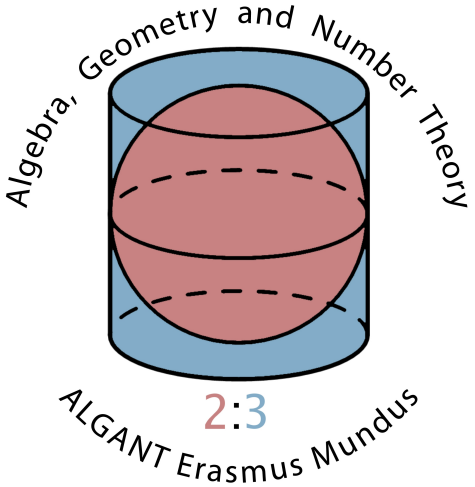


Takagi's Theorem on lemniscate extensions

Roberta LUBIANA

Advised by Prof. Boas EREZ

ALGANT Master Thesis - July 2014
Università degli Studi di Milano and Université Bordeaux 1

Takagi's Theorem on lemniscate extensions

Roberta Lubiana

July 2014

Contents

Introduction

The existence of consistent similarities between the theories related to the division of the circle and that of the lemniscate was firstly recognized by Gauss in the *Discquisitiones Arithmeticae*. There, while proving that a regular n-gon can be constructed with ruler and compass if $n = 2^a p_1 p_2 \dots p_t$ where the p_j are distinct Fermat primes, the mathematician stated that the principles underlying that theory apply not only to circular functions like sine and cosine, but also to the transcendental functions "that depend on the integral $\int dt/\sqrt{1-t^4}$ " which parametrizes the lemniscate ([14]). Abel, during his work on the division equations on the elliptic functions, came across the hint given by Gauss, and he was able to prove in his *Recherches sur les fonctions elliptiques* ([1], [2]) that

Proposition. The lemniscate can be divided into n equal parts with ruler and compass if $n = 2^a p_1 p_2 \dots p_t$ where the p_j are distinct Fermat primes.

Later, in 1853, Kronecker stated what we currently know as Kronecker-Weber's theorem:

Theorem. *Every finite abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field.*

and in the same paper ([13]) he also suggested that all the finite abelian extensions of the quadratic field can be obtained by dividing the lemniscate instead of the circle. As Iwasawa reports in [11], this conjecture was the origin of *Kronecker's Jugendtraum*, the conjecture stating (in its precise form) that *all abelian extensions of an imaginary quadratic field k can be generated by singular values of the elliptic modular function and by the values of the corresponding elliptic functions in the division points* ([19], § 4.3, p. 79). In 1903, in his doctoral thesis [17], Takagi was able to prove the conjecture regarding $\mathbb{Q}(i)$, adapting to this case the ideas used in the proof of the Kronecker-Weber theorem given by Hilbert in 1896 (a modern account of that proof can be found in [8]). Later, in 1920, Takagi was also able to prove the general conjecture in his paper "*Über eine Theorie der relativ-Abel'schen Zahlkörper*" [18] using mainly class field theory and a few facts about elliptic and modular function.

Even though the similarities between the case of the circle and that of the lemniscate are profound, as we have pointed out, they do not go as far as one could expect. An example of a negative result is Leopoldt's Theorem. If $\mathbb{Q} \subset N$ is a finite abelian extension with Galois group Γ, and if set

$$\Lambda = \{\lambda \in \mathbb{Q}\Gamma | \lambda \mathcal{O}_N \subseteq \mathcal{O}_N\}$$

then Leopoldt's Theorem states that the ring of integers $\mathcal{O}_N$ is isomorphic to Λ as a Λ-module and that we can find some idempotents e_i linked to the ramification of the extension $N/\mathbb{Q}$ such that $\Lambda = \bigoplus_i \mathbb{Z}\Gamma e_i$. Recall that

Definition. We say that a Galois extension $\mathbb{Q} \subset N$ admits a *normal integral basis* if the ring $\mathcal{O}_N$ of integers in N admits a $\mathbb{Z}$-basis consisting of the translates of a single element by the elements in the Galois group of $\mathbb{Q} \subset N$.

Then, as a Corollary of Leopoldt's Theorem we can obtain the following result:

Hilbert-Speiser Theorem. If $\mathbb{Q} \subset N$ is a tame extension, then $\mathbb{Q} \subset N$ has a normal integral basis.

Unluckily, the result is not true for the extensions with base field $\mathbb{Q}(i)$, since we can actually prove that

Theorem. *For every number field K different from $\mathbb{Q}$, there exists a finite tamely ramified abelian extension of K that doesn't have a normal integral basis.*

Since Leopoldt's theorem can be proven exploiting Kronecker-Weber's theorem and the peculiar features of the cyclotomic fields, it seems natural to wonder whether we can use Takagi's theorem on the division of the lemniscate with some additional conditions in order to obtain a similar result. The main motivation of this thesis is exactly this one: we are going to follow Takagi's first paper [17], and give a detailed account of the explicit construction of the fields obtained by the division of the lemniscate, in order to fully understand the structure of those fields, that we could possibly use in the future to investigate the problem of finding a normal basis at least for some tame extension of $\mathbb{Q}(i)$.

Finally, the structure of this Thesis is going to be the following. In Chapter 1, we are going to define and study the function sin am(z) (which will play the same role of the sine in the circle case), its relation with a certain Weierstrass $\wp$-function, and we will give an accurate description of the formulas that are involved in its complex multiplication by $\mathbb{Z}[i]$. In Chapter 2, we will describe the fields that we can obtain by considering the division point of the lemniscate, and we will analize which are the primes that ramify in those extensions of $\mathbb{Q}(i)$, and finally the whole third Chapter will be dedicated to the proof of Takagi's Theorem.

Chapter 1

Fundamental tools

1.1 Parametrization of the lemniscate

In the following discussion, we are going to use the useful relations that may be obtained by considering a special parametrization of the lemniscate. First of all, let us recall

Definition 1.1.1. Given two fixed point $\mathfrak{n}_1$,$\mathfrak{n}_2$ and a constant c, the associated lemniscate is the locus of all the points P such that the product of the distance between P and $\mathfrak{n}_1$ with the distance between P and $\mathfrak{n}_2$ has constant value c^2.

We are interested in a peculiar lemniscate, the one where the fixed points have coordinates $(-\frac{1}{\sqrt{2}}, 0)$ and $(\frac{1}{\sqrt{2}}, 0)$, and where $c = \frac{1}{\sqrt{2}}$. With this choice, we get the familiar horizontal figure 8 and a parametrization in cartesian coordinates

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

which translates in polar coordinates to

$$r^2 = \cos(2\theta)$$

If $s = s(r)$ is the arc length associated to the lemniscate, it is clear that (denoting with a dot the differentiation with respect to r)

$$\dot{s} = \dot{x} + \dot{y}$$

and so we obtain by direct computation (see [15], Chapter 1) that

$$ds = \frac{dr}{\sqrt{1 - r^4}}$$

So if we measure arc-length starting from the origin and passing into the first quadrant, by integrating we have the explicit relation

$$s = s(r) = \int_0^r \frac{dt}{\sqrt{1 - t^4}} \qquad \text{for } 0 \leq r < 1$$

Note that for $r = 1$ this integral is improper, but since it converges, its value is the arc length of the first quadrant portion of the lemniscate. In this context, we set

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

so that, due to the symmetry of the lemniscate, and the fact that r increases in each quadrant from 0 to 1, the total arch length is 2ω.

Definition 1.1.2. For every $v \in \mathbb{R}$ such that $|v| < \frac{\omega}{2}$ consider the element $x \in \mathbb{R}$ such that

$$v = \int_0^x \frac{dt}{\sqrt{1-t^4}}$$

Then, setting $A = \{v \in R || v| < \frac{\omega}{2}\}$ we define a function as

$$\begin{array}{rccc} \text{sin am} : A & \to & \mathbb{R} \\ v & \mapsto & x \end{array}$$

Moreover, for $v \in A$, we set

$$\text{cos am}(v) = \sqrt{1 - \text{sin am}^2(v)}$$

$$\Delta \text{ am}(v) = \sqrt{1 + \text{sin am}^2(v)}$$

Remark 1.1.1. With this definition, $r = \text{sin am}(s)$ if and only if s is the arc length from the origin to the point with polar coordinates (r, θ) in the upper semiplane of $\mathbb{R}^2$.

Now we would like to extend this definition to arbitrary real values of v. Given the resemblance to the trigonometric case, the idea is to find an addition formula for the integral. If we consider $u, v \in A$, and $x_u = \text{sin am}(u), x_v = \text{sin am}(v)$, it is possible to prove that there is an $r \in \mathbb{R}$ such that

$$u + v = \int_0^{x_u} \frac{dt}{\sqrt{1-t^4}} + \int_0^{x_v} \frac{dt}{\sqrt{1-t^4}} = \int_0^r \frac{dt}{\sqrt{1-t^4}}$$

and (as it is described in [15], Chapter 1)

$$r = \frac{x_u\sqrt{1-x_v^4} + x_v\sqrt{1-x_u^4}}{1 + x_u^2 x_v^2} \tag{1.1}$$

Hence, we can set

$$\text{sin am}(u + v) := r$$

and this formula gives us the possibility to extend the domain of our function to the whole $\mathbb{R}$.

Noticing that under the transformation $t \mapsto it$ the expression $dt/\sqrt{1-t^4}$ is multiplied by i, Gauss set

$$\text{sin am}(iv) := i \text{ sin am}(v)$$

At this point, it is clear how to define sin am$(u+iv)$ for arbitrary $u, v \in \mathbb{R}$.

Moreover, now that we have defined sin am(z) for arbitrary complex values, we can easily prove the following

Proposition 1.1.1. *The function sin am(z) is analytic on*

$$\Omega = \{z \in \mathbb{C} | z \neq (m+in)\frac{\omega}{2},\ m, n \in \mathbb{Z}\}$$

Proof. Let $z = x + iy$, with $x, y \in \mathbb{R}$. Looking at Eq. (1.1), it is clear that sin am(z) is not defined only for those elements for which

$$1 + \text{sin am}^2(x)\text{sin am}^2(iy) = 1 - \text{sin am}^2(x)\text{sin am}^2(y) = 0$$

Since by definition sin am$^2(x) \leq 1$ for all $x \in \mathbb{R}$, and the equality holds if and only if x is an odd multiple of $\frac{\omega}{2}$, sin am is defined on the open set

$$\Omega = \{z \in \mathbb{C} | z \neq (m+in)\frac{\omega}{2},\ m, n \in \mathbb{Z}\}$$

As $(\text{sin am}'(x))^2 = 1 - \text{sin am}^4(x)$ for all $x \in \mathbb{R}$ (see [4], Proposition 15.2.1), sin am(x) is infinitely differentiable on $\mathbb{R}$, so if we denote $f(x,y)$ and $g(x,y)$ the real and imaginary part of the right-hand side of Eq. (1.1), it is clear that they are differentiable on Ω as functions of (x,y). So we are only left to show that $f(x,y)$ and $g(x,y)$ satisfy the Cauchy-Riemann conditions, but since we have that

$$\begin{aligned} f(x,y) &= \frac{\text{sin am}(x)\sqrt{1-\text{sin am}^4(y)}}{1-\text{sin am}^2(x)\text{sin am}^2(y)} = \frac{\text{sin am}(x)\text{sin am}'(y)}{1-\text{sin am}^2(x)\text{sin am}^2(y)} \\ g(x,y) &= \frac{\text{sin am}(y)\sqrt{1-\text{sin am}^4(x)}}{1-\text{sin am}^2(x)\text{sin am}^2(y)} = \frac{\text{sin am}(y)\text{sin am}'(x)}{1-\text{sin am}^2(x)\text{sin am}^2(y)} \end{aligned}$$

this is only matter of a straightforward computation. □

This Proposition leads to the following result, that we will use extensively in this thesis:

Corollary 1.1.1. *The addition law*

$$sin\ am(u+v) = \frac{sin\ am(u)cos\ am(v)\Delta\ am(v) + sin\ am(v)cos\ am(u)\Delta\ am(u)}{1 + sin\ am^2(u)sin\ am^2(v)} \tag{1.2}$$

holds for all $u, v \in \mathbb{C}$ such that both sides are defined.

The proof can be found in [4], Proposition 15.3.1: it uses only the fact that sin am(z) is analytical and that Eq.(1.1) holds for $\mathbb{R}$.

1.2 Some properties of sin am

First of all we have to note that as a function of a complex variable, this new function sin am is doubly periodic, of periods $(1+i)\omega$ and $(1-i)\omega$. This can be seen manipulating the equation given in the previous Corollary. In fact, since by definition $\text{sin am}(\frac{\omega}{2}) = 1$, and since $\text{sin am}(iu) = i\text{sin am}(u)$ for every $u \in \mathbb{C}$, it holds that

$$\cos \text{am}(\pm\frac{\omega}{2}) = 0 = \Delta \text{ am}(\pm\frac{\omega}{2}i)$$

so if we substitute v with $\pm\frac{\omega}{2}$ or $\pm\frac{\omega}{2}i$ in Eq.(1.2) we get

$$\begin{aligned} \text{sin am}(u \pm \frac{\omega}{2}) &= \pm\frac{\cos \text{am}(u)}{\Delta \text{ am}(u)} \\ \text{sin am}(u \pm \frac{\omega}{2}i) &= \pm\frac{\Delta \text{ am}(u)}{\cos \text{am}(u)}i \end{aligned}$$

At this point, we have to remark that for every $v \in \mathbb{C}$ from the equation $\text{sin am}(iv) = i\text{sin am}(v)$ follows directly that

$$\text{sin am}(-v) = -\text{sin am}(v) \tag{1.3}$$

Therefore

$$\begin{aligned} \text{sin am}(\frac{\omega}{2} - u) &= -\text{sin am}(u - \frac{\omega}{2}) \\ &= -\left(-\frac{\cos \text{am}(u)}{\Delta \text{ am}(u)}\right) \\ &= \text{sin am}(u + \frac{\omega}{2}) \end{aligned} \tag{1.4}$$

and in the same way

$$\text{sin am}(\frac{\omega}{2}i - u) = \text{sin am}(\frac{\omega}{2}i + u) \tag{1.5}$$

If now we substitute u with $u + \frac{\omega}{2}$ in Eq.(1.4) and with $u + \frac{\omega}{2}i$ in Eq.(1.5), we get

$$\text{sin am}(u + \omega) = -\text{sin am}(u) \tag{1.6}$$

$$\text{sin am}(u + \omega i) = -\text{sin am}(u) \tag{1.7}$$

and then if we substitute again u with $u + i\omega$ or and with $u - \omega i$ in Eq.(1.6) we finally obtain that for every $u \in \mathbb{C}$

$$\text{sin am}(u + (1+i)\omega) = \text{sin am}(u) \tag{1.8}$$

$$\text{sin am}(u + (1-i)\omega) = \text{sin am}(u) \tag{1.9}$$

Clearly, we can sum up the previous discussion in the following statement:

Proposition 1.2.1. *For every $u \in \mathbb{C}$ and for every $n, m \in \mathbb{Z}$*

$$sin\ am(m\omega + n\omega i \pm u) = \pm(-1)^{m+n} sin\ am(u)$$

which immediately implies

Corollary 1.2.1. *For every $n, m \in \mathbb{Z}$*

$$sin\ am(m\omega + n\omega i) = 0$$

Actually, also the converse of this Corollary holds. In fact

Proposition 1.2.2. *Let $u \in \mathbb{C}$. Then $sin\ am(u) = 0$ if and only if there are $m, n \in \mathbb{Z}$ such that $u = m\omega + n\omega i$.*

Proof. Suppose that $\text{sin am}(u) = 0$, and consider the elements $a, b \in \mathbb{R}$ such that $u = a + ib$.
Using Eq.(1.2) it follows that

$$\frac{\text{sin am}(a)\text{cos am}(bi)\Delta\ \text{am}(bi) + \text{sin am}(bi)\text{cos am}(a)\Delta\ \text{am}(a)}{1 + \text{sin am}^2(a)\text{sin am}^2(bi)} = 0$$

Note that

$$\text{sin am}(a)\text{cos am}(bi)\Delta\ \text{am}(bi) \in \mathbb{R}$$

while

$$\text{sin am}(bi)\text{cos am}(a)\Delta\ \text{am}(a) = iA \text{ with } A \in \mathbb{R}$$

because

- $a \in \mathbb{R}$, so $\text{sin am}(a), \text{cos am}(a), \Delta\ \text{am}(a) \in \mathbb{R}$
- $b \in \mathbb{R}$ so $\text{sin am}(b) \in \mathbb{R}$, which means that

$$\begin{aligned} \text{cos am}(ib)\Delta\ \text{am}(ib) &= \sqrt{1 - (sin(ib))^4} \\ &= \sqrt{1 - (sin(b))^4} \\ &= \text{cos am}(b)\Delta\ \text{am}(b) \in \mathbb{R} \end{aligned}$$

Therefore, it must be that

$$\text{sin am}(a)\text{cos am}(bi)\Delta\ \text{am}(bi) = 0 = i\text{sin am}(b)\text{cos am}(a)\Delta\ \text{am}(a)$$

Since $\Delta\ \text{am}(a) \neq 0$ for every $a \in \mathbb{R}$ and since

$$\text{cos am}(ib) = \sqrt{1 + sin(b)^2} = \Delta\ \text{am}(b)$$

the previous equations become

$$\text{sin am}(a)\Delta\ \text{am}(bi) = 0 = \text{sin am}(b)\text{cos am}(a)$$

If $\text{sin am}(a) = 0$, then $\text{cos am}(a) = 1$ and so $\text{sin am}(b) = 0$. If $\text{sin am}(a) \neq 0$, we get

$$0 = \Delta\ \text{am}(bi) = \sqrt{1 + \text{sin am}(ib)^2} = \text{cos am}(b)$$

which means that $\text{cos am}(a) = 0$ because at this point $\text{sin am}(b) = \pm 1$.
We consider first the second case. Let $n \in \mathbb{Z}$ be such that $a = n\omega + a'$, where $0 \leq a' \leq \frac{\omega}{2}$. Then, using Proposition (1.2.1),

$$\text{sin am}(a) = (-1)^n \text{sin am}(a')$$

hence we get the equation

$$0 = \text{cos am}(a) = \sqrt{1 - \text{sin am}(a)^2} = \sqrt{1 - \text{sin am}(a')^2}$$

which implies that $\text{sin am}(a') = \pm 1$. But since $0 \leq a' \leq \frac{\omega}{2}$, $\text{sin am}(a')$ must be positive, so $\text{sin am}(a') = 1$ which means (since sin am is invertible in $[0, \frac{\omega}{2}]$) that $a' = \frac{\omega}{2}$ and $a = (n + \frac{1}{2})\omega$. In the same way,

$$0 = \Delta\ \text{am}(bi) = \text{cos am}(b)$$

implies that b can be written as $b = (m + \frac{1}{2})\omega$ for some $m \in \mathbb{Z}$. Those values actually lead to a contradiction. In fact, if we consider the general equations

$$\begin{aligned} \text{sin am}(v \pm \frac{\omega}{2}) &= \pm \frac{\text{cos am}(v)}{\Delta\ \text{am}(v)} \\ \text{sin am}(v \pm \frac{\omega}{2} i) &= \pm \frac{\Delta\ \text{am}(v)}{\text{cos am}(v)} i \end{aligned}$$

we obtain

$$\text{sin am}(v + \frac{\omega}{2}) \text{sin am}(v + \frac{\omega}{2} i) = i \tag{1.10}$$

If now we consider $u = a + ib = (n + \frac{1}{2})\omega + (m + \frac{1}{2})\omega i$ it holds that (again by Proposition (1.2.1))

$$\text{sin am}(u) = (-1)^{m+n} \text{sin am}(\frac{\omega}{2} + \frac{\omega}{2} i)$$

Finally, recalling that $\text{sin am}(\omega) = 0$, the substitution $v = \frac{\omega}{2}$ in Eq.(1.10) shows that $\frac{\omega}{2} + \frac{\omega}{2} i$ is a pole of sin am, not a zero.
Thus the only possible case is the first. Using the same argument as before, we can see that the request $\text{sin am}(a) = 0 = \text{sin am}(b)$ implies that $a = n\omega$ and $b = m\omega$ for some $n, m \in \mathbb{Z}$, and hence we are done. □

Remark 1.2.1. All the zeros of $\text{sin am}(u)$ are simple, because whenever $\text{sin am}(u) = 0$ for some $u \in \mathbb{C}$

$$(\text{sin am}'(u))^2 = 1 - \text{sin am}^4(u) = 1$$

Corollary 1.2.2. *For any $n, m \in \mathbb{Z}$*

$$u = \left(m + \frac{1}{2}\right)\omega + \left(n + \frac{1}{2}\right)\omega i$$

is a pole of sin am.

Also in this case we can prove that actually

Proposition 1.2.3. *Let $u \in \mathbb{C}$. Then u is a pole of sin am if and only if there are $m, n \in \mathbb{Z}$ such that .*

$$u = \left(m + \frac{1}{2}\right)\omega + \left(n + \frac{1}{2}\right)\omega i$$

Proof. Considering again the equations

$$\begin{aligned} \text{sin am}(v \pm \pm\frac{\omega}{2}) &= \pm\frac{\text{cos am}(v)}{\Delta \text{ am}(v)} \\ \text{sin am}(v \pm \pm\frac{\omega}{2}i) &= \pm\frac{\Delta \text{ am}(v)}{\text{cos am}(v)}i \end{aligned}$$

and setting $v = u - \frac{\omega}{2}$, we see that

$$\text{sin am}(u) \cdot \text{sin am}\left(u - \frac{\omega}{2} - \frac{\omega}{2}i\right) = -i \tag{1.11}$$

Hence if u is a pole, $u - \frac{\omega}{2} - \frac{\omega}{2}i$ must be a zero of sin am. But from the previous Proposition this implies that $u - \frac{\omega}{2} - \frac{\omega}{2}i = (m + in)\omega$ for some $n, m \in \mathbb{Z}$, and thus

$$u = \left(m + \frac{1}{2}\right)\omega + \left(n + \frac{1}{2}\right)\omega i$$

as we wanted to show. □

Remark 1.2.2. Since all the zeros of sin am(u) are simple, considering Eq.(1.11) we can see that all the poles are simple.

After treating zeros and poles, we are interested in solving more general equations.

Proposition 1.2.4. *Given $\alpha \in \mathbb{C}$, the equation*

$$sin\ am(x) = sin\ am(\alpha)$$

is satisfied by x if and only if

$$x = (-1)^{m+n}\alpha + m\omega + n\omega i$$

for some $m, n \in \mathbb{Z}$.

A rigorous proof of this statement can be found in [4], Theorem 15.3.3, but here, we are only going to illustrate the train of thought of Abel (who was the first to state and use this result), that can be found also in [1]. First of all, Abel considered the equation

$$\text{sin am}(x) - \text{sin am}(\alpha) = 0$$

Using Eq.(1.2) twice, it follows directly that for (suitable) $u, v \in \mathbb{C}$

$$\text{sin am}(u+v) - \text{sin am}(u-v) = \frac{2\left(\text{sin am}(v)\text{cos am}(u)\Delta\ \text{am}(u)\right)}{1 + \text{sin am}^2(u)\text{sin am}^2(v)}$$

So if we set $u = \frac{x+\alpha}{2}, v = \frac{x-\alpha}{2}$ what we get is

$$0 = \text{sin am}(x) - \text{sin am}(\alpha) = \frac{2\left(\text{sin am}(\frac{x-\alpha}{2})\text{cos am}(\frac{x+\alpha}{2})\Delta\ \text{am}(\frac{x+\alpha}{2})\right)}{1 + \text{sin am}^2(\frac{x+\alpha}{2})\text{sin am}^2(\frac{x-\alpha}{2})}$$

In its paper, Abel continues without asking himself whether or not the right hand side is defined, instead he remarks that this last equation can be "satisfied" in five different ways:

- if $\text{sin am}(\frac{x-\alpha}{2}) = 0$, i.e if $\frac{x-\alpha}{2} = (n+mi)\omega$ for some $n, m \in \mathbb{Z}$.
- if $\text{cos am}(\frac{x+\alpha}{2}) = 0$, i.e if $\frac{x+\alpha}{2} = (n+mi)\omega + \frac{\omega}{2}$ for some $n, m \in \mathbb{Z}$.
- if $\Delta\ \text{am}(\frac{x+\alpha}{2}) = 0$, i.e if $\frac{x+\alpha}{2} = (n+mi)\omega + \frac{\omega}{2}i$ for some $n, m \in \mathbb{Z}$.
- if $\frac{x-\alpha}{2}$ is a pole of sin am, i.e $\frac{x-\alpha}{2} = \left(m+\frac{1}{2}\right)\omega + \left(n+\frac{1}{2}\right)\omega i$ for some $n, m \in \mathbb{Z}$.
- if $\frac{x+\alpha}{2}$ is a pole of sin am, i.e $\frac{x+\alpha}{2} = \left(m+\frac{1}{2}\right)\omega + \left(n+\frac{1}{2}\right)\omega i$ for some $n, m \in \mathbb{Z}$.

So, according to the previous computations, the different possibilities are

- $x = \alpha + 2n\omega + 2m\omega i$ for some $n, m \in \mathbb{Z}$.
- $x = -\alpha + (2n+1)\omega + 2m\omega i$ for some $n, m \in \mathbb{Z}$.
- $x = -\alpha + 2n\omega + (2m+1)\omega i$ for some $n, m \in \mathbb{Z}$.
- $x = \alpha + (2m+1)\omega + (2n+1)\omega i$ for some $n, m \in \mathbb{Z}$.
- $x = -\alpha + (2m+1)\omega + (2n+1)\omega i$ for some $n, m \in \mathbb{Z}$.

Finally Abel checks, using Proposition (1.2.1), whether sin am(x) is really equal to sin am(α) or not: all the cases give sin am$(x) =$ sin am(α), except the fifth, which gives sin am$(x) = -$sin am(α). Thus all the solutions of the equation are given by the four remaining cases, and they can be summarized by saying that we must have

$$x = (-1)^{m+n}\alpha + m\omega + n\omega i$$

for some $m, n \in \mathbb{Z}$.

1.3 Jacobi elliptic function

For reasons that will become clear in the next chapter, we would like to link the function defined in the previous section to the Weierstrass $\wp$-function associated to the lattice $\Lambda = \omega\mathbb{Z}+i\omega\mathbb{Z}$. Note that this is not the most natural choice for Λ: in fact, since $\sin \mathrm{am}(u)$ is a doubly periodic meromorphic function with linearly independent periods (and hence an elliptic function), the natural idea would be to take the lattice $L = (1+i)\omega\mathbb{Z} + (1-i)\omega\mathbb{Z}$ and to find the Weierstrass equation of the elliptic curve $E = \mathbb{C}/L$, in order to finally link $\sin \mathrm{am}(u)$ with $\wp_L(z) = \wp(z, L)$, the Weierstrass $\wp$-function of L. As can be seen in [5], Section 2, in this case the Weierstrass equation of E is $Y^2 = 4X^3 + X$. Moreover

$$\sin \mathrm{am}(u) = -2\frac{\wp_L(z)}{\wp'_L(z)}$$

and

$$\sin \mathrm{am}'(u) = \frac{4\wp_L^2(z) - 1}{4\wp_L^2(z) + 1}$$

The relations are surely interesting, but following Takagi approach as we are going to do, the relation is actually even more interesting, since we will prove that for every $u \in \mathbb{C}$

$$\wp_\Lambda(u) = \frac{1}{\sin \mathrm{am}^2(u)}$$

Unluckily, the proof of this relation is not short, and we will first need to introduce a whole new set of functions, the Jacobi elliptic functions.

Definition 1.3.1. For any $k \in \mathbb{C}$, consider the integral

$$u = \int_0^\phi \frac{dt}{\sqrt{1 - k^2 sin^2(t)}}$$

where t is a complex variable. Define a new family of functions (the Jacobi elliptic functions) by setting

$$\mathrm{sn}(u, k) = \sin(\phi)$$

Considering

$$K = \int_0^{\frac{\pi}{2}} \frac{dt}{\sqrt{1 - k^2 sin^2(t)}}$$

it is easy to see that

$$\mathrm{sn}(u + 4K, k) = \mathrm{sn}(u, k)$$

In addition, Jacobi introduces the functions

$$\begin{aligned} \mathrm{cn}(u,k) &= \sqrt{1-\mathrm{sn}^2(u,k)} \\ \mathrm{dn}(u,k) &= \sqrt{1-k^2\mathrm{sn}^2(u,k)} \end{aligned}$$

Note that the substitution $\sin(\phi) = i\,\tan(\psi)$ yields

$$\frac{d\phi}{\sqrt{1-k^2\sin^2\phi}} = \frac{i\cdot d\psi}{\sqrt{1-k'^2\sin^2\psi}}$$

where $k^2+k'^2 = 1$, hence we get the extension of the Jacobi elliptic functions to the whole complex plane

$$\mathrm{sn}(iu,k) = i\cdot\frac{\mathrm{sn}(u,k')}{\mathrm{cn}(u,k')}$$

The functions $\mathrm{sn},\mathrm{cn},\mathrm{dn}$ have two periods, which are $(4K, 2iK')$, $(4K, 2(K+iK'))$ and $(2K, 4iK')$ respectively, where

$$K' = \int_0^{\frac{\pi}{2}} \frac{dt}{\sqrt{1-k'^2 sin^2(t)}}$$

(compare with [19], Section 2.2). Furthermore, for a fixed k, and thus writing $\mathrm{sn}(u,k)$=$\mathrm{sn}(u)$ for convenience, it is possible to prove (as in [20], Chapter XXII, paragraph 22.2, p.494) that the following relations hold :

$$\mathrm{sn}(u+v) = \frac{\mathrm{sn}(u)\mathrm{cn}(v)\mathrm{dn}(v)+\mathrm{sn}(v)\mathrm{cn}(u)\mathrm{dn}(u)}{1-k^2\mathrm{sn}^2(u)\mathrm{sn}^2(v)} \tag{1.12}$$

$$\mathrm{cn}(u+v) = \frac{\mathrm{cn}(u)\mathrm{cn}(v)-\mathrm{sn}(u)\mathrm{sn}(v)\mathrm{dn}(u)\mathrm{dn}(v)}{1-k^2\mathrm{sn}^2(u)\mathrm{sn}^2(v)} \tag{1.13}$$

$$\mathrm{dn}(u+v) = \frac{\mathrm{dn}(u)\mathrm{dn}(v)-k^2\mathrm{sn}(u)\mathrm{sn}(v)\mathrm{dn}(u)\mathrm{dn}(v)}{1-k^2\mathrm{sn}^2(u)\mathrm{sn}^2(v)} \tag{1.14}$$

There is an evident similarity between these functions and our function $\sin\mathrm{am}(u)$. Actually, $\sin\mathrm{am}(u)$ is related to them by the following result:

Remark 1.3.1. For $u \in \mathbb{C}$

$$\sin\mathrm{am}(u) = \frac{\mathrm{sn}(u\sqrt{2},\frac{1}{\sqrt{2}})}{\sqrt{2}\mathrm{dn}(u\sqrt{2},\frac{1}{\sqrt{2}})}$$

Proof. If we write $\mathrm{sd}(u,k) := \mathrm{sn}(u,k)/\mathrm{dn}(u,k)$, it is possible to prove that

$$u = \int_0^{\mathrm{sd}(u,k)} \frac{dt}{\sqrt{(1-k'^2t^2)(1+k^2t^2)}}$$

where as $k^2 + k'^2 = 1$ (compare with [20], p.429). Hence, we can consider the equation

$$u\sqrt{2} = \int_0^{\mathrm{sd}(u\sqrt{2}, \frac{1}{\sqrt{2}})} \frac{dt}{\sqrt{(1-\frac{1}{2}t^2)(1+\frac{1}{2}t^2)}} = \int_0^{\mathrm{sd}(u\sqrt{2}, \frac{1}{\sqrt{2}})} \frac{dt}{\sqrt{1-\frac{1}{4}t^4}}$$

and using the trivial substitution $\frac{1}{\sqrt{2}}t \mapsto z$ we get that

$$u = \int_0^{\frac{1}{\sqrt{2}}\mathrm{sd}(u\sqrt{2}, \frac{1}{\sqrt{2}})} \frac{dz}{\sqrt{1-z^4}}$$

which means that

$$\sin \mathrm{am}(u) = \frac{1}{\sqrt{2}}\mathrm{sd}(u\sqrt{2}, \frac{1}{\sqrt{2}}) = \frac{\mathrm{sn}(u\sqrt{2}, \frac{1}{\sqrt{2}})}{\sqrt{2}\mathrm{dn}(u\sqrt{2}, \frac{1}{\sqrt{2}})}$$

□

1.3.1 An equivalent definition

The form in which we presented the Jacobi elliptic functions is the good one in order to prove the formulas we have given previously, but unfortunately it is not so suitable if we want to establish a connection between the functions and the $\wp$-function. In order to fix this problem, let us introduce a new family of functions.

