SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Applying the Hilbert Class Field to Primes of the Form $x^2 + ny^2$

av

Carl Lindblom

2019 - No M3

Applying the Hilbert Class Field to Primes of the Form $x^2 + ny^2$

Carl Lindblom

Självständigt arbete i matematik 30 högskolepoäng, avancerad nivå

Handledare: Wushi Goldring

2019

Abstract

In this thesis we discuss some already known methods for determining when, given a fixed positive integer n, a prime number can be expressed as $x^2 + ny^2$, where x and y are integers. In particular, we focus mainly on the theory behind a method involving the Hilbert class field, i.e., the maximal unramified abelian field extension, of the quadratic field $\mathbb{Q}(\sqrt{-n})$. This method can be applied only for n satisfying some special conditions, once the corresponding Hilbert class field is known. Before discussing the theory behind this method, we give some background in number theory and Galois theory, and we look at the theory of cubic and biquadratic reciprocity, and how to apply it to the cases $n = 27$ and $n = 64$ respectively, in which the Hilbert class field cannot be applied. In the last section, we give a brief explanation of the ring class field of an order in a number field, and a more general method involving the ring class field.

Acknowledgements

I would like to thank my advisor Wushi Goldring for all his support and for always showing trust in me.

Contents

1 Introduction

The problem of determining whether a prime $p \in \mathbb{Z}$ is of the form $x^2 + ny^2$ for some $x, y \in \mathbb{Z}$ given a fixed $n \in \mathbb{Z}_{\geq 1}$ has been studied by some of the greatest mathematicians during the last few hundred years. In this thesis, we will explain the theory for solving the problem of primes of the form $x^2 + ny^2$, for some special cases. The main source is the book *Primes of the Form* $x^2 + ny^2$ by D. A. Cox.[1] This book includes many more methods, which do not appear in this thesis, as well as an excellent explanation of the historical background, dating back to Fermat in the 17th century.

The cases of $n = 27$ and $n = 64$ can be solved using the theories of cubic and biquadratic reciprocity, and are the main focus of Section 3. This section is based on Cox, Chapter 1, §4.[1] A method for n satisfying some special conditions will be described in Section 4, which is based on Cox, Chapter 2, §5.[1] This method involves the Hilbert class field of the number field $\mathbb{Q}(\sqrt{-n})$. In Section 5 we will briefly describe a more general theorem, which holds for any $n \in \mathbb{Z}_{\geq 1}$. This method involves the ring class field of $\mathbb{Q}(\sqrt{-n})$ and is given in Cox, Chapter 2, §9. Sadly, methods involving the Hilbert class field and ring class field can be applied only if we know the Hilbert and ring class field respectively. Methods for actually determining these fields, which involves finding a primitive element for the field extension, require way more advanced theory in most cases.

Section 2 covers some background in number theory and Galois theory. We assume the reader to be somewhat familiar with the theory of groups, rings, and modules, and anything that would appear in a first-level course in mathematics. In particular, integral domains, principal ideal domains, unique factorization domains, Euclidean domains, and fields, and all basic properties of ideals and elements in these types of rings (such as being a zero-divisor, prime, maximal, unit, etc.), as well as notions such as the field of fractions of an integral domain, finite fields, and the multiplicative group of a ring, are some of the required background knowledge.

The main focus of this thesis is the theory behind the methods for solving the problem of primes of the form $x^2 + ny^2$, rather than applications of these methods. Since n could be arbitrarily large, there is an infinite number of cases to explore further, some of which may be solved relatively easily using the methods presented in this thesis (such as $n = 243$ for applying cubic reciprocity and $n = 17$ for applying the Hilbert class field, according to Cox, Chapter 1, §4, Exercis 4.15, and Chapter 2, §5, Exercises 5.25–5.26 respectively[1]) and some requiring more advanced theory, such as the theory of complex multiplication, which appears in Chapter 3 of Cox.[1]. There is a wide range of related topics to explore further, such as problems involving reciprocity (e.g., reciprocity of higher degrees, discussed in Cox, Chapter 1, §4(C)[1]) or the Hilbert class field (e.g., field towers, mentioned in Cox, Chapter 2, §5(C)[1]).

2 Some background in number and Galois theory

In this part we will present some necessary background from number theory (Section 2.1) and Galois theory (Section 2.2).

2.1 Number theory

Definitions 2.1 and 2.3 below are according to Dummit and Foote, Chapter 13, Sections 13.1 and 13.2 respectively, and Proposition 2.2, is stated and proved as Theorem 14 in Section 13.2.[2]

Definition 2.1. Let F be a field. Any field K such that $F \subset K$ is called a *field extension of* K. This extension is often denoted K/F or $F \subset K$. The dimension of K as a vector space over F is called the *degree of* K *over* F and is denoted $[K : F]$. If $[K : F]$ is finite, then we say that the extension is *finite*. If there exists $\alpha_1, \alpha_2, \cdots \in K$ such that K is the smallest field containing all of $\alpha_1, \alpha_2 \cdots$ (that is, for any field L such that $F \subset L$, it holds that $K \subset L$ whenever $\alpha_1, \alpha_2, \cdots \in L$), then we write $K = F(\alpha_1, \alpha_2, \cdots)$, and we say that K is *generated by* $\alpha_1, \alpha_2 \cdots$ *over* F. If $K = F(\alpha)$ for some element element $\alpha \in K$, then α is called a *primitive element* for the extension $F \subset K$.

Proposition 2.2. Let F, K and L be fields such that $F \subset K \subset L$. Then

$$[L : F] = [L : K][K : F].$$

Proof. See Dummit and Foote, Chapter 13, Section 13.2, Theorem 14. □

Definition 2.3. Let F be a field and let K be any field extension of F. An element $\alpha \in K$ is said to be *algebraic over* F if $f(\alpha) = 0$ for some nonzero $f \in F[x]$. If every element in K is algebraic over F, then K is said to be an *algebraic field extension of* F.

Definitions 2.4 and 2.5 below are according to Ireland and Rosen, Chapter 12, §2, and Chapter 6, §1 respectively.[3]

Definition 2.4. A field K is called an *(algebraic) number field* if K is a subfield of $\mathbb{C}$ and $[K : \mathbb{Q}]$ is finite. (Note that any subfield of $\mathbb{C}$ is a field extension of $\mathbb{Q}$, since any subfield of $\mathbb{C}$ contains $\{0, 1\}$, and, thus, $n \cdot 1 = n$ and $1/n$ for every $n \in \mathbb{Z} \setminus \{0\}$)

Definition 2.5. An element $\alpha \in \mathbb{C}$ is called an *algebraic number* if α is algebraic over $\mathbb{Q}$, that is, $f(\alpha) = 0$ for some nonzero $f \in \mathbb{Z}[x]$. (Note that this is equivalent to $f(\alpha) = 0$ for some nonzero $f \in \mathbb{Q}[x]$, by multiplication by the least common multiple of the denominators of the coefficients.) If there exists a monic $g \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$, then α is called an *algebraic integer*.

In accordance with Cox, Chapter 2, §5, Section A,[1] and Dummit and Foote, Chapter 15, Section 15.3,[2] if K is a number field, we denote the set of algebraic integers in K by $\mathcal{O}_K$. Dummit and Foote define this set as the integral closure of $\mathbb{Z}$ in K, see Definition 2.6 below.[2]

Definition 2.6. Let R be a ring and let S be a subring of R. Let $r \in R$. We say that r is *integral over* S if there exists a monic $g \in S[x]$ such that $g(r) = 0$. The subset of R consisting of the elements which are integral over S is called the *integral closure of* S *in* R. If S is its own integral closure in R, then we say that S is *integrally closed in* R.

Lemma 2.7. Let R be a ring and let S be a subring of R. Then the integral closure of S in R is a ring.

Proof. This fact is proved in Dummit and Foote, Chapter 15, Section 15.3, Corollary 24(2).[2] □

Proposition 2.8. Let K be a number field. Then $\mathcal{O}_K$ is an integral domain.

Proof. By definition $\mathcal{O}_K$ is the set of all $\alpha \in K$ satisfying that $g(\alpha) = 0$ for some monic $g \in \mathbb{Z}[x]$, i.e., the integral closure of $\mathbb{Z}$ in K. By Lemma 2.7, $\mathcal{O}_K$ is a ring. Since $\mathcal{O}_K$ is a subring of K, any zero-divisor of $\mathcal{O}_K$ is also a zero-divisor of K. Since K is an integral domain (since it is a field), it has no zero-divisors, and the same goes for $\mathcal{O}_K$. This shows that $\mathcal{O}_K$ is an integral domain. □

Remark 2.9. A number field K is always the field of fractions of its ring of integers $\mathcal{O}_K$. This fact is proved in Dummit and Foote, Chapter 15, Section 15.3, Theorem 29(2).[2]

The following definition is given in Ireland and Rosen, Chapter 5, §3.[3]

Definition 2.10. Let $n \in \mathbb{Z}_{\geq 1}$. If ζ is a root of the polynomial $x^n - 1$, then ζ is called an *nth root of unity.* The nth roots of unity are precisely the elements $e^{2k\pi i/n}$, $k = 1, 2, \cdots, n$. If $\zeta = e^{2k\pi i/n}$ where k and n are relatively prime, then ζ is called a *primitive nth root of unity.*

The proposition below follows from Theorem 2 in Samuel, §2.9 and the remark which follows.[5]

Proposition 2.11. Let $p \in \mathbb{Z}$ be a prime, let $r \in \mathbb{Z}$ be any positive integer, and let ζ be a p^rth root of unity. Then, if $K = \mathbb{Q}(\zeta)$, it holds that $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Proof. In Samuel, §2.9, Theorem 2, this results is proved for primitive p^1th roots of unity, and in the remark, it is stated that, for all $k \in \mathbb{Z}_{\geq 1}$, the result holds for all primitive p^k-roots of unity.[5] Since every p^rth root of unity is a primitive p^kth root of unity for some $k \in \mathbb{Z}_{\geq 1}$, the result must hold for all p^rth roots of unity. □

The following proposition is stated and proved in Dummit and Foote, Chapter 13, Section 13.2.[2] In Ireland and Rosen, Chapter 6, §1, the corresponding proposition (6.1.7) is stated and proved for $F = \mathbb{Q}$ and α being any algebraic number.[3] Definitions 2.13 and 2.14 is according to Dummit and Foote, Chapter 13, Section 13.2, and Chapter 14, Section 14.6, respectively.[2]

Proposition 2.12. Let F be a field and let K be any field extension of F. If $\alpha \in K$ is algebraic over F, then, there exists a unique polynomial $m_{\alpha,F} \in F[x]$ such that $m_{\alpha,F}$ is monic and irreducible over F, $m_{\alpha,F}(\alpha) = 0$, and for any $f \in F[x]$ such that $f(\alpha) = 0$, it holds that $m_{\alpha,F} \mid f$ in F. □

Definition 2.13. The polynomial $m_{\alpha,F}$ of the previous proposition is called the *minimal polynomial of α in F.*

Definition 2.14. Given any polynomial $f \in \mathbb{C}[x]$ in one variable (of degree $n \geq 1$). Then, we define the *discriminant D_f of f* to be

$$D_f := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1, \cdots, \alpha_n$ are the roots of f.

2.2 Galois Theory

Definition 2.15. Let F be a field and let K be any extension of F. We denote by $\mathrm{Aut}(K/F)$ the set of automorphisms of K which fix F.

The following proposition is stated as part of Proposition 1 in Dummit and Foote, Chapter 14, Section 14.1.[2]

Proposition 2.16. The set $\mathrm{Aut}(K/F)$ of Definition 2.15 is a group under composition.

Proof. This proposition is proved in less detail in Dummit and Foote, Chapter 14, Section 14.1, Proposition 1. Clearly the identity automorphism $\mathrm{id} : \alpha \mapsto \alpha$ fixes F and, thus, belongs to $\mathrm{Aut}(K/F)$. Given any two $\sigma_1, \sigma_2 \in \mathrm{Aut}(K/F)$, we have that, for any $\alpha \in F$,

$$(\sigma_1 \circ \sigma_2)(\alpha) = \sigma_1(\sigma_2\alpha) = \sigma_1\alpha = \alpha,$$

thus, $\sigma_1 \circ \sigma_2 \in \mathrm{Aut}(K/F)$, since the composition of any two automorphisms is an automorphism. The inverse automorphism σ_1^{-1} also fixes F, and, thus, belongs to $\mathrm{Aut}(K/F)$. Since the composition of maps is associative, the set $\mathrm{Aut}(K/F)$ satisfies all the group axioms. □

The following proposition is also stated and proved in Dummit and Foote, as Corollary 10 in Chapter 14, Section 14.2.[2]

Proposition 2.17. Given any finite extension K of F, it holds that

$$|\mathrm{Aut}(K/F)| \leq [K : F].$$

Proof. See Dummit and Foote, Chapter 14, Section 14.2, Corollary 10.[2] □

Definitions 2.18 and 2.19 below are given in Dummit and Foote, Chapter 14, Section 14.1, in the definitions following Proposition 5 and Corollary 6 respectively, and Definition 2.20 is given in Section 14.2, Exercise 17.[2] Theorem 2.21 below is stated as Theorem 14 in Dummit and Foote, Chapter 14, Section 14.2.[2]

Definition 2.18. Let F be a number field and let K be any finite extension of F. We say that K is *Galois over* F if $|\mathrm{Aut}(K/F)| = [K : F]$. If K is Galois over F, then we call $\mathrm{Aut}(K/F)$ the *Galois group of* K *over* F and we denote it by $\mathrm{Gal}(K/F)$.

