Q}(E[n])$ is the field obtained by adjoining to $\mathbb{Q}$ all the x- and y-coordinates of the points in $E[n]$, it follows that $\wp(z), \wp'(z) \in \mathbb{Q}(E[n])$. Finally, by example 3.6, it follows that $\mathrm{sl}(z) = -2\wp(z)/\wp'(z)$, so we conclude that $\mathrm{sl}(z) \in \mathbb{Q}(E[n])$. □

3.3 Elliptic Curves with complex multiplication

The fact that the lemniscatic extensions are abelian follows from the more general fact that any elliptic curve defined over a field K with complex multiplication satisfies that $\mathrm{Gal}(K(E[n])/K)$ is almost abelian.

The aim of this section is to develop a more restricted version of the theory of complex multiplication to prove that all lemniscatic extensions $L_n/\mathbb{Q}(i)$ are abelian, including those with n even.

Definition 3.6. A lattice $\mathcal{L} \subseteq \mathbb{C}$ has *complex multiplication* (CM for short) if there exists $\gamma \in \mathbb{C}$, $\gamma \notin \mathbb{R}$, such that $\gamma\mathcal{L} \subseteq \mathcal{L}$. An elliptic curve associated to a lattice with CM is said to have CM.

Notice that if $\gamma\mathcal{L} \subseteq \mathcal{L}$, then $K = \mathbb{Q}(\gamma)$ is an imaginary quadratic field. This is because in this case $(\gamma\varpi_1, \gamma\varpi_2) = (\varpi_1, \varpi_2)M$ for some $M \in M_2(\mathbb{Z})$,

so γ is an eigenvalue of M and thus a root of its characteristic polynomial, which is quadratic.

In the sequel, we will assume the much stronger condition $\gamma\mathcal{L} = \mathcal{L}$. In fact, notice that this condition implies that $\gamma \in \mathcal{O}_K^\times$ (because γ is an eigenvalue of a matrix $M \in GL_2(\mathbb{Z})$), so $\gamma \neq \pm 1$ implies $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, with $\omega = e^{2\pi i/3}$, and so there are only two essentially different possibilities for γ, namely $\gamma = i$ or ω.

Proposition 3.20. *Let $\mathcal{L}$ be a lattice with CM by γ. Then, the map m_γ which sends $(x, y) \mapsto (\gamma^{-2}x, \gamma^{-3}y)$ is an automorphism of the elliptic curve associated to $\mathcal{L}$.*

Proof. Since $\gamma\mathcal{L} = \mathcal{L}$, multiplication by γ induces an automorphism on the torus $\mathbb{C}/\mathcal{L} \to \mathbb{C}/\mathcal{L}$, which corresponds to the automorphism of the elliptic curve given by $(\wp(z), \wp'(z)) \mapsto (\wp(\gamma z), \wp'(\gamma z))$. Now we compute $\wp(\gamma z)$:

$$\wp(\gamma z) = \frac{1}{\gamma^2 z^2} + \sum_{\substack{\alpha\in\mathcal{L}\\ \alpha\neq 0}} \left(\frac{1}{(\gamma z - \alpha)^2} - \frac{1}{\alpha^2} \right) =$$

$$= \frac{1}{\gamma^2} \left[\frac{1}{z^2} + \sum_{\substack{\alpha\in\mathcal{L}\\ \alpha\neq 0}} \left(\frac{1}{(z - \frac{\alpha}{\gamma})^2} - \frac{1}{(\frac{\alpha}{\gamma})^2} \right) \right] = \gamma^{-2}\wp(z),$$

where the last equality holds because $\gamma^{-1}\mathcal{L} = \mathcal{L}$. Taking derivatives in $\wp(\gamma z) = \gamma^{-2}\wp(z)$ we obtain $\wp'(\gamma z) = \gamma^{-3}\wp'(z)$, concluding the proof. □

Proposition 3.21. *In the conditions of the previous proposition, let K be a field containing γ and the coefficients of the associated elliptic curve. Then, the elements of $\mathrm{Gal}(K(E[n])/K)$ and m_γ, viewed as endomorphisms of the group $E[n]$, commute.*

Proof. Ineed, let σ be any automorphism of $\mathrm{Gal}(K(E[n])/K)$. Since σ fixes $\gamma \in K$, then $(\sigma \circ m_\gamma)(x, y) = \sigma((\gamma^{-2}x, \gamma^{-3}y)) = (\gamma^{-2}\sigma(x), \gamma^{-3}\sigma(y))$. Similarly, $(m_\gamma \circ \sigma)(x, y) = m_\gamma(\sigma(x), \sigma(y)) = (\gamma^{-2}\sigma(x), \gamma^{-3}\sigma(y))$. □

To conclude from the previous proposition that the Galois group is abelian we apply a general result on centralizers of matrices.

Lemma 3.22. *Let $M \in M_2(\mathbb{Z}/n\mathbb{Z})$ be such that M is not scalar over $\mathbb{Z}/p\mathbb{Z}$ for every prime $p \mid n$. Then, there exists some $P \in GL_2(\mathbb{Z}/n\mathbb{Z})$ such that $P^{-1}MP$ is of the form $\left(\begin{smallmatrix} 0 & 1 \\ a & b \end{smallmatrix}\right)$ for some $a, b \in \mathbb{Z}/n\mathbb{Z}$.*

Proof. By the Chinese Reminder Theorem it suffices to prove the result for $n = p^e$ with p prime.

Since M is not scalar over $\mathbb{Z}/p\mathbb{Z}$, there exists some $u \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ such that $\{u, uM\}$ is a $\mathbb{Z}/p\mathbb{Z}$-basis of this space. Let $P \in M_2(\mathbb{Z}/p\mathbb{Z})$ be the

matrix whose rows are u and uM. Since $\{u, uM\}$ is a basis, P is invertible over $\mathbb{Z}/p\mathbb{Z}$, and so, P, viewed as a matrix in $M_2(\mathbb{Z})$, has $\det(P)$ coprime with p, so coprime with n too. This means that P is invertible over $\mathbb{Z}/n\mathbb{Z}$, so $\{u, uM\}$ is a $\mathbb{Z}/n\mathbb{Z}$-basis of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which implies that M is similar to a matrix of the desired form. □

Proposition 3.23. *For any commutative ring R, the centralizer in $M_2(R)$ of a matrix $C = \left(\begin{smallmatrix} 0 & 1 \\ a & b \end{smallmatrix}\right)$ is the R-submodule of $M_2(R)$ generated by the identity matrix and C. In particular, this centralizer is a commutative subring of $M_2(R)$, so in the conditions of Lemma 3.22 the centralizer of M is a commutative subring of $M_2(\mathbb{Z}/n\mathbb{Z})$.*

Proof. The centralizer in $M_2(R)$ of $C = \left(\begin{smallmatrix} 0 & 1 \\ a & b \end{smallmatrix}\right)$ is the set $\{B \in M_2(R) \mid BC = CB\}$. By considering an arbitrary matrix $B \in M_2(R)$ of the form $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ and imposing it to satisfy $BC = CB$, one gets the equations $z = ay$ and $w = x + by$, which imply that $B = xI_2 + yC$. Hence, the centralizer is generated by I_2 and C, and since they commute, it is abelian. □

Definition 3.7. A lattice $\mathcal{L} \subseteq \mathbb{C}$ is *invariant under conjugation* if $\overline{\mathcal{L}} = \mathcal{L}$. An elliptic curve associated to a lattice invariant under conjugation is said to be *invariant under conjugation*.