Definition 1.3.2. For complex variables u and z and a complex constant k, define

$$F(k, v) = \int_0^v \frac{dz}{\sqrt{(1-z^2)(1-k^2z^2)}}$$

Then, denote by $\alpha(k, v)$ the function such that

$$F(k, \alpha(k, v)) = v$$

Remark 1.3.2. For any k, and any u, we have

$$\mathrm{sn}(u, k) = \alpha(k, u)$$

Proof. For fixed k and u we have by definition

$$u = \int_0^{\phi} \frac{dt}{\sqrt{1-k^2 sin^2(t)}} \tag{1.15}$$

where

$$\mathrm{sn}(u, k) = \sin(\phi)$$

So, we have to prove that

$$u = \int_0^{\sin(\phi)} \frac{dz}{\sqrt{(1-z^2)(1-k^2z^2)}}$$

But this follows immediately if in Eq. (1.15) we make the change of variables $\sin(t) = z$. □

1.4 The link between $\wp_\Lambda(z)$ and sin am(z)

Let us start with a general $\wp$-function defined by the differential equation

$$\wp'^2(t) = 4\wp(t)^3 - g_2\wp(t) - g_3$$

for some suitable g_2 and g_3. Due to the differential equation, substituting $z = \wp(t)$ in the integral

$$\int \frac{dz}{\sqrt{4z^3 - g_2z - g_3}}$$

we get

$$\int \frac{dz}{\sqrt{4z^3 - g_2z - g_3}} = \int dt = t = \wp^{-1}(z) \tag{1.16}$$

Since z goes to infinity when t tends to 0, we may consider, for a fixed $\bar{z}$,

$$\wp^{-1}(\bar{z}) = \int_{\bar{z}}^{\infty} \frac{dz}{\sqrt{4z^3 - g_2z - g_3}}$$

and so

$$-\bar{t} = \wp^{-1}(\bar{z}) = \int_{\infty}^{\bar{z}} \frac{dz}{\sqrt{4z^3 - g_2z - g_3}} \tag{1.17}$$

Suppose that the $\wp$- function we are studing is associated to the lattice $\Lambda = 2\omega_1\mathbb{Z} \oplus 2\omega_2\mathbb{Z}$.
It is well know that in this situation the zeros of $\wp'$ are

$$e_1 = \wp(\omega_1)$$

$$e_2 = \wp(\omega_1 + \omega_2)$$

$$e_3 = \wp(\omega_2)$$

so that in Eq.(1.17) we actually have

$$-\bar{t} = \int_{\infty}^{\bar{z}} \frac{dz}{\sqrt{4(z-e_1)(z-e_2)(z-e_3)}}$$

Making use of the substitution

$$z = e_3 + \frac{e_1 - e_3}{u^2} \tag{1.18}$$

and setting

$$k^2 = \frac{e_2 - e_3}{e_1 - e_3}$$

we easily obtain that

$$\frac{dz}{\sqrt{4(z-e_1)(z-e_2)(z-e_3)}} = -\frac{1}{\sqrt{e_1 - e_3}} \frac{du}{\sqrt{(1-u^2)(1-k^2u^2)}}$$

Setting $e_1 - e_3 = \frac{1}{\epsilon}$, the previous discussion implies that

$$\begin{aligned} -\frac{\bar{t}}{\sqrt{\epsilon}} &= \frac{1}{\sqrt{\epsilon}} \int_\infty^{\bar{z}} \frac{dz}{\sqrt{4(z-e_1)(z-e_2)(z-e_3)}} \\ &= -\int_0^{\bar{u}} \frac{du}{\sqrt{(1-u^2)(1-k^2u^2)}} \end{aligned}$$

which means that

$$\bar{u} = \mathrm{sn}(\frac{\bar{t}}{\sqrt{\epsilon}}, k)$$

and so since $\bar{z} = \wp(\bar{t})$, using Eq.(1.18) we finally obtain (considering the generality of $\bar{t}$)

$$\wp(t) = e_3 + \frac{1}{\epsilon\ \mathrm{sn}^2(\frac{t}{\sqrt{\epsilon}}, k)} \tag{1.19}$$

Finally, we can prove the following crucial result:

Theorem 1.4.1. *Let $\wp(z)$ be the Weierstrass function associated to the lattice $\Lambda = \omega\mathbb{Z} \oplus i\omega\mathbb{Z}$ where*

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

Then

$$\wp(u) = \frac{1}{\sin\ \mathrm{am}^2(v)}$$

Proof. First of all, we need to compute the coefficients g_2 and g_3 of the differential equation of $\wp$. Since $i\Lambda = \Lambda$ and $i^6 = -1$, we see that

$$g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6} = 0$$

Due to a general result (proved by [10]) we have that $\sum(r+is)^{-4} = \omega^4/15$ where the sum is over all non zero Gaussian integers. Therefore,

$$\begin{aligned} g_2(\Lambda) &= 60 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4} \\ &= 60 \sum_{r,s \neq 0} \frac{1}{(r\omega + is\omega)^4} \\ &= \frac{60}{\omega^4} \sum_{r,s \neq 0} \frac{1}{(r+is)^4} \\ &= \frac{60}{\omega^4} \cdot \frac{\omega^4}{15} = 4 \end{aligned}$$

Hence $\wp(z)$ is parametrized by

$$\wp'^2(z) = 4\wp(z)^3 - 4\wp(z)$$

and this means that the zeros of $\wp'$ are exactly $0, 1, -1$. Since $i\Lambda = \Lambda$, we easily get that $\wp(iz) = -\wp(z)$, hence we get

$$\begin{aligned} e_1 &= \wp(\frac{\omega}{2}) = 1 \\ e_2 &= \wp(\frac{\omega + i\omega}{2}) = 0 \\ e_3 &= \wp(\frac{i\omega}{2}) = -1 \end{aligned}$$

As a consequence, $k = 1/\sqrt{2}$. Now, using Eq.(1.19) and the previous remarks, we have

$$\begin{aligned} \wp(u) &= -1 + \frac{2}{\mathrm{sn}^2(\sqrt{2}u, \frac{1}{\sqrt{2}})} \\ &= \frac{2 - \mathrm{sn}^2(\sqrt{2}u, \frac{1}{\sqrt{2}})}{\mathrm{sn}^2(\sqrt{2}u, \frac{1}{\sqrt{2}})} \\ &= \frac{2(1 - \frac{1}{2}\mathrm{sn}^2(\sqrt{2}u, \frac{1}{\sqrt{2}}))}{\mathrm{sn}^2(\sqrt{2}u, \frac{1}{\sqrt{2}})} \\ &= \frac{(\sqrt{2}(\sqrt{1 - \frac{1}{2}\mathrm{sn}^2(\sqrt{2}u, \frac{1}{\sqrt{2}})}))^2}{\mathrm{sn}^2(\sqrt{2}u, \frac{1}{\sqrt{2}})} \\ &= \left(\frac{\sqrt{2}\mathrm{dn}(\sqrt{2}, \frac{1}{\sqrt{2}})}{\mathrm{sn}(\sqrt{2}u, \frac{1}{\sqrt{2}})} \right)^2 \\ &= \frac{1}{\sin \mathrm{am}^2(v)} \end{aligned}$$

□

1.5 Division points of the lemniscate

Note : from now on, for typographic reasons, we are going to write $\varphi(u)$,$f(u)$, $F(u)$ instead of $\sin\operatorname{am}(u), \cos\operatorname{am}(u), \Delta\operatorname{am}(u)$, following Abel's notation.

1.5.1 The division in n parts

A natural question regarding the lemniscate is the one concerning the division points. Clearly if we divide the arc length of the lemniscate in n parts, by definition of $\varphi(u)$ the polar distances of the points that we obtain (the *n-division points*) are

$$\varphi\left(m\frac{2\omega}{n}\right), \qquad m = 0, 1, \ldots, n-1$$

so we would like to find an easy way to compute all of them: with the following results we will be actually able to prove that they are the roots of one specific polynomial, that we will call the *n-division polynomial*.

Using only the machinery developed so far, it is possible to prove that for every $u \in \mathbb{C}$,

$$\begin{aligned} \varphi(2u) &= \frac{2\varphi(u)f(u)F(u)}{1+\varphi^4(u)} \\ \varphi(3u) &= -\varphi(u)\frac{\varphi^8(u)+6\varphi^4(u)-3}{1+6\varphi^4(u)-3\varphi^8(u)} \end{aligned}$$

(see [4], Example 15.2.4) so we would like to find similar expression for $\varphi(nu)$ when we consider an arbitrary natural number $n \in \mathbb{N}$. Note that using the formula given by Corollary (1.1.1) we immediately obtain, for any $\alpha \in \mathbb{C}$, the equation

$$\varphi(\alpha+u)+\varphi(\alpha-u) = \frac{2\varphi(\alpha)f(u)F(u)}{1+\varphi^2(\alpha)\varphi^2(u)}$$

Now, if we suppose $\alpha = nu$ for some $n \in Z$, we get

$$\varphi((n+1)u) = -\varphi((n-1)u) + \frac{2\varphi(nu)f(u)F(u)}{1+\varphi^2(nu)\varphi^2(u)} \tag{1.20}$$

and so by recursion $\varphi((n+1)u)$ is a rational function of $\varphi(u)$,$f(u)$ and $F(u)$. More precisely:

Lemma 1.5.1. *Let $u \in \mathbb{C}$. For any m positive rational integer, we can find*

$T_1, \ldots, T_6$ *rational functions of* $(\varphi(u))^2$ *with integral coefficients such that*

$$\begin{aligned} \varphi(2mu) &= T_1\varphi(u)f(u)F(u) \\ f(2mu) &= T_2 \\ F(2mu) &= T_3 \\ \varphi((2m+1)u) &= T_4\varphi(u) \\ f((2m+1)u) &= T_5 f(u) \\ F((2m+1)u) &= T_6 F(u) \end{aligned}$$

This result follows from Eq.(1.20) via a direct (and not so interesting) computation. The reader can find the whole proof in [1], p. 115.

Lemma 1.5.2. *Given an integer* $n > 0$*, there are relatively prime polynomials* $\psi_n(u), \chi_n(u) \in \mathbb{Z}[u]$ *such that, setting* $x = \varphi(u)$*, if* n *is odd*

$$\varphi(nu) = \varphi(u)\frac{\psi_n(x^4)}{\chi_n(x^4)}$$

and if n *is even*

$$\varphi(nu) = \varphi(u)f(u)F(u)\frac{\psi_n(x^4)}{\chi_n(x^4)}$$

Proof. Using the description of the previous Lemma, if n is odd it is clear that

$$\varphi(nu) = \varphi(u)T$$

where T is a rational function of $(\varphi(u))^2$. So we only have to check that T is actually a function of $(\varphi(u))^4$ (we can always assume that $\psi_n(u), \chi_n(u)$ are coprime since $\mathbb{Z}[u]$ is an UFD). Let us set $\varphi(u) = x$. Then, if we set $T = \psi(x^2)$, we have

$$\varphi(nu) = x\psi(x^2)$$

Via the substitution $u \mapsto iu$ the last equation becomes

$$i\varphi(nu) = ix\psi(-x^2)$$

and hence

$$\psi(x^2) = \psi(-x^2)$$

so $\psi(x^2)$ must be the quotient of two polynomials composed only by powers of the form x^{4n}, as we wanted to show. The even case can be treated in the same way seen that $f(u)F(u) = f(iu)F(iu)$ for every $u \in \mathbb{C}$. □

The previous description allows us prove the following result.

Corollary 1.5.1. *Let* $n \in \mathbb{N}$ *odd. Then the polar distances of the* n*-division points of the lemniscate are roots of the polynomial* $x\psi_n(x^4)$*, that from now on we will call* n-division polynomial*.*

Proof. Since $\varphi(2\omega u)$ is equal to zero for every $u \in \mathbb{N}$, we have that if $t = \varphi(m\frac{2\omega}{n})$ is the polar distance of an n-division point,

$$0 = \varphi(m2\omega) = \varphi(n \cdot m\frac{2\omega}{n}) = t\frac{\psi_n(t^4)}{\chi_n(t^4)}$$

so t is a root of $x\psi_n(x^4)$ as we wanted to prove. □

Analogously, we can prove that for $n \in \mathbb{N}$ even the n-division points are roots of $x\psi_n(x^4)(1-x^2)$: using the same argument, they are surely roots of

$$x\psi_n(x^4)\sqrt{1-x^4} = x\psi_n(x^4)\sqrt{(1-x^2)(1+x^2)}$$

and so of

$$x\psi_n(x^4)(1-x^2)(1+x^2)$$

but $\varphi(u) \in \mathbb{R}$ if $u \in \mathbb{R}$, so they are necessarily roots of $x\psi_n(x^4)(1-x^2)$.

1.5.2 μ-division points

In the previous subsection, we were able to give a description of the formulas relating $\varphi(nu)$ with $\varphi(u)$ for every $n \in \mathbb{N}$. However, we know that $\varphi(u)$ is defined on all $\mathbb{C}$, so we would like to know whether similar formulas can be found for $\varphi(\mu u)$ where $\mu \in Z[i]$.
Actually, the answer is positive: using the equation $\varphi(iu) = i\varphi(u)$ and the addition formula (1.2) we can clearly obtain a formula relating $\sin((m+in)u)$ with $\varphi(u)$ if $m + in \in \mathbb{Z}[i]$, i.e. $\varphi(u)$ *has complex multiplication by* $\mathbb{Z}[i]$. Moreover, for every $\mu \in \mathbb{Z}[i]$ we can give a very precise description of the formulas involved in the multiplication by μ, but in order to do so, we first need to introduce some definitions.

Definition 1.5.1. An integer $\mu \in \mathbb{Q}(i)$ is said to be *odd* if it is coprime with $(1+i)$. At the contrary, μ is *even* if it is divisible by $(1+i)$.

It is easy to prove that if $\mu = a + ib$ with $a, b \in \mathbb{Z}$ then

$$\mu \text{ is even} \iff (a+b) \text{ is even}$$

Furthermore, if $\alpha, \beta \in \mathbb{Z}[i]$, then

$$\begin{aligned} \alpha\beta \text{ is odd} &\iff \alpha \text{ and } \beta \text{ are odd} \\ \alpha + \beta \text{ is even} &\iff \alpha \text{ and } \beta \text{ are both even or both odd} \end{aligned}$$

Now we can start investigating the formulas for complex multiplication; we will treat separately the three cases $\mu = i+1$, $\mu \neq i+1$ even, and μ odd.

Proposition 1.5.1. *If $\mu = 1 + i$, if $\wp(z)$ is the Weierstrass $\wp$-function described in Theorem (1.4.1) then we have the following equations*

$$\wp((1+i)u) = \frac{\wp^2(u) - 1}{2i\wp(u)}$$

$$\varphi((1+i)u) = \frac{(1+i)\varphi(u)}{f(u)F(u)}$$

Proof. In this case, the proof is straightforward: using the addition law stated in Eq.(1.2) we get

$$\begin{aligned}
\varphi((i+1)u) &= \frac{\varphi(iu)f(u)F(u) + \varphi(u)f(iu)F(iu)}{1 + \varphi^2(iu)\varphi^2(u)} \\
&= \frac{(i+1)\varphi(u)f(u)F(u)}{1 - \varphi^4(u)} \\
&= \frac{(i+1)\varphi(u)f(u)F(u)}{f^2(u)F^2(u)} \\
&= \frac{(i+1)\varphi(u)}{f(u)F(u)}
\end{aligned}$$

and the other equation follows applying Theorem (1.4.1). □

In general we have that

Proposition 1.5.2. *Given an even element $\mu \in Z[i]$, there are two polynomials prime to each other $f_\mu(X), g_\mu(X) \in \mathbb{Z}[i][X]$ such that for every $u \in \mathbb{C}$*

$$\varphi(\mu u) = \varphi(u)f(u)F(u)\frac{f_\mu(x^4)}{g_\mu(x^4)}$$

where $x = \varphi(u)$

Proof. Since μ is even, if $a, b \in Z$ are such that $\mu = a + ib$, then $a + b$ is even, so they must be both odd or both even. In case a and b are both even, using the addition formula (1.2) and then Lemma (1.5.1) we get

$$\begin{aligned}
\varphi((a+ib)u) &= \frac{\varphi(au)f(bu)F(bu) + i\varphi(bu)f(au)F(au)}{1 - \varphi^2(au)\varphi^2(bu)} \\
&= \frac{T_1S_2S_3\varphi(u)f(u)F(u) + iS_1T_2T_3\varphi(u)f(u)F(u)}{1 - \varphi^4(u)f^4(u)F^4(u)T_1^2S_1^2} \\
&= \varphi(u)f(u)F(u)\frac{T_1S_2S_3 + iS_1T_2T_3}{1 - \varphi^4(u)f^4(u)F^4(u)T_1^2S_1^2}
\end{aligned}$$

where T_1, T_2, T_3 and S_1, S_2, S_3 are rational functions of $\varphi^4(u)$ (compare with the proof of Lemma (1.5.2)). The other case can be treated in the same way. □

Actually, the really interesting case is the odd one. In fact, we can prove the following result:

Proposition 1.5.3. *Let $\mu \in \mathbb{Z}[i]$ be odd, and let $\epsilon \in \{0,1,2,3\}$ such that $\mu \equiv i^\epsilon \bmod 2(i+1)$. Then there exist two relatively prime polynomials $\psi_\mu(x), \chi_\mu(x)$ with integral coefficients such that for all $u \in \mathbb{C}$*

$$\varphi(\mu u) = i^\epsilon x \frac{\psi_\mu(x^4)}{\chi_\mu(x^4)} \quad \text{where } x = \varphi(u)$$

$\psi_\mu(x)$ and $\chi_\mu(x)$ can be written as

$$\psi_\mu(y) = y^M + a_1 y^{M-1} + \ldots + a_{M-1} y + i^{-\epsilon}\mu$$
$$\chi_\mu(y) = \mu y^M + a_{M-1} y^{M-1} + \ldots + a_1 y + 1$$

where

$$M = \frac{1}{4}(m-1)$$

if m is the norm of μ. Moreover, if μ is a prime number, the coefficients $a_1, a_2, \ldots, a_M$ are all divisible by μ.

Note that the Proposition makes sense since

Remark 1.5.1. For every $\mu \in \mathbb{Z}[i]$ odd, there is an $\epsilon \in \{0,1,2,3\}$ such that

$$\mu \equiv i^\epsilon \bmod 2(i+1)$$

Proof. Being odd, μ is a unit of $\mathbb{Z}[i]/2(i+1)\mathbb{Z}[i]$, so we are only left to prove that there is an isomorphism

$$\left(\frac{\mathbb{Z}[i]}{2(i+1)\mathbb{Z}[i]}\right)^* \cong \{\pm i, \pm 1\}$$

Note that $a+ib$ is not coprime with $2(i+1)$ only if $i+1$ or $1-i$ divide $a+ib$. But

$$\frac{a+ib}{(i+1)} = \frac{a+b}{2} + \frac{b-a}{2}i$$

is an integer if and only if $a \equiv b \bmod 2$ and the same holds for

$$\frac{a+ib}{(1-i)} = \frac{a+b}{2} + \frac{a+b}{2}i$$

hence $a+ib$ is not a unit if and only if $a \equiv b \bmod 2$. Since

$$\left|\frac{\mathbb{Z}[i]}{2(i+1)\mathbb{Z}[i]}\right| = \mathbf{N}_{\mathbb{Q}[i]|\mathbb{Q}}(2(i+1)) = 8$$

and we have to avoid all the cases in which $a \equiv b \bmod 2$, it follows that

$$\left|\left(\frac{\mathbb{Z}[i]}{2(i+1)\mathbb{Z}[i]}\right)^*\right| = 8 - 4 = 4$$

and since $\pm i, \pm 1$ are clearly units, and they are different modulo $2(i+1)$, we get the desired isomorphism. □

The proof in this case is quite long, so we are going to treat the different steps separately.

Lemma 1.5.3. *Let $u \in \mathbb{C}$ and let $\mu \in \mathbb{Z}[i]$ be odd. Then*

$$\varphi(\mu u) = \varphi(u)T$$

where T is a rational function of $(\varphi(u))^4$.

Proof. Since μ is odd, if $\mu = s + it$ with $s, t \in \mathbb{Z}$ then it must be that s is odd and t is even or viceversa. In the first case, using Corollary (1.1.1) and then applying Lemma (1.5.1) to s and t we get

$$\begin{aligned}\varphi(\mu u) &= \varphi(su + itu) \\ &= \frac{\varphi(su)f(tu)F(tu) + i\varphi(tu)f(su)F(su)}{1 - (\varphi(su))^2(\varphi(tu))^2} \\ &= \frac{T_4T_2T_3\varphi(u) + iT_1T_5T_6\varphi(u)(f(u))^2(F(u))^2}{1 - T_4^2(\varphi(u))^2T_1^2(\varphi(u)f(u)F(u))^2}\end{aligned}$$

where as before $T_1, \ldots, T_6$ are rational functions of $(\varphi(u))^4$, i.e

$$\varphi(\mu u) = \varphi(u)T$$

where T is a rational function of $(\varphi(u))^4$. The other case can be treated in the same way. □

Lemma 1.5.4. *Let $\mu \in \mathbb{Z}[i]$ be odd, let m be its norm and let $u \in \mathbb{C}$. Consider $P_\mu(X), Q_\mu(X) \in Z[i][X]$ such that, if we set $\varphi(u) = x$,*

$$\varphi(\mu u) = x\frac{P_\mu(x)}{Q_\mu(x)}$$

and such that $P_\mu(X), Q_\mu(X)$ do not have any common factor. Then the degree of $P_\mu(X)$ with respect to X is equal to $m - 1$.

Proof. If $x = \varphi(u) \in \mathbb{C} \setminus \{0\}$ is such that $P_\mu(x) = 0$, then

$$\varphi(\mu u) = 0$$

and so, following Proposition (1.2.2) we have that there must be $s, t \in \mathbb{Z}$ such that

$$\mu u = (s + it)\omega$$

and so

$$x = \varphi\left(\frac{(s + it)}{\mu}\omega\right)$$

Moreover, again because of the Proposition, if we choose arbitrarily $s, t \in \mathbb{Z}$ we always have that $\varphi\left(\frac{(s+it)}{\mu}\omega\right)$ is a root. Actually, we can show that we

can always suppose $\rho = s + it$ to be odd and to be unique modulo $\mu\mathbb{Z}[i]$. First of all, if ρ is even, then $\mu - \rho$ is odd, and by Eq.(1.6) we have

$$\varphi\left((\mu-\rho)\frac{\omega}{\mu}\right) = \varphi\left(\omega - \rho\frac{\omega}{\mu}\right) = \varphi\left(\rho\frac{\omega}{\mu}\right)$$

Moreover, if we suppose that

$$\varphi\left(\rho\frac{\omega}{\mu}\right) = \varphi\left(\rho'\frac{\omega}{\mu}\right)$$

with $\rho, \rho' \in \mathbb{Z}[i]$ odd, by Proposition (1.2.4) we get that there are $c, d \in \mathbb{Z}$ such that

$$\frac{\rho\omega}{\mu} = (-1)^{c+d}\frac{\rho'\omega}{\mu} + (c+di)\omega$$

which implies that

$$\rho = (-1)^{c+d}\rho' + (c+di)\mu$$

Since ρ, ρ' are odd, $\rho - (-1)^{c+d}\rho'$ is even, and then $(c+di)$ must be even. This means that $c+d$ is even, hence $(-1)^{c+d} = 1$ and

$$\rho = \rho' + (c+di)\mu$$

so ρ is unique modulo $\mu\mathbb{Z}[i]$. At this point, it is clear that the roots different from 0 are in one-to-one correspondence with the cosets of $\mathbb{Z}[i]/\mu\mathbb{Z}[i]$ (given a representative $\alpha \in \mathbb{Z}[i]/\mu\mathbb{Z}[i]$, either α or $\alpha + \mu$ is odd), and so their number (regardless of the multiplicity) is equal to

$$\left|\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}\right| - 1 = m - 1$$

We still do not know whether 0 is a root of $P_\mu(x)$ or not. Since P_μ is composed only by powers of x of the form x^{4n}, if 0 is a root it must be a multiple root. Actually, we can prove that P_μ does not have multiple roots. In fact, differentiating the equation

$$\varphi(\mu u) = x\frac{P_\mu(x)}{Q_\mu(x)}$$

and noticing that we always have

$$\frac{\partial\ \varphi(\alpha)}{\partial u} = f(\alpha)F(\alpha)\frac{\partial\alpha}{\partial u}$$

we obtain

$$\mu f(\mu u)F(\mu u)Q_\mu(x) + \varphi(\mu u)\tfrac{\partial Q_\mu(x)}{\partial u} = \\ = xf(u)F(u)\frac{\partial P_\mu(x)}{\partial x} + P_\mu(x)f(u)F(u) \quad (1.21)$$

If we suppose that P_μ has a multiple root $\bar{x} = \varphi(\bar{u})$, it holds that

$$P_\mu(\bar{x}) = \frac{\partial P_\mu(x)}{\partial x}(\bar{x}) = 0$$

Then (since $\varphi(\mu\bar{u}) = 0$) the previous equation becomes

$$\mu f(\mu\bar{u})F(\mu\bar{u})\mathbb{Q}_\mu(\bar{x}) = 0$$

which means that $\mathbb{Q}_\mu(\bar{x}) = 0$, seen that $f(\mu\bar{u}) = 1 = F(\mu\bar{u})$; but this is a contradiction, because $P_\mu(x)$ and $Q_\mu(x)$ do not have any common factor. Therefore, P_μ does not have multiple roots: so 0 is not a root. Moreover, since we have seen that all the roots are simple, of the form $\varphi(\frac{\rho\omega}{\mu})$ with $\rho \in \mathbb{Z}$, $|\rho| \leq \frac{m-1}{2}$ and they are all different, the degree of P_μ is $m-1$ as we wanted to show. □

Proposition 1.5.4. *Using the previous notation, if $\mu \equiv i^\epsilon$ mod $2(i+i)$ then*

$$Q_\mu(x) = \frac{1}{i^\epsilon}x^{m-1}P_\mu(x)$$

Proof. Let $y = \varphi(\mu u)$. Considering $x = \varphi(u)$ as before, we clearly have

$$\int_0^y \frac{dy}{\sqrt{1-y^4}} = \mu u = \mu \int_0^x \frac{dx}{\sqrt{1-x^4}}$$

and hence

$$\frac{dy}{\sqrt{1-y^4}} = \mu\frac{dx}{\sqrt{1-x^4}} \tag{1.22}$$

Let us set $y = \frac{1}{\eta}$ and $x = \frac{1}{i^t\xi}$ where $\eta, \xi \in \mathbb{C}$ while $t \in \mathbb{Z}$ is still to be determined. Using the previous equation we get by direct computation that

$$\frac{d\eta}{\sqrt{\eta^4-1}} = \frac{\mu i^t d\xi}{\sqrt{\xi^4-1}}$$

and then we can choose a suitable t in order to have

$$\frac{d\eta}{\sqrt{1-\eta^4}} = \mu\frac{d\xi}{\sqrt{1-\xi^4}}$$

and we know that this equation implies that

$$\eta = \xi\frac{P_\mu(\xi)}{Q_\mu(\xi)} \tag{1.23}$$

On the other hand, since we started with $y = \frac{1}{\eta}$ and $x = \frac{1}{i^t\xi}$ we also have

$$\frac{1}{\eta} = y = x\frac{P_\mu(x)}{Q_\mu(x)} = \frac{1}{i^t\xi}\cdot\frac{P_\mu(\frac{1}{i^t\xi})}{Q_\mu(\frac{1}{i^t\xi})} = \frac{P_\mu(\frac{1}{\xi})}{i^t\xi Q_\mu(\frac{1}{\xi})}$$

and therefore

$$\eta = \frac{i^t \xi Q_\mu(\frac{1}{\xi})}{P_\mu(\frac{1}{\xi})}$$

which means that we can express η using the rational function

$$\eta = i^t \xi \frac{\xi^{m-1} Q_\mu(\frac{1}{\xi})}{\xi^{m-1} P_\mu(\frac{1}{\xi})} \tag{1.24}$$

(recall that the degree of $P_\mu(x)$ is $m-1$).
At this point, we can equate Eq.(1.23) with Eq.(1.24) and since P_μ and Q_μ are coprime, up to a complex unit i^ν we obtain (having in mind the arbitrariness of η and ξ)

$$Q_\mu(x) = i^\nu x^{m-1} P_\mu(\frac{1}{x})$$

Now we only have to prove that $i^\nu = i^{-\epsilon}$ where $\mu \equiv i^\epsilon \bmod 2(i+1)$. This can be done giving a precise value to x. If for example we consider $\bar{u} = \frac{\omega}{2}$, since by definition

$$\bar{x} = \varphi(\bar{u}) = \varphi(\frac{\omega}{2}) = 1$$

it holds that

$$\varphi(\mu\frac{\omega}{2}) = \bar{x}\frac{P_\mu(\bar{x})}{Q_\mu(\bar{x})} = 1 \cdot \frac{P_\mu(1)}{i^\nu 1^{m-1} P_\mu(\frac{1}{1})} = \frac{1}{i^\nu}$$

Since $\mu \equiv i^\epsilon \bmod 2(i+1)$ we can find $a, b \in \mathbb{Z}$ such that

$$\mu = (2a - 2b) + (2a + 2b)i + i^\epsilon$$

and thus

$$\varphi(\mu\frac{\omega}{2}) = \varphi((a-b)\omega + (a+b)i\omega + i^\epsilon\frac{\omega}{2})$$

But by Proposition (1.2.1)

$$\varphi((a-b)\omega + (a+b)i\omega + i^\epsilon\frac{\omega}{2}) = (-1)^{(a-b)+(a+b)}\varphi(i^\epsilon\frac{\omega}{2})$$

hence

$$i^\nu = \frac{1}{\varphi(\mu\frac{\omega}{2})} = \frac{1}{i^\epsilon\varphi(\frac{\omega}{2})} = \frac{1}{i^\epsilon}$$

as we wanted to show. □

Note: From now on, for sake of convenience we are going to denote by $Q_\mu(X)$ the polynomial $X^{m-1}P_\mu(\frac{1}{X})$, so that we have the formula

$$\varphi(\mu u) = i^\epsilon x \frac{P_\mu(x)}{Q_\mu(x)}$$

Finally, we need the following

Lemma 1.5.5. *Let $\mu \in \mathbb{Z}[i]$ be an odd prime such that $\mu \equiv i^{\epsilon}$ mod $2(i+1)$, and suppose that $P_\mu(x)$ is a monic polynomial (which is always possible). Then*

$$P_\mu(x) = x^{m-1} + a_{(m-5)/4}x^{m-5} + \ldots + a_1x^4 + i^{-\epsilon}\mu$$

where $a_1, \ldots, a_{(m-1)/4}$ are all divisible by μ.

The proof is quite long and it can be found in [4], Theorem 15.4.8, p. 492. Here we only remark that we already know that the polynomial $P_\mu(x)$ is of the form

$$P_\mu(x) = x^{m-1} + a_{(m-5)/4}x^{m-5} + \ldots + a_1x^4 + a_0$$

and that, since by the equation

$$y = i^{\epsilon}x\frac{P_\mu(x)}{Q_\mu(x)}$$

follows that $i^{\epsilon}a_0 = \frac{dy}{dx}|_{x=0}$, using Eq.(3.1) we can see directly that

$$a_0 = i^{-\epsilon}\mu.$$

Note that with all those lemmas the Proposition (1.5.3) is finally proven.

Chapter 2

Lemniscate extensions

We are now ready to start to investigate the properties of the fields which are constructed by adding to $\mathbb{Q}(i)$ the points obtained from the division of the lemniscate. We are not only interested in the discriminant of those fields, but also in finding an explicit information about the subfields they have. In order to do so, we are splitting the discussion in different cases, depending on the characteristics of the integer $\mu \in \mathbb{Q}(i)$.

2.1 The case of an odd prime number

For a general odd integer, it holds that

Theorem 2.1.1. *Let μ be an odd integer of $\mathbb{Q}(i)$, m its norm, and consider the field $C_\mu = \mathbb{Q}(i, \varphi(\frac{\omega}{\mu}))$. Then $\mathbb{Q}(i) \subset C_\mu$ is a Galois extension, and there is an injective homomorphism*

$$\mathrm{Gal}(\frac{C_\mu}{\mathbb{Q}(i)}) \hookrightarrow \left(\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}\right)^*$$

Proof. Consider the μ-division polynomial $xP_\mu(x) = 0$. From the proof of Lemma (1.5.4) we know that all the roots of this polynomial are given by

$$\varphi(\rho\frac{\omega}{\mu}) \quad \text{with } \rho \in \mathbb{Z}[i] \text{ odd}$$

and that ρ unique modulo $\mu\mathbb{Z}[i]$. Since we are considering only the case in which ρ is odd, $\varphi(\rho\frac{\omega}{\mu})$ is always a rational function in $\varphi(\frac{\omega}{\mu})$ with coefficients in $\mathbb{Q}(i)$, and thus $xP_\mu(x)$ splits completely in C_μ. Since $\varphi(\frac{\omega}{\mu})$ is one of the roots, it is clear that C_μ is the splitting field of $xP_\mu(x)$ over $\mathbb{Q}(i)$. Moreover, we know from the proof of Lemma (1.5.4) that $xP_\mu(x)$ does not have multiple roots, so $\mathbb{Q}(i) \subset C_\mu$ is a Galois extension.
Now if we consider an automorphism $\sigma \in Gal(C_\mu/\mathbb{Q}(i))$ we have that

$\sigma\left(\varphi(\frac{\omega}{\mu})\right)$ is still a root of $P_\mu(x)$, so there must be an odd $\rho \in Z[i]$ such that

$$\sigma(\varphi(\frac{\omega}{\mu})) = \varphi(\rho\frac{\omega}{\mu})$$

and from what we have seen before, ρ must be unique modulo $\mu\mathbb{Z}[i]$.
Now we claim that for every $\alpha \in \mathbb{Z}[i]$ odd,

$$\sigma(\varphi(\alpha\frac{\omega}{\mu})) = \varphi(\alpha\rho\frac{\omega}{\mu}) \tag{2.1}$$

In fact, since α is odd,

$$\varphi(\alpha\frac{\omega}{\mu}) = \varphi(\frac{\omega}{\mu})\frac{P_\alpha\left(\varphi(\frac{\omega}{\mu})\right)}{Q_\alpha\left(\varphi(\frac{\omega}{\mu})\right)}$$

and so

$$\begin{aligned}
\sigma(\varphi(\alpha\frac{\omega}{\mu})) &= \sigma(\varphi(\frac{\omega}{\mu}))\frac{\sigma(P_\alpha\left(\varphi(\frac{\omega}{\mu})\right))}{\sigma(Q_\alpha\left(\varphi(\frac{\omega}{\mu})\right))} \\
&= \varphi(\rho\frac{\omega}{\mu})\frac{P_\alpha(\sigma(\varphi(\frac{\omega}{\mu})))}{Q_\alpha(\sigma(\varphi(\frac{\omega}{\mu})))} \\
&= \varphi(\rho\frac{\omega}{\mu})\frac{P_\alpha(\varphi(\rho\frac{\omega}{\mu}))}{Q_\alpha(\varphi(\rho\frac{\omega}{\mu}))} \\
&= \varphi(\alpha\rho\frac{\omega}{\mu})
\end{aligned}$$

At this point, if we are able to prove that $[\rho] \in (\mathbb{Z}[i]/\mu\mathbb{Z}[i])^*$, it is clear how to define the morphism we need. Let s be the order of σ in $Gal(C_\mu/\mathbb{Q}(i))$, then using repeatedly Eq.(2.1) we obtain that

$$\varphi(\frac{\omega}{\mu}) = \sigma^s\left(\varphi(\frac{\omega}{\mu})\right) = \varphi(\rho^s\frac{\omega}{\mu})$$

and so by the uniqueness this means that

$$1 \equiv \rho^s \bmod \mu$$

Thus ρ is coprime with μ, and this means that $[\rho] \in (\mathbb{Z}[i]/\mu\mathbb{Z}[i])^*$. As a consequence, the map

$$\begin{aligned}
\mathrm{Gal}\left(\frac{C_\mu}{\mathbb{Q}(i)}\right) &\to \left(\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}\right)^* \\
\sigma &\mapsto \rho
\end{aligned}$$

is a well defined map, and it is an homomorphism because if $\sigma, \tau \in Gal(C_\mu/\mathbb{Q}(i))$ map to ρ, ρ' respectively, then

$$\begin{aligned}\sigma\tau(\varphi(\frac{\omega}{\mu})) &= \sigma(\rho'\varphi(\frac{\omega}{\mu})) \\ &= \varphi(\rho\rho'\frac{\omega}{\mu})\end{aligned}$$

where the last step holds thanks to Eq.(2.1), i.e $\sigma\tau \mapsto \rho\rho'$. Furthermore, the map is injective: if $[\rho] = [\rho'] \in (\mathbb{Z}[i]/\mu\mathbb{Z}[i])^*$, there must be $c, d \in \mathbb{Z}$ such that

$$\rho = \rho' + (c + id)\mu$$

Note that then $c + id$ is even in $\mathbb{Z}[i]$, and $c + d$ is an even rational integer. But then by Proposition (1.2.1)

$$\begin{aligned}\varphi(\rho\frac{\omega}{\mu}) &= \varphi((\rho' + (c + id)\mu)\frac{\omega}{\mu}) \\ &= \varphi(\rho'\frac{\omega}{\mu} + (c + id)\omega) \\ &= (-1)^{c+d}\varphi(\rho'\frac{\omega}{\mu}) \\ &= \varphi(\rho'\frac{\omega}{\mu})\end{aligned}$$

and so

$$\sigma(\varphi(\frac{\omega}{\mu})) = \tau(\varphi(\frac{\omega}{\mu}))$$

Seen that the automorphisms are determined by the image of $\frac{\omega}{\mu}$, this means that $\sigma = \tau$, as we wanted to show. □

If now we suppose in addition that $\mu \in Z[i]$ is prime, the polynomial $P_\mu(x)$ is separable over $\mathbb{Q}(i)$: in fact, we have already seen and used the fact that $P_\mu(x)$ does not have any multiple root, and furthermore by Proposition (1.5.3) the coefficients of $P_\mu(x)$ satisfy the requests of the Eisenstein criterion, which holds also for $\mathbb{Z}[i]$, since this is a PID. With this information, we can prove the following result, which is crucial for our discussion.