Definition 2.19. Let F be a number field. Assume that $f(x) \in F[x]$ is separable (meaning that all of its roots are distinct). We define the *Galois group of* f to be the Galois group of the splitting field of f (the smallest field containing all the roots of f). This field is Galois over F, according to Dummit and Foote, Chapter 14, Section 14.1, Corollary 6.[2]

Definition 2.20. Let F be a number field and let K be any finite extension of F. Let $\alpha \in K$. Assume that K is Galois over F. Then, the *norm* $N(\alpha)$ *of* α *from* K *to* F is defined to be the product

$$N(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma\alpha.$$

Theorem 2.21. (The Fundamental Theorem of Galois Theory) Let F be a field and let K be a Galois extension of F. Then there is a one-to-one correspondence between the subgroups of $\mathrm{Gal}(K/F)$ and the subfields of K containing F, such that a subfield E of K containing F corresponds to the subgroup H of $\mathrm{Gal}(K/F)$ which fixes E. This correspondence is inclusion reversing. Furthermore, if E and H are such a subfield and subgroup respectively, then

(i) $[K : E] = |H|$ and $[E : F] = |\mathrm{Gal}(K/F) : H|$ (where $|\mathrm{Gal}(K/F) : H|$ denotes the index of H in $\mathrm{Gal}(K/F)$),

(ii) the extension K/E is Galois and $\mathrm{Gal}(K/E) = H$

(iii) the extension E/F is Galois if and only if $H \trianglelefteq \mathrm{Gal}(K/F)$ (where the notation $H \trianglelefteq \mathrm{Gal}(K/F)$ indicates that H is a normal subgroup of $\mathrm{Gal}(K/F)$),

(iv) if the extension E/F is Galois, then $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/H$,

(v) if E' is another subfield of K containing F and H' is the subgroup of $\mathrm{Gal}(K/F)$ corresponding to E', then $E \cap E'$ corresponds to $\langle H, H' \rangle$ (the group generated by H and H') and E_1E_2 corresponds to $H \cap H'$.

Proof. See Dummit and Foote, Chapter 14, Section 14.2, Theorem 14.[2] □

3 Cubic and biquadratic reciprocity

In 1849, the unfinished book in number theory *Tractatus de numerorum doctrina capita sedecim, quae supersunt* written by Euler in 1749–1750, was published. According to Cox, Chapter 1, §1(D),[1] Euler states, in the two chapters which deal with cubic and biquadratic residues respectively, the following conjectures for primes of the form x^2+27y^2 and x^2+64y^2, which were first proved by Gauss using the theories of cubic and biquadratic reciprocity.

Theorem 3.1. For any prime p, it holds that

$$p = x^2 + 27y^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} p \equiv 1 \pmod 3 \text{ and} \\ 2 \text{ is a cubic residue modulo } p \end{cases}$$

Theorem 3.2. For any prime p, it holds that

$$p = x^2 + 64y^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} p \equiv 1 \pmod 4 \text{ and} \\ 2 \text{ is a biquadratic residue modulo } p \end{cases}$$

In Definition 3.3 below we explain the notions of quadratic, cubic, and biquadratic residue.

Definition 3.3. Given any prime $p \in \mathbb{Z}$ and any $a \in \mathbb{Z}$, the integer a is said to be a *quadratic residue modulo* p if $x^2 \equiv a \pmod p$ has a solution in $\mathbb{Z}$. Similarly, a is said to be a *cubic residue modulo* p if there is an integer solution to $x^3 \equiv a \pmod p$ and a *biquadratic residue modulo* p if there is an integer solution to $x^4 \equiv a \pmod p$.

Related to this is the notion of the Legendre symbol, see Definition 3.4. This definition can also be extended to the cubic and biquadratic cases (see Sections 3.1–3.3). The first version of this definition is given in Samuel, Chapter 5, Section 5.5,[5] (without considering the case $p \mid z$) and in Ireland and Rosen, Chapter 5, §1.[3] The second version is equivalent to the first, by Proposition 3.5, and is analogous to the definitions of the generalized Legendre in the cubic and biquadratic cases, given in Cox, Chapter 1, §4.[1]

Definition 3.4. Given an integer prime $p \neq 2$, the *Legendre symbol* is the function $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{0, \pm 1\}$ defined by

$$\left(\frac{z}{p}\right) := \begin{cases} 0 & \text{if } p \mid z \\ 1 & \text{if } p \nmid z \text{ and } z \text{ is a quadratic residue modulo } p \\ -1 & \text{if } p \nmid z \text{ and } z \text{ is not a quadratic residue modulo } p. \end{cases}$$

For $z \in \mathbb{Z}$, we can also define the Legendre symbol $\left(\frac{z}{p}\right)$ as 0 if $p \mid z$, and otherwise as the unique square root of unity such that

$$z^{(p-1)/2} \equiv \left(\frac{z}{p}\right) \pmod p.$$

Proposition 3.5. Given an integer prime p, The two definitions of the Legendre symbol $\left(\frac{z}{p}\right)$, for $z \in \mathbb{Z}$ such that $p \nmid z$, stated in Definition 3.4 are equivalent.

Proof. Note that $(p-1)/2$ is an integer, since p is odd. Thus, if $p \nmid z$ and z is a quadratic residue modulo p, then $z \equiv a^2 \pmod p$ for some $a \in \mathbb{Z}$, hence

$$z^{(p-1)/2} \equiv (a^2)^{(p-1)/2} \equiv a^{2(p-1)/2} \equiv a^{p-1} \equiv 1 \pmod p,$$

where the last congruence is according to Fermat's Little Theorem. If instead z is not a quadratic residue modulo p, then, since the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of $\mathbb{Z}/p\mathbb{Z}$ is cyclic of order $p-1$, (since $\mathbb{Z}/p\mathbb{Z}$ is a finite field, see Dummit and Foote, Chapter 9, Section 9.5, Proposition 18[2]), we can write $z = b^k$ for some nonzero $b \in (\mathbb{Z}/p\mathbb{Z})^*$ and some odd $k \in \mathbb{Z}_{\geq 1}$, which gives us

$$z^{(p-1)/2} \equiv 1 \pmod p \implies b^{k(p-1)/2} \equiv 1 \pmod p \implies$$

$$(p-1) \mid k(p-1)/2 \text{ in } \mathbb{Z} \implies k/2 \in \mathbb{Z} \implies k \text{ is even.}$$

This shows that $z^{(p-1)/2} \not\equiv 1$ whenever z is not a quadratic residue modulo p. Since, by Fermat's Little Theorem,

$$(z^{(p-1)/2})^2 \equiv z^{2(p-1)/2} \equiv z^{(p-1)} \equiv 1 \pmod{p},$$

we have that $z^{(p-1)/2} \equiv \pm 1 \pmod{p}$, that is, $z^{(p-1)/2}$ is always congruent to a square root of unity modulo p. (The square roots of unity are ± 1 and are always incongruent modulo p, since $p \neq 2$.) This completes the proof. □

3.1 The rings $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$

This section is based on Cox, Chapter 1, §4.[1] All definitions are according to Cox, unless stated otherwise. Studying the theory of cubic and biquadratic reciprocity involves studying the sets $\mathbb{Z}[\omega] = \{a+b\omega \mid a, b \in \mathbb{Z}\}$ and $Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ respectively, where

$$\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2, \qquad i = e^{2\pi i/4} = \sqrt{-1}$$

are primitive third and fourth roots of unity respectively (see Definition 2.10). The latter is known as the ring of *Gaussian integers*, named after Gauss, who, according to Ireland and Rosen, Chapter 1, §4,[3] was the first to study its properties in detail. Note that

$$\omega + \omega^2 = (-1 + \sqrt{-3} - 1 - \sqrt{-3})/2 = -1. \tag{3.1}$$

According to Proposition 2.11, $Z[\omega]$ and $Z[i]$ are the rings of integers of $\mathbb{Q}(\omega)$ and $\mathbb{Q}(i)$ respectively. This also follows from Proposition 4.23.

Proposition 3.6. The fields $\mathbb{Q}(\omega)$ and $\mathbb{Q}(i)$ are Galois extensions of $\mathbb{Q}$.

Proof. A basis for $\mathbb{Q}(\omega)$ as a vector space over $\mathbb{Q}$ is given by $\{1, \omega\}$, since $\omega^2 = -1 - \omega$, by (3.1), and $\omega^3 = 1$, thus,

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2.$$

The map

$$\sigma : (\omega, \omega^2) \mapsto (\omega^2, \omega),$$

is an automorphism which fixes $\mathbb{Q}$, since it takes $\omega^2 = -1 - \omega$ to $\omega = -1 - \omega^2$. The identity automorphism $\mathrm{id}_{\mathbb{Q}(\omega)} : x \leftrightarrow x$ on $\mathbb{Q}(\omega)$ also fixes $\mathbb{Q}$. By Proposition 2.17, $\mathbb{Q}(\omega)$ cannot have more than two automorphisms that fix $\mathbb{Q}$, hence,

$$|\mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})| = 2 = [\mathbb{Q}(\omega) : \mathbb{Q}],$$

i.e., the extension $\mathbb{Q} \subset \mathbb{Q}(\omega)$ is Galois. The proof is very similar for the extension $\mathbb{Q} \subset \mathbb{Q}(i)$. We have that

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2,$$

since $\{1, i\}$ is a basis for $\mathbb{Q}(i)$ over $\mathbb{Q}$ (since $i^2 = -1$). The map

$$\tau : i \mapsto -i$$

is indeed an automorphism of $\mathbb{Q}(i)$ which fixes $\mathbb{Q}$, since $\tau(-i) = -\tau(i)$. (This automorphism is the complex conjugate map.) Again, the identity automorphism $\mathrm{id}_{\mathbb{Q}(i)}$ fixes $\mathbb{Q}$. By Proposition 2.17, $\mathbb{Q}(\omega)$ cannot have more than two automorphisms that fix $\mathbb{Q}$, hence,

$$|\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q})| = 2 = [\mathbb{Q}(i) : \mathbb{Q}],$$

i.e., the extension $\mathbb{Q} \subset \mathbb{Q}(i)$ is Galois. □

Remark 3.7. Since $\mathbb{Q}(\omega)$ and $\mathbb{Q}(i)$ are Galois extensions of $\mathbb{Q}$, we can compute their field norm according to Definition 2.20. In the proof of Proposition 3.6 above, we saw that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\omega)/\mathbb{Q})$ consists of the identity and the automorphism $\sigma : \omega \leftrightarrow \omega^2$. Since

$$\omega^2 = -1 - \omega = -1 - \frac{-1+\sqrt{-3}}{2} = \frac{-2+1-\sqrt{-3}}{2} = \frac{-1-\sqrt{-3}}{2} = \overline{\omega},$$

we see that σ is the complex conjugate map. In the proof, we saw that the same goes for $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q})$. It is well known that the complex conjugate is additive and multiplicative, thus, we see that, for any element α in $\mathbb{Q}(\omega)$ or $\mathbb{Q}(i)$, the norm of α is given by

$$N(\alpha) = \alpha\overline{\alpha}$$

This norm is multiplicative, by Definition 2.20, since any ring automorphism is multiplicative. (This also follows from the multiplicativity of complex conjugation).

Remark 3.8. For $u, v \in \mathbb{Q}$ not both zero, it holds that

$$N(u+v\omega) = (u+v\omega)\overline{(u+v\omega)} = (u+v\omega)(u+v\omega^2) = \tag{3.2}$$

$$u^2 + uv(\omega+\omega^2) + v^2\omega^3 = u^2 - uv + v^2 > 0$$

(where the last inequality holds because $u^2 - uv + v^2 \geq u^2 - 2uv + v^2 = (u-v)^2 \geq 0$ if u and v have the same signs, and $-uv \geq 0$ if u and v have opposite signs), and

$$N(u+vi) = (u+vi)\overline{(u+vi)} = (u+vi)(u-vi) = u^2 + v^2 > 0. \tag{3.3}$$

By (3.2) and (3.4), N takes any nonzero element in $\mathbb{Z}[\omega]$ or $\mathbb{Z}[i]$ respectively to some positive integer.

Proposition 3.9. $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ are Euclidean domains, with Euclidean function being the field norm of $\mathbb{Q}(\omega)$ and $\mathbb{Q}(i)$ respectively restricted to $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ respectively.