Notice that in this case the conjugation map $\mathbb{C}/\mathcal{L} \to \mathbb{C}/\mathcal{L}$ is well defined, and so it induces and endomorphism on the elliptic curve associated to $\mathcal{L}$, which is in fact the map $(x, y) \mapsto (\overline{x}, \overline{y})$.

Proposition 3.24. *Assume the conditions of Proposition 3.21, and also that $\mathcal{L}$ is invariant under conjugation. Then, the endomorphism m_γ acting on $E[p]$ is not scalar for any prime $p \mid n$.*

Proof. If $p = 2$ then $E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, by Proposition 3.9, and so m_γ is scalar if and only if it is the identity. Now, since $z = \varpi_1/2$ is of the form $\alpha/2$ for some $\alpha \in \mathcal{L}$, $P_z = (x, 0) \in E[2]$. Then, $m_\gamma(x, 0) = (\gamma^{-2}x, 0)$, so m_γ is not the identity and thus not scalar.

If $p > 2$ then $E[p]$ has at least 9 elements by Proposition 3.9, so there exists some $(x, y) \in E[p]$ with $x, y \neq 0$. If we assume that m_γ is scalar, then it commutes with the conjugation map, which implies both $\gamma^{-2} = \overline{\gamma^{-2}}$ and $\gamma^{-3} = \overline{\gamma^{-3}}$. However, this is a contradiction because $\gamma = i$ or ω. □

Theorem 3.25. *Any elliptic curve defined over a field K with CM by $\gamma \in K$ and invariant under conjugation satisfies that* $\mathrm{Gal}(K(E[n])/K)$ *is abelian.*

Proof. Any $\sigma \in \mathrm{Gal}(K(E[n])/K)$ commutes with the action of m_γ in $E[n]$ by Proposition 3.21, so $\mathrm{Gal}(K(E[n])/K)$ is contained in the centralizer of m_γ in $\mathrm{End}(E[n]) \simeq M_2(\mathbb{Z}/n\mathbb{Z})$, which is commutative by Propositions 3.23 and 3.24. □

Corollary 3.26. *The lemniscatic extensions are abelian.*

Proof. The lemniscatic elliptic curve $y^2 = 4x^3 + x$ over $\mathbb{Q}(i)$ has CM by i, since $i\mathcal{L} = \mathcal{L}$ for $\mathcal{L} = \langle(1 \pm i)\varpi\rangle$. Furthermore, it is invariant under conjugation since $\overline{1 \pm i} = 1 \mp i$ and $\varpi \in \mathbb{R}$. Applying the last theorem, it follows that $\mathrm{Gal}(\mathbb{Q}(E[n], i)/\mathbb{Q}(i))$ is abelian. Since $\mathrm{sl}(2\varpi/n) \in \mathbb{Q}(E[n])$ by Corollary 3.19, we conclude by Galois theory that $\mathrm{Gal}(\mathbb{Q}(\mathrm{sl}(2\varpi/n), i)/\mathbb{Q}(i))$ is abelian. □

Notice that Corollary 3.26 is true for both n odd or even.

3.4 Final comments

Let ζ_n be a primitive n-th root of unity and consider the cyclotomic field $\mathbb{Q}(\zeta_n)$. Then, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, and it is in particular abelian. The Kronecker-Weber Theorem provides a partial converse.

Theorem 3.27 (Kronecker-Weber)**.** *Every finite abelian extension of* $\mathbb{Q}$ *is contained inside some cyclotomic field.*

In fact, one could ask for analogues of the Kronecker-Weber Theorem for any number field. If K is any number field, what are the algebraic numbers necessary to construct all abelian extensions of K analogue to the roots of unity in the Kronecker-Weber Theorem? This problem is known as Hilbert's twelfth problem and it remains unsolved in this generality.

However, there are some particular cases in which Hilbert's twelfth problem has been solved. For example, consider the following theorem concerning the abelian extensions of $\mathbb{Q}(i)$, due to Takagi (see [Tak03]).

Theorem 3.28 (Takagi)**.** *Every finite abelian extension of* $\mathbb{Q}(i)$ *is contained inside some lemniscatic extension.*

The case when the field is quadratic imaginary is known as Kronecker's Jugendtraum, and in this context Hilbert's twelfth problem is solved. In what follows, we will provide some ideas in order to explain the solution.

Let K be a quadratic imaginary field and $\mathcal{O}_K = \mathbb{Z}[\tau]$ its ring of integers. Define $\mathcal{L}_K$ to be the set of lattices of $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$ modulo homotheties. Here, two lattices $\mathcal{L}$ and $\mathcal{L}'$ are *homothetic* if $\mathcal{L}' = \lambda\mathcal{L}$ for some $\lambda \in \mathbb{C}$. Then, the ideal class group of K acts naturally on $\mathcal{L}_K$.

Indeed, let $\mathcal{L} \in \mathcal{L}_K$ be some lattice. If $\mathfrak{a} \subseteq \mathcal{O}_K$ is an ideal, then $\mathfrak{a}\mathcal{L} \in \mathcal{L}_K$ is another lattice too (this is basically because $\mathfrak{a}\mathcal{L} \subseteq \mathcal{L}$ has rank 2 as a $\mathbb{Z}$-module). Notice also that since $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, $\mathfrak{a}\mathcal{L}$ has complex multiplication by $\mathcal{O}_K$. Furthermore, if $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same ideal class, then $\mathfrak{a} = \lambda\mathfrak{b}$ for some $\lambda \in K$, so $\mathfrak{a}\mathcal{L} = \lambda\mathfrak{b}\mathcal{L}$ and they are homothetic.

The action of the ideal class group of K on $\mathcal{L}_K$ turns out to be regular, as it can be seen in Proposition 1.2 of [Sil94]. In particular, this implies that there are at most h_K (the class number of K) different lattices (up to homotheties) with complex multiplication by $\mathcal{O}_K$.

Now we introduce the j-invariant of an elliptic curve, which is an important invariant of elliptic curves. As we will see later, the j-invariant plays an important role in constructing a solution to Kronecker's Jugendtraum.

Definition 3.8. Let E be an elliptic curve over K given by the Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$. The j-invariant associated to this elliptic curve is defined as

$$j(E) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Notice that $g_2^3 - 27g_3^2$ is non-zero since it is the discriminant of the cubic polynomial $4x^3 - g_2x - g_3$, which has three different roots by construction (see equation (3.2)).

The j-invariant is a fundamental invariant of elliptic curves, since it distinguishes isomorphic elliptic curves.