Proposition 2.1.1. *Let $\mu \in \mathbb{Z}[i]$ be an odd prime. Then*

$$\mathrm{Gal}(\frac{C_\mu}{\mathbb{Q}(i)}) \cong \left(\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}\right)^*$$

Proof. In order to show that the map defined in Theorem (2.1.1) is an isomorphism we only need to prove that

$$\left|Gal(\frac{C_\mu}{\mathbb{Q}(i)})\right| = \left|\left(\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}\right)^*\right| \tag{2.2}$$

Since C_μ is the splitting field of the separable polynomial $P_\mu(X)$ we have that

$$\left| Gal(\frac{C_\mu}{\mathbb{Q}(i)}) \right| = [C_\mu : \mathbb{Q}(i)] = deg P_\mu(X) = m - 1$$

On the other hand, since $\mathbb{Z}[i]$ is a PID, $\mu\mathbb{Z}[i]$ is a maximal ideal, and consequently $\mathbb{Z}[i]/\mu\mathbb{Z}[i]$ is a field. Thus,

$$\left| \left(\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]} \right)^* \right| = \left| \frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]} \right| - 1 = m - 1$$

and Eq.(2.2) holds. □

Moreover, recalling that every finite subgroup of the multiplicative group of a field is always cyclic, we obtain that

Corollary 2.1.1. *If μ is prime then $\mathbb{Q}(i) \subset C_\mu$ is a cyclic extension.*

Now we want to look a little closer. First of all, we are interested in the discriminant. We begin the discussion by considering the $\mathbb{Q}(i)$-basis $\mathcal{B}$ formed by the $m-1$ roots of $P_\mu(x)$.

Proposition 2.1.2. *The discriminant of $\mathcal{B}$ over $\mathbb{Q}(i)$ is*

$$D = 2^{\frac{(m-1)^2}{2}} \mu^{m-2}$$

Proof. We begin by considering two arbitrary elements $u, v \in \mathbb{C}$. Using repeatedly Corollary (1.1.1), it easily follows that

$$\begin{aligned}(\varphi(u) - \varphi(v))(\varphi(u) + \varphi(v))(\varphi(u+v) - \varphi(u-v)) = \\ = 2\varphi(v) f(u) F(u) \varphi(u+v) \varphi(u-v) \quad (2.3)\end{aligned}$$

In order to compute the discriminant, at this point we substitute $\varphi(u), \varphi(v)$ in the expression

$$(\varphi(u) - \varphi(v))(\varphi(u) + \varphi(v))(\varphi(u+v) - \varphi(u-v)) \quad (2.4)$$

with all the possible couples of roots

$$x_\rho = \varphi(\rho\frac{\omega}{\mu}),\ x_{\rho'} = \varphi(\rho'\frac{\omega}{\mu})$$

of $P_\mu(x) = 0$, leaving aside the values of ρ and ρ' such that $\rho = \rho'$ or $\varphi(\rho\frac{\omega}{\mu} + \rho'\frac{\omega}{\mu}) = \varphi(\rho\frac{\omega}{\mu} - \rho'\frac{\omega}{\mu})$.
Renaming the roots of $P_\mu(x)$ as $x_1 = \varphi(\rho_1\frac{\omega}{\mu}), \ldots, x_{m-1} = \varphi(\rho_{m-1}\frac{\omega}{\mu})$, if now

we multiply together all the expressions previously obtained via (2.4) what we get is the following expression involving the discriminant

$$\frac{D^3}{\left(\prod_{j=1}^{m-1} 2x_j\right)^3} = \left[2^{m-1}\left(\prod_{j=1}^{m-1} x_j\right)^3 \prod_{j=1}^{m-1} f\left(\rho_j \frac{\omega}{\mu}\right) \prod_{j=1}^{m-1} F\left(\rho_j \frac{\omega}{\mu}\right)\right]^{m-3} \tag{2.5}$$

We claim that

$$\prod_{j=1}^{m-1} f\left(\rho_j \frac{\omega}{\mu}\right) \prod_{j=1}^{m-1} F\left(\rho_i \frac{\omega}{\mu}\right) = (1+i)^{m-1} \tag{2.6}$$

In fact, for every j, using Proposition (1.5.1) we get that

$$\varphi\left((1+i)\frac{\rho_j \omega}{\mu}\right) = \frac{(i+1)\varphi\left(\rho_j \frac{\omega}{\mu}\right)}{f\left(\rho_j \frac{\omega}{\mu}\right) F\left(\rho_j \frac{\omega}{\mu}\right)}$$

which implies that

$$\prod_{j=1}^{m-1} \varphi\left((1+i)\frac{\rho_j \omega}{\mu}\right) = \frac{(i+1)^{m-1} \prod_{j=1}^{m-1} \varphi\left(\rho_j \frac{\omega}{\mu}\right)}{\prod_{j=1}^{m-1} f\left(\rho_j \frac{\omega}{\mu}\right) \prod_{j=1}^{m-1} F\left(\rho_j \frac{\omega}{\mu}\right)}$$

But seen that if $\varphi(x)$ is a root of $P_\mu(x)$ then also $\varphi((1+i)x)$ is a root

$$\prod_{j=1}^{m-1} \varphi\left((1+i)\frac{\rho_j \omega}{\mu}\right) = \prod_{j=1}^{m-1} \varphi\left(\frac{\rho_j \omega}{\mu}\right)$$

and thus Eq.(2.6) holds.
Finally,

$$\prod_{j=1}^{m-1} x_j = \mu$$

(since μ is the constant term of $P_\mu(x)$ and since $m-1 \equiv 0 \bmod 4$) and so Eq.(2.5) becomes

$$D = 2^{\frac{(m-1)^2}{2}} \mu^{m-2}$$

as we wanted to show. □

Our next goal is to prove the following result, which is fundamental for our discussion.

Theorem 2.1.2. *Let μ be an odd prime integer of $\mathbb{Q}(i)$. Denoting the norm of μ by m as usual, the discriminant of the extension $\mathbb{Q}(i) \subseteq C_\mu$ is equal to $2^{m-1}\mu^{m-2}$. Moreover, if*

$$m - 1 = 2^{h+2} p_1^{h_1} p_2^{h_2} \dots p_t^{h_t}$$

is the prime factorization of $m-1$ then C_μ contains for each prime divisor p_i one subfield which is cyclic over $\mathbb{Q}(i)$ and such that it is

of degree over $\mathbb{Q}(i)$	of discriminant over $\mathbb{Q}(i)$	
$p_1^{\lambda_1}$	$\mu^{p_1{}^{\lambda_1}-1}$	$(\lambda_1 = 1, 2, \dots, h_1)$
$p_2^{\lambda_2}$	$\mu^{p_2{}^{\lambda_2}-1}$	$(\lambda_2 = 1, 2, \dots, h_2)$
.....	.....	.....
2^{λ}	$\mu^{2^{\lambda}-1}$	$(\lambda = 1, 2, \dots, h)$
2^{h+1}	$(1+i)^{2^{h+1}}\mu^{2^{h+1}-1}$	
2^{h+2}	$(1+i)^{2^{h+3}}\mu^{2^{h+2}-1}$	

In the proof of Theorem (2.1.2) we are going to need different complementary results. Since the proof itself is quite long, for the sake of convenience we are going to discuss these results in the next Subsection, and then we are going to develop the proof in Subsection (2.1.2).

2.1.1 Some auxiliary results

First of all, just for future reference, we recall that

Lemma 2.1.1. *If E and L are Galois extensions of a field k with Galois group respectively G,H, then the composite field EL of E and F is a Galois extension of k. Moreover, the Galois group of the extension $k \subseteq EF$ is isomorphic to the subgroup U of $G \times H$ formed by the ordered pairs (σ, τ) such that σ and τ have the same restriction on $E \cap L$. The isomorphism sends each k-automorphism ρ of EL to the couple of its restrictions $(\rho\mid_E, \rho\mid_L)$.*

which obviously implies that

Corollary 2.1.2. *The composite field of two abelian extensions of $\mathbb{Q}(i)$ is still an abelian extension of $\mathbb{Q}(i)$.*

One of the key arguments of the proof of Theorem (2.1.2) is based on the following lemma:

Lemma 2.1.2. *Let $\mathbb{Q}(i) \subseteq K$ be a cyclic extension of $\mathbb{Q}(i)$ of odd degree. Then the discriminant of this extension is not divisible by $1 + i$.*

Instead of directly proving the Lemma, we are going to prove a more general result, but before we need another general Proposition (that we report here for sake of convenience).

Proposition 2.1.3. *Let $k \subseteq L$ be an abelian field extension of degree $m = p_1^{h_1} p_2^{h_2} \dots p_t^{h_t}$. Suppose moreover that there are some cyclic extensions of k $C_1, C_2, \dots, C_t$ of degree respectively $p_1^{h_1}, p_2^{h_2}, \dots, p_t^{h_t}$ such that $L = C_1 C_2 \dots C_t$, and let B be a cyclic extension of k of degree $n = p^l$, where $l \leq h_i$ for every i. If in addition L and B have a common subfield that has degree g over k, then the field K obtained by composing L and B may also be built by composing L with $\bar{L}$, another cyclic extension of k, such that $\bar{L} \cap L = k$ and*

$$[\bar{L} : k] = \frac{n}{g}$$

Proof. Due to the Primitive Element Theorem, we can find an element α generating L, and then we can consider the subgroup S of the Galois group of K formed by all k-automorphisms of K which fix α. Using the construction of Lemma (2.1.1), it is clear that S must be isomorphic to a subgroup of the Galois group of B over k: but the latter is by assumption cyclic thus also S is cyclic. In L, for each i we will denote by α_i the element generating C_i, and by $\alpha_i', \alpha_i'', \dots$ its conjugates under the action of the Galois group. For each i, let $\sigma_i \in Gal(K/k) \setminus L$ be the automorphism which sends α_i to α_i' and fixes all the other α_j's. Since the restriction of σ_i to C_i has order $p_i^{h_i}$ being in $Gal(C_i/k)$, and since the restriction of σ_i to the other C_j's is the identity, we get that σ_i has order $p_i^{h_i}$.

Now we focus on the subgroup T of $Gal(K/k)$ generated by all the σ_i's. Note that due to the definition of S and T, we have that $Gal(K/k) = ST$. Furthermore T is isomorphic to $Gal(L/k)$: in fact, we may consider the map (which is actually an isomorphism)

$$T =< \sigma_1 >< \sigma_2 > \dots < \sigma_t > \to Gal(A/k)$$

$$x_1 x_2 \dots x_t \mapsto x = x_1 \cdot x_2 \dots \cdot x_t$$

and prove the isomorphism considering the orders. Being a subgroup of $Gal(K/k)$ which is abelian, T is a normal subgroup and so it fixes a Galois subextension of K that we are going to denote by D. Note that since all elements in D are fixed by T and for every element in $L \setminus k$ there is at least a transformation that does not act trivially on it, the intersection $L \cap D$ is only k; thus $K = LD$. Finally, the Galois group of D over k is isomorphic to the quotient group $Gal(K/k)/T$ and so it is also isomorphic to S: but this group is cyclic, and so D is a cyclic extension. In order to conclude, note that being isomorphic to $Gal(L/k)$, T has order m. Since

$$[K : k] = \frac{[L : k][B : k]}{[L \cap B]} = \frac{mn}{g}$$

this means that D has degree

$$[D : k] = \frac{[K : k]}{m} = \frac{n}{g}$$

□

With this machinery at hand, we are ready for the general result we mentioned before.

Lemma 2.1.3. *Consider a cyclic extension $\mathbb{Q}(i) \subseteq C$ such that $[C : \mathbb{Q}(i)] = p^h$ for p prime, and for all $k \leq h$ denote by C_k the unique subextension of C such that $[C_k : \mathbb{Q}(i)] = p^k$. Let C_{h_0} be the maximal subfield of C which has the property of being contained in a cyclotomic field and the property of having the discriminant with respect to $\mathbb{Q}(i)$ divisible only by divisors of p. Suppose that the discriminant of the extension $\mathbb{Q}(i) \subseteq C$ is divided by a prime element $\mu \in \mathbb{Q}(i)$ which is coprime with p, and denote by m the norm of μ. Then if, for some k, μ divides the discriminant of the extension $\mathbb{Q}(i) \subseteq C_k$, we have that*

$$m \equiv 1 \ mod \ p^{h-h_0-k+1}$$

Proof. Let us consider the subfield $E_h \cap C$, where E_h is a cyclic extension of $\mathbb{Q}(i)$ of degree p^h such that the discriminant of $\mathbb{Q}(i) \subseteq E_h$ is only divisible by divisors of p and such that E_h is contained in a cyclotomic extension of $\mathbb{Q}$.

Remark 2.1.1. For every p prime and $h \in \mathbb{N}$, we can actually find a field E_h with the requested characteristics.

Proof. For p odd, consider a primitive p^{h+1}-th root of unity ζ and the cyclotomic extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$, that as we know is a cyclic extension of degree $p^h(p-1)$. If $p - 1 = \prod_j q_j^{l_j}$ is the prime decomposition of $p-1$ (where the q_j's are pairwise different primes) using the Sylow theorem for finite groups on the group $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ we can find for every j a cyclic subgroup $H_j \subseteq Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ of order $q_j^{l_j}$, and thus by composition a subgroup $H \subseteq Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ of order $p-1$ (which is normal since being a subgroup of a cyclic group). Then if we denote by K_H the subfield of $\mathbb{Q}(\zeta)$ fixed by H we have that $[K_H : Q] = p^h$ and that the extension is cyclic Galois extension, seen that

$$Gal\left(\frac{K_H}{\mathbb{Q}}\right) \cong \frac{Gal(\mathbb{Q}(\zeta)/\mathbb{Q})}{H}$$

Now consider the composite field $K_H \cdot \mathbb{Q}(i)$: it is evident that $K_H \cap \mathbb{Q}(i) = \mathbb{Q}$, thus $\mathbb{Q}(i) \subseteq K_H \cdot \mathbb{Q}(i)$ is a cyclic extension of degree p^h (which is contained in a cyclotomic extension since both K_H and $\mathbb{Q}(i)$ are). So, in order to conclude we only have to show that if μ is a prime which ramifies in $K_H \cdot \mathbb{Q}(i)$ then μ divides p. Since $K_H \cap \mathbb{Q}(i) = \mathbb{Q}$, it holds that (denoting by $\Delta(L|F)$ the discriminant of any extension $F \subseteq L$)

$$\Delta(K_H \cdot \mathbb{Q}(i)|\mathbb{Q}) = \Delta(K_H|\mathbb{Q})^2 \Delta(\mathbb{Q}(i)|\mathbb{Q})^{[K:\mathbb{Q}]}$$

(compare with [9], Theorem 87, p. 98) and so we get that

$$\mathbf{N}_{\mathbb{Q}(i)|\mathbb{Q}}\left(\Delta(K_H\cdot\mathbb{Q}(i)|\mathbb{Q}(i))\right)\Delta(\mathbb{Q}(i)|\mathbb{Q})^{[K:\mathbb{Q}]}=\Delta(K_H|\mathbb{Q})^2\Delta(\mathbb{Q}(i)|\mathbb{Q})^{[K:\mathbb{Q}]}$$

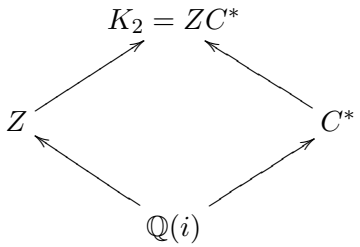
which means that if μ divides $\Delta(K_H\cdot\mathbb{Q}(i)|\mathbb{Q}(i))$ then $\mu\bar{\mu}$ must divide $\Delta(K_H|\mathbb{Q})$, which is a power of p since $K_H\subseteq\mathbb{Q}(\zeta)$ and p is the unique prime ramifying in $\mathbb{Q}(\zeta)$.
For $p=2$, we can basically repeat the argument, having in mind the fact that in this case the Galois group of $\mathbb{Q}(\zeta)$ is the direct product of two different cyclic groups. □

Note that due to the property of C_{h_0} of being the maximal subfield contained in a cyclotomic extension, we have that $E_h\cap C\subseteq C_{h_0}$. Moreover, $C_{h_0}\subseteq C$ by definition, but also $C_{h_0}\subseteq E_h$: in fact, both fields are contained in a cyclotomic extension and contain i, both have a power of p as degree over $\mathbb{Q}(i)$ and both have the discriminant over $\mathbb{Q}(i)$ divisible only by divisors of p, so that by the structure of the cyclotomic fields, we have the inclusion. Hence

$$E_h\cap C=C_{h_0}$$

and so by the composition of the two fields we obtain a field K of degree p^{2h-h_0} over $\mathbb{Q}(i)$, that (by Proposition (2.1.3)) can also be obtained by E_h and another cyclic extension C^* of $\mathbb{Q}(i)$ such that $[C^*:\mathbb{Q}(i)]=p^{h-h_0}$ and $C^*\cap E_h=\mathbb{Q}(i)$.

It is important for the following discussion to remark that μ must ramify in C^*: in fact, it ramifies in K, and it does not ramify in E_h.
Now we are interested in the field $Z=\mathbb{Q}(i,\zeta)$ where ζ is a primitive root of unity of degree p^{h-h_0}. Note that if p is odd $Gal(Z/\mathbb{Q}(i))$ may be generated by the automorphism s which sends ζ in another primitive root of unity of degree p^{h-h_0}, which may be written as ζ^g where g is a primitive root modulo p^{h-h_0} (i.e. a generator of the group of unities of $\mathbb{Z}/p^{h-h_0}\mathbb{Z}$). On the other hand, if $p=2$ then the group of units of $\mathbb{Z}/p^{h-h_0}\mathbb{Z}$ is generated by -1 and 5 and so considering $\eta=\zeta+\zeta^{-1}$ we get that $Z=\mathbb{Q}(i,\eta)$ and that $Gal(Z/\mathbb{Q}(i))$ is generated by the automorphism s which sends ζ in ζ^5 (compare with [3], p. 85, and [16], Proposition A.9, p. 281). Moreover, Z is by construction contained in a cyclotomic extension of $\mathbb{Q}$, so that the intersection $C^*\cap Z$ is actually contained in a cyclotomic extension. But we built C^* removing all the subfields satisfying this property: hence $C^*\cap Z$ must be the trivial intersection, i.e. $C^*\cap Z=\mathbb{Q}(i)$.
Let us denote K_2 the composite field ZC^*. From what we have said before, it follows that K_2 is an abelian extension of $\mathbb{Q}(i)$ (since C^* and Z are, and we can use Corollary (2.1.2)) and it is also a cyclic extension of Z, because we are in the situation



and so $Gal(K_2/Z) \cong Gal\,(C^*/\mathbb{Q}(i))$. Then, we are in the hypothesis of the following general lemmas

Lemma 2.1.4. *Let K be a field of characteristic coprime with n in which $x^n - 1$ splits, and let ζ be a primitive n-th root of unity. If a is a non zero element of K, there is a well defined normal extension $K(\sqrt[n]{a})$, the splitting field of $x^n - a$. If α is a root of $x^n = a$, there is an injective map*

$$\begin{aligned} Gal\left(\frac{K(\sqrt[n]{a})}{K}\right) &\to K^* \\ \sigma &\mapsto \frac{\sigma(\alpha)}{\alpha} \end{aligned}$$

In particular, if a is of order n in $K^*/(K^*)^n$, the Galois group is cyclic and can be generated by the element σ such that $\sigma(\alpha) = \zeta\alpha$.

Lemma 2.1.5. *If K be a field of characteristic coprime with n in which $x^n - 1$ splits and L is a cyclic extension of K of degree n then $L = K(\sqrt[n]{b})$ for some $b \in K$, and b must generate $K^*/(K^*)^n$.*

All the proofs are given in [3] in the third chapter, "Cyclotomic Fields and Kummer Extensions", written by B. J. Birch.
In our situation, this simply means that there is an element $\chi \in Z$ such that

$$K_2 = Z(\sqrt[\bar{n}]{\chi})$$

where $\bar{n} = p^{h-h_0}$.
Note that

Remark 2.1.2. With the notations of the previous lemmas, the discriminant of $K(\sqrt[n]{a})$ over K divides $n^n a^{n-1}$.

The proof might be found in [3], Chapter III, Lemma 5. This means that χ can't be coprime with μ: in fact, if it was, since the discriminant $\Delta(K_2|Z)$ of the extension $Z \subseteq K_2$ divides $(p^{h-h_0})^{p^{h-h_0}}\chi^{p^{h-h_0}-1}$, this would imply that μ is coprime with $\Delta(K_2|Z)$. But we know that

$$\Delta(K_2|\mathbb{Q}(i)) = \Delta(Z|\mathbb{Q}(i))^{\bar{n}}\mathbf{N}_{K_2|Z}(\Delta(K_2|Z))$$

and at the same time $\Delta(Z|\mathbb{Q}(i))$ is coprime with the prime μ since in the extension

$$\mathbb{Q}(i) \subseteq Z = \mathbb{Q}(i, \zeta)$$

μ is unramified, being coprime with p by hypothesis.
On the other hand,

$$N_{K_2|Z}(\Delta(K_2|Z)) = \prod q_i^{a_i f_i}$$

where

$$\Delta(K_2|Z) = \mathfrak{q}_1^{a_1} \dots \mathfrak{q}_t^{a_t}$$

is the decomposition in prime ideals of $\Delta(K_2|Z)$ in Z, $q_i = \mathfrak{q}_i \cap \mathbb{Z}(i)$ and f_{q_i} is the inertia degree of q_i in K_2. So if μ divides $N_{K_2|Z}(\Delta(K_2|Z))$, (μ) must be one of the q_i, and this means that μ divides $\Delta(K_2|Z)$, which is absurd. But then, μ does not divide $\Delta(K_2|\mathbb{Q}(i))$, and thus we also get that μ does not divide $\Delta(C^*|\mathbb{Q}(i))$, which is a contradiction since μ ramifies in C^*.

Let

$$\mu\mathcal{O}_Z = \mathfrak{M}_1\mathfrak{M}_2 \dots \mathfrak{M}_e$$

be the decomposition of μ in prime ideals in Z (recall that μ is not ramified there), and

$$\chi\mathcal{O}_Z = \mathfrak{M}\mathfrak{R}$$

where $\mathfrak{M}$ denotes the product of all the powers of $\mathfrak{M}_1, \mathfrak{M}_2, \dots$ that divide χ and $\mathfrak{R}$ is coprime with μ.

At this point recall that we defined s as the generator of $Gal(Z/\mathbb{Q}(i))$ such that $s(\zeta) = \zeta^g$ where for p odd g is a primitive root modulo p^{h-h_0}, and for p even g is equal to 5 . If h' is the natural number such that $p^{h'}$ is the highest power of p dividing $g^e - 1$ (the definition makes sense in the odd case since g is a primitive root modulo p^{h-h_0}, and in the even case because $5^e - 1$ is always even), consider the unique subgroup of index $p^{h'}$ of $Gal(C^*/\mathbb{Q}(i))$, and call the subfield fixed by this group $L_{h-h_0-h'}$. Now consider the composition $L_{h-h_0-h'}Z$. Since $L_{h-h_0-h'} \subset C^*$, $L_{h-h_0-h'} \cap Z = \mathbb{Q}(i)$, thus $Z \subset L_{h-h_0-h'}Z$ is a cyclic extension of degree $p^{h-h_0-h'}$. We claim that $L_{h-h_0-h'}Z = Z(\sqrt[n]{\nu})$ where $n = p^{h-h_0}$ and $\nu \in Z$ is coprime with μ.
In order to simplify the notation, from now on we will use the exponential notation, i.e. for every function f we will denote by x^f the element $f(x)$. For example, we will denote $\frac{s^e(\chi)}{\chi}$ by χ^{s^e-1}. If we consider the polynomial expressions (of variable s) $s^e - 1$ and $s - g$, they clearly are coprime modulo p^{h-h_0}, so we can actually find three polynomial expressions $f_1(s), f_2(s), f_3(s)$ such that

$$1 = (s^e - 1)f_1(s) + (s - g)f_2(s) + f_3(s)p^{h-h_0}$$

and consequently also

$$g^e - 1 = (s^e - 1)f_1(s)(g^e - 1) + (s - g)f_2(s)(g^e - 1) + f_3(s)p^{h-h_0}(g^e - 1) \quad (2.7)$$

At this point, we need to use the following general result:

Lemma 2.1.6. *Let $\mathbb{Q}(i) \subset E_h$ a cyclic extension of degree l^h (l prime) such that $\mathbb{Q}(i,\zeta) \cap E_h = \mathbb{Q}(i)$ where ζ is a primitive l^h-th root of unity. If χ is the element of $\mathbb{Q}(i,\zeta)$ such that $\mathbb{Q}(i,\zeta) \cap E_h = \mathbb{Q}(i,\zeta)(\sqrt[l^h]{\chi})$, and if r is a rational integer not divisible by l, considering the automorphism $\sigma \in Gal(\mathbb{Q}(i,\zeta)/\mathbb{Q}(i))$ which sends ζ into ζ^r we have that $\chi^{-r}\sigma(\chi)$ is the l^h-th power of an element of $\mathbb{Q}(i,\zeta)$.*

The proof of this lemma can be obtained imitating the argument used in [9], Lemma 15, §101, using $\mathbb{Q}(i)$ as base field instead of $\mathbb{Q}$. In our situation, the previous result means that χ^{s-g} is the p^{h-h_0}-th power of an element of Z, thus by Eq.(2.7) there must be an element $\alpha \in Z$ such that

$$\chi^{g^e-1} = \chi^{(s^e-1)f_1(s)(g^e-1)}\alpha^{p^{h-h_0}} \tag{2.8}$$

Since s acts transitively on the primes dividing μ, we have that (arranging the order)

$$s(\mathfrak{M}_1) = \mathfrak{M}_2,\ s^2(\mathfrak{M}_1) = \mathfrak{M}_3, \ldots, s^e(\mathfrak{M}_1) = \mathfrak{M}_{e-1}$$

while

$$s^e(\mathfrak{M}_1) = \mathfrak{M}_1$$

Of course, for every other j we also have

$$s^e(\mathfrak{M}_j) = \mathfrak{M}_j$$

This means that actually χ^{s^e-1} can be written as a fraction in which both numerator and denominator are integers coprime with μ, and consequently the same holds for $\chi^{(s^e-1)f_1(s)(g^e-1)}$, hence we can write

$$\chi^{(s^e-1)f_1(s)(g^e-1)} = \frac{\nu}{a^{p^{h-h_0}}}$$

where ν is an integer of Z coprime with μ and a is a rational integer. Consequently, using Eq. (2.8), we obtain that

$$\nu = \frac{a^{p^{h-h_0}}}{\alpha^{p^{h-h_0}}} \cdot \chi^{g^e-1}$$

and thus if $n = p^{h-h_0}$ and $g^e - 1 = rp^{h'}$

$$\begin{aligned} \sqrt[n]{\nu} &= \frac{a}{\alpha} \cdot \chi^{\frac{g^e-1}{p^{h-h_0}}} \\ &= \frac{a}{\alpha} \cdot (\chi^r)^{\frac{1}{p^{h-h_0-h'}}} \end{aligned}$$

Then, $L_{h-h_0-h'}Z$ and $Z(\sqrt[n]{\nu})$ must be equal, seen that they are both contained in C^*Z, they have the same degree over $\mathbb{Q}(i)$ and the extension $\mathbb{Q}(i) \subset C^*Z$ is cyclic. But this means that (μ) is not ramified in $L_{h-h_0-h'}$:

in fact, ν being coprime with μ, the discriminant of $Z \subset L_{h-h_0-h'}Z$ is not divisible by μ, so μ is not ramified in $L_{h-h_0-h'}Z$ which contains $L_{h-h_0-h'}$.

On the other hand, if m is the norm of μ, and $\gamma \in \mathbb{N}$ is such that p^γ is the highest power of p dividing $m-1$, we have

$$m^{p^{h-h_0-\gamma}} \equiv 1 \bmod p^{h-h_0}$$

In fact, since $p^\gamma | m-1$, there is an $l \in \mathbb{N}$ such that $m-1 = lp^\gamma$ and so

$$\begin{aligned} m^{p^{h-h_0-\gamma}} &= (lp^\gamma + 1)^{p^{h-h_0-\gamma}} \\ &= \sum_{i=0}^{p^{h-h_0-\gamma}} \binom{p^{h-h_0-\gamma}}{i} (lp^\gamma)^i \end{aligned}$$

But

$$\begin{aligned} \binom{p^{h-h_0-\gamma}}{i} p^{\gamma i} &= \frac{p^{h-h_0-\gamma}!}{i!(p^{h-h_0-\gamma}-i)!} p^{\gamma i} \\ &= \frac{p^{h-h_0-\gamma}(p^{h-h_0-\gamma}-1)! p^{\gamma i}}{i!(p^{h-h_0-\gamma}-i)!} \end{aligned}$$

and this is divisible for p^{h-h_0} for every i, except for $i=0$, where we get 1: thus the congruence is true. Also, $h-h_0-\gamma$ is the smallest exponent for which this congruence holds.

Remark 2.1.3. For p odd, μ decomposes in $e = p^{\gamma-1}(p-1)$ different primes in Z. If $p=2$, then $e = p^{\gamma-2}$.

In fact, since $\mathbb{Q}(i) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$, we have that $Gal(Z/\mathbb{Q}(i)) \cong Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, so the inertia degree of μ in Z is equal to the inertia degree of its norm m in $\mathbb{Q}(\zeta)$, and since the latter is $p^{h-h_0-\gamma}$ ([3], Chapter III, Lemma 4) we conclude that the inertia degree $\bar{f}$ of μ is also $p^{h-h_0-\gamma}$. At the same time the ramification index is $\bar{e}=1$, because of the fact that μ is not ramified in Z. Then, if we consider $\bar{g} = e$ we have from the general theory that

$$\bar{e}\bar{f}\bar{g} = [Z : \mathbb{Q}(i)]$$

so that if p is odd we get

$$e = \bar{g} = \frac{p^{h-h_0-1}(p-1)}{p^{h-h_0-\gamma}} = p^{\gamma-1}(p-1)$$

and if $p=2$

$$e = \bar{g} = \frac{p^{h-h_0-2}}{p^{h-h_0-\gamma}} = p^{\gamma-2}$$

Note that actually $\gamma = h'$: in fact, we know that $g^e - 1 = rp^{h'}$ where r is coprime with p, hence for p odd

$$g^{p^{\gamma-1}(p-1)} = 1 + rp^{h'}$$

and

$$g^{p^{h-h_0-1}(p-1)} = \left(g^{p^{\gamma-1}(p-1)}\right)^{p^{h-h_0-\gamma}} = \left(1 + rp^{h'}\right)^{p^{h-h_0-\gamma}}$$

and for analogously for $p = 2$

$$5^{2^{\gamma-2}} = 1 + rp^{h'}$$

and

$$5^{2^{h-h_0-2}} = \left(g^{p^{\gamma-2}}\right)^{p^{h-h_0-\gamma}} = \left(1 + rp^{h'}\right)^{p^{h-h_0-\gamma}}$$

Since for p odd g is a primitive root of unity modulo p^{h-h_0} then

$$g^{p^{h-h_0-1}(p-1)} \equiv 1 \bmod p^{h-h_0}$$

and

$$g^{p^{h-h_0-1}(p-1)} \not\equiv 1 \bmod p^{h-h_0+t}$$

for every $t > 0$. On the other hand, if $p = 2$ by induction on $l \geq 3$ we may establish the congruences

$$\begin{aligned} 5^{2^{l-3}} = (1 + 2^2)^{2^{l-3}} &\equiv 1 + 2^{l-1} \bmod 2^l \\ 5^{2^{l-2}} \equiv (1 + 2^{l-1})^2 &\equiv 1 \bmod 2^l \end{aligned}$$

and

$$5^{2^{l-2}} \equiv (1 + 2^{l-1})^2 \not\equiv 1 \bmod 2^{l+t}$$

for every $t > 0$. Therefore in both cases we have (choosing $l = h - h_0$)

$$\left(1 + rp^{h'}\right)^{p^{h-h_0-\gamma}} \equiv 1 \bmod p^{h-h_0}$$

and

$$\left(1 + rp^{h'}\right)^{p^{h-h_0-\gamma}} \not\equiv 1 \bmod p^{h-h_0+t}$$

for every $t > 0$, but this holds if and only if $h' = \gamma$.

