

Georg-August-Universität Göttingen  
Fakultät für Mathematik und Informatik  
Mathematisches Institut  
Summer Term 2022

---

# Perfect numbers in the Eisenstein integers and sums of integral squares in quadratic extensions

---

JOHANN CHRISTIAN STUMPENHUSEN  
Master's Thesis

Student-ID: 21675783  
E-mail: j.stumpenhusen@stud.uni-goettingen.de  
M. Sc. Mathematik  
Worked on during the 2<sup>nd</sup> and 3<sup>rd</sup> terms of study  
Supervisor: Dr. Victoria Cantoral Farfán  
Co-supervisor: Prof. Dr. Frank Gounelas  
Handed in: 20 May 2022



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Perfect numbers in the Eisenstein integers . . . . .	2
1.2	Sums of integral squares in quadratic extensions . . . . .	3
<b>I</b>	<b>Perfect numbers in the Eisenstein integers</b>	<b>8</b>
<b>2</b>	<b>Perfect numbers in the rational integers</b>	<b>9</b>
2.1	Even perfect rational integers . . . . .	9
2.2	Odd perfect rational integers . . . . .	10
<b>3</b>	<b>Generalisation to cyclotomic fields</b>	<b>12</b>
3.1	The concept of odd and even in $\mathbb{Z}[\zeta_p]$ . . . . .	12
3.2	Perfect numbers in the Gaussian integers . . . . .	16
<b>4</b>	<b>Perfect numbers in the Eisenstein integers and cyclotomic fields of higher degree</b>	<b>20</b>
4.1	Even perfect Eisenstein integers . . . . .	22
4.2	Odd perfect Eisenstein integers . . . . .	28
4.3	Cyclotomic fields of higher degree . . . . .	30
<b>5</b>	<b>Generalisation to quadratic number fields</b>	<b>33</b>
5.1	Imaginary quadratic fields . . . . .	34
5.2	Real quadratic fields . . . . .	39
<b>II</b>	<b>Sums of integral squares in quadratic extensions</b>	<b>45</b>
<b>6</b>	<b>Sums of integral squares</b>	<b>46</b>
6.1	The counting function in cyclotomic fields . . . . .	48
6.2	Non-cyclotomic quadratic extensions . . . . .	53
<b>7</b>	<b>Prime numbers of the form <math>\alpha^2 + d\beta^2</math></b>	<b>56</b>
7.1	A short insight to class field theory . . . . .	57
7.2	The case of $d = 1$ . . . . .	59
7.3	The case of general square-free $d$ . . . . .	60



# Chapter 1

## Introduction

In this thesis, two different topics will be presented and discussed. The link between these two is what we commonly call algebraic number theory: the study of numbers which satisfy a monic polynomial with coefficients in  $\mathbb{Z}$ .

Throughout this work,  $K$  denotes an algebraic number field over the rational numbers, that is a finite algebraic extension of  $\mathbb{Q}$ . For any such  $K$ , the ring  $\mathcal{O}_K$  contains all the elements of  $K$  which satisfy a monic polynomial in  $\mathbb{Z}[x]$ , i.e. every  $\alpha \in K$  such that  $f(\alpha) = 0$  for some monic  $f \in \mathbb{Z}[x]$ . We call  $\mathcal{O}_K$  the *ring of integers* of  $K$  and its elements *algebraic integers* or *integers* of  $K$ . In order to avoid confusion, the elements of  $\mathbb{Z}$  are called *rational integers*.

We will be working with rings that have different groups of units and thus we will often make use of the following definition.

**Definition 1.0.1.** Let  $R$  be a ring and  $a, b \in R$  such that  $a = \varepsilon b$  for a unit  $\varepsilon \in R$ . Then we call  $a$  and  $b$  *associates* of each other and write  $a \simeq b$ .

In any algebraic number field, we may also define the norm function which gives us a sense of how large the residue ring of the ideal generated by the respective element is.

**Definition 1.0.2.** Let  $K$  be an algebraic number field and  $\alpha \in K$ . The *norm* of  $\alpha$  in  $K$  is

$$N_K(\alpha) = \prod_{\varphi \in \text{Gal}(\overline{K}/\mathbb{Q})} \varphi(\alpha)$$

where  $\overline{K}$  is an algebraic normal closure of  $K$  in the algebraic numbers  $\mathbb{A}$  and  $\text{Gal}(\cdot)$  denotes the GALOIS group of an extension.

For an ideal  $\mathfrak{a} \subset \mathcal{O}_K$ , we define its norm to be

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|,$$

the cardinality of its residue ring.

We know from basic algebraic number theory, that the norm of an algebraic integer is a rational integer. Closely related to the structure of the ideals of  $\mathcal{O}_K$  is the *ideal class group* of  $K$ .

**Definition 1.0.3.** Let  $K$  be a number field. We call  $\mathfrak{a} \subset K$  a fractional ideal of  $K$  if there is an  $\alpha \in \mathcal{O}_K$  such that  $\alpha\mathfrak{a} \subset \mathcal{O}_K$ . The set of (principal) fractional ideals is denoted by  $I_K$  ( $P_K$  resp.). We call

$$Cl(K) := I_K/P_K$$

the *ideal class group* of  $K$ . Its cardinality is the *class number* of  $K$ .

## 1.1 Perfect numbers in the Eisenstein integers

In the first part, we will generalise a concept which the reader may be familiar with to a certain class of algebraic fields. The sum-of-divisors-function  $\sigma$  is given for any natural number  $n$  by

$$\sigma(n) = \sum_{d|n} d \quad (1.1)$$

where  $d$  is a natural number. It adds up all the positive divisors of  $n$ . There is also an alternative form which we will use as a definition of the  $\sigma$ -function.

**Definition 1.1.1.** Let  $n = \prod_{p|n} p^{e_p}$  be a natural number with its decomposition into prime numbers  $p \in \mathbb{P}$ . We define

$$\sigma(n) = \prod_{p|n} \frac{p^{e_p+1} - 1}{p - 1}. \quad (1.2)$$

Using the fact that  $\sum_{k=0}^{e_p} p^k = \frac{p^{e_p+1} - 1}{p - 1}$  and the fundamental theorem of arithmetic shows that the two Equations 1.1 and 1.2 coincide.

Numbers satisfying certain properties based on their image under this function have already been studied by EUCLID (4<sup>th</sup>/3<sup>rd</sup> century BC) and the ancient Greeks. The interest they had in these numbers is clearly represented by the first term in the following definition.

**Definition 1.1.2.** A natural number  $n$  is called

- *perfect* if  $\sigma(n) = 2n$ ,
- *abundant* if  $\sigma(n) - 2n > 0$ , or
- *deficient* if  $\sigma(n) - 2n < 0$ .

The absolute value of the difference is called the *abundance* or *deficiency* of  $n$ , respectively.

**Example 1.1.3.** The smallest perfect number is 6 because

$$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6.$$

The smallest abundant number is 12, with abundance 4, because

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28 = 2 \cdot 12 + 4.$$

And the smallest deficient number is 1, with deficiency 1, because

$$\sigma(1) = 1 = 2 \cdot 1 - 1.$$

In particular, any proper multiple of a perfect or abundant number is abundant and any proper divisor of a perfect or deficient number is deficient.

Back in the days of the ancient Greeks, it was already known to them that there is a significant difference between the even and odd perfect natural numbers. That is, they were solely able to find even numbers of that kind.

**Theorem 1.1.4.** (EUCLID–EULER) An even natural number is perfect if and only if it is of the form  $2^{k-1}(2^k - 1)$  for some  $k \in \mathbb{N}$  such that  $2^k - 1$  is prime.

The *if*-direction was proven by EUCLID while the converse remained unknown until the Swiss mathematician LEONARD EULER (1707 – 1783 AD) proved it in 1747. EULER himself also stated a condition on the form of an odd perfect rational integer and further conditions have been added by the subsequent work of different mathematicians during the past centuries. However, not a single such number has been found yet and it is uncertain whether there are any.

In the 20<sup>th</sup> century, the concept of an even number was generalised to the ring of integers of some cyclotomic fields. A cyclotomic field is the splitting field of the polynomial  $x^n - 1$  and generated by a primitive  $n$ -th root of unity  $\zeta_n$ . In this thesis, we will focus especially on the primitive roots of unity  $\zeta_4 =: i$  and  $\zeta_3 =: \omega$ .

**Definition 1.1.5.** Let  $K = \mathbb{Q}(\zeta_p)$  for some  $p \in \mathbb{P}$  or  $p = 4$ . An element  $\alpha \in \mathcal{O}_K$  is called *even* if it is divisible by  $1 - \zeta_p$ . Otherwise, we call it *odd*.

This definition is even extendable to  $\mathbb{Q}$  which can be seen as  $\mathbb{Q}(\zeta_2)$  with  $\zeta_2 = -1$ . Then  $1 - \zeta_2 = 2$  gives us the familiar meaning of evenness in the rational integers.

SPIRA [26] and MCDANIEL [14] did this generalisation explicitly for the GAUSSIAN integers  $\mathbb{Z}[i]$ , named after CARL FRIEDRICH GAUSS (1777 – 1885 AD), being the ring of integers of  $\mathbb{Q}(i)$  and worked towards transferring the EUCLID–EULER Theorem to the GAUSSIAN integers via a generalisation of the  $\sigma$ -function. The latter succeeded in doing so whereas PARKER, RUSHALL, and HUNT [34], who tried the same for the EISENSTEIN integers  $\mathbb{Z}[\omega]$ , named after GOTTHOLD EISENSTEIN (1823 – 1852 AD), only managed to find an even so-called *norm-perfect* integer which will be defined in Chapter 2.

We will refine the results by PARKER et al. and also state a theorem on the form of an odd perfect EISENSTEIN integer, using a helpful paper published by WARD [30]. The work on perfect integers in the rational, GAUSSIAN, and EISENSTEIN integers is briefly summarised in the following table.

Ring	Even norm-perfect integers	Odd norm-perfect integers (form)
$\mathbb{Z}$	EUCLID and EULER	EULER
$\mathbb{Z}[i]$	MCDANIEL [14]	WARD [30]
$\mathbb{Z}[\omega]$	PARKER et al. [34] and this thesis	this thesis
$\mathbb{Z}[\zeta_p], p \geq 5$	conjectured in this thesis	this thesis

Table 1.1: Summary of the work on norm-perfect integers in cyclotomic fields

The first part of this thesis will be concluded with an excursion to other quadratic extensions  $K/\mathbb{Q}$  and discuss possible perfect numbers therein.

## 1.2 Sums of integral squares in quadratic extensions

The second part of this thesis concentrates on the representation of algebraic integers in a number field  $K$  as sums of squares of algebraic integers of that same field, i.e. of integral squares. One of the most notable results is a theorem, conjectured by ALBERT GIRARD (1595 – 1632 AD) in 1625 and proven by EULER in 1755.

**Theorem 1.2.1.** For any positive rational prime  $p$ , there exist  $x, y \in \mathbb{Z}$  such that

$$p = x^2 + y^2$$

if and only if  $p \not\equiv 3 \pmod{4\mathbb{Z}}$ .

Since there are primes  $p \in \mathbb{P}$  with  $p \equiv 3 \pmod{4\mathbb{Z}}$ , the question about the smallest  $k \in \mathbb{N}$  such that every natural number can be represented as sum of  $k$  squares arose. In 1770, JOSEPH LOUIS LAGRANGE (1736 – 1813 AD) presented a proof for the following infamous theorem.

**Theorem 1.2.2.** (LAGRANGE's Four-Square-Theorem) For any  $n \in \mathbb{N}$ , there exist

$$w^2 + x^2 + y^2 + z^2 = n$$

with  $w, x, y, z \in \mathbb{Z}$ .

Similarly to the question of perfect numbers, this may be transferred to the ring of integers of any algebraic number field. Before heading on in this direction, we state an often used definition.

**Definition 1.2.3.** Let  $K$  be a number field.

1. Any embedding  $\sigma : K \rightarrow \mathbb{C}$  is called *real* if  $\sigma(K) \subset \mathbb{R}$ .
2. An element  $\alpha \in K$  such that  $\sigma(\alpha) > 0$  for all real embeddings  $\sigma$  of  $K$  is called *totally positive*.

Note that, if  $K$  does not admit any real embedding, every element of  $K$  is totally positive.

In 1921, CARL SIEGEL (1896 – 1981 AD) proved a theorem, conjectured by DAVID HILBERT (1862 – 1943 AD) in 1902.

**Theorem 1.2.4.** [25] Let  $K$  be a number field and  $\alpha \in \mathcal{O}_K$  be totally positive. Then there exist

$$w^2 + x^2 + y^2 + z^2 = \alpha$$

with  $w, x, y, z \in K$ .

We may rejoice, seeing that LAGRANGE's Theorem can be transferred in such a direct manner. Unfortunately, this generalisation has two restrictions: It only holds for totally positive  $\alpha$  and the squares may not be integral. Nevertheless, there has been a lot of work towards generalising the statement where the negative of the latter condition holds. A particular interesting work was published by IVAN M. NIVEN (1915 – 1999 AD) [20], dealing with the case of quadratic fields.

**Theorem 1.2.5.** [20] Let  $K = \mathbb{Q}(\sqrt{d})$  be a quadratic extension of  $\mathbb{Q}$  with a square-free rational integer  $d < 0$ .

1. If  $d \not\equiv 1 \pmod{4}$ , then an integer  $a + b\sqrt{d} \in \mathcal{O}_K$ ,  $a, b \in \mathbb{Z}$  is expressible as sum of three integral squares if and only if  $2 \mid b$ .
2. If  $d \equiv 1 \pmod{4}$ , then every integer in  $\mathcal{O}_K$  is expressible as sum of three integral squares.



Interestingly, NIVEN also stated necessary and sufficient conditions for integers of real quadratic fields to be expressible as sum of four or five integral squares but we will focus on the representation counting function of LAGRANGE's Theorem and its pendant in the imaginary quadratic extensions.

**Definition 1.2.6.** For  $k, n \in \mathbb{N}, k \neq 0$ , we define  $r_k(n)$  to be the number of representations of  $n$  as sum of  $k$  squares, i.e.

$$r_k(n) = \left| \left\{ (x_1, \dots, x_k) \in \mathbb{Z}^k : \sum_{j=1}^k x_j^2 = n \right\} \right|.$$

In particular, a representation  $(x_1, \dots, x_k)$  is different from  $(x_k, x_1, \dots, x_{k-1})$ .

In complex extensions, squares may have almost any angle with respect to the positive real line. In order to properly work with this, a certain notation is needed.

**Definition 1.2.7.** Let  $K$  be a number field and  $k \in \mathbb{N}_{\geq 1}$ . Then define

$$\mathfrak{Q}(K) = \{x^2 : x \in K\}$$

the set of squares of  $K$  and

$$\mathfrak{Q}'(K) = \{x^2 : x \in \mathcal{O}_K\}$$

the set of integral squares of  $K$ . Similarly, let  $\mathfrak{R}(K)$  be the set of finite sums of elements in  $\mathfrak{Q}(K)$  and  $\mathfrak{R}'(K)$  the set of finite sums of elements in  $\mathfrak{Q}'(K)$ .

We may now turn to the counting function.

**Definition 1.2.8.** Let  $K$  be a number field and  $k \in \mathbb{N}_{\geq 1}$ . Then define

$$r_{k,K} : \mathcal{O}_K \rightarrow \mathbb{N} \cup \{\infty\}$$

such that  $r_{k,K}(\alpha)$  is the number of representations of  $\alpha$  as sum of  $k$  elements of  $\mathfrak{Q}'(K)$ , i.e.

$$r_{k,K}(\alpha) = \left| \left\{ (x_1, \dots, x_k) \in \mathcal{O}_K^k : \sum_{j=1}^k x_j^2 = \alpha \right\} \right|,$$

similar to above.

Note that  $r_k(s) = r_{k,\mathbb{Q}}(s)$  for all  $s \in \mathbb{Z}$ . We immediately see that  $\mathfrak{R}'(K)$  is the set of integers  $\alpha$  in  $K$  for which there is a  $k_\alpha \in \mathbb{N}$  such that  $r_{k_\alpha,K}(\alpha) > 0$ . We will study these functions for certain  $k$  and  $K$  and present some interesting observations.

Lastly, the Theorem 1.2.1 reminds us of certain other ways to express primes as sums of squares. It may be regarded as a special case of the equation

$$p = x^2 + dy^2 \tag{1.3}$$

with  $p \in \mathbb{P}$ ,  $x, y \in \mathbb{Z}$  and  $d \in \mathbb{N}$ . Such a representation of a rational prime is closely related to the structure of the ring  $\mathbb{Z}[\sqrt{-d}]$  via the decomposition of

$$x^2 + dy^2 = (x + y\sqrt{-d})(x - y\sqrt{-d}).$$

For  $d \in \{2, 3\}$ , the ancient Greeks knew the solutions. However, the solubility of the factorisation of the right-hand side heavily depends on two properties of  $\mathbb{Z}[\sqrt{-d}]$ : Is it

the ring of integers of a number field and is it a UFD? If the answer is positive for both questions, the rational positive primes  $p$  for which Equation 1.3 has a solution in the rational integers are simply those who split in  $\mathbb{Z}[\sqrt{-d}]$ . But this holds only true for a few  $d$ , the most prominent obstacle being  $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \neq \mathbb{Z}[\sqrt{-d}]$  for  $d \equiv 3 \pmod{4\mathbb{Z}}$ . A huge break-through occurred with the publication of *Primes of The Form  $x^2 + ny^2$*  by DAVID COX, solving the question for all  $d \in \mathbb{N}$ .

We will transfer Equation 1.3 to certain quadratic extensions  $K$  of the rational numbers, namely those with class number 1. Our solutions will come from  $\mathcal{O}_K$ , leading us to investigate the ring  $\mathcal{O}_K[\sqrt{-d}]$  and finding a pendant of COX's main theorem.

**Theorem 1.2.9.** Let  $n \equiv 1 \pmod{4\mathbb{Z}}$  a square-free natural number such that  $K = \mathbb{Q}(\sqrt{n})$  is a real quadratic field of class number 1. Let  $d > 0$  be a square-free natural number with  $d \equiv 2 \pmod{4\mathbb{Z}}$  and coprime to  $n$ . Let  $p$  be an odd natural prime below the prime ideal  $\mathfrak{p} = \langle \psi \rangle \subset \mathcal{O}_K$ . Then there is a monic irreducible polynomial  $f_{n,d} \in \mathcal{O}_K[t]$  such that if  $p$  divides neither  $d$  nor the discriminant of  $f_{n,d}$ , then

$$\psi = \alpha^2 + d\beta^2 \iff \begin{cases} \text{either } \left(\frac{-d}{p}\right) = 1 \text{ or } \left(\frac{-d}{p}\right) = \left(\frac{n}{p}\right) = -1 \\ \text{and } f_{n,d}(t) \equiv 0 \pmod{\mathfrak{p}} \text{ has an integer solution.} \end{cases}$$

Furthermore,  $f_{n,d}$  may be taken to be the minimal polynomial of a real algebraic integer  $\alpha$  for which  $H = L(\alpha)$  is the HILBERT class field of the CM-field  $L = K(\sqrt{-d})$ .



# Part I

## Perfect numbers in the Eisenstein integers

# Chapter 2

## Perfect numbers in the rational integers

In this chapter, we will briefly recollect some facts about the sum-of-divisors-function that have been known for some time. Elementary number theory tells us that the  $\sigma$ -function as defined in Definition 1.1.1 is multiplicative, i.e.  $\sigma(mn) = \sigma(m)\sigma(n)$  for any coprime  $m, n \in \mathbb{N}$  and  $\sigma(\varepsilon) = 1$  for any unit  $\varepsilon$ . It feels natural to extend this function to the ring of rational integers by defining  $\sigma(-n) = \sigma(n)$ . A negative number is called perfect, abundant, or deficient if its positive associate fulfils the respective property.

### 2.1 Even perfect rational integers

We restate the EUCLID–EULER Theorem and present EULER’s proof.

**Theorem 2.1.1.** (Theorem 1.1.4, EUCLID–EULER) An even natural number is perfect if and only if it is of the form  $2^{k-1}(2^k - 1)$  for some  $k \in \mathbb{N}$  such that  $2^k - 1$  is prime.

*Proof.* Let  $2^k - 1$  be prime. Obviously, it is odd, so

$$\sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)2^k$$

and we see that  $2^{k-1}(2^k - 1)$  is perfect.

Conversely, suppose  $n = 2^{k-1}x$  is a perfect natural number with  $x$  odd and  $k \geq 2$ . As  $n$  is perfect, we have

$$2^k x = 2n = \sigma(n) = \sigma(2^{k-1})\sigma(x) = (2^k - 1)\sigma(x)$$

Since  $2^k - 1$  is odd, it has to divide  $x$ , say  $(2^k - 1)y = x$  for a  $y \in \mathbb{N}$ . We divide the left most and right most term by  $2^k - 1$  to get

$$2^k y = \sigma(x) = x + y + z = 2^k y + z$$

where  $z$  is the sum of the remaining divisors of  $x$ . Comparing both sides yields  $z = 0$  and consequently  $y = 1$ . Thus,  $x = 2^k - 1$  is a prime.  $\square$

**Definition 2.1.2.** The numbers  $2^k - 1$  for  $k \in \mathbb{N}$  are called MERSENNE numbers.

These numbers are named after the French monk MARIN MERSENNE (1588 – 1648 AD) who studied those numbers while searching for large prime numbers. MERSENNE primes are still among the largest known prime numbers. A necessary condition for such a number to be prime is that  $k$  is prime itself. However, this is not sufficient as we may see by the example

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

The Theorem 1.1.4 solved the question of the form of even perfect natural numbers and proved that there is a bijection between these numbers and MERSENNE primes. It does not make any statement about the amount of such numbers. Presently, the *Great Internet Mersenne Prime Search* [15], abbreviated GIMPS, is working on testing several large MERSENNE numbers on primality. Since 1996, GIMPS has increased the number of known MERSENNE primes from 34 to 51, the largest so far being  $2^{82,589,933} - 1$ . Proving by brute force that so great a number is prime is very inefficient. Fortunately, there has been an effective primality test for MERSENNE primes, the LUCAS–LEHMER test, named after the french mathematician ÉDOUARD LUCAS (1842 – 1891 AD) and the U.S.-american mathematician DERRICK HENRY LEHMER (1905 – 1991 AD). The test uses properties of the ring  $\mathbb{Z}[\sqrt{3}]$  and the author recommends that the interested reader has a look into it (see [here](#)).

## 2.2 Odd perfect rational integers

The question of the last section can be regarded as completely solved, meanwhile the odd perfect rational integers are an open problem. Over the last few decades, there has been a significant progress towards the form which such a number can have. Noteworthy contributions have been made by NIELSEN [19] and OCHEM and RAO [21] who provided an upper (based on the number of prime factors) and an unconditional lower bound for any odd perfect rational integer. Some other authors proved a lower bound for the amount of prime divisors of odd perfect rational integers. For the purpose of this thesis, we will focus on the theorem EULER himself stated.

**Theorem 2.2.1.** (EULER) Let  $n$  be an odd perfect natural number. Then

$$n = p^k q^2$$

for some prime  $p \in \mathbb{P}$  and odd natural number  $q$ . Moreover,  $p \equiv k \equiv 1 \pmod{4\mathbb{Z}}$  and  $\langle p, q \rangle = \mathbb{Z}$ .

In order to prove this, we will provide another lemma first.

**Lemma 2.2.2.** Let  $p$  be an odd natural prime.

1. If  $m$  is even, then  $\sigma(p^m) \equiv 1 \pmod{2\mathbb{Z}}$ .
2. If  $m \equiv p \equiv 1 \pmod{4\mathbb{Z}}$ , then  $\sigma(p^m) \equiv 2 \pmod{4\mathbb{Z}}$ .
3. Otherwise,  $\sigma(p^m) \equiv 0 \pmod{4\mathbb{Z}}$ .

*Proof.* Recall that  $\sigma(p^m) = \sum_{k=0}^m p^k$ .

1. Every power of  $p$  is odd and a sum of an odd number of odd integers is odd.

2. If  $p \equiv 1 \pmod{4\mathbb{Z}}$ , then each power  $p^k \equiv 1 \pmod{4\mathbb{Z}}$ . Hence,

$$\sigma(p^m) \equiv m + 1 \equiv 2 \pmod{4\mathbb{Z}}$$

since  $m \equiv 1 \pmod{4\mathbb{Z}}$ .

3. This leaves the cases where at least one amongst  $p$  and  $m$  has to be congruent to 3 modulo  $4\mathbb{Z}$ .

If  $p \equiv 1 \pmod{4\mathbb{Z}}$ , we easily see by comparing this with the second bullet that  $\sigma(p^m) \equiv 0 \pmod{4\mathbb{Z}}$  since  $m \equiv 3 \pmod{4\mathbb{Z}}$ .

If  $p \equiv 3 \pmod{4\mathbb{Z}}$ , then each pair of consecutive powers of  $p$  satisfies  $p^{k-1} + p^k \equiv 3 + 1$  or  $\equiv 1 + 3 \pmod{4\mathbb{Z}}$ . Additionally,

$$\sigma(p) = 1 + p \equiv 1 + 3 \equiv 0 \pmod{4\mathbb{Z}}.$$

This covers all the cases. □

*Proof of Theorem 2.2.1.* Due to the multiplicativity of the  $\sigma$ -function, we may factorise

$$\sigma(n) = \prod_{k=0}^s \sigma(p_k^{e_k})$$

where the product is over the prime factors of  $n = \prod_{k=0}^s p_k^{e_k}$ . As  $n$  is perfect and odd, we get

$$\prod_{k=0}^s \sigma(p_k^{e_k}) = 2n \equiv 2 \pmod{4\mathbb{Z}}.$$

Therefore, none of the prime divisors of  $n$  may satisfy the third case of Lemma 2.2.2 and exactly one satisfies the second case. All the others have to appear with an even power. In total, this yields the claimed form. □

While dealing with odd perfect numbers in other rings of integers we will copy the basic strategy of this proof and, especially, deduce counterparts to Lemma 2.2.2.