Definition 3.9. Two elliptic curves E and E' are said to be *isomorphic* if they there exists an isomorphism between E and E' as algebraic varieties which sends the identity of E to the identity of E'.

Theorem 3.29. *Two elliptic curves E and E' are isomorphic if and only if $j(E) = j(E')$.*

Proof. See Proposition 1.4 in page 50 of [Sil86]. □

There is a correspondence between isomorphism classes of elliptic curves and lattices modulo homotheties, so there are finitely many possible values for the j-invariants of elliptic curves with complex multiplication by $\mathcal{O}_K$. In fact, there are at most h_K possible such values.

On the other hand the group of field automorphisms of $\mathbb{C}$ acts on the set of elliptic curves with complex multiplication by $\mathcal{O}_K$ acting on the corresponding Weierstrass equations and therefore permutes the possible values of j. Since there are finitely many of them, we conclude that $j(E)$, the j-invariant of an elliptic curve E with complex multiplication by $\mathcal{O}_K$, is algebraic and $|\mathbb{Q}(j(E))\colon \mathbb{Q}| \leq h_K$. In fact, $|K(j(E))\colon K| = h_K$ and even more, $K(j(E))$ is the Hilbert class field of K (the maximal abelian extension of K which is unramified everywhere).

Of course, if K has class number 1, as in the case when $K = \mathbb{Q}(i)$, then $j(E)$ is a rational number. In fact it is an integer because in general $j(E)$ is an algebraic integer (which is more difficult to prove).

In general, $K(j(E), E[n])/K$ is a Galois extension but not always abelian. However, $K(j(E), E[n])/K(j(E))$ is indeed abelian. To get genuine abelian extensions of K one has to adjoin $E[n]$ only partially (usually the x-coordinates will do) and these extensions provide the solution to Kronecker's Jugendtraum (see Corollary 5.7 in chapter 2 of [Sil94]).

Appendix A

Straightedge and compass constructions

In this appendix we formalize what is a straightedge and compass construction introducing the concepts of constructible points and constructible numbers. We go on to characterize the regular polygons that can be constructed with straightedge and compass.

Definition A.1. A point P in the plane is *constructible with straightedge and compass* or *constructible* for short, if there is a sequence of points $P_0 = (0,0), P_1 = (1,0), P_2, \ldots, P_n = P$ such that for all $2 \leq i \leq n$, one of the following cases hold:

(i) P_i is the intersection point of two lines, each of which goes through two points P_j and P_k with $j, k < i$.

(ii) P_i is one of the intersection points of two circles, each of which has center in a point P_j and passes through another point P_k, with $j, k < i$.

(iii) P_i is one of the intersection points of a line joining two points P_j and P_k with $j, k < i$ and a circle with center P_l passing trough another point P_m with $l, m < i$.

Definition A.2. A complex number $z = a + bi$ is *constructible* if the point $P = (a, b)$ is constructible.

Remark. Notice that most of the classical constructions using straightedge and compass determine constructible points. In particular, the following points are constructible.

(i) The midpoint of a segment with constructible endpoints.

(ii) The points that complete a parallelogram, given three constructible points.

(iii) The midpoint of an arc with constructible endpoints and constructible center (bisection of an angle).

(iv) Given three constructible points A, B and C in a circle, the point X in the same circle such that $\widehat{BX} = \widehat{AC}$ (so that the arc $\widehat{AX}$ is the sum of $\widehat{AB}$ and $\widehat{AC}$; angle addition).

Theorem A.1. *The set of constructible numbers $\mathcal{C}$ is a subfield of $\mathbb{C}$.*

Proof. $\mathcal{C}$ is an additive subgroup of $\mathbb{C}$, because $0 \in \mathcal{C}$ by definition and it is closed for addition (by (ii) in the previous remark) and for taking additive inverses. For multiplication we consider the numbers in polar form. To prove that $\mathcal{C}$ is closed for multiplication, it suffices to prove closeness for multiplication of constructible positive real numbers, since adding the arguments can be done by (iv) in the remark. Similarly, to prove that $\mathcal{C}-\{0\}$ is closed for inversion, it is enough to consider real positive numbers. Both constructions are immediate from the pictures in Figure A.1. □

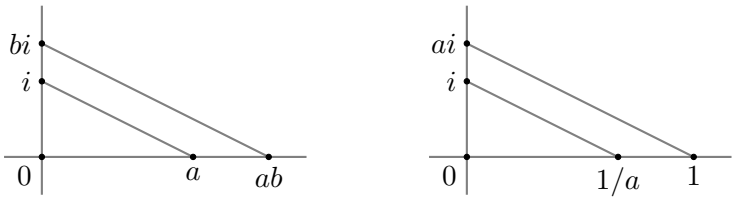

Figure A.1: Constructions for the product of two real constructible numbers and the inverse of a real constructible number.

Theorem A.2. *$\mathcal{C}$ is closed under taking square roots.*

Proof. Consider the numbers in polar form. To compute the square roots of a constructible number we need to bisect the argument ((iii) in the remark) and take the square root of its modulus (see Figure A.2). Since the angle at di is a right angle, the two small triangles that share side from 0 to di are similar. Consequently $1/d = d/r$, which shows that $d = \sqrt{r}$ is constructible. □

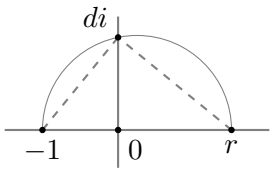

Figure A.2: Construction of the square root of a real constructible number.

Corollary A.3. *Let $F \subseteq \mathbb{C}$ be a field such that there exists a tower of subfields*

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n = F,\ [F_i : F_{i-1}] = 2,\ 1 \leq i \leq n. \tag{A.1}$$

Then $F \subseteq \mathcal{C}$.

Proof. Obviously $F_0 = \mathbb{Q} \subseteq \mathcal{C}$. Argue by induction using the fact that since $[F_i : F_{i-1}] = 2$, $F_i = F_{i-1}(\sqrt{u})$ for some $u \in F_{i-1}$ and $\mathcal{C}$ is closed under taking square roots. □

Theorem A.4. *Let $z \in \mathcal{C}$. Then there exists a tower of fields as in* (A.1) *such that $z \in F_n$. As a consequence z is algebraic and $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of* 2*.*

Proof. Observe that if (x, y) is a point of intersection between two lines, two circles or a line and a circle whose equations have coefficients in some field F, then $|F(x, y) : F| \leq 2$. Let z be a constructible number and take the sequence of numbers $0, 1, z_1, \ldots, z_n = z$, where $z_k = x_k + iy_k$, given by the constructibility of z. Consider the tower of fields

$$\mathbb{Q} \subset \mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n, \text{ where } F_k = F_{k-1}(x_k, y_k) \text{ for } 1 \leq k \leq n.$$

Then, $|F_k : F_{k-1}| \leq 2$ for $1 \leq k \leq n$ and $z \in F_n$. □

As a consequence of the previous theorem, the three classical problems have a negative solution.