Proof. The proof given here is a more detailed version of the proof of Proposition 4.3 in Cox, Chapter 1, §4(A),[1], where Cox assumes that the field norm $\mathbb{Q}(\omega)$ is multiplicative (which we have already shown in Remark 3.7), and leaves that part of the proof as an exercise. For $\alpha, \beta \in \mathbb{Z}[\omega]$ such that $\beta \neq 0$, we have that

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{N(\beta)}.$$

Since $N(\beta) \in \mathbb{Q}$, we have that $\alpha/\beta \in \mathbb{Q}(\omega)$, thus, we can write $\alpha/\beta = u + v\omega$ for some $u, v \in \mathbb{Q}$. Let u_1 and v_1 be the integers obtained when rounding u and v respectively to the nearest integer. We have that $|u-u_1|, |v-v_1| \leq 1/2$. If we let $\gamma := u_1 + v_1\omega$ and $\delta := \alpha - \gamma\beta$, then $\gamma, \delta \in \mathbb{Z}[\omega]$ and

$$\alpha = \gamma\beta + \delta.$$

Since

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = N((u-u_1) + (v-v_1)\omega) = (u-u_1)^2 - (u-u_1)(v-v_1) + (v-v_1)^2 \leq$$

$$\frac{1}{4} + \frac{1}{4} - \underbrace{(u-u_1)(v-v_1)}_{\in[-1/4,\ 1/4]} < 1,$$

we have that

$$N(\delta) = N(\alpha - \gamma\beta) = N\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta).$$

This shows that $\mathbb{Z}[\omega]$ is a Euclidean domain. The same argument goes for $\mathbb{Z}[i]$ if we replace ω by i and compute $N(\alpha/\beta - \gamma)$ as

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = N((u-u_1) + (v-v_1)i) = (u-u_1)^2 + (v-v_1)^2 \leq$$

$$\frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1. \qquad \square$$

Proposition 3.10. Every Euclidean domains is a principal ideal domain (P.I.D.) and every principal ideal domain is a unique factorization domain (U.F.D.).

Proof. These two facts are proved in Dummit and Foote, Chapter 8, Section 8.1, Proposition 1 and Section 8.3, Theorem 15, respectively.[2] □

Corollary 3.11. The rings $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ are principal ideal domains and unique factorization domains.

Proof. By Proposition 3.9, the two rings are Euclidean domains, hence, by Proposition 3.10, they are principal ideal domains and unique factorization domains. □

The following two propositions are, in the case of $\mathbb{Z}[\omega]$, stated as Lemma 4.5 and Lemma 4.6 respectively in Cox, Chapter 1, §4(A), and in Chapter 1, §4(B) it is stated that the analogs hold in the case of $\mathbb{Z}[i]$.[1] Proposition 3.12 is also stated as Proposition 9.1.1 in Ireland and Rosen, Chapter 9, §1, for the cubic case, and as Exercise 33 in Chapter 1 for the biquadratic case.[3]

Proposition 3.12.

(i) An element α in $\mathbb{Z}[\omega]$ or $\mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$.

(ii) The units in $\mathbb{Z}[\omega]$ are $\pm 1, \pm\omega, \pm\omega^2$.

(iii) The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Proof. This proof is based on the proof of the cubic case given in Ireland and Rosen, Chapter 9, §1, Proposition 9.1.1.[3] Assume that $\alpha \in \mathbb{Z}[\omega]$ is a unit. Then, there exists a $\beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$. Since N is multiplicative, it holds that

$$1 = 1^2 = N(1) = N(\alpha)N(\beta).$$

Since N takes every nonzero element in $\mathbb{Z}[\omega]$ to some positive integer (by Remark 3.8), we have

$$N(\alpha) = N(\beta) = 1.$$

The exact same argument can be used for $\mathbb{Z}[i]$ instead of $\mathbb{Z}[\omega]$. Conversely, assume that $\alpha = a + b\omega \in \mathbb{Z}[\omega],\ a, b \in \mathbb{Z}$ satisfies that $N(\alpha) = 1$. Then, since (by Remark 3.7)

$$1 = N(\alpha) = \alpha\overline{\alpha}$$

and since

$$\overline{\alpha} = \overline{(a + b\omega)} = a + b\omega^2 = \underbrace{a - b}_{\in\mathbb{Z}} - b\omega \in \mathbb{Z}[\omega],$$

we have that $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[\omega]$ (namely, $\beta = \overline{\alpha}$), that is, α is a unit. If instead $\alpha = a + bi \in \mathbb{Z}[i],\ a, b \in \mathbb{Z}$, then, again $1 = N(\alpha) = \alpha\overline{\alpha}$, and, since $\overline{\alpha} = a - bi \in \mathbb{Z}[i],\ \alpha$ is a unit. This proves (i).

In order to prove (ii), we will use some theory of quadratic forms discussed in Section 4.37. Since

$$1 = 1 \cdot 1 = (-1) \cdot (-1) = \omega \cdot \omega^2 = (-\omega) \cdot (-\omega^2),$$

we see that $\pm 1, \pm\omega, \pm\omega^2$ are units of $\mathbb{Z}[\omega]$. If some element $\alpha = a + b\omega \in \mathbb{Z}[\omega],\ a, b \in \mathbb{Z}$, is a unit, then, by (i),

$$1 = N(\alpha) = N(a + b\omega) = a^2 - ab + b^2,$$

or, equivalently,

$$4 = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2.$$

Since $(2a - b)^2$ and $3b^2$ are both positive integers, one of the following must hold.

(1) $2a - b = \pm 1$ and $b = \pm 1$.

(2) $2a - b = \pm 2$ and $b = 0$.

In case (1) above, if the two $\pm$ symbols have the same sign, then $b = \pm 1$ and $a = (\pm 1 + \pm 1)/2 = \pm 2/2 = \pm 1$, that is,

$$\alpha = \pm 1 + \pm\omega = - \pm (-1 - \omega) = - \pm \omega^2.$$

If instead the two $\pm$ symbols have opposite signs, then $b = \pm 1$ and $a = (- \pm 1 + \pm 1)/2 = 0/2 = 0$, that is, $\alpha = \pm\omega$. In case (2) above, we have that $b = 0$ and $2a = \pm 2/2 = \pm 1$, that is $\alpha = \pm 1$. This proves (ii). Similarly, (iii) holds, since

$$1 \cdot 1 = -1 \cdot -1 = i \cdot (-i) = 1,$$

thus, $\pm 1, \pm i$ are units of $\mathbb{Z}[i]$, and if some element $\gamma = c + di \in \mathbb{Z}[i]$ is a unit, then

$$1 = N(\gamma) = N(c + di) = c^2 + d^2,$$

which implies that either $c = 0$ and $d = \pm 1$, or $c = \pm 1$ and $d = 0$, since c^2 and d^2 are positive integers and add up to 1, hence either

$$\gamma = 0 \pm i = \pm i$$

or

$$\gamma = \pm 1 + 0 = \pm 1.$$

This proves (iii).

□

Proposition 3.13. An element α in $\mathbb{Z}[\omega]$ or $\mathbb{Z}[i]$ is prime whenever $N(\alpha)$ is a prime in $\mathbb{Z}$.

Proof. This proof is, in the case $\alpha \in \mathbb{Z}[\omega]$, given in Cox, Chapter 1, §4(A), Lemma 4.6.[1] Using the multplicativity of the norm N, the unique factorization into primes in $\mathbb{Z}$, and the property that, in a unique factorization domain, the irreducible elements are precisely the prime elements. By exactly the same argument, this Proposition also holds in the case $\alpha \in \mathbb{Z}[i]$. The argument goes as follows: if $N(\alpha)$ is prime in $\mathbb{Z}$, and α is not a prime in $\mathbb{Z}[i]$ (or $\mathbb{Z}[\omega]$), then, we can write $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathbb{Z}[i]$ (or $\mathbb{Z}[\omega]$), thus

$$N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma),$$

which implies that one of $N(\beta)$ and $N(\gamma)$ is 1 (since $N(\alpha)$ is prime in $\mathbb{Z}$), that is, one of β and γ is a unit by Proposition 3.12(i). Since $\mathbb{Z}[i]$ ($\mathbb{Z}[\omega]$) is a unique factorization domain, α is a prime in $\mathbb{Z}[i]$ ($\mathbb{Z}[\omega]$), since it is irreducible and $\mathbb{Z}[i]$ (and $\mathbb{Z}[\omega]$) are unique factorization domains. □

3.2 Cubic reciprocity

This section is based on Cox, Chapter 1, §4(A).[1] The following theorem is stated as Proposition 4.7 in Cox, Chapter 1, §4(A),[1] and as Proposition 9.1.4 in Ireland and Rosen, Chapter 9, §1.[3]

Proposition 3.14. Let $p \in \mathbb{Z}$ be a prime. Then,

(i) if $p = 3$, then $p = -\omega^2(1 - \omega)^2$, and $1 - \omega$ is a prime in $\mathbb{Z}[\omega]$ (by Proposition 3.13 and (3.4) below),

(ii) if $p \equiv 1 \pmod 3$, then $p = \pi\overline{\pi}$ for some prime π in $\mathbb{Z}[\omega]$, and $\overline{\pi}$ is a prime not associate to π,

(iii) if $p \equiv 2 \pmod 3$, then p is a prime in $\mathbb{Z}[\omega]$,

and every prime in $\mathbb{Z}[\omega]$ is associate to one of those listed above.

Proof. See Ireland and Rosen, Chapter 9, §1, Proposition 9.1.4.[3] □

We use the following notation in accordance with Cox, Chapter 1, §4(A) (apart from the parentheses, which are omitted in Cox).[1]

Definition 3.15. Given $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$, we write $\alpha \equiv \beta \pmod \gamma$ to indicate that α and β belong to the same coset in $\mathbb{Z}[\omega]/\gamma\mathbb{Z}[\omega]$.

The following lemma is necessary for defining the Legendre symbol in the cubic case (see Definition 3.4) and how it relates to cubic reciprocity. It is stated as Lemma 4.8 in Cox, Chapter 1, §4(A).[1]

Lemma 3.16. Let $\pi \in \mathbb{Z}[\omega]$ be a prime. Then $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ has $N(\pi)$ elements and either $N(\pi) = p$ or $N(\pi) = p^2$ for some integer prime p. Furthermore,

(i) if $N(\pi) = p$, then $p = 3$ or $p \equiv 1 \pmod 3$, and $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$,

(ii) if $N(\pi) = p^2$, then $p \equiv 2 \pmod 3$ and, $\mathbb{Z}/p\mathbb{Z}$ is the unique subfield of $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ of order p.

Proof. In Ireland and Rosen, Chapter 9, §2, Proposition 9.2.1 it is stated and proved that $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ has $N(\pi)$ elements and is a field. Since

$$N(1-\omega) = (1-\omega)(1-\omega^2) = 1 - \omega^2 - \omega + \omega^3 = 1 - (-1-\omega) - \omega + 1 = 1 + 1 + 1 = 3. \tag{3.4}$$

and, if $\pi = p$ for some prime $p \equiv 2 \pmod 3$,

$$N(\pi) = N(p) = p\overline{p} = p^2,$$

we see that the cases (i)–(ii) of Proposition 3.14 correspond to the case $N(\pi) = p$ (case (i) of this Lemma), and the case (iii) of Proposition 3.14 corresponds to the case $N(\pi) = p^2$ (case (ii) of this Lemma). Proposition 3.14. The isomorphism of (i) in this Lemma follows from the argument given in the proof in Ireland and Rosen, where it is shown that every element in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is congruent to some element in $\mathbb{Z}/p\mathbb{Z}$ modulo π.[3] It is well-known that $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements (See Dummit and Foote, Chapter 13, Section 13.1, Example (2) following Proposition 1[2]). In the proof in Ireland and Rosen,[3] it is shown that, in the case $N(\pi) = p^2$,

$$\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \{0, 1, \cdots, p-1\}\},$$

thus

$$\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega].$$

To see that $\mathbb{Z}/p\mathbb{Z}$ is the unique subfield of p elements, note that any subfield F of $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ with p elements must contain 1 and 0, since it is a field, and all of $\{0, 1, 1+1, 1+1+1, \cdots\} = \{0, 1, \cdots, p-1\}$. (Both $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ and F have characteristic p.) □

Remark 3.17. If $\pi \nmid 3$ and $N(\pi) = p$, then, by (i) of Lemma 3.16,

$$N(\pi) - 1 \equiv p - 1 \equiv 1 - 1 \equiv 0 \pmod 3,$$

and if $N(\pi) = p^2$, then, by (ii) of Lemma 3.16,

$$N(\pi) - 1 \equiv p^2 - 1 \equiv 2^2 - 1 \equiv 1 - 1 \equiv 0 \pmod 3,$$

thus, $3 \mid N(\pi) - 1$ always holds whenever $\pi \nmid 3$.