# Chapter 3

## Generalisation to cyclotomic fields

Before defining what it means for an algebraic integer to be perfect, we need to think about what the  $\sigma$ -function is supposed to express. In the rational integers, it symbolises the accumulated size of all divisors of an integer. In order to conserve a somewhat constant ratio between the sizes of elements which we will deem interchangeable in some way, i.e. associates, we will restrict ourselves to the cyclotomic fields  $\mathbb{Q}(\zeta_n)$  where  $\zeta_n$  is an  $n$ -th root of unity. Their ring of integers is given by  $\mathbb{Z}[\zeta_n]$ .

### 3.1 The concept of odd and even in $\mathbb{Z}[\zeta_p]$

The second property we need to address regarding the  $\sigma$ -function is that in the naive definition on the natural numbers (and their extension to the rational integers) we constrain the sum to positive divisors. However, the cyclotomic fields over  $\mathbb{Q}$  are complex extensions and hence, we do not really have a sense of positivity, not even in  $\mathbb{Z}[\zeta_n]$ . Aiming towards creating something of that kind, we restrict the set of fields we want to work on even further: We only consider cyclotomic fields  $K = \mathbb{Q}(\zeta_p)$  where  $p \in \mathbb{P}$  is a natural prime or  $p = 4$  and  $\mathcal{O}_K$  is a UFD. We will call this set  $\mathcal{R}$ . The set of primes of an algebraic number field  $K$  will be denoted by  $\mathbb{P}_K$ .

**Definition 3.1.1.** Let  $K = \mathbb{Q}(\zeta_p) \in \mathcal{R}$ . A prime  $\psi \in \mathcal{O}_K$  is *positive* if its angle with respect to the positive real line is smaller than any of its associates' and, if  $p \neq 3, 4$ , its absolute value in  $\mathbb{C}$  is the smallest such that  $|\psi| \geq \sqrt[p-1]{N_K(\psi)}$ . An integer  $\alpha$  of  $K$  is *positive* if it is the product of positive primes. We denote the sets of positive primes or integers by  $\mathbb{P}_K^+$  or  $\mathcal{O}_K^+$ , respectively.

We note that this is—again—coherent with  $\mathbb{Q}$  being the field containing the second root of unity. The additional condition for  $p \neq 3, 4$  is due to  $\mathbb{Z}[\zeta_p]$  containing an infinite group of units. It is also clearly different from the definition of being totally positive. Moreover, every non-zero integer has exactly one positive associate so that we can easily define a function that yields the same value for different associates just based on the positive integers of  $K$ . We point out that the choice of our positive set  $\mathbb{P}_K^+$  is completely arbitrary, any representative system of the associate equivalence class may be chosen. Since  $\mathcal{O}_K$  is a UFD, the following definition makes sense and extends the  $\sigma$ -function to the integers of  $K$ . It is inspired by the works by SPIRA [26], MCDANIEL [14], and PARKER et al. [34].



**Definition 3.1.2.** Let  $K \in \mathcal{R}$ . Let  $\alpha = \prod_{k=1}^l \pi_k^{e_k}$  be a positive integer in  $\mathcal{O}_K$  and  $\pi_k \in \mathbb{P}_K^+$  for all  $k$ . We define the *sum-of-divisors-function* of  $K$  as

$$\sigma_K(\alpha) = \prod_{k=1}^l \frac{\pi_k^{e_k+1} - 1}{\pi_k - 1}.$$

Furthermore, any associate of  $\alpha$  has the same value under  $\sigma_K$ . Additionally, we set  $\sigma_K(0) = 0$ .

If the ring of integers is not a UFD, this definition is not well-defined. The most common example for such a ring of integers is  $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$  where the irreducible elements  $1 \pm \sqrt{-5}$ , 2, and 3 are not prime. Nevertheless, there is still a way to define the  $\sigma$ -function on a field  $K$  reasonably, done so by the author in a previous work [27] where it depends on the size of the divisors of the ideal generated by the argument. The definition we use has the advantage that  $\sigma_K(q) = \sigma(q)$  for any rational prime  $q \in \mathbb{P}$  that is prime in  $\mathbb{Z}[\zeta_p]$ , too.

The  $\sigma$ -function on the natural numbers has the property that  $\sigma(n) \geq n$  for all  $n \in \mathbb{N}$ . We will now investigate why the choice we made for  $\mathcal{O}_K^+$  is advantageous. The following lemma was proven by SPIRA [26].

**Lemma 3.1.3.** (SPIRA) Let  $K \in \{\mathbb{Q}, \mathbb{Q}(\zeta_3), \mathbb{Q}(\zeta_4)\}$  and  $\alpha \in \mathcal{O}_K$ . We have

$$N_K \left( \frac{\alpha^{n+1} - 1}{\alpha - 1} \right) \geq N_K(\alpha^n)$$

if  $\Re(\alpha) \geq 1$  and  $\bar{\alpha} \neq 0$ .

*Proof.* Firstly, recall that both sides are rational integers and the norm is the absolute value (if  $K = \mathbb{Q}$ ) or its square (otherwise). It is

$$N_K \left( \frac{\alpha^{n+1} - 1}{\alpha - 1} \right) > N_K \left( \frac{\alpha^{n+1} - 1}{\alpha} \right) \geq N_K(\alpha^n) - \frac{1}{N_K(\alpha)}$$

where the second term of the right-hand side is between 0 and 1, so we may neglect it if we substitute  $>$  by  $\geq$ .  $\square$

Taking the differences we encountered in the previous chapter into account, it may seem fit to generalise the concept of *odd* and *even* to other rings of integers. For this purpose, we recall some definitions and basic statements from elementary algebraic number theory. These may be found in one of KOCH's books [10], for example.

**Lemma 3.1.4.** Let  $K$  be a number field.  $\mathcal{O}_K$  is a DEDEKIND domain, i.e. each ideal factorises into a unique decomposition of prime ideals.

**Definition 3.1.5.** Let  $K$  be as above and  $p \in \mathbb{P}$  a natural prime. Decompose  $p\mathcal{O}_K = \prod_{k=1}^g \mathfrak{p}_k^{e_k}$  into prime ideals  $\mathfrak{p}_k$  of  $\mathcal{O}_K$ .  $p$  is said to

1. *ramify* if there is a subscript  $k$  such that  $e_k > 1$ .
2. *split* if  $g > 1$ .
3. be *inert* if there is a subscript  $k$  such that the cardinality of  $\mathcal{O}_K/\mathfrak{p}_k$  is divisible by  $p^2$ .

If exactly one of the cases applies to  $p$ , we say that  $p$  totally ramifies, totally splits, or is totally inert in  $K$ .

We recall the next lemma from any elementary algebraic number theory course.

**Lemma 3.1.6.** Let  $K/\mathbb{Q}$  be a GALOIS extension and  $p\mathcal{O}_K = \prod_{k=1}^g \mathfrak{p}_k^{e_k}$  a decomposition into prime ideals of  $\mathcal{O}_K$ . Then there exist  $e, f \in \mathbb{N}$  such that  $e_k = e$  and  $N(\mathfrak{p}_k) = f$  for any  $1 \leq k \leq g$  and  $efg = [K : \mathbb{Q}]$ .

It follows one more definition and a few helpful statements which lead us to a well-chosen sense of *odd* and *even* in  $\mathcal{O}_K$ .

**Definition 3.1.7.** Let  $K$  be a number field and  $\{\alpha_1, \dots, \alpha_n\}$  a basis of  $\mathcal{O}_K$  over  $\mathbb{Z}$ . The *discriminant* of  $K$  is

$$\Delta_K = \det \begin{pmatrix} \varphi_1(\alpha_1) & \varphi_2(\alpha_1) & \dots & \varphi_n(\alpha_1) \\ \varphi_1(\alpha_2) & \varphi_2(\alpha_2) & \dots & \varphi_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(\alpha_n) & \varphi_2(\alpha_n) & \dots & \varphi_n(\alpha_n) \end{pmatrix}^2$$

where  $\varphi_1, \dots, \varphi_n$  are the embeddings of  $K$  into  $\mathbb{C}$ .

**Lemma 3.1.8.** Let  $K$  be any number field.

1. It is  $\Delta_K \in \mathbb{Z}$  and
2. A natural prime  $p \in \mathbb{P}$  ramifies in  $K$  if and only if  $p$  divides  $\Delta_K$  in  $\mathbb{Z}$ . (DEDEKIND)

Computing the discriminant of  $K = \mathbb{Q}(\zeta_p)$  for a natural prime  $p$  yields

$$\Delta_K = (-1)^{\frac{p-1}{2}} p^{p-2}$$

and for  $p = 4$ , we have

$$\Delta_K = -4.$$

This implies that  $p$  or  $2$  (in the case of  $p = 4$ ) is the only prime ramifying in  $K$ . Another helpful tool to find the explicit decomposition of the ideal  $p\mathcal{O}_K$  is the following theorem. The reader may be familiar with another form of this statement but we will use this one as it perfectly fits our requirements.

**Theorem 3.1.9.** (DEDEKIND–KUMMER)[22, p. 46] Let  $K = \mathbb{Q}(\alpha)$  be a number field and  $p \in \mathbb{P}$ , such that  $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ . Let  $f \in \mathbb{Z}[x]$  be the minimal polynomial of  $\alpha$  and  $\bar{f} \equiv f \pmod{p\mathbb{Z}}$ . Additionally, let

$$\bar{f} = \bar{f}_1^{e_1} \dots \bar{f}_r^{e_r}$$

for some  $r \in \mathbb{N}$  be the decomposition of  $\bar{f}$  in pairwise coprime, irreducible, monic polynomials in  $\mathbb{F}_p[x]$ . For any  $i$ , choose an  $f_i \in \mathbb{Z}[x]$ , such that  $\bar{f}_i \equiv f_i \pmod{p\mathbb{Z}}$ , and denote by  $\mathfrak{p}_i$  the ideal  $\langle p, f_i(\alpha) \rangle \subset \mathcal{O}_K$ . Then, it holds that

$$\langle p \rangle = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$$

in  $\mathcal{O}_K$  and  $N(\mathfrak{p}_i) = p^{\deg f_i}$ .

Using the DEDEKIND–KUMMER Theorem, we get

$$p\mathcal{O}_K = \langle 1 - \zeta_p \rangle^{p-1}$$

where  $\langle 1 - \zeta_p \rangle$  is, indeed, a prime ideal of  $\mathcal{O}_K$ , so  $p$  totally ramifies. We also compute  $N_K(1 - \zeta_p) = p$ . As we already defined what it means for a prime to be positive in  $\mathcal{O}_K$ , we now finally choose  $\zeta_p$  explicitly.

**Definition 3.1.10.**  $\zeta_p$  is the primitive  $p$ -th root of unity such that  $1 - \zeta_p$  is positive.

For any other prime, we may use the following lemma for computing the norm of the prime ideals above it after recalling that the norm  $N(\mathfrak{a})$  of an ideal  $\mathfrak{a}$  is equal to the norm of its generator if  $\mathcal{O}_K$  is a PID.

**Lemma 3.1.11.** Let  $p, q \in \mathbb{P}$ ,  $p \neq q$ , be positive rational primes and  $\mathfrak{Q} \supset \langle q \rangle$  a prime ideal in  $K = \mathbb{Q}(\zeta_p)$ . Then  $N(\mathfrak{Q}) = q^f$  where  $f$  is the order of  $q$  in  $(\mathbb{Z}/p\mathbb{Z})^*$ .

*Proof.* Because of DEDEKIND–KUMMER, we consider the equation

$$x^p - 1 \equiv 0 \pmod{q\mathbb{Z}}$$

since any of its irreducible factors other than  $x - 1$  is an irreducible factor of  $g := \sum_{k=0}^{p-1} x^k \pmod{q\mathbb{Z}}$  which is the reduction of the minimal polynomial of  $\zeta_p$ . Let  $F$  be the smallest extension of  $\mathbb{F}_q$  such that it contains all the roots of  $x^p - 1$ , say  $F = \mathbb{F}_{q^f}$ . By LAGRANGE'S Theorem about the order of an element, it is  $p \mid q^f - 1$  and hence,  $q^f \equiv 1 \pmod{p\mathbb{Z}}$ . As  $F$  is the smallest such extension, we also deduce that  $f$  is the smallest positive integer satisfying that congruence condition. Thus, each irreducible factor of  $g$  has degree  $f$  and it follows  $N(\mathfrak{Q}) = q^f$ .  $\square$

For any positive rational prime  $q < p$ , we have  $q > 1$  and thus  $q^f > p$  if  $q^f \equiv 1 \pmod{p}$ . Hence, we may say that  $1 - \zeta_p$  is the non-unit of minimal norm because the norm is a multiplicative function. Moreover, we see that the norm only takes values being  $\equiv 0, 1 \pmod{p\mathbb{Z}}$  because each prime element has norm satisfying that congruence condition as we saw above. In combination with the fact that the prime ideals of  $\mathcal{O}_K$  are exactly the prime ideals we derive from the decomposition of the prime ideals of  $\mathbb{Z}$  in  $\mathcal{O}_K$ , we deduce the following lemma.

**Lemma 3.1.12.** Let  $K = \mathbb{Q}(\zeta_p) \in \mathcal{R}$  and  $p \neq 4$ . An element  $\alpha \in \mathcal{O}_K$  is even if and only if its norm is divisible by  $p$ . If  $p = 4$ ,  $\alpha$  is even if and only if its norm is even in  $\mathbb{Z}$ .

*Proof.*  $1 - \zeta_p$  is the only prime up to associates that has norm  $p$  if  $p \neq 4$ . Otherwise,  $1 + i$  is the only prime of norm 2.  $\square$

The concept of evenness in any field  $K \in \mathcal{R}$  is established, so we may now advance to the main definition of Part I following the equivalent definitions presented by MCDANIEL [14] and PARKER et al. [34].

**Definition 3.1.13.** Let  $K = \mathbb{Q}(\zeta_p) \in \mathcal{R}$  and  $\alpha \in \mathcal{O}_K$ . We call  $\alpha$

1. *perfect* if  $\sigma_K(\alpha) = (1 - \zeta_p)\alpha$  or
2. *norm-perfect* if  $N_K(\sigma_K(\alpha)) = N_K(1 - \zeta_p)N_K(\alpha)$ .

For the sake of completeness, we will also establish that  $\alpha$  is

3. *abundant* if  $N_K(\sigma_K(\alpha)) > N_K(1 - \zeta_p)N_K(\alpha)$  or
4. *deficient* if  $N_K(\sigma_K(\alpha)) < N_K(1 - \zeta_p)N_K(\alpha)$ .

Giving this a moment's thought, we notice that this extends to the case where  $K = \mathbb{Q}$  because  $\mathbb{Q} = \mathbb{Q}(\zeta_2)$ . Moreover, every perfect integer is also norm-perfect. However, we have to be aware that the set of (norm-)perfect integers depends on our choice of the set  $\mathbb{P}_K^+$ .

Lastly, we want to generalise the MERSENNE numbers.

**Definition 3.1.14.** Let  $K = \mathbb{Q}(\zeta_p) \in \mathcal{R}$ . We call the numbers  $(1 - \zeta_p)^k - 1$  with  $k \in \mathbb{N}$  the MERSENNE numbers of  $K$ .

We generalise a result from the rational MERSENNE numbers to any field  $K \in \mathcal{R}$ .

**Lemma 3.1.15.** If  $(1 - \zeta_p)^k - 1$  with  $k \in \mathbb{N}_{\geq 2}$  is prime, then  $k$  is a rational prime.

*Proof.* Suppose  $k$  is not prime, i.e.  $k = mn$  with  $m, n \in \mathbb{N}_{\geq 2}$ . Then

$$\begin{aligned} (1 - \zeta_p)^k - 1 &= [(1 - \zeta_p)^m]^n - 1 \\ &= [(1 - \zeta_p)^m - 1] \sum_{j=0}^{n-1} (1 - \zeta_p)^{mj}. \end{aligned}$$

As  $m \geq 2$ , we have that the left factor is not a unit. Moreover, as  $n \geq 2$ , we have  $m < k$ , so  $(1 - \zeta_p)^m - 1 \not\equiv (1 - \zeta_p)^k - 1$ .  $\square$

In the case of the GAUSSIAN and EISENSTEIN MERSENNE numbers, BERRIZBEITIA and ISKRA [1] presented primality tests similar to the LUCAS–LEHMER test for the rational MERSENNE numbers.

## 3.2 Perfect numbers in the Gaussian integers

One of the most commonly known algebraic extensions of the rationals  $\mathbb{Q}$  is  $\mathbb{Q}(i)$ . We recall some properties of this number field:

1. It is the splitting field of  $x^2 + 1 \in \mathbb{Q}[x]$  and thus a GALOIS extension of  $\mathbb{Q}$ . Its automorphism group consists of two elements: the identity and the complex conjugation.
2. Therefore, it is a cyclotomic field and a quadratic extension of  $\mathbb{Q}$ .
3. Its ring of integers is  $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ , the GAUSSIAN integers.
4. The norm function is given by  $N_{\mathbb{Q}(i)}(a + bi) = a^2 + b^2$ .
5. Its discriminant is  $\Delta_{\mathbb{Q}(i)} = -4$ .
6. Its set of positive primes is  $\mathbb{P}_{\mathbb{Q}(i)}^+ = \{a + bi \in \mathbb{Z}[i] : a > 0, b \geq 0\} \cap \mathbb{P}_{\mathbb{Q}(i)}$ . Thus, the minimal prime is  $1 + i$ .

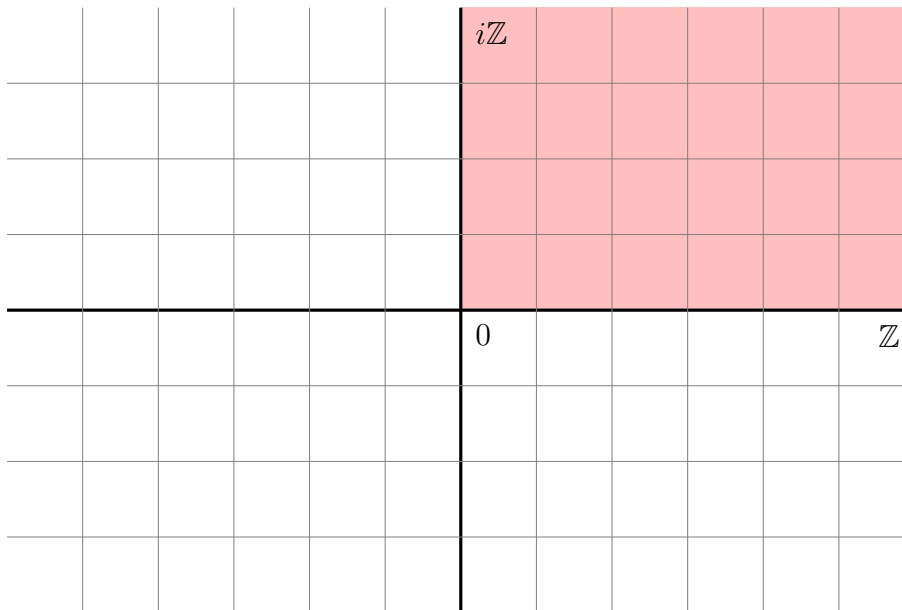


Figure 3.1: The GAUSSIAN integers near the origin, each represented by an intersection of two lines. The positive primes lie in the shaded domain, excluding the left boundary.

If we pay a close look to the behaviour of odd and even numbers in  $\mathbb{Z}[i]$ , we see that, due to  $N_{\mathbb{Q}(i)}(1+i) = 2$ , it is

$$\mathbb{Z}[i]/\langle 1+i \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

Hence, there is only one congruence class of odd GAUSSIAN integers and the computations modulo  $(1+i)\mathbb{Z}[i]$  are similar to those modulo  $2\mathbb{Z}$  in the rational integers. We may therefore distinguish between odd and even perfect GAUSSIAN integers.

This section presents the main ideas used by MCDANIEL [14] in order to transfer the EUCLID–EULER Theorem to the GAUSSIAN integers. A crucial step is the improvement of SPIRA’s inequality in Lemma 3.1.3.

**Lemma 3.2.1.** (MCDANIEL [14, p. 138]) Let  $\alpha \in \mathbb{Z}[i]$  and  $|\alpha| \geq \sqrt{5}$ . Then

$$N_{\mathbb{Q}(i)}\left(\frac{\alpha^{n+1} - 1}{\alpha - 1}\right) > N_{\mathbb{Q}(i)}(\alpha^n) \left(1 + \frac{2\Re(\alpha) - 1.4}{N_{\mathbb{Q}(i)}(\alpha)}\right)$$

for all  $n \in \mathbb{N}_{>0}$ .

The proof consists mostly of computations. However, using the definition of  $\sigma_{\mathbb{Q}(i)}$  and the multiplicativity of the norm function, this lemma yields a very useful corollary.

**Corollary 3.2.2.** Let  $\psi$  be an odd positive GAUSSIAN prime. Then

$$N_{\mathbb{Q}(i)}\left(\frac{\sigma_{\mathbb{Q}(i)}(\psi^n)}{\psi^n}\right) > 1 + \frac{2\Re(\psi) - 1.4}{N_{\mathbb{Q}(i)}(\psi)}$$

for all  $n \in \mathbb{N}_{>0}$ .

In order to use the previous lemma to prove this corollary, we point out that any odd positive GAUSSIAN prime has an absolute value of at least  $\sqrt{5}$ .

When taking a closer look at  $N_{\mathbb{Q}(i)}(\alpha)$  for an arbitrary  $\alpha \in \mathbb{Z}[i]$ , we get an inequality which looks quite similar to one we are familiar with from the rational integers.

**Lemma 3.2.3.** Let  $\alpha \in \mathbb{Z}[i]$ . Then  $N_{\mathbb{Q}(i)}(\sigma_{\mathbb{Q}(i)}(\alpha)) \geq N_{\mathbb{Q}(i)}(\alpha)$ .

*Proof.* The norm on  $\mathbb{Z}[i]$  is multiplicative and any positive GAUSSIAN prime satisfies Lemma 3.1.3.  $\square$

In the rational integers, the EULCID–EULER Theorem is restricted to even perfect numbers and, similarly, MCDANIEL’s theorem only answers the question about even (norm-) perfect GAUSSIAN integers. Corollary 3.2.2 and Lemma 3.2.3 together yield some lower bounds on the norm of an odd prime divisor of an even norm-perfect GAUSSIAN integer. These are joint by MCDANIEL with a theorem by SPIRA.

**Lemma 3.2.4.** (SPIRA [26, p. 123]) Let  $\eta = (1 + i)^{k-1}\mu$  be a norm-perfect GAUSSIAN integer with  $k \in \mathbb{N}_{\geq 2}$  and  $\mu$  odd. Then  $k \equiv 0, \pm 1 \pmod{12\mathbb{Z}}$ .

Before we move on to the main theorem of this section, we need another definition.

**Definition 3.2.5.** Let  $\eta$  be a (norm-)perfect GAUSSIAN integer.  $\eta$  is called *primitive* if there is no  $\theta \in \mathbb{Z}[i]$  such that  $\theta$  is (norm-)perfect,  $\theta \mid \eta$  and  $\theta \neq \eta$ .

This deals with the fact that Lemma 3.2.3 does not provide a strict inequality.

**Theorem 3.2.6.** (MCDANIEL [14, p. 137]) Let  $M_p = (1 + i)^p - 1$  be a GAUSSIAN MERSENNE prime and  $\varepsilon$  a unit in  $\mathbb{Z}[i]$ .

1. If  $p \equiv 1 \pmod{8\mathbb{Z}}$ , then  $\eta = \varepsilon(1 + i)^{p-1}M_p$  is a primitive norm-perfect GAUSSIAN integer.
2. If  $p \equiv -1 \pmod{8\mathbb{Z}}$ , then  $\eta = \varepsilon(1 + i)^{p-1}\overline{M_p}$  is a primitive norm-perfect GAUSSIAN integer.

Conversely, if  $\eta$  is an even norm-perfect, then, for some unit  $\varepsilon$ , there is either

1. a rational prime  $p \equiv 1 \pmod{8\mathbb{Z}}$  such that  $\eta = \varepsilon(1 + i)^{p-1}M_p$  or
2. a rational prime  $p \equiv -1 \pmod{8\mathbb{Z}}$  such that  $\eta = \varepsilon(1 + i)^{p-1}\overline{M_p}$

where  $M_p$  is a GAUSSIAN MERSENNE prime. Moreover, *norm-perfect* may be substituted by *perfect* if we only consider the first bullet in each part and replace  $\varepsilon$  by  $-i$ .

This settles the even (norm-)perfect GAUSSIAN integers. So far, there has not been much work about their odd counterparts but WARD proved a theorem on the form of such an integer.

**Theorem 3.2.7.** (WARD [30, p. 2]) Let  $\eta$  be an odd norm-perfect GAUSSIAN integer. Then it is of the form

$$\eta = \psi^k \rho^2$$

for an odd  $k \in \mathbb{Z}$ , an odd GAUSSIAN prime  $\psi$ , and an odd GAUSSIAN integer  $\rho$ .