(i) The duplication of the cube is not possible with straightedge and compass because $\sqrt[3]{2}$ is not constructible since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(ii) The angle trisection is not possible with straightedge and compass. Indeed, observe that the trisection of 60° implies the constructibility of $\cos 20°$, which contradicts that the minimal polynomial of $\cos 20°$ is $4x^3 - 3x - 1/2$.

(iii) The squaring of the circle is not possible with straightedge and compass because π is trascendental and thus not constructible.

Theorem A.5. *If a regular polygon of n sides is constructible then $n = 2^m p_1 \ldots p_r$, where $m \geq 0$ and $p_1, \ldots, p_r$ are Fermat primes.*

Proof. The constructibility of a regular polygon of n sides is equivalent to the constructibility of a primitive n-th root of unity, say $\zeta_n = e^{\frac{2\pi i}{n}}$. If ζ_n is constructible, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ is a power of 2 by Theorem A.4. Recall that if $n = q_1^{a_1} \ldots q_r^{a_r}$, where q_i are distinct primes, then

$$\varphi(n) = q_1^{a_1 - 1}(q_1 - 1) \ldots q_r^{a_r - 1}(q_r - 1).$$

If q_i is odd, then $q_i^{a_i - 1}(q_i - 1)$ is a power of 2, and so $a_i = 1$ and q_i is a Fermat prime. □

A number z with $[\mathbb{Q}(z) : \mathbb{Q}]$ a power of 2 is not necessarily constructible. We need a stronger condition, namely, that the normal closure of $\mathbb{Q}(z)/\mathbb{Q}$ has a power of 2 degree. We procede to prove that in fact this condition is necessary for z to be constructible.

Lemma A.6. *Let $E \subseteq F \subseteq \mathbb{C}$ be a field extension where $[F : E] = 2$ and $E/\mathbb{Q}$ is a Galois extension. Then, there exists a Galois extension $E'/\mathbb{Q}$ such that $F \subseteq E'$ and $[E' : E]$ is a power of 2.*

Proof. Since $[F : E] = 2$, $F = E(\sqrt{u})$ for some $u \in E$. Let $p(x)$ be the minimal polynomial of u over $\mathbb{Q}$ and consider $g(x) = p(x^2)$. Since $E/\mathbb{Q}$ is Galois, it is the splitting field of some polynomial $f(x) \in \mathbb{Q}[x]$. Let E' be the splitting field of $f(x)g(x)$. Then $E'/\mathbb{Q}$ is Galois and clearly $E \subseteq E'$. If $u_1 = u, u_2, \ldots, u_k$ are the roots of $p(x)$, then $\pm\sqrt{u_1}, \pm\sqrt{u_2}, \ldots, \pm\sqrt{u_k}$ are the roots of $g(x)$. As a consequence, $E' = E(\sqrt{u_1}, \ldots, \sqrt{u_k}) = F(\sqrt{u_2}, \ldots, \sqrt{u_k})$ and $[E' : F]$ is a power of 2. □

Theorem A.7. *Consider a tower of fields as in* (A.1)*. Then, there exists a Galois extension $E/\mathbb{Q}$ such that $F \subseteq E$ and $[E : \mathbb{Q}]$ is a power of 2.*

Proof. Proceed by induction. The case $n = 0$ is trivial. Assume the result is true for $n - 1$ and let's prove it for n. By induction, there exists a Galois extension $E/\mathbb{Q}$ such that $F_{n-1} \subseteq E$ and $[E : \mathbb{Q}]$ is a power of 2. Since $F_n = F_{n-1}(\sqrt{u})$, apply the previous lemma with $F = E(\sqrt{u})$. □

Theorem A.8. *Constructible numbers are cointained in Galois extensions of $\mathbb{Q}$ of degree a power of 2.*

Proof. Let $z \in \mathcal{C}$ and consider an extension as in (A.1), which exists by Theorem A.4. By the previous theorem, there exists a Galois extension $E/\mathbb{Q}$ such that $z \in E$ and $[E : \mathbb{Q}]$ is a power of 2. □

Observe that if z is a root of an irreducible quartic with Galois group not a 2-group then $\mathbb{Q}(z)/\mathbb{Q}$ has degree 4 but according to this last theorem z is not constructible.

Theorem A.9. *Let $E/\mathbb{Q}$ be a Galois extension of degree a power of 2. Then $E \subseteq \mathcal{C}$.*

Proof. Consider the group $G = \mathrm{Gal}(E/\mathbb{Q})$. Since $[E : \mathbb{Q}]$ is a power of 2, G is a 2-group. By a standard property of 2-groups, there exists a sequence of subgroups

$$1 = N_0 \leq N_1 \leq \ldots \leq N_n = G$$

such that $|N_i : N_{i-1}| = 2$ for $1 \leq i \leq n$. Applying the Galois correspondence, we get a tower of fields as in (A.1). By Corollary A.3, we get that $E \subseteq \mathcal{C}$. □

Theorem A.10. *Let $z \in \mathbb{C}$. Then z is constructible if and only if it is algebraic and the normal closure of $\mathbb{Q}(z)/\mathbb{Q}$ has degree a power of 2.*

Proof. Assume that z is constructible. Then by Theorem A.4, z is algebraic, and by Theorem A.8 the normal closure of $\mathbb{Q}(z)/\mathbb{Q}$ has degree a power of 2. For the converse, assume that z is algebraic and that the normal closure of $\mathbb{Q}(z)/\mathbb{Q}$, say F, has degree a power of 2. Then $F/\mathbb{Q}$ is Galois and has degree a power of 2, so by Theorem A.9, $F \subseteq \mathcal{C}$ and in particular z is constructible. □

Theorem A.11. *Assume that $n = 2^m p_1 \dots p_r$ where $m \geq 0$ and p_i are Fermat primes. Then, the regular polygon with n sides is constructible.*

Proof. In this case $\varphi(n)$ is a power of 2, so for a primitive n-th root of unity ζ_n, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension of degree a power of 2, which by Theorem A.10 is equivalent to ζ_n being constructible. □

Together, Theorems A.5 and A.11 characterize which regular polygons are constructible in terms of the number of sides they have. This characterization is known as Gauss-Wantzel Theorem.

Theorem A.12 (Gauss-Wantzel Theorem)**.** *A regular polygon with n sides is constructible if and only if $n = 2^m p_1 \dots p_r$ where $m \geq 0$ and p_i are Fermat primes.*

Proof. It follows from combining Theorems A.5 and A.11. □

Appendix B

Problems

Problem 1. Find a rational parametrization of the lemniscate. (Hint. By considering the intersection of the lemniscate with the lines $y = mx$ one gets an irrational parametization, which is transformed into a trigonometric parametrization with the change $m = \cos t$, which, as usual, finally yields a rational parametrization in terms of $s = \tan t/2$.)