Remark 3.18. The quotient ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is indeed a field, by Lemma 4.3 of Section 4.1, since the prime ideal $\pi\mathbb{Z}$ is maximal (since $\mathbb{Z}[\omega]$ is a principal ideal domain, see Dummit and Foote, Chapter 8, Section 8.2, Proposition 7[2]). Since $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field, by Lemma 3.16, it follows that its multiplicative group $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ is cyclic of order $N(\pi) - 1$ (see Dummit and Foote, Chapter 9, Section 9.5, Proposition 18[2]).

This gives us the following corollary, stated as Corollary 4.9 in Cox, Chapter 1, §4(A),[1] which is an analog to Fermat's Little Theorem.

Corollary 3.19. Let $\pi \in \mathbb{Z}[\omega]$ be a prime and let $\alpha \in \mathbb{Z}[\omega]$ be such that $\pi \nmid \alpha$. Then

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi.$$

□

Proof. Let x be a generator of $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$. We have that $x^{N(\pi)-1}$ is the identity in $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$. Since we can write $\alpha = x^r$ for some $r \in \mathbb{Z}_{\geq 1}$, we have that

$$\alpha^{N(\pi)-1} = (x^r)^{N(\pi)-1} = x^{r(N(\pi)-1)} = (x^{N(\pi)-1})^r$$

is the identity on $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$, that is,

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi.$$

□

If π and $\alpha \in \mathbb{Z}[\omega]$ are defined as in Corollary 3.19, and, furthermore, $\pi \nmid 3$, then, since $3 \mid N(\pi) - 1 \in \mathbb{Z}$, by Remark 3.17, it holds that $\alpha^{(N(\pi)-1)/3} \in \mathbb{Z}[\omega]$ and

$$(\alpha^{(N(\pi)-1)/3})^3 - 1 \equiv \alpha^{(N(\pi)-1)} - 1 \equiv 0 \pmod{\pi},$$

thus $\alpha^{(N(\pi)-1)/3}$ is congruent to a cube root of unity modulo π. Note that all cube roots of unity are incongruent modulo π, since if any two were congruent, then we would have, $1 - \omega \equiv 0 \pmod{\pi}$ (by multiplying each side of the congruences $1 \equiv \omega$, $\omega \equiv \omega^2$, $\omega^2 \equiv 1 \pmod{\pi}$ by 1, ω^2, and ω respectively) contradicting that $1 - \omega$ is prime. A similar argument is given in Cox, Chapter 1, §4(A)[1]). In accordance with Cox,[1] we can, therefore, generalize the Legendre symbol (defined for the quadratic case in Definition 3.4) to the cubic case in the following way.

Definition 3.20. Let $\pi \in \mathbb{Z}[\omega]$ be a prime and let $\alpha \in \mathbb{Z}[\omega]$ be such that $\pi \nmid 3, \alpha$. Then the *Legendre symbol* $\left(\frac{\alpha}{\pi}\right)_3$ is defined to be the unique cube root of unity satisfying

$$\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}.$$

Lemma 3.21 below explains how this generalized Legendre symbol relates to cubic reciprocity.

Lemma 3.21. If $\alpha, \pi \in \mathbb{Z}[\omega]$ and π is a prime such that $\pi \nmid 3, \alpha$, then

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff x^3 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[\omega].$$

Proof. We have that

$$\begin{gathered} x^3 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[\omega] \implies \\ \alpha \equiv \beta^3 \pmod{\pi} \text{ for some } \beta \in (\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^* \implies \\ \alpha^{(N(\pi)-1)/3} \equiv \beta^{N(\pi)-1} \pmod{\pi} \text{ for some } \beta \in (\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^* \implies \\ \alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi}, \end{gathered}$$

where the last implication follows from Corollary 3.19. Conversely, since the group $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ is cyclic of order $N(\pi) - 1$, we may assume that it is generated by some element $y \in (\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ and that $\alpha \equiv y^m \pmod{\pi}$ for some integer $m \in \{1, \cdots, N(\pi) - 1\}$, thus,

$$\begin{gathered} \alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi} \implies y^{m(N(\pi)-1)/3} = 1 \implies \\ y^{m(N(\pi)-1)/3} = y^{N(\pi)-1} \implies (N(\pi) - 1) \mid m(N(\pi) - 1)/3 \text{ in } \mathbb{Z} \implies \\ 3 \mid m \text{ in } \mathbb{Z} \implies x^3 \equiv y^m \pmod{\pi} \text{ solvable in } \mathbb{Z}[\omega] \implies \\ x^3 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[\omega]. \end{gathered}$$

This shows that

$$x^3 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[\omega] \iff \alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi}. \qquad \square$$

Below, the Law of Cubic Reciprocity is stated, in accordance with Cox, Chapter 1, §4(A), Theorem 4.12.[1] First note that, by Proposition 3.12, given a prime $\pi \in \mathbb{Z}[\omega]$, the elements $\pm\pi, \pm\pi\omega$, and $\pm\pi\omega^2$ are associates, and, by Ireland and Rosen, Chapter 9, §3, Proposition 9.3.5[3], if $\pi \nmid 3$, then precisely one of these pairs are congruent to ± 1 modulo 3. Therefore, we can restrict ourselves to primes $\pi \in \mathbb{Z}[\omega]$ such that $\pi \nmid 3$ and $\pi \equiv \pm 1$. In Cox, Chapter 1, §4(A), such a prime is referred to as a *primary* prime.[1]

Theorem 3.22. (The Law of Cubic Reciprocity) If $\pi, \theta \in \mathbb{Z}[\omega]$ are primes such that $\pi, \theta \nmid 3$, $\pi, \theta \equiv \pm 1$, and $N(\pi) \neq N(\theta)$, then

$$\left(\frac{\pi}{\theta}\right)_3 = \left(\frac{\theta}{\pi}\right)_3$$

Proof. See Ireland and Rosen, Chapter 9, §4 and §5, for two different proofs. $\square$

3.3 Biquadratic reciprocity

This section is mostly based on Cox, Chapter 1, §4(B).[1] Proposition 3.23 below is stated as Proposition 4.18 in Cox, Chapter 1, §4(B),[1] and as Proposition 18(2) in Dummit and Foote, Chapter 8, Section 8.3.[2]

Proposition 3.23. Let $p \in \mathbb{Z}$ be a prime. Then,

(i) if $p = 2$, then $p = i^3(1+i)^2$, and $1+i$ is a prime in $\mathbb{Z}[i]$,

(ii) if $p \equiv 1 \pmod 4$, then $p = \pi\overline{\pi}$ for some prime π in $\mathbb{Z}[i]$, and $\overline{\pi}$ is a prime not associate to π,

(iii) if $p \equiv 3 \pmod 4$, then p is a prime in $\mathbb{Z}[i]$,

and every prime in $\mathbb{Z}[i]$ is associate to one of those listed above.

Proof. See Dummit and Foote, Chapter 8, Section 8.3, Proposition 18(2).[2] □

The following notation is analogous to the one given in Definition 3.15, and is also used by Cox (apart from the parentheses, which are omitted in Cox).[1]

Definition 3.24. Given $\alpha, \beta, \gamma \in \mathbb{Z}[i]$, we write $\alpha \equiv \beta \pmod \gamma$ to indicate that α and β belong to the same coset in $\mathbb{Z}[i]/\gamma\mathbb{Z}[i]$.

Remark 3.25. As in the case of $\mathbb{Z}[\omega]$ (Lemma 3.16), given a prime $\pi \in Z[i]$, the set $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a finite field of $N(\pi)$ elements, by Proposition 9.8.1 in Ireland and Rosen, Chapter 9, §8.[3] As in the case of $Z[\omega]$, there are two possibilities: either $N(\pi) = p$ for some prime $p \in \mathbb{Z}$ or $N(\pi) = p^2$ for some prime $p \in \mathbb{Z}$, and, by Proposition 3.23, the former corresponds to the case $p = 2$ or $p \equiv 1 \pmod 4$, and the latter to the case $p \equiv 3 \pmod 4$. Note that

$$N(1+i) = (1+i)\overline{(1+i)} = (1+i)(1-i) = 1+1 = 2.$$

By the same argument as in the case of $\mathbb{Z}[\omega]$ (Corollary 3.19), we have that $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ is cyclic of order $N(\pi) - 1$, implying the following corollary, stated as (4.19) in Cox, Chapter 1, §4(B),[1] which is also an analog to Fermat's Little Theorem.

Corollary 3.26. Let $\pi \in \mathbb{Z}[i]$ be a prime and let $\alpha \in \mathbb{Z}[i]$ be such that $\pi \nmid \alpha$. Then

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi.$$

Proof. The proof is analogous to the proof of Corollary 3.19, replacing every $\mathbb{Z}[\omega]$ with $\mathbb{Z}[i]$. □

Given any prime π not dividing 2, i.e., not associate to $1+i$, it follows from Proposition 3.23 that

$$N(\pi) \equiv 1 \pmod 4,$$

since $3^2 \equiv 1 \pmod 4$, thus $4 \mid N(\pi) - 1$. Also the four fourth roots of unity $\pm 1, \pm i$ are incongruent modulo π, since

$$i \equiv -i \pmod \pi \implies 1 \equiv -1 \pmod \pi \implies 2 \equiv 0 \pmod \pi,$$

and

$$-1 \equiv -i \pmod \pi \implies 1 \equiv i \pmod \pi \implies -i \equiv 1 \pmod \pi \implies$$
$$i \equiv -1 \pmod \pi \implies 1+i \equiv 0 \pmod \pi,$$

which shows that any congruence modulo π between two units of $\mathbb{Z}[i]$ implies a contradiction, since $\pi \nmid 2, 1+i$. If α is such that $\pi \nmid \alpha$, then

$$(\alpha^{(N(\pi)-1)/4})^4 - 1 \equiv \alpha^{N(\pi)-1} - 1 \equiv 0 \pmod 4,$$

which shows that $\alpha^{(N(\pi)-1)/4}$ is a fourth root of unity. In accordance with Cox, Chapter 1, §4(B),[1] we can, therefore, generalize the Legendre symbol to the biquadratic case in the following way.

Definition 3.27. If $\pi, \alpha \in \mathbb{Z}[i]$, π is prime, and $\pi \nmid 2,\ \alpha$, then the *Legendre symbol* $\left(\frac{\alpha}{\pi}\right)_4$ is defined to be the unique fourth root of unity satisfying

$$\alpha^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \pmod{\pi}.$$

As in the cubic and quadratic cases, the Legendre symbol is related to biquadratic reciprocity, as explained in the following result.

Lemma 3.28. If $\pi, \alpha \in \mathbb{Z}[i]$, π is prime, and $\pi \nmid 2, \alpha$, then

$$\left(\frac{\alpha}{\pi}\right)_4 = 1 \iff x^4 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[i].$$

Proof. This proof is analogous to the proof of Lemma 3.21. We have that

$$x^4 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[i] \implies$$

$$\alpha \equiv \beta^4 \pmod{\pi} \text{ for some } \beta \in (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^* \implies$$

$$\alpha^{(N(\pi)-1)/4} \equiv \beta^{N(\pi)-1} \pmod{\pi} \text{ for some } \beta \in (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^* \implies$$

$$\alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi},$$

where the last implication follows from Corollary 3.26. Conversely, since the group $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ is cyclic of order $N(\pi) - 1$, we may assume that it is generated by some element $y \in (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ and that $\alpha \equiv y^m \pmod{\pi}$ for some integer $m \in \{1, \cdots, N(\pi) - 1\}$, thus,

$$\alpha^{(N(\pi)-1)/4} \equiv 1 \pmod{\pi} \implies y^{m(N(\pi)-1)/4} = 1 \implies$$

$$y^{m(N(\pi)-1)/4} = y^{N(\pi)-1} \implies (N(\pi) - 1) \mid m(N(\pi) - 1)/4 \text{ in } \mathbb{Z} \implies$$

$$4 \mid m \text{ in } \mathbb{Z} \implies x^4 \equiv y^m \pmod{\pi} \text{ solvable in } \mathbb{Z}[i] \implies$$

$$x^4 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[i].$$

This shows that

$$x^4 \equiv \alpha \pmod{\pi} \text{ solvable in } \mathbb{Z}[i] \iff \alpha^{(N(\pi)-1)/4} \equiv 1 \pmod{\pi}. \qquad \square$$

An important property of the Legendre symbol is the one stated in the following proposition.

Proposition 3.29. If $\pi, \alpha, \beta \in \mathbb{Z}[i]$ satisfy that π is prime and $\pi \nmid 2, \alpha, \beta$, then

$$\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4,$$

that is, the Legendre symbol is multiplicative.