Surprisingly and in contrast to the rational integers, WARD is able to present an odd positive norm-perfect GAUSSIAN integer:  $2 + i$  which is also prime. We quickly check that

$$N_{\mathbb{Q}(i)}(\sigma_{\mathbb{Q}(i)}(2 + i)) = N_{\mathbb{Q}(i)}(3 + i) = 3^2 + 1^2 = 10 = 2 \cdot 5 = 2N_{\mathbb{Q}(i)}(2 + i).$$

However, this is the only norm-perfect GAUSSIAN prime which can be seen by evaluating the equation

$$N_{\mathbb{Q}(i)}(\psi + 1) = N_{\mathbb{Q}(i)}(\sigma_{\mathbb{Q}(i)}(\psi)) = 2N_{\mathbb{Q}(i)}(\psi)$$

as  $\sigma_{\mathbb{Q}(i)}(\psi) = \psi + 1$  for any positive prime  $\psi$ . If we choose our set of positive primes  $\mathbb{P}_{\mathbb{Q}(i)}^+$  differently, such that  $2-i$  is positive instead of  $1+2i$ , it will be another odd positive norm-perfect prime. This underlines the fact that our set of (norm-)perfect integers depends on the set  $\mathbb{P}_K^+$  for  $K \in \mathcal{R}$ .

# Chapter 4

## Perfect numbers in the Eisenstein integers and cyclotomic fields of higher degree

The degree of the field extension  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$  is  $\varphi(n)$  where  $\varphi$  is EULER's totient function. There are exactly two solutions to  $\varphi(n) = 2$  which are  $n \in \{3, 4\}$ . We dealt with  $n = 4$  in the previous chapter but less has been done in the case of  $n = 3$  so far.

**Definition 4.0.1.** We define

$$\omega := \exp\left(\frac{2\pi i}{3}\right),$$

the primitive third root of unity in the upper complex half-plane.

The extensions  $\mathbb{Q}(i)/\mathbb{Q}$  and  $\mathbb{Q}(\omega)/\mathbb{Q}$  have a lot in common. We recapitulate some of the properties of the latter, starting with the two it shares with the former.

1. It is the splitting field of  $x^2 + x + 1 \in \mathbb{Q}[x]$  and thus a GALOIS extension of  $\mathbb{Q}$ . Its automorphism group consists of two elements: the identity and the complex conjugation.
2. Therefore, it is a cyclotomic field and a quadratic extension of  $\mathbb{Q}$ .
3. Its ring of integers is  $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$ , the EISENSTEIN integers.
4. The norm function is given by  $N_{\mathbb{Q}(\omega)}(a + b\omega) = a^2 - ab + b^2$ .
5. Its discriminant is  $\Delta_{\mathbb{Q}(\omega)} = -3$ .
6. Its set of positive primes is  $\mathbb{P}_{\mathbb{Q}(\omega)}^+ = \{a + b\omega \in \mathbb{Z}[\omega] : a > b \geq 0\} \cap \mathbb{P}_{\mathbb{Q}(\omega)}$ . Thus, the minimal prime is  $2 + \omega = 1 - \omega^2$ .

A main difference to  $\mathbb{Z}[i]$  and  $\mathbb{Z}$  directly impacting the computations we want to do in  $\mathbb{Z}[\omega]$  is that, since  $N_{\mathbb{Q}(\omega)}(1 - \omega^2) = 3$ ,

$$\mathbb{Z}[\omega]/\langle 1 - \omega^2 \rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

So there are two congruence classes of odd EISENSTEIN integers, namely those congruent to 1 or 2 modulo  $(1 - \omega^2)\mathbb{Z}[\omega]$ .

We will also copy the definition of a primitive (norm-)perfect number.



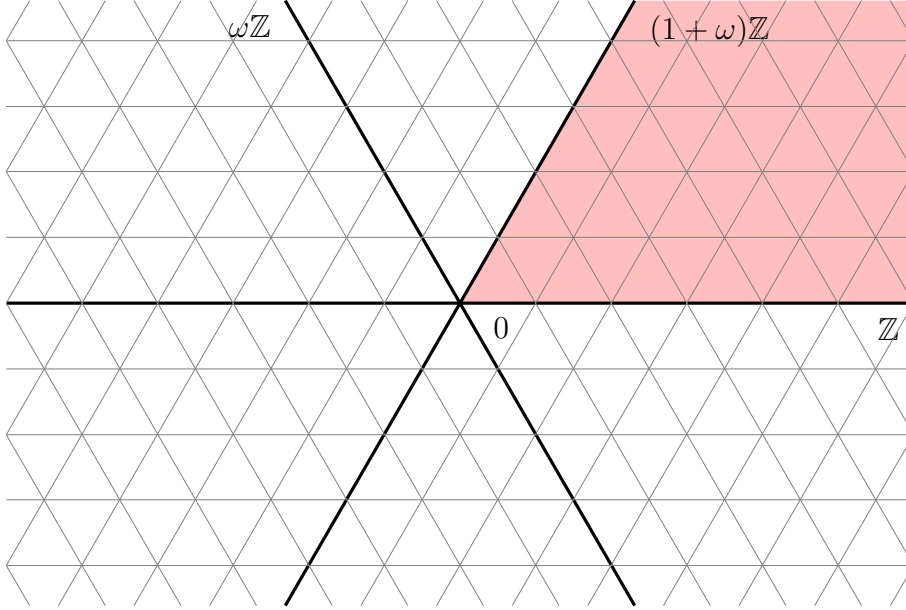


Figure 4.1: The EISENSTEIN integers near the origin, each represented by an intersection of three lines. The positive primes lie in the shaded domain, excluding the upper boundary.

**Definition 4.0.2.** Let  $\alpha$  be a (norm-)perfect EISENSTEIN integer.  $\alpha$  is called *primitive* if there is no  $\beta \in \mathbb{Z}[\omega]$  such that  $\beta$  is (norm-)perfect,  $\beta \mid \alpha$  and  $\beta \neq \alpha$ .

In 2016, PARKER, RUSHALL, and HUNT published a short paper [34] transferring some of MCDANIEL’s results to the EISENSTEIN integers. Even though they use a similar definition of  $\sigma_{\mathbb{Q}(\omega)}$ , they do not introduce the concept of positive EISENSTEIN integers. So for simplicity, they choose  $1 - \omega$  to be their minimal prime while the relevant—in our sense of definition 3.1.1 *positive*—associate is still chosen to be  $1 - \omega^2$ . However, they present a sufficient condition for an even norm-perfect EISENSTEIN integer. The theorem is cited in its original form and therefore uses PARKER et al.’s definitions.

**Theorem 4.0.3.** (PARKER, RUSHALL, HUNT [34, p. 10]) Given any rational integer  $k > 1$ , if  $(1 - \omega)^k - 1$  is an EISENSTEIN MERSENNE prime and if  $k \equiv 11 \pmod{12\mathbb{Z}}$ , then  $\alpha = (1 - \omega)^{k-1}[(1 - \omega)^k - 1]$  is an even norm-perfect EISENSTEIN integer.

Oddly enough, PARKER et al. do not refine their computations in this theorem’s proof to show that—with their definitions—a particular associate of  $\alpha$  is indeed perfect. We will adjust the theorem to our own definitions in the next section and close this gap. The main aim of this part of the thesis will be to also prove a converse statement, i.e. to prove the counterpart of the EUCLID–EULER Theorem for EISENSTEIN integers. The inspiration for this is given by MCDANIEL’s Theorem 3.2.6.

PARKER et al. also state a conjecture about the form of an odd norm-perfect EISENSTEIN integer.

**Conjecture 4.0.4.** [34, p. 11] Any odd norm-perfect EISENSTEIN integer has to be of the form  $\alpha = \psi^k \gamma^3$  where  $\psi$  is an odd EISENSTEIN prime,  $k \equiv 2 \pmod{3\mathbb{Z}}$  a rational integer and  $\gamma$  an odd EISENSTEIN integer coprime to  $\psi$ .

So far, there has not been any proof for this conjecture to be true but we will prove another form in the next-again section, presenting this form as a mere subcase.

## 4.1 Even perfect Eisenstein integers

The aim of this section is to prove the following two main theorems of this part, transferring the EUCLID–EULER Theorem to the EISENSTEIN integers.

**Theorem 4.1.1.**  $\alpha \in \mathbb{Z}[\omega]$  is an even primitive perfect number if and only if

$$\alpha = -\omega(1 - \omega^2)^{k-1}[(1 - \omega^2)^k - 1]$$

where  $(1 - \omega^2)^k - 1$  is prime with a rational integer  $k \equiv 1 \pmod{12\mathbb{Z}}$ .

Since perfect implies norm-perfect and the norm of any unit is 1, any associate of a perfect number is norm-perfect. This thus covers the first half of the second theorem.

**Theorem 4.1.2.**  $\alpha \in \mathbb{Z}[\omega]$  is an even primitive norm-perfect  $\omega$  number if and only if either

1.  $\alpha = \varepsilon(1 - \omega^2)^{k-1}[(1 - \omega^2)^k - 1]$  where  $(1 - \omega^2)^k - 1$  is prime with a rational integer  $k \equiv 1 \pmod{12\mathbb{Z}}$  or
2.  $\alpha = \varepsilon(1 - \omega^2)^{k-1}[\overline{(1 - \omega^2)^k - 1}]$  where  $(1 - \omega^2)^k - 1$  is prime with a rational integer  $k \equiv -1 \pmod{12\mathbb{Z}}$

and  $\varepsilon$  is a unit in  $\mathbb{Z}[\omega]$ .

Notice the similarity to the results by MCDANIEL. The significantly more difficult part is proving the *only-if*-direction in either theorem since computing the value of the  $\sigma_{\mathbb{Q}(\omega)}$ -function of a given element is fairly easy. To this end, we transfer two of SPIRA's lemmata.

**Lemma 4.1.3.** Let  $\alpha \in \mathbb{Z}[\omega]$ . Then  $N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\alpha)) \geq N_{\mathbb{Q}(\omega)}(\alpha)$ .

*Proof.* The norm is multiplicative and any positive EISENSTEIN prime satisfies Lemma 3.1.3. □

In particular, this lemma tells us that any multiple of an abundant number is also abundant. This helps us say something about the exponent  $k$  of an even norm-perfect number.

**Lemma 4.1.4.** Let  $\alpha = (1 - \omega^2)^{k-1}\mu$  be an even norm-perfect EISENSTEIN integer with  $\mu$  odd and a rational  $k \geq 2$ . Then  $k \equiv \pm 2, \pm 1, 0 \pmod{12\mathbb{Z}}$ .

*Proof.* Recall that the norm and  $\sigma_{\mathbb{Q}(\omega)}$ -function are multiplicative and thus, so is their composition. We decompose

$$3N_{\mathbb{Q}(\omega)}(\alpha) = N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\alpha)) = N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}((1 - \omega^2)^{k-1})) N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\mu)).$$

We are interested in the left factor and continue our computations.

$$\begin{aligned} N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}((1 - \omega^2)^{k-1})) &= N_{\mathbb{Q}(\omega)}\left(\frac{(1 - \omega^2)^k - 1}{1 - \omega^2 - 1}\right) \\ &= N_{\mathbb{Q}(\omega)}(-\omega((1 - \omega^2)^k - 1)) \\ &= 3^k - 2\Re((1 - \omega^2)^k) + 1. \end{aligned}$$

For  $k \not\equiv \pm 2, \pm 1, 0 \pmod{12\mathbb{Z}}$ , the middle term is less than or equal to 0, so the whole expression is greater than  $3^k = 3N_{\mathbb{Q}(\omega)}((1 - \omega^2)^{k-1})$ . Using Lemma 4.1.3, this would imply that  $\alpha$  is abundant. Therefore,  $k \equiv \pm 2, \pm 1, 0 \pmod{12\mathbb{Z}}$ .  $\square$

This considerably reduces the possible residue classes of  $k \pmod{12\mathbb{Z}}$ . Now, we will extend Lemma 3.2.1 and its corollary 3.2.2 to the EISENSTEIN integers.

**Lemma 4.1.5.** Let  $\psi$  be an odd positive EISENSTEIN prime. Then

$$N_{\mathbb{Q}(\omega)}\left(\frac{\sigma_{\mathbb{Q}(\omega)}(\psi^n)}{\psi^n}\right) > 1 + \frac{2\Re(\psi) - 1.4}{N_{\mathbb{Q}(\omega)}(\psi)}$$

for all  $n \in \mathbb{N}_{>0}$ .

*Proof.* Firstly, we remark that the computations in the proof of Lemma 3.2.1 [14] are based on the norm on  $\mathbb{Z}[i]$ . If we have a look at definition 1.0.2 and the fact that the automorphism groups of both  $\mathbb{Q}(i)$  and  $\mathbb{Q}(\omega)$  only consist of the identity and the complex conjugation and therefore have a similar image, we may easily transfer that lemma to the EISENSTEIN integers for  $|\psi| > \sqrt{5}$ .

We are left to examine the inequality for all odd positive primes  $\psi$  with absolute value less than  $\sqrt{5}$ . There is only one such prime, namely 2. However, we have

$$\begin{aligned} N_{\mathbb{Q}(\omega)}\left(\frac{2^{n+1} - 1}{2 - 1}\right) &= N_{\mathbb{Q}(\omega)}(2^n)N_{\mathbb{Q}(\omega)}\left(2 - \frac{1}{2^n}\right) \\ &= N_{\mathbb{Q}(\omega)}(2^n)\left(4 - \frac{1}{2^{n-2}} + \frac{1}{2^{2n}}\right) \\ &> N_{\mathbb{Q}(\omega)}(2^n)\left(1 + \frac{13}{4}\right) \\ &= N_{\mathbb{Q}(\omega)}(2^n)\left(1 + \frac{2\Re(2) - 1.4}{N_{\mathbb{Q}(\omega)}(2)}\right) \end{aligned}$$

for all  $n \in \mathbb{N}_{>0}$ . We deduce the desired inequality by dividing both sides by  $N_{\mathbb{Q}(\omega)}(2^n)$ .  $\square$

We move on to find some estimate about the norm of an odd divisor of an even norm-perfect EISENSTEIN integer, so that we can minimise the number of possible prime divisors. This technique is inspired by MCDANIEL's work but a bit more straight forward, since the setting of the EISENSTEIN integers lets us drop one extra lemma that was crucial in MCDANIEL's proof.

**Lemma 4.1.6.** Let  $\alpha = (1 - \omega^2)^{k-1}\mu$  be a norm-perfect EISENSTEIN integer with  $\mu$  odd and a rational  $k \geq 2$ . Let  $\psi$  be a positive prime divisor of  $\mu$ . Then

$$N(\psi) > \frac{13}{5} \cdot \frac{N_{\mathbb{Q}(\omega)}((1 - \omega^2)^k - 1)}{3^k - N_{\mathbb{Q}(\omega)}((1 - \omega^2)^k - 1)}.$$

*Proof.* Let  $e$  be the maximal exponent such that  $\psi^e \mid \mu$ . Using the fact that  $\alpha$  is norm-perfect and Lemma 4.1.3, we get

$$1 = \frac{N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\alpha))}{3N_{\mathbb{Q}(\omega)}(\alpha)} \geq \frac{N_{\mathbb{Q}(\omega)}((1 - \omega^2)^k - 1)N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\psi^e))}{3^k N_{\mathbb{Q}(\omega)}(\psi^e)}.$$

The previous lemma then tells us that

$$\begin{aligned} & \frac{N_{\mathbb{Q}(\omega)}((1-\omega^2)^k-1) N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\psi^e))}{3^k N_{\mathbb{Q}(\omega)}(\psi^e)} \\ & > \frac{N_{\mathbb{Q}(\omega)}(((1-\omega^2)^k-1)(N_{\mathbb{Q}(\omega)}(\psi)+2\Re(\psi)-1.4))}{3^k(N_{\mathbb{Q}(\omega)}(\psi))}. \end{aligned}$$

Solving this for  $N_{\mathbb{Q}(\omega)}(\psi)$  yields

$$N_{\mathbb{Q}(\omega)}(\psi) > (2\Re(\psi) - 1.4) \frac{N_{\mathbb{Q}(\omega)}((1-\omega^2)^k-1)}{3^k - N_{\mathbb{Q}(\omega)}((1-\omega^2)^k-1)}.$$

We have a quick look at the smallest odd positive primes of  $\mathbb{Z}[\omega]$  so that we can estimate  $2\Re(\psi)$ . In the following table,  $p$  is the rational prime such that  $\psi$  lies above  $p$ .

$p$	$\psi$	$\Re(\psi)$
2	2	2
5	5	5
7	$2 - \omega^2$	$\frac{5}{2}$
7	$1 - 2\omega^2$	2
11	11	11

Table 4.1: Real parts of the odd positive primes of the least norm

Thus,  $\Re(\psi) \geq 2$  and we are done since  $2 \cdot 2 - 1.4 = \frac{13}{5}$ .  $\square$

Examining the primes of  $\mathbb{Z}[\omega]$  with regard to their norm brings another property back to our minds that we know from elementary algebraic number theory. It will be left without proof but we refer to DEDEKIND–KUMMER and the fact that the EISENSTEIN integers form a UFD.

**Lemma 4.1.7.** Let  $\alpha \in \mathbb{Z}[\omega]$  and  $N_{\mathbb{Q}(\omega)}(\psi) \mid N_{\mathbb{Q}(\omega)}(\alpha)$  in  $\mathbb{Z}$  for a prime  $\psi \in \mathbb{Z}[\omega]$ , then  $\psi \mid \alpha$  or  $\bar{\psi} \mid \alpha$ . Moreover, if  $p \mid N_{\mathbb{Q}(\omega)}(\alpha)$  for some rational prime  $p$ , then there is a prime  $\rho \in \mathbb{Z}[\omega]$  such that  $\rho \mid \alpha$  and  $N_{\mathbb{Q}(\omega)}(\rho) = p$  or  $N_{\mathbb{Q}(\omega)}(\rho) = p^2$ .

Due to Lemma 4.1.4, we need to apply Lemma 4.1.6 to only five residue classes. Fortunately, some of them can be dealt with at the same time. The following lemma will now join most of the results we have acquired so far.

**Lemma 4.1.8.** Let  $\alpha = (1-\omega^2)^{k-1}\mu \in \mathbb{Z}[\omega]$  be norm-perfect with  $\mu$  odd and a rational  $k \geq 2$ . Then  $k \equiv \pm 1 \pmod{12\mathbb{Z}}$ ,  $(1-\omega^2)^k - 1$  is prime and either  $(1-\omega^2)^k - 1$  or  $\overline{(1-\omega^2)^k - 1}$  divide  $\mu$ .

*Proof.* Let  $\psi$  be an odd positive prime divisor of  $(1-\omega^2)^k - 1 \simeq \sigma_{\mathbb{Q}(\omega)}((1-\omega^2)^{k-1})$ , say  $(1-\omega^2)^k - 1 = \psi\rho$  for a  $\rho \in \mathbb{Z}[\omega]$ , and such that  $\psi$  has the least norm among such divisors of  $(1-\omega^2)^k - 1$ . Since  $\alpha$  is norm-perfect and the norm of any unit is 1, we have

$$3N_{\mathbb{Q}(\omega)}(\alpha) = N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\alpha)) = N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\mu)) N_{\mathbb{Q}(\omega)}(\rho) N_{\mathbb{Q}(\omega)}(\psi).$$

By Lemma 4.1.7 and since  $\psi$  is odd, it follows either  $\psi \mid \alpha$  or  $\bar{\psi} \mid \alpha$ . It is  $N_{\mathbb{Q}(\omega)}(\psi) = N_{\mathbb{Q}(\omega)}(\bar{\psi})$ , so we may apply the Lemma 4.1.6. We examine the norm of  $(1 - \omega^2)^k - 1$  depending on  $k$ .

$k \pmod{12\mathbb{Z}}$	$\Re((1 - \omega^2)^k)$	$N_{\mathbb{Q}(\omega)}((1 - \omega^2)^k - 1)$
$\pm 2$	$\frac{3^{\frac{k}{2}}}{2}$	$3^k - 3^{\frac{k}{2}} + 1$
$\pm 1$	$\frac{3^{\frac{k+1}{2}}}{2}$	$3^k - 3^{\frac{k+1}{2}} + 1$
$0$	$3^{\frac{k}{2}}$	$3^k - 2 \cdot 3^{\frac{k}{2}} + 1$

Table 4.2: The norm of  $(1 - \omega^2)^k - 1$  depending on  $k$

Notice the symmetry in this table. We go ahead and insert these numbers into our inequality from Lemma 4.1.6.

$k \pmod{12\mathbb{Z}}$	$N_{\mathbb{Q}(\omega)}(\psi) >$
$\pm 2$	$\frac{13}{5} \cdot \frac{3^k - 3^{\frac{k}{2}} + 1}{3^{\frac{k}{2}} - 1}$
$\pm 1$	$\frac{13}{5} \cdot \frac{3^k - 3^{\frac{k+1}{2}} + 1}{3^{\frac{k+1}{2}} - 1}$
$0$	$\frac{13}{5} \cdot \frac{3^k - 2 \cdot 3^{\frac{k}{2}} + 1}{2 \cdot 3^{\frac{k}{2}} - 1}$

Table 4.3: Some estimates for  $N_{\mathbb{Q}(\omega)}(\psi)$

We will distinguish between three cases.

Case 1: Suppose  $k \equiv 0 \pmod{12\mathbb{Z}}$ , say  $k = 12t$  for some  $t \in \mathbb{N}_{>0}$ . Then, the norm of  $(1 - \omega^2)^k - 1$  is

$$(3^{6t} - 1)^2 = (3^t - 1)^2(3^t + 1)^2(3^{2t} - 3^t + 1)^2(3^{2t} + 3^t + 1)^2.$$

By Lemma 4.1.7, we have  $N_{\mathbb{Q}(\omega)}(\psi) \leq (3^t - 1)^2$ . However, table 4.3 gives

$$\begin{aligned} N_{\mathbb{Q}(\omega)}(\psi) &> \frac{13}{5} \cdot \frac{3^k - 2 \cdot 3^{\frac{k}{2}} + 1}{2 \cdot 3^{\frac{k}{2}} - 1} \\ &= \frac{13}{5} \cdot \frac{(3^{\frac{k}{2}} - 1)^2}{2 \cdot 3^{\frac{k}{2}} - 1} \\ &= \frac{13}{10} \cdot \frac{(3^{\frac{k}{2}} - 1)^2}{3^{\frac{k}{2}} - \frac{1}{2}} \\ &> 3^{\frac{k}{2}} - 1 \\ &> (3^t - 1)^2 \end{aligned}$$

for  $t \geq 1$ .

Case 2: For  $k \equiv \pm 2 \pmod{12\mathbb{Z}}$ , we have

$$N_{\mathbb{Q}(\omega)}(\psi) > \frac{13}{5} \cdot \frac{3^k - 3^{\frac{k}{2}} + 1}{3^{\frac{k}{2}} - 1} > \frac{13}{5} \cdot \frac{3^k - 2 \cdot 3^{\frac{k}{2}} + 1}{3^{\frac{k}{2}} - 1} = \frac{13}{5} (3^{\frac{k}{2}} - 1).$$

Using Lemma 4.1.7, we will show a contradiction for both cases.

*Subcase 2.1:* Suppose  $k \equiv 2 \pmod{12\mathbb{Z}}$ , say  $k = 12t + 2$  for some  $t \in \mathbb{N}_{\geq 0}$ . Then, the norm of  $(1 - \omega^2)^k - 1$  is

$$3^{12t+2} - 3^{6t+1} + 1 = (3^{6t+1} - 3^{3t+1} + 1)(3^{6t+1} + 3^{3t+1} + 1).$$

The left factor is less than  $\frac{13}{5}(3^{\frac{k}{2}} - 1)$  since  $\frac{k}{2} = 6t + 1$ .

*Subcase 2.2:* Suppose  $k \equiv -2 \pmod{12\mathbb{Z}}$ , say  $k = 12t - 2$  for some  $t \in \mathbb{N}_{> 0}$ . Then, the norm of  $(1 - \omega^2)^k - 1$  is

$$3^{12t-2} - 3^{6t-1} + 1 = (3^{6t-1} - 3^{3t} + 1)(3^{6t-1} + 3^{3t} + 1).$$

The left factor is less than  $\frac{13}{5}(3^{\frac{k}{2}} - 1)$  since  $\frac{k}{2} = 6t - 1$ .

*Case 3:* Suppose  $k \equiv \pm 1 \pmod{12\mathbb{Z}}$  such that  $k \geq 11$ . By table 4.3, we get

$$\begin{aligned} N_{\mathbb{Q}(\omega)}(\psi) &> \frac{13}{5} \cdot \frac{3^k - 3^{\frac{k+1}{2}} + 1}{3^{\frac{k+1}{2}} - 1} \\ &= \frac{13}{5} \cdot \frac{3^{k-1} - 3^{\frac{k-1}{2}} + \frac{1}{3}}{3^{\frac{k-1}{2}} - \frac{1}{3}} \\ &> \frac{13}{5} \cdot \frac{3^{k-1} - 2 \cdot 3^{\frac{k-1}{2}} + 1}{3^{\frac{k-1}{2}} - \frac{1}{3}} \\ &> \frac{12}{5} \cdot \frac{3^{k-1} - 2 \cdot 3^{\frac{k-1}{2}} + 1}{3^{\frac{k-1}{2}} - 1} \\ &= \frac{12}{5} \left( 3^{\frac{k-1}{2}} - 1 \right) \\ &> \sqrt{N_{\mathbb{Q}(\omega)}((1 - \omega^2)^k - 1)}, \end{aligned}$$

so, by multiplicity of the norm and minimality of  $N_{\mathbb{Q}(\omega)}(\psi)$ ,  $(1 - \omega^2)^k - 1$  has exactly one prime divisor, hence it is prime and  $\psi = (1 - \omega^2)^k - 1$  or  $\psi = \overline{(1 - \omega^2)^k - 1}$ . Thus, either  $(1 - \omega^2)^k - 1$  or  $\overline{(1 - \omega^2)^k - 1}$  divide  $\mu$ .