Solution. Consider the intersection of the lemniscate with the lines $y = mx$, that is, the system

$$\begin{cases} (x^2 + y^2)^2 = x^2 - y^2 \\ y = mx. \end{cases}$$

After solving this system, one gets an irrational parametrization, which is transformed into a trigonometric parametrization with the change $m = \cos t$. To obtain a rational parametrization, use the change $s = \tan t/2$, which finnaly yields to

$$\begin{cases} x = \dfrac{s(1+s^2)}{s^4+1} \\ y = \dfrac{s(1-s^2)}{s^4+1}. \end{cases}$$

□

Problem 2. Compute the area enclosed by the lemniscate. (Hint. An easy computation using polar coordinates. Explain how to do it using cartesian coordinates.)

Solution. By symmetry, we only need to compute the area enclosed in the first quadrant. Using the polar equation of the lemniscate, we get that

$$A = 4\int_0^{\pi/4} \frac{r^2}{2} d\theta = \int_0^{\pi/4} 2\cos 2\theta d\theta = 1.$$

To compute the area in cartesian coordinates, we first write y as a function of x from the equation $(x^2+y^2)^2 = x^2-y^2$ and then compute the corresponding

integral

$$A = \int_0^1 \sqrt{\frac{-(2x^2-1) + \sqrt{(2x^2+1)^2 - 4x^2(x^2-1)}}{2}} dx.$$

Using the rational parametrization obtained in the previous exercise, this integral is equivalent to the following rational integral.

$$A = \int_{-\infty}^{\infty} \frac{s(1-2s^3-s^4-6s^5)}{(1+s^4)^2} ds.$$

□

Problem 3. The goal of this problem is to relate ϖ and π with the arithmetic-geometric mean of two positive numbers.

(i) Given $0 < a < b$ define the sequence $x_1 = a, x_2 = b, x_{2n+1} = \sqrt{x_{2n}x_{2n-1}}$, $x_{2n+2} = (x_{2n} + x_{2n-1})/2, n \geq 1$. Show that this sequence converges to a limit $a < l < b$, which is called the aritmetic-geometric mean of a and b. We denote it $\mathrm{agm}(a, b)$. (Hint. For any $x, y > 0$, $\sqrt{xy} \leq (x+y)/2$, so the odd terms of $\{x_n\}$ increase and the even terms decrease).

(ii) Let

$$I(a,b) = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(a^2+(b^2-a^2)t^2)}}.$$

Show that the changes of variables $t^2 = \frac{x^2}{x^2+b^2}$ and $x = s + \sqrt{s^2+ab}$ transform this integral into

$$I(a,b) = \int_0^{+\infty} \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}} = \int_0^{+\infty} \frac{ds}{\sqrt{(s^2+a_1^2)(s^2+b_1^2)}},$$

where $a_1 = \sqrt{ab}$ and $b_1 = \frac{a+b}{2}$. Conclude that $I(a,b) = I(a_1, b_1)$ and $I(a,b) = \frac{\pi}{2\mathrm{agm}(a,b)}$.

(iii) Show that $\varpi = \frac{\pi}{\mathrm{agm}(1,\sqrt{2})}$.

Solution.

(i) Observe that since $\sqrt{xy} \leq (x+y)/2, \forall x, y > 0$, it follows that $x_{2n+1} < x_{2n+2}, \forall n \geq 1$. From here we deduce that the sequence of odd (even) terms is increasing (decreasing):

$$x_{2n+3} = \sqrt{x_{2n+2}x_{2n+1}} > \sqrt{x_{2n+1}x_{2n+1}} = x_{2n+1}.$$

This implies that the sequence of odd (even) terms is upper (lower) bounded, $x_{2n+1} < x_{2n} < x_2 = b$, and hence it has limit l_1. Similarly, the sequence of even terms has limit l_2. By taking limits in any of the expressions defining the sequence, $l_1 = l_2 = l$, and so, the sequence is convergent with limit l.

(ii) It is a matter of routine calculations to check that the specified changes of variables transform the integral into the equivalent expressions. From this expressions it is clear that $I(a,b) = I(a_1,b_1)$, and as a consequence, $I(a,b) = I(x_{2n+1},x_{2n}), \forall n \geq 1$. In order to be able to take limits in this last expression, we need to apply the dominated convergence theorem. Since $\{x_n\}$ is bounded, there exists some constant $c > 0$ for which

$$\int_0^{+\infty} \frac{ds}{\sqrt{(s^2+a_n^2)(s^2+b_n^2)}} \leq \int_0^{+\infty} \frac{ds}{\sqrt{(s^2+c^2)(s^2+c^2)}} = \\ = \int_0^{+\infty} \frac{ds}{(s^2+c^2)} = \frac{\pi}{2c} < \infty.$$

As a consequence, by taking limits, $I(a,b) = I(\operatorname{agm}(a,b),\operatorname{agm}(a,b))$ and from here we deduce that

$$I(a,b) = I(\operatorname{agm}(a,b),\operatorname{agm}(a,b)) = \\ = \int_0^{+\infty} \frac{ds}{\sqrt{(s^2+\operatorname{agm}(a,b)^2)(s^2+\operatorname{agm}(a,b)^2)}} = \frac{\pi}{2\operatorname{agm}(a,b)}.$$

(iii)
$$\operatorname{agm}(1,\sqrt{2}) = \frac{2}{\pi} I(1,\sqrt{2}) = \frac{2}{\pi}\int_0^1 \frac{dt}{\sqrt{1-t^4}} = \frac{\varpi}{\pi}.$$

□

Problem 4. Define the *lemniscate cosine* function cl by $\operatorname{cl}(x) = \operatorname{sl}(\frac{\varpi}{2} - x)$.

(i) Use the addition formula for sl to prove that

$$\operatorname{sl}^2 x + \operatorname{cl}^2 x + \operatorname{sl}^2 x \operatorname{cl}^2 x = 1.$$

(ii) Show that $\operatorname{sl}' x = (1 + \operatorname{sl}^2 x)\operatorname{cl} x$.

(iii) Prove that

$$\operatorname{sl}(u+v) = \frac{\operatorname{sl} u \operatorname{cl} v + \operatorname{cl} u \operatorname{sl} v}{1 - \operatorname{sl} u \operatorname{sl} v \operatorname{cl} u \operatorname{cl} v}.$$

Solution.

(i) By the addition formula and the identity for sl' we get

$$\operatorname{cl}(x) = \operatorname{sl}(\varpi/2 - x) = \frac{\pm\sqrt{1-\operatorname{sl}^4(x)}}{1+\operatorname{sl}^2(x)}.$$

From which follows that

$$(\operatorname{cl}(x) + \operatorname{cl}(x)\operatorname{sl}^2(x))^2 = 1 - \operatorname{sl}^4(x).$$

After expanding and factorizing accordingly, we get the following equality,

$$(\mathrm{sl}^2(x) + \mathrm{cl}^2(x) + \mathrm{sl}^2(x)\mathrm{cl}^2(x))(1 + \mathrm{sl}^2(x)) = |1 + \mathrm{sl}^2(x)|,$$

from which the result follows.