Proof. By Definition, $\left(\frac{\alpha\beta}{\pi}\right)_4$ is the unique fourth root of unity such that

$$(\alpha\beta)^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha\beta}{\pi}\right)_4 \pmod{\pi},$$

that is,

$$\alpha^{(N(\pi)-1)/4}\beta^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha\beta}{\pi}\right)_4 \pmod{\pi}.$$

Since $\left(\frac{\alpha}{\pi}\right)_4$ and $\left(\frac{\beta}{\pi}\right)_4$ are the unique fourth roots of unity such that

$$\alpha^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \pmod{\pi}$$

and

$$\beta^{(N(\pi)-1)/4} \equiv \left(\frac{\beta}{\pi}\right)_4 \pmod{\pi}$$

respectively, it follows that

$$\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4,$$

□

Below, the Law of Biquadratic Reciprocity is stated, in accordance with Cox, Chapter 1, §4(B), Theorem 4.21.[1] First note that, by Proposition 3.12, given a prime $\pi \in \mathbb{Z}[i]$, the elements $\pm\pi, \pm\pi i$ are associates, and, by Ireland and Rosen, Chapter 9, §8, Lemma 7,[3] if $\pi \nmid 2$, then precisely one of these elements congruent to 1 modulo $(1+i)^3 = (1+i)(1+i)(1+i) = (1+2i-1)(1+i) = 2i-2$, or, equivalently, modulo $-i(2i-2) = 2+2i$). Therefore, we can restrict ourselves to primes $\pi \in \mathbb{Z}[i]$ such that $\pi \nmid 2$ and $\pi \equiv 1$ (2 + 2i). In Cox, Chapter 1, §4(B), such a prime is referred to as a *primary* prime.[1]

Theorem 3.30. (The Law of Biquadratic Reciprocity) If $\pi, \theta \in \mathbb{Z}[i]$ are primes such that $\pi \neq \theta$ and $\pi, \theta \equiv 1$ (2 + 2i), then

$$\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4 (-1)^{(N(\pi)-1)(N(\theta)-1)/16}$$

Proof. See Ireland and Rosen, Chapter 9, §9.[3] □

3.4 The case $n = 27$

Proof of Theorem 3.1. The proof presented here is a version of the proof given at the end of Cox, Chapter 1, §4(A),[1] and is a great example of how the result in Section 3.2 (especially the Law of Cubic Reciprocity) can be applied. Assume that $p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p. By Proposition 3.14, there exists a prime $\pi \in \mathbb{Z}$ such that

$$p = N(\pi) = \pi\overline{\pi},$$

where π and $\overline{\pi}$ are nonassociate. We may assume that $\pi \equiv \pm 1 \pmod 3$, since it is associate to such a prime. It follows that there exist $a, b \in \mathbb{Z}$, such that $\pi = a + 3b\omega$ and $a \equiv 1 \pmod 3$, hence,

$$4p = 4N(\pi) = 4(a^2 - 3ab + 9b^2) = 4a^2 - 12ab + 36b^2 = (4a^2 - 12ab + 9b^2) + 27b^2 = (2a - 3b)^2 + 27b^2.$$

Note that 2 is a prime in $\mathbb{Z}[\omega]$, by Proposition 3.14. Also note that $2 \equiv -1 \pmod 3$. By the isomorphism of Lemma 3.16(i), since 2 is a cubic residue modulo p, the congruence $x^3 \equiv 2 \pmod{\pi}$ also has a solution in $\mathbb{Z}[\omega]$, that is

$$\left(\frac{2}{\pi}\right)_3 = 1,$$

which, by the Law of Cubic Reciprocity (Theorem 3.22), implies that

$$\left(\frac{\pi}{2}\right)_3 = 1.$$

By Definition 3.20, since $(N(2) - 1)/3 = (4 - 1)/3 = 1$,

$$a + 3b\omega \equiv \pi \equiv \pi^1 \equiv \pi^{(N(2)-1)/3} \equiv \left(\frac{\pi}{2}\right)_3 \equiv 1 \pmod 2,$$

which implies that b is even and a is odd. Since b is even, it follows that $2a - 3b$ and b are even, thus,

$$p = \frac{(2a-3b)^2}{4} + 27\frac{b^2}{4} = \left(\frac{2a-3b}{2}\right)^2 + 27\left(\frac{b}{2}\right)^2,$$

is of the form $x^2 + 27y^2$.

Conversely, assume that $p = x^2 + 27y^2$ for some $x, y \in \mathbb{Z}$. Then $p \equiv 1 \pmod 3$, since $27y^2 \equiv 0 \pmod 3$ and $x \not\equiv 0 \pmod 3$ (since $p = x^2 + 27y^2 > 3$ is a prime), which implies that $x^2 \equiv 1 \pmod 3$. As in the first part of this proof, by Proposition 3.14, there exists a prime $\pi \in \mathbb{Z}$ such that

$$p = N(\pi) = \pi\overline{\pi},$$

where π and $\overline{\pi}$ are nonassociate, and we may again assume that $\pi \equiv \pm 1 \pmod 3$. Since

$$p = x^2 + 27y^2 = (x + 3\sqrt{-3}y)(x - 3\sqrt{-3}y),$$

and

$$\sqrt{-3} = 1 + 2\omega \in \mathbb{Z}[\omega],$$

we have that $\pi = (x + 3\sqrt{-3}y)$ is a prime in $\mathbb{Z}[\omega]$, by Proposition 3.13, since its norm is a prime, and, by Proposition 3.14, $\overline{\pi}$ is a prime not associate to π. Since $2 \equiv -1 \pmod 3$, $(x + 3\sqrt{-3}y) \equiv x \bmod 3$, and $x \equiv 1$ or $x \equiv -1 \pmod 3$, we can apply the Law of Cubic Reciprocity (Theorem 3.22), which gives us

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3.$$

By Definition 3.20, since $(N(2) - 1)/3 = (4 - 1)/3 = 1$,

$$\pi \equiv \pi^1 \equiv \pi^{(N(2)-1)/3} \equiv \left(\frac{\pi}{2}\right)_3 \pmod 2.$$

Since, $p = x^2 + 27y^2 > 2$ is a prime, it is not even, hence, x must be odd if y is even and vice versa. This implies that

$$\pi \equiv x + 3\sqrt{-3}y \equiv x + 3(1 + 2\omega)y \equiv x + 3y + 6\omega y \equiv x + 3y \equiv x + y \equiv 1 \pmod 2,$$

This gives us

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 = 1$$

By the isomorphism of Lemma 3.16(i), it follows that 2 is a cubic residue modulo p. □

3.5 The case $n = 64$

As in the previous section, this section contains a version of a proof given in Cox, Chapter 1, §4.[1] This time it is the result of Section 3.3 that will be applied, but we will also use the following two lemmas, referred to as *supplementary laws* in Cox, Chapter 1, §4(B).[1]

Lemma 3.31. If $\pi = a + bi \in \mathbb{Z}[i],\ (a, b \in \mathbb{Z})$ is a prime such that $\pi \equiv 1 \pmod{2 + 2i}$, then

$$\left(\frac{i}{\pi}\right)_4 = i^{-(a-1)/2}.$$

Lemma 3.32. If $\pi = a + bi \in \mathbb{Z}[i],\ (a, b \in \mathbb{Z})$ is a prime such that $\pi \equiv 1\ (2 + 2\mathrm{i})$, then

$$\left(\frac{1+i}{\pi}\right)_4 = i^{(a-b-1-b^2)/4}.$$

The following lemma is stated as Theorem 4.23(i) in Cox, Chapter 1, §4(B), [1] and follows from the previous two, although, acoording to Cox, it can also be proved using only biquadratic reciprocity.[1]

Lemma 3.33. If $\pi = a + bi \in \mathbb{Z}[i],\ (a, b \in \mathbb{Z})$ is a prime such that $\pi \equiv 1\ (2 + 2\mathrm{i})$, then

$$\left(\frac{2}{\pi}\right)_4 = i^{ab/2}.$$

Proof of Theorem 3.2. The proof presented here is based on the proof given in Cox, Chapter 1, §4(B), Theorem 4.23(ii).[1] If $p \equiv 1 \pmod 4$, then, by Proposition 3.23, $\pi\overline{\pi}$ for some π not associate to its complex conjugate $\overline{\pi}$. In the discussion right before Theorem 3.30 near the end of Section 3.3, we saw that this prime is associate to a prime congruent to 1 modulo $2+2i$, hence, we may assume that π itself satisfies this property. If we write $\pi = a + bi$, we have that

$$\pi = (2+2i)\gamma + 1$$

for some $\gamma \in \mathbb{Z}[i]$. Let $c, d \in \mathbb{Z}$ be such that $\gamma = c + di$. Then

$$\pi = a + bi = 2c + 2di + 2ci - 2d + 1 = (2c - 2d + 1) + 2i(c + d),$$

which implies that a is odd and b is even. By the same argument as in the case of $\mathbb{Z}[\omega]$, we have the isomorphism $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$. By Lemma 3.33,

$$2 \text{ is a biquadratic residue} \iff i^{ab/2} = 1 \iff 4 \mid ab/2 \iff 8 \mid b.$$

Note that $8 \mid b$ if and only if $p = \pi\overline{\pi} = a^2 + b^2$ is of the form $x^2 + 64y^2$. Conversely, if p is of the form $x^2 + 64y^2$, then x must be odd, since p is prime, and, since $3^2 \equiv 1^2 \equiv 1 \pmod 4$, it follows that $p \equiv 1 \pmod 4$. □

4 The case $n \not\equiv 3 \pmod 4$, n squarefree, and the Hilbert class field

In the previous part, we were working in the rings $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$, which are the rings of integers (see Definition 2.5) of $\mathbb{Q}[\omega]$ and $\mathbb{Q}[i]$ respectively, by Proposition 2.11 (or by Proposition 4.23). We saw that the rings of integers in these cases are Euclidean domains and, thus, principal ideal domains and unique factorization domains. This need not be the case for an arbitrary field extension K of $\mathbb{Q}$. In the Section 4.1, we see that the ring $\mathcal{O}_K$ of integers in K is always a Dedekind domain (see Theorem 4.5) in which unique factorization holds for ideals. The theory of number fields discussed in this section allows us to state the existence theorem of the Hilbert Class field in Section 4.2. In Sections 4.3–4.4 we explained how to apply the Hilbert class field to primes of the form $x^2 + ny^2$. In Section 4.3 we also discuss some theory of quadratic forms which will prove helpful for applying the Hilbert class fields (e.g., for the case $n = 14$ considered in Section 4.5).

4.1 Dedekind domains

The following definition is according to §3.4 in Samuel.[5]

Definition 4.1. Let R be an integral domain. Then, R is called a *Dedekind domain* if

(i) R is integrally closed, i.e., if α belongs to the fraction field of R and $f(\alpha) = 0$ for some monic $f \in R[x]$, then $\alpha \in R$, (see Definition 2.6)

(ii) R is Noetherian, i.e., for every ascending chain $I_1 \subset I_2 \subset \cdots$ of ideals in R, there exists an index $n_0 \in \mathbb{Z}_{\geq 1}$ such that $I_n = I_{n_0}$ for all integers $n \geq n_0$,

(iii) every nonzero prime ideal P of R is maximal

The corollary of Theorem 9 in Marcus states the following.[4]

Proposition 4.2. Let K be a number field. Then its ring of integers $\mathcal{O}_K$ is a free Z-module of rank $[K : \mathbb{Q}]$.

Proof. See the corollary of Theorem 9 in Marcus,[4] where the term *abelian group* is used instead of *Z-module.* (The two notions are equivalent, as explained in Dummit and Foote, Chapter 10.[2]) □

The two lemmas below is stated as Propositions 12–13 and Corollary 3 in Dummit and Foote, Chapter 7, Section 7.4 and 7.1 respectively.[2]

Lemma 4.3. Let R be any commutative ring with a multiplicative identity 1 and let I be an ideal of R. Then

(i) I is a prime ideal of R if and only if R/I is an integral domain

(ii) I is a maximal ideal of R if and only if R/I is a field.

Proof. This proof is based on the proofs Dummit and Foote, Chapter 7, Section 7.4, Proposition 12. Part (i) follows from the definitions of a prime ideal, an integral domain, and a quotient ring in the following way.

$$I \text{ is prime} \iff \text{for all } a, b \in R,\ a \in I \text{ or } b \in I \text{ if } ab \in I \iff$$

$$\text{for all } a, b \in R,\ a + I = 0 + I \text{ or } b + I = 0 + I \text{ if } ab + I = 0 + I \iff$$

$$\text{for all } a, b \in R/I,\ a = 0 \text{ or } b = 0 \text{ if } ab = 0 \iff R/I \text{ is an integral domain}$$

The proof of part (ii) uses the Fourth Ring Isomorphism Theorem, stated in Dummit and Foote, Chapter 7, Section 7.3, Theorem 8(3), which states that, for ideals A of R containing I, the map $A \mapsto R/A$ is bijective.[2] Since

$$I \text{ is maximal} \iff J = I \text{ or } J = R \text{ whenever } I \subset J \subset R \iff$$

it follows from the Fourth Ring Isomorphism Theorem that

$$I \text{ is maximal} \iff J/I = I/I \text{ or } J/I = R/I \text{ whenever } I/I \subset J/I \subset R/I,$$

that is, if I is maximal, R/I has only two ideals $I/I = (0)$ and R/I itself. This is equivalent to R/I being a field, since, if (0) and R/I are the only ideals of R/I, then, for any nonzero $a \in R/I$, the ideal (a) contains the multiplicative identity 1, that is, a has a multiplicative inverse in R/I, thus, R/I is a field, and, conversely, if R/I is a field, then any nonzero element in R/I has a multiplicative inverse, thus, any ideal other than (0) contains $(1) = R/I$. □

Lemma 4.4. Every finite integral domain is a field.