The last inequality in the previous computation holds because

$$\begin{aligned} \left( \frac{12}{5} \left( 3^{\frac{k-1}{2}} - 1 \right) \right)^2 &> \left( \frac{11}{5} \left( 3^{\frac{k-1}{2}} - \frac{1}{2} \right) \right)^2 \\ &= \frac{121}{25} \left( 3^{k-1} - 3^{\frac{k-1}{2}} + \frac{1}{4} \right) \\ &= \frac{121}{75} \left( 3^k - 3^{\frac{k+1}{2}} + \frac{3}{4} \right) \\ &> 3^k - 3^{\frac{k+1}{2}} + 1 \\ &= N_{\mathbb{Q}(\omega)}((1 - \omega^2)^k - 1) \end{aligned}$$

for  $k \geq 11$ . This finishes the proof.  $\square$

We are ready to take the last few steps towards proving the two main theorems of this section.

**Lemma 4.1.9.** Let  $\alpha = (1 - \omega^2)^{k-1}\mu$  be a norm-perfect EISENSTEIN integer such that  $k \geq 2$  and  $\mu$  is odd.

1. If  $k \equiv 1 \pmod{12\mathbb{Z}}$ , then  $\mu = ((1 - \omega^2)^k - 1)\rho$  for some odd  $\rho$ , and
2. if  $k \equiv -1 \pmod{12\mathbb{Z}}$ , then  $\mu = \left(\overline{(1 - \omega^2)^k - 1}\right)\rho$  for some odd  $\rho$ .

*Proof.* Suppose  $k \equiv 1 \pmod{12\mathbb{Z}}$ . Since  $k \geq 2$ ,  $\overline{(1 - \omega^2)^k - 1}$  is not a unit and its positive associate is

$$(1 + \omega)\overline{(1 - \omega^2)^k - 1} = 3(1 - \omega)^{k-2} - 1 - \omega.$$

Thus,

$$\sigma_{\mathbb{Q}(\omega)}\left(\overline{(1 - \omega^2)^k - 1}\right) = 3(1 - \omega)^{k-2} - \omega$$

because  $(1 - \omega^2)^k - 1$  and its complex conjugate are prime by Lemma 4.1.8. Furthermore,

$$\begin{aligned} N_{\mathbb{Q}(\omega)}\left(\sigma_{\mathbb{Q}(\omega)}\left(\overline{(1 - \omega^2)^k - 1}\right)\right) &= (3(1 - \omega)^{k-2} - \omega)(3(1 - \omega^2)^{k-2} - \omega^2) \\ &= 3^k - 6\Re(\omega(1 - \omega^2)^{k-2}) + 1. \end{aligned}$$

We compute, since  $k$  is a *rationaly* odd natural number, that

$$\omega(1 - \omega^2)^{k-2} = (\omega - 1)^{k-2} = - (3(1 - \omega)^{k-3}),$$

so

$$\Re(\omega(1 - \omega^2)^{k-2}) = -\frac{3^{\frac{k-1}{2}}}{2}.$$

Thus,

$$N_{\mathbb{Q}(\omega)}\left(\sigma_{\mathbb{Q}(\omega)}\left(\overline{(1 - \omega^2)^k - 1}\right)\right) = 3^k + 3^{\frac{k+1}{2}} + 1 > 3^k = 3N_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^{k-1}\right).$$

Since

$$N_{\mathbb{Q}(\omega)}\left(\sigma_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^{k-1}\right)\right) = N_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^k - 1\right) = N_{\mathbb{Q}(\omega)}\left(\overline{(1 - \omega^2)^k - 1}\right)$$

their product is greater than  $3N_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^{k-1}\overline{(1 - \omega^2)^k - 1}\right)$ , hence the prime dividing  $\mu$  must be  $(1 - \omega^2)^k - 1$ .

The proof for  $k \equiv -1 \pmod{12\mathbb{Z}}$  works analogously.  $\square$

This lemma proves in particular that a norm-perfect number is never divisible by  $3^k - 3^{\frac{k+1}{2}} + 1$ , i.e. by the product of an EISENSTEIN MERSENNE prime and its conjugate. The rest is just putting all the pieces together.

*Proof of Theorem 4.1.2.* The *only-if*-direction is a corollary of the previous lemma since we proved that every norm-perfect number is divisible by exactly one of the presented primitive norm-perfect numbers.

The *if*-direction is a simple computation and will be shown for the case  $k \equiv -1 \pmod{12\mathbb{Z}}$ . Quickly check beforehand that  $\overline{(1 - \omega^2)^k - 1}$  is positive. It is

$$\begin{aligned} N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\alpha)) &= N_{\mathbb{Q}(\omega)}\left(\frac{(1 - \omega^2)^k - 1}{1 - \omega^2 - 1} \cdot \left(\overline{(1 - \omega^2)^k - 1} + 1\right)\right) \\ &= N_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^k - 1\right) N_{\mathbb{Q}(\omega)}\left(\overline{(1 - \omega^2)^k - 1} + 1\right) \\ &= N_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^k - 1\right) N_{\mathbb{Q}(\omega)}\left(\overline{(1 - \omega^2)^k}\right) \\ &= 3N_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^k - 1\right) N_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^{k-1}\right) \\ &= 3N_{\mathbb{Q}(\omega)}(\alpha), \end{aligned}$$

hence  $\alpha$  is norm-perfect. However,  $\overline{(1 - \omega^2)^k - 1}$  and any power of  $(1 - \omega^2)$  are deficient, so  $\alpha$  is primitive.

The computation for  $k \equiv 1 \pmod{12\mathbb{Z}}$  works analogously.  $\square$

*Proof of Theorem 4.1.1.* The *if*-direction is given by a similar computation as in the previous proof but without the norm function. Notice, if  $k \equiv 1 \pmod{12\mathbb{Z}}$ , then

$$\sigma_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^k - 1\right) = (1 - \omega^2)^k,$$

yielding

$$\sigma_{\mathbb{Q}(\omega)}\left((1 - \omega^2)^{k-1}\left((1 - \omega^2)^k - 1\right)\right) = (1 - \omega^2)^k\left((1 - \omega^2)^k - 1\right).$$

Conversely, the *only-if*-direction is proven by examining all the possible primitive norm-perfect numbers, since every perfect number is also norm-perfect. The associates of a perfect number cannot be perfect, since all of them have the same image under the  $\sigma_{\mathbb{Q}(\omega)}$ -function. In the case of  $k \equiv -1 \pmod{12\mathbb{Z}}$ , we see from the computations in the previous proof that the equation

$$\sigma_{\mathbb{Q}(\omega)}(\alpha) = (1 - \omega^2)\alpha$$

cannot hold, since the left-hand side is divisible by  $(1 - \omega^2)^k - 1$  and the right-hand side by its complex conjugate but neither of them is divisible by the product of those two factors, which is  $3^k - 3^{\frac{k+1}{2}} + 1$ .  $\square$

## 4.2 Odd perfect Eisenstein integers

Similarly to the previous cases of the rational and the GAUSSIAN integers, the case of odd norm-perfect EISENSTEIN integers proves to be a bit more difficult to come by. PARKER et al. presented a form for such a number in their conjecture 4.0.4. We will work in a similar way like WARD who transferred Lemma 2.2.2 to  $\mathbb{Z}[i]$ . Due to two congruence classes of odd numbers being existent in  $\mathbb{Z}[\omega]$ , we will have to work a bit differently.

**Lemma 4.2.1.** Let  $\psi \in \mathbb{P}_{\mathbb{Q}(\omega)}^+$  be an odd positive prime and  $m \in \mathbb{N}$ . It is

$$N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\psi^m)) \equiv 0 \pmod{3\mathbb{Z}}$$

if and only if one of the following cases applies:

1.  $\psi \equiv 1 \pmod{1 - \omega^2}$  and  $m \equiv 2 \pmod{3\mathbb{Z}}$ .



2.  $\psi \equiv 2 \pmod{1 - \omega^2}$  and  $m \equiv 1 \pmod{2\mathbb{Z}}$ .

*Proof.* By Lemma 3.1.12, the norm of  $\sigma_{\mathbb{Q}(\omega)}(\psi^m) = \sum_{k=0}^m \psi^k$  is divisible by 3 if and only if the sum itself is even. Recall that

$$\mathbb{Z}[\omega]/\langle 1 - \omega^2 \rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

1. If  $\psi \equiv 1 \pmod{1 - \omega^2}$ , each of its powers is congruent to 1  $\pmod{1 - \omega^2}$ . Thus,

$$\sum_{k=0}^m \psi^k \equiv m + 1 \pmod{1 - \omega^2}$$

which is 0 if and only if  $m \equiv 2 \pmod{3\mathbb{Z}}$ .

2. If  $\psi \equiv 2 \pmod{1 - \omega^2}$ , we have  $\psi^l \equiv l \pmod{2\mathbb{Z}}$ . For *rationaly* odd  $k \in \mathbb{N}$ , this implies

$$\psi^{k-1} + \psi^k \equiv 0 \pmod{1 - \omega^2}.$$

Now just use the sum above. □

**Theorem 4.2.2.** Let  $\alpha$  be an odd norm-perfect EISENSTEIN integer and define  $P_j = \{\psi \in \mathbb{P}_{\mathbb{Q}(\omega)}^+ : \psi \equiv j \pmod{1 - \omega^2} \wedge \psi \mid \alpha\}$  for  $j \in \{1, 2\}$ .  $\alpha$  has to be of the form

$$\varepsilon \psi_0^k \prod_{\psi_1 \in P_1, \psi_1 \neq \psi_0} \psi_1^{e_{\psi_1}} \prod_{\psi_2 \in P_2, \psi_2 \neq \psi_0} \psi_2^{e_{\psi_2}}$$

with either

1.  $\psi_0 \in P_1$ ,  $k \equiv 2 \pmod{3\mathbb{Z}}$  or
2.  $\psi_0 \in P_2$ ,  $k \equiv 1 \pmod{2\mathbb{Z}}$

as well as  $e_{\psi_1} \not\equiv 2 \pmod{3\mathbb{Z}}$  and  $e_{\psi_2} \equiv 0 \pmod{2\mathbb{Z}}$  and  $\varepsilon$  being a unit in either case.

*Proof.* Since  $\alpha$  is norm-perfect, we have

$$N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\alpha)) = 3N_{\mathbb{Q}(\omega)}(\alpha).$$

Write

$$\alpha = \varepsilon \prod_{\psi_1 \in P_1} \psi_1^{e_{\psi_1}} \prod_{\psi_2 \in P_2} \psi_2^{e_{\psi_2}}.$$

As the norm and  $\sigma_{\mathbb{Q}(\omega)}$ -function are both multiplicative, so is their composition and we may write the first equation as

$$\begin{aligned} & \prod_{\psi_1 \in P_1} N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\psi_1^{e_{\psi_1}})) \prod_{\psi_2 \in P_2} N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\psi_2^{e_{\psi_2}})) \\ &= 3 \prod_{\psi_1 \in P_1} N_{\mathbb{Q}(\omega)}(\psi_1^{e_{\psi_1}}) \prod_{\psi_2 \in P_2} N_{\mathbb{Q}(\omega)}(\psi_2^{e_{\psi_2}}), \end{aligned}$$

using that the norm of a unit is 1 and the  $\sigma_{\mathbb{Q}(\omega)}$ -function is defined up to associates. By Lemma 3.1.11, the norm of any odd EISENSTEIN is congruent to 1 modulo  $3\mathbb{Z}$ . Therefore, the right-hand side is congruent to 3 modulo  $9\mathbb{Z}$  implying that exactly one of the prime factors of  $\alpha$  satisfies the conditions listed in Lemma 4.2.1. The possible forms are the ones presented above. □

This theorem is a bit weaker than the conjecture. Nevertheless, we get a corollary if we distinguish between the two congruence classes of odd integers.

**Corollary 4.2.3.** In the case of the previous theorem, each case corresponds to exactly one congruence class of odd positive integers, i.e.  $\psi_0 \in P_1$  if and only if  $\alpha \equiv 1 \pmod{1-\omega^2}$  under the assumption that  $\alpha$  is positive.

*Proof.* We evaluate the product from the theorem and remark that  $\varepsilon = 1$  since we are focusing on positive integers. In any case, the powers

$$\psi_1^{e_{\psi_1}} \equiv 1 \pmod{1-\omega^2}$$

since  $\psi_1 \equiv 1 \pmod{1-\omega^2}$  and also

$$\psi_2^{e_{\psi_2}} \equiv 1 \pmod{1-\omega^2}$$

since  $e_{\psi_2} \equiv 0 \pmod{2\mathbb{Z}}$  and  $\psi_2 \equiv 2 \pmod{1-\omega^2}$ . Hence, the congruence class of the whole product only depends on  $\psi_0^k$  which is  $\equiv 1$  modulo  $1-\omega^2$  if  $\psi_0 \in P_1$  and  $\equiv 2$  modulo  $1-\omega^2$  if  $\psi_0 \in P_2$ .  $\square$

Similarly to the case of the rational integers, the author has not been able to present any odd norm-perfect integers yet. However, we can prove that the GAUSSIAN integers feature a kind of numbers which cannot be found in the EISENSTEIN integers.

**Theorem 4.2.4.** There is no odd norm-perfect EISENSTEIN prime.

*Proof.* Suppose  $\psi$  is an odd norm-perfect positive EISENSTEIN prime. Then,

$$3N_{\mathbb{Q}(\omega)}(\psi) = N_{\mathbb{Q}(\omega)}(\sigma_{\mathbb{Q}(\omega)}(\psi)) = N_{\mathbb{Q}(\omega)}(\psi + 1).$$

Evaluating this yields the equation

$$3(a^2 - ab + b^2) = (a + 1)^2 - (a + 1)b + b^2$$

which has the integer solutions  $a = 0, b = -1$  and  $a = b = 1$  but  $-\omega$  and  $1 + \omega$  are units and non-positive, too. Since all associates of a norm-perfect number are also norm-perfect, this is sufficient to prove the claim.  $\square$

An interesting fact is that the previous theorem is independent of our choice of the set of positive primes.

The results in this section apply solely to odd norm-perfect integers but the author believes that there is not much more that can be said about odd perfect integers and has not been listed here.

### 4.3 Cyclotomic fields of higher degree

Recall our set  $\mathcal{R}$  of cyclotomic fields over  $\mathbb{Q}$  with class number 1 and generated by  $\zeta_n$  with  $n$  being a rational prime or 4. So far, we have presented results concerning the two fields with the smallest degree,  $\mathbb{Q}(i)$  and  $\mathbb{Q}(\omega)$ . We will have a look at the other fields in  $\mathcal{R}$  and there is a nice theorem about which fields exactly are contained in it.

**Theorem 4.3.1.** [31, theorem 11.1] The numbers  $n \in \mathbb{N}$  such that  $\mathbb{Q}(\zeta_n)$  has class number 1 are:

- 1 through 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 40, 42, 44, 45, 48, 50, 54, 60, 66, 70, 84, and 90.

The set  $\mathcal{R}$  does not contain all of those fields but the number being finite tells us that the problem of (norm-)perfect numbers in such fields is a soluble one. It is even less than we may think in the first moment, since it is  $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$  for odd  $n \in \mathbb{N}$ . Thus, our shortened list of  $n$  such that  $\mathbb{Q}(\zeta_n)$  is a UFD is:

- 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, and 84.

Picking  $n$  such that  $n$  is a rational prime or 4, yields the list

- 2, 3, 4, 5, 7, 11, 13, 17, and 19.

The cases  $n \in \{2, 3, 4\}$  were dealt with in the preceding chapters and sections. Since the degree  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ , the norm of an element in  $\mathbb{Z}[\zeta_n]$  is the product of an increasing number of factors which complicates its computation. However, based on our experiences already gained, we may formulate a conjecture.

**Conjecture 4.3.2.** Let  $K = \mathbb{Q}(\zeta_p) \in \mathcal{R}$  with  $p \neq 2, 4$  where  $\zeta_p$  is the primitive  $p$ -th root of unity such that  $1 - \zeta_p$  is positive in  $\mathbb{Z}[\zeta_p]$ . Then,

- the even perfect integers in this ring are given by

$$-\zeta_p^{-1}(1 - \zeta_p)^{k-1} \left( (1 - \zeta_p)^k - 1 \right)$$

for  $k \equiv 1 \pmod{4p\mathbb{Z}}$  and  $(1 - \zeta_p)^k - 1$  being prime and

- the even norm-perfect integers are the associates of the perfect integers from item 1 and the associates of

$$(1 - \zeta_p)^{k-1} \left( \overline{(1 - \zeta_p)^k - 1} \right)$$

for  $k \equiv -1 \pmod{4p\mathbb{Z}}$  and  $(1 - \zeta_p)^k - 1$  being prime.

When we turn to the odd norm-perfect integers in  $\mathbb{Z}[\zeta_p]$ , however, presenting the form they have is possible. As

$$\mathbb{Z}[\zeta_p]/\langle 1 - \zeta_p \rangle \cong \mathbb{Z}/p\mathbb{Z},$$

we have to take care about an increasing amount of residue classes of odd primes which may be factors of an odd norm-perfect number  $\alpha$ . Thus, the simplicity of the form of  $\alpha$  heavily depends on the structure of  $(\mathbb{Z}/p\mathbb{Z})^*$ .

**Lemma 4.3.3.** Let  $p$  be an odd prime,  $a \in \mathbb{N}$  such that  $a \not\equiv 0, 1 \pmod{p\mathbb{Z}}$  and  $t$  the order of  $a$  in  $(\mathbb{Z}/p\mathbb{Z})^*$ . Then  $p \mid \sum_{k=0}^{t-1} a^k$ .

*Proof.* By assumption  $t > 1$ . Then  $a$  is a root of

$$x^t - 1 = (x - 1) \sum_{k=0}^{t-1} x^k \pmod{p\mathbb{Z}}.$$

Since  $a \not\equiv 1 \pmod{p\mathbb{Z}}$  and  $\mathbb{Z}/p\mathbb{Z}$  is a field,  $a$  has to be a root of the sum, and we get  $\sum_{k=0}^{t-1} a^k \equiv 0 \pmod{p\mathbb{Z}}$ .  $\square$

The following theorem is the generalisation of the work we got familiar with while working with odd norm-perfect EISENSTEIN integers.

**Theorem 4.3.4.** Let  $K = \mathbb{Q}(\zeta_p) \in \mathcal{R}$  with  $p \neq 2, 4$  where  $\zeta_p$  is the primitive  $p$ -th root of unity such that  $1 - \zeta_p$  is positive in  $\mathbb{Z}[\zeta_p]$ . Let  $\alpha \in \mathbb{Z}[\zeta_p]$  be an odd norm-perfect integer and

$$P_j = \{\psi \in \mathbb{P}_{\mathbb{Q}(\zeta_p)}^+ : \psi \equiv j \pmod{1 - \zeta_p} \wedge \psi \mid \alpha\}$$

for all  $j \in \{1, \dots, p-1\}$ . Then  $\alpha$  is of the form

$$\alpha = \varepsilon \psi_0^k \prod_{j=1}^{p-1} \left( \prod_{\psi_j \in P_j \setminus \{\psi_0\}} \psi_j^{e_{\psi_j}} \right)$$

where

1. each  $\psi$  with a subscript is an odd positive prime,
2.  $\varepsilon$  is a unit,
3. if  $j \neq 1$ ,  $e_{\psi_j} \not\equiv -1 \pmod{t\mathbb{Z}}$  where  $t$  is the order of  $j$  in  $(\mathbb{Z}/p\mathbb{Z})^*$ ,
4.  $e_{\psi_1} \not\equiv -1 \pmod{p\mathbb{Z}}$ , and
5. if  $\psi_0 \in P_j$  for  $j \neq 1$ , then  $k \equiv -1 \pmod{t\mathbb{Z}}$  where  $t$  is the order of  $j$  in  $(\mathbb{Z}/p\mathbb{Z})^*$ , or if  $\psi_0 \in P_1$ , then  $k \equiv -1 \pmod{p\mathbb{Z}}$ .

*Proof.* We use that, since  $\alpha$  is odd,  $N_K(\alpha)$  is not divisible by  $p$  according to Lemma 3.1.12. Thus,  $p^2 \nmid pN_K(\alpha) = N_K(\sigma_K(\alpha))$ . By the same argument as in the proof of Theorem 4.2.2, there is only one particular positive prime divisor  $\psi_0$  of  $\alpha$  such that  $p \mid N_K(\sigma_K(\psi_0^k))$  for  $k$  being the exponent of  $\psi_0$  in the prime decomposition of  $\alpha$ . For  $\psi_0 \in P_1$  this is the case if and only if  $k \equiv -1 \pmod{p\mathbb{Z}}$  and, for  $j \neq 1$  and  $\psi_0 \in P_j$ , this is the case if and only if  $k \equiv -1 \pmod{t\mathbb{Z}}$  by the previous lemma. All the other primes must not satisfy these congruence conditions.  $\square$

# Chapter 5

## Generalisation to quadratic number fields

The second type of field extensions over  $\mathbb{Q}$  that have been widely studied are the quadratic extensions.

**Lemma 5.0.1.** For any quadratic extension  $K$  of  $\mathbb{Q}$ , there is a unique square-free  $d \in \mathbb{Z}$  such that  $K \cong \mathbb{Q}(\sqrt{d})$ . The ring of integers is given by

1.  $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$  if  $d \equiv 1 \pmod{4\mathbb{Z}}$  or
2.  $\mathbb{Z}[\sqrt{d}]$  if  $d \not\equiv 1 \pmod{4\mathbb{Z}}$ .

*Proof.* Easy exercise. Recall that  $d$  is square-free, so  $d \not\equiv 0 \pmod{4\mathbb{Z}}$ . □

Since the automorphisms of such a  $K$  are given by

- $\sqrt{d} \mapsto \sqrt{d}$  and
- $\sqrt{d} \mapsto -\sqrt{d}$ ,

the norm of an element  $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$  is

$$N_{\mathbb{Q}(\sqrt{d})}(a + b\sqrt{d}) = a^2 - db^2.$$

In order to work out how we want to define positivity in these fields, we examine the unit group of its ring of integers. In any elementary algebraic number theory course, the following theorem is discussed.

**Theorem 5.0.2.** (DIRICHLET's Unit Theorem) Let  $K$  be an algebraic number field and  $[K : \mathbb{Q}] = s + 2t$  where  $s$  is the number of real embeddings and  $2t$  is the number of complex embeddings of  $K$ . Then

$$(\mathcal{O}_K)^* \cong W \times \mathbb{Z}^{s+t-1}$$

where  $W$  is the group of roots of unity in  $K$ .

Since we work with quadratic extensions, we are in the case of  $s = 2$  or  $t = 1$ , so it seems fit to distinguish between imaginary and real extensions. Additionally, we want our ring of integers to be a UFD, so we cite the following theorem.

**Theorem 5.0.3.** [18] Let  $K = \mathbb{Q}(\sqrt{d})$  be a quadratic extension of  $\mathbb{Q}$ .

1. If  $d > 0$ , then there is an undetermined number of  $d$  such that  $\mathcal{O}_K$  is a UFD.
2. If  $d < 0$ , then  $\mathcal{O}_K$  is a UFD if and only if

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

The set of the quadratic extensions of class number 1 will be denoted by  $\mathcal{Q}$ .

## 5.1 Imaginary quadratic fields

Let  $d < 0$  be a square-free rational integer throughout this section such that  $K = \mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$  if not stated otherwise. By DIRICHLET'S Unit Theorem, we have that  $(\mathcal{O}_K)^*$  is exactly the group of roots of unity in  $K$ .

**Lemma 5.1.1.** Let  $K = \mathbb{Q}(\sqrt{d})$ . It is

- $(\mathcal{O}_K)^* = \{1, i, -1, -i\}$  if  $d = -1$ ,
- $(\mathcal{O}_K)^* = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$  if  $d = -3$ , and
- $(\mathcal{O}_K)^* = \{1, -1\}$  otherwise.

*Proof.* The cases  $d = -1, -3$  were dealt with in the preceding chapters because  $\mathbb{Q}(\sqrt{-1}) \cong \mathbb{Q}(i)$  and  $\mathbb{Q}(\sqrt{-3}) \cong \mathbb{Q}(\omega)$ .

For the last case, we simply evaluate the equation

$$a^2 - db^2 = 1$$

for  $d \not\equiv 1 \pmod{4\mathbb{Z}}$  and

$$a^2 - db^2 = 4$$

for  $d \equiv 1 \pmod{4\mathbb{Z}}$  with  $a, b \in \mathbb{Z}$ . These are only soluble with  $a = \pm 1, b = 0$  which yields the claim.  $\square$

The previous theorem tells us that in the cases we have not dealt with yet, the unit group consists of  $\pm 1$ , so there are only two associates in each class. We now choose a representative system to be our set of positive primes but we point out that this is arbitrary.