Finally, take k such that μ ramifies in C_k. Then, since μ is not ramified in $L_{h-h_0-h'}$, we get that

$$L_{h-h_0-h'} \subsetneq C_k$$

so that

$$[L_{h-h_0-h'} : \mathbb{Q}(i)] + 1 \leq [C_k : \mathbb{Q}(i)]$$

which means that

$$h - h_0 - \gamma + 1 = h - h_0 - h' + 1 \leq k$$

i.e

$$h - h_0 - k + 1 \leq \gamma$$

Then,

$$\begin{aligned} m - 1 &\equiv 0 \bmod p^{\gamma} \\ &\equiv 0 \bmod p^{h-h_0-k+1} \end{aligned}$$

as we wanted to prove. □

Clearly at this point Lemma (2.1.2) follows as a trivial corollary.

2.1.2 The proof of Theorem (2.1.2)

Now we are ready to start with the proof of our theorem. Note that in the following discussion, if K is a number field we are going to denote by $\mathcal{O}_K$ its ring of integers.

Proof. Since $\mathbb{Q}(i) \subseteq C_\mu$ is a Galois extension of degree $m-1$, using Sylow's Theorem we get that for every i the group $Gal(C_\mu/\mathbb{Q}(i))$ has a subgroup G_i of order $p_i^{h_i}$ (we are calling $p_0 = 2$, and $h_0 = h + 2$). So when we consider the subfield L_j of C_μ fixed by the product

$$\prod_{i \neq j} G_i$$

we get that this field is a cyclic Galois extension of $\mathbb{Q}(i)$ (since every subgroup of a cyclic field is normal) of degree $p_j^{h_j}$. Moreover, $L_0 L_1 \dots L_t = C_\mu$, because $A = L_0 L_1 \dots L_t$ is contained in C_μ, and so $Gal(C_\mu/A) \subseteq Gal(C_\mu/K_i) = \prod_{j \neq i} G_i$ for all i. But this means that $Gal(C_\mu/A) \subseteq \bigcap_{1 \leq i \leq t} \prod_{j \neq i} G_i = \{1_G\}$ and so $C_\mu = A = L_0 L_1 \dots L_t$.
According to Lemma (2.1.2), for every $j \neq 0$ the discriminant $\Delta(L_j|\mathbb{Q}(i))$ of the extension $\mathbb{Q}(i) \subseteq L_j$ is not divisible by $1 + i$, and at the same time, by Proposition (2.1.2) it must divide

$$2^{\frac{(m-1)^2}{2}} \mu^{m-2}$$

So, since μ is prime in $\mathbb{Q}(i)$ there must be a number $s_j \in \mathbb{N}$, $s_j \neq 0$, such that $\Delta(L_j|\mathbb{Q}(i)) = (\mu)^{s_j}$.
Now, since the last extension is cyclic, it holds that for all $r \leq h_j$ we have a subextension L_j^r of L_j such that $[L_j^t : \mathbb{Q}(i)] = p_j^r$. We note that $\Delta(L_j^t|\mathbb{Q}(i))$

must divide $\Delta(L_j|\mathbb{Q}(i)) = \mu^{s_j}$, and so there must be a number $a_{j,t} \in N$, $1 \leq a_{j,t} \leq s_j$ such that

$$\Delta(L_j^t|\mathbb{Q}(i)) = (\mu)^{a_{j,t}}$$

Now, let $\mathfrak{m}_r$ be a prime of L_j^r lying over μ. Since for all r we have $L_j^r \subsetneq L_j^{r+1}$, and since the discriminant of this extension must divide a power of μ, $\mathfrak{m}_r$ must ramify in L_j^{r+1}, and since the well known formula states $efg = p$ in this case, then e must be equal to the prime p. Thus $L_j^r \subsetneq L_j^{r+1}$ is a totally ramified extension, and so also $\mathbb{Q}(i) \subseteq L_j$ is. Hence there is a prime ideal $\mathfrak{M}_j$ of L_j such that

$$\mu\mathcal{O}_{L_j} = \mathfrak{M}_j^{p_j^{h_j}}$$

We have to understand what happens in L_0. We have already seen that

$$\prod_{j=1}^{m-1} = \mu$$

where $x_1 = \varphi(\rho_1 \frac{\omega}{\mu}), \ldots, x_{m-1} = \varphi(\rho_{m-1} \frac{\omega}{\mu})$ are the roots of $P_\mu(x)$. Furthermore, since $P_\mu(x)$ is formed only by powers of x of the form x^{4n} for some $n \in \mathbb{N}$, it is clear that if $\bar{x}$ is a root, then

$$-\bar{x}, i\bar{x}, -i\bar{x}$$

are roots too; and so since $m - 1 \equiv 0 \bmod 4$ we conclude that μ is a square in C_μ, i.e. that $\sqrt{\mu} \in C_\mu$.
Clearly $[C_\mu : \mathbb{Q}(i)(\sqrt{\mu})] = 2$, thus $\mathbb{Q}(i)(\sqrt{\mu})$ must be contained in L_0. Since the discriminant $\Delta(\mathbb{Q}(i)(\sqrt{\mu})|\mathbb{Q}(i))$ is surely divided by μ, μ must divide also the discriminant of L_0. Now consider the inertia field K_μ of μ in C_μ. From what we have seen before, it follows that $K_\mu \subseteq L_0$; moreover, due to the fact that L_0 is a cyclic extension, it must be that either $K_\mu \subseteq \mathbb{Q}(i)(\sqrt{\mu})$ or $\mathbb{Q}(i)(\sqrt{\mu}) \subsetneq K_\mu$. Since μ is already ramified in $\mathbb{Q}(i)(\sqrt{\mu})$, it follows that the inertia field is trivial, and so μ is totally ramified in C_μ (and consequently also in L_0).

The previous discussion implies that there must be a prime ideal $\mathfrak{M}$ of C_μ lying over μ such that

$$\mu\mathcal{O}_{C_\mu} = \mathfrak{M}^{m-1}$$

and consequently

$$\begin{aligned} \mathfrak{M}^{m-1} &= (x_1 \cdot x_2 \cdot \ldots \cdot x_{m-1})\mathcal{O}_{C_\mu} \\ &= (x_1) \cdot (x_2) \cdot \ldots \cdot (x_{m-1}) \end{aligned}$$

Recalling that $\mathcal{O}_{C_\mu}$ is a Dedekind domain, by unique factorization we get that for every j

$$\mathfrak{M} = (x_j)$$

so that all the roots are associated (in the following, we will write $x \sim y$ meaning that x and y are associated).

Now we consider the prime $(1+i) \in \mathbb{Q}(i)$. If $\rho \in \mathbb{Z}[i]$ is odd, both $\varphi(\rho\frac{\omega}{\mu})$ and $\varphi((1+i)\rho\frac{\omega}{\mu})$ are roots of $P_\mu(x)$, and from what we have just seen they are associated. Then, from

$$\varphi((1+i)\rho\frac{\omega}{\mu}) = \frac{(1+i)\varphi(\rho\frac{\omega}{\mu})}{f(u)F(u)}$$

it follows that

$$f(u)F(u) \sim (1+i)$$

If now we consider two roots $x_1 = \varphi(u), x_1' = \varphi(v)$ such that $x_1 \neq \pm x_1'$, then $x_2 = \varphi(u+v)$ and $x_2' = \varphi(u-v)$ are also roots of $P_\mu(x)$, and $x_2 \neq \pm x_2'$. Using Eq.(2.3), it follows that

$$(x_1 - x_1')(x_1 + x_1')(x_2 - x_2') \sim (1+i)^3 x_1^3$$

and the substitution $v \mapsto -v$ show that $(x_1 + x_1')(x_1 - x_1')(x_2 + x_2')$ is also associated with $(1+i)^3 x_1^3$, thus $(x_2 + x_2') \sim (x_2 - x_2')$.
Consider now two arbitrary roots $x \neq \pm y$. Since we can always find two suitable elements $u, v \in \mathbb{C}$ such that $x = \varphi(u+v)$ and $y = \varphi(u-v)$, it is clear that the previous argument still holds for x and y. As a consequence, $(x_1 + x_1')$ is associated with $(x_1 - x_1')$, and thus also $(x_1 - x_1')^2(x_2 - x_2')$ and $(1+i)^3 x_1^3$ are associated. If now we repeat the whole argument with x_2 and x_2', clearly we find two other roots x_3, x_3' such that $x_3 \neq \pm x_3'$ and

$$(x_2 - x_2')^2(x_3 - x_3') \sim (1+i)^3 x_1^3$$

and continuing this way we see that for every $j < \frac{m-1}{2} - 1$, we can find a couple of roots (x_j, x_j'), where $x_j \neq \pm x_j'$, such that

$$(x_{j-1} - x_{j-1}')^2(x_j - x_j') \sim (1+i)^3 x_1^3 \sim (x_j - x_j')^2(x_{j+1} - x_{j+1}')$$

and also a couple of roots $(x_{\frac{m-1}{2}}, x_{\frac{m-1}{2}}')$, where $x_{\frac{m-1}{2}} \neq \pm x_{\frac{m-1}{2}}'$, such that

$$(x_{(\frac{m-1}{2}-1)} - x_{(\frac{m-1}{2}-1)}')^2(x_{\frac{m-1}{2}} - x_{\frac{m-1}{2}}') \sim (1+i)^3 x_1^3 \sim (x_{\frac{m-1}{2}} - x_{\frac{m-1}{2}}')^2(x_1 - x_1')$$

Multiplying all these relations together we get that

$$(x_1 - x_1')^3 \sim (1+i)^3 x_1^3$$

and so

$$x_1 - x_1' \sim (1+i)x_1$$

Since x_1 and x_1' where two arbitrary roots such that $x_1 \neq \pm x_1'$, this means that for every two roots $x \neq \pm y$ it holds that

$$x - y \sim (i+1)x \tag{2.9}$$

Keeping these properties in mind, we now claim that *if x is any root of $P_\mu(x)$ for $\mu \neq -1+2i$, then the element $\frac{x^4-1+2i}{4}$ is a unit.*
First of all, note that if we consider $\mu = -1+2i$, then the polynomial of the μ-division has degree 4 (the norm of μ is 5), and it has μ as constant term, hence from what we have seen before we must have $P_\mu(x) = x^4 + (-1+2i)$, and therefore for every $u \in \mathbb{C}$ it holds that

$$\varphi((-1+2i)u) = \varphi(u)\frac{(\varphi(u))^4 + (-1+2i)}{(-1+2i)(\varphi(u))^4 + 1}$$

From this equation it follows immediately that

$$\frac{\varphi(u) - \varphi((-1+2i)u)}{\varphi((-1+2i)u)} = \frac{2(i-1)((\varphi(u))^4 - 1)}{(\varphi(u))^4 + (-1+2i)} \tag{2.10}$$

Now consider $\mu \neq (-1+2i)$. Since if $\varphi(u)$ is a root of $P_\mu(x)$ then also $\varphi((-1+2i)u)$ is a root, Eq.(2.9) implies that

$$\frac{\varphi(u) - \varphi((-1+2i)u)}{\varphi((-1+2i)u)} \sim (1+i)$$

and thus, by Eq.(2.10),

$$\frac{(\varphi(u))^4 + (-1+2i)}{4} \sim \frac{(i-1)((\varphi(u))^4 - 1)}{2(1+i)} \tag{2.11}$$

Actually $(\varphi(u))^4 - 1 \sim (i+1)^2$: in fact, using the addition formula, we get that

$$\varphi(u+iu) = \frac{(i+1)\varphi(u)f(u)F(u)}{1-(\varphi(u))^4}$$

and we know from the previous discussion that $f(u)F(u) \sim (i+1)$ and that $\varphi(u+iu) \sim \varphi(u)$ (both of them are roots). Consequently, the relation expressed in Eq.(2.11) proves our claim.
The previous information is crucial in order to find the discriminant of the extension $\mathbb{Q}(i) \subseteq K = \mathbb{Q}(i, (\varphi(u))^4)$. In fact, since $\alpha = \frac{(\varphi(u))^4 + (-1+2i)}{4}$ is a unit, the discriminant of $\mathbb{Q}(i, (\varphi(u))^4)$ is the principal ideal generated by $\Delta(\alpha)$, the discriminant of the basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{\frac{m-1}{4}}\}$.
We can compute this discriminant from the discriminant $\Delta((\varphi(u))^4)$. In

fact, setting $\theta_i = \sigma_i((\varphi(u))^4)$ for every $\sigma_i \in Gal(K/\mathbb{Q}(i))$ the well known formula for $\Delta(\alpha)$ implies that

$$\begin{aligned}
\Delta(\alpha) &= \prod_{i>j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \\
&= \prod_{i>j} \left(\frac{(\theta_i + (-1+2i)}{4} - \frac{\theta_j + (-1+2i)}{4} \right)^2 \\
&= \prod_{i>j} \frac{(\theta_i - \theta_j)^2}{4^2} \\
&= \frac{\Delta((\varphi(u))^4)}{4^{M(M-1)}} \quad \text{where } M = \frac{m-1}{4}
\end{aligned}$$

At this point, we are only left to compute the discriminant of $(\varphi(u))^4$ using the informations we already have. Before starting, note that from now on if $L' = L(\theta)$ is a separable extension of dimension n we will denote by $\Delta(\theta|L)$ the discriminant of the L-basis $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$

Claim 2.1.1. *In our situation,*

$$\Delta(\varphi(u)|\mathbb{Q}(i)) = \mathbf{N}_{K|\mathbb{Q}(i)} \left(\Delta(\varphi(u))|K\right) \Delta((\varphi(u))^4|\mathbb{Q}(i))^{[C_\mu:K]}$$

We know that in general if $L' = L(\theta)$ is a separable extension of dimension n then

$$\Delta(\theta|L) = (-1)^{n(n-1)/2} \mathbf{N}_{L'|L}(f'(\theta)) \tag{2.12}$$

where $f(X)$ is the minimum polynomial of θ over L and $f'(X)$ is its derivative (compare with [12], Theorem 7.6, p. 39). Hence in our case we get that

$$\begin{aligned}
\Delta(\varphi(u)|\mathbb{Q}(i)) &= (-1)^{(m-1)(m-2)/2} \mathbf{N}_{C_\mu|\mathbb{Q}(i)}(P'_\mu(\varphi(u))) \\
&= \mathbf{N}_{C_\mu|\mathbb{Q}(i)}(P'_\mu(\varphi(u)))
\end{aligned}$$

(recall that $m - 1 \equiv 0 \bmod 4$) Now let ψ_μ be the polynomial such that $P_\mu(X) = \psi_\mu(X^4)$. Since $g(X) = X^4 - (\varphi(u))^4$ is the minimum polynomial of $\varphi(u)$ over K we also get

$$\Delta(\varphi(u)|K) = (-1)^{4(4-1)/2} \mathbf{N}_{C_\mu|K}(g'(\varphi(u))) = \mathbf{N}_{C_\mu|K}(f'(\varphi(u)))$$

where $f(X) = X^4$. In the same way,

$$\Delta((\varphi(u))^4|\mathbb{Q}(i)) = (-1)^{M(M-1)/2} \mathbf{N}_{K|\mathbb{Q}(i)}(\psi'_\mu((\varphi(u))^4))$$

and therefore

$$\begin{aligned}
&\mathbf{N}_{K|\mathbb{Q}(i)} \left(\Delta(\varphi(u))|K\right) \Delta((\varphi(u))^4|\mathbb{Q}(i))^{[C_\mu:K]} = \\
&\quad = \mathbf{N}_{K|\mathbb{Q}(i)} \left(\mathbf{N}_{C_\mu|K}(f'(\varphi(u)))\right) \mathbf{N}_{K|\mathbb{Q}(i)}(\psi'_\mu((\varphi(u))^4))^4 \\
&\quad\quad = \mathbf{N}_{C_\mu|\mathbb{Q}(i)}(f'(\varphi(u))) \mathbf{N}_{K|\mathbb{Q}(i)}(\psi'_\mu(f(\varphi(u))))^4 \\
&\quad\quad\quad = \mathbf{N}_{C_\mu|\mathbb{Q}(i)}(\psi'_\mu(f(\varphi(u))) f'(\varphi(u)))
\end{aligned}$$

where the last equation holds because since $\psi'_\mu(f(\varphi(u))) \in K$ it must be

$$(\psi'_\mu(f(\varphi(u))))^4 = \mathbf{N}_{C_\mu|K}(\psi'_\mu(f(\varphi(u))))$$

Hence we conclude by simply remarking that $P'_\mu(X) = \psi'_\mu(f(X))f'(X)$.

Now recall that we have already seen that

$$\Delta(\varphi(u)|\mathbb{Q}(i)) = 2^{\frac{(m-1)^2}{2}}\mu^{m-2}$$

Moreover, we can show that $\Delta(\varphi(u)|K) = -16^2(\varphi(u))^{12}$ applying Eq. (2.12). The last information we need is the value of $\mathbf{N}_{K|\mathbb{Q}(i)}(\Delta(\varphi(u))|K)$ but seen that $\mathbf{N}_{C_\mu|K}(\varphi(u))$ is the constant term of $g(X) = X^4 - (\varphi(u))^4$ and since the ideal $(\varphi(u))C_\mu$ lies over μ (and is totally ramified) it holds that

$$\begin{aligned}\mathbf{N}_{K|\mathbb{Q}(i)}(-(\varphi(u))^4) &= \mathbf{N}_{K|\mathbb{Q}(i)}(\mathbf{N}_{C_\mu|K}(\varphi(u))) \\ &= \mathbf{N}_{C_\mu|\mathbb{Q}(i)}(\varphi(u)) \\ &= \mu\end{aligned}$$

Hence it follows that

$$\mathbf{N}_{K|\mathbb{Q}(i)}(\Delta(\varphi(u))|K) = 16^{\frac{m-1}{2}}\mu^3$$

so using the previous Claim we obtain

$$\Delta((\varphi(u))^4|\mathbb{Q}(i)) = 4^{M(M-1)}\mu^{M-1}$$

which means that the discriminant of K over $\mathbb{Q}(i)$ is μ^{M-1}.
At this point, it might be useful to stop for a second and summarize what we have proven so far.

- We have seen how we can find all the subfields mentioned in the statement of the theorem.
- We have proven that the subfield K (which is unique since all the roots of $P_\mu(x)$ are associated) has discriminant $\Delta(K|\mathbb{Q}(i)) = \mu^{M-1}$
- We have seen that μ is totally ramified in C_μ, and consequently in all its subfields. Moreover, it is the only ramified prime in the subfields whose degree is an odd power, and in the subfields of degree 2^λ where $\lambda \leq h$.

Note that we still need to find the discriminant of the previously enlisted subfields. But it holds in general (a convenient reference is [21], Theorem 28, p. 302)

Theorem 2.1.3. *Let R be a Dedekind domain, and R' its integral in a finite algebraic separable extension K' of the quotient field K of R. If $\mathfrak{p}$ is a proper prime ideal in R, let $\mathfrak{P}$ be a prime ideal in R' lying over $\mathfrak{p}$ and denote by $e(\mathfrak{P})$ the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. Then the different $\mathfrak{D}_{K'|K}$ may be factored in prime ideal as the product*

$$\mathfrak{D}_{K'|K} = \prod_{\mathfrak{P}} \mathfrak{P}^{m(\mathfrak{P})}$$

where $m(\mathfrak{P}) \geq e(\mathfrak{P})-1$ and the equality holds if and only if both the following conditions hold:

a) $e(\mathfrak{P})$ is not a multiple of the characteristic of $R/\mathfrak{p}$,

b) $R'/\mathfrak{P}$ is separable over $R/\mathfrak{p}$.

Our setting satisfies all the hypothesis, so we immediately have that if L is one of the subfields whose degree is an odd power, or one of the subfields of degree 2^λ where $\lambda \leq h$, denoting by $\mathfrak{M}$ a prime ideal lying over μ in $\mathcal{O}_L$ we get that

$$\mathfrak{D}_{L|\mathbb{Q}(i)} = \mathfrak{M}^{[L:\mathbb{Q}(i)]-1}$$

since μ is not only the unique ramified prime, but it is also totally ramified. Therefore it follows trivially

$$\Delta(L|\mathbb{Q}(i)) = \mu^{[L:\mathbb{Q}(i)]-1}$$

as we wanted to show.

Now we are left to prove the following statements:

Claim 2.1.2. *The relative different of the extensions*

$$K = \mathbb{Q}(i, (\varphi(u))^4) \subset \mathbb{Q}(i, (\varphi(u))^2) = K'$$

is equal to $(i+1)(\varphi(u)^2)$.

Claim 2.1.3. *The relative different of the extensions*

$$K' \subset C_\mu$$

is equal to $(i+1)(\varphi(u))$

In fact, using these claims, we can conclude in the following way: if for every suitable field extension $L \subset L'$ we denote by $\mathfrak{D}_{L'|L}$ its relative different, it holds that

$$\mathfrak{D}_{C_\mu|K} = \mathfrak{D}_{C_\mu|K'}(\mathfrak{D}_{K'|K}\mathcal{O}_{C_\mu}) = (1+i)^2\varphi(u)^3$$

Therefore,

$$\begin{aligned}\Delta(C_\mu|\mathbb{Q}(i)) &= \mathbf{N}_{K|\mathbb{Q}(i)}(\Delta(C_\mu|K))\Delta(K|\mathbb{Q}(i))^{[C_\mu:K]} \\ &= \mathbf{N}_{C_\mu|\mathbb{Q}(i)}(\mathfrak{D}_{C_\mu|K})\mu^{(M-1)4} \\ &= (1+i)^{2(m-1)}\mu^3\mu^{m-5} \\ &= 2^{m-1}\mu^{m-2}\end{aligned}$$

as we needed to prove. Moreover, since $(i+1)$ divides the different $K \subset K'$, it must be ramified in K', and since it cannot be ramified in any field extension of odd power degree, it must ramify in L_0. But we know that it is not ramified in L_0^h (the subfield of L_0 such that $[L_0^h : \mathbb{Q}(i)] = 2^h$) so it must ramify in the extension $L_0^h \subset L_0^{h+1}$: indeed $L_0^{h+1}L_1 \dots L_t = K'$ due to the fact that $[C_\mu : K'] = 2$. Hence (again by Theorem (2.1.3))

$$\mathfrak{D}_{L_0^{h+1}|\mathbb{Q}(i)} = (1+i)(\varphi(u)^2)^{2^{h+1}-1}$$

(μ is totally ramified in C_μ) and analogously

$$\mathfrak{D}_{L_0^{h+2}|\mathbb{Q}(i)} = (1+i)^2(\varphi(u))^{2^{h+2}-1}$$

which means that

$$\begin{aligned}\Delta(L_0^{h+1}|\mathbb{Q}(i)) &= (1+i)^{2^{h+1}}\mu^{2^{h+1}-1} \\ \Delta(L_0^{h+1}|\mathbb{Q}(i)) &= (1+i)^{2^{h+3}}\mu^{2^{h+2}-1}\end{aligned}$$

as we wanted to show. At this point, we are only left to prove the claims.

For the first claim, we shall consider the elements

$$\tau = \frac{i + (\varphi(u))^2}{f(u)F(u)} \in K'$$

and

$$\bar{\tau} = \frac{i - (\varphi(u))^2}{f(u)F(u)} \in K'$$

Since $(\varphi(u))^2$ and $-(\varphi(u))^2$ are both roots of the polynomial $X^2 - (\varphi(u))^4$, which is irreducible over K, it is clear that the Galois group of $K \subset K'$ is formed by the identity and by the automorphism defined by

$$(\varphi(u))^2 \mapsto -(\varphi(u))^2$$

Hence $\bar{\tau}$ must be a root of the minimum polynomial $T(X)$ of τ, and consequently we have that $T(X) = (X - \tau)(X - \bar{\tau})$.
Actually τ and $\bar{\tau}$ are two associated integers. Since

$$T(X) = X^2 - (\tau + \bar{\tau})X + \bar{\tau}\tau$$

and $\frac{\tau}{\bar{\tau}}$ is a root of $X^2 - (\frac{\tau}{\bar{\tau}} + \frac{\bar{\tau}}{\tau})X + 1$, in order to prove that they are associated integers it is enough to show that $\tau + \bar{\tau}, \bar{\tau}\tau$ and $\frac{\tau}{\bar{\tau}} + \frac{\bar{\tau}}{\tau}$ are integers. Note that since $\varphi(2u) = \frac{2\varphi(u)f(u)F(u)}{1+(\varphi(u))^4}$ and since $\varphi(2u)$ and $\varphi(u)$ are associated (being two roots of $P_\mu(X)$), recalling that $f(u)F(u) \sim (1+i)$ and $(1-(\varphi(u))^4) \sim (i+1)^2$ (as we have seen before in the proof) we get

$$\begin{aligned} \tau + \bar{\tau} &= \frac{2i}{f(u)F(u)} \sim (i+1) \\ \tau\bar{\tau} &= -\frac{1+(\varphi(u))^4}{(f(u)F(u))^2} \sim \frac{2f(u)F(u)}{(f(u)F(u))^2} \sim (i+1) \\ \frac{\tau}{\bar{\tau}} + \frac{\bar{\tau}}{\tau} &= \frac{2(1-(\varphi(u))^4)}{1+(\varphi(u))^4} \sim \frac{2f(u)F(u)}{(i+1)^2} \sim (i+1) \end{aligned}$$

thus τ and $\bar{\tau}$ are associated integers.
Moreover, the previous discussion implies that as principal ideals

$$(i+1) = (\tau\bar{\tau}) = (\tau)(\bar{\tau}) = (\tau)^2$$

hence $(i+1)$ ramifies in $K \subset K'$. Since the ramification index $e(1+i)$ of $(1+i)$ must be $1 < e(i+1) \leq [K : K'] = 2$, $(1+i)$ is totally ramified in $K \subset K'$, and using again Theorem (2.1.3) we obtain

$$\mathfrak{D}_{K'|K} = (1+i)(\varphi(u)^2)$$

(μ is totally ramified in C_μ, and $\varphi(u)^2$ lies over μ).
Finally, we turn our attention to the extension $K' \subset C_\mu$. Let $\gamma \in C_\mu$. Clearly γ can be represented in the form

$$\gamma = a + b\varphi(u)$$

where $a, b \in K' = \mathbb{Q}(i, (\varphi(u))^2)$. Hence we may write

$$\gamma = \frac{a + b\varphi(u)}{c}$$

where $a, b, c \in \mathbb{Z}[i][(\varphi(u))^2]$ and no prime divides all of a, b, c. We know that γ is an integer if and only if the coefficients of the minimum polynomial

$$\left(X - \frac{a + b\varphi(u)}{c}\right)\left(X - \frac{a - b\varphi(u)}{c}\right)$$

are integers, thus if and only if

$$\frac{a^2 - b^2(\varphi(u))^2}{c^2} \in \mathcal{O}_K$$

$$\frac{2a}{c} \in \mathcal{O}_K$$

Since $\mathcal{O}_K$ is a free $\mathbb{Z}[i]$-module, c must divide $2a$. If a and c have a common factor λ, then the first relation implies that λ divides b (the unique prime dividing $(\varphi(u))^2$ is $(\varphi(u))$ which is not in K') contradicting our assumption. As a consequence, c must be either a unit or an element associated to 2. In the second case, $c = 2\nu$ where ν is a unit and so

$$\gamma = \frac{a + b\varphi(u)}{2\nu} = \frac{a\nu^{-1} + b\nu^{-1}\varphi(u)}{2} = \frac{\tilde{a} + \tilde{b}\varphi(u)}{2}$$

where $\tilde{a}$ and $\tilde{b}$ are integers of K'; moreover

$$\frac{a^2 - b^2(\varphi(u))^2}{c^2} = \frac{\tilde{a}^2 - \tilde{b}^2(\varphi(u))^2}{4} \in \mathcal{O}_K$$

if and only if

$$\tilde{a}^2 - \tilde{b}^2(\varphi(u))^2 \equiv 0 \bmod 4$$

In the other case, if c is a unit then γ is always an integer, and furthermore $\tilde{a} = 2ac^{-1}$ and $\tilde{b} = 2bc^{-1}$ are integers such that

$$\gamma = \frac{a + b\varphi(u)}{c} = \frac{\tilde{a} + \tilde{b}\varphi(u)}{2}$$

and again

$$\tilde{a}^2 - \tilde{b}^2(\varphi(u))^2 \equiv 0 \bmod 4$$

Thus an element γ is an integer if and only if

$$\gamma = \frac{a + b\varphi(u)}{2}$$

where $a, b \in \mathcal{O}_K$ and

$$a^2 - b^2(\varphi(u))^2 \equiv 0 \bmod 4 \tag{2.13}$$

but we are now going to prove that

Claim 2.1.4. *If a couple (a, b) satisfies the congruence (2.13), then $(i + 1)$ divides b. On the other hand, if b is an integer in K' which is divisible by $(1+i)$ then there is another integer a such that (a, b) satisfies the congruence (2.13).*

We need to consider the element

$$\xi = 1 + if(u) = 1 + i\sqrt{1 - (\varphi(u))^2}$$

ξ is an integer since its is a root of the polynomial $X^2 - 2X + 2 - (\varphi(u))^2$. Moreover, since

$$\frac{f(u)}{F(u)} + \frac{F(u)}{f(u)} = \frac{2}{f(u)F(u)} \sim (i + 1)$$

is an integer, $f(u)$ and $F(u)$ are associate, thus as ideals

$$(1+i) = (f(u)F(u)) = (f(u))^2$$

which implies that if

$$\mathfrak{z}_1^2\mathfrak{z}_2^2\cdots\mathfrak{z}_g^2 = (1+i)$$

is the prime decomposition of $(1+i)$ in K' then

$$\xi^2 - (\varphi(u))^2 = 2if(u) \equiv 0 \bmod \mathfrak{z}_1^5\mathfrak{z}_2^5\cdots\mathfrak{z}_g^5$$

and the congruence does not hold for any higher power.
Note that for every element $\zeta \in K'$ and for every $1 \leq l \leq g$ the congruence

$$\zeta^2 - (\varphi(u))^2 \equiv 0 \bmod \mathfrak{z}_l^6$$

is impossible. This can be shown in the following way: if $\zeta^2 \equiv (\varphi(u))^2 \bmod \mathfrak{z}_l^6$, then

$$\zeta^2 \equiv (\varphi(u))^2 \bmod \mathfrak{z}_l^5$$

and so

$$(\zeta - \xi)(\zeta + \xi) = \zeta^2 - \xi^2 \equiv 0 \bmod \mathfrak{z}_l^5$$

But if $(\zeta - \xi)$ is divided by $\mathfrak{z}_l$ then

$$\begin{aligned} \zeta + \xi &= \zeta - \xi + 2\xi \\ &\equiv 0 + 2\xi \bmod \mathfrak{z}_l \\ &\equiv 0 \bmod \mathfrak{z}_l \end{aligned}$$

since $\mathfrak{z}_l$ divides the ideal (2), thus we actually have

$$\zeta^2 - \xi^2 = (\zeta - \xi)(\zeta + \xi) \equiv 0 \bmod \mathfrak{z}_l^6$$

and so

$$\xi^2 - (\varphi(u))^2 = (\zeta^2 - (\varphi(u))^2) - (\zeta^2 - \xi^2) \equiv 0 \bmod \mathfrak{z}_l^6$$

which is absurd.
Now suppose that b is not divisible by $(1+i)$, which means that there is an index $1 \leq l \leq g$ such that $\mathfrak{z}_l^2$ does not divide b. From congruence (2.13) it follows that a and b are divided by the same power of $\mathfrak{z}_l$ and so we can find an element ζ such that

$$a \equiv b\zeta \bmod \mathfrak{z}_l^4$$

Hence $b^2\zeta^2 - b^2(\varphi(u))^2$ must by divisible by $\mathfrak{z}_l^8$, and seen that b is not divisible by $\mathfrak{z}_l^2$ this implies that

$$\zeta^2 - (\varphi(u))^2 \equiv 0 \bmod \mathfrak{z}_l^6$$

which is a contradiction.
On the other hand, if $(i+1)$ divides b, we simply take $a = b\xi$ so that

$$a^2 - b^2 2(\varphi(u))^2 = b^2(\xi^2 - 2(\varphi(u))^2) = 2if(u)b^2 \equiv 0 \bmod 4$$

Hence actually every integer γ can be represented in the form

$$\frac{a + b\varphi(u)}{1+i}$$

and moreover, we can find an integer $\gamma = \frac{a+b\varphi(u)}{(1+i)}$ such that b is coprime with $(1+i)$. If now we consider the element

$$\gamma' = \frac{a - b\varphi(u)}{(1+i)}$$

we get that

$$\gamma - \gamma' = (1-i)b\varphi(u)$$

and since b is arbitrary, this means that

$$\mathfrak{D}_{C_\mu|K'} = (1+i)(\varphi(u))$$

as we wanted to prove. □

2.2 The division by an odd prime power.

As before, we are considering a odd complex prime μ and its norm m. The multiplication formula related to the element μ^h where h is an integer can clearly be obtained by iteration of the formula

$$\varphi(\mu u) = x\frac{P_\mu(x^4)}{Q_\mu(x)}$$

where as usual $x = \varphi(u)$. More precisely

Theorem 2.2.1. *Let μ be an odd complex prime, m its norm. Then for every $h \in \mathbb{N}$ it holds that*

$$\varphi(\mu^h u) = x\frac{\Psi_{\mu,h}(x)}{\mathbf{X}_{\mu,h}(x)}, \text{ where } x = \varphi(u)$$

where $\Psi_{\mu,h}(X), \mathbf{X}_{\mu,h}(X)$ are polynomials such that:

i) every power of X composing these polynomials is of the form X^{4n} for some $n \in \mathbb{N}$.

ii) $\Psi_{\mu,h}(X)$ *can be factorized as*

$$\Psi_{\mu,h}(X) = P_\mu \psi_2 \psi_3 \dots \psi_h$$

where for every $j \in \{2, \dots, h\}$ *and for every* $x \in \mathbb{C}$*, we have that* x *is a root of* ψ_j *if and only if* x *is one of the* μ^j*-division points of the lemniscate.*

iii) for every $j \in \{2, \dots, h\}$ ψ_j *is of degree* $m^{j-1}(m-1)$*.*

iv) for every j *all the coefficients of* ψ_j *are divisible by* μ *except the leading coefficient which is equal to* 1*. Moreover, the constant term is associated to* μ*.*