Proof. This lemma follows from the cancellation law in integral domains. Let R be any finite integral domain. Let $a \in R \setminus \{0\}$ be arbitrary. We need to show that there exists a multiplicative inverse a^{-1} of a such that $aa^{-1} = 1$. For any two $b_1, b_2 \in R$,

$$ab_1 = ab_2 \implies b_1 = b_2,$$

since R is an integral domain. This shows that the map $b \mapsto ab$ (multiplication by a) is injective. Since R is finite, the map $a \mapsto ab$ is an automorphism. It follows that $aa^{-1} = 1$ for some $a^{-1} \in R$. The proof given in Dummit and Foote, Chapter 7, Section 7.1, Corollary 3 follows the same idea (it is stated as a corollary of the cancellation law).[2] □

The following theorem is stated in Dummit and Foote, Chapter 16, Section 16.3 as Proposition 14(2),[2] and in Cox, Chapter 2, §5(A) as Theorem 5.5.[1]

Theorem 4.5. Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.

Proof. See Dummit and Foote, Chapter 16, Section 16.3, Proposition 14(2).[2] □

Below we discuss some important properties of Dedekind domain. In particular, these properties hold in $\mathcal{O}_K$ for any number field K, by Theorem 4.5. Most of these definitions and propositions can be extended to integral domains (with some modification), as seen in Dummit and Foote, Chapter 16, Section 16.2.[2] Dummit and Foote state the following definition.[2]

Definition 4.6. Let R be a Dedekind domain and let K be its field of fractions. An R-submodule A of K is called a *fractional ideal of* R if it satisfies one of the following equivalent conditions.

(i) $dA \subset R$ for some $d \in R \setminus \{0\}$.

(ii) $A = d^{-1}I$ for some $d \in R \setminus \{0\}$ and some nonzero ideal I of R.

A *principal fractional ideal of* R is an ideal of the form xR, where $x \in K \setminus \{0\}$. This definition agrees with the definitions given in Cox, Chapter 2, §5(A),[1] where it is stated for rings of integers of a number field in particular, and in Dummit and Foote, Chapter 16, Section 16.2.[2]

Remark 4.7. To see that (i) implies (ii), note that, if $dA \subset R$, then dA is an R-submodule of R. Since the R-submodules of R are precisely the ideals of R (by the definition of a module and the definition of an ideal in a commutative ring, see Dummit and Foote, Chapter 10, Section 10.1, Example (1)[2]) we may put $I = dA$, which gives us

$$A = d^{-1}dA = d^{-1}I,$$

where I is an ideal of R. Is is also clear that (ii) implies (i), because if $A = d^{-1}I$, for some $d \in K \setminus \{0\}$ and some nonzero ideal I of R, then $dA = I \subset R$.

Remark 4.8. In Marcus, Chapter 3, Exercise 31,[4] a fractional ideal in a Dedekind domain is defined differently, namely, as a set of the form xI, where $x \in K \setminus \{0\}$ and I is a nonzero ideal.

In Definition 4.9 below, we give the definition of the product of two fractional ideals. This definition is given Dummit and Foote, Chapter 16, Section 16.2.[2]

Definition 4.9. Let R be a Dedekind domain and let K be its field of fractions. Given two fractional ideals $A = c^{-1}I$ and $B = d^{-1}J$, where $c, d \in R \setminus \{0\}$ and I, J are nonzero ideals of R, we define their product AB as

$$AB := \Big\{ \sum_{i=1}^{r} a_i b_i \mid r \in \mathbb{Z}_{\geq 1},\ a_i \in A,\ b_i \in B \text{ for all } i \in \{1, \cdots, r\} \Big\} =$$

$$\Big\{ \sum_{i=1}^{r} c^{-1} g_i d^{-1} h_i \mid r \in \mathbb{Z}_{\geq 1},\ g_i \in I,\ h_i \in J \text{ for all } i \in \{1, \cdots, r\} \Big\} =$$

$$c^{-1}d^{-1}\Big\{ \sum_{i=1}^{r} g_i h_i \mid r \in \mathbb{Z}_{\geq 1},\ g_i \in I,\ h_i \in J \text{ for all } i \in \{1, \cdots, r\} \Big\} = c^{-1}d^{-1}IJ = (cd)^{-1}IJ$$

The following proposition is stated as part of Theorem 15 in Dummit and Foote, Chapter 16, Section 16.3,[2]

Proposition 4.10. Let R be a Dedekind domain. Then any nonzero fractional ideal A of R is invertible, that is, there exists a fractional ideal A^{-1} such that $AA^{-1} = R$.

Proof. See Dummit and Foote, Chapter 16, Section 16.3, Theorem 15.[2] □

Definition 4.11. Let R be a Dedekind domain and let K be its field of fractions. In accordance with Cox, Chapter 2, §5(A),[1] we let I_K denote the *set of fractional ideals of* R and we let P_K denote the *set of principal fractional ideals of* R. If R is a Dedekind domian, then, by Proposition 4.10, I_K and P_K denote the sets of all fractional ideals and principal fractional ideals respectively.

The following proposition is stated as part of Proposition 9 in Dummit and Foote, Chapter 16, Section 16.2.[2]

Proposition 4.12. Let R be a Dedekind domain and let K be its field of fractions. Then I_K is a group under multiplication and P_K is a subgroup of I_K.

Proof. Since R itself is an ideal of R and P_K consists of invertible ideals of the form $xR,\ x \in K \setminus \{0\}$, we have that $P_K \subset I_K$. It follows from Definition 4.9 that P_K and I_K are closed under multiplication, and that the multiplication is associative and commutative in both sets (since this is the case in R). By the definition of the product of ideals, $R \in P_K \subset I_K$ is the identity element, and, since every fractional ideal in I_K is invertible, I_K is closed under inversion. The same is true for P_K, since the inverse of xR is given by $x^{-1}R$. □

The following definition is stated in Dummit and Foote, Chapter 16, Section 16.2.[2]

Definition 4.13. Let R be a Dedekind domain and let K be its field of fractions. Then the quotient group I_K/P_K is called the *ideal class group of* R. In accordance with Cox, Chapter 2, §5(A) (where this definition is stated for a ring of integers in a number field in particular),[1] we denote the ideal class group by $\mathcal{C}(R)$. The class number of R is defined as the order of $\mathcal{C}(R)$.

The following Proposition, is stated as part of Theorem 15 in Dummit and Foote, Chapter 16, Section 16.3,[2] and Proposition 4.15 follows. (It is stated as part of Corollary 5.6 in Cox, Chapter 2, §5(A).[1])

Proposition 4.14. Let R be a Dedekind domain. Then every nonzero proper ideal I of R can be written uniquely (up to order) as the product

$$I = P_1 \cdots P_r, \quad r \in \mathbb{Z}_{\geq 1},$$

of nonzero prime ideals.

Proof. See Dummit and Foote, Chapter 16, Section 16.3, Theorem 15.[2] □

Proposition 4.15. Let R be a Dedekind domain, and let $I, r, P_1, \cdots, P_r$ be as in 4.14, then, given any prime ideal P in R, it holds that $I \subset P$ if and only if $P = P_i$ for some $i \in \{1, \cdots, r\}$.

Proof. This argument is based on the proof of $A \subset B \iff B|A$, for ideals A, B in a Dedekind domain, given in Dummit and Foote, Chapter 16, Section 16.3.[2] If $P = P_i$ for some $i \in \{1, \cdots, r\}$, then every element in I is the sum of terms of the form ap, $a \in R$, $p \in P$, hence every element in I is also an element in P. Conversely, if $I \subset P$, we have that

$$IP^{-1} \subset PP^{-1} = R,$$

thus, IP^{-1} is a fractional ideal contained in R, i.e., an ideal. Since

$$I = IP^{-1}P$$

and since the factorization into prime ideals is unique, by Proposition 4.14, we can conclude that $P = P_i$ for some $i \in \{1, \cdots, r\}$. □

Remark 4.16. The $P_i's$ in Proposition 4.14 need not be distinct, and, therefore, we may write the product as

$$I = P_1^{n_1} \cdots P_s^{n_s}, \quad s \in \mathbb{Z}_{\geq 1}, \quad n_1, \cdots, n_s \in \mathbb{Z}_{\geq 1}.$$

From now on, we will, in particular, restrict ourselves to rings of integers in number field, which are Dedekind domains by Proposition 4.5 The following definitions are stated in Cox, Chapter 2, §5(A).[1]

Definition 4.17. Given two number fields K, L such that $K \subset L$, and given a prime ideal P of $\mathcal{O}_K$, we can, according to Proposition 4.14, write the ideal $P\mathcal{O}_L$ of $\mathcal{O}_L$ generated by the set P as the product $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_g}$, where, $g \in \mathbb{Z}_{\geq 1}$, the Q_i's are distinct (nonzero) prime ideals of $\mathcal{O}_L$, and, for each $i \in \{1, \cdots, g\}$, $e_i \in \mathbb{Z}$. We call e_i the *ramification index of P in Q_i*, and we call the degree $f_i := [\mathcal{O}_L/Q_i : \mathcal{O}_K/P]$ of the field extension $\mathcal{O}_K/P \subset \mathcal{O}_L/Q_i$, the *inertial degree of P in Q_i*. If $e_i > 1$ for some $i \in \{1, \cdots, g\}$, then we say that P *ramifies in L*. If $K \subset L$ is a Galois extension, then, by Cox, Chapter 2, §5(A), Theorem 5.9,[1] the ramification indices e_i, $i = 1, \cdots, g$ are all equal, and the same goes for the inertia degrees. In this case, if we let e denote the ramification index and let f denote the inertia degree, we say that P *splits completely in L* if $e = f = 1$.

For fractional ideals of $\mathcal{O}_K$, we have a similar unique factorization, as explained in the following proposition, which is stated as Proposition 5.7 in Cox, Chapter 2, §5(A),[1] but in this case we also allow the exponents to be negative.

Proposition 4.18. Let K be a number field. Then every fractional ideal I of $\mathcal{O}_K$ can be written uniquely (up to order) as the product

$$I = P_1^{n_1} \cdots P_r^{n_r}, \quad r \in \mathbb{Z}_{\geq 1}, \quad n_1, \cdots, n_r \in \mathbb{Z},$$

where $P_1, \cdots, P_r$ are prime ideals of $\mathcal{O}_K$.

Proof. See Cox, Chapter 2, §5(A), Proposition 5.7.[1] □

The following theorem is stated as Theorem 21 in Marcus, Chapter 3,[4] and as Theorem 5.8 in Cox, Chapter 2, §5(A).[1]

Theorem 4.19. Using the same notation as in Definition 4.17, it holds that

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Proof. See Marcus, Chapter 3, Theorem 21, where this Theorem is proved both for the special case $K = \mathbb{Q}$ and for the general case.[4] □

Regarding the problem of primes of the form $x^2 + ny^2$, there is one type of number fields that play an important role, namely, the quadratic fields, and, in particular, the imaginary quadratic fields (see Definition 4.20 below). Quadratic fields are explained in more detail in Cox, Chapter 2, §5(B),[1] in Ireland and Rosen, Chapter 13, §1,[3] and in Samuel, Chapter 2, §2.5.[5]

Definition 4.20. A field K is called a *quadratic (number) field* if $[K : \mathbb{Q}] = 2$. Every such field K is of the form $\mathbb{Q}(\sqrt{m})$, where $m \in \mathbb{Z}$ is squarefree (as shown in Samuel, Chapter 2, §2.5, Proposition 1[5]), and, thus, a number field. If $\sqrt{m}$ is imaginary, i.e., if $m < 0$, then K is called an *imaginary quadratic (number) field*. Note that $m \neq 0$, since 0 is not squarefree, and m could be any squarefree integer except 1, since $\sqrt{m} \in \mathbb{Q}$ if and only if $m = 1$.