(ii) From (i) it follows that

$$\mathrm{cl}^2(x)(1 + \mathrm{sl}^2(x)) = 1 - \mathrm{sl}^2(x).$$

Multiplying both sides of the equation by $1+\mathrm{sl}^2(x)$ and taking square roots, we get

$$|\mathrm{cl}(x)|(1 + \mathrm{sl}^2(x)) = |\mathrm{sl}'(x)|,$$

by using the formula for $\mathrm{sl}'(x)$. Since $\mathrm{sl}'(x)$ and $\mathrm{cl}(x)$ have the same sign in $[-\varpi/2, 3\varpi/2]$, then by periodicity they have the same sign in $\mathbb{R}$, and so we get the desired equality.

(iii) By the addition formula

$$\mathrm{sl}(u + v) = \frac{\mathrm{sl}(u)\mathrm{sl}'(v) + \mathrm{sl}'(u)\mathrm{sl}(v)}{1 + \mathrm{sl}^2(u)\mathrm{sl}^2(v)}.$$

After multiplying and dividing by $1 - \mathrm{sl}(u)\mathrm{sl}(v)\mathrm{cl}(u)\mathrm{cl}(v)$, one can factorize the numerator into $(\mathrm{sl}(u)\mathrm{cl}(v)+\mathrm{sl}(v)\mathrm{cl}(u))(1+\mathrm{sl}^2(u)\mathrm{sl}^2(v))$, from which the result follows.

□

Problem 5.

(i) Show that $\mathrm{sl}(mx) \in \mathbb{Q}(\mathrm{sl}(x), \mathrm{sl}'(x))$. Conclude that if the point in the lemniscate with arc length u is constructible, so are the points with arc length mu. In particular, if $\mathrm{sl}(2\varpi/n)$ is constructible, so are all the nth division points of the lemniscate.

(ii) Show that if $\mathrm{sl}(2\varpi/n)$ and $\mathrm{sl}(2\varpi/m)$ are constructible, $\mathrm{sl}(2\varpi/l)$, where l is the least common multiple of n and m, is also constructible. (Hint. Use Bezout's identity.)

Solution.

(i) By induction on m, we will show that both $\mathrm{sl}(mx)$ and $\mathrm{sl}'(mx)$ belong to $F = \mathbb{Q}(\mathrm{sl}(x), \mathrm{sl}'(x))$. First observe that $\mathrm{sl}(0) = 0 \in F$ and $\mathrm{sl}'(0) = 1 \in F$. Now let $m \geq 1$ and assume the result is true for all $n < m$. Then, by the addition formula

$$\mathrm{sl}(mx) = \mathrm{sl}((m-1)x + x) = \frac{\mathrm{sl}(x)\mathrm{sl}'((m-1)x) + \mathrm{sl}'(x)\mathrm{sl}((m-1)x)}{1 + \mathrm{sl}^2(x)\mathrm{sl}^2((m-1)x)}.$$

By the induction hypothesis $\mathrm{sl}((m-1)x)$ and $\mathrm{sl}'((m-1)x)$ are in F, and so $\mathrm{sl}(mx) \in F$. Now consider

$$\mathrm{sl}((m-1)x) = \mathrm{sl}(mx - x) = \frac{\mathrm{sl}(mx)\mathrm{sl}'(x) - \mathrm{sl}'(mx)\mathrm{sl}(x)}{1 + \mathrm{sl}^2(x)\mathrm{sl}^2(mx)}.$$

From this expression we can write

$$\mathrm{sl}'(mx) = \frac{\mathrm{sl}((m-1)x)(1 + \mathrm{sl}^2(x)\mathrm{sl}^2(mx)) - \mathrm{sl}(mx)\mathrm{sl}'(x)}{\mathrm{sl}(x)},$$

and since $\mathrm{sl}(x), \mathrm{sl}'(x), \mathrm{sl}((m-1)x)$ and $\mathrm{sl}(mx)$ are in F, it follows that $\mathrm{sl}'(mx) \in F$.

Now assume that the point in the lemniscate (x, y) with arc length u is constructible. Then

$$\mathrm{sl}(u) = r = \sqrt{x^2 + y^2}$$

is constructible, and since $\mathcal{C}$ is closed under taking square roots,

$$\mathrm{sl}'(u) = \sqrt{1 - \mathrm{sl}^4(u)}$$

is also constructible. Consequently, $F \subset \mathcal{C}$, and thus, by part (i), $\mathrm{sl}(mu)$ is constructible. In particular, this implies that the point in the lemniscate with arc length mu is constructible.

If we assume that $\mathrm{sl}(2\varpi/n)$ is constructible, then the points in the lemniscate with arc length $2m\varpi/n$ are also constructible, and thus all nth division points of the lemniscate are constructible.

(ii) Let $l = lcm(m, n)$ and $d = mcd(m, n)$. By Bezout's identity, there exist $x, y \in \mathbb{Z}$ such that $nx + my = d$. Then

$$\frac{y}{n} + \frac{x}{m} = \frac{my + nx}{nm} = \frac{d}{nm} = \frac{1}{l}.$$

Then, applying the addition formula we get

$$\mathrm{sl}\left(\frac{2\varpi}{l}\right) = \mathrm{sl}\left(y\frac{2\varpi}{n} + x\frac{2\varpi}{m}\right) = \frac{\mathrm{sl}\left(x\frac{2\varpi}{m}\right)\mathrm{sl}'\left(y\frac{2\varpi}{n}\right) + \mathrm{sl}'\left(x\frac{2\varpi}{m}\right)\mathrm{sl}\left(y\frac{2\varpi}{n}\right)}{1 + \mathrm{sl}^2\left(x\frac{2\varpi}{m}\right)\mathrm{sl}^2\left(y\frac{2\varpi}{n}\right)}.$$

If we assume that $\mathrm{sl}(2\varpi/m)$ and $\mathrm{sl}(2\varpi/n)$ are constructible, then by part (i) so are $\mathrm{sl}(2x\varpi/m)$ and $\mathrm{sl}(2y\varpi/n)$, and thus, $\mathrm{sl}(2\varpi/l)$ is constructible too.

□

Problem 6. Use $\sin((m+1)x)+\sin((m-1)x)=2\sin(mx)\cos(x)$ to prove that there exist polynomials $P_m(x)$ such that $\sin(mx)=\sin(x)P_m(\sin^2(x))$ if m is odd and $\sin(mx)=\sin(x)\cos(x)P_m(\sin^2(x))$ if m is even. Find recurrence formulas for these polynomials.

Solution. Proceed by induction. The cases $m=0$ and $m=1$ trivially hold true with $P_0(x)=0$ and $P_1(x)=1$. Let $m\geq 3$ and assume that the result is true for $n\leq m$. Then, if $m+1$ is odd

$$\begin{aligned}\sin((m+1)x) &= 2\sin(mx)\cos(x)-\sin((m-1)x)= \\ &= 2\sin(x)\cos^2(x)P_m(\sin^2(x))-\sin(x)P_{m-1}(\sin^2(x))= \\ &= \sin(x)(2P_m(\sin^2(x))-2\sin^2(x)P_m(\sin^2(x))-P_{m-1}(\sin^2(x)))= \\ &= \sin(x)P_{m+1}(\sin^2(x)),\end{aligned}$$

where $P_{m+1}(x)=2P_m(x)(1-x)-P_{m-1}(x)$.