Proof. We will proceed by induction, so let us start with the case $h = 2$. We have that for every $u \in \mathbb{C}$

$$\begin{aligned} \varphi(\mu^2 u) &= \varphi(\mu u)\frac{P_\mu(\varphi(u))}{Q_\mu} \\ &= \varphi(u)\frac{P_\mu(x)}{Q_\mu(x)} \cdot \frac{P_\mu\left(\varphi(u)\frac{P_\mu(x)}{Q_\mu(x)}\right)}{Q_\mu\left(\varphi(u)\frac{P_\mu(x)}{Q_\mu(x)}\right)} \end{aligned}$$

Seen that both $P_\mu(X)$ and $Q_\mu(X)$ have degree equal to $m-1$, multiplying the numerator and the denominator with $Q_\mu(x)^{m-1}$ we obtain that

$$\varphi(\mu^2 u) = \varphi(u)\frac{P_\mu(x)}{Q_\mu(x)} \cdot \frac{\psi_2(x)}{\tau_2(x)}$$

where $\psi_2(X)$ and $\tau_2(X)$ are two polynomials of the same degree prime to each other, and so we can set $\Psi_{\mu,2}(X) = P_\mu(X)\psi_2(X)$. Moreover, since every power of X which appears in $P_\mu(X)$ and $Q_\mu(X)$ is of the form X^{4n}, the same holds for $\psi_2(X)$. Furthermore, since all the coefficients of $P_\mu(X)$ and $Q_\mu(X)$ are divisible by μ, except for the leading coefficient of $P_\mu(X)$ and the constant term of $Q_\mu(X)$, all the coefficients of $\psi_2(X)$ except the leading one are divisible by μ. Moreover, $\psi_2(X)$ is monic and its constant term is associated to μ (since $P_\mu(0) = i^\epsilon\mu$ and $Q_\mu^{m-1}(0) = (Q_\mu(0))^{m-1} = 1$). Finally, the leading term of $\psi_2(X)$ is equal to the leading term of $P_\mu(\varphi(u)P_\mu(x))$, i.e.

$$\varphi(u)^{m-1}\left(\varphi(u)^{m-1}\right)^{m-1}$$

so $\psi_2(X)$ is of degree $m(m-1) = m^{2-1}(m-1)$.
Now, supposing that the theorem holds for $h \in \mathbb{N}$, we are proving it for $h+1$. We know that

$$\varphi(\mu^h u) = x\frac{\Psi_{\mu,h}(x)}{\mathbf{X}_{\mu,h}(x)}$$

thus

$$\begin{aligned}\varphi(\mu^{h+1}u) &= \varphi(\mu^h u)\frac{P_\mu(\varphi(\mu^h u))}{Q_\mu(\varphi(\mu^h u))} \\ &= x\frac{\Psi_{\mu,h}(x)}{\mathbf{X}_{\mu,h}(x)}\cdot\frac{P_\mu\left(x\frac{\Psi_{\mu,h}(x)}{\mathbf{X}_{\mu,h}(x)}\right)}{Q_\mu\left(x\frac{\Psi_{\mu,h}(x)}{\mathbf{X}_{\mu,h}(x)}\right)}\end{aligned}$$

As before, if we multiply both the numerator and the denominator by $(\mathbf{X}_{\mu,h}(x))^{m-1}$ we obtain

$$\varphi(\mu^{h+1}u) = x\frac{\Psi_{\mu,h}(x)}{\mathbf{X}_{\mu,h}(x)}\cdot\frac{\psi_{h+1}(x)}{\tau_{h+1}(x)}$$

where $\psi_{h+1}(X)$ and $\tau_{h+1}(X)$ are two polynomials of the same degree prime to each other, and so

$$\Psi_{\mu,h+1}(X) = \Psi_{\mu,h}(X)\psi_{h+1}(X) = P_\mu(X)\psi_2(X)\dots\psi_h(X)\psi_{h+1}(X)$$

as we wanted to show in ii). In order to prove point i) we only need to repeat the same argument used for the case $h = 2$. For iv), note that since $Q_\mu(X) = \frac{1}{i^\epsilon}X^{m-1}P_\mu(X)$ (see Proposition (1.5.4)) then using the same argument used for $\psi_2(X)$ we have that the constant term of $\tau_2(X)$ is equal to 1, and all the other coefficients are divisible by μ. Hence the same holds for $\mathbf{X}_{\mu,2}(x)$, and by inductive hypothesis on $\mathbf{X}_{\mu,h}(x)$: so, using the same argument as in the case $h = 2$, we conclude that $\psi_{h+1}(X)$ has leading coefficient equal to 1, constant term associated to μ, and all the other coefficient divisible by μ (and analogously all the coefficients of $\mathbf{X}_{\mu,h+1}(x)$ are divisible by μ except for the constant term which is equal to 1). Finally, since the leading term of $\psi_{h+1}(X)$ is equal to the leading term of the polynomial $P_\mu(X\Psi_{\mu,h}(X))$, we have that

$$\deg(\psi_{h+1}(X)) = \deg(\Psi_{\mu,h}(X) + 1)\deg(P_\mu(X))$$

Therefore, seen that

$$\begin{aligned}\deg(\Psi_{\mu,h}(X)) &= \deg(P_\mu(X)) + \sum_{j=2}^{h}\deg(\psi_h(X)) \\ &= (m-1) + \sum_{j=2}^{h} m^{h-1}(m-1) \\ &= \sum_{j=1}^{h} m^{h-1}(m-1) \\ &= m^h - 1\end{aligned}$$

we get that

$$\deg(\psi_{h+1}(X)) = m^h(m-1)$$

as we needed to show. □

Theorem 2.2.2. *Let μ be an odd prime integer of $\mathbb{Q}(i)$, m its norm, and for $h \in \mathbb{N}$ denote by C_{μ^h} the splitting field of $\psi_h(X)$. Then $\mathbb{Q}(i) \subset C_{\mu^h}$ is a Galois extension of degree $m^{h-1}(m-1)$ and moreover:*

- *if μ is not real, then $Gal(C_{\mu^h}/\mathbb{Q}(i))$ is cyclic.*
- *if μ is a real number q, then*

$$Gal(\frac{C_{\mu^h}}{\mathbb{Q}(i)}) = ST$$

where S and T are cyclic groups of degree respectively $q^{h-1}(q^2-1)$ and q^{h-1}.

Proof. Since by point iv) of the previous theorem $\psi_h(X)$ satisfies the hypothesis of the Eiseinstein criterion, $\psi_h(X)$ is irreducible, so in order to prove that $\mathbb{Q}(i) \subset C_{\mu^h}$ is a Galois extension is sufficient to show that $\psi_h(X)$ is separable.
Since μ^h is odd it holds that

$$x\frac{\Psi_{\mu,h}(x)}{\mathbf{X}_{\mu,h}(x)} = \varphi(\mu^h u) = x\frac{P_\mu(x)}{Q_\mu(x)}$$

and in the proof of the previous theorem we have shown that

$$\deg \Psi_{\mu,h}(x) = m^h - 1 = \deg P_{\mu^h}(X)$$

Therefore, we see that $\psi_h(X)$ must be separable, otherwise $\Psi_{\mu,h}(x)$ would have a multiple root, contradicting the fact that $P_{\mu^h}(X)$ does not have any multiple root.
Now let us start with the second part of the proof. If μ is not real, we need the following general result that we are not going to prove (see Theorem 2, [7])

Proposition 2.2.1. *If a and b are relatively prime integers, then there is an isomorphism*

$$\frac{\mathbb{Z}[i]}{(a+ib)\mathbb{Z}[i]} \cong \frac{\mathbb{Z}}{(a^2+b^2)\mathbb{Z}}$$

Let $c, d \in \mathbb{Z}$ be such that $\mu^h = c + id$. Suppose that there is a rational prime e dividing both c and d, then it must divide μ^h. There are only three different cases, according to the prime factorization of e in $\mathbb{Z}[i]$.

- if e is inert, it must be equal to μ, which is impossible because μ is not real.

- if e splits, then μ^h id divided by two different primes, that is absurd.
- if e ramifies, then it must be equal to 2, which is a contradiction seen that μ^h is odd.

Hence using the previous Proposition we get that

$$\frac{\mathbb{Z}[i]}{\mu^h\mathbb{Z}[i]} \cong \frac{\mathbb{Z}}{m^h\mathbb{Z}}$$

and thus with the help of Theorem (2.1.1) we obtain

$$Gal(\frac{C_{\mu^h}}{\mathbb{Q}(i)}) \hookrightarrow \left(\frac{\mathbb{Z}[i]}{\mu^h\mathbb{Z}[i]}\right)^* \cong \left(\frac{\mathbb{Z}}{m^h\mathbb{Z}}\right)^*$$

Since m is a prime different from 2 being the norm of the prime $\mu \in \mathbb{Z}[i]$, the group of units of $\mathbb{Z}/m^h\mathbb{Z}$ is a cyclic group of order $m^{h-1}(m-1)$ (compare with [16], Proposition A.8.). Recalling that $[C_{\mu^h} : \mathbb{Q}(i)] = m^{h-1}(m-1)$ it follows that

$$Gal(\frac{C_{\mu^h}}{\mathbb{Q}(i)}) \cong \left(\frac{\mathbb{Z}}{m^h\mathbb{Z}}\right)^*$$

which proves that the extension if μ is not real $\mathbb{Q}(i) \subset C_{\mu^h}$ is cyclic.
If μ is a real integer q, we cannot apply the same argument, but we can instead compute directly the number of units in the following way. First of all we need to find the cardinality of the group of units. Since q is inert, the equivalence classes of $\mathbb{Z}[i]/q^h\mathbb{Z}[i]$ are given as

$$\{[a+ib] : 0 \leq a \leq q^h - 1 \text{ and } 0 \leq b \leq q^h - 1\}$$

(see [6], Theorem 1). Moreover, since $a+ib$ is coprime with q if at least one between a and b is not divisible by q, it is easy to see that the cardinality is equal to $q^{2h-2}(q^2-1)$. This means that actually there is an isomorphism

$$Gal(\frac{C_{q^h}}{\mathbb{Q}(i)}) \cong \left(\frac{\mathbb{Z}[i]}{q^h\mathbb{Z}[i]}\right)^*$$

so in order to conclude, we only have to find the structure of $(\mathbb{Z}[i]/q^h\mathbb{Z}[i])^*$.

Consider a primitive root modulo q, i.e. a generator of the the group of units of $\mathbb{Z}[i]/q\mathbb{Z}[i]$, which is cyclic of order $m-1 = q^2-1$. Since γ is a a primitive root modulo q, clearly

$$\gamma^{q^2-1} \equiv 1 \bmod q$$

For the following argument, γ must be such that

$$\gamma^{q^2-1} \not\equiv 1 \bmod q^2$$

If our γ does not satisfy the previous condition, we only need to choose an integer $\lambda \not\equiv 0 \bmod q$ and substitute γ with $\gamma + q\lambda$: indeed,

$$(\gamma + q\lambda)^{q^2-1} \equiv 1 \bmod q$$

and

$$(\gamma + q\lambda)^{q^2-1} \not\equiv 1 \bmod q^2$$

The previous discussion means that we can assume that our primitive root γ satisfies the equation

$$\gamma^{q^2-1} = 1 + \xi q$$

for some integer $\xi \not\equiv 0 \bmod q$, and so

$$\gamma^{q(q^2-1)} = (1 + \xi q)^q = 1 + \xi_1 q^2$$

for some $\xi_1 \not\equiv 0 \bmod q$.
Repeating the argument $h-2$ times, we can find an element $\xi_{h-1} \not\equiv 0 \bmod q$ such that

$$\gamma^{q^{h-1}(q^2-1)} = 1 + \xi_{h-1} q^h$$

Therefore, due to the fact that γ generates $(\mathbb{Z}[i]/q\mathbb{Z}[i])^*$, for every integer $\alpha \not\equiv 0 \bmod q$ we have that

$$\alpha^{q^{h-1}(q^2-1)} \equiv 1 \bmod q^h$$

Now suppose that there is an element ν such that $\nu^{q^{h-1}} \equiv \gamma^s \bmod q^h$ for some s, and such that for every $l < q^{h-1}$ and every t,

$$\nu^l \not\equiv \gamma^t \bmod q^h$$

Consider an element of the form

$$\gamma^j \nu^l$$

where $0 \leq j \leq q^{h-1}(q^2-1) - 1$ and $0 \leq l \leq q^{h-1} - 1$: seen that

$$(\gamma^j \nu^l)^{q^{h-1}(q^2-1)} \equiv 1 \bmod q^h$$

$\gamma^j \nu^l$ is always a unit mod q^h. Moreover, if

$$\gamma^j \nu^l \equiv \gamma^r \nu^t \bmod q^h$$

for a couple $(r,t) \neq (j,l)$ where $0 \leq r \leq q^{h-1}(q^2-1)-1$ and $0 \leq t \leq q^{h-1}-1$, then it must be

$$\gamma^{j-r} \equiv \nu^{t-l} \bmod q^h$$

which is impossible since $0 < t - l < q^{h-1}$, so the elements $\gamma^j \nu^l$ are all different. Since the total number of these elements is equal to the cardinality of $(\mathbb{Z}[i]/q^h\mathbb{Z}[i])^*$, it follows that if $S =< \gamma >$ and $T =< \nu >$ we get

$$Gal(\frac{C_{q^h}}{\mathbb{Q}(i)}) \cong ST$$

So we are only left to show that a suitable ν exists. Consider any element a such that

$$a^{q^{h-1}} \equiv 1 \bmod q^h$$

and

$$a^l \not\equiv 1 \bmod q^h$$

for every $l < q^{h-1}$. From

$$\begin{aligned} a^{q^{h-1}} &\equiv (1 + (a-1))^{q^{h-1}} \bmod q^h \\ &\equiv \sum_{i=0}^{q^{h-1}} \binom{q^{h-1}}{i} (a-1)^i \bmod q^h \end{aligned}$$

we get that

$$\sum_{i=0}^{q^{h-1}} \binom{q^{h-1}}{i} (a-1)^i \equiv 1 \bmod q^h \equiv 1 \bmod q$$

and so $1 + (a-1)^{q^{h-1}} \equiv 1 \bmod q$, i.e.

$$a \equiv 1 \bmod q$$

On the other hand

$$a \not\equiv 1 \bmod q^2$$

because if $a = 1 + \eta q^2$ with $\eta \in \mathbb{Z}[i]$ then

$$\begin{aligned} a^{q^{h-2}} &= (1 + \eta q^2)^{q^{h-2}} \\ &= (1 + q\eta q^2 + \ldots)^{q^{h-3}} \\ &\vdots \\ &= (1 + q\bar{\eta} q^{h-2} + \ldots)^q \\ &= 1 + \tilde{\eta} q^h + \ldots \\ &\equiv 1 \bmod q^h \end{aligned}$$

which is a contradiction since $q^{h-2} < q^{h-1}$. Hence there is an element $\eta \not\equiv 0 \bmod q$ such that

$$a = 1 + \eta q$$

and so from what we have seen before, the powers of γ that could possibly be equal to a are only those of the form

$$\gamma^{\lambda(q^2-1)}$$

for $\lambda \in \{1, \ldots, q-1\}$. Now, choose ν avoiding the powers of γ (which is possible, since we have q^2-1 choices for η and only $q-1$ elements to avoid): we are going to prove that ν respect the required condition.
So let l be the smallest exponent such that

$$\nu^l \equiv \gamma^t \bmod q^h$$

for some $t \in \mathbb{N}$. First of all, we have to remark that l must divide q^{h-1}, since $\nu^{q^{h-1}} \equiv 1 \bmod q$. Then, note that since γ generates $(\mathbb{Z}[i]/q\mathbb{Z}[i])^*$ and $\nu^l \equiv \gamma^t \bmod q$ then t must be divisible by l. Moreover, seen that

$$\begin{aligned} (\gamma^t)^{q^{h-1}} &\equiv (\nu^l)^{q^{h-1}} \bmod q^h \\ &\equiv 1 \bmod q^h \end{aligned}$$

tq^{h-1} must be divisible by $q^{h-1}(q^2-1)$, so we conclude that $t = bl(q^2-1)$ for some $b \in \mathbb{N}$. Finally consider the congruence

$$\left(\nu\gamma^{-b(q^2-1)}\right)^l = \nu^l\gamma^{-bl(q^2-1)} \equiv 1 \bmod q^h$$

If $l < q^{h-1}$, then the equation holds only if

$$\nu\gamma^{-b(q^2-1)} \equiv 1 \bmod q^2$$

(it is enough to use the same argument we used in order to prove that $a \not\equiv 1 \bmod q^2$), but then since $\gamma^{q^2-1} \equiv 1 \bmod q^2$ we get that

$$\nu \equiv 1 \bmod q^2$$

which is a contradiction, thus $l = q^{h-1}$ as we wanted to show. □

2.2.1 Some further details on the fields C_{μ^h}

Note that we can easily obtain other meaningful informations about the fields C_{μ^h}:

- Using the same kind of argument used in Proposition (2.1.2), it is possible to prove that the discriminant of the $\mathbb{Q}(i)$-basis of C_{μ^h} formed by taking the powers of any root of $\psi_h(X)$ is divisible only by $(i+1)$ and μ.
- Moreover, following the argument used in the proof of Theorem (2.1.2) we can see that μ is totally ramified in C_{μ^h} and that the prime ideal $\mathfrak{M}$ lying over μ can be generated by any of the roots of $\psi_h(X)$ (which are then all associated).

- If μ is not real, using Sylow's theorem on the Galois group of $\mathbb{Q}(i) \subset C_{\mu^h}$ we see that there is a cyclic extension $\mathbb{Q}(i) \subset K \subset C_{\mu^h}$ such that $[K : \mathbb{Q}(i)] = m^{h-1}$. Since the degree of the extension is odd, it follows from Proposition (2.1.2) that the discriminant of this field is a power of μ. Moreover, C_μ is the field corresponding to the unique subgroup of $Gal(C_{\mu^h}/\mathbb{Q}(i))$ of order $m-1$, so

$$\mathbb{Q}(i) \subset C_\mu \subset C_{\mu^h}$$

- If $\mu = q$ is real, then in the Galois group of $\mathbb{Q}(i) \subset C_{q^h}$ we can find $q^{h-1}+1$ different groups of order q^{h-1}: for every $h \in T =< \nu >$ the group $< h\gamma^{q^2-1} >$ has order q^{h-1} and then we have to take in account T. All those groups fix a different subextension of C_{q^h} of degree q^{h-1} over $\mathbb{Q}(i)$, and the discriminant of these fields is a power of q. Moreover, as in the previous case C_q is the field corresponding to the unique subgroup of $Gal(C_{q^h}/\mathbb{Q}(i))$ of order $m-1$.

2.3 The division by a power of $(1+i)$

So far we have considered μ-division points for μ odd prime and then we have looked at the division by μ^h, using the detailed description of the μ^h-division polynomial which is available in this case. Now we have to shift our attention to the case of any power of $(1+i)$, and we will need a slightly different approach.

Our starting point is the equation

$$\wp((1+i)u) = \frac{\wp^2(u)-1}{2i\wp(u)} \tag{2.14}$$

which was established in Proposition (1.5.1). Clearly, by iteration, for any $h \in \mathbb{N}$ $\wp((1+i)^h u)$ must be a rational function of $\wp(u)$, so let us set

$$\wp(1+i)^h u = \frac{f_h(x)}{g_h(x)} \qquad x = \wp u$$

where $f_h(x), g_h(x) \in \mathbb{Z}[i][x]$. Since

$$\wp((1+i)^{h+1}u) = \frac{\wp^2((1+i)^h u)-1}{2i\wp((1+i)^h u)}$$

we get by straightforward computation that

$$f_{h+1}(x) = f_h^2(x) - g_h^2(x) \tag{2.15}$$

$$g_{h+1(x)} = 2i f_h(x) g_h(x) \tag{2.16}$$

so, because of the fact that $f_1(x) = x^2 - 1$ and $g_1(x) = 2ix$ these polynomials can be completely determined by recursion.
First of all we are interested in the degree of $f_h(x)$ and $g_h(x)$ (for typographical reasons, we will denote by ∂f_h the degree of $f_h(x)$). We proceed by induction, and we claim that $\partial f_h = \partial g_h + 1$ for every h. In fact, $\partial f_1 = 2$ and $\partial g_1 = 1$; moreover, if we suppose that $\partial f_h = \partial g_h + 1$ then

$$\begin{aligned} \partial g_{h+1} &= \partial f_h + \partial g_h \\ &= 2\partial g_h + 1 \end{aligned}$$

while

$$\begin{aligned} \partial f_{h+1} &= \partial 2 f_h \\ &= 2\partial g_h + 2 \end{aligned}$$

Thus we actually have that for every $h \in \mathbb{N}$

$$\partial f_{h+1} = 2\partial f_h$$

which implies that $f_h(x)$ is of degree 2^h for every h.

Theorem 2.3.1. *Considering the previous notation, let D_h be the splitting field of $f_h(x)$ over $\mathbb{Q}(i)$. Then $\mathbb{Q}(i) \subset D_h$ is an abelian extension of degree 2^{h-2} whose discriminant $\Delta(D_h|\mathbb{Q}(i))$ is divisible only by powers of $(1+i)$.*

Proof. Since

$$f_h(x) = (f_{h-2}(x) - ig_{h-2}(x))^2 (f_{h-2}(x) + ig_{h-2}(x))^2$$

we can consider separately the roots of $f_{h-2}(x) - ig_{h-2}(x) = 0$ and those of $f_{h-2}(x) + ig_{h-2}(x) = 0$. Let us focus first on

$$f_{h-2}(x) - ig_{h-2}(x) = 0 \tag{2.17}$$

If $\bar{x} = \wp(\bar{u})$ is a root of Eq.(2.17), then either $g_{h-2}(\bar{x}) = f_{h-2}(\bar{x}) = 0$ or

$$\wp((1+i)^{h-2}\bar{u}) = \frac{f_{h-2}(\bar{x})}{g_{h-2}(\bar{x})} = i$$

Note that the first option actually leads to a contradiction. In fact, using Eq.(2.15) and Eq.(2.16), we get

$$\begin{aligned} 0 = f_{h-2}(\bar{x}) &= f_{h-3}^2(\bar{x}) - g_{h-3}^2(\bar{x}) \\ 0 = g_{h-2}(\bar{x}) &= 2i f_{h-3}(\bar{x}) g_{h-3}(\bar{x}) \end{aligned}$$

and so $f_{h-3}(\bar{x}) = g_{h-3}(\bar{x}) = 0$. Repeating the argument, we get that

$$\begin{aligned} 0 = f_1(\bar{x}) &= \bar{x}^2 - 1 \\ 0 = g_1(\bar{x}) &= 2i\bar{x} \end{aligned}$$

which is clearly impossible. So the only feasible case is the second one, i.e it must be

$$\wp((1+i)^{h-2}\bar{u}) = i$$

for every root $\bar{x} = \wp(\bar{u})$.
In order to proceed, we have to prove first the following:

Claim 2.3.1. *Consider the fundamental parallelogram of the lattice associated to $\wp$ and a point u inside of it. Then $\wp(u) = i$ if and only if*

$$u \in \{\frac{\omega}{4}(1+3i), \frac{\omega}{4}(3+i)\}$$

Moreover $\wp(u) = -i$ if and only if

$$u \in \{\frac{\omega}{4}(1+i), \frac{\omega}{4}(3+3i)\}$$

This claim can be proved in the following way. First of all (using the periodicity of $\wp$ and the fact that $\wp(-u) = \wp(u)$)

$$\begin{aligned} \wp\left(\frac{\omega}{2(1+i)}\right) &= \wp\left(\frac{\omega(1-i)}{4}\right) \\ &= \wp\left(\frac{\omega(1-i)}{4} + \omega i\right) \\ &= \wp\left(\frac{\omega(1+3i)}{4}\right) \end{aligned}$$

and

$$\begin{aligned} \wp\left(\frac{\omega i}{2(1+i)}\right) &= \wp\left(\frac{\omega(1+i)}{4}\right) \\ &= \wp\left(-\frac{\omega(1+i)}{4} + \omega i + \omega\right) \\ &= \wp\left(\frac{\omega(3+3i)}{4}\right) \end{aligned}$$

Moreover

$$\begin{aligned} \wp\left(\frac{\omega(1+3i)}{4}\right) &= \wp\left(-\frac{\omega(1+3i)}{4}\right) \\ &= \wp\left(-\frac{\omega(1+3i)}{4} + \omega + \omega i\right) \\ &= \wp\left(\frac{\omega(3+i)}{4}\right) \end{aligned}$$

and analogously

$$\wp\left(\frac{\omega(1+i)}{4}\right) = \wp\left(\frac{\omega(3+3i)}{4}\right)$$

Let us set $u_1 = \frac{\omega}{2(1+i)}$ and $u_2 = \frac{\omega i}{2(1+i)}$. Then since

$$1 = \wp(\frac{\omega}{2}) = \frac{\wp^2\left(\frac{\omega}{2(1+i)}\right) - 1}{2i\wp\left(\frac{\omega}{2(1+i)}\right)}$$

we have that $x_1 = \wp(u_1)$ is such that

$$x_1^2 - 2ix_1 - 1 = 0$$

which means that $x_1 = i$ as we wanted to prove. In the same way, we can show that $\wp(u_2) = -i$, so we are left to prove the "only if " part of the statement. Suppose that there is another $\tilde{u}$ in the fundamental parallelogram such that $\wp(\tilde{u}) = i$: recalling that $\wp(u) = \frac{1}{\varphi^2(u)}$ we get that

$$\varphi^2(\tilde{u}) = \varphi^2\left(\frac{\omega(1+3i)}{4}\right) = \varphi^2\left(\frac{\omega(3+i)}{4}\right)$$

Since by Proposition (1.2.4) $\varphi(x) = \varphi(\alpha)$ if and only if there are $m, n \in \mathbb{Z}$ such that $x = (-1)^{m+n}\alpha + m\omega + n\omega i$, if $\varphi(\tilde{u}) = \varphi\left(\frac{\omega(1+3i)}{4}\right)$ then $\tilde{u}$ is outside the fundamental parallelogram contrarily to our assumption. So,

$$\varphi(\tilde{u}) = -\varphi\left(\frac{\omega(1+3i)}{4}\right)$$

but since the argument was general, we also get that

$$\varphi\left(\frac{\omega(3+i)}{4}\right) = -\varphi\left(\frac{\omega(1+3i)}{4}\right)$$

and hence

$$\varphi(\tilde{u}) = \varphi\left(\frac{\omega(3+i)}{4}\right)$$

which leads us to a contradiction exactly as before. Using the same argument for the other set of points, we conclude.

In our contest, this last results means that if $\bar{x} = \wp(\bar{u})$ is a root of Eq.(2.17) then it must be that either

$$(1+i)^{h-2}\bar{u} = \pm\frac{\omega(1+3i)}{4} + m\omega + n\omega i$$

for some $m, n \in \mathbb{Z}$ or

$$(1+i)^{h-2}\bar{u} = \pm\frac{\omega(3+i)}{4} + m\omega + n\omega i$$

so (by direct computation) we can see that

$$\bar{u} = \frac{\xi + \eta i}{(1+i)^{h+1}}\omega$$

where $\xi, \eta \in \mathbb{Z}$, ξ is even and $\eta \equiv \pm 1 \bmod 4$. Note that since $\wp(-u) = \wp(u)$ the previous discussion implies that the roots of Eq.(2.17) are of the form

$$\wp\left(\frac{\xi + \eta i}{(1+i)^{h+1}}\omega\right)$$

where ξ is even and $\eta \equiv 1 \bmod 4$. With the same argument we can also see that the roots of $f_{h-2} + ig_{h-2} = 0$ are of the form

$$\wp\left(\frac{\xi + \eta i}{(1+i)^{h+1}}\omega\right)$$

where $\xi, \eta \in \mathbb{Z}$, η is even and $\xi \equiv 1 \bmod 4$.

Since $\wp(iu) = -\wp(u)$ it is clear that the roots of $f_{h-2}(x) - ig_{h-2}(x) = 0$ and $f_{h-2}(x)+ig_{h-2}(x) = 0$ define the same field extension: thus we can focus our attention on $f_{h-2}(x) + ig_{h-2}(x) = 0$ instead of considering $f_h(x) = 0$. Moreover the equation

$$\wp\left(\frac{\xi + \eta i}{(1+i)^{h}}\omega\right) = \frac{\wp^2\left(\frac{\xi+\eta i}{(1+i)^{h+1}}\omega\right) - 1}{2i\wp\left(\frac{\xi+\eta i}{(1+i)^{h+1}}\omega\right)}$$

implies that $D_h \subsetneq D_{h+1}$ for every $h \in \mathbb{N}$ and therefore

Claim 2.3.2. *It is sufficient to prove the theorem only for h even.*

In fact

- if $[D_h : \mathbb{Q}(i)] = 2^{h-2}$ and $[D_{h-2} : \mathbb{Q}(i)] = 2^{h-4}$ then the degree of D_{h-1} over $\mathbb{Q}(i)$ can only be 2^{h-3}.
- if $\mathbb{Q}(i) \subset D_h$ is an abelian extension then clearly also $\mathbb{Q}(i) \subset D_{h-1}$ is abelian.
- if the discriminant of $\mathbb{Q}(i) \subset D_h$ is divisible only by $(i+1)$ the same must be true for the discriminant of $\mathbb{Q}(i) \subset D_{h-1}$.

In view of this last remark, let us consider the equation

$$f_{2l}(x) + ig_{2l}(x) = 0 \tag{2.18}$$

which is of degree 2^{2l}. Note that actually, due to Eq.(2.14), to solve Eq. (2.18) is equivalent to solve the following chain of quadratic equations:

$$\begin{aligned} y_0 = -i &= \frac{y_1^2 - 1}{2iy_1} \\ y_1 &= \frac{y_2^2 - 1}{2iy_2} \\ \cdots &\quad \cdots\cdots \\ \cdots &\quad \cdots\cdots \\ y_{2l-1} &= \frac{y_{2l}^2 - 1}{2iy_{2l}} \end{aligned}$$

where for every j

$$y_j = \wp\left(\frac{\xi + \eta i}{(1+i)^j}\omega\right)$$

and ξ and η are fixed (and satisfy the previously stated requests): thus in order to prove that $\mathbb{Q}(i) \subset D_{2l+2} = \mathbb{Q}(i)(y_{2l})$ is an extension of degree 2^{2l} we just need to prove that $\mathbb{Q}(i)(y_j) \neq \mathbb{Q}(i)(y_{j+1})$ for every j.
We proceed by induction. Since $y_1 = 1 \pm \sqrt{2}$, $\mathbb{Q}(i)(y_j) \neq \mathbb{Q}(i)$. Now choose $n < 2l$ and consider the extension $\mathbb{Q}(i)(y_n) \subset \mathbb{Q}(i)(y_{n+1})$. If $\mathbb{Q}(i)(y_n) \neq \mathbb{Q}(i)(y_{n+1})$ then this extension must be cyclic of degree 2, and so there must an element $a \in \mathbb{Q}(i)(y_n)$ which is not a square such that

$$\mathbb{Q}(i)(y_{n+1}) = \mathbb{Q}(i)(y_n)(\sqrt{a})$$

and consequently the discriminant of this extension must be divisible by a (we are using again Lemma (2.1.5)). But we know that the field $\mathbb{Q}(i)(y_{n+1})$ is defined by the equation

$$y_{n+1}^2 - 2iy_n y_{n+1} - 1 = 0$$

whose discriminant d_{n+1} is

$$d_{n+1} = -4(y_n^2 - 1) = -8iy_{n+1}y_n$$

so a must divide $-8iy_{n+1}y_n$. Since we can suppose that a is not divisible by 2 ((2) is a square in $\mathbb{Q}(i)$) and since $y_{n+1} \notin \mathbb{Q}(i)(y_n)$ we conclude that if $\mathbb{Q}(i)(y_n) \neq \mathbb{Q}(i)(y_{n+1})$ then $\mathbb{Q}(i)(y_{n+1}) = \mathbb{Q}(i)(y_n)(\sqrt{y_n})$, so *we only need to show that y_n is not a square in $\mathbb{Q}(i)(y_n)(\sqrt{y_n})$.*

If y_n is actually a square in $\mathbb{Q}(i)(y_n)$, then there must be $\alpha, \beta \in \mathbb{Q}(i)(y_{n-1})$ such that $y_n = (\alpha + \beta y_n)^2$ and so

$$\beta^2 y_n^2 + (2\alpha\beta - 1)y_n + \alpha^2 = 0$$

But by inductive hypothesis the equation

$$y_n^2 - 2iy_{n-1}y_n - 1 = 0$$

is irreducible in $\mathbb{Q}(i)(y_{n-1})$ hence we must have

$$\begin{aligned} \frac{\alpha^2}{\beta^2} &= -1 \\ \frac{(2\alpha\beta - 1)}{\beta^2} &= -2iy_{n-1} \end{aligned}$$

If $\alpha = \pm i\beta$ we get that

$$y_{n-1} \pm 1 = \frac{1}{2i\beta^2} = \left(\frac{1}{(1+i)\beta}\right)^2$$

so the norm of $y_{n-1} \pm 1$ must be a square in $\mathbb{Q}(i)(y_{n-2})$. But since the roots of

$$y_{n-1}^2 - 2iy_{n-2}y_{n-1} - 1 = 0$$

are $iy_{n-2} \pm \sqrt{-y_{n-2}^2 - 1}$ the norm of $y_{n-1} \pm 1$ is equal to $2iy_{n-2}$: then we have a contradiction, because by the inductive hypothesis y_{n-2} is not a square in $\mathbb{Q}(i)(y_{n-2})$. Therefore, y_n is not a square, which means that $[D_{2l+2} : \mathbb{Q}(i)] = 2^{2l}$ as we wanted to show.

We still have to prove the extension is abelian and that the discriminant is divisible only by $(1+i)$.
Suppose that the discriminant of $\mathbb{Q}(i) \subset \mathbb{Q}(i)(y_n)$ is a power of $(1+i)$. Since we already know that for every $n < 2l$ the discriminant Δ_n of $\mathbb{Q}(i)(y_n) \subset \mathbb{Q}(i)(y_{n+1})$ divides $4y_n$, it must be a power of $(1+i)$, because the equation

$$y_n(y_n - 2iy_{n-1}) = 1$$

implies that y_n is a unit. But

$$\Delta(\mathbb{Q}(i)(y_{n+1})|\mathbb{Q}(i)) = \Delta(\mathbb{Q}(i)(y_n)|\mathbb{Q}(i))^2\mathbf{N}(\Delta_n)$$

($\mathbf{N}$ is the norm of $\mathbb{Q}(i)(y_n) \subset \mathbb{Q}(i)(y_{n+1})$) so clearly the discriminant $\Delta(\mathbb{Q}(i)(y_{n+1})|\mathbb{Q}(i))$ is a power of $(1+i)$, and by induction we obtain that the discriminant of $\mathbb{Q}(i) \subset D_{2l+2}$ is divisible only by $(1+i)$.