The following definition is given in Ireland and Rosen, Chapter 12, §1–2.[3]

Definition 4.21. Let K be any number field and let L/K be any algebraic field extension of K (see Definition 2.3). If $\alpha_1, \cdots, \alpha_n,\ n \in \mathbb{Z}_{\geq 1}$ is a basis for this extension. Given an element $\alpha \in L$, the *trace of* α is the sum

$$\mathrm{tr}(\alpha) := a_1 + \cdots + a_n,$$

where $a_i,\ i \in \{1, \cdots, n\}$, denotes the coefficient of the α_i-term when expressing $\alpha\alpha_i$ as a linear combination of $\alpha_1, \cdots, \alpha_n$. Given some elements $\beta_1, \cdots, \beta_r \in L,\ r \in \mathbb{Z}_{\geq 1}$, their *discriminant* is defined to be $\det(\mathrm{tr}(\beta_i\beta_j))$, where $(\mathrm{tr}(\beta_i\beta_j))$ denotes the matrix

$$\begin{pmatrix} \mathrm{tr}(\beta_1\beta_1) & \cdots & \mathrm{tr}(\beta_1\beta_r) \\ \vdots & \ddots & \vdots \\ \mathrm{tr}(\beta_r\beta_1) & \cdots & \mathrm{tr}(\beta_n\beta_n) \end{pmatrix}.$$

If K is an arbitrary algebraic extension of $\mathbb{Q}$, then the *discriminant of* K (or *the discriminant of* $\mathcal{O}_K$) is the discriminant of *any integral basis for* $\mathcal{O}_K$, i.e., any basis $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_K$ for $K/\mathbb{Q}$ such that $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. (Such a basis exists according to Ireland and Rosen, Chapter 12, §2, Proposition 12.2.2.[3])

Proposition 4.22 is stated (as Proposition 13.1.2) and proved in Ireland and Rosen, Chapter 13, §1,[3] and Proposition 4.23 is stated (as Theorem 1) and proved in Samuel, Chapter 2, §2.5.[5]

Proposition 4.22. Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field. Then the discriminant D_K of K is given by

$$D_K = \begin{cases} m & \text{if } m \equiv 1 \pmod 4 \\ 4m & \text{otherwise} \end{cases}$$

Proof. See Ireland and Rosen, Chapter 13, §1, Proposition 13.1.2.[3] □

Proposition 4.23. Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field. Then the ring of integers $\mathcal{O}_K$ in K is given by

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[(1 + \sqrt{m})/2] & \text{if } m \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{m}] & \text{otherwise} \end{cases}$$

Proof. See Samuel, Chapter 2, §2.5, Theorem 1.[5] □

Remark 4.24. If $K = \mathbb{Q}(\sqrt{-m})$, $m \in \mathbb{Z}_{\geq 1}$, is an imaginary quadratic field, then, the extension $K/\mathbb{Q}$ is Galois (as is the case for every quadratic extension of $\mathbb{Q}$ as explained in Dummit and Foote, Chapter 14, Section 14.1, page 563, Example 2[2]), and the automorphisms of K which fix $\mathbb{Q}$ are the identity automorphism and complex conjugation $\tau : \sqrt{-m} \mapsto -\sqrt{-m}$. To prove this, one can use the same argument as for $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ in the proof of Proposition 3.6.

The following Proposition is stated as part of Exercise 5.19(a) in Cox, Chapter 2, §5.[1]

Proposition 4.25. Given an imaginary quadratic field K and a Galois extension L of K. Then the extension $L/\mathbb{Q}$ is Galois whenever $L = \tau(L)$, where τ denotes complex conjugation.

Proof. Suppose that $L = \tau(L)$. Then, for any $\sigma \in \mathrm{Gal}(L/K)$, it holds that $\tau \circ \sigma \in \mathrm{Aut}(L/\mathbb{Q})$, since τ and σ fix $\mathbb{Q}$. Since τ does not fix K, we have that $\tau \circ \sigma \notin \mathrm{Gal}(L/K)$. This shows that each $\sigma \in \mathrm{Gal}(L/K)$ gives rise to two distinct automorphism $\sigma, \tau \circ \sigma \in \mathrm{Aut}(L/\mathbb{Q})$. For any two $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$,

$$\tau \circ \sigma_1 = \tau \circ \sigma_2 \implies \sigma_1 = \tau \circ \tau \circ \sigma_1 = \tau \circ \tau \circ \sigma_2 = \sigma_2,$$

since τ is its own inverse, which shows that

$$|\mathrm{Aut}(L/\mathbb{Q})| \geq 2|\mathrm{Gal}(L/K)| = 2[L : K].$$

By Proposition 2.2,

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2[L : K] \leq |\mathrm{Aut}(L/\mathbb{Q})|,$$

and, by Proposition 2.17,

$$|\mathrm{Aut}(L/\mathbb{Q})| \leq [L : \mathbb{Q}],$$

thus, $|\mathrm{Aut}(L/\mathbb{Q})| = [L : \mathbb{Q}]$, i.e., the extension $L/\mathbb{Q}$ is Galois. □

Remark 4.26. The converse of Proposition 4.25 also holds, according to Cox, Chapter 2, §5, Exercise 5.19(a),[1] but we leave out the proof of this fact.

4.2 The Hilbert Class Field

In this section we will state the existence and uniqueness of the Hilbert class field of a number field (Theorem 4.29), which is stated as Theorem 5.18 in Cox, Chapter 2, §5(C) and proved in Chapter 2, §8(A).[1] In order to define the Hilbert class field, we need a few more definitions, namely, Definitions 4.27 and 4.28 below, which are both stated in Cox, Chapter 2, §5(C).

Definition 4.27. Let K, L be number fields such that $K \subset L$. The extension $K \subset L$ is called *abelian* if it is Galois and the Galois group $\mathrm{Gal}(L/K)$ is abelian.

Definition 4.28. Let K be a number field. A nonzero prime ideal of $\mathcal{O}_K$ is called a *finite prime of* K. An embedding $K \to \mathbb{R}$ is called a *real infinite prime of* K and a pair of embeddings $K \to \mathbb{C}$, where the embedding are complex conjugates of each other, is called a *complex infinite prime of* K. Let L be extension of K. We say that an infinite prime σ of K *ramifies in* L if it is real and can be extended to a complex infinite prime of L. We say that the extension $K \subset L$ is *unramified* if no infinite nor finite primes of K ramify in L.

The following proposition states the existence and uniqueness of the Hilbert class field, and is stated as Theorem 5.18 in Cox, Chapter 2, §5(C), and proved i $x8(A)$.[1]

Theorem 4.29. Let K be any number field. Then there exists a finite extension L of K, such that L is an unramified and abelian extension of K, and $M \subset L$ whenever M is an unramified abelian extension of K, that is, L is the maximal everywhere unramified abelian extension of K.

Proof. This theorem is proved in Cox, Chapter 2, §8(A) (see Theorem 8.10 of this section).[1] □

Definition 4.30. The field L of Theorem 4.29 is called the *Hilbert class field of* K.

The following proposition states the existence and uniqueness of the Artin symbol, and is stated as Lemma 5.19 in Cox, Chapter 2, §5(C).[1]

Proposition 4.31. Let K be any number field, and let L/K be a Galois extension. If a prime P of K is unramified in L and Q is a prime of L containing P, then there is a unique $\sigma \in \mathrm{Gal}(L/K)$ such that

$$\sigma\alpha \equiv \alpha^{|\mathcal{O}_K/P|} \pmod{Q},$$

i.e., $\sigma\alpha$ and $\alpha^{|\mathcal{O}_K/P|}$ belong to the same coset in $\mathcal{O}_K/P$, for all $\alpha \in \mathcal{O}_K$.

Proof. See Cox, Chapter 2, §5(C), Lemma 5.19.[1] □

Definition 4.32. The element σ of Proposition 4.31 is called the *Artin symbol* and is denoted

$$\left(\frac{L/K}{Q}\right).$$

This symbol depends on Q (and the fields K and L), since $P = K \cap Q$.

Remark 4.33. If L/K is an abelian extension, that is, $\mathrm{Gal}(L/K)$ is abelian, then the Artin symbol depends only on P, as explained in Cox, Chapter 2, §5(C),[1] thus, in this case, we can write

$$\left(\frac{L/K}{P}\right) := \left(\frac{L/K}{Q}\right)$$

If $\mathrm{Gal}(L/K)$ is abelian, the Artin symbol can also be extended to fractional ideals of K in the following way.

Definition 4.34. Given a fractional ideal F of a number field K with prime factorization (according to Proposition 4.18)

$$F = P_1^{n_1} \cdots P_r^{n_r},$$

where $r \in \mathbb{Z}_{\geq 1}$, $n_1, \cdots, n_r \in \mathbb{Z}$, and $P_1, \cdots, P_r$ being prime ideals of K, and an unramified abelian extension L of K, we can define the *Artin symbol* to be

$$\left(\frac{L/K}{F}\right) := \prod_{i=1}^{r} \left(\frac{L/K}{P_i}\right)^{n_i}.$$

Definition 4.35. Let K be any number field, and let L/K be an unramified abelian extension. Then, the map

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$$

is called the *Artin map.* This map is a homomorphism, since $\mathrm{Gal}(L/K)$ is abelian.

The following theorem relates the ideal class group (see Definition 4.13) to the Hilbert class field and is stated as Theorem 5.23 in Cox, Chapter 2, §5(C).[1]

Theorem 4.36. (The Artin Reciprocity Theorem for the Hilbert Class Field) Let K be a number field and let L be its Hilbert class field. Then the Artin map $\left(\frac{L/K}{\cdot}\right)$ is surjective with kernel P_K (see Definition 4.11), thus, by the First Isomorphism Theorem for Groups (see Dummit and Foote, Chapter 3, Section 3.3, Theorem 16[2]),

$$\mathcal{C}(\mathcal{O}_K) = I_K/P_K \cong \mathrm{Gal}(L/K).$$

Proof. See Cox, Chapter 2, §8(A), (8.9).[1] □

4.3 The form class group and its relation to the ideal class group

In this section we will discuss some results from the theory of quadratic forms. In the end of this section, we will define the form class group and explain how it relates to the ideal class group. In the next section we will see that this result is of high importance for the problem of applying the Hilbert class field to primes of the form $x^2 + ny^2$. Most of this section is based on Cox, Chapter 1, §2(A),[1] where, if not stated otherwise, the definitions, propositions and theorems of this section are to be found.

Definition 4.37. Given a quadratic form $f(x, y) = ax^2 + bxy + cy^2,\ a, b, c \in \mathbb{Z}$, in the two variables x and y, we say that $m \in \mathbb{Z}$ is *represented by* f (or that f *represents* m) if $m = f(x, y)$ for some nonzero $(x, y) \in \mathbb{Z}^2$. Furthermore, if $m = f(x, y)$ where x and y are relatively prime, we say that m is *properly represented by* f. We say that f is *positive definite* if it represents only positive integers and *negative definite* if it represents only negative integers. If f represents both positive and negative integers, then we say that f is *indefinite*. The quadratic form f is called *primitive* if a, b, c are all relatively prime. Throughout this section, all quadratic forms will be assumed to be primitive, even if not stated.

Definition 4.38. Given a primitive quadratic form $ax^2 + bxy + cy^2,\ a, b, c \in \mathbb{Z}$, in the two variables x and y, the *discriminant* D *of* $ax^2 + bxy + cy^2$ is defined to be the integer

$$D = b^2 - 4ac.$$

Proposition 4.39. Given a primitive quadratic form $f(x, y) = ax^2 + bxy + cy^2,\ a, b, c \in \mathbb{Z}$ with discriminant D, it holds that $D < 0$ if and only if f is positive or negative definite. Furthermore, if $D < 0$, then f is positive definite if and only if $a > 0$, and negative definite if and only if $a < 0$.

Proof. This proposition is stated in Cox, Chapter 1, §2(A) without a proof and as Exercise 2.4(b).[1] Suppose that $D < 0$. Then either $a > 0$ or $a < 0$, because $a = 0$ implies that $D = b^2 \geq 0$, which is a contradiction. Since

$$4af(x, y) = 4a^2x^2 + 4abxy + 4acy^2 = 4a^2x^2 + 4abxy + 4acy^2 + b^2y^2 - b^2y^2 =$$
$$4a^2x^2 + 4abxy + b^2y^2 - (b^2 - 4ac)y^2 = (2ax + by)^2 - Dy^2,$$

it follows that, if $D < 0$, then, for every nonzero $(x, y) \in \mathbb{Z}^2$, $4af(x, y) > 0$, thus f is positive definite whenever $a > 0$ and negative definite whenever $a < 0$.

Conversely, suppose that f is either positive or negative definite, then $a \neq 0$, because $a = 0$ implies that $f(x, y) = bxy + cy^2$, which is indefinite, since the sign of $f(\pm 2c, 1) = c(\pm 2b + 1)$ depends on the sign $\pm$. Analogously, it also holds that $c \neq 0$. It follows that $4af(x, y)$ is either positive or negative definite. It must be the case that a and c have the same sign, because otherwise $ac < 0$, which in turn implies that $4af(x, y)$ is negative for $x = 0$ and some y large enough, and positive for $y = 0$ and some x large enough, thus, indefinite. If $D \geq 0$, then b must be nonzero (since D is negative otherwise), thus

$$4af(-2c, b) = (-4ac + b^2)^2 - Db^2 = D^2 - Db^2 = D(D - b^2) = -4Dac \leq 0$$

and

$$4af(-2c, 0) = (-4ac)^2 > 0,$$

contradicting that $4af(x, y)$ is positive or negative definite. It follows that $D < 0$. □

Definition 4.40. Two primitive quadratic forms f and g in the two variables x and y are said to be *equivalent* if $f(x, y) = g(ax + by, cx + dy)$ for some $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = \pm 1$. If $ad - bc = 1$, then f and g are said to be *properly equivalent.*

Proposition 4.41. Proper equivalence between quadratic forms in the two variables x and y is an equivalence relation.