Similarly, when $m+1$ is even we have

$$\begin{aligned}\sin((m+1)x) &= 2\sin(mx)\cos(x)-\sin((m-1)x)= \\ &= 2\sin(x)\cos(x)P_m(\sin^2(x))-\sin(x)\cos(x)P_{m-1}(\sin^2(x))= \\ &= \sin(x)\cos(x)P_{m+1}(\sin^2(x)),\end{aligned}$$

where $P_{m+1}(x)=2P_m(x)-P_{m-1}(x)$. □

Problem 7. The polynomials $xP_n(x^4)$ (n odd) and $x(1-x^2)P_n(x^4)$ (n even) are called the nth *division polynomials* of the lemniscate. Show that $\mathrm{sl}(m\frac{2\varpi}{n})$, $m\in\mathbb{Z}$ are real roots of modulus smaller than 1 of these polynomials.

Solution. By periodicity of sl, we have that $\mathrm{sl}(2m\varpi)=\mathrm{sl}(0)=0$, for all $m\in\mathbb{Z}$. Thus, $\mathrm{sl}(n\frac{2m\varpi}{n})=0$. If n is odd, then

$$\begin{aligned}0=\mathrm{sl}\left(n\frac{2m\varpi}{n}\right)&=\mathrm{sl}\left(\frac{2m\varpi}{n}\right)R_n\left(\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right)= \\ &=\mathrm{sl}\left(\frac{2m\varpi}{n}\right)\frac{P_n\left(\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right)}{Q_n\left(\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right)}.\end{aligned}$$

Thus, $\mathrm{sl}(\frac{2m\varpi}{n})$ is a root of the polynomial $xP_n(x^4)$ for all $m\in\mathbb{Z}$.

Conversly, assume that r is a real root of $xP_n(x^4)$ with modulus $|r|\leq 1$ and let $u=\mathrm{arcsl}(r)$, so that $\mathrm{sl}(u)=r$. Then

$$0=rP_n(r^4)=\mathrm{sl}(u)P_n(\mathrm{sl}^4(u))=\mathrm{sl}(u)\frac{P_n(\mathrm{sl}^4(u))}{Q_n(\mathrm{sl}^4(u))}=\mathrm{sl}(u)R_n(\mathrm{sl}^4(u))=\mathrm{sl}(nu).$$

Since the zeros of sl are of the form $2m\varpi$ with $m \in \mathbb{Z}$, it follows that $r = \mathrm{sl}(\frac{2m\varpi}{n})$ for some $m \in \mathbb{Z}$.

In the case where n is even, we proceed analogously. Using the formula for sl', we get

$$0 = \mathrm{sl}\left(n\frac{2m\varpi}{n}\right) = \mathrm{sl}\left(\frac{2m\varpi}{n}\right)\mathrm{sl}'\left(\frac{2m\varpi}{n}\right)R_n\left(\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right) =$$
$$= \mathrm{sl}\left(\frac{2m\varpi}{n}\right)\sqrt{1-\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)}\frac{P_n\left(\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right)}{Q_n\left(\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right)}.$$

By taking squares at both sides, this means that

$$0 = \mathrm{sl}^2\left(\frac{2m\varpi}{n}\right)\left(1-\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right)P_n^2\left(\mathrm{sl}^4\left(\frac{2m\varpi}{n}\right)\right).$$

Hence, $\mathrm{sl}(\frac{2m\varpi}{n})$ is a root of the polynomial $x^2(1-x^4)P_n^2(x^4)$. Since $1-x^4 = (1+x^2)(1-x^2)$ and $(1+x^2)$ has no real roots, it follows that $\mathrm{sl}(\frac{2m\varpi}{n})$ is a root of the polynomial $x^2(1-x^2)P_n^2(x^4)$.

Conversly, assume that r is a real root of $x^2(1-x^2)P_n^2(x^4)$ with modulus $|r| \leq 1$ and let $u = \mathrm{arcsl}(r)$, so that $\mathrm{sl}(u) = r$. Then r is a root of $x^2(1-x^4)P_n^2(x^4)$, and thus

$$0 = \mathrm{sl}^2(u)(1-\mathrm{sl}^4(u))P_n^2(\mathrm{sl}^4(u)).$$

Then, dividing by $Q_n^2({}^4(u))$ at both sides and then taking square roots, it follows that

$$0 = \mathrm{sl}(u)\mathrm{sl}'(u)R_n(\mathrm{sl}^4(u)) = \mathrm{sl}(nu).$$

Similarly, as before, since the zeros of sl are of the form $2m\varpi$ with $m \in \mathbb{Z}$, it follows that $r = \mathrm{sl}(\frac{2m\varpi}{n})$ for some $m \in \mathbb{Z}$.

□

Problem 8. Let n be an odd number and P_n the polynomial in Problem 6.

(i) Show that $\sin nx = (-1)^{(n-1)/2}T_n(\sin x)$, where T_n is the n-th Chebyshev polynomial, so $T_n(x) = xP_n(x^2)$. (Chebyshev polynomials are defined by the relation $\cos nx = T_n(\cos x)$.)

(ii) Show that the roots of T_n are

$$\{\sin(k\pi/n)|k \in \mathbb{Z}\} = \{\sin(k\pi/n), k = 0, \ldots, n-1\} =$$
$$= \{\sin(2k\pi/n)|k \in \mathbb{Z}, k \text{ odd}\}.$$

Conclude that $\mathbb{Q}(\sin(2\pi/n))$ is the splitting field of T_n over $\mathbb{Q}$, so $\mathbb{Q}(\sin(2\pi/n))/\mathbb{Q}$ is a Galois extension.

(iii) Let G be the Galois group of the extension $\mathbb{Q}(\sin(2\pi/n))/\mathbb{Q}$. If $\sigma \in G$, then $\sigma(\sin(2\pi/n)) = \sin(2k\pi/n)$ for some odd integer k, which is unique mod n. Show that the map $\rho\colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\sigma_k \mapsto \overline{k}$ is a well-defined injective homomorphism.

(iv) Show that $\mathbb{Q}(i, \sin(2\pi/n)) = \mathbb{Q}(i, \zeta_n)$, where ζ_n is a primitive n-th root of unity. (Hint. Use the double angle formula for $\sin(4\pi/n)$.) What is the degree of $\mathbb{Q}(\sin(2\pi/n))/\mathbb{Q}$? Conclude that the homomorphism ρ in (iii) is an isomorphism. (Hint. The key is that $i \notin \mathbb{Q}(\zeta_n)$ because $i\zeta_n$ is a primitive $4n$-th root of unity.). Show also that the Galois group of $\mathbb{Q}(i, \sin(2\pi/n))/\mathbb{Q}(i)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

(v) Show that if p is an odd prime, $T_p(x)/x$ is an irreducible polynomial over $\mathbb{Q}(i)$.

Solution. (i) It follows by replacing x by $\pi/2 - x$ in the definition of T_n.