Finally, the extension is clearly a Galois extension, since it has been built by repeatedly adding square roots. It is abelian because the Galois group is isomorphic to the product $\frac{\mathbb{Z}}{2^l\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$. In fact, it is possible to prove (compare with [17], §5) that we can find two odd elements $\gamma, \gamma' \in \mathbb{Z}[i]$ such that all the roots of Eq. (2.18) are of the form

$$x_{\lambda,\lambda'} = \wp\left(\gamma^\lambda \gamma'^{\lambda'} \frac{\omega}{(1+i)^{2m+3}}\right)$$

where $\lambda, \lambda' \in \{0, 1, 2, \ldots, 2^m - 1\}$ (we are not proving this statement, due to its similarity to the cases we treated in Theorem (2.2.2)). Then, if we consider an $\mathbb{Q}(i)$-automorphism σ of D_{2l+2}, we have that

$$\sigma\left(\wp\left(\frac{\omega}{(1+i)^{2m+3}}\right)\right) = \wp\left(\gamma^{\lambda}\gamma'^{\lambda'}\frac{\omega}{(1+i)^{2m+3}}\right)$$

for a couple $(\lambda, \lambda') \in \frac{\mathbb{Z}}{2^l\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$ (the image of a root must be a root). Now choose $s \in N$: since γ^s is odd we get (setting $k = \left(\frac{\omega}{(1+i)^{2m+3}}\right)$ for typographical reasons)

$$\begin{aligned}
\sigma(\varphi^2(\gamma^s k)) &= \sigma(\varphi^2(k))\frac{\sigma\left(P^2_{\gamma^s}(\varphi(k))\right)}{\sigma\left(Q^2_{\gamma^s}(\varphi(k))\right)} \\
&= \varphi^2(\gamma^{\lambda}\gamma'^{\lambda'}k)\frac{P^2_{\gamma^s}(\sigma(\varphi(k)))}{Q^2_{\gamma^s}(\sigma(\varphi(k)))} \\
&= \varphi^2(\gamma^{\lambda}\gamma'^{\lambda'}k)\frac{P^2_{\gamma^s}\left(\varphi(\gamma^{\lambda}\gamma'^{\lambda'}k)\right)}{Q^2_{\gamma^s}(\varphi(\gamma^{\lambda}\gamma'^{\lambda'}k))} \\
&= \varphi^2(\gamma^{\lambda+s}\gamma'^{\lambda'}k)
\end{aligned}$$

and so

$$\begin{aligned}
\sigma\left(\wp\left(\gamma^s\frac{\omega}{(1+i)^{2m+3}}\right)\right) &= \frac{1}{\sigma(\varphi^2(\gamma^s k))} \\
&= \frac{1}{\varphi^2(\gamma^{\lambda+s}\gamma'^{\lambda'}k)} \\
&= \wp\left(\gamma^{\lambda+s}\gamma'^{\lambda'}\frac{\omega}{(1+i)^{2m+3}}\right)
\end{aligned}$$

Of course we can repeat the same argument with γ', obtaining

$$\sigma\left(\wp\left(\gamma^s\gamma'^r\frac{\omega}{(1+i)^{2m+3}}\right)\right) = \wp\left(\gamma^{\lambda+s}\gamma'^{\lambda'+r}\frac{\omega}{(1+i)^{2m+3}}\right)$$

thus σ is completely determined by (λ, λ') and it is clear how to define the isomorphism we were searching for. □

Note that since

$$Gal(D_{2l+2}/\mathbb{Q}(i)) \cong \frac{\mathbb{Z}}{2^l\mathbb{Z}} \times \frac{\mathbb{Z}}{2^l\mathbb{Z}}$$

for every subgroup H of the Galois group there must be two subgroups $H_1, H_2 \subseteq \mathbb{Z}/2^l\mathbb{Z}$ such that $H \cong H_1 \times H_2$. So if H is of order 2^l (thus if it fixes a subextension of degree 2^l) then

$$|H_1| = \frac{2^l}{|H_2|}$$

which obviously implies that

Corollary 2.3.1. *The field D_{2l+2} has 2^l+1 subfields of degree 2^l over $\mathbb{Q}(i)$. The discriminant of all these subextensions is divisible only by $(i+1)$.*

Proposition 2.3.1. *Let $x = \varphi(u)$ and consider $y_x = \wp(u) = \frac{1}{\varphi^2(u)}$. For every $h \geq 2$, x is the polar distance of an $(1+i)^{h+1}$-division point of the lemniscate which is not a $(1+i)^h$-division point if and only if y_x is a solution of the polynomial $f_h(X)$ defined above. Moreover, the polar distances of the $(1+i)^{h+1}$-division points generate the field extension $\mathbb{Q}(i) \subset D_{h+1}$.*

Proof. Clearly, if $x = \varphi(u)$ corresponds to a $(1+i)^{h+1}$-division point of the lemniscate then

$$0 = \varphi((1+i)^{h+1}u)$$

which implies that

$$(1+i)^{h+1}u = r_1\omega + r_2\omega i$$

for some $r_1, r_2 \in \mathbb{Z}$ and consequently

$$y_x = \wp(u) = \wp(\frac{r_1\omega + r_2\omega i}{(1+i)^{h+1}})$$

But then

$$\begin{aligned} \wp\left((1+i)^h u\right) &= \wp\left((1+i)^h \frac{r_1\omega + r_2\omega i}{(1+i)^{h+1}}\right) \\ &= \wp\left(\frac{r_1\omega + r_2\omega i}{(1+i)}\right) \\ &= \wp\left(\frac{(r_1+r_2)\omega + (r_2-r_1)\omega i}{2}\right) \end{aligned}$$

Note that $r_1 + r_2$ must be odd. In fact, if it were even, then $r_2 - r_1$ would be even too, and consequently we would have

$$\wp\left((1+i)^h u\right) = 0$$

contradicting the fact that x is not the polar distance of an $(1+i)^h$-division point.
Hence $r_1 + r_2$ and $r_2 - r_1$ are both odd: this means that $(1+i)^h u$ is a pole of φ and that $\wp((1+i)^h u) = 0$, so

$$f_h(\wp(u)) = 0$$

as we wanted to show.
On the other hand, if $y_x = \wp(u)$ is a root of $f_h(X)$ we can find two numbers $\xi, \eta \in \mathbb{Z}$ such that η is even, $\xi \equiv 1 \bmod 4$ and

$$\wp(u) = \wp\left(\frac{\xi + \eta i}{(1+i)^{h+1}}\omega\right)$$

Hence there must be $r_1, r_2 \in \mathbb{Z}$ such that

$$u = \frac{\xi + \eta i}{(1+i)^{h+1}}\omega + r_1\omega + r_2\omega i$$

and therefore

$$\varphi((1+i)^{h+1}u) = \varphi\left(\xi\omega + \eta i\omega + r_1(1+i)^{h+1}\omega + r_2(1+i)^{h+1}\omega i\right) = 0$$

Finally,

$$(1+i)^h u = \frac{\xi + \eta i}{(1+i)}\omega + r_1(1+i)^h\omega + r_2(1+i)^{h+1}\omega i$$

so

$$\varphi((1+i)^h u) \quad = \quad \varphi\left(\frac{(\xi+\eta)\omega}{2} + \frac{(\xi-\eta)\omega i}{2} + r_1(1+i)^h\omega + r_2(1+i)^{h+1}\omega i\right)$$

which means that $(1+i)^h u$ is a pole because $\xi - \eta$ and $\xi + \eta$ are both odd (we are using Proposition (1.2.3)), thus $\wp(u)$ is not the polar distance of an $(1+i)^h$-division point.
Now we are left to prove that the polar distances of the $(1+i)^{h+1}$-division points generate the field extension $\mathbb{Q}(i) \subset D_{h+1}$. Let $x = \varphi(u)$ be the polar distance of one of the division points and let $y_x = \wp(u) = \frac{1}{x^2}$ be the corresponding root of $f_h(X)$. In Theorem (2.3.1) we saw that $y_x \in D_h$, and that $D_{h+1} = D_h(\sqrt{y_x})$, hence

$$x = \frac{1}{\sqrt{y_x}} \in D_{h+1}$$

Moreover, since $x^2 \in D_h$ and $x \notin D_h$ (otherwise $\sqrt{y_x} \in D_h$, which is absurd) we get that $[D_h(x) : D_h] = 2 = [D_{h+1} : D_h]$: their intersection is not empty (it contains x) so we get that $D_h(x) = D_{h+1}$ as we wanted to show. □

In Theorem (2.3.1), we already saw that the discriminant of the fields D_h is divisible only by $(1+i)$, and thus $(1+i)$ is the only ramified prime. Moreover, it holds that

Proposition 2.3.2. *Consider all the notations exploited in the proof of Theorem (2.3.1). For every $h \geq 1$, $(1+i)$ is totally ramified in D_{h+2}. Moreover, the prime $\mathfrak{P}$ of D_h lying over $(1+i)$ can be generated by the element*

$$\tau_h = \frac{2}{y_h - y_{h-1}}$$

Proof. Since $\Delta(D_{h+2}|\mathbb{Q}(i))$ is divisible only by $(1+i)$, and since no nontrivial extension of $\mathbb{Q}(i)$ can have its discriminant equal to a unit, $(1+i)$ must be equal to the 2^h-th power of a prime $\mathfrak{P}$ of D_{h+2}.
For every $n \leq h$ let us consider

$$\tau_n = \frac{2}{y_n - y_{n-1}} \in k(y_n)$$

Since y_n is a root of

$$x^2 - 2iy_{n-1}x - 1 = 0$$

the $\mathbb{Q}(i)(y_{n-1})$-automorphism of $D_{n+2} = \mathbb{Q}(i)(y_n)$ different from the identity sends y_n in $2iy_{n-1} - y_n$ and consequently

$$\tau_n \mapsto \tau_n' = \frac{2}{2iy_{n-1} - y_n - y_{n-1}}$$

Using the fact that

$$y_j - y_{j-1} = \frac{(2i-1)y_j^2 + 1}{2iy_n}$$

and

$$2iy_j y_{j-1} = y_j^2 - 1$$

we can see that

$$\begin{aligned} \tau_n + \tau_n' &= \frac{-2(1+i)}{y_{n-1} - y_{n-2}} \\ \tau_n \tau_n' &= \frac{-i}{y_{n-1}} \cdot \frac{2}{y_{n-1} - y_{n-2}} \end{aligned}$$

We have already seen that the y_j's are units: hence, τ_n is an integer if $\tau_{n-1} = \frac{2}{y_{n-1} - y_{n-2}}$ is an integer. Then by induction we only need to prove that

$$\tau_1 = \frac{2}{y_1 - y_0} = \frac{2}{y_1 + i}$$

is an integer: this can be done by simply observing that the trace of τ_1 is equal to $-2i$ and that its norm is -$(1+i)$. Since

$$\begin{aligned} \mathbf{N}_{\mathbb{Q}(i)(y_n)|\mathbb{Q}(i)}(\tau_n) &= \mathbf{N}_{\mathbb{Q}(i)(y_{n-1})|\mathbb{Q}(i)}\left(\mathbf{N}_{\mathbb{Q}(i)(y_n)|\mathbb{Q}(i)(y_{n-1})}(\tau_n)\right) \\ &= \mathbf{N}_{\mathbb{Q}(i)(y_{n-1})|\mathbb{Q}(i)}\left(\frac{-i}{y_{n-1}} \cdot \frac{2}{y_{n-1} - y_{n-2}}\right) \\ &= \epsilon_n \mathbf{N}_{\mathbb{Q}(i)(y_{n-1})|\mathbb{Q}(i)}(\tau_{n-1}) \end{aligned}$$

where ϵ_n is a unit, so by induction, we conclude that

$$\mathbf{N}_{\mathbb{Q}(i)(y_n)|\mathbb{Q}(i)}(\tau_n) = \epsilon N_{\mathbb{Q}(i)(y_1)(\tau_1)} = -\epsilon(1+i)$$

and that

$$(\tau_n)^{2^n} = (1+i)$$

as ideals. Consequently the same holds also for $n = h$, so we get

$$(\tau_h)^{2^h} = (1+i)$$

as we wanted to prove. □

2.4 The case of the division of the lemniscate by a composite number

In previous sections, we have described the extensions that we can obtain by choosing any prime $p \in \mathbb{Z}[i]$ and adding to $\mathbb{Q}(i)$ the polar distances of the p^h-division points ($h \in \mathbb{N}$). So a natural question is to ask what happens when instead of a prime we are considering a composite number $\lambda \in Z[i]$. Also in this case, in complete analogy with what we have done before, let us define C_λ as the field obtained by adding to $\mathbb{Q}(i)$ the polar distances of the λ-division points. Unluckily, we are not able to give a satisfying description of the minimum polynomial of the polar distances of the λ-division points. Nevertheless, we have at hand the following result

Theorem 2.4.1. *If the prime factorization of $\lambda \in \mathbb{Q}(i)$ is $\lambda = p_1^{h_1} \dots p_n^{h_n}$ where $p_1, \dots, p_n$ are pairwise different primes, then the field C_λ is contained in the composite field*

$$C_{p_1^{h_1}} C_{p_2^{h_2}} \dots C_{p_n^{h_n}}$$

where if p_j is equal to $(1+i)$ for some j we are denoting by $C_{p_j^{h_j}}$ the field D_h, and we are setting conventionally $D_1 = D_2 = \mathbb{Q}(i)$.

Proof. We will proceed in the following way:

Step 1 : the theorem holds for $\lambda = p_1 p_2$

Step 2 : the theorem holds for $\lambda = p_1^h p_2$ for every h (and hence for $\lambda = p_1 p_2^h$ for every h due to the symmetry of the argument).

Step 3 : the theorem holds for $\lambda = p_1^h p_2^l$ for every h, l.

Step 4 : the theorem holds in general.

Step 1 : in order to prove that $C_\lambda \subseteq C_{p_1} C_{p_2}$, it is enough to show that $\varphi(\rho\frac{\omega}{\lambda}) \in C_{p_1} C_{p_2}$ for all $\rho \in Z[i]$. Note that if ρ is divisible by λ, then $\varphi(\rho\frac{\omega}{\lambda}) = 0 \in C_{p_1} C_{p_2}$, and if $\rho = cp_1$ where c is coprime with p_2,

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{p_2}) \in C_{p_2} \subseteq C_{p_1} C_{p_2}$$

(and we can repeat the argument for $\rho = cp_2$) so actually we only need to consider the elements coprime with λ; moreover, using the periodicity of $\varphi(u)$, we can restrict ourselves to the $\phi(\lambda)$ invertible elements of $\frac{\mathbb{Z}[i]}{\lambda\mathbb{Z}[i]}$. At this point, let $\zeta \in \left(\frac{\mathbb{Z}[i]}{\lambda\mathbb{Z}[i]}\right)^*$. Suppose that p_1 and p_2 are both different from $(1+i)$. Due to Bézout's identity, we can represent ζ as

$$\zeta = \eta p_1 + \xi p_2$$

where

$$\eta \in \left(\frac{\mathbb{Z}[i]}{p_2\mathbb{Z}[i]}\right)^* \quad \text{and } \xi \in \left(\frac{\mathbb{Z}[i]}{p_1\mathbb{Z}[i]}\right)^*$$

Then, if we set

$$w = \frac{\zeta\omega}{\lambda}, \quad u = \frac{\xi\omega}{p_1}, \quad v = \frac{\eta\omega}{p_2}$$

we obviously get, using the Corollary (1.1.1)

$$\varphi(w) = \varphi(\frac{\eta p_1 + \xi p_2}{p_1 p_2}\omega) = \varphi(u+v) = \frac{\varphi(u)f(v)F(v) + \varphi(v)f(u)F(u)}{1+\varphi^2(u)\varphi^2(v)}$$

We have seen before (in the proof of Theorem (2.1.2)) that when p_1 is prime $f(u)F(u) \sim (i+1) \in C_{p_1}$ (and so we also have $f(v)F(v) \sim (i+1) \in C_{p_2}$): hence in this case $\varphi(w)$ is equal to a rational expression of elements of C_{p_1} and C_{p_2}, thus $\varphi(w) \in C_{p_1}C_{p_2}$, i.e $C_\lambda \subseteq C_{p_1}C_{p_2}$.
If at the contrary $p_2 = (1+i)$, we simply observe that we always have

$$\varphi\left((1+i)p_1 u\right) = \frac{(1+i)\varphi\left(p_1 u\right)}{f\left(p_1 u\right) F\left(p_1 u\right)}$$

so the $(i+1)p_1$-division points are exactly the p_1-division points, and thus they all belong to C_{p_1}.
Step 2 : here we proceed by induction on the exponent h. We have proved the case $h = 1$ in the previous step, so we only need to prove the claim for $n+1$ supposing it holds for n. So let $\lambda = p_1^{n+1}p_2$. As before, we only need to consider the elements coprime with λ: in fact, if ρ is a multiple of λ, $\varphi(\rho\frac{\omega}{\lambda}) = 0 \in C_{p_1^{n+1}}C_{p_2}$; if $\rho = cp_2 \not\equiv 0 \mod \lambda$ then

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{p_1^{n+1}}) \in C_{p_1^{n+1}} \subseteq C_{p_1^{n+1}}C_{p_2}$$

and finally if $\rho = cp_1$ then

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{p_1^n p_2}) \in C_{p_1^n}C_{p_2}$$

by induction, which implies that $\varphi(\rho\frac{\omega}{\lambda}) \in C_{p_1^{n+1}}C_{p_2}$ since $C_{p_1^n} \subseteq C_{p_1^{n+1}}$. If p_1 is odd, using the same argument as before we can conclude if we are able

to prove that for every $\xi \in \left(\frac{\mathbb{Z}[i]}{p_1^{n+1}\mathbb{Z}[i]}\right)^*$,

$$f(\xi\frac{\omega}{p_1^{n+1}})F(\xi\frac{\omega}{p_1^{n+1}}) \sim (i+1) \quad \text{in } C_{p_1^{n+1}}$$

But this can easily be done by copying the argument used in the proof of Theorem (2.1.2), since as we have remarked previously in Subsection (2.2.1) p_1 is totally ramified in $C_{p_1^{n+1}}$, and it is equal to the product of all the roots of the p_1^{n+1}-division, being the constant term of the polynomial ψ_{n+1}.
If $p_1 = (1+i)$ we have to prove directly that

$$f(\xi\frac{\omega}{(1+i)^{n+1}})F(\xi\frac{\omega}{(1+1)^{n+1}}) \in D_{n+1}$$

Since ξ is coprime with $(1+i)$, we get that $\xi = a+ib$ where $a, b \in \mathbb{Z}$ and $a+b$ is odd so we can suppose that b is even and a is odd, so that $x = \varphi(\xi\frac{\omega}{(1+i)^{n+1}})$ is the polar distance of one of the $(1+i)^{n+1}$-division points. Hence $x \in D_{n+1}$ and

$$y_x = \wp\left(\xi\frac{\omega}{(1+i)^{n+1}}\right) \in D_n$$

We know that D_{n+1} can be generated by adding to D_n the roots α, β of the polynomial $X^2 - 2iy_xX - 1$. Let us set $\alpha = iy_x + \sqrt{1-y_x^2}$: then $\alpha x^2 \in D_{n+1}$, but

$$\begin{aligned}
\alpha x^2 &= x^2\frac{i}{x^2} + \sqrt{x^4\left(1-\frac{1}{x^4}\right)} \\
&= i + i\sqrt{1-x^4} \\
&= i + if(\xi\frac{\omega}{(1+i)^{n+1}})F(\xi\frac{\omega}{(1+1)^{n+1}})
\end{aligned}$$

so we are done, and we can conclude as in the other case.
Step 3 : Since we have proved that the statement holds for $\lambda = p_1^h p_2$ for every h, and for $\lambda = p_1 p_2^l$ for every l, the idea here is use the induction for $\mathbb{N} \times \mathbb{N}$. We are proceeding in this way: our claim is
"if a couple of exponents (h,l) is such that the statement holds for every couple (n,m) where $(n,m) < (h,l)$ according to the reverse lexicographic order*, then the statement holds for (h,l)".*
Note that (if we are able to prove the claim) we really cover $\mathbb{N} \times \mathbb{N}$; in fact it is easy to see that representing $\mathbb{N} \times \mathbb{N}$ using the first quadrant of the cartesian coordinate system, keeping in mind that due to the symmetry of the problem we only need to consider the part of the quadrant above the diagonal (because if we prove something for (h,l) it also holds for (l,h)), if we ideally choose at each step the point of integer coordinates that is less distant from the origin *according to the reverse lexicographic order* we really take into account all the points of $\mathbb{N} \times \mathbb{N}$.

We first need to prove that the claim holds for $(2,2)$: if $\rho \in \mathbb{Z}[i]$ is not coprime with $\lambda = p_1^2 p_2^2$, it could mean that

- ρ is a multiple of λ, so we conclude as before.
- $\rho = cp_1$ where c is coprime with $p_1 p_2$ hence

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{p_1 p_2^2}) \in C_{p_1} C_{p_2^2} \subseteq C_{p_1^2} C_{p_2^2}$$

  using **Step 2** (and the same argument applies in case $\rho = cp_2$ where c is coprime with $p_1 p_2$)

- $\rho = cp_1 p_2$ where c is coprime with $p_1 p_2$ hence

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{p_1 p_2}) \in C_{p_1} C_{p_2} \subseteq C_{p_1^2} C_{p_2^2}$$

  using **Step 1**

- $\rho = cp_1^2$ where c is coprime with p_2 hence

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{p_2^2}) \in C_{p_2^2} \subseteq C_{p_1^2} C_{p_2^2}$$

  (and the same argument applies in case $\rho = cp_2^2$ where c is coprime with p_1)

- $\rho = cp_1 p_2^2$ where c is coprime with p_1 hence

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{p_1}) \in C_{p_1} \subseteq C_{p_1^2} C_{p_2^2}$$

  (and the same argument applies in case $\rho = cp_2 p_1^2$ where c is coprime with p_2)

So we can restrict ourselves to the elements ρ which are coprime with λ, and in this case we can follow the argument used before, and we can conclude directly since we know from the proof of the previous step that for every prime p, every natural integer n and for every $\xi \in \left(\frac{\mathbb{Z}[i]}{p^n\mathbb{Z}[i]}\right)^*$,

$$f(\xi\frac{\omega}{p^n})F(\xi\frac{\omega}{p^n}) \in C_{p^n}$$

Now we are ready to prove the claim. It is now evident that the only thing that we have to prove is that we can restrict ourselves to the case in which the element ρ is coprime with $\lambda = {p_1}^h {p_2}^l$. Thus, let us suppose that ρ is not coprime:

- if ρ is a multiple of λ then $\varphi(\rho\frac{\omega}{\lambda}) = 0 \in C_{{p_1}^h} C_{p_2^l}$.

- if $\rho = cp_2^r p_1^s$ for some $s < h, r < l$ (where at least one between s and r is different from 0) and c is coprime with $p_1 p_2$, we get

$$\varphi(\rho\frac{\omega}{\lambda}) = \varphi(c\frac{\omega}{{p_1}^{h-s}{p_2}^{l-r}})$$

and by the inductive hypothesis (since $(h-s, l-r) < (h, l)$) this last element belongs to $C_{{p_1}^{h-s}} C_{{p_2}^{l-r}}$, which is contained in $C_{{p_1}^h} C_{p_2^l}$.

Therefore also **Step 3** is proven.
Step 4 : here we have to follow a slightly different path. There are two substeps that need to be made, i.e we must prove the following claims:

a) Let $\mathcal{A}_n$ be the set of elements λ in $\mathbb{Z}[i]$ such that the prime factorization of λ involves less than $n+1$ primes. If the statement holds for all the elements in $\mathcal{A}_n$, choosing $\lambda \in \mathcal{A}_n$ and a prime p which does not divide λ then the statement holds for λp.

b) If the statement holds for all the elements in $\mathcal{A}_n$, choosing $\lambda \in \mathcal{A}_n$ and a prime p which does not divide λ then the statement holds for λp^h for every $h \in \mathbb{N}$.

Note that since the case $n = 1$ of both claims has been proved earlier, (**Step 1** and **Step 2**), and since trough *a*) and *b*) we basically show that if the statement holds for $\mathcal{A}_n$ then it holds for $\mathcal{A}_{n+1}$, the two substeps are enough to conclude with the proof of this theorem.
Let us start with *a*). First of all, as usual, we have to show that we can restrict ourselves to the elements coprime with λp. If ρ is not coprime with λp, then the following cases can occur:

- If ρ is a multiple of λp we conclude as in the previous cases.
- if $\rho = cp$ for some integer c, then if $\lambda = {p_1}^{h_1}{p_2}^{h_2}\dots{p_n}^{h_n}$

$$\varphi(\rho\frac{\omega}{\lambda p}) = \varphi(c\frac{\omega}{\lambda}) \in C_{p_1^{h_1}} C_{p_2^{h_2}} \dots C_{p_n^{h_n}}$$

since we are supposing that the statement holds for $\mathcal{A}_n$, and this last field is obviously a subfield of $C_{p_1^{h_1}} C_{p_2^{h_2}} \dots C_{p_n^{h_n}} C_p$.

- If ρ is not divisible by p, there must be an element $c \in Z[i]$ such that $\lambda = cd$ and $\rho = ce$. Hence

$$\varphi(\rho\frac{\omega}{\lambda p}) = \varphi(e\frac{\omega}{dp})$$

and now e is coprime with dp. Moreover, the primes dividing d are some of the primes dividing λ, so if we prove that the statement holds for dp, then it holds for λp, since we have $C_{s^h} \subseteq C_{s^{h+1}}$ for every prime s. Furthermore, due to the previous discussion, the fact that $d \in \mathcal{A}_n$ shows that we actually can restrict ourselves to the cases in which ρ is coprime with λ.

At this point, we need to use the following general property:

Lemma 2.4.1. *Let $\mu \in \mathbb{Z}[i]$ be odd. Then $f(\frac{\omega}{\mu})F(\frac{\omega}{\mu}) \in C_\mu$.*

Proof. Since $\mu - 1$ is even, by Proposition (1.5.2)

$$\varphi((\mu-1)u) = \varphi(u)f(u)F(u)T$$

where T is a rational function of $\varphi(u)^4$. Moreover,

$$\varphi((\mu-1)\frac{\omega}{\mu}) = \varphi(\omega - \frac{\omega}{\mu}) = \varphi(\frac{\omega}{\mu})$$

thus

$$\varphi(\frac{\omega}{\mu}) = \varphi(\frac{\omega}{\mu})f(\frac{\omega}{\mu})F(\frac{\omega}{\mu})T$$

and finally

$$f(\frac{\omega}{\mu})F(\frac{\omega}{\mu}) = \frac{1}{T} \in C_\mu$$

□

This result gives use the possibility to repeat the previous argument (because the polar distance of every μ-division point is a rational expression of $\varphi(\frac{\omega}{\mu})$). In fact, if $(i+1)$ is the maximum power of $(1+i)$ which divides λp it holds as before that the λp-division points are exactly the $\frac{\lambda p}{(1+i)}$-division points. If on the contrary there is an $h \geq 2$ such that $(1+i)^h$ is the maximum power of $(1+i)$ dividing λp , we only have to make sure that we consider λp as the product of $\frac{\lambda p}{(1+i)^h}$ and $(1+i)^h$, which is always possible. Finally, we should prove *b*), and we will do it by induction. In point *a*) we proved the case $h = 1$, now we should show that the statement holds for $h+1$ if we suppose it holds for h. Clearly this is equivalent (using what we have seen in the previous steps and in *a*)) to prove that we can always restrict ourselves to a coprime element also in this case. In fact, if ρ is not coprime with λp^{h+1}, then the following cases can occur:

- If ρ is a multiple of λp we conclude as in the previous cases.
- if $\rho = cp^s$ for some integer c, and some $s \leq h+1$ then since $\lambda = {p_1}^{h_1}{p_2}^{h_2}\dots{p_n}^{h_n}$

  $$\varphi(\rho\frac{\omega}{\lambda p^{h+1}}) = \varphi(c\frac{\omega}{\lambda}p^{h+1-s}) \in C_{{p_1}^{h_1}}C_{{p_2}^{h_2}}\dots C_{{p_n}^{h_n}}C_{p^{h+1-s}}$$

  by the inductive hypothesis, and since the last field is a subfield of $C_{{p_1}^{h_1}}C_{{p_2}^{h_2}}\dots C_{{p_n}^{h_n}}C_{p^{h+1}}$, we conclude.

- If ρ is not divisible by p, there must be an element $c \in Z[i]$ such that $\lambda = cd$ and $\rho = ce$. Hence

$$\varphi(\rho\frac{\omega}{\lambda p^{h+1}}) = \varphi(e\frac{\omega}{dp^{h+1}})$$

and repeating the argument used in a) we can conclude.

□

2.5 Prime ideals decomposition in C_{μ^h}

A crucial information that we need in order to fully understand the fields that we have considered so far is the following:

Proposition 2.5.1. *Let $\mu \in \mathbb{Z}[i]$ be any prime, and $h \in \mathbb{N}$. If μ is odd and m is its norm, set $M = \varphi(\mu^h) = m^{h-1}(m-1)$ and let $K = C_{\mu^h}$. If $\mu = (1+i)$ set $M = 2^{h-2}$ and $K = D_h$. Then:*

i) μ is totally ramified in K. Let $\mathfrak{M}$ be the prime ideal $\left(\varphi(\frac{\omega}{\mu^h})\right)$ if μ is odd, and the ideal generated by $\frac{2}{y_{h-2}-y_{h-3}}$ if $\mu = (i+1)$. Then we have that

$$\mu\mathcal{O}_K = \mathfrak{M}^M$$

ii) If $\nu \in \mathbb{Z}[i]$ is an odd prime different from μ, and f is the smallest integer such that $\nu^f \equiv 1 \ mod\ \mu^h$, then

$$v\mathcal{O}_K = \mathfrak{N}_1\mathfrak{N}_2\dots\mathfrak{N}_g$$

where $gf = M$ and the $\mathfrak{N}_j$'s are pairwise different primes.

iii) If $(i+1) \neq \mu$, let g be such that $gf = \frac{M}{4}$ where f is the smallest integer such that $(i+1)^f \equiv i^\epsilon \ mod\ \mu^h$ for some $\epsilon \in \{0,1,2,3\}$. Then

$$(i+1)\mathcal{O}_K = (\mathfrak{P}_1\mathfrak{P}_2\dots\mathfrak{P}_g)^4$$

Proof. Point i) was already discussed for μ odd in Subsection (2.2.1), and and for $(i+1)$ in Proposition (2.3.2), so we only have to focus on *ii*) and *iii*).
Consider any odd prime $\nu \in \mathbb{Z}[i]$ different from μ, and denote by n its norm over $\mathbb{Q}(i)$. If $x = \varphi(u)$ is one root of the μ^h-division polynomial, then clearly also $x' = \varphi(\nu u)$ is a root. Since we know that

$$x' = \varphi(\mu u) = \varphi(u)\frac{P_\nu(x)}{Q_\nu(x)}$$

using the description of $P_\nu(x)$ and $Q_\nu(x)$ given in Proposition (1.5.3) we get that we can find two suitable integers γ and γ' such that

$$x' = x\frac{x^{n-1} + \nu\gamma}{\nu\gamma' + 1}$$

This directly implies that $x' \equiv x^n \bmod \nu$. Note that we can't find another root x'' such that $x'' \equiv x^n \bmod \nu$, because then $x' - x''$ would be divisible by ν, contradicting the fact that since x', x'' are roots of the μ^h- division polynomial they are associated and $x' - x''$ belongs only to the primes dividing μ. At this point, let us consider the $\mathbb{Q}(i)$-automorphism of K mapping x to x' (we will denote it by σ). If we write σ_l to denote the composition

$$\underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{l-times}$$

we immediately have that

$$\sigma_l(x) \equiv x^{n^l} \bmod \nu$$

hence if r is the order of σ in $Gal(K/\mathbb{Q}(i))$ it holds that

$$x^{n^r} \equiv x \bmod \nu$$

Let us remark that r is the smallest possible exponent for this congruence, since as we have seen before $x'' \not\equiv x^n \bmod \nu$ for every root $x'' \neq x'$.
Now consider an integer $\theta \in \mathcal{O}_K$. Since it can be represented as

$$\theta = b_0 + b_1 x + \ldots + b_{M-1}x^{M-1}$$

where the b_j's are all gaussian integers, it holds that

$$\theta^{n^r} \equiv \theta \bmod \nu$$

In fact, since the binomial coefficients $\binom{n^r}{i}$ where $0 < i < n^r$ are all divisible by n (which is a rational prime being the norm of a prime) and $n = \nu\bar{\nu}$ we have that

$$\begin{aligned}
\theta^{n^r} &\equiv b_0^{n^r} + (b_1 x + \ldots + b_{M-1}x^{M-1})^{n^r} \bmod \nu \\
&\equiv b_0^{n^r} + b_1^{n^r}x^{n^r} + (b_2 x^2 \ldots + b_{M-1}x^{M-1})^{n^r} \bmod \nu \\
&\vdots \\
&\equiv b_0^{n^r} + b_1^{n^r}x^{n^r} + \ldots + b_{M-1}^{n^r}x^{(M-1)n^r} \bmod \nu
\end{aligned}$$

But since n is the norm of ν, for every integer $b \in Z[i]$ it holds that $b^n \equiv b \bmod \nu$, and as we have already seen $x^{n^r} \equiv x \bmod \nu$, so

$$\theta^{n^r} \equiv \theta \bmod \nu$$

as wanted to show. Then of course the norm of any prime ideal $\mathfrak{N}$ lying over ν must be a power of n of exponent $f \leq r$ (f is the relative degree of $\mathfrak{N}$ over ν). Note that the equivalence

$$x^{n^f} \equiv x \bmod \mathfrak{N}$$

cannot hold for $f < r$. In fact, since we are in a Galois extension, this would mean that the same equivalence holds for all the other primes lying over ν, and we would obtain that

$$x^{n^f} \equiv x \bmod \nu$$

but this contradicts the fact that r is the smallest exponent such that $x^{n^r} \equiv x \bmod \nu$. Hence $f = r$, but we still have to show that $\nu^f \equiv 1 \bmod \mu^h$. We know that $\sigma(\varphi(u)) = \varphi(\nu u)$, so

$$\sigma_r(\varphi(u)) = \varphi(\nu^r u)$$

which implies that

$$\varphi(\nu^r u) = \varphi(u)$$

for every u such that $\varphi(u)$ is a root of the μ^h-division polynomial. This means that actually

$$\varphi(\nu^r \frac{\omega}{\mu^h}) = \varphi(\frac{\omega}{\mu^h})$$

thus we can find $c, d \in \mathbb{Z}$ such

$$\nu^r \frac{\omega}{\mu^h} = \frac{\omega}{\mu^h} + c\omega + d\omega i$$

and finally

$$\nu^r \equiv 1 \bmod \mu^h$$

Therefore the proof of point *ii*) can be completed by noticing that since r is the order of σ, it is the smallest number which can satisfy the last congruence, and by recalling that ν does not ramify in K since it does not divide the discriminant.
iii) As usual, denote by $x = \varphi(u)$ a root of the μ^h-division polynomial. In order to analyze the decomposition of $(i+1)$ in C_{μ^h}, in analogy with what we have done in the proof of Theorem (2.1.2) let us consider K', the unique subfield of C_{μ^h} of index 4. As we have seen there, if we set $a = (1-2i)$ then the powers of the element

$$y = \frac{x^4 - a}{4}$$

form an integral basis of K' (recall that in the proof of Theorem (2.4.1) we have seen that $f(u)F(u) \sim (i+1)$ in C_{μ^h}).
Now, let us consider

$$x' = \varphi((i+1)u) = \frac{(i+1)\varphi(u)}{f(u)F(u)}$$

which is clearly another root of the μ^h-division polynomial, and define

$$y' = \frac{x'^4 - a}{4}$$

Since

$$\begin{aligned} y' &= -\frac{x^4}{(x^4-1)^2} - \frac{a}{4} \\ &= -\frac{(4y+a) + a(2y-i)^2}{4(2y-i)^2} \\ &= \frac{-ay^2 - (1-ia)y}{(2y-i)^2} \end{aligned}$$

we get that

$$y' = \frac{-(1-2i)y^2 + (1+1)y}{(2y-i)^2} \equiv y^2 \bmod (i+1)$$

Furthermore, suppose that there is another root x'' of the μ^h-division polynomial such that $y'' = \frac{x''^2 - a}{4}$ satisfies the last congruence: then

$$\frac{x'^4 - x''^4}{4} = y' - y'' \equiv 0 \bmod (i+1)$$

which is absurd since x'^4 and x''^4 are associated and $x'^4 - x''^4 \in \mu\mathcal{O}_K$. At this point we can clearly repeat the argument used in the previous point, and we get that if f is the smallest integer such that $(1+i)^{4f} \equiv 1 \bmod \mu^h$, then

$$(1+i)\mathcal{O}_{K'} = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_g$$

where $gf = \frac{M}{4}$ and the $\mathfrak{p}_j$'s are pairwise different prime ideals. But in the proof of Theorem (2.1.2) we saw that K' is the inertia field of $(i+1)$: so we can conclude directly that

$$(1+i)\mathcal{O}_K = (\mathfrak{P}_1\mathfrak{P}_2\ldots\mathfrak{P}_g)^4$$

where the $\mathfrak{P}_j$'s are pairwise different prime ideals. □

2.6 The definition and the statement

With the work we have done so far, we have shown the existence of a large number of different field extensions of $\mathbb{Q}(i)$ linked to the division points of the lemniscate. For future reference, let us enlist the results here.