**Definition 5.1.2.** Let  $K = \mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$  with rationally negative  $d \neq -1, -3$ . A prime  $\psi \in \mathcal{O}_K$  is called *positive* if either  $\Re(\psi) > 0$  or  $\Re(\psi) = 0$  and  $\Im(\psi) < 0$ . An integer  $\alpha \in \mathcal{O}_K$  is called *positive* if it is the product of positive primes. We call the sets of positive primes or integers  $\mathbb{P}_K^+$  or  $\mathcal{O}_K^+$ , respectively.

Having defined positivity, we may also define the  $\sigma$ -function on an imaginary quadratic number field.

**Definition 5.1.3.** Let  $K \in \mathcal{Q}$  such that  $K$  is an imaginary extension of the rationals. Let  $\alpha = \prod_{k=1}^l \pi_k^{e_k}$  be a positive integer in  $\mathcal{O}_K$  and  $\pi_k \in \mathbb{P}_K^+$  for all  $k$ . We define the *sum-of-divisors-function* of  $K$  as

$$\sigma_K(\alpha) = \prod_{k=1}^l \frac{\pi_k^{e_k+1} - 1}{\pi_k - 1}.$$

Furthermore, any associate of  $\alpha$  has the same value under  $\sigma_K$ . Additionally, we set  $\sigma_K(0) = 0$ .

A considerable difference to the case of cyclotomic fields is that we cannot generalise SPIRA's Lemma 3.1.3 as it is shown in the following example.

**Example 5.1.4.** Let  $K = \mathbb{Q}(\sqrt{-7})$ . Then  $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$  since  $-7 \equiv 1 \pmod{4\mathbb{Z}}$ . Then  $N_K(-\sqrt{-7}) = 7$ , so it is prime. Since  $\Re(-\sqrt{-7}) = 0$  and  $\Im(-\sqrt{-7}) < 0$ , it is also positive. By our formula,

$$N_K(\sigma_K((-\sqrt{-7})^2)) = N_K(\sqrt{-7}^2 - \sqrt{-7} + 1) = N_K(-6 - \sqrt{-7}) = 36 + 7 = 43$$

but clearly

$$N_K((-\sqrt{-7})^2) = N_K(-7) = 49,$$

so  $N_K((-\sqrt{-7})^2) > N_K(\sigma_K((-\sqrt{-7})^2))$ .

The missing piece towards defining perfect integers in imaginary quadratic fields is to find our even positive prime. Looking at the cases of the GAUSSIAN and EISENSTEIN integers and the computation done in order to present even perfect integers in those rings, we see that the important property of the prime with minimal norm  $1 - \zeta_p$  is that  $(1 - \zeta_p) - 1$  is a unit. In the cases we are looking at, i.e.  $d \neq -1, -3$ , the only non-zero integer satisfying this is 2. However, 2 is not always prime in  $\mathcal{O}_K$ . We will state two short lemmata about the ramification and splitting of rational primes in quadratic extensions but before that we will introduce a sign often used in number theory.

**Definition 5.1.5.** Let  $a \in \mathbb{Z}$  and  $p \in \mathbb{P}$ . The LEGENDRE symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \text{ is a quadratic residue modulo } p\mathbb{Z} \\ -1 & \text{otherwise} \end{cases}$$

which is determined by whether the congruence  $x^2 \equiv a \pmod{p\mathbb{Z}}$  has a solution.

**Lemma 5.1.6.** Let  $K = \mathbb{Q}(\sqrt{d})$ . Then an odd prime  $p \in \mathbb{P}$

1. ramifies if  $p \mid d$ ,
2. splits if  $\left(\frac{d}{p}\right) = 1$ , or
3. remains inert if  $\left(\frac{d}{p}\right) = -1$ .

For the prime 2, a special case applies.

**Lemma 5.1.7.** Let  $K = \mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$ . In  $\mathcal{O}_K$ , 2

1. ramifies if and only if  $d \not\equiv 1 \pmod{4\mathbb{Z}}$ ,
2. splits if and only if  $d \equiv 1 \pmod{8\mathbb{Z}}$ , or
3. is inert if and only if  $d \equiv 5 \pmod{8\mathbb{Z}}$ .

*Proofs.* These can be found in most introduction to algebraic number theory courses and are based on the DEDEKIND–KUMMER Theorem.  $\square$

**Corollary 5.1.8.** Let  $K = \mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$  be an imaginary number field with  $d \neq -1, -3$ . Then

1. the rational prime 2 remains prime in  $\mathcal{O}_K$  if and only if

$$d \in \{-11, -19, -43, -67, -163\},$$

and

2. the rational prime 3 is
  - split for  $d \in \{-2, -11\}$  and
  - inert for  $d \in \{-7, -19, -43, -67, -163\}$ .

*Proof.* This directly follows from the previous lemmata.  $\square$

This motivates the following definition that covers the cases in which 2 is the positive prime of minimal norm.

**Definition 5.1.9.** Let  $K = \mathbb{Q}(\sqrt{d})$  with  $d \in \{-19, -43, -67, -163\}$ . An integer  $\alpha \in \mathcal{O}_K$  is called *even* if it is divisible by 2, otherwise *odd*.

An integer  $\alpha \in \mathcal{O}_K$  is called

1. *perfect* if  $\sigma_K(\alpha) = 2\alpha$  and
2. *norm-perfect* if  $N_K(\sigma_K(\alpha)) = 4N_K(\alpha)$ .

Clearly, we keep the property that any perfect integer is norm-perfect, too. Since 2 is the even positive prime, we may think about the perfect rational integers to be perfect in  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$  for  $d \in \{-19, -43, -67, -163\}$  as well. If  $2^k - 1$  is prime, i.e. inert in the extension  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/\mathbb{Q}$ , then  $2^{k-1}(2^k - 1)$  is perfect by the same computation as for the rationals. Since  $d$  is a natural prime number in any case, we may use the Law of Reciprocity by GAUSS which is part of most introduction to number theory courses.

**Theorem 5.1.10.** (Law of Reciprocity by GAUSS) Let  $p, q \in \mathbb{P}$  be prime numbers. Then

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod{4\mathbb{Z}} \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases}$$



In our settings,  $d \equiv 1 \pmod{4\mathbb{Z}}$  and is a natural prime, so we are always in the second case. Hence, we are interested in computing the LEGENDRE symbol

$$\left(\frac{d}{2^k - 1}\right) = \left(\frac{2^k - 1}{d}\right)$$

for MERSENNE primes  $2^k - 1$  and  $d \in \{-19, -43, -67, -163\}$ . Firstly, we need to compute  $2^k - 1 \pmod{d\mathbb{Z}}$ . Since  $d$  is prime and thus coprime to 2, we have a quick look at the order of 2 in  $(\mathbb{Z}/d\mathbb{Z})^*$ .

$d$	order of 2 in $(\mathbb{Z}/d\mathbb{Z})^*$
-19	18
-43	14
-67	66
-163	162

Table 5.1: Order of 2 in  $(\mathbb{Z}/d\mathbb{Z})^*$

Finally, we can compute  $2^k - 1 \pmod{d\mathbb{Z}}$  for all  $d$  that we are interested in and MERSENNE primes  $2^k - 1$ . This was done using a simple *Java* program. We point out that  $d\mathbb{Z} = (-d)\mathbb{Z}$ , so switching the sign in the lower part of the LEGENDRE symbol is negligible.

$k \setminus d$	-19	$\left(\frac{2^k-1}{19}\right)$	-43	$\left(\frac{2^k-1}{43}\right)$	-67	$\left(\frac{2^k-1}{63}\right)$	-163	$\left(\frac{2^k-1}{163}\right)$
2	3	-1	3	-1	3	-1	3	-1
3	7	1	7	-1	7	-1	7	-1
5	12	-1	31	1	31	-1	31	-1
7	13	-1	41	1	60	-1	127	-1
13	2	-1	21	1	17	1	41	-1
17	9	1	7	-1	19	1	19	-1
19	1	1	31	1	12	-1	79	-1
31	2	-1	7	-1	49	1	49	1
61	13	-1	31	1	44	-1	109	-1
89	9	1	31	1	6	-1	70	1
107	9	1	38	-1	11	-1	29	-1
127	1	1	1	1	44	-1	76	-1
521	9	1	7	-1	11	-1	147	-1

Table 5.2:  $2^k - 1 \pmod{d\mathbb{Z}}$  and its LEGENDRE symbol

$k \setminus d$	-19	$\left(\frac{2^k-1}{19}\right)$	-43	$\left(\frac{2^k-1}{43}\right)$	-67	$\left(\frac{2^k-1}{63}\right)$	-163	$\left(\frac{2^k-1}{163}\right)$
607	2	-1	31	1	17	1	154	-1
1279	1	1	31	1	27	-1	106	-1
2203	13	-1	31	1	27	-1	153	-1
2281	2	-1	21	1	50	-1	41	-1
3217	2	-1	26	-1	56	-1	129	-1
4253	12	-1	26	-1	45	-1	17	-1
4423	2	-1	21	1	1	1	43	1
9689	12	-1	1	1	40	-1	75	-1
9941	12	-1	1	1	11	-1	68	-1
11213	9	1	21	1	11	-1	147	-1
19937	14	-1	1	1	31	-1	91	1
21701	14	-1	1	1	40	-1	149	-1
23209	13	-1	26	-1	47	1	71	1
44497	1	1	31	1	17	1	116	1
86243	12	-1	7	-1	30	-1	68	-1
110503	1	1	1	1	12	-1	79	-1
132049	1	1	1	1	56	-1	79	-1
216091	1	1	1	1	60	-1	106	-1
756839	14	-1	21	1	19	1	73	-1
859433	12	-1	1	1	30	-1	138	-1
1257787	1	1	21	1	27	-1	79	-1
1398269	14	-1	31	1	11	-1	10	-1
2976221	14	-1	7	-1	19	1	120	1
3021377	12	-1	38	-1	45	-1	112	1
6972593	12	-1	31	1	6	-1	63	-1
13466917	1	1	38	-1	17	1	79	-1
20996011	1	1	1	1	27	-1	1	1
24036583	2	-1	26	-1	47	1	107	-1
25964951	12	-1	31	1	6	-1	112	1
30402457	13	-1	1	1	12	-1	122	1
32582657	14	-1	38	-1	11	-1	159	-1
37156667	12	-1	38	-1	40	-1	138	-1
42643801	1	1	26	-1	17	1	45	-1
43112609	9	1	1	1	6	-1	147	-1
57885161	12	-1	31	1	11	-1	75	-1
74207281	2	-1	1	1	56	-1	12	-1

Table 5.3:  $2^k - 1 \pmod{d\mathbb{Z}}$  and its LEGENDRE symbol (continued)

Thus, by Lemma 5.1.6,  $2^{k-1}(2^k - 1)$  is perfect in  $\mathbb{Q}(\sqrt{d})$  if  $\left(\frac{2^k-1}{d}\right) = -1$ . This gives solutions for  $d \in \{-19, -43, -67, -163\}$ . The case  $d = -11$  may be treated similarly but we have to let go of the property that our positive even prime is also the positive prime of minimal norm. For the cases  $d \in \{-2, -7\}$ , we have to think of something else since 2 is not prime but this will not be discussed in this thesis.

## 5.2 Real quadratic fields

Let  $d > 0$  be a square-free integer throughout this section such that  $\mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$ . By DIRICHLET's Unit Theorem and the fact that  $\mathbb{R}$  contains only two roots of unity, we have that

$$(\mathcal{O}_K)^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Unfortunately, the list of Theorem 5.0.3 is incomplete regarding the quadratic number fields with  $d > 0$  and class number 1 but we may still find some results considering an arbitrary  $d$ . To this end, we delay the definition of being positive in  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$  and distinguish primarily between a few cases depending on the primality of 2 and 3 in  $\mathbb{Q}(\sqrt{d})$ . For this, recall the DEDEKIND–KUMMER Theorem and, especially, that  $N_{\mathbb{Q}(\sqrt{d})}(2) = 4$ .

1. 2 and 3 are inert, so 2 is a prime of minimal norm.
2. 2 is inert and 3 is not, thus the prime divisors of 3 are primes of minimal norm.
3. 2 is not inert, so its prime divisors are primes of minimal norm.

We put this together, using the Lemmata 5.1.7 and 5.1.6 from the previous section.

**Lemma 5.2.1.** Let  $K = \mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$ .

1. 2 is a prime of minimal norm if and only if  $d \equiv 5 \pmod{24\mathbb{Z}}$ .
2. 3 is non-prime and one of its prime divisors is a prime of minimal norm if and only if  $d \equiv 13, 21 \pmod{24\mathbb{Z}}$ .
3. 2 is non-prime and one of its prime divisors is a prime of minimal norm if and only if  $d \not\equiv 5 \pmod{8\mathbb{Z}}$ .

*Proof.* Lemma 5.1.6 tells us that 3 is inert in  $\mathcal{O}_K$  if and only if  $d \equiv 2 \pmod{3\mathbb{Z}}$ . We then determine the congruence classes of  $d$  modulo  $8\mathbb{Z}$  and combine these via the Chinese Remainder Theorem.

Now, we work on each case separately.

1. Case 1 lets us simply take 2 as the even positive prime. For the other cases, we now think about whether any of those primes  $\psi$  of minimal norm also satisfy the property that  $\psi - 1$  is a unit.
2. In case 2, we want to take one of the prime divisors of 3. Suppose  $\frac{a+b\sqrt{d}}{2}$  for some  $a, b \in \mathbb{Z}$  is such a prime and  $\frac{a+b\sqrt{d}}{2} - 1$  is a unit. We have the two equations

$$a^2 - db^2 = \pm 12, \quad (a - 2)^2 - db^2 = \pm 4$$

which let us divide even more cases, identified by the sign of the right-hand side of each equation.

- (a) (12, 4): Thus  $12 = 4a$  implying  $a = 3$ , so  $db^2 = -3$  which is impossible for  $d > 0$ .
- (b) (12, -4): Thus  $12 = 4a - 8$  implying  $a = 5$ , so  $db^2 = 13$ , hence  $d = 13$  and  $b = \pm 1$ .

- (c)  $(-12, 4)$ : Thus  $-12 = 4a$  implying  $a = -3$ , so  $db^2 = 21$ , hence  $d = 21$  and  $b = \pm 1$ .
- (d)  $(-12, -4)$ : Thus  $-12 = 4a - 8$  implying  $a = -1$ , so  $db^2 = 13$ , hence  $d = 13$  and  $b = \pm 1$ .

3. Case 3 is similar to case 2, we just have a look at the prime divisors of 2 instead of 3.

We will have a look at  $d \equiv 1 \pmod{4\mathbb{Z}}$  first, so suppose a prime divisor is of the form  $\frac{a+b\sqrt{d}}{2}$ . Then, we have the equations

$$a^2 - db^2 = \pm 8, \quad (a-2)^2 - db^2 = \pm 4$$

which again lets us consider a few subcases.

- (e)  $(8, 4)$ : Thus  $8 = 4a$  implying  $a = 2$ , so  $db^2 = -4$  which is impossible for  $d > 0$ .
- (f)  $(8, -4)$ : Thus  $8 = 4a - 8$  implying  $a = 4$ , so  $db^2 = -8$  implying  $d \equiv 0 \pmod{2\mathbb{Z}}$  which is a contradiction.
- (g)  $(-8, 4)$ : Thus  $-8 = 4a$  implying  $a = -2$ , so  $db^2 = 16$ , hence  $d = 1$  but  $\mathbb{Q}(\sqrt{1}) \cong \mathbb{Q}$ .
- (h)  $(-8, -4)$ : Thus  $-8 = 4a - 8$  implying  $a = 0$ , so  $db^2 = 8$  implying  $d \equiv 0 \pmod{2\mathbb{Z}}$  again.

The above subcases are impossible, therefore we now assume  $d \equiv 2, 3 \pmod{4\mathbb{Z}}$  and a prime divisor has the form  $a + b\sqrt{d}$ . This yields the equations

$$a^2 - db^2 = \pm 2, \quad (a-1)^2 - db^2 = \pm 1.$$

- (i)  $(2, 1)$ : Thus  $2 = 2a$  implying  $a = 1$ , so  $db^2 = -1$  which is impossible for  $d > 0$ .
- (j)  $(2, -1)$ : Thus  $2 = 2a - 2$  implying  $a = 2$ , so  $db^2 = 2$ , hence  $d = 2$  and  $b = \pm 1$ .
- (k)  $(-2, 1)$ : Thus  $-2 = 2a$  implying  $a = -1$ , so  $db^2 = 1$ , hence  $d = 1$ .
- (l)  $(-2, -1)$ : Thus  $-2 = 2a - 2$  implying  $a = 0$ , so  $db^2 = 2$ , hence  $d = 2$  and  $b = \pm 1$ .  $\square$

These three cases showed that we can find appropriate primes for

$$d \in \mathcal{D}' := \{2, 13, 21\} \cup (5 + 24\mathbb{N}).$$

Fortunately, all elements of the left-hand set satisfy  $\mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$ . For the right-hand set, this is unknown. We call  $\mathcal{D} \subset \mathcal{D}'$  the subset such that for  $d \in \mathcal{D}$ , we have  $\mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$ . The question we now have to take care of is whether we are able to define an appropriate set of positive primes. A few properties we probably want  $\mathbb{P}_K^+$  to have are the following:

- A)** It contains exactly one even prime. Otherwise, defining perfect numbers will be difficult. If multiple even primes occur among the positive primes, we are still able to define norm-perfect numbers though.
- B)** The primes each have a *length*, i.e. absolute value in  $\mathbb{R}$ , that is significantly different from the others in order to conserve the equation  $\sigma_K(p) = \sigma_{\mathbb{Q}}(p)$  for inert primes  $p \in \mathbb{P}$ . Additionally, this should help us to imagine the differences between two images more easily.

A crucial condition is that our positive even prime  $\psi$  satisfies  $\psi - 1 \in \mathcal{O}_K^*$ . So the following elements are possible:

1.  $d \equiv 5 \pmod{24\mathbb{Z}}$ : 2.
2.  $d = 2$ :  $\pm\sqrt{2}$  and  $2 \pm \sqrt{2}$ .
3.  $d = 13$ :  $\frac{5 \pm \sqrt{13}}{2}$  and  $\frac{-1 \pm \sqrt{13}}{2}$ .
4.  $d = 21$ :  $\frac{-3 \pm \sqrt{21}}{2}$ .

The second and third cases offer more possible representatives, so we want to have a look at how the splitting behaviour of 2 and 3 affects how reasonable the choices we have are.

**Definition 5.2.2.** Let  $K$  be a number field and  $\mathbb{P}_K = \text{Spec}(K) \setminus \{\{0\}\}$  its set of non-zero prime ideals. We define

1.  $\text{Ram}(K) := \{\mathfrak{p} \in \mathbb{P}_K : \mathfrak{p} \text{ is ramified}\}$ ,
2.  $\text{Spl}(K) := \{\mathfrak{p} \in \mathbb{P}_K : \mathfrak{p} \text{ is split}\}$ , and
3.  $\text{In}(K) := \{\mathfrak{p} \in \mathbb{P}_K : \mathfrak{p} \text{ is inert}\}$ .

Recall that we assume  $\mathcal{O}_K$  to be a PID, so all the generators are associated. Moreover, we also consider quadratic extensions only, therefore any ideal is totally ramified, split, or inert.

Because of property  $\mathcal{B}$ , we want the positive rational integer generators of the ideals in  $\text{In}(K)$  to be contained in  $\mathbb{P}_K^+$ . Lemma 3.1.8 tells us that there are only finitely many ideals in  $\text{Ram}(K)$  but, by CHEBOTAREV's Theorem, infinitely many gather in  $\text{Spl}(K)$ . We might hope to contain all the positive rational primes in  $\mathcal{O}_K^+$ .

**Example 5.2.3.** Let  $d = 21$  and  $K = \mathbb{Q}(\sqrt{21})$ , so  $\Delta_K = 21 = 3 \cdot 7$  and we know that the ramifying rational primes are 3 and 7. Suppose  $\psi = a + b\sqrt{21}$  is a positive generator of the prime ideal  $\mathfrak{p}$  such that  $\mathfrak{p}^2 = 7\mathcal{O}_K$ . As  $\psi \in \mathbb{R}$ , we have  $\psi^2 > 0$ , hence 7 is the only one among 7 and  $-7$  that can be in  $\mathcal{O}_K^+$ . However, this would imply

$$7 = a^2 + 21b^2, \quad 0 = 2ab$$

thus, by the latter equation, either  $a = 0$  or  $b = 0$  but both cases yield a contradiction to the former equation for  $a, b \in \frac{1}{2}\mathbb{Z}$ . So 7 is not a square in  $\mathcal{O}_K$  and it cannot be positive.

Even though this discovery set us back, we may let ourselves get inspired by the definition of positive primes in the cyclotomic fields in  $\mathcal{R}$ . By DIRICHLET's Unit Theorem, there is a fundamental unit which is not  $\pm 1$  and thus has absolute value other than 1, so the following definition makes sense. The separate definition for the case  $d = 2$  is due to the fact that the four possible positive even primes are all associated to each other. For this, quickly check that  $\pm\sqrt{2} \pm 1$  are units.

**Definition 5.2.4.** Let  $d \in \mathcal{D}$  such that  $K = \mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$ .  $\alpha \in \mathcal{O}_K$  is called *even* if it is divisible by a prime of minimal norm. Otherwise, it is called *odd*.

If  $d \neq 2$ , an even prime  $\psi \in \mathcal{O}_K$  is *positive* if  $\psi > 0$  and  $\psi - 1$  is a unit. Otherwise,  $\sqrt{2}$  is the positive even prime.

An odd prime  $\psi \in \mathcal{O}_K$  is *positive* if its absolute value in  $\mathbb{R}$  is the smallest amongst its associates' such that  $|\psi| \geq \sqrt{|N_K(\psi)|}$  and  $\psi > 0$ .

An integer  $\alpha$  of  $K$  is *positive* if it is the product of positive primes. We denote the sets of positive primes or integers by  $\mathbb{P}_K^+$  or  $\mathcal{O}_K^+$ , respectively.

After pondering about this for a moment, we see that the definition we chose ensures property  $\mathcal{B}$  is satisfied because  $N_K(p) = p^2$ . We can now define the sum-of-divisors function.

**Definition 5.2.5.** Let  $K = \mathbb{Q}(\sqrt{d}) \in \mathcal{Q}$  such that  $d \in \mathcal{D}$ . Let  $\alpha = \prod_{k=1}^l \pi_k^{e_k}$  be a positive integer in  $\mathcal{O}_K$  and  $\pi_k \in \mathbb{P}_K^+$  for all  $k$ . We define the *sum-of-divisors-function* of  $K$  as

$$\sigma_K(\alpha) = \prod_{k=1}^l \frac{\pi_k^{e_k+1} - 1}{\pi_k - 1}.$$

Furthermore, any associate of  $\alpha$  has the same value under  $\sigma_K$ . Additionally, we set  $\sigma_K(0) = 0$ .

It remains to evaluate whether it fulfils property  $\mathcal{A}$  as well. To this end, we need to distinguish cases again.

**Lemma 5.2.6.** Property  $\mathcal{A}$  may be satisfied for  $d \in \mathcal{D} \setminus \{13\}$ .

*Proof.* We have the four cases:

1. If  $d \equiv 5 \pmod{24\mathbb{Z}}$ , then 2 and 3 are inert, so there is only one positive even prime which is 2.
2. The discriminant of  $\mathbb{Q}(\sqrt{13})$  is 13, so 3 splits in  $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$  and  $\psi_1 \neq \psi_2$  for the two prime divisors  $\psi_1, \psi_2$  of 3. As every integer has a positive associate by definition, both associate classes have a positive representative and we cannot fulfil property  $\mathcal{A}$ .
3. Similarly, the discriminant of  $\mathbb{Q}(\sqrt{21})$  is 21, so 3 ramifies in  $\mathbb{Z}[\frac{1+\sqrt{21}}{2}]$ , thus there is only one class of associates and  $\frac{-3-\sqrt{21}}{2} < 0$  but  $\frac{-3+\sqrt{21}}{2} > 0$ .
4. If  $d = 2$ , then by definition there is only one positive even prime. □

The *good* set therefore is  $\mathcal{D} \setminus \{13\}$  and we finally derive our definition for perfect numbers in these fields.

**Definition 5.2.7.** Let  $d \in \mathcal{D} \setminus \{13\}$ ,  $K = \mathbb{Q}(\sqrt{d})$ ,  $\alpha \in \mathcal{O}_K$  and  $\psi$  be the positive even prime. We call  $\alpha$

1. *perfect* if  $\sigma_K(\alpha) = \psi\alpha$ , and
2. *norm-perfect* if  $N_K(\sigma_K(\alpha)) = N_K(\psi)N_K(\alpha)$ .

We are now interested in what these positive even primes look like.

**Lemma 5.2.8.** The positive even primes in  $\mathbb{Q}(\sqrt{d})$  are given by

1. 2 if  $d \equiv 5 \pmod{24\mathbb{Z}}$  and  $d \in \mathcal{D}$ ,
2.  $\sqrt{2}$  if  $d = 2$ , and
3.  $\frac{-3+\sqrt{21}}{2}$  if  $d = 21$ .

*Proof.* We plug in the values we received from the items (a) to (l).  $\square$

Similarly to the case of imaginary quadratic fields, proving an equivalent of the EUCLID–EULER Theorem turns out to be not quite as easy. We therefore settle for the following theorem which only presents even perfect integers in certain cases.

**Theorem 5.2.9.** Let  $K = \mathbb{Q}(\sqrt{d})$  with  $d \in \mathcal{D} \setminus \{2, 13, 21\}$ . Then

$$2^{k-1}(2^k - 1)$$

is perfect if  $2^k - 1$  is a prime.