(ii) Clearly $T_n(\sin k\pi/n) = 0$ and the first equality holds. On the other hand, $\deg(T_n) = n$ so these are all roots of T_n. To show the second equality, notice that if k is odd, then $\sin\frac{k\pi}{n} = \sin(\pi - \frac{k\pi}{n}) = \sin(\frac{(n-k)\pi}{n})$ and $n - k$ is even. Then every root is of the form $\sin\frac{2k\pi}{n}$, and if k is even consider $\sin\frac{2k\pi}{n} = \sin(2\pi + \frac{k\pi}{n}) = \sin(\frac{2(n+k)\pi}{n})$. Since $\sin(k\frac{2\pi}{n}) = (-1)^{(n-1)/2}T_k(\sin\frac{2\pi}{n}) \in \mathbb{Q}(\sin\frac{2\pi}{n})$ for k odd, T_n splits over $\mathbb{Q}(\sin\frac{2\pi}{n})$ and so it is the splitting field of T_n.

(iii) Since σ permutes the roots of T_n, $\sigma(\sin(2\pi/n)) = \sin(2k\pi/n)$ for some odd integer k. Then, if $\sin(2k\pi/n) = \sin(2m\pi/n)$, using that $\sin x = \sin y$ if and only if $y = (-1)^l x + l\pi$ and that k, m, n are odd, we conclude that l is even and that k is unique mod n. If we denote σ by σ_n we get

$$\begin{aligned}(\sigma_k \cdot \sigma_m)(\sin(2\pi/n)) &= \sigma_k(\sigma_m(\sin(2\pi/n))) = \sigma_k(\sin(2m\pi/n)) = \\ &= \sigma_k((-1)^{(n-1)/2}T_m(\sin(2\pi/n))) = \\ &= (-1)^{(n-1)/2}T_m(\sin(2k\pi/n)) = \sin(2km\pi/n),\end{aligned}$$

that is, $\sigma_k \cdot \sigma_m = \sigma_{km}$. The inverse of σ_k is of the form σ_m, and $\sigma_k \cdot \sigma_m = \sigma_{km} = \sigma_1$, so $kl \equiv 1 \pmod{n}$, and so $(k, n) = 1$. Consequently, the map $\rho\colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ given by $\sigma_k \mapsto \overline{k}$ is a well-defined monomorphism.

(iv) The inclusion $\mathbb{Q}(i, \sin(2\pi/n)) \subseteq \mathbb{Q}(i, \zeta_n)$ follows from the fact that $\sin(2\pi/n) = (\zeta - \zeta^{-1})/2i$. By (ii), $\sin(4\pi/n) \in \mathbb{Q}(i, \sin(2\pi/n))$, and using the double angle formula, it follows that $\cos(2\pi/n) = \sin(4\pi/n)/(2\sin(2\pi/n)) \in \mathbb{Q}(i, \sin(2\pi/n))$. As a consequence, $\zeta_n \in \mathbb{Q}(i, \sin(2\pi/n))$, and the reverse inclusion holds.

Observe $[\mathbb{Q}(\zeta_n, i)\colon \mathbb{Q}(\zeta_n] \leq [\mathbb{Q}(i)\colon \mathbb{Q}] = 2$. Assume it is 1. Then, $i \in \mathbb{Q}(\zeta_n)$, so in particular $i\zeta_n \in \mathbb{Q}(\zeta_n)$. Since n is odd, $i\zeta_n$ is $4n$-th primitive root of unity, and we get a contradiction by studying the degrees of the tower of fields $\mathbb{Q} \subset \mathbb{Q}(i\zeta_n) \subset \mathbb{Q}(\zeta_n)$. Thus, $[\mathbb{Q}(\zeta_n, i)\colon \mathbb{Q}(\zeta_n] = 1$, from which we deduce that $[\mathbb{Q}(\zeta_n, i)\colon \mathbb{Q}] = 2\varphi(n)$.

As a consequence, $[\mathbb{Q}(\sin(2\pi/n), i)\colon \mathbb{Q}] = 2\varphi(n)$. Similarly as before, $[\mathbb{Q}(\sin(2\pi/n), i)\colon \mathbb{Q}(\sin(2\pi/n))] \leq 2$, and since $\mathbb{Q}(\sin(2\pi/n)) \subset \mathbb{R}$, we conclude that $[\mathbb{Q}(\sin(2\pi/n))\colon \mathbb{Q}] = \varphi(n)$. Then, $|G| = \varphi(n)$, and since $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ too, it follows that the monomorphism ρ of (iii) is an isomorphism. Consider the map

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\sin(2\pi/n), i)/\mathbb{Q}(i)) &\to \mathrm{Gal}(\mathbb{Q}(\sin(2\pi/n))/\mathbb{Q}) \\ \sigma &\mapsto \sigma\big|_{\mathbb{Q}(\sin(2\pi/n))}. \end{aligned}$$

It is a well defined homomorphism, and clearly injective. Since both extensions have the same degree, it is also bijective and thus and isomorphism. Consequently, $\mathbb{Q}(i, \sin(2\pi/n))/\mathbb{Q}(i)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

(v) If p is an odd prime then $[\mathbb{Q}(\sin(2\pi/p), i)\colon \mathbb{Q}(i)] = \varphi(p) = p - 1$. Then, since $\sin(2\pi/p)$ is a root of the polynomial $T_p(x)/x$ and it has degree $p - 1$, it follows that $T_p(x)/x$ is the minimal polynomial of $\sin(2\pi/p)$ over $\mathbb{Q}(i)$ and hence irreducible. □

Problem 9. Let p be an odd prime number and T_p the p-th Chebyshev polynomial. Prove using Theorem 2.10 that $T_p(x)/x$ is irreducible over $\mathbb{Q}$.

Solution. $\deg(T_p(x)/x) = p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$. By Problem 8, $T_p(x)/x = P_n(x^2)$, where P_n is defined in Problem 6, so by induction, the leading coefficient of $T_p(x)/x$ is 2^{p-1} and no odd prime divides it. Furthermore, this problem says that

$$\sin px = (-1)^{(p-1)/2} T_p(\sin x),$$

where $T_p \in \mathbb{Z}[x]$, and $\sin x$ has power series expansion $\sin x = x + \ldots$ Hence, applying Theorem 2.10, it follows that $T_p(x)/x$ is irreducible over $\mathbb{Q}$. □

Bibliography

[CH14] David A. Cox and Trevor Hyde. The Galois theory of the lemniscate. *Journal of Number Theory*, **135** (2014) 43–59.

[Cox12] David A. Cox. *Galois Theory*. John Wiley & Sons Ltd., Hoboken, New Jersey, second edition, 2012.

[Kob84] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer, New York, 1984.

[Ros13] Michael Rosen. Abel's Theorem on the Lemniscate. *The American Mathematical Monthly*, **88** (2013) 387–395.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, New York, 1994.

[ST15] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer, New York, second edition, 2015.

[Tak03] Teji Takagi. *Über die im Bereich der rationalen complexen Zahlen Abel'schen Zahlkörper*. Ph.D. thesis, J. College of Science, Imperial Univ. of Tokyo, 1903.