Lemma 2.6.1. *Let $\mu \in \mathbb{Z}[i]$ be an odd prime, m its norm.*

i) If p^h is the maximum power of the odd prime p dividing $m-1$, for every $\lambda \leq h$ we can find a subfield $C \subseteq C_\mu$ such that the discriminant of C over $\mathbb{Q}(i)$ is equal to $\mu^{p^\lambda - 1}$ and $\mathbb{Q}(i) \subset C$ is a cyclic extension of degree p^λ.

ii) If 2^h is the maximum power of 2 dividing $\frac{1}{4}(m-1)$, for every $\lambda \leq h$ there exist a cyclic extension $\mathbb{Q}(i) \subset C \subset C_\mu$ such that $[C : \mathbb{Q}(i) = 2^\lambda$ and the discriminant of C over $\mathbb{Q}(i)$ is $\mu^{2^\lambda - 1}$. Moreover, if $\lambda \in \{h+1, h+2\}$ there is a cyclic extension of $\mathbb{Q}(i)$ of degree 2^λ such that the discriminant is equal to $(1+i)^{2^\lambda}\mu^{2^\lambda - 1}$.

Moreover

iii) If $q \in \mathbb{Z}$ is a prime that splits in $\mathbb{Q}(i)$ and $\pi \in \mathbb{Z}[i]$ is a prime dividing q, then for every $\lambda \in \mathbb{N}$ there is a cyclic extension of $\mathbb{Q}(i)$ of degree q^λ such that its discriminant over $\mathbb{Q}(i)$ is a power of π.

iv) If $q \in \mathbb{Z}$ is a prime which is inert in $\mathbb{Q}(i)$, then for every $\lambda \in \mathbb{N}$ we can find $q^\lambda + 1$ cyclic extensions of $\mathbb{Q}(i)$ with discriminant over $\mathbb{Q}(i)$ equal to a power of q.

v) For every $\lambda \in \mathbb{N}$, we can find $2^\lambda + 1$ cyclic extensions of $\mathbb{Q}(i)$ of degree 2^λ whose discriminant is a power of $(1+i)$.

Note that *i)* and *ii)* were proven in Theorem (2.1.2), *iii)* and *iv)* in Subsection (2.2.1), and finally *v)* was proven in Corollary (2.3.1).

Actually, we can prove that the fields listed in *i)* and *ii)* of Lemma (2.6.1) are unique:

Lemma 2.6.2. *Let $\mu \in Q(i)$ be a prime number, m its norm, p^h the the highest power of the odd prime number $p \in \mathbb{Z}$ dividing $m-1$.*
Let $\mathbb{Q}(i) \subseteq \Gamma$ be a cyclic extension with $[\Gamma : \mathbb{Q}(i)] = p^{h'}$ for some $h' \leq h$, and such that its discriminant is not divisible by any prime factor except for μ. Then Γ coincides with one of the elementary lemniscate fields we described in Lemma (2.6.1).

Proof. Let's suppose that Γ is different from the elementary lemniscate field C with same degree that we find in Lemma (2.6.1). Then we can consider the composite field $K = \Gamma C$, and note that

$$p^{h'} \leq [K : \mathbb{Q}(i)] \leq [\Gamma : \mathbb{Q}(i)][C : \mathbb{Q}(i)] = p^{2h'}$$

Hence there must be an n such that $h' \leq n \leq 2h'$ and $[K : \mathbb{Q}(i)] = p^n$. Suppose that k is a subfield of K such that k is cyclic over $\mathbb{Q}(i)$. Then, due to the structure of the composite field, it must be $k \subseteq C$ or $k \subseteq \Gamma$, and hence $[k : \mathbb{Q}(i)] \leq p^{h'}$.
Now we look at the ramification field of μ in K. Let V any subfield of K

in which μ ramifies. Recall that $m = a^{f_V}$ where f_V is the inertial degree of μ in V, and a is the prime such that $(a) = (\mu) \cap \mathbb{Z}$. It is known that since $Z[i]$ is the ring of integer of $\mathbb{Q}(i)$ it holds that

$$|\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}| = m = a^{f_V}$$

hence $\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}$ has characteristic $a \neq 1$, and since $a|m$, $a \nmid (m-1)$. Now, let η be a prime of V lying over μ, and let $e_V = e(\eta|\mu)$ be the ramification index. e_V must divide p^n: in fact, if η' is a prime of K lying over η, then η' lies over μ and

$$e(\eta'|\mu) = e(\eta'|\eta)e(\eta|\mu)$$

and at the same time

$$e(\eta'|\mu)f(\eta'|\mu)g(\eta'|\mu) = [K : \mathbb{Q}(i)] = p^n$$

Hence a, the characteristic of $\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}$, is coprime with e_V, since otherwise we would have $a = p|(m-1)$ which is a contradiction. Due to the fact that V was chosen arbitrarily, all this means that K itself is the ramification field of μ in K, and so that the extension is tamely ramified.
In this situation, the inertia group of μ is cyclic. In order to prove this claim, we consider the higher ramification groups.

Definition 2.6.1. Let η be a prime of K lying over μ, and let $\mathcal{O}_K$ be the ring of integers of K. For every integer $n \geq 1$, we call n-th ramification group of η the subgroup of the inertia group T

$$G_n = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \mod (\eta)^n \text{ for all } \alpha \in \mathcal{O}_K\}$$

Note that $G_1 = T$ and that the groups form a descending chain, and that G_n is reduced to the identity for n large enough. Moreover, it is possible to prove (for example as in [21], Chapter V, §.10, Theorem 25) that

Theorem 2.6.1. *$\frac{T}{G_2}$ is isomorphic to a subgroup of the multiplicative group of $\frac{\mathcal{O}_K}{\eta\mathcal{O}_K}$ and it is therefore cyclic. For every $i \geq 2$, $\frac{G_i}{G_{i+1}}$ is isomorphic to a subgroup of the additive group of $\frac{\mathcal{O}_K}{\eta\mathcal{O}_K}$.*

Now let $\bar{n}$ be the minimum index such that $G_{\bar{n}} = \{1\}$. Then

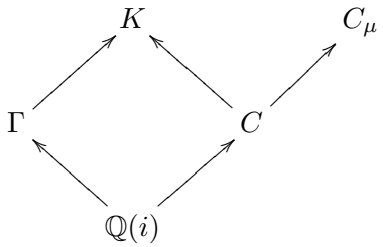
$$|G_{\bar{n}-1}| = |\frac{G_{\bar{n}-1}}{G_{\bar{n}}}|$$

but since $\frac{G_{\bar{n}-1}}{G_{\bar{n}}}$ is isomorphic to a subgroup of the additive group of $\frac{\mathcal{O}_K}{\eta\mathcal{O}_K}$, and the latter has cardinality a^{f_K}, this means that $|G_{\bar{n}-1}|$ divides a^{f_K}. At the same time, being a subgroup of T, $G_{\bar{n}-1}$ must have a cardinality that divides e_K, and so $G_{\bar{n}-1} = \{1\}$ because e_K and a^{f_K} are coprime. Repeating

the argument, we find that for every $i \geq 2$, $G_i = \{1\}$, and thus in particular $T \cong \frac{T}{G_2}$ is cyclic.
Since T is a cyclic subgroup of $Gal(K/\mathbb{Q}(i))$, and since we know that the latter is isomorphic to $Gal(\Gamma/\mathbb{Q}(i)) \times Gal(C/\mathbb{Q}(i))$, it must necessarily be that

$$e_k = |T| \leq p^{h'} \tag{2.19}$$

On the other hand, we know that $C \subseteq C_\mu$, and so we are in the following situation:



We know from Theorem (2.1.2) that μ is totally ramified in C_μ, and so it must be totally ramified also in C. This means that $e_C = p^{h'}$, and so e_K, which is a multiple of e_C, must be bigger than $p^{h'}$. So, using Eq. (2.19), we get that $e_k = p^{h'}$, that implies that the inertia field K^T, i. e the field fixed by T, is of degree $p^{n-h'}$ over $\mathbb{Q}(i)$. The assumption $n > h'$ implies that K^T is a nontrivial extension of $\mathbb{Q}(i)$, and its discriminant is not divisible by μ (otherwise μ would ramify). But since the inertia field is a subfield of K, and the discriminant of the composite field K is only divisible by μ by construction, we get that K^T is a nontrivial extension of $\mathbb{Q}(i)$ whose discriminant is a unit, which is absurd. Hence $n = h'$, and this implies that $K = \Gamma$, which means that C and Γ are actually the same field, as we wanted to prove. □

Remark 2.6.1. The previous Lemma holds also if we consider $p = 2$ and p^h is chosen to be the highest power of 2 dividing $\frac{1}{4}(m-1)$. The proof is identical to the one used in the odd case: we choose p^h to be the highest power of 2 dividing $\frac{1}{4}(m-1)$ (instead of $m-1$) only because we have seen that the discriminant of the subextensions of C_μ of degree 2^{h+1} and 2^{h+2} is divided also by $(1+i)$ (so for these fields we cannot use the final argument regarding K^T).

Using all these results with Theorem (2.4.1), it is clear that the following result holds:

Theorem 2.6.2. *Every field C_μ obtained from the division of the lemniscate is contained in a field that is the composite of a finite number of the fields described in Lemma (2.6.1). Being the composite of a finite number of abelian fields, the composite field is abelian, and so also C_μ is an abelian extension of $\mathbb{Q}(i)$.*

At this point, the similarity to the situation we encounter with the cyclotomic extensions of $\mathbb{Q}$ gives the motivation in order to introduce the following definition

Definition 2.6.2. We call **lemniscate field** any field extension $\mathbb{Q}(i) \subseteq K$ such that K is one of the fields described in Lemma (2.6.1), and also any composite field obtained by composing a finite number of the previous fields.

Definition 2.6.3. An extension $\mathbb{Q}(i) \subseteq K$ is said to be a **lemniscate extension** if K is the subfield of a lemniscate field.

So finally we can state the main result we are going to prove in this thesis:

Takagi's Theorem. *Every abelian field extension $\mathbb{Q}(i) \subseteq K$ which is finite is a lemniscate extension.*

Chapter 3

The proof of Takagi's Theorem

In order to prove Takagi's Theorem, we will need to make different reduction steps. It may be interesting to remark that from this point of view there are several similarities between the techniques that Takagi uses and the ones that are exploited in Hilbert's proof of the Kroneker-Weber Theorem, as it might be seen reading the paper of Greenberg on the subject ([8]).

3.1 Reduction to prime power order.

Proposition 3.1.1. *If Takagi's Theorem is true for cyclic extensions of $\mathbb{Q}(i)$ whose degree over $\mathbb{Q}(i)$ is a prime power, then it holds for all finite abelian extensions of $\mathbb{Q}(i)$.*

Proof. Suppose that we have a finite abelian extension $\mathbb{Q}(i) \subseteq K$ with Galois group $G = Gal(K/\mathbb{Q}(i))$. Using the Structure Theorem for finite abelian groups, we can decompose G into the direct product of r cyclic subgroups G_i whose order is a prime power. If K_i is the subfield fixed by $\prod_{j\neq i} G_i$, since $K/\mathbb{Q}(i)$ is a Galois extension, it holds that $Gal(K_i/\mathbb{Q}) = {}^{G}/_{\prod_{j\neq i} G_i} = G_i$. Moreover, K is equal to E , the field obtained by composing all the K_i: in fact, E is surely contained in K, thus $Gal(K/E) \subseteq Gal(K/K_i) = \prod_{j\neq i} G_i$ for all i. This implies that $Gal(K/E) \subseteq \bigcap_{1\leq i\leq r} \prod_{j\neq i} G_i = \{1_G\}$ and so $K = E$.

Then, if we prove that all the extensions that have a cyclic Galois group of prime power order are lemniscate extension, then K_i is a subfield of some lemniscate extension for all i, and thus, due to the definition of lemniscate extension, also the composite field K is a lemniscate extension. □

3.2 The second reduction step

In order to proceed with the proof of Takagi's Theorem, we would like to be able to determine exactly the elements dividing the discriminant of the extension that we are considering. The second (and most important) reduction step is the one illustrated by the following

Proposition 3.2.1. *In order to prove that Takagi's Theorem holds for cyclic extensions $\mathbb{Q}(i) \subseteq K$ such that $[K : \mathbb{Q}(i)] = p^h$ for p prime, we can reduce ourselves to the case in which the discriminant of the extension is divisible only by the primes $\mathfrak{p} \in Q(i)$ dividing p.*

Since the proof of this statement is quite long, and involves different intermediate steps, we need to first prove some additional results.

Proposition 3.2.2. *Let $\mathbb{Q}(i) \subset C$ be a cyclic extension of degree p^h where p is prime, and for all $k \leq h$ denote by C_k the unique subextension of C such that $[C_k : \mathbb{Q}(i)] = p^k$. Suppose that the discriminant of $\mathbb{Q}(i) \subset C$ is divided by a prime $\mu \in \mathbb{Z}[i]$ which is coprime with p. If μ ramifies in C_1, we can find a cyclic extension $\mathbb{Q}(i) \subseteq D \subseteq C_h$ such that*

- *$DM = C_h M$*
- *$D \cap M = \mathbb{Q}(i)$.*
- *the discriminant of $\mathbb{Q}(i) \subseteq D$ is divisible by all prime factors dividing the discriminant $\mathbb{Q}(i) \subseteq C_h$ except for μ.*

where we denote by M the unique lemniscate field of degree $[M : \mathbb{Q}(i)] = p^h$ whose discriminant is divisible only by μ.

Proof. Using Lemma (2.1.3), we have that $m - 1 \equiv \mod p^h$. Since the last congruence holds, we can find a suitable field M among the fields listed in Lemma (2.6.1), and according to Lemma (2.6.2) M is then the only field with these characteristics. Suppose $\mathbb{Q}(i) \subsetneq C_h \cap M$. According to Corollary (2.1.2) the composite field $C_h M$ is an abelian extension of $\mathbb{Q}(i)$ of degree $[C_h M : \mathbb{Q}(i)] = p^{h+h'}$ for a certain $h' \leq h$. Using Proposition (2.1.3) we can find another cyclic extension C^* of $\mathbb{Q}(i)$ of degree $[C^* : \mathbb{Q}(i)] = p^{h'}$ such that $C_h M = C^* M$ and $C^* \cap M = \mathbb{Q}(i)$. For this reason,

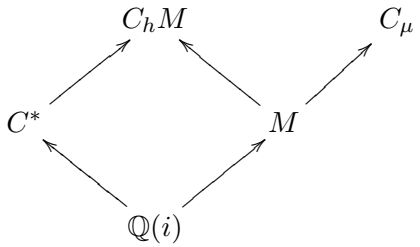
$$Gal\left(\frac{C_h M}{\mathbb{Q}(i)}\right) = Gal\left(\frac{C^* M}{\mathbb{Q}(i)}\right) \cong Gal\left(\frac{C^*}{\mathbb{Q}(i)}\right) \times Gal\left(\frac{M}{\mathbb{Q}(i)}\right)$$

where $Gal(C^*/\mathbb{Q}(i))$ is cyclic of order $p^{h'}$ and $Gal(M/\mathbb{Q}(i))$ is cyclic of order p^h. What we want to prove next is that the inertia group T of μ in $C_h M$ is cyclic of order p^h. We start by considering that if we have a cyclic extension of $C_h M$, due to the structure of $Gal(C_h M/\mathbb{Q}(i))$ this extension must be of

degree smaller than p^h. Note that if m is the norm of μ, and $(\mu) \cap \mathbb{Z} = (a)$, we have that $m = N(\mu) = a^f$ and

$$|\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}| = a^f$$

so that $\frac{\mathbb{Z}[i]}{\mu\mathbb{Z}[i]}$ has characteristic a, with a such that $a|m$ and a does not divide $m-1$. Using the same argument as in Lemma (2.6.2), we first observe that C_hM is a tamely ramified extension of $\mathbb{Q}(i)$, and then that the inertia group is cyclic. Furthermore, we know that $M \subseteq C_\mu$, and so we are in the following situation:



So, μ must be totally ramified in M (since it is totally ramified in C_μ) and so denoting by $e(K|\mu)$ the ramification index of μ in an extension K we get

$$p^h = [M : \mathbb{Q}(i)] = e(M|\mu) \leq e(C_hM|\mu) = |T| \leq p^h$$

Then the inertia field (that we are going to denote by C^T) has degree $[C^T : \mathbb{Q}(i)] = p^{h'}$. Note that since

$$Gal\left(\frac{C_hM}{\mathbb{Q}(i)}\right) \cong Gal\left(\frac{C^*}{\mathbb{Q}(i)}\right) \times Gal\left(\frac{M}{\mathbb{Q}(i)}\right)$$

we have that

$$Gal\left(\frac{C^T}{\mathbb{Q}(i)}\right) \cong \frac{Gal\left(\frac{C_hM}{\mathbb{Q}(i)}\right)}{T} \cong \frac{Gal\left(\frac{C^*}{\mathbb{Q}(i)}\right) \times Gal\left(\frac{M}{\mathbb{Q}(i)}\right)}{T}$$

and since T is cyclic of order p^h, it must be that

$$Gal\left(\frac{C^T}{\mathbb{Q}(i)}\right) \cong Gal\left(\frac{C^*}{\mathbb{Q}(i)}\right)$$

so that C^T is a cyclic extension of $\mathbb{Q}(i)$. Furthermore, since μ is totally ramified in M and inert in C^T, it holds that $M \cap C^T = \mathbb{Q}(i)$. On the other hand, $MC^T \subseteq MC_h$ and

$$[MC^T : \mathbb{Q}(i)] = [M : \mathbb{Q}(i)][C^T : \mathbb{Q}(i)] = p^{h+h'} = [MC_h : \mathbb{Q}(i)]$$

hence $MC_h = MC^T$.
Finally, the discriminant of the extension $\mathbb{Q}(i) \subseteq C^T$ is divisible by all the prime factors dividing the discriminant $\mathbb{Q}(i) \subseteq C_h$ except for μ: in fact, all the primes ramifying in C_h ramifies in $C_hM = C^TM$ but they don't ramify in M so they have to ramify in C^T. □

Proposition 3.2.3. *Proposition (3.2.2) holds also if the first field in which μ ramifies is C_k, $1 < k \leq h$.*

Proof. We proceed by induction. We already proved the case $i = 1$, so now we suppose that the statement holds for $i = k$ and we prove it for $i = k+1$. The congruence

$$m \equiv 1 \bmod p^{h-k}$$

holds, so we consider the cyclic extension $\mathbb{Q}(i) \subseteq M$ where $[M : \mathbb{Q}(i)] = p^{h-k}$ and such that the only prime ramifying in M is μ. Repeating the argument used in the case $i = 1$, we can suppose that $C_h \cap M = \mathbb{Q}(i)$ and we have that

$$Gal\left(\frac{C_h M}{\mathbb{Q}(i)}\right) \cong Gal\left(\frac{C_h}{\mathbb{Q}(i)}\right) \times Gal\left(\frac{M}{\mathbb{Q}(i)}\right)$$

Let $\mu = \mathfrak{m}_1\mathfrak{m}_2...\mathfrak{m}_g$ be the decomposition of μ in prime ideals of C_k(μ is not ramified in C_k by hypothesis, so all the $\mathfrak{m}_i$ are distinct). For every i let $\mathfrak{M}_i$ be a prime lying over $\mathfrak{m}_i$ in $C_h M$. We want to prove that the p^{h-k}-th power of $(\mathfrak{M}_i)$ divides exactly $\mathfrak{m}_i$ in $C_h M$. In order to do so, we note that μ is totally ramified in M, since this field is a subextension of C_μ and μ is totally ramified in C_μ. This implies that the ramification index of μ in $C_h M$ is

$$e(\mu | C_h M) \geq p^{h-k}$$

At the same time,

$$e(\mu | C_h M) = e(\mu | C_k) e(\mathfrak{m} | C_h M) = e(\mathfrak{m} | C_h M)$$

since μ is not ramified in C_k. Hence

$$e(\mathfrak{m} | C_h M) \geq p^{h-k}$$

For the same reasons as in the previous proofs, the extension $C_k \subseteq C_h M$ is tamely ramified, and so using the same argument as before we see that the inertia group T is cyclic. But the subgroup of

$$Gal\left(\frac{C_h M}{\mathbb{Q}(i)}\right) \cong Gal\left(\frac{C_h}{\mathbb{Q}(i)}\right) \times Gal\left(\frac{M}{\mathbb{Q}(i)}\right)$$

corresponding to the extension $C_k \subseteq C_h M$ is the subgroup formed by all the transformations fixing C_k, so it must be the direct product of a subgroup of $Gal(C_h/\mathbb{Q}(i))$ of order p^{h-k} with $Gal(M/\mathbb{Q}(i))$. As a consequence, every cyclic subgroup of $Gal(MC_h/C_k)$ must have order at most p^{h-k}, and this means that

$$e(\mathfrak{m} | C_h M) = |T| = p^{h-k}$$

Thus, the p^{h-k}-th power of $(\mathfrak{M}_i)$ divides exactly $\mathfrak{m}_i$ in $C_h M$, and therefore the ramification index of μ in $C_h M$ is exactly p^{h-k}. Note that as before,

we can prove that also $\mathbb{Q}(i) \subseteq MC_h$ is tamely ramified: as a consequence, $\bar{T}$, which is the inertia group of this last extension, is cyclic, of order p^{h-k}. The inertia field, that we will denote by $C^{\bar{T}}$, is then of degree

$$[C^{\bar{T}} : \mathbb{Q}(i)] = \frac{[MC_h : \mathbb{Q}(i)]}{p^{h-k}} = p^h$$

Furthermore, $\mathbb{Q}(i) \subseteq C^{\bar{T}}$ is a cyclic extension, since

$$Gal\left(\frac{C^{\bar{T}}}{\mathbb{Q}(i)}\right) \equiv \frac{Gal\left(\frac{C_h M}{\mathbb{Q}(i)}\right)}{T}$$

and we can proceed as in the previous proof. Moreover, $C^{\bar{T}} \cap M = \mathbb{Q}(i)$ (μ is totally ramified in M, and inert in $C^{\bar{T}}$) and by looking at the degree of the extension we find that $MC_h = MC^{\bar{T}}$. So the last thing we need to prove is that the discriminant of this new extension is divisible by all the primes dividing the discriminant of $\mathbb{Q}(i) \subseteq C_h$ except for μ, but this is clear if we reason as in the previous case. □

Having this machinery, we are now able to prove Proposition (3.2.1) stating that

Proposition. In order to prove that Takagi's Theorem holds for cyclic extensions $\mathbb{Q}(i) \subseteq K$ such that $[K : \mathbb{Q}(i)] = p^h$ for p prime, we can reduce ourselves to the case in which the discriminant of the extension is divisible only by the primes $\mathfrak{p} \in Q(i)$ dividing p.

Proof. Let μ be a prime dividing the discriminant of $C_h = K$ but which does not divide p. From the previous Propositions, we know that, considering to the first k such that μ ramifies in C_k, we can find a suitable elementary lemniscate field M_μ and a field C_k^μ depending on k and μ such that:

- $C_h \subseteq M_\mu C_h = M_\mu C_k^\mu$
- the discriminant of $\mathbb{Q}(i) \subseteq C_k^\mu$ is divisible by all prime factors dividing the discriminant $\mathbb{Q}(i) \subseteq C_h$ except for μ.
- $[C_k^\mu : \mathbb{Q}(i)]$ is a power of p.
- $\mathbb{Q}(i) \subseteq C_k^\mu$ is a cyclic extension.

In the case in which there is another prime $\nu \in \mathbb{Q}(i)$ which does not divide p, we can repeat the argument for C_k^μ, that is we find another index k', and two field M_ν and C_l^ν such that

- $C_k^\mu \subseteq M_\nu C_k^\mu = M_\nu C_l^\nu$

- the discriminant of $\mathbb{Q}(i) \subseteq C_l^\nu$ is divisible by all prime factors dividing the discriminant $\mathbb{Q}(i) \subseteq C_h$ except for μ and ν.
- $[C_l^\nu : \mathbb{Q}(i)]$ is a power of p.
- $\mathbb{Q}(i) \subseteq C_l^\nu$ is a cyclic extension.

Therefore,

$$C_h \subseteq M_\mu C_h = M_\mu C_k^\mu \subseteq M_\mu M_\nu C_k^\mu = M_\mu M_\nu C_l^\nu$$

Repeating the argument for all the primes $\mu_1, \ldots, \mu_s$ dividing the discriminant of $\mathbb{Q}(i) \subseteq C_h$ but not dividing p, we find that

$$C_h \subseteq M_{\mu_1} \ldots M_{\mu_s} \widetilde{C}$$

where $M_{\mu_1}, \ldots, M_{\mu_s}$ are the elementary lemniscate fields described before and $\widetilde{C}$ is a cyclic extension of $\mathbb{Q}(i)$ of degree a power of p, whose discriminant is only divisible by primes dividing p.
Then, if we are able to prove Takagi's Theorem for $\widetilde{C}$, we are done, since if $\widetilde{C}$ is contained in a lemniscate field V, then

$$C_h \subseteq M_{\mu_1} \ldots M_{\mu_s} \widetilde{C} \subseteq M_{\mu_1} \ldots M_{\mu_s} V$$

and then by definition C_h is a lemniscate extension, as we wanted to prove. □

3.3 The final steps

In order to prove the Theorem, from what we have seen before, we only need to consider the case of a cyclic extension $\mathbb{Q}(i) \subseteq C$ such that $[C : \mathbb{Q}(i)]$ is a power of a prime p and such that the discriminant $\Delta(C|\mathbb{Q}(i))$ is only divisible by elements of $\mathbb{Q}(i)$ dividing p.

We would like to be dealing with only one prime dividing the discriminant, but we know that if $p \equiv 1 \bmod 4$ then $p\mathbb{Q}(i) = \pi_1\pi_2$ with $\pi_1 \neq \pi_2$, so that it is possible that the discriminant is divided by two different primes. In order to avoid this kind of problem, the idea is to separate the three cases that may occur:

- $p \equiv 1 \bmod 4$ so that in this case $p\mathbb{Q}(i) = \pi_1\pi_2$ with $\pi_1 \neq \pi_2$, hence in standard notation we have $g = 2$, the ramification index is $e = 1$ and the inertia degree is $f = 1$.
- $p \equiv 3 \bmod 4$ and here $g = 1,\ e = 1,\ f = 2$.
- $p = 2$ and $2 = (1+i)(1-i)$ hence $g = 2,\ e = 1,\ f = 1$.

and treat them with different techniques.

3.3.1 $p \equiv 1 \bmod 4$

We first prove that the principle is true in a particular case and then we show that this case is enough for our purposes.