*Proof.* Since  $d \in \mathcal{D} \setminus \{2, 13, 21\}$ , 2 is the positive even prime and thus totally inert. Similarly, if  $2^k - 1$  is prime, it is totally inert as well because it is also a rational integer. The values under  $\sigma_K$  are hence identical with those of the even perfect rational integers under  $\sigma_{\mathbb{Q}}$ .  $\square$

The remaining cases of  $d \in \{2, 21\}$  are more difficult. The author was not able to present an even perfect prime in those cases but a conjecture can be stated.

**Conjecture 5.2.10.** Let  $d \in \{2, 21\}$  and  $\psi$  be the positive prime in  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ . Then there exist  $k_d, m_d \in \mathbb{N}$  such that if  $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$  is an even perfect number, then

$$\psi^k - 1 \mid \alpha$$

for a  $k \equiv k_d \pmod{m_d \mathbb{Z}}$  such that  $\psi^k - 1$  is prime.





## Part II

# Sums of integral squares in quadratic extensions

# Chapter 6

## Sums of integral squares

In this chapter, we will focus on the equations

$$\alpha = \sum_{j=1}^k x_j^2 \tag{6.1}$$

for  $\alpha, x_j \in \mathcal{O}_K, 1 \leq j \leq k$ , for a quadratic number field  $K$ , and its corresponding counting function  $r_{k,K}(\alpha)$  as introduced in Definition 1.2.8. After pondering about the structure of a representation for a moment, we derive an easy first observation about  $r_{k,K}$ .

**Lemma 6.0.1.** Let  $K$  be a number field. For any  $\alpha \in \mathcal{O}_K \setminus \{0\}$ , it is

$$r_{1,K}(\alpha) = 2 \quad \text{or} \quad r_{1,K}(\alpha) = 0$$

corresponding to  $\alpha$  being a square in  $\mathcal{O}_K$  or not.

*Proof.* In this case, we consider the polynomial

$$f(x) = x^2 - \alpha$$

which has either two or no roots for  $\alpha \neq 0$ . □

As pointed out in Chapter 1, the integers of certain non-real subfields of  $\mathbb{C}$  lack the restrictions of squares being particular subsets, e.g.  $x^2 \in \mathbb{N}$  for any  $x \in \mathbb{Z}$ . To measure the *unrealness* of such number fields, the *Stufe* (German for *level*) has been established by many researchers.

**Definition 6.0.2.** Let  $K$  be a field. We define the *Stufe*  $\mathfrak{S}(K)$  of  $K$  to be the smallest natural number  $k$  such that  $-1$  is the sum of the squares of  $k$  elements of  $K$ . If no such  $k$  exists, then  $\mathfrak{S}(K) = \infty$  and we call  $K$  *formally real*.

Additionally, if  $K$  is a number field, we define the *integral Stufe* of  $K$  to be

$$\mathfrak{S}'(K) := \min\{k \in \mathbb{N} : r_{k,K}(-1) > 0\}.$$

If  $\mathfrak{S}'(K) = \infty$ , then we call  $K$  *integrally real*.

Notice that  $K$  may be any field. We will focus on algebraic number fields but the interested reader may be intrigued by the work by LAM [11] who investigated the Stufe in arbitrary fields.

In a way, the (integral) Stufe determines how easily the (integral) squares of a field  $K$  touch the negative real line. At this point, the author remarks that the terms *positive* and *negative* will have their familiar meaning from the real numbers from now on. A property of the Stufe which is easy to find is the following one.

**Lemma 6.0.3.** Let  $K \subset L$  be fields, then  $\mathfrak{S}(L) \leq \mathfrak{S}(K)$ . If  $K$  is a number field, then  $\mathfrak{S}(K) \leq \mathfrak{S}'(K)$ , too. Hence, every formally real number field is integrally real.

*Proof.* This follows directly from  $\mathcal{O}_K \subset K \subset L$  with the first relation only applying to number fields.  $\square$

Without any further ado, we might try to construct a field  $K$  for any natural  $k$  such that  $\mathfrak{S}(K) = k$ . This is not always possible and the question about the range of values of the Stufe has already been solved.

**Theorem 6.0.4.** [11] Let  $K$  be any field, such that  $\mathfrak{S}(K)$  is finite. Then

$$\mathfrak{S}(K) = 2^k$$

for some  $k \in \mathbb{N}$ .

For the special case of number fields, there is an improvement known as SIEGEL's Theorem. It may be derived as a corollary by combining the previous theorem with Theorem 1.2.4 because  $-1$  is an integer.

**Corollary 6.0.5.** (SIEGEL's Theorem) [11] If  $K$  is an algebraic number field in the case of Theorem 6.0.4, then  $k \in \{0, 1, 2\}$ .

LAGRANGE's Four-Square-Theorem proved that every natural number is expressible as a sum of four integral squares but it does not tell us anything about numbers that are not expressible as a sum of three such squares. ADRIEN-MARIE LEGENDRE (1752 – 1833 AD) showed that there are in fact natural numbers needing at least four squares.

**Theorem 6.0.6.** (LEGENDRE's Three-Square-Theorem) Let  $n$  be a natural number such that

$$n = 4^k(8m + 7)$$

for some  $k, m \in \mathbb{N}$ . Then  $n$  is not a sum of three rational integral squares.

Noting that  $\mathfrak{R}'(\mathbb{Q}) = \mathbb{N}$ , we may generalise this to a definition for all fields inspired by the work of JI and WEI [2].

**Definition 6.0.7.** Let  $K$  be a field. We call

$$p(K) := \inf\{k \in \mathbb{N} : \forall \alpha \in \mathfrak{R}(K) \exists x_1, \dots, x_k \in K : \sum_{j=1}^k x_j^2 = \alpha\}$$

the PYTHAGOREAN number of  $K$ . If  $p(K) = 1$ , then  $K$  is said to be PYTHAGOREAN.

Similarly, the *integral* PYTHAGOREAN number is given by

$$p'(K) := \inf\{k \in \mathbb{N} : r_{k,K}(\alpha) > 0 \forall \alpha \in \mathfrak{R}'(K)\}$$

for any number field  $K$ . If  $p'(K) = 1$ , then  $K$  is called *integrally* PYTHAGOREAN.

LAGRANGE's Theorem and Theorem 1.2.5 may thus be interpreted as

$$p'(\mathbb{Q}) = 4 \quad \text{and} \quad p'(\mathbb{Q}(\sqrt{d})) \leq 3$$

for  $d < 0$  such that  $d \equiv 1 \pmod{4\mathbb{Z}}$ . In 1993, RAJWADE proved a correlation between the Stufe and PYTHAGOREAN number of a field.

**Theorem 6.0.8.** [24] Let  $K$  be a field. Then

$$p(K) \leq \mathfrak{S}(K) + 1.$$

If  $K$  is not formally real, then also  $\mathfrak{S}(K) \leq p(K)$ .

## 6.1 The counting function in cyclotomic fields

We briefly recollect the facts we know about the equation (6.1) in the rational integers. In 1834, CARL GUSTAV JAKOB JACOBI (1804 – 1851 AD) found an explicit formula for the case of LAGRANGE's Theorem.

**Theorem 6.1.1.** (JACOBI) For any  $n \in \mathbb{N}$ , it is

$$r_4(n) = 8 \sum_{m|n, 4 \nmid m} m$$

where  $m \in \mathbb{N}$ . Moreover, if  $4 \nmid n$ , then  $r_4(n) = 8\sigma(n)$ .

Unfortunately, the last sentence is not particularly useful with respect to the first part of this thesis because, due to the EUCLID–EULER Theorem, we only know one perfect natural number being not divisible by 4 so far, which is 6.

**Lemma 6.1.2.** The following facts are true:

1.  $\mathbb{Q}$  is formally real.
2. The function  $r_{4,\mathbb{Q}}$  is unbounded but finite everywhere.

*Proof.* The proofs are short and constructive.

1. Since all squares in  $\mathbb{Q}$  are positive, their sum can never be  $-1$  which is negative.
2. The formula given by JACOBI in Theorem 6.1.1 implies  $r_{4,\mathbb{Q}}(z) < \infty$  for every  $z \in \mathbb{Z}$  since  $r_{4,\mathbb{Q}}(z) = 0$  if  $z < 0$ . Moreover, we see that the sequence

$$(a_n)_{n \in \mathbb{N}} = 3^n$$

is sent to the sequence

$$(b_n)_{n \in \mathbb{N}} = r_{4,\mathbb{Q}}((a_n)_{n \in \mathbb{N}}) = 8 \sum_{j=0}^n 3^j$$

which is unbounded. □

We also know some more things about the Stufe of a number field  $K$ .

**Theorem 6.1.3.** The following facts are true:

1. For any number field  $K$ ,  $\mathfrak{S}'(K) = 1$  if and only if  $\mathfrak{S}(K) = 1$  if and only if  $\mathbb{Q}(i) \subset K$ .
2.  $\mathfrak{S}'(\mathbb{Q}(i)) = 1$  and  $\mathfrak{S}'(\mathbb{Q}(\omega)) = 2$ .
3.  $\mathfrak{S}'(\mathbb{Q}(\zeta_n)) \leq n - 1$  for odd  $n$ .
4.  $\mathfrak{S}'(K) \leq 8$  for any non-formally real number field  $K$ . (PETERS, 1972)
5.  $\mathfrak{S}(\mathbb{Q}(\zeta_n)) = 3$  if  $m | n$  for some  $m \equiv 3 \pmod{8\mathbb{Z}}$ . (CHOWLA, 1968)

*Proof.* Again, we have some short proofs.

1. If  $\mathfrak{S}'(K) = 1$ , then  $\mathfrak{S}(K) = 1$  due to Lemma 6.0.3, so  $K$  contains a root of  $f(x) = x^2 + 1$  which are  $\pm i$ . Furthermore, if  $i \in K$ , then  $i \in \mathcal{O}_K$ , so  $\mathfrak{S}'(K) = 1$ .
2. See the above item and  $-1 = \omega^2 + (\omega^2)^2$ . It is an easy exercise to prove that  $i \notin \mathbb{Q}(\omega)$ .
3. The ring of integers is given by  $\mathbb{Z}[\zeta_n]$ , so  $\zeta_n^k \in \mathcal{O}_{\mathbb{Q}(\zeta_n)}$  for all  $1 \leq k \leq n-1$ . The group  $(W, \cdot)$  of roots of unity in  $K$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z}, +)$  via

$$\iota : W \rightarrow \mathbb{Z}/n\mathbb{Z}, \quad \zeta_n^k \mapsto k \pmod{n\mathbb{Z}},$$

so  $\iota((\zeta_n^k)^2) = 2k \pmod{n\mathbb{Z}}$ . Since 2 is coprime to  $n$ , squaring is thus bijective with  $1^2 = 1$ , so its restriction to  $W \setminus \{1\}$  is bijective as well. Hence,

$$\sum_{k=1}^{n-1} (\zeta_n^k)^2 = \sum_{k=1}^{n-1} \zeta_n^k = -1$$

because  $\zeta_n$  is a root of  $\sum_{k=0}^n x^k$  and  $x^0 = 1$ .

4. For the proof, we refer to [23].
5. For the proof, we refer to [3]. □

In 2007, JI and WEI proved the following improvement to both Theorem 1.2.5 and item 4 of the previous theorem.

**Theorem 6.1.4.** [2] Let  $K = \mathbb{Q}(\zeta_n)$  with  $n \geq 3$  and  $n \not\equiv 2 \pmod{4\mathbb{Z}}$ . Then

$$p'(K) = \begin{cases} 4 & \text{if } n \text{ is odd and the order of } 2 \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \text{ is odd,} \\ 3 & \text{otherwise.} \end{cases}$$

Moreover, if  $n$  is odd, then

$$\mathfrak{S}(K) = \begin{cases} 4 & \text{if the order of } 2 \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \text{ is odd,} \\ 2 & \text{otherwise.} \end{cases}$$

Of course—since this is a thesis in algebraic number theory—we are rather interested in  $\mathfrak{S}'(K)$  but it turns out that this not as easy because  $\mathcal{O}_K$  is a *proper* subset of  $K$ . Similarly, for the computation of the number  $p'(K)$  of any number field  $K$ , we ignore all integers of  $K$  that are not sums of integral squares. Until now, we might have hoped that, in the case of imaginary number field, we would get rid of the restriction of squares being positive and thus be able to express any integer of such a field as sum of squares. However, this is not possible as pointed out in Theorem 1.2.5.

**Example 6.1.5.** Consider  $K = \mathbb{Q}(i)$ , so any non-zero element is totally positive. Then  $i \in \mathcal{O}_K$  and

$$i = \frac{i}{2} + \frac{i}{2} + 0 + 0 = \left(\frac{1+i}{2}\right)^2 + \left(\frac{1+i}{2}\right)^2 + 0^2 + 0^2,$$

as we know from Theorem 1.2.4. However,  $\frac{1+i}{2}$  is not an algebraic integer because its minimal polynomial over  $\mathbb{Z}$  is  $2x^2 - 2x + 1$ .

Moreover, we if we take  $a + bi \in \mathbb{Z}[i]$  with  $a, b \in \mathbb{Z}$ , then

$$(a + bi)^2 = a^2 - b^2 + 2abi,$$

so the imaginary part of any sum of integral squares is an even rational integer and hence,  $i$  is not the sum of any number of integral squares in  $K$ .

In Theorem 6.1.1, JACOBI provided a closed formula for  $r_{4, \mathbb{Q}}$  but restricted to the set  $\mathbb{N} = \mathfrak{R}'(\mathbb{Q})$ . Here, we will discuss the appearance of certain special values.

**Lemma 6.1.6.** Let  $K$  be a number field and  $k \in \mathbb{N}$ . Then

$$\binom{m}{k} r_{k, K}(\alpha) \leq r_{m, K}(\alpha)$$

for all  $\alpha \in \mathcal{O}_K$  and  $k \leq m$ .

*Proof.* We may add arbitrarily many zeros to any sum without changing its value and  $0^2 = 0$ . The binomial coefficient is derived from the fact that we may put the  $k$  entries of a representation of  $k$  squares in any of the  $m$  entries of the larger representation.  $\square$

We will start with  $\mathbb{Q}(i)$  being the most common of these extensions. Due to Theorem 1.2.5 and Example 6.1.5, we know that  $\mathfrak{R}'(\mathbb{Q}(i)) = \{a + bi : a, b \in \mathbb{Z}, 2 \mid b\}$ . It also tells us that we are interested in  $r_{3, \mathbb{Q}(i)}$  rather than  $r_{4, \mathbb{Q}(i)}$  but it only provides the fact that  $r_{3, \mathbb{Q}(i)}(\alpha) > 0$  for all  $\alpha \in \mathfrak{R}'(\mathbb{Q}(i))$ . A particular property of the GAUSSIAN integers regarding squares is that they contain  $i$  which leads to this first observation.

**Lemma 6.1.7.** Let  $\alpha \in \mathbb{Z}[i]$  such that  $\alpha = \beta^2$  for some  $\beta \in \mathbb{Z}[i]$ . Then  $r_{k, \mathbb{Q}(i)}(\alpha) = \infty$  for all  $m \in \mathbb{N}_{\geq 3}$ .

*Proof.* For any  $s \in \mathbb{Z}$ , it is

$$\alpha = \beta^2 = \beta^2 + s^2 - s^2 = \beta^2 + s^2 + (si)^2$$

a sum of three integral squares. Hence,

$$(\beta, s, si) \in \left\{ (x_1, \dots, x_k) \in \mathcal{O}_K^k : \sum_{j=1}^k x_j^2 = \alpha \right\},$$

for infinitely many  $s$ . So  $r_{3, \mathbb{Q}(i)}(\alpha) = \infty$ , and the claim follows by the previous lemma.  $\square$

This is a huge difference compared to the second item of Lemma 6.1.2. However, squares are in fact only sporadically distributed amongst the GAUSSIAN integers as we see in the figure below.

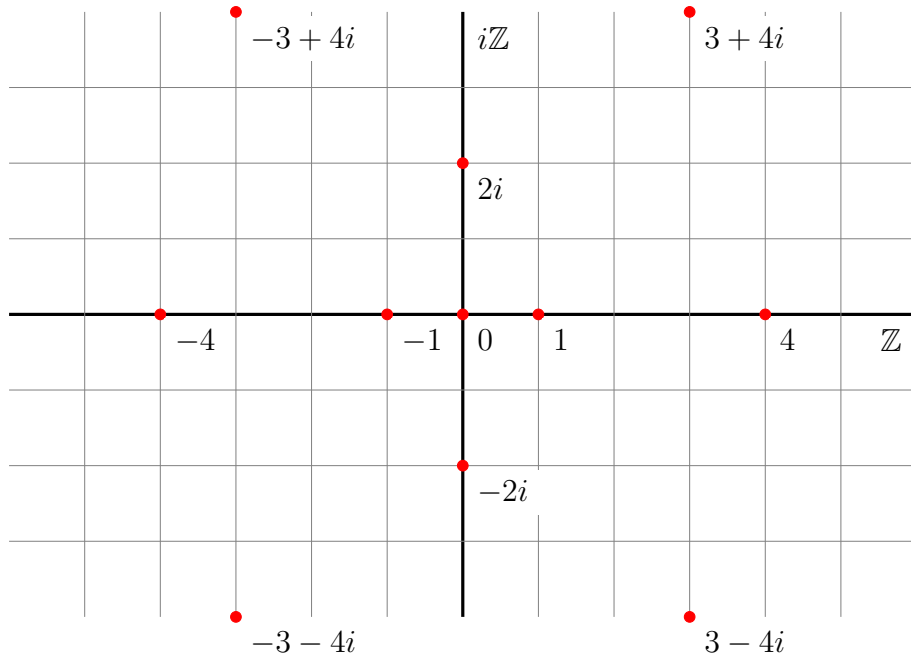


Figure 6.1: The integral squares near the origin in the GAUSSIAN integers

But the previous lemma also raises the question whether computing  $r_{3, \mathbb{Q}(i)}(\alpha)$  for any arbitrary GAUSSIAN integer  $\alpha$  is a task that can be done in a reasonable amount of time and whether we find any good ansatz to cope with the possibilities given by non-integrally real fields. Focusing on the number of representations  $r_{3, \mathbb{Q}(i)}$  of rational integers with three squares from  $\mathbb{Z}[i]$  may help because we are far more familiar with the arithmetic on  $\mathbb{Z}$ . Before proving Lemma 6.1.9, we start with a useful lemma about the rational integers.

**Lemma 6.1.8.** Let  $n$  be an arbitrary rational integer.

1. If  $n \equiv 2, 3 \pmod{4\mathbb{Z}}$ , then there are infinitely many  $l, m \in \mathbb{Z}$  such that

$$n = 2(2m + 1) + l^2.$$

2. If  $n \equiv 1 \pmod{4\mathbb{Z}}$ , then there are infinitely many  $l, m \in \mathbb{Z}$  such that

$$n = 2(2m + 1) - l^2.$$

3. If  $n \equiv 0 \pmod{4\mathbb{Z}}$ , then there are infinitely many  $l, m \in \mathbb{Z}$  such that

$$n = 8(m + 1) + l^2.$$

*Proof.* We handle each case separately.

1. Suppose  $n \equiv 2, 3 \pmod{4\mathbb{Z}}$ . Choose  $l$  to be an integer such that  $l \equiv n \pmod{2\mathbb{Z}}$ , so  $l^2 + 2 \equiv n \pmod{4\mathbb{Z}}$  implying  $l^2 + 2 = n - 4m$  for some  $m \in \mathbb{Z}$ . Rearranging yields the claim.
2. Suppose  $n \equiv 1 \pmod{4\mathbb{Z}}$ . Choose  $l$  to be an odd integer, so  $l^2 \equiv n \equiv 1 \pmod{4\mathbb{Z}}$  implying  $2 - l^2 = n - 4m$  for some  $m \in \mathbb{Z}$  which yields the claim.

3. Suppose  $n \equiv 0 \pmod{4\mathbb{Z}}$ . Let  $l$  be a rational integer such that  $l^2 \equiv n \pmod{8\mathbb{Z}}$ , so  $l^2 = n - 8m'$  for some  $m' \in \mathbb{Z}$ . Substituting  $m'$  by  $m + 1$  finishes the proof.  $\square$

It feels natural to include the  $l$  of such a representation to the representation of a rational integer  $n$  as sum of four integral squares from the GAUSSIAN integers. The question how to express the other term as a sum of two squares will be answered in the next lemma.

**Lemma 6.1.9.** It is

$$r_{k, \mathbb{Q}(i)}(n) = \infty$$

for all  $n \in \mathbb{Z}$  and  $k \geq 3$ .

*Proof.* Due to Lemma 6.1.6, we only need to prove this for  $k = 3$ . For this, we will use the following identity

$$\pm 2mg + g^2 = (m \pm g)^2 - m^2 \tag{6.2}$$

which hold for all  $m, g \in \mathbb{N}$ . We now distinguish the same cases as in Lemma 6.1.8 which gives us infinitely many pairs  $(l, m)$  for a certain representation.

1. Suppose  $n \equiv 2, 3 \pmod{4\mathbb{Z}}$ . Then use 6.2 with  $g = 1$ , so

$$\begin{aligned} n &= 2(2m + 1) + l^2 \\ &= 2[(m + 1)^2 - m^2] + l^2 \\ &= 2[(m + 1)^2 - m^2] + 2(m + 1)mi - 2(m + 1)mi + l^2 \\ &= [(m + 1) + mi]^2 + [(m + 1) - mi]^2 + l^2. \end{aligned}$$

2. Suppose  $n \equiv 1 \pmod{4\mathbb{Z}}$ . Then use 6.2 with  $g = 1$ , so

$$\begin{aligned} n &= 2(2m + 1) - l^2 \\ &= 2[(m + 1)^2 - m^2] + (li)^2 \\ &= 2[(m + 1)^2 - m^2] + 2(m + 1)mi - 2(m + 1)mi + (li)^2 \\ &= [(m + 1) + mi]^2 + [(m + 1) - mi]^2 + (li)^2. \end{aligned}$$

3. Suppose  $n \equiv 0 \pmod{4\mathbb{Z}}$ . Then use 6.2 with  $g = 2$ , so

$$\begin{aligned} n &= 2(4m + 4) + l^2 \\ &= 2[(m + 2)^2 - m^2] + l^2 \\ &= 2[(m + 2)^2 - m^2] + 2(m + 2)mi - 2(m + 2)mi + l^2 \\ &= [(m + 2) + mi]^2 + [(m + 2) - mi]^2 + l^2. \end{aligned}$$

This finishes the proof.  $\square$

So far we found a subset of the set

$$\{\alpha \in \mathbb{Z}[i] : r_{3, \mathbb{Q}(i)}(\alpha) = \infty\} \subset \mathfrak{R}'(\mathbb{Q}(i))$$

whose elements each have infinitely many representations and a set  $\mathbb{Z}[i] \setminus \mathfrak{R}'(\mathbb{Q}(i))$  whose elements have none whatsoever. This is last set is in fact non-empty as we saw in Example 6.1.5 because the imaginary part of a sum of squares is always an even rational integer. The author has not been able to prove or disprove the following conjecture so far but is fairly interested in its resolution.



**Conjecture 6.1.10.** For every  $\alpha \in \mathbb{Z}[i]$ , it is either  $r_{3, \mathbb{Q}(i)}(\alpha) = 0$  or  $r_{3, \mathbb{Q}(i)}(\alpha) = \infty$ .

As we did before in the course of this thesis, we will have a look at the case of the EISENSTEIN integers next. Since  $i \notin \mathbb{Q}(\omega)$ , there are no non-zero pairs  $\alpha, \beta \in \mathbb{Z}[\omega]$  such that  $\alpha^2 = -\beta^2$ , so we will not be able to use the trick from Lemma 6.1.7. Moreover, due to Theorem 1.2.5, we know that  $r_{3, \mathbb{Q}(\omega)}(\alpha) > 0$  for all  $\alpha \in \mathbb{Z}[\omega]$ . Being able to use three squares makes it still possible to find at least one element which has infinitely many representations:

$$0 = 0 \cdot \alpha^2 = (1 + \omega + \omega^2)\alpha^2 = \alpha^2 + (\omega^2\alpha)^2 + (\omega\alpha)^2$$

for all  $\alpha \in \mathbb{Z}[\omega]$ .

## 6.2 Non-cyclotomic quadratic extensions

Proceeding in the same fashion as in the first part of this thesis, we will now consider the non-cyclotomic quadratic extension of the rationals and—once again—there is a difference between the real and imaginary ones. Each one has a particular advantage compared to the other.

This time, we start with the real extensions. The advantage they have compared to the imaginary extensions is that every square is positive. It follows straight from the definition and the property of squares of real numbers being positive that every real extension of  $\mathbb{Q}$  is formally real. Among these fields, there is one standing out.

**Theorem 6.2.1.** (GÖTZKY [8]) Let  $K$  be a real quadratic extension of  $\mathbb{Q}$  such that every totally positive integer of  $\mathcal{O}_K$  is the sum of four integral squares from  $K$ . Then  $K = \mathbb{Q}(\sqrt{5})$ .

The similarity to LAGRANGE'S Four-Square-Theorem is remarkable. This was later improved by MAASS [13].

**Lemma 6.2.2.** Every totally positive integer of  $\mathbb{Q}(\sqrt{5})$  is the sum of three integral squares.

In 2016, THOMPSON [29] presented explicit formulas for  $r_{4, \mathbb{Q}(\sqrt{5})}$  and  $r_{4, \mathbb{Q}(\sqrt{2})}$  using modular forms and the theory of local densities by SIEGEL.

**Theorem 6.2.3.** The following formulas hold:

1. If  $\alpha \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$  is totally positive, then

$$r_{4, \mathbb{Q}(\sqrt{5})}(\alpha) = 8 \sum_{0 \neq \langle d \rangle | \langle \alpha \rangle} N_{\mathbb{Q}(\sqrt{5})}(d) - 4 \sum_{\langle 2 \rangle | \langle d \rangle | \langle \alpha \rangle} N_{\mathbb{Q}(\sqrt{5})}(d) + 8 \sum_{\langle 4 \rangle | \langle d \rangle | \langle \alpha \rangle} N_{\mathbb{Q}(\sqrt{5})}(d).$$

2. If  $\alpha \in \mathbb{Z}[\sqrt{2}]$  is expressible as sum of four integral squares, then

$$r_{4, \mathbb{Q}(\sqrt{2})}(\alpha) = 8 \sum_{0 \neq \langle d \rangle | \langle \alpha \rangle} N_{\mathbb{Q}(\sqrt{2})}(d) - 6 \sum_{\langle 2 \rangle | \langle d \rangle | \langle \alpha \rangle} N_{\mathbb{Q}(\sqrt{2})}(d) + 4 \sum_{\langle 4 \rangle | \langle d \rangle | \langle \alpha \rangle} N_{\mathbb{Q}(\sqrt{2})}(d).$$

By Lemma 6.1.6, we deduce  $r_{3, \mathbb{Q}(\sqrt{5})}(\alpha) < \infty$  for all  $\alpha \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$  or fitting  $\alpha \in \mathbb{Z}[\sqrt{2}]$  because each ideal of those rings has only finitely many divisors and the norm of each of those is finite.

The imaginary non-cyclotomic quadratic extensions are still very close to the cyclotomic extensions  $\mathbb{Q}(i)$  and  $\mathbb{Q}(\omega)$ . Theorem 1.2.5 tells us that, for any extension  $\mathbb{Q}(\sqrt{d})$  with  $d < 0$ , we have  $r_{3, \mathbb{Q}(\sqrt{d})}(\alpha) > 0$  for all  $\alpha \in \mathfrak{R}'(\mathbb{Q}(\sqrt{d}))$ . Moreover, it tells us that its integral Stufe satisfies

$$1 \leq \mathfrak{S}'(\mathbb{Q}(\sqrt{d})) \leq 3.$$

The extensions we are interested in right now are non-cyclotomic, so by Theorem 6.1.3 the lower bound can be improved such that

$$\mathfrak{S}'(\mathbb{Q}(\sqrt{d})) \in \{2, 3\}.$$

Thus, in order to determine the integral Stufe of an imaginary quadratic extension  $K = \mathbb{Q}(\sqrt{d})$ , we only need to check whether  $-1$  is expressible as sum of two squares. Fortunately, NIVEN stated sufficient and necessary conditions for an integer of an imaginary quadratic extension to be expressible as sum of two squares with rational integral coefficients.

**Theorem 6.2.4.** [20, p. 410] Let  $K = \mathbb{Q}(\sqrt{d})$  be an imaginary quadratic extension with  $d \not\equiv 1 \pmod{4\mathbb{Z}}$  and  $\alpha = a + 2b\sqrt{d} \in \mathcal{O}_K$ .  $\alpha$  is expressible as a sum of two squares of integers of  $\mathcal{O}_K$  with rational integral coordinates if and only if there exists an integer  $t$  such that

$$(-d)t^2 + at - b^2$$

is a perfect square such that the greatest common divisor of  $t, b$  and  $a - dt$  is not divisible by an odd power of a prime congruent to 3 modulo  $4\mathbb{Z}$ .

There are two important details in this theorem that we must pay close attention to:

1. A perfect square is meant to be non-zero, and
2. the phrase “with rational integral coordinates” means that we only consider squares of integers of the form  $e + f\sqrt{d}$  with  $e, f \in \mathbb{Z}$ , regardless of  $d$ . Thus, we cannot say much about the case when  $d \equiv 1 \pmod{4\mathbb{Z}}$ .

**Corollary 6.2.5.** Let  $d \not\equiv 1 \pmod{4\mathbb{Z}}$  be a square-free negative rational integer. It is  $\mathfrak{S}'(\mathbb{Q}(\sqrt{d})) = 2$  if and only if  $-dt_0^2 = n^2 + 1$  for some  $t_0, n \in \mathbb{N} \setminus \{0\}$ .

*Proof.* We apply the previous theorem. In the case of  $\alpha = -1$ , we have

$$(-d)t^2 + at - b^2 = (-d)t^2 - t - 0^2 = (-dt - 1)t.$$

The two factors on the right-hand side are coprime, so in order for the product to be a perfect square, both of them have to be perfect squares. As 0 is not a perfect square,  $t \neq 0$  and by an assumption  $d \neq 0$ . Rearranging and setting  $t = t_0^2$  yields the *only-if*-direction.

Conversely, the greatest common divisor of  $t = t_0^2, b = 0$  and  $a - dt = n^2$  satisfies the condition from Theorem 6.2.4 because  $t_0$  and  $n^2 = -dt_0^2 - 1$  are coprime.  $\square$

Finding a solution to the equation

$$x^2 + y^2 = -1$$

in  $\mathbb{Z}[\sqrt{d}]$  in the case of  $-dt_0^2 = n^2 + 1$  for some  $t_0, n \in \mathbb{N}$  is given by

$$x = n, \quad y = t_0\sqrt{d}.$$

A closer look to the condition of Corollary 6.2.5 reveals that the  $d < 0, d \not\equiv 1 \pmod{4\mathbb{Z}}$  whose Stufe is 2 are exactly those for which the negative PELL's equation

$$x^2 + dy^2 = -1 \tag{6.3}$$

is soluble in the rational integers. The list of the first few such  $-d$  is given by the sequence [A031396](#) (excluding 1) in the OEIS. Again, this is not a necessary condition for  $\mathfrak{S}'(\mathbb{Q}(\sqrt{d})) = 2$ . Notably, Equation 6.3 is not soluble if  $d$  is divisible by a natural prime  $p \equiv 3 \pmod{4\mathbb{Z}}$  because  $-1$  is not a quadratic residue modulo  $p$  for such  $p$ . Nevertheless, we saw in Theorem 6.1.3 that  $\mathfrak{S}'(\mathbb{Q}(\sqrt{-3})) = 2$ . More involved results concerning the integral Stufe of certain algebraic number fields and related invariants thereof may be found in [23].

We may use our knowledge about deriving solutions for PELL's equation from the so-called *fundamental* solution.

**Lemma 6.2.6.** Let  $d < -1$  be a square-free rational integer such that

$$x^2 + dy^2 = -1$$

is soluble. Then  $r_{2, \mathbb{Q}(\sqrt{d})}(-\alpha^2) = \infty$  for all  $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ .

*Proof.* From basic number theory, we know that due to  $d < -1$  if one solution exists, then there infinitely many solutions for the equation above. This produces the solutions for  $\alpha = -1$ . For arbitrary  $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ , just multiply each pair of those solutions by  $\alpha$ .  $\square$

If we wish to be able to somehow compare this result to the one we have about  $r_{3, K}$  where  $K$  is either  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\omega)$ , we may just combine the previous Lemma with Lemma 6.1.6. That is, if  $d$  satisfies Lemma 6.2.6, then

$$r_{3, \mathbb{Q}(\sqrt{d})}(-\alpha^2) = r_{3, \mathbb{Q}(i)}(\beta^2) = r_{3, \mathbb{Q}(\omega)}(0) = \infty$$

with  $\alpha \in \mathbb{Q}(\sqrt{d})$  and  $\beta \in \mathbb{Z}[i]$  arbitrary.

# Chapter 7

## Prime numbers of the form $\alpha^2 + d\beta^2$

In this chapter, we will focus on the Equation 1.3 applied to a quadratic number field  $K$ :

$$\psi = \alpha^2 + d\beta^2 \tag{7.1}$$

with square-free  $d \in \mathbb{Z}$ ,  $\psi$  a prime element of  $\mathcal{O}_K$  and  $\alpha, \beta \in \mathcal{O}_K$ . COX proved the following formidable theorem over the rationals.

**Theorem 7.0.1.** [5, p. 98] Let  $d > 0$  be a square-free integer with  $d \not\equiv 3 \pmod{4\mathbb{Z}}$ . Then there is a monic irreducible polynomial  $g_d \in \mathbb{Z}[t]$  such that if an odd natural prime  $p$  divides neither  $d$  nor the discriminant of  $g_d$ , then

$$p = x^2 + dy^2 \iff \begin{cases} \left(\frac{-d}{p}\right) = 1 \text{ and } g_d(t) \equiv 0 \pmod{p\mathbb{Z}} \\ \text{has a rational integer solution.} \end{cases}$$

Furthermore,  $g_d$  may be taken to be the minimal polynomial of a real algebraic integer  $\alpha$  for which  $L = K(\alpha)$  is the HILBERT class field of the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{-d})$ .

Under the assumption that we know the HILBERT class field of a number field  $K$ —which is equivalent to knowing  $g_d$  by the latter part of the above theorem—, finding those natural primes  $p$  turns out to be fairly simple. Be that as it may, this only applies to  $d \not\equiv 3 \pmod{4\mathbb{Z}}$ . Fortunately, COX was also able to solve Equation 1.3 for any  $d$ , even non-square-free.

**Theorem 7.0.2.** [5, p. 180] Let  $d > 0$  be an integer. Then there is a monic irreducible polynomial  $f_d \in \mathbb{Z}[t]$  such that if an odd natural prime  $p$  divides neither  $d$  nor the discriminant of  $f_d$ , then

$$p = x^2 + dy^2 \iff \begin{cases} \left(\frac{-d}{p}\right) = 1 \text{ and } f_d(t) \equiv 0 \pmod{p\mathbb{Z}} \\ \text{has a real integer solution.} \end{cases}$$

Furthermore,  $f_d$  may be taken to be the minimal polynomial of a real algebraic integer  $\alpha$  for which  $L = K(\alpha)$  is the ring class field of the ring  $\mathbb{Z}[\sqrt{-d}]$  in the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{-d})$ .

The remarkable part is the equivalence and the existence of the polynomial  $f_d$  in particular. The so-called *ring class field* is a generalisation of the HILBERT class field. It is one of the class fields which arise from the study of ABELIAN extensions.

## 7.1 A short insight to class field theory

In this section, we will recapitulate some chapters of COX's book *Primes of The Form  $x^2 + ny^2$*  [5]. Most of the definitions and notations are standard if not stated otherwise.

**Definition 7.1.1.** Let  $K$  be a number field. We call a GALOIS extension  $L/K$  ABELIAN if  $\text{Gal}(L/K)$  is ABELIAN.

ABELIAN extensions are the foundation of class field theory. The most prominent example is called the HILBERT class field. For this, we first need another last definition.

**Definition 7.1.2.** Let  $K$  be a number field. We call

1. the prime ideals  $\mathfrak{P} \subset \mathcal{O}_K$  the *finite places* of  $K$ , and
2. the real embeddings  $\sigma$  of  $K$  the *infinite places* of  $K$ .

An infinite place is said to ramify in  $L/K$  if there are two different embeddings  $\sigma_1, \sigma_2$  of  $L$  whose restrictions to  $K$  are both identical to  $\sigma$ . An extension  $L/K$  is said to be unramified if none of its places ramifies. A *product* of places is called a *modulus*.

The HILBERT class field  $H(K)$  has a few fascinating properties which are closely related to the splitting behaviour of the prime ideals of  $\mathcal{O}_K$ .

**Theorem 7.1.3.** Let  $K$  be a number field. Then there is a unique maximal unramified ABELIAN extension of  $K$ , the HILBERT class field  $H(K)$ .

1. It is

$$\text{Gal}(H(K)/K) \cong \text{Cl}(K) = I_K/P_K.$$

2. A prime ideal  $\mathfrak{P} \subset \mathcal{O}_K$  totally splits in  $H(K)$  if and only if it is principal.

The first item of the above theorem explains why the case of  $\mathbb{Z}[\sqrt{-d}]$  being a UFD may be easily solved. In that case,  $I_K = P_K$ , so the class number is 1 and  $H(K) = K$ . Henceforth, the polynomial  $g_d$  from Theorem 7.0.1 is linear and leaves the solubility of the Equation 1.3 solely relying on  $-d$  being a quadratic residue modulo  $p$  or not.

The second item presents the reason why we need to substitute the HILBERT class field by the ring class field in Theorem 7.0.2. As pointed out in Chapter 1, we are only interested in integer solutions of Equation 1.3, thus in the decomposition

$$p = x^2 + dy^2 = (x + y\sqrt{-d})(x - y\sqrt{-d})$$

in  $\mathbb{Z}[\sqrt{-d}]$  but this ring is not  $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$  for  $d \equiv 3 \pmod{4}$ . In order to have a similar statement about the splitting of a prime ideal  $\mathfrak{P} \subset \mathbb{Z}[\sqrt{-d}]$  we must consider the ring class field and adjust our definitions concerning the fractional ideal groups of a number field.

**Definition 7.1.4.** [5] Let  $K$  be a number field and  $\mathfrak{m}$  a modulus of  $K$ . We define

$$I_K(\mathfrak{m}) := \{\mathfrak{a} \in I_K : \mathfrak{a} \text{ is coprime to } \mathfrak{m}\}.$$

Likewise, for  $\alpha \in \mathcal{O}_K$ ,

$$P_{K,\alpha}(\mathfrak{m}) := \{\mathfrak{a} \in P_K \cap I_K(\mathfrak{m}) : \exists \beta \in \mathcal{O}_K \text{ such that } \beta \equiv \alpha \pmod{\mathfrak{m}} \wedge \mathfrak{a} = \beta \mathcal{O}_K\}.$$

We also define

$$P_{K,\mathbb{Z}}(\mathfrak{m}) := \{\mathfrak{a} \in P_K \cap I_K(\mathfrak{m}) : \exists \beta \in \mathcal{O}_K \text{ such that } \beta \equiv \alpha \pmod{\mathfrak{m}} \text{ with } \alpha \mathcal{O}_K \text{ and } \mathfrak{m} \text{ being coprime } \wedge \mathfrak{a} = \beta \mathcal{O}_K\}.$$

It is important to keep in mind that in the case of the definition of  $P_{K,\mathbb{Z}}(\mathfrak{m})$  the symbol  $\mathbb{Z}$  is used in lack of a better option. At first sight, we may think that this yields groups completely different from  $I_K$  and  $P_K$ . In fact, there are ways in interpret those groups in terms of Definition 7.1.4.

**Lemma 7.1.5.** [5] It is

$$Cl(K) = I_K/P_K = I_K(\mathcal{O}_K)/P_{K,\mathbb{Z}}(\mathcal{O}_K) = I_K(\mathcal{O}_K)/P_{K,1}(\mathcal{O}_K)$$

for any number field  $K$ .

*Proof.* The ring  $\mathcal{O}_K$  is coprime to all of its ideals and every element is congruent to 1 modulo  $\mathcal{O}_K$ .  $\square$

In class field theory, a certain kind of groups is introduced in order to work with the splitting behaviour of ideals in general subrings of  $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$  for any  $d \in \mathbb{N}$ .

**Definition 7.1.6.** [5, p. 160] Let  $K$  be a number field,  $\mathfrak{m}$  a modulus of  $K$ , and  $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$  a group. Then we call

$$Cl_H(\mathfrak{m}) := I_K(\mathfrak{m})/H$$

a *generalised ideal class group* of  $\mathfrak{m}$ .

In class field theory, we finally may use the Existence Theorem to connect those generalised ideal class groups to certain class fields.

**Theorem 7.1.7.** (Existence Theorem) [5, p. 162] Let  $\mathfrak{m}$  be a modulus of a number field  $K$ , and let  $H$  be a congruence subgroup for  $\mathfrak{m}$ , i. e.,

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Then there exists a unique ABELIAN extension  $L$  of  $K$ , all of whose ramified places, finite or infinite, divide  $\mathfrak{m}$ , such that if

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \rightarrow \text{Gal}(L/K)$$

is the ARTIN map of  $K \subset L$ , then

$$H = \ker(\Phi_{\mathfrak{m}}).$$

*Proof.* See JANUSZ [9, Chapter V, Theorem 9.16].  $\square$

Here, the correspondence to the generalised ideal groups is clearly visible by the fact that such a group is given by the quotient of  $I_K$  and a congruence subgroup  $H$ . The GALOIS group of the extension  $L/K$  is isomorphic to that quotient. To put this into the context of Definition 7.1.6, we point out that  $P_{K,1}(\mathfrak{m})$  and  $P_{K,\mathbb{Z}}(\mathfrak{m})$  are such possible subgroups. We may finally define the ring class field.

**Definition 7.1.8.** [5] Let  $\mathfrak{m}$  be a modulus of an imaginary quadratic number field  $K$ . We call the extension  $L$  of  $K$  given by the Existence Theorem, the modulus  $\mathfrak{m}$ , and

1. the congruence subgroup  $P_{K,\mathbb{Z}}(\mathfrak{m})$  the *ring class field of conductor  $\mathfrak{m}$* , and
2. the congruence subgroup  $P_{K,1}(\mathfrak{m})$  the *ray class field of conductor  $\mathfrak{m}$* .

For a subring  $R \subset \mathcal{O}_K$  with  $[\mathcal{O}_K : R] = c < \infty$ , we call the ring class field of conductor  $c\mathcal{O}_K$  also the ring class field of  $R$  in  $K$ .

## 7.2 The case of $d = 1$

Throughout this short section, we will briefly collect the known facts on the popular case  $d = 1$ , i. e., we will have a look at further investigations regarding the expressions

$$\psi = \alpha^2 + \beta^2$$

for a prime element  $\psi \in \mathbb{P}_K$  and integral  $\alpha, \beta \in \mathcal{O}_K$  where  $K$  is a number field. If  $\psi \equiv 1 \pmod{4\mathbb{Z}}$  is a natural prime, then we know by Theorem 1.2.1 that solutions  $(\alpha, \beta) \in \mathbb{Z}^2 \subset \mathcal{O}_K^2$  exist. If we do not restrict ourselves to find an equivalent condition as in Theorem 7.0.2, we may separate  $\alpha \in \mathbb{Z}$  and  $\beta \in \mathcal{O}_K \setminus \mathbb{Z}$  in order to be able to use COX's results to say something about those  $\psi$  in  $\mathcal{O}_K$  and squares in  $\mathbb{Z}[\sqrt{n}]$ .

**Theorem 7.2.1.** Let  $n > 0$  be a square-free integer. Then there is a monic irreducible polynomial  $f_n \in \mathbb{Z}[t]$  as described in Theorem 7.0.2 such that if an odd natural prime  $p$  divides neither  $n$  nor the discriminant of  $f_n$ , then  $p$  is the sum of two integral squares from  $\mathbb{Z}[\sqrt{n}]$  if

$$\left(\frac{-n}{p}\right) = 1 \quad \text{and} \quad f_n(t) \equiv 0 \pmod{p\mathbb{Z}} \text{ has an integer solution.}$$

Moreover,  $f_n$  may be chosen to be the minimal polynomial of a real algebraic integer  $\alpha$  such that  $K(\alpha)$  is the ring class field of  $\mathbb{Z}[\sqrt{-n}]$  in  $K = \mathbb{Q}(\sqrt{-n})$ .

*Proof.* The solution  $(x, y) \in \mathbb{Z}^2$  for

$$p = x^2 + ny^2$$

we obtain from Theorem 7.0.2 yields the solutions  $(\alpha, \beta) = (x, y\sqrt{n})$  for the equation

$$p = \alpha^2 + \beta^2$$

in  $\mathbb{Z}[\sqrt{n}]^2$ . □

It is important to note that this theorem relies on a certain construction. Thus, it does not provide an equivalence because  $\mathbb{Z} \subset \mathbb{Z}[\sqrt{n}]$ .

**Example 7.2.2.** Let  $K = \mathbb{Q}(\sqrt{3})$ , so  $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ , and  $p = 5$ . We deduce  $H(K) = K$  because  $\mathcal{O}_K$  is a PID. Furthermore,

$$\left(\frac{-3}{5}\right) = \left(\frac{2}{5}\right) = -1$$

but  $5 = 1^2 + 2^2$  and  $1, 2 \in \mathcal{O}_K$ .

A similar approach may be used to find solutions for the case of negative  $n$ . The DIOPHANTINE equations

$$p = x^2 + ny^2$$

with  $n < 0$  are known as *generalised PELL's equations*. LAGRANGE reduced the question to the case  $|p| < \sqrt{-n}$ . However, finding fundamental solutions is not as simple. CONRAD treated this case in an article [4].

Some work about the general case of a quadratic number field  $K$  has been done by ELIA and MONICO in [6] and [7] for the fields  $\mathbb{Q}(\sqrt{5})$  and  $\mathbb{Q}(\sqrt{2})$  respectively. Furthermore, NAGELL [16, 17] examined the cases  $K = \mathbb{Q}(\sqrt{n})$  where

$$n \in \{\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 19, \pm 43, \pm 67, \pm 163\}$$

using the fact that, in those cases, the class number of  $\mathbb{Q}(\sqrt{n}, \sqrt{-n})$  is 1. WEI [32] studied various cases, depending on certain congruence conditions given by prime divisors of  $n$ .

As WEI also remarked, if we consider  $K = \mathbb{Q}(\sqrt{-n})$  with a positive, square-free rational integer  $n \not\equiv 3 \pmod{4\mathbb{Z}}$ , then the Theorem 6.2.4 gives us equivalent conditions on  $\alpha = a + 2b\sqrt{-n} \in \mathcal{O}_K$  for being the sum of two integral squares. Recall that is the case if and only if there exists an integer  $t$  such that

$$nt^2 + at - b^2$$

is a perfect square and the greatest common divisor of  $t$ ,  $b$  and  $a + nt$  is not divisible by an odd power of a natural prime congruent to 3 modulo  $4\mathbb{Z}$ . WEI presented an equivalent condition for the case in which

1.  $n \not\equiv -1 \pmod{8\mathbb{Z}}$  and there is a prime  $p|n$  with  $p \equiv -1 \pmod{8\mathbb{Z}}$ , or
2.  $n \equiv 1, 2 \pmod{4\mathbb{Z}}$  and there is a prime  $p|n$  with  $p \equiv 3 \pmod{8\mathbb{Z}}$ , or
3.  $n \equiv 3 \pmod{8\mathbb{Z}}$  and there is a prime  $p|n$  with  $p \equiv 5 \pmod{8\mathbb{Z}}$ .

### 7.3 The case of general square-free $d$

We now assume that  $d$  is a square-free rational integer in the Equation 1.3 over  $\mathcal{O}_K$  for  $K = \mathbb{Q}(\sqrt{n})$ . In the fashion of Example 7.2.2, the solutions from Theorem 7.0.2 also apply in  $\mathcal{O}_K$ . As mentioned in Chapter 1, we investigate the ring  $\mathcal{O}_K[\sqrt{-d}]$  which is a subring of  $L = K(\sqrt{-d})$ . This will result in the proof of Theorem 1.2.9.

**Theorem 7.3.1.** (Theorem 1.2.9) Let  $n \equiv 1 \pmod{4\mathbb{Z}}$  a square-free natural number such that  $K = \mathbb{Q}(\sqrt{n})$  is a real quadratic field of class number 1. Let  $d > 0$  be a square-free natural number with  $d \equiv 2 \pmod{4\mathbb{Z}}$  and coprime to  $n$ . Let  $p$  be an odd natural prime below the prime ideal  $\mathfrak{p} = \langle \psi \rangle \subset \mathcal{O}_K$ . Then there is a monic irreducible polynomial  $f_{n,d} \in \mathcal{O}_K[t]$  such that if  $p$  divides neither  $d$  nor the discriminant of  $f_{n,d}$ , then

$$\psi = \alpha^2 + d\beta^2 \iff \begin{cases} \text{either } \left(\frac{-d}{p}\right) = 1 \text{ or } \left(\frac{-d}{p}\right) = \left(\frac{n}{p}\right) = -1 \\ \text{and } f_{n,d}(t) \equiv 0 \pmod{\mathfrak{p}} \text{ has an integer solution.} \end{cases}$$

Furthermore,  $f_{n,d}$  may be taken to be the minimal polynomial of a real algebraic integer  $\alpha$  for which  $H = L(\alpha)$  is the HILBERT class field of the CM-field  $L = K(\sqrt{-d})$ .

In 1970, WILLIAMS [33] constructed the integral bases for the ring of integers of any biquadratic field, which applies to  $L$ . Beforehand, we may allude to the fact that for any  $a, b \in \mathbb{Z}$ , it holds true that

$$\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{a_1 b_1}) = \mathbb{Q}(\sqrt{b}, \sqrt{a_1 b_1})$$

for  $k_1 = \frac{k}{\gcd(a,b)}$  for  $k \in \{a, b\}$ . Hence, WILLIAMS assumed that the pair  $(a, b)$  is congruent to  $(1, 1)$ ,  $(1, 2)$ ,  $(2, 3)$  or  $(3, 3)$  modulo  $4\mathbb{Z}$ .