Proposition 3.3.1. *If $p \equiv 1$ mod 4 and C is a cyclic extension of $\mathbb{Q}(i)$ of degree p^h whose discriminant over $\mathbb{Q}(i)$ is a power of only one of the two primes dividing p, then C is one of the elementary lemniscate fields whose existence was proved in Lemma (2.6.1).*

Proof. We proceed by induction on h. So in the case $h = 1$, suppose that we have two different fields $C \neq C'$ with the same characteristics listed before. We may consider the composite field CC' and add a primitive p-th root of unity ζ, obtaining an abelian extension $K = CC'(\zeta)$ which has degree $p^2(p-1)$ over $\mathbb{Q}(i)$: in fact, we conclude that $\zeta \notin C, C'$ thinking about the degree, and for the same reason $C \cap C' = \mathbb{Q}(i)$. Considering as usual $Z = \mathbb{Q}(i, \zeta)$, we have that since $p \equiv 1 \bmod 4$ and p is totally ramified in $\mathbb{Q}(\zeta)$, there are two primes $\mathfrak{p}, \mathfrak{p}'$ of $Z = \mathbb{Q}(i, \zeta)$ such that

$$p\mathbb{Q}(i, \zeta) = (\mathfrak{p}\mathfrak{p}')^{p-1}$$

Moreover, $p\mathbb{Q}(i) = \pi\pi'$, so $\pi\mathbb{Q}(i, \zeta) = \mathfrak{p}^{p-1}$ and $\pi'\mathbb{Q}(i, \zeta) = \mathfrak{p}'^{p-1}$. Furthermore, as it may be proved following [3], Lemma 3, Chapter III, p. 87, if we set $\eta = 1 - \zeta$ we get that

$$(\eta) = \mathfrak{p}\mathfrak{p}'$$

Now, we consider $Z \subseteq C(\zeta)$. It holds that

$$[C(\zeta) : Z] = \frac{[C(\zeta) : \mathbb{Q}(i)]}{[Z : \mathbb{Q}(i)]} = \frac{p(p-1)}{p-1} = p$$

so the extension is necessarily cyclic and by Lemma (2.1.5) there must be an element χ in Z such that $C(\zeta) = Z(\sqrt[p]{\chi})$. Now we show that it is possible to choose χ with the property

$$\chi \equiv 1 \bmod \mathfrak{p}$$

since if χ does not satisfy the congruence, we can use the same type of argument we exploited in the proof of Lemma (2.1.3). In fact, if we choose $g \in \mathbb{N}$ such that $1 < g < p$ then the automorphism of Z sending ζ into ζ^g (that we are going to denote by s) is a generator of $Gal(Z/\mathbb{Q}(i))$, and we have that

$$s(\mathfrak{p}) = \mathfrak{p}', \ s^2(\mathfrak{p}) = \mathfrak{p}$$

So, following the idea of Lemma (2.1.3), we note that $s^2 - 1$ and $s - g$ are coprime modulo p, which means that we can find three polynomial expressions $f_1(s), f_2(s), f_3(s)$ such that

$$1 = (s^2 - 1)f_1(s) + (s - g)f_2(s) + pf_3(s)$$

As a consequence, since by Lemma (2.1.6) χ^{s-g} is a p-th power, there must be an element $\alpha \in Z$ such that

$$\chi = \chi^{(s^2-1)f_1(s)}\alpha^p$$

Seen that $s^2(\mathfrak{p}) = \mathfrak{p}$, $\chi^{(s^2-1)}$ can be written as a fraction in which neither the denominator nor the numerator are divisible by $\mathfrak{p}$. The same holds for $\chi^{(s^2-1)f_1(s)}$ which then can be written as

$$\chi^{(s^2-1)f_1(s)} = \frac{\chi^*}{a^p}$$

where $\chi^* \in Z$ is an integer coprime with $\mathfrak{p}$ and a is a rational integer. In conclusion, $\chi^* = \frac{a^p}{\alpha^p}\chi$ so clearly $\sqrt[p]{\chi^*}$ and $\sqrt[p]{\chi}$ define the same field, and

$$\chi^* \equiv 1 \bmod \mathfrak{p}$$

Now, since $\mathfrak{p}$ is an ideal of degree 1, the congruence

$$\begin{aligned} \chi^* &\equiv 1 + a\eta \bmod \mathfrak{p}^2 \\ (\eta &= 1 - \zeta) \end{aligned}$$

is satisfied by an element $a \in \mathbb{Z}$: in fact $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}\mathfrak{p}'$ since the two ideals are coprime, and

$$\frac{Z}{\mathfrak{p}Z} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$$

We claim that a is not divisible by p. In fact, if a is divisible by p then

$$a \in (p) = (\mathfrak{p}\mathfrak{p}')^{p-1} = \mathfrak{p}^{p-1}(\mathfrak{p}')^{p-1} \subseteq \mathfrak{p}^2(\mathfrak{p}')^{p-1} \subseteq \mathfrak{p}^2$$

and then the congruence

$$\chi^* \equiv 1 \bmod \mathfrak{p}^2$$

holds. Now let d be the maximum natural number such that we can find $l \in \mathbb{Z}$ coprime with $\mathfrak{p}$ such that

$$\chi^* - 1 \equiv l\eta^d \bmod \mathfrak{p}^{d+1} \tag{3.1}$$

and suppose $d < p$. Seen that χ^{s-g} is a p-th power, $(\chi^*)^{s-g} = \left(\frac{a^p}{\alpha^p}\right)^{s-g}\chi^{s-g}$ must be the p-th power of an element $\beta \in Z$. Using the congruence (3.1), we see that

$$\begin{aligned} \beta^p &\equiv (1 + l\eta^d)^{s-g} \bmod \mathfrak{p}^{d+1} \\ &\equiv (1 + ls(\eta)^d)(1 + l\eta^d)^{-g} \bmod \mathfrak{p}^{d+1} \end{aligned}$$

First of all, let us remark that

$$s(\eta) = 1 - \zeta^g \equiv g\eta \bmod \mathfrak{p}^2$$

so $s(\eta)^d = (g\eta)^d \bmod \mathfrak{p}^{d+1}$. On the other hand,

$$\begin{aligned}(1+l\eta^d)^g(1-l\eta^d)^g &\equiv (1-l\eta^{2d})^g \bmod \mathfrak{p}^{d+1}\\ &\equiv 1 \bmod \mathfrak{p}^{d+1}\end{aligned}$$

hence

$$\begin{aligned}(1+l\eta^d)^{-g} &\equiv (1-l\eta^d)^g \bmod \mathfrak{p}^{d+1}\\ &\equiv 1-gl\eta^d \bmod \mathfrak{p}^{d+1}\end{aligned}$$

Therefore,

$$\begin{aligned}\beta^p &\equiv (1+l(g\eta)^d)(1-gl\eta^d) \bmod \mathfrak{p}^{d+1}\\ &\equiv 1+l(g\eta)^d-gl\eta^d \bmod \mathfrak{p}^{d+1}\end{aligned}$$

which implies first that $\beta \equiv 1 \bmod \mathfrak{p}$ and then $\beta^p \equiv 1 \bmod \mathfrak{p}^p$. Finally, this means that $l(g\eta)^d \equiv gl\eta^d \bmod \mathfrak{p}$ which is a contradiction, because g is a primitive root modulo p and $e < p$; as a consequence, we get that $\chi^* \equiv 1 \bmod \mathfrak{p}^p$ and so

$$\sqrt[p]{\chi*} \equiv 1 \bmod \mathfrak{p}$$

At this point, if we choose an algebraic integer $\nu \in \mathfrak{p}' \setminus \mathfrak{p}$, we can define the element

$$\omega = \frac{\nu}{\eta}(1-\sqrt[p]{\chi^*})$$

which is a root of the polynomial

$$(\eta X-\nu)^p + \nu^p\chi^*$$

Since $\eta = 1-\zeta, \nu, \chi^*$ are algebraic integers, and since

$$\nu(1-\sqrt[p]{\chi^*}) \in \mathfrak{p}\mathfrak{p}' = (1-\zeta)$$

ω is also an algebraic integer. Clearly, $Z(\omega) = C(\zeta)$, so the discriminant of the extension $Z \subset C(\zeta)$ must divide the discriminant $\Delta(\omega|Z)$ of ω. Using Eq.(2.12) we get that

$$\begin{aligned}\Delta(\omega|Z) &= (-1)^{\frac{p(p-1)}{2}}\mathbf{N}_{C(\zeta)|Z}\left(p(\eta\omega-\nu)^{p-1}\eta\right)\\ &= \nu^{p(p-1)}(\chi^*)^{p-1}p^p\eta^p\end{aligned}$$

But we know that $(p) = (\mathfrak{p}\mathfrak{p}')^{p-1}$ and that $\eta = (\mathfrak{p}\mathfrak{p}')$, so we have

$$(p^p\eta^p) = (\mathfrak{p}\mathfrak{p}')^{p(p-1)} \equiv 1 \bmod \mathfrak{p}$$

since $\mathfrak{p}, \mathfrak{p}' \subset Z = \mathbb{Q}(i,\zeta)$ so the discriminant is coprime with $\mathfrak{p}$, and so $\mathfrak{p}$ does not ramify in $C(\zeta)$. Now let $\mathfrak{P} \subseteq \mathcal{O}_{C(\zeta)}$ denote a prime ideal lying over $\mathfrak{p}$. $\mathfrak{P}^{p-1}$ is the maximal power of $\mathfrak{P}$ that divides π: in fact,

$$(\mathfrak{P} \cap Z)^{p-1} = \mathfrak{p}^{p-1} = \pi$$

and as we have seen before $\mathfrak{p}$ does not ramify in $C(\zeta)$. This means that the ramification index $e(\pi|C(\zeta)) = p-1$ and so the inertia field D^T related to π has degree

$$[D^T : \mathbb{Q}(i)] = \frac{[C(\zeta) : \mathbb{Q}(i)]}{e(\pi|C(\zeta))} = \frac{p(p-1)}{p-1} = p$$

But this result yields a contradiction. In fact, consider the intersection $D^T \cap C$: if $D^T \cap C = \mathbb{Q}(i)$ then since $D^T \subseteq C(\zeta) = CZ$ we have that $D^T \subseteq Z$ which is absurd since $[D^T : \mathbb{Q}(i)] = p > p-1 = [Z : \mathbb{Q}(i)]$. If otherwise, $\mathbb{Q}(i) \subsetneq D^T \cap C$, then the intersection is a subfield of C, but since $[C : \mathbb{Q}(i)] = p$ this implies $D^T \cap C = C$. Then $D^T = C$ since $[D^T : \mathbb{Q}(i)] = p$, and so at the same time π must be inert in D^T and ramified in C, which is impossible since the extension is not trivial. So, we are in the situation

$$\begin{aligned} \chi^* &\equiv 1 + a\eta \bmod \mathfrak{p}^2 \\ a &\neq 0 \bmod p \end{aligned}$$

With the same argument, we can find an element ρ such that

$$C'(\zeta) = \mathbb{Q}(i, \zeta, \sqrt[p]{\rho})$$

where

$$\begin{aligned} \rho &\equiv 1 + b\eta \bmod \mathfrak{p}^2 \\ b &\neq 0 \bmod p \end{aligned}$$

If we denote by c an integer number satisfying

$$a + bc \equiv 0 \bmod p$$

and we set $\theta = \chi^* \rho^c \in Z$ it holds that

$$\begin{aligned} \theta &\equiv (1 + a\eta)(1 + b\eta)^c \bmod \mathfrak{p}^2 \\ &\equiv (1 + a\eta)\,(1 + cb\eta) \bmod \mathfrak{p}^2 \\ &\equiv 1 + a\eta + cb\eta + abc\eta^2 \bmod \mathfrak{p}^2 \\ &\equiv 1 \bmod \mathfrak{p}^2 \end{aligned}$$

Now suppose that $C \neq C'$. In this case, θ is not a p-th power in Z, seen that

$$\sqrt[p]{\theta} = \sqrt[p]{\chi^*}\sqrt[p]{\rho^c}$$

and $\sqrt[p]{\chi^*}$, $\sqrt[p]{\rho^c} \notin Z$. Since $C(\zeta, \sqrt[p]{\theta}) = CC'(\zeta) = K$ as before we can find a contradiction starting from the congruence

$$\theta \equiv 1 \bmod \mathfrak{p}^2$$

In fact, starting from the last congruence we can find as before that $\mathfrak{p}$ does not ramify in K. Then, if $\mathfrak{Q} \subset \mathcal{O}_K$ is a prime ideal lying over $\mathfrak{p}$, exactly as before we see that the maximum power of $\mathfrak{Q}$ dividing π is $p-1$, hence the ramification index is $e(\pi|K) = p-1$ and the inertia field $D^T \subset K$ of π has degree $[D^T : \mathbb{Q}(i)] = p^2$. Also in this case the intersection $D^t \cap C$ cannot be trivial, because otherwise $D^T \subset C'(\zeta)$ which is absurd because

$$[C'(\zeta) : \mathbb{Q}(i)] = p(p-1) < p^2 = [D^T : \mathbb{Q}(i)]$$

The only other possibility is $D^t \cap C = C$, which implies that $C \subset D^T$: but this is impossible, because π is ramified in C and inert in D^T. Hence C must be equal to C', proving our assertion for this case.

We are left to prove the inductive step. In order to do so, we suppose that the statement holds for $h = k-1$, and we prove it for $h = k$. Suppose that we have two different fields C, C' with the same desired properties. If C_{k-1} and C'_{k-1} are subfields respectively of C and C' , such that they are both cyclic extensions of $\mathbb{Q}(i)$ of degree p^{k-1},by the inductive hypothesis they must coincide.
However, composing C and C' we get a field K such that

$$[K : \mathbb{Q}(i)] = \frac{[C : \mathbb{Q}(i)][C' : \mathbb{Q}(i)]}{[C \cap C' : \mathbb{Q}(i)]} = \frac{p^h p^h}{p^{h-1}} = p^{h+1}$$

By Proposition (2.1.3) K might be composed also by C and another cyclic extension L_1 of $\mathbb{Q}(i)$ of degree $[L_1 : \mathbb{Q}(i)] = p$ such that $L_1 \cap C = \mathbb{Q}(i)$ But then the discriminant of the extension $\mathbb{Q}(i) \subseteq L_1$ must be a power of π. Now note that, being a cyclic extension, C has a subfield that has degree p over $\mathbb{Q}(i)$, and whose discriminant is a power of π or an unit. By the previous discussion, the first case implies that the subfield coincides with L_1, so that we find the contradiction $L_1 \subseteq C$. On the other hand, the other case is impossible since $[L_1 : \mathbb{Q}(i) = p]$ and so L_1 would be a non trivial extension of $\mathbb{Q}(i)$ with trivial discriminant. Therefore, C and C' must be the same field, as we wanted to prove. □

Lemma 3.3.1. *Studying the case $p \equiv 1$ mod 4, we can always reduce the problem to the case in which the discriminant is the power of only one of the two primes dividing p.*

Proof. Suppose we have a cyclic extension $\mathbb{Q}(i) \subseteq C$ of degree p^h, where the discriminant is divided only by elements dividing p. If $p\mathbb{Q}(i) = \pi\pi'$ is the prime decomposition of p in $\mathbb{Q}(i)$, we denote by Π_h and Π'_h the two elementary lemniscate fields of degree p^h whose discriminant over $\mathbb{Q}(i)$ is respectively a power of π or of π'. Let us consider the field $P_h = \Pi_h \Pi'_h$: it's an abelian extension of $\mathbb{Q}(i)$ of degree p^{2h}, seen that $\Pi_h \cap \Pi'_h = \mathbb{Q}(i)$ since the two discriminant are coprime. In P^h, we find $p^h + 1$ different subfields

of degree p^h over $\mathbb{Q}(i)$ whose discriminant is divisible only by π and π': they are built by composing, for every $i \in \{1, \dots, h\}$, the subfield $\Pi_{h-k} \subset \Pi_h$ of degree p^{h-k} over $\mathbb{Q}(i)$ with the subfield $\Pi'_k \subset \Pi'_h$ of degree p^k over $\mathbb{Q}(i)$ (where we set $\Pi_0 = \Pi'_0 = \mathbb{Q}(i)$).
Now we want to prove that C is one of these subfields. We proceed by induction on h.
Suppose that $h = 1$, i.e. $[C : \mathbb{Q}(i)] = p$. Consider a primitive p-th root of unity ζ. As before, since p is totally ramified in $\mathbb{Q}(\zeta)$, there are two primes $\mathfrak{p}, \mathfrak{p}'$ of $Z = \mathbb{Q}(i, \zeta)$ such that

$$p\mathbb{Q}(i, \zeta) = (\mathfrak{p}\mathfrak{p}')^{p-1}$$

If now we set $K = CZ = C(\zeta)$, due the fact that we find $Z \cap C = \mathbb{Q}(i)$ by looking at the degree of the two extensions, we get

$$[K : Z] = \frac{[C(\zeta) : \mathbb{Q}(i)]}{[Z : \mathbb{Q}(i)]} = \frac{p(p-1)}{p-1} = p$$

and so $Z \subseteq K$ must be a cyclic extension. Therefore, there is an element $\chi \in Z$ such that $K = Z(\sqrt[p]{\chi})$.
Also in this case it is possible to find a particular χ such that there is an element $\alpha \in \mathbb{Z}$ such that

$$\chi \equiv 1 + \alpha\eta \bmod \mathfrak{p}^2$$

where $\eta = 1 - \zeta$ and

$$\alpha \neq 0 \bmod p$$

Moreover, since we can check easily that for every $r \in \mathbb{Z}$

$$\zeta^r \equiv 1 - r\eta \bmod \mathfrak{p}^2$$

setting $\rho = \zeta^\alpha \chi$ we get that

$$\rho \equiv 1 \bmod \mathfrak{p}^2$$

Consider now $K' = \mathbb{Q}(i, \zeta, \sqrt[p]{\rho})$. $K' \subseteq K$ and the discriminant $\Delta(K'|Z)$ is coprime with $\mathfrak{p}$ since $\rho \equiv 1 \bmod \mathfrak{p}^2$: hence $\Delta(K'|Z)$ is only divided by $\mathfrak{p}'$.

Then $K' = Z\Pi'$. In fact, $K' = Z\mathbb{Q}(i, \sqrt[p]{\rho})$ is an abelian extension satisfying the hypothesis of Proposition (2.1.3), so there must be a field $\mathbb{Q}(i) \subseteq \widetilde{C}$ such that $[\widetilde{C} : \mathbb{Q}(i)] = p$, $\widetilde{C} \cap Z = \mathbb{Q}(i)$ and $K' = Z\widetilde{C}$. Therefore

$$\Delta(K'|\mathbb{Q}(i)) = \Delta(Z|\mathbb{Q}(i))^{[\widetilde{C}:\mathbb{Q}(i)]} \Delta(\widetilde{C}|\mathbb{Q}(i))^{[Z:\mathbb{Q}(i)]}$$

and

$$\Delta(K'|\mathbb{Q}(i)) = \mathbf{N}_{Z|\mathbb{Q}(i)}) \left(\Delta(K'|Z)\right) \Delta(Z|\mathbb{Q}(i))^{[K':Z]}$$

which implies that

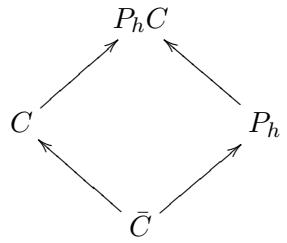
$$\Delta(\widetilde{C}|\mathbb{Q}(i))^{[Z:\mathbb{Q}(i)]} = \mathbf{N}_{Z|\mathbb{Q}(i)}\left(\Delta(K'|Z)\right)$$

because we know that $[K' : Z] = [\tilde{C} : \mathbb{Q}(i)]$. Since $\Delta(K'|Z)$ is only divided by $\mathfrak{p}'$, it means that $\Delta(\widetilde{C}|\mathbb{Q}(i))$ is a power of π', and from what we have seen in Proposition (3.3.1), this implies that $\widetilde{C} = \Pi'_1$.
In the same way, we can prove that also $K_2 = Z\Pi_1$ is a subfield of K. Thus, we can consider the composite field $K'K_2 \subseteq K$, but considering the degree, it is actually true that $K = K_2 = K'$. Hence

$$K = K'K_2 = Z\Pi'_1 Z\Pi_1 = Z\Pi_1\Pi'_1 = ZP_1$$

and since $C \cap Z = \mathbb{Q}(i)$, this means that $C \subseteq P_1$ as we wanted to prove.

Now we want to prove it for a general $h+1$, supposing that the property holds for h. If $[C : \mathbb{Q}(i)] = p^{h+1}$, we can consider the subfield $\bar{C} \subsetneq C$ such that $[\bar{C} : \mathbb{Q}(i)] = p^h$. Then by induction $\bar{C} \subseteq P_h$, therefore we are in the situation



It follows that

$$\begin{aligned}
[P_hC : \mathbb{Q}(i)] &= \frac{[C : \mathbb{Q}(i)][P_h : \mathbb{Q}(i)]}{[C_h : \mathbb{Q}(i)]} \\
&= \frac{p^{h+1}p^{2h}}{p^h} \\
&= p^{2h+1}
\end{aligned}$$

Being an abelian extension of $\mathbb{Q}(i)$ satisfying the hypothesis of Proposition (2.1.3) P_hC can be formed also by P_h and a field $\widetilde{C}$ such that $\widetilde{C} \cap P_h = \mathbb{Q}(i)$ and $[\widetilde{C} : \mathbb{Q}(i)] = p$. But again by induction, $\widetilde{C} \subseteq P_1$, thus

$$P_hC = P_h\widetilde{C} \subseteq P_hP_1$$

but

$$P_hP_1 = \Pi_h\Pi'_h\Pi_1\Pi'_1 \subseteq \Pi_h\Pi'_h = P_h$$

since $\Pi_1 \subseteq \Pi_h$ and $\Pi'_1 \subseteq \Pi'_h$ so that

$$P_hC \subseteq P_h \subseteq P_{h+1}$$

and finally $C \subseteq P_{h+1}$ as we wanted to show. □

3.3.2 $p \equiv 3$ **mod** 4

In Lemma (2.6.1) we have seen that for every prime $q \equiv 3 \bmod 4$ and any $h \in \mathbb{N}$ there are $q^h + 1$ different cyclic extensions of $\mathbb{Q}(i)$ of degree q^h and whose discriminant is a power of q. All those fields are subfields of an abelian extension $\mathbb{Q}(i) \subseteq Q_h$ of degree q^{2h}.

Proposition 3.3.2. *The fields listed in the previous discussion are all the cyclic extensions of $\mathbb{Q}(i)$ with the property of having degree q^h and discriminant divisible only by q.*

If we prove this Proposition, we have proved Takagi's Theorem for this case, since all the fields we are considering are lemniscate fields.

Proof. We first consider the case $h = 1$. Let ζ be a primitive root of unity of order q^2. The extension $\mathbb{Q}(i) \subseteq \mathbb{Q}(i, \zeta)$ is cyclic, and since $[\mathbb{Q}(i, \zeta) : \mathbb{Q}(i)] = q(q-1)$ we can consider the unique subfield $\widetilde{C}$ of $\mathbb{Q}(i, \zeta)$ which is a cyclic extension of $\mathbb{Q}(i)$ of degree q.

Claim 3.3.1. *$\widetilde{C}$ is actually one of the $q+1$ subfields of Q_1.*

Proof. Let us set $Z = \mathbb{Q}(i, \zeta)$. Suppose that $\tilde{C} \not\subset Q_1$, and choose $C \neq C'$ between the $q+1$ subfields of Q_1 of degree q. By considering the degree, we see that $Q_1 = CC'$. Moreover, since

$$[Z : \mathbb{Q}(i)] = q(q-1)$$

and

$$[Q_1 : \mathbb{Q}(i)] = q^2$$

it holds that $[Z \cap Q_1 : \mathbb{Q}(i)]$ must divide q. So if $Z \cap Q_1 \neq \mathbb{Q}(i)$, it would follow that $Z \cap Q_1 = \tilde{C}$, since the latter is the unique subfield of Z of degree q, contradicting the fact that $\tilde{C} \not\subset Q_1$. As a consequence

$$\mathbb{Q}(i) \subset Q_1(\zeta) = CC'(\zeta)$$

is a field extension of degree $q^3(q-1)$.
By [3], Lemma 3, Chapter III, p.87, we know that if $\eta = 1 - \zeta$ then $(\eta) = \mathfrak{q}$ is a prime ideal such that

$$q\mathcal{O}_Z = \mathfrak{q}^{q(q-1)}$$

Furthermore, since $Z \subset C(\zeta)$ is a cyclic extension satisfying the requests of Lemma (2.1.5), following the argument that we used in order to prove Proposition (3.3.1), we observe that there are $\chi, \theta \in Z$ such that

$$\begin{aligned} CZ &= C(\tau) = Z(\sqrt[q]{\chi}) \\ \bar{C}Z &= \bar{C}(\tau) = Z(\sqrt[q]{\theta}) \end{aligned}$$

and

$$\begin{aligned}\chi &\equiv 1 \bmod \mathfrak{q} \not\equiv 1 \bmod \mathfrak{q}^2\\ \theta &\equiv 1 \bmod \mathfrak{q} \not\equiv 1 \bmod \mathfrak{q}^2\end{aligned}$$

Copying what we did before, since $\mathfrak{q}$ is of degree 1 in the extension $\mathbb{Q}(i) \subseteq Z$ we can find $a, a', b, b' \in \mathbb{Z}$ such that $a + ib$ and $a' + ib'$ are not divisible by q and such that

$$\begin{aligned}\chi &\equiv 1 + (a + ib)\eta \bmod \mathfrak{q}^2\\ \theta &\equiv 1 + (a' + ib')\eta \bmod \mathfrak{q}^2\end{aligned}$$

Since for every $r \in \mathbb{Z}$ it holds that

$$\tau^r \equiv 1 - r\eta \bmod \mathfrak{q}^2$$

if we set

$$\rho = \tau^r \chi \theta^c$$

(where $r, c \in \mathbb{N}$ are arbitrary) we obtain, by direct computation,

$$\rho \equiv 1 + (u + iv)\eta \bmod \mathfrak{q}$$

where $u = a + ca' - r$ and $v = b + cb'$. At this point, we can choose c and r so that u and v are both divided by q, and consequently

$$\rho \equiv 1 \bmod \mathfrak{q}^2$$

From here, we can follow the argument used in the proof of Proposition (3.3.1) in order to find a contradiction: in fact $\mathbb{Q}(i) \subset CZ(\sqrt[q]{\rho}) \subset CC'(\zeta)$ is an extension of degree $q^2(q-1)$, and as before we can see that $\mathfrak{q}$ is not ramified there and that the ramification index of q is equal to $q(q-1)$, so that for the inertia field $D^T \subset CZ(\sqrt[q]{\rho})$ it holds that

$$[D^T : \mathbb{Q}(i)] = \frac{q^2(q-1)}{q(q-1)} = q$$

If now we consider the intersection $D^T \cap C$, because of the degree we can only have $D^T = C$ or $D^T \cap C = \mathbb{Q}(i)$.
In the first case, we immediately have a contradiction, because q ramifies in C and it is inert in D^T by definition. In the second case, note that

$$D^T \subset CZ(\sqrt[q]{\rho}) \subset CC'(\zeta)$$

thus the fact that $D^T \cap C = \mathbb{Q}(i)$ implies that $D^T \subset C'(\zeta)$. Consequently, $D^T \cap C' \neq \mathbb{Q}(i)$, because otherwise $D^T \subset Z$, but this is impossible because q is totally ramified in Z and inert in D^T which is not the trivial extension. Then considering again the degree we obtain that $D^T = C'$, and we conclude as in the first case: therefore $\tilde{C}$ must be contained in Q_1, as we wanted to prove. □

Now that we have proved this claim, we can continue with the proof of the Proposition.

Let $C \neq \widetilde{C}$ be another of the $q+1$ subfields of Q_1, and suppose that there is a cyclic extension $\mathbb{Q}(i) \subset \bar{C}$ of degree q whose discriminant is a power of q and which is not contained in Q_1. Our goal now is to show that also in this situation we can reproduce the argument used in the proof of Proposition (3.3.1) and in the previous Claim: in order to do so, let us prove that

$$Q_1\bar{C}(\tau) = C\bar{C}(\sqrt[q]{\tau})$$

where τ is a primitive q-th root of unity.
Clearly

$$[Q_1(\tau) : \mathbb{Q}(i)] = [Q_1 : \mathbb{Q}(i)](q-1) = q^2(q-1)$$

and at the same time

$$[C(\sqrt[q]{\tau}) : \mathbb{Q}(i)] = q[C(\tau) : \mathbb{Q}(i)] = q^2(q-1)$$

Note that $(\sqrt[q]{\tau})^{q^2} = 1$ so $\sqrt[q]{\tau}$ is a q^2-root of unity which is also primitive since τ is. Then in $C(\sqrt[q]{\tau})$ we can find all the q^2-th roots of unity, but the same holds for $Q_1(\tau)$, because in $\tilde{C} \subset Q_1$ we can find all the q^2-th roots of unity that are not q-th roots of the unity, and by adding τ we add all the q-th roots (which are clearly q^2-th roots too). Then, if we consider as before the field of q^2-th roots $Z = \mathbb{Q}(i, \zeta)$ we obtain, by considering the degree, that $CZ = Q_1(\tau)$ (C cannot be contained in Z because $\widetilde{C}$ is the unique field with that property, and looking at the degree we get that $C \cap Z = \mathbb{Q}(i)$) but at the same time $CZ = C(\sqrt[q]{\tau})$ for the same reasons, so $C(\sqrt[q]{\tau}) = Q_1(\tau)$ and hence $Q_1\bar{C}(\tau) = C\bar{C}(\sqrt[q]{\tau})$.
At this point, the proof becomes identical to the one we have used before (we only have minor adjustments to make) so for sake of brevity here we are proceeding a little faster than usual. Setting $\bar{Z} = \mathbb{Q}(i, \tau)$, if $\eta = 1 - \tau$ then $(\eta) = \mathfrak{q}$ is a prime ideal such that

$$q\mathcal{O}_Z = \mathfrak{q}^{q-1}$$

and arguing in the usual way we can find $\chi_2, \theta_2 \in \bar{Z}$ such that

$$\begin{aligned} C\bar{Z} &= C(\tau) = \bar{Z}(\sqrt[q]{\chi_2}) \\ \bar{C}\bar{Z} &= \bar{C}(\tau) = \bar{Z}(\sqrt[q]{\theta_2}) \end{aligned}$$

and

$$\begin{aligned} \chi_2 &\equiv 1 \bmod \mathfrak{q} \not\equiv 1 \bmod \mathfrak{q}^2 \\ \theta_2 &\equiv 1 \bmod \mathfrak{q} \not\equiv 1 \bmod \mathfrak{q}^2 \end{aligned}$$

Since $\mathfrak{q}$ is of degree 1 in the extension $\mathbb{Q}(i) \subseteq \bar{Z}$, as in the proof of the previous claim we can choose opportunely $c, r \in \mathbb{N}$ so that setting

$$\rho_2 = \tau^r \chi_2 \theta_2^c$$

we get

$$\rho_2 \equiv 1 \bmod \mathfrak{q}^2$$

Then the extension $\mathbb{Q}(i) \subset C\bar{Z}(\sqrt[q]{\rho_2})$ is such that

- its degree is equal to $q^2(q-1)$.
- $\mathfrak{q}$ is not ramified in $C\bar{Z}(\sqrt[q]{\rho_2})$.
- the ramification index of q is equal to $q-1$.
- the inertia field $D^T \subset C\bar{Z}(\sqrt[q]{\rho_2})$ has degree

$$[D^T : \mathbb{Q}(i)] = \frac{q^2(q-1)}{(q-1)} = q^2$$

If $D^T \cap C = \mathbb{Q}(i)$, since

$$D^T \subset C(\zeta)(\sqrt[q]{\rho_2}) \subseteq C\bar{C}(\sqrt[q]{\tau})$$

we get that $D^T \subset \bar{C}(\sqrt[q]{\tau})$, but this means that $D^T \cap \bar{C} \neq \mathbb{Q}(i)$, otherwise we would have $D^T \subset \bar{Z}(\sqrt[q]{\tau})$ which is impossible since

$$[\bar{Z}(\sqrt[q]{\tau}) : \mathbb{Q}(i)] = q(q-1) < q^2 = [D^T : \mathbb{Q}(i)]$$

Then $D^T \cap \bar{C} = \bar{C}$ because $[\bar{C} : \mathbb{Q}(i)]$ is prime, and this is a contradiction because q is ramified in $\bar{C}$ but not in its inertia field D^T. If at the contrary $D^T \cap C \neq \mathbb{Q}(i)$, we get $D^T \cap C = C$ and we conclude as above, hence $\bar{C}$ must be contained in Q_1 as we wanted to show, and the proof of the case $h = 1$ is completed.

Now we are left to prove the inductive step: consider is a field extension $\mathbb{Q}(i) \subset C$ with the required properties. By inductive hypothesis, the subfield $C_{h-1} \subset C$ of degree q^{h-1} must be contained in $Q_{h_1} \subset Q_h$ so we can find a fields $C' \subset Q_h$ with the required properties and such that $C \cap C' = C_{h-1}$ (we are supposing that $C \neq C'$, otherwise there is nothing to prove) and then

$$[CC' : \mathbb{Q}(i)] = \frac{[C : \mathbb{Q}(i)][C' : \mathbb{Q}(i)]}{[C \cap C' : \mathbb{Q}(i)]} = \frac{q^h q^h}{q^{h-1}} = q$$

Consequently as in Proposition (3.3.1) we can find a field extension $\mathbb{Q}(i) \subset L$ of degree q such that $CC' = C'L$. Then, q must be the only prime ramifying in L, so by induction $L \subset Q_1 \subset Q_h$ and finally

$$CC' = C'L \subset Q_h Q_1 \subset Q_h$$

which means that $C \subset Q_h$ as we wanted to prove. □

3.3.3 $p = 2$

Proposition 3.3.3. *Every cyclic extension $\mathbb{Q}(i) \subseteq C$ whose degree is a power of 2 and whose discriminant is a power of $1+i$ is a lemniscate extension.*

Proof. Consider the abelian extension $\mathbb{Q}(i) \subseteq D_4$ of degree 4 obtained by considering the $(1+i)^7$-division points of the lemniscate. As we saw in Theorem (2.3.1), this field is generated by the element y satisfying the equation

$$y^2 - 2ixy - 1 = 0$$

where

$$x^2 - 2x - 1 = 0$$

Then $D_4 = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{x}, i)$ with $x = 1 \pm \sqrt{2}$.
Let us set now $\alpha := \sqrt{2}+1$ and $\beta = \sqrt{2}-1$: α and β are in D_4, and so since

$$2(1 \pm i) = (\sqrt{\alpha} \pm i\sqrt{\beta})^2$$

also $\sqrt{1+i}, \sqrt{1-i} \in D_4$. Moreover, also $\sqrt{i} = \frac{\sqrt{1+i}}{\sqrt{1-i}} \in D_4$, hence

$$\mathbb{Q}(\sqrt{i}), \mathbb{Q}(\sqrt{i+1}), \mathbb{Q}(\sqrt{i-1}) \subseteq D_4$$

and those are all the quadratic extensions of $\mathbb{Q}(i)$ with discriminant which is a power of $1+i$. Hence the principle is true if we consider fields C of degree $[C : \mathbb{Q}(i)] = 2^h$ where $h = 1$. Then we can repeat the inductive proof used in the previous Propositions, and we are done.

□

Bibliography

[1] N.H. Abel, *Recherches sur les fonctions elliptiques*, J. Reine Angew. Math., Vol. 2 (1827), 101-181.

[2] N. H. Abel, *Recherches sur les fonctions elliptiques. (Suite du mmoire Nr.12., tom.II., cah. 2 de ce journal).*, J. Reine Angew. Math., Vol. 3 (1828), 160-196.

[3] J.W.S. Cassels, A. Frölich, eds., Algebraic Number Theory. *Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union*, Academic Press, London (1967).

[4] D. A. Cox, Galois Theory, Wiley & Sons, Hoboken, NJ USA, (2004).

[5] D. A. Cox, T. Hyde, *The Galois theory of the lemniscate*, J. Number Theor., Vol. 135,(Feb, 2014), 43-59.

[6] J. T. Cross, *The Euler φ-function in the Gaussian integers*, Amer. Math. Monthly, Vol. 90, No. 8 (Oct, 1983), 518-528.

[7] G. Dresden, W. Dymacek, *Finding Factors of Factor Rings over the Gaussian Integers*, Amer. Math. Monthly, Vol. 112, (Aug-Sep, 2005), 602–611.

[8] M. J. Greenberg, *An elementary proof of the Kronecker-Weber Theorem*, Amer. Math. Monthly, Vol. 81, 16 (1974), 601-607.

[9] D. Hilbert, The Theory of Algebraic Number Fields, Springer-Verlag, Berlin, (1998).

[10] A. Hurwitz, *Über die Entwicklungskoeffizienten der lemniscatischen Funktionen*, Mathematische Werke, Birkhäuser, Vol. 2, (1932) 342-373.

[11] K. Iwasawa, *On papers of Takagi in number theory*, Teji Takagi Collected Papers, Springer-Verlag, Tokyo, (1990), pp. 342-351.

[12] G. J. Janusz, Algebraic Number Fields,volume 7 of *Graduate Studies in Mathematics*,2nd ed., American Mathematical Society, Providence, RI, (1996).

[13] L. Kronecker, *Über die algebraisch auflösbaren Gleichungen*, Ber. Königl. Akad. Wiss., Berlin (1853).

[14] M. Rosen, *Abel's theorem on the lemniscate*, Amer. Math. Monthly 88, (1981), 387-395.

[15] C. L. Siegel, Topics in Complex Function Theory, Vol. 1, Wiley-Interscience, New York, (1969).

[16] I. Stewart, D. Tall, Algebraic Number Theory and Fermat's Last Theorem, 3rd ed., A K Peters, Natick, Massachussetts, (2002).

[17] T. Takagi, *Ueber die im Bereiche der rationalen complexen Zahlen Abel'schen Zahlkörpher*, J. Coll, Sci. Imp. Univ. Tokyo, Vol. XIX:5, (1903), 1-42.

[18] T. Takagi, *Über eine Theorie der relativ-Abel'schen Zahlkörper*, J. Coll, Sci. Imp. Univ. Tokyo, Vol. 41:9, (1920), 1-133.

[19] S. G. Vladut, Kronecker's Jugendtraum and Modular Functions, Gordon and Breach, Netherlands, (1991).

[20] E. T. Whittaker, G. N. Watson, A Course of Modern Analysis, 4th ed., Cambridge University Press (1927).

[21] O. Zariski, P. Samuel, Commutative Algebra, Vol. 1, Van Nostrand, Princeton, NJ USA, (1958).