**Theorem 7.3.2.** [33] Let  $a, b$  be square-free rational integers. An integral basis for  $\mathbb{Q}(\sqrt{a}, \sqrt{b})$  is given by

1.

$$\left\{ 1, \frac{1 + \sqrt{a}}{2}, \frac{1 + \sqrt{b}}{2}, \frac{1 + \sqrt{a} + \sqrt{b} + \sqrt{a_1 b_1}}{4} \right\},$$

if  $a \equiv b \equiv a_1 \equiv b_1 \equiv 1 \pmod{4\mathbb{Z}}$ ,

2.

$$\left\{ 1, \frac{1 + \sqrt{a}}{2}, \frac{1 + \sqrt{b}}{2}, \frac{1 - \sqrt{a} + \sqrt{b} + \sqrt{a_1 b_1}}{4} \right\},$$

if  $a \equiv b \equiv 1 \pmod{4\mathbb{Z}}$  and  $a_1 \equiv b_1 \equiv 3 \pmod{4\mathbb{Z}}$ ,

3.

$$\left\{ 1, \frac{1 + \sqrt{a}}{2}, \sqrt{b}, \frac{\sqrt{b} + \sqrt{a_1 b_1}}{2} \right\}$$

if  $a \equiv 1 \pmod{4\mathbb{Z}}$  and  $b \equiv 2 \pmod{4\mathbb{Z}}$ ,

4.

$$\left\{ 1, \sqrt{a}, \sqrt{b}, \frac{\sqrt{a} + \sqrt{a_1 b_1}}{2} \right\}$$

if  $a \equiv 2 \pmod{4\mathbb{Z}}$  and  $b \equiv 3 \pmod{4\mathbb{Z}}$ ,

5.

$$\left\{ 1, \sqrt{a}, \frac{\sqrt{a} + \sqrt{b}}{2}, \frac{\sqrt{b} + \sqrt{a_1 b_1}}{2} \right\}$$

if  $a \equiv b \equiv 3 \pmod{4\mathbb{Z}}$ .

*Proof.* See [33, p. 525]. □

We see that  $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}[\sqrt{b}]$  rarely equals  $\mathcal{O}_{\mathbb{Q}(\sqrt{a}, \sqrt{b})}$ . In fact, the only possible case is item 3 of the previous theorem because either the generator of  $\mathcal{O}_{\mathbb{Q}(\sqrt{a}, \sqrt{b})}$  over  $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$  is  $\frac{1+\sqrt{b}}{2}$  (items 1 and 2) or the last base element contains a fraction which is not generated over  $\mathbb{Z}$  by  $\sqrt{a}$  and  $\sqrt{b}$  (items 4 and 5).

Thus, if  $n \equiv 1 \pmod{4\mathbb{Z}}$  and  $d \equiv 2 \pmod{4\mathbb{Z}}$  with  $d, n > 1$  both square-free and coprime, then

$$\frac{\sqrt{-d} + \sqrt{-nd}}{2} = \sqrt{-d} \frac{1 + \sqrt{n}}{2},$$

so  $\mathcal{O}_{\mathbb{Q}(\sqrt{n})}[\sqrt{-d}] = \mathcal{O}_{\mathbb{Q}(\sqrt{n}, \sqrt{-d})}$ . Therefore, we may invoke Theorem 7.1.3 and adjust the proof of Theorem 7.0.1 so that we may apply it to prime elements of the field  $\mathbb{Q}(\sqrt{n})$  instead of  $\mathbb{Q}$ . To avoid complications, we assume further that  $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$  is a PID, i. e.  $\mathbb{Q}(\sqrt{n}) \in \mathcal{Q}$ . We start by stating some more widely used definitions and statements which can be found in LANG's book *Algebraic Number Theory* [12]. The reader may compare these to Definition 3.1.5.

**Definition 7.3.3.** Let  $L/K$  be an extension of number fields and  $\mathfrak{p} \subset \mathcal{O}_K$  a prime ideal. Let

$$p\mathcal{O}_L = \prod_{k=1}^g \mathfrak{P}_k^{e_k}$$

be a decomposition into prime ideals of  $\mathcal{O}_L$ . The index  $e_k$  is called the *ramification index* of the ideal  $\mathfrak{P}_k$ .

In a ring of integers, every prime ideal is maximal, so its residue ring is a field. The prime ideals  $\mathfrak{P}_k$  above a prime ideal  $\mathfrak{p}$  have the property that

$$(\mathcal{O}_L/\mathfrak{P}_k)/(\mathcal{O}_K/\mathfrak{p})$$

is a well-defined extension of finite fields.

**Definition 7.3.4.** Let  $L/K$  be an extension of number fields and  $\mathfrak{p} \subset \mathcal{O}_K$  a prime ideal. Let

$$p\mathcal{O}_L = \prod_{k=1}^g \mathfrak{P}_k^{e_k}$$

be a decomposition into prime ideals of  $\mathcal{O}_L$ . Then

$$f_k := |(\mathcal{O}_L/\mathfrak{P}_k)/(\mathcal{O}_K/\mathfrak{p})|$$

is called the *inertia degree* of  $\mathfrak{P}_k$ .

The decomposition and the extensions of residue fields mentioned above motivates the definition of two subgroups of the GALOIS group of an extension.

**Definition 7.3.5.** Let  $L/K$  be a GALOIS extension of number fields and  $\mathfrak{p} \subset \mathcal{O}_K$  a prime ideal. Let

$$p\mathcal{O}_L = \prod_{k=1}^g \mathfrak{P}_k^{e_k}$$

be a decomposition into prime ideals of  $\mathcal{O}_L$ . Then the group

$$D_k = \{\sigma \in \text{Gal}(L/K) : \sigma(\mathfrak{P}_k) = \mathfrak{P}_k\}$$

is called the *decomposition group* of  $\mathfrak{P}_k$ . Additionally,

$$I_k = \{\sigma \in D_k : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}_k} \quad \forall \alpha \in \mathcal{O}_L\}$$

is called the *inertia group* of  $\mathfrak{P}_k$ .

We will utilise various statements and further notation about these invariants and groups found in [12], for example in order to prove an often used property of the HILBERT class field.

**Lemma 7.3.6.** Let  $L/K$  be a finite GALOIS extension of number fields. Then  $H(L)/K$  is GALOIS. If  $K/\mathbb{Q}$  is a totally real GALOIS extension and  $L = K(\sqrt{-d})$  for some positive square-free rational integer  $d$ , then complex conjugation is a non-trivial element in  $\text{Gal}(H(L)/K)$ .

*Proof.* Let  $\overline{K}$  be some algebraic closure of  $K$  containing  $H(L)$  and  $\sigma : L \rightarrow \overline{K}$  be an injective  $K$ -homomorphism (because it is a field homomorphism). Since  $L/K$  is a GALOIS extension, we know that  $\sigma(L) = L$  from GALOIS theory. We then get isomorphisms

$$\mathrm{Gal}(H(L)/L) \cong \mathrm{Gal}(\sigma(H(L))/\sigma(L)) \cong \mathrm{Gal}(\sigma(H(L))/L).$$

Thus, we have that  $\sigma(H(L))/L$  is both ABELIAN and unramified. Now, the compositum  $H(L)\sigma(H(L))$  is ABELIAN over  $L$  because we have an injective homomorphism

$$\mathrm{Gal}(H(L)\sigma(H(L))/L) \cong \mathrm{Gal}(H(L)/L) \times \mathrm{Gal}(H(L)/L), \quad \tau \mapsto (\tau|_{H(L)}, \tau|_{\sigma(H(L))}).$$

Moreover, it is unramified because  $H(L)$  and  $\sigma(H(L))$  are subfields of the maximal unramified extension  $(H(L)\sigma(H(L)))^I/L$  where  $I$  is the inertia group. Hence,  $H(L)\sigma(H(L))/L$  is an unramified ABELIAN extension but by maximality  $H(L)\sigma(H(L)) = H(L)$ , so  $\sigma(H(L))$  equals  $H(L)$ . This implies that  $H(L)/K$  is normal and hence GALOIS.

Furthermore, if  $K/\mathbb{Q}$  is a totally real GALOIS extension and  $L = K(\sqrt{-d})$  for some positive square-free rational integer, then complex conjugation generates  $\mathrm{Gal}(L/K)$  which is a non-trivial normal subgroup of  $\mathrm{Gal}(H(L)/K)$ .  $\square$

The next thing we care about is determining the splitting behaviour of a prime element  $\psi \in \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ . The reader may be familiar with the following lemma from an introductory course in algebraic number theory.

**Lemma 7.3.7.** Let  $K$  be a number field and  $L_1/K, L_2/K$  be two GALOIS extensions. Set  $L_3 = L_1L_2$ . Let further  $\mathfrak{p}$  be a prime ideal in  $\mathcal{O}_K$  and  $e_i, f_i$  be the ramification and inertia indices of  $\mathfrak{p}$  in  $L_i/K$  for  $i \in \{1, 2, 3\}$ . Then

1.  $e_3 \geq \max\{e_1, e_2\}$  and  $f_3 \geq \max\{f_1, f_2\}$ , and
2.  $e_3 \leq e_1e_2$  and  $f_3 \leq f_1f_2$ .

In our setting,  $L_1$  and  $L_2$  will be replaced by  $\mathbb{Q}(\sqrt{n})$  and  $\mathbb{Q}(\sqrt{-d})$ , so, for each prime ideal  $\mathfrak{p} = \langle p \rangle$ , exactly one value among its ramification index, inertia degree, and number of prime ideals above it in each of the quadratic extensions is equal to 2, the others are 1. Depending on the splitting and ramification behaviour of each prime  $p \in \mathbb{P}$ , we can determine the primes which split in  $\mathbb{Q}(\sqrt{n}, \sqrt{-d})/\mathbb{Q}(\sqrt{n})$ .

**Theorem 7.3.8.** Let  $n, -d \in \mathbb{Z} \setminus \{0, 1\}$  be square-free and coprime such that  $n \equiv 1 \pmod{4\mathbb{Z}}$ . Let  $K = \mathbb{Q}(\sqrt{n})$  and  $\mathfrak{p}$  be a prime ideal above the natural odd prime  $p \in \mathbb{P}$  in  $\mathcal{O}_K$ . Then  $\mathfrak{p}$  splits in  $K(\sqrt{-d})/K$  if and only if

1.  $\left(\frac{-d}{p}\right) = 1$  or
2.  $\left(\frac{-d}{p}\right) = \left(\frac{n}{p}\right) = -1$ .

*Proof.* Define  $M = \mathbb{Q}(\sqrt{-d})$ , so  $L = K(\sqrt{-d}) = KM$ . Note that each of the extensions  $K/\mathbb{Q}$ ,  $M/\mathbb{Q}$  and  $L/\mathbb{Q}$  is GALOIS. Let  $p$  be a natural odd prime,  $e_1, e_2, e_3$  its (unique) ramification indices in  $K$ ,  $M$  or  $L$  respectively, likewise  $f_1, f_2, f_3$  being the corresponding inertia indices.

We will now handle each case separately, depending on the splitting and ramification behaviour of a natural prime  $p$  in  $K$  and  $M$ . Throughout, we will use Lemma 7.3.7. Define  $E = \frac{e_3}{e_1}$  and  $F = \frac{f_3}{f_1}$ , the ramification index and the inertia degree of a prime  $\mathfrak{p}$  above  $p$  in the extension  $L/K$ .

1. As  $n$  and  $d$  are coprime and  $n \equiv 1 \pmod{4\mathbb{Z}}$ , there is no prime ramifying in both extensions.
2. If  $p$  ramifies in  $K$  and splits in  $M$ , we have  $\max\{1, 1\} = 1 \leq f_3 \leq 1 = 1 \cdot 1$  and  $\max\{2, 1\} = 2 \leq e_3 \leq 2 = 2 \cdot 1$ . Therefore,  $E = 1$  and  $F = 1$  and the prime above  $p$  in  $K$  splits in  $L$ .
3. If  $p$  ramifies in  $K$  and is inert in  $M$ , we have  $\max\{1, 2\} = 2 \leq f_3 \leq 2 = 1 \cdot 2$  and  $\max\{2, 1\} = 2 \leq e_3 \leq 2 = 2 \cdot 1$ . Thus,  $E = 1$  and  $F = 2$  and the prime above  $p$  in  $K$  is inert in  $L$ .
4. If  $p$  splits in  $K$  and ramifies in  $M$ , we have  $\max\{1, 1\} = 1 \leq f_3 \leq 1 = 1 \cdot 1$  and  $\max\{1, 2\} = 2 \leq e_3 \leq 2 = 1 \cdot 2$ . Hence,  $E = 2$  and  $F = 1$  and the primes above  $p$  in  $K$  ramify in  $L$ .
5. If  $p$  splits in  $K$  and  $M$ , then every ramification index and inertia degree is 1, so the primes above  $p$  in  $K$  split in  $L$ .
6. If  $p$  splits in  $K$  and is inert in  $M$ , we have  $\max\{1, 2\} = 2 \leq f_3 \leq 2 = 1 \cdot 2$  and  $\max\{1, 1\} = 1 \leq e_3 \leq 1 = 1 \cdot 1$ . Therefore,  $E = 1$  and  $F = 2$  and the primes above  $p$  in  $K$  are inert in  $L$ .
7. If  $p$  is inert in  $K$  and ramifies in  $M$ , we have  $\max\{2, 1\} = 2 \leq f_3 \leq 2 = 2 \cdot 1$  and  $\max\{1, 2\} = 2 \leq e_3 \leq 2 = 1 \cdot 2$ . Thus,  $E = 2$  and  $F = 1$  and the prime above  $p$  in  $K$  ramifies in  $L$ .
8. If  $p$  is inert in  $K$  and splits in  $M$ , we have  $\max\{2, 1\} = 2 \leq f_3 \leq 2 = 2 \cdot 1$  and  $\max\{1, 1\} = 1 \leq e_3 \leq 1 = 1 \cdot 1$ . Hence,  $E = 1$  and  $F = 1$  and the prime above  $p$  in  $K$  splits in  $L$ .
9. If  $p$  remains inert in  $K$  as well as in  $M$ , we have  $\max\{2, 2\} = 2 \leq f_3 \leq 4 = 2 \cdot 2$  and  $\max\{1, 1\} = 1 \leq e_3 \leq 1 = 1 \cdot 1$ . So,  $E = 1$  but  $f_3$  can be either 2 or 4. However, suppose  $f_3 = 4$ , then  $p$  would be totally inert in  $L$ . The extension  $L/\mathbb{Q}$  is clearly non-cyclic and hence Lemma 7.3.9 yields a contradiction. Thus,  $f_3 = 2$  and  $F = 1$ , so the prime above  $p$  in  $K$  splits in  $L$ .

We see that the prime ideal  $\mathfrak{p}$  splits in  $L$  if and only if either  $p$  splits in  $M$  (which is equivalent to  $\left(\frac{-d}{p}\right) = 1$ ) or  $p$  remains inert in  $K$  and  $M$  simultaneously (which is equivalent to  $\left(\frac{-d}{p}\right) = \left(\frac{n}{p}\right) = -1$ ).  $\square$

We provide the lemma we used in the last item of the previous proof.

**Lemma 7.3.9.** Let  $L/K$  be a GALOIS extension of number fields. If there exists a totally inert prime  $\mathfrak{p}$  of  $K$ , then  $L/K$  is a cyclic extension.

*Proof.* Suppose there is a totally inert prime  $\mathfrak{p}$  of  $K$ . Let  $D$  and  $I$  be its decomposition and inertia groups as well as  $L^D \subset L^I$  the respective fixed fields. As  $\mathfrak{p}$  is totally inert, we have  $L^D = K$  and  $L^I = L$ . Since the quotient  $D/I \cong \text{Gal}(L^I/L^D) = \text{Gal}(L/K)$  is cyclic, so is  $L/K$ .  $\square$

We have found an equivalent condition for our prime element  $\psi \in \mathbb{Z}[\sqrt{n}]$  to split in the extension  $\mathbb{Q}(\sqrt{n}, \sqrt{-d})/\mathbb{Q}(\sqrt{n})$ . A prime ideal  $\mathfrak{P}$  above it is principal if and only if it splits completely in the HILBERT class field of  $\mathbb{Q}(\sqrt{n}, \sqrt{-d})$  by Theorem 7.1.3. If  $\mathfrak{P}$  is indeed principal, then its generator will be of the form

$$\alpha \pm \beta\sqrt{-d}$$

where  $\alpha, \beta$  satisfy Equation 7.1.

*Proof of Theorem 1.2.9.* The first part was dealt with in Theorem 7.3.8. The second part of the proof, i. e. proving that the polynomial  $f_{n,d}$  fulfils the requirements, follows by the one in COX's *Primes of The Form  $x^2 + ny^2$*  [5, pp. 110 – 112]. The only thing we need to take care of is to replace  $\mathbb{Q}$  by the real quadratic field  $\mathbb{Q}(\sqrt{n})$ . As it is still the fixed field of complex conjugation in  $\mathbb{Q}(\sqrt{n}, \sqrt{-d})$ , the proof works out identically.  $\square$

We finish this section with an example.

**Example 7.3.10.** Let  $K = \mathbb{Q}(\sqrt{5})$ , which has class number 1,  $L = K(\sqrt{-2})$  and  $p$  be a natural prime other than 2 or 5. We know

$$\mathcal{O}_L = \mathbb{Z} \left[ \frac{1 + \sqrt{5}}{2}, \sqrt{-2} \right]$$

by Theorem 7.3.2.  $L$  has class number 1 (see [here](#) [28]), so it is identical to its HILBERT class field. Also, it is the splitting field of the polynomial  $x^4 + 6x^2 + 4$ . By Theorem 1.2.9,  $f_{n,d}$  may be taken to be  $t - 1$  and a prime element  $\psi$  above  $p$  is expressible as

$$\psi = \alpha^2 + 2\beta^2$$

with  $\alpha, \beta \in \mathcal{O}_L$  if

$$\left( \frac{-2}{p} \right) = 1$$

or

$$\left( \frac{-2}{p} \right) = \left( \frac{5}{p} \right) = -1.$$

The first condition may be rewritten as

$$p \equiv 1, 3 \pmod{8\mathbb{Z}}$$

by the supplements of the Law of Reciprocity (Theorem 5.1.10). For the second condition, we have

$$-1 = \left( \frac{-2}{p} \right) = \left( \frac{2}{p} \right) \left( \frac{-1}{p} \right) \iff p \equiv 5, 7 \pmod{8\mathbb{Z}}$$

and

$$-1 = \left( \frac{5}{p} \right) = \left( \frac{p}{5} \right) \iff p \equiv 2, 3 \pmod{5\mathbb{Z}}.$$

Using the Chinese Remainder Theorem for the latter condition and adding the residue classes from the former, we get

$$p \equiv 1, 3, 7, 9, 11, 13, 17, 19, 23, 27, 33, 37 \pmod{40\mathbb{Z}}$$

as final set of classes after dismissing the residue classes which satisfy the first condition but are multiples of 5.

# Bibliography

- [1] P. BERRIZBEITIA AND B. ISKRA, *Gaussian Mersenne and Eisenstein Mersenne primes*, Mathematics of Computation, 79 (2010), pp. 1779 – 1991.
- [2] C.-G. JI AND D. WEI, *Sum of integral squares in cyclotomic fields*, C. R. Math. Acad. Sci. Paris, 344 (2007), pp. 413 – 416.
- [3] P. CHOWLA, *On the representation of  $-1$  as a sum of squares in a cyclotomic field*, Journal of Number Theory, 1 (1968), pp. 208 – 210.
- [4] K. CONRAD, *Pell's equation, II*. <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf>, 2021.
- [5] D. COX, *Primes of The Form  $x^2 + ny^2$* , John Wiley & Sons, Inc., 2<sup>nd</sup> ed., 2013.
- [6] M. ELIA, *Representation of primes as the sums of two squares in the golden section quadratic field*, J. Discrete Math. Sci. Cryptogr., 9 (2006), pp. 25–37.
- [7] M. ELIA AND C. MONICO, *On the representation of primes in  $\mathbb{Q}(\sqrt{2})$  as sums of squares*, JP J. Algebra Number Theory Appl., 8 (2007), pp. 121–133.
- [8] F. GÖTZKY, *Über eine zahlentheoretische Verwendung von Modulfunktionen einer Veränderlichen*, Math. Ann., 100 (1928), pp. 411 – 437.
- [9] G. JANUSZ, *Algebraic Number Fields*, Academic Press, 1973.
- [10] H. KOCH, *Algebraic Number Theory*, Springer, 1997.
- [11] T. Y. LAM, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics, 2005.
- [12] S. LANG, *Algebraic Number Theory*, Graduate Texts in Mathematics, Springer, 1994.
- [13] H. MAASS, *Über die Darstellung total positiver Zahlen des Körpers  $r(\sqrt{5})$  als Summe von drei Quadraten*, Abh. Math. Sem. Hansischen Univ., 14 (1941), pp. 185 – 191.
- [14] W. L. MCDANIEL, *Perfect Gaussian integers*, Acta Arithmetica, XXV (1974), pp. 137 – 144.
- [15] MERSENNE RESEARCH, INC. <https://www.mersenne.org/>, 2021.
- [16] T. NAGELL, *On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields*, Nova Acta Soc. Sci. Upsal., 15 (1953), p. 77 sq.
- [17] ———, *On the sum of two integral squares in certain quadratic fields*, Ark. Mat., 4 (1961), pp. 267–286.

- [18] J. NEUKIRCH, *Algebraische Zahlentheorie. Grundlage der mathematischen Wissenschaften*, Springer Verlag, 1999.
- [19] P. P. NIELSEN, *An upper bound for odd perfect numbers*, *Integers*, 3 (2003), p. 9.
- [20] I. M. NIVEN, *Integers of quadratic fields as sums of squares*, *Trans. Amer. Math. Soc.*, 48 (1940).
- [21] P. OCHEM AND M. RAO, *Odd perfect numbers are greater than  $10^{1500}$* , *Math. Comp.*, 81 (2012), pp. 1869 – 1877.
- [22] M. ORR, *Algebraic Number Theory*, Lecture notes, 2019.
- [23] M. PETERS, *Die Stufe von Ordnungen ganzer Zahlen in algebraischen Zahlkörpern*, *Math. Ann.*, 195 (1972), pp. 309–314.
- [24] A. R. RAJWADE, *Squares*, vol. 171 of London Mathematical Society Lecture Note Series, Cambridge University Press, 1993.
- [25] C. L. SIEGEL, *Darstellung total positiver Zahlen durch Quadrate*, *Math. Z.*, 11 (1921), pp. 80 – 99.
- [26] R. SPIRA, *The complex sum of divisors*, *Amer. Math. Monthly*, 68 (1961), pp. 120 – 124.
- [27] J. C. STUMPENHUSEN, *Lösungen der Gleichungen  $\phi(n) = \phi(n + h)$  und  $\sigma(n) = \sigma(n + h)$  sowie deren Übertrag auf algebraische Ganzheitsringe*. Preprint, 2021.
- [28] THE *L*-FUNCTIONS AND MODULAR FORMS DATABASE. <https://www.lmfdb.org>.
- [29] K. THOMPSON, *The sum of four squares over real quadratic number fields*. <https://arxiv.org/abs/1610.06935>, 2016.
- [30] M. WARD, *On the form of odd perfect Gaussian integers*. <https://arxiv.org/abs/0805.2092v1>, 2008.
- [31] L. WASHINGTON, *Introduction to Cyclotomic fields*, Graduate Texts in Mathematics, Springer Verlag, 2<sup>nd</sup> ed., 1997.
- [32] D. WEI, *On the sum of two integral squares in certain quadratic fields*, *Forum Math.*, 27 (2015), pp. 1923 – 1944.
- [33] K. S. WILLIAMS, *Integers of biquadratic fields*, *Canad. Math. Bull.*, 13 (1970), pp. 519 – 526.
- [34] Z. PARKER, J. RUSHALL AND J. HUNT, *Perfect numbers in the ring of Eisenstein integers*. <https://arxiv.org/abs/1602.09106v1>, 2016.

# Verification of examination registration in FlexNow

Name: Mr Johann Christian Stumpenhusen  
Matriculation No.: 21675783

Semester: SoSe22  
Degree Course: Mathematik (Master of Science)  
Module: Masterarbeit  
Exam: Masterarbeit  
Lecturer: Dr. Victoria Cantoral Farfán

## Declaration

I hereby declare that I have produced this work independently and without outside assistance, and have used only the sources and tools stated.

I have clearly identified the sources of any sections from other works that I have quoted or given in essence.

I have complied with the guidelines on good academic practice at the University of Göttingen.

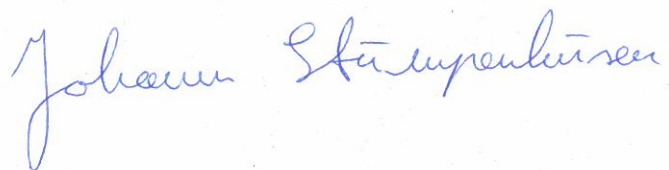
If a digital version has been submitted, it is identical to the written one.

I am aware that failure to comply with these principles will result in the examination being graded "nicht bestanden", i.e. failed.

Göttingen, 10th May 2022

Johann  
Stumpenhusen

Christian





# Verification of examination registration in FlexNow

Name: Mr Johann Christian Stumpenhusen  
Matriculation No.: 21675783

Semester: SoSe22  
Degree Course: Mathematik (Master of Science)  
Module: Masterarbeit  
Exam: Masterarbeit  
Lecturer: Prof. Dr. Frank Gounelas

## Declaration

I hereby declare that I have produced this work independently and without outside assistance, and have used only the sources and tools stated.

I have clearly identified the sources of any sections from other works that I have quoted or given in essence.

I have complied with the guidelines on good academic practice at the University of Göttingen.

If a digital version has been submitted, it is identical to the written one.

I am aware that failure to comply with these principles will result in the examination being graded "nicht bestanden", i.e. failed.

Göttingen, 10th May 2022

Johann  
Stumpenhusen

Christian