Proof. This proposition is stated in Cox, Chapter 1, §2(A) without a proof and as part of Exercise 2.2(a).[1] Let f, g, and h be quadratic forms in the two variables x and y. By putting $a = d = 1$ and $b = c = 0$, we see that

$$ad - bc = 1 - 0 = 1,$$

and,

$$g(x, y) = g(ax + by, cx + dy)$$

which shows that g is properly equivalent to itself, that is, proper equivalence is a reflexive relation. If $f(x, y) = g(ax + by, cx + dy)$ for some $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$, then, $g(x, y) = f(px + qy, rx + sy)$ holds for some $p, q, r, s \in \mathbb{Z}$ if and only if

$$g(x, y) = g(apx + aqy + brx + bsy, cpx + cqy + drx + dsy) =$$

$$g((ap + br)x + (aq + bs)y, (cp + dr)x + (cq + ds)y).$$

Since $ad - bc = 1$, putting $p = d,\ r = -c,\ q = -b$, and $s = a$ gives us that

$$ps - qr = ad - bc = 1,$$

$$ap + br = cq + ds = ad - bc = 1,$$

$$aq + bs = -ab + ab = 0$$

$$cp + dr = cd - cd = 0,$$

thus, we can write $g(x, y) = f(dx - by, -cx + ay)$, which shows that proper equivalence is a symmetric relation. If $f(x, y) = g(ax + by, cx + dy)$ for some $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$, and $g(x, y) = h(a'x + b'y, c'x + d'y)$ for some $a', b', c', d' \in \mathbb{Z}$ such that $a'd' - b'c' = 1$, then

$$f(x, y) = h(a'(ax + by) + b'(cx + dy), c'(ax + by) + d'(cx + dy)) =$$

$$h(a'ax + a'by + b'cx + b'dy, c'ax + c'by + d'cx + d'dy) =$$

$$h((a'a + b'c)x + (a'b + b'd)y, (c'a + d'c)x + (c'b + d'd)y).$$

Since

$$(a'a + b'c)(c'b + d'd) - (a'b + b'd)(c'a + d'c) =$$

$$a'c'ab + a'd'ad + b'c'bc + b'd'cd - a'c'ab - a'd'bc - b'c'ad - b'd'cd =$$

$$a'd'ad + b'c'bc - a'd'bc - b'c'ad = (a'd' - b'c')(ad - bc) = 1 \cdot 1 = 1,$$

hence, the proper equivalence relation is transitive. □

Proposition 4.42. Let $f(x, y)$ be a quadratic form (with integer coefiicients). Then $a \in \mathbb{Z}$ is properly represented by f if and only if f is properly equivalent to $ax^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$.

Proof. This proposition is proved in Cox, Chapter 1, §2(A), Lemma 2.3,[1] using that $ps - qr = 1$ for some $r, s \in \mathbb{Z}$ if and only if $p, q \in Z$ are relatively prime. Assuming that $a = f(p, q)$ where p and q are relatively prime, one can construct the quadratic form $f(px + ry, qx + sy)$ which is properly equivalent to f with the coefficient of the x^2-term being $a = f(p, q)$. In order to prove the converse, one can assume that $f(px + ry, qx + sy)$ has a as the coefficient of the x^2-term and that $ps - qr = 1$, and put $(x, y) = (1, 0)$. □

Proposition 4.43. If f and g are equivalent quadratic forms in the two variables x and y, then they have the same discriminant.

Proof. This is proved in less detail in Cox, Chapter 1, §2(A).[1] Let $f = ax^2 + bxy + cy^2$, and let $g(x, y) = f(px + qy, rx + sy)$, where $p, q, r, s \in \mathbb{Z}$ such that $ps - qr = \pm 1$. Let $D = b^2 - 4ac$ be the discriminant of f. Then

$$g(x,y) = a(px+qy)^2 + b(px+qy)(rx+sy) + c(rx+sy)^2 =$$
$$ap^2x^2 + 2apqxy + aq^2y^2 + bprx^2 + bpsxy + bqrxy + bqsy^2 + cr^2x^2 + 2crsxy + cs^2y^2 =$$
$$(ap^2 + bpr + cr^2)x^2 + (2apq + bps + bqr + 2crs)xy + (aq^2 + bqs + cs^2)y^2$$

has discriminant

$$(2apq + bps + bqr + 2crs)^2 - 4(ap^2 + bpr + cr^2)(aq^2 + bqs + cs^2) =$$
$$4a^2p^2q^2 + 4abpq^2r + b^2q^2r^2 + 4abp^2qs + 2b^2pqrs + 8acpqrs + 4bcqr^2s +$$
$$b^2p^2s^2 + 4bcprs^2 + 4c^2r^2s^2 - 4a^2p^2q^2 - 4abpq^2r - 4acq^2r^2 -$$
$$4abp^2qs - 4b^2pqrs - 4bcqr^2s - 4acp^2s^2 - 4bcprs^2 - 4c^2r^2s^2 =$$
$$b^2q^2r^2 - 4acq^2r^2 - 2b^2pqrs + 8acpqrs + b^2p^2s^2 - 4acp^2s^2 =$$
$$b^2q^2r^2 + (D - b^2)q^2r^2 - 2b^2pqrs - 2(D - b^2)pqrs + b^2p^2s^2 + (D - b^2)p^2s^2 =$$
$$D(q^2r^2 - 2pqrs + p^2s^2) + b^2 \underbrace{(q^2r^2 - q^2r^2 - 2pqrs + 2pqrs + p^2s^2 - p^2s^2)}_{=0} =$$
$$D(ps - qr)^2 = D \cdot 1 = D$$

□

Definition 4.44. A positive definite quadratic form $ax^2 + bxy + cy^2,\ a, b, c \in \mathbb{Z}$, in the two variables x and y, is called *reduced* if

(i) $|b| \leq a \leq c$, and

(ii) $b \geq 0$ whenever $|b| = a$ or $a = c$

Theorem 4.45. For every primitive positive definite quadratic form $f(x, y)$ in the two variables x and y, there exists a unique reduced quadratic form $g(x, y)$ such that f and g are properly equivalent.

Proof. See Cox, Chapter 1, §2(A), Theorem 2.8.[1] □

The following definition is according to Cox, Chapter 1, §2(A) and §3(A).[1]

Definition 4.46. Let $D < 0$ be an integer. We denote by $\mathcal{C}(D)$ the set of primitive positive definite reduced quadratic forms of discriminant D. This set is called the *(form) class group of D* since it consists of the equivalence classes under proper equivalence of primitive quadratic forms and it forms an abelian group under Dirichlet composition (defined by Dirichlet in *Zahlentheori,* inspired by the work of Legendre), as shown in Cox, Chapter 1, §3(A), Theorem 3.9, as well as under composition, as was shown by Gauss in *Disquisitiones Arithmetica*, according to Cox.[1] We denote by $h(D)$ the order of $\mathcal{C}(D)$, i.e., (by Theorem 4.45) the number of primitive positive definite reduced quadratic forms of discriminant D. This number is called the *class number of D*.

Theorem 4.47. Let $D < 0$ be an integer. Then $h(D)$ is finite

Proof. This theorem is proved in Cox, Chapter 1, §2(A), Theorem 2.13,[1] by showing that for a primitive positive definite reduced quadratic form $ax^2 + bxy + cy^2$, the coefficients a and b can be chosen in only a finite number of ways (and the same goes for c, which, for any fixed D, is determined by a and b, since $D = b^2 - 4ac$). This follows from the fact that $b^2 \leq a^2$ and $|b| \leq a \leq c$ (since $ax^2 + bxy + cy^2$ is reduced), since

$$-D = 4ac - b^2 \geq 4a^2 - b^2 \geq 3a^2$$

implies that

$$a \leq \sqrt{-D/3},$$

which is a finite positive number. □

The following theorem, stated as Theorem 5.30 in Cox, Chapter 2, §5(D),[1] gives us the relationship between the form class group and the ideal class group (see Definition 4.13).

Theorem 4.48. Let K be any imaginary quadratic field and let D_K be the discriminant of K (see Definition 4.21). Then,

(i) for any primitive positive definite quadratic form $ax^2 + bxy + cy^2,\ a, b, c \in \mathbb{Z}$, in the two variables x and y, the set
$$I_{a,b,c} := \{ma + n(-b + \sqrt{D_K})/2 \mid m, n \in \mathbb{Z}\}$$
is an ideal of $\mathcal{O}_K$, and

(ii) the map $\mathcal{C}(D_K) \to \mathcal{C}(O_K),\ ax^2 + bxy + cy^2 \mapsto I_{a,b,c}$, between the form class group $\mathcal{C}(D_K)$ of D_K and the ideal class group $\mathcal{C}(O_K)$ of O_K is an isomorphism.

(Note that, by Proposition 4.22, since K is an imaginary quadratic field, it holds that $D_K < 0$.)

Proof. See Cox, Chapter 2, §7(B), Theorem 7.7,[1] which is a more general theorem, stating that (i) and (ii) hold for orders in a quadratic field (see Definition 5.1), which include the ring of integers. In Cox, Chapter 2, §7(A),[1] the notions of discriminant and the ideal class group is extended to orders of a number field. □

4.4 Theorem for primes of the form $x^2 + ny^2$, where $n \not\equiv 3 \pmod 4$, n squarefree

The main theorem of this thesis, Theorem 4.49 below, gives us a necessary and sufficient condition for a prime p to be of the form $x^2 + ny^2$, for $n \in \mathbb{Z}_{\geq 1}$ satisfying that n is squarefree and $n \not\equiv 3 \pmod 4$. Note that the latter implies that $-n \not\equiv 1 \pmod 4$, hence, by Proposition 4.23, the ring of integers in $\mathbb{Q}(\sqrt{-n})$ is $\mathbb{Z}[\sqrt{-n}]$. If we know the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$, them, we can easily apply this theorem. Although it holds for an infinite number of n's, there is no general method for computing the Hilbert class field.

Theorem 4.49. Let n be a positive integer satisfying that n is squarefree and $n \not\equiv 3 \pmod 4$, and let $p \in \mathbb{Z}$ be a prime such that $p \nmid n$ and $p \neq 2$. Let $K = \mathbb{Q}(\sqrt{-n})$ and let $\alpha \in R$ be a real algebraic number such that $L = K(\alpha)$ is the Hilbert class field of K. Then, there exists a monic irreducible $f \in \mathbb{Z}[x]$ of degree $h(-4n)$, which is the minimal polynomial of α, such that, provided that p does not divide the discriminant of f,
$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and } f(z) \equiv 0 \pmod p \\ \text{has a solution in } \mathbb{Z} \end{cases}$$

The proof of this theorem is given in Cox, Chapter 2, §5(D), Proof of Theorem 5.1.[1] Cox uses the following lemmas.

Lemma 4.50. If K is an imaginary quadratic field and L is the Hilbert class field of K. Then the extension $L/\mathbb{Q}$ is Galois.

Proof. This proof is given in Cox, Chapter 2, §5(D), Lemma 5.28.[1] The idea is to use that $K = \tau(K) \subset \tau(L)$ (where τ denotes complex conjugation) is an unramified abelian extension of degree $[\tau(L) : \tau(K)] = [L : K]$, and that L is the maximal unramified abelian extension of K. It follows that $L = \tau(L)$, hence, by Proposition 4.25, the extension $L/\mathbb{Q}$ is Galois.[1] □

Lemma 4.51. If $K = \mathbb{Q}(\sqrt{-n})$, where $n \in \mathbb{Z}$ is squarefree and $n \not\equiv 3 \pmod 4$, L is the Hilbert class field of K, and $p \in \mathbb{Z}$ is a prime such that $p \nmid n$ and $p \neq 2$, then
$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \iff p\mathcal{O}_K \text{ splits completely in } L.$$

Proof. See Cox, Chapter 2, §5(D), Theorem 5.26.[1] □

Lemma 4.52. If K is an imaginary quadratic field and L is a number field containing K such that $L/\mathbb{Q}$ is a Galois extension, then,

(i) there is a real algebraic integer α such that $L = K(\alpha)$, and

(ii) if $f \in \mathbb{Z}[x]$ is the minimal polynomial of α over $\mathbb{Q}$ and D_f is the discriminant of f, then, for any prime $p \in \mathbb{Z}$ such that $p \nmid D_f$,

$$p\mathcal{O}_K \text{ splits completely in } L \iff \begin{cases} \left(\frac{D_K}{p}\right) = 1 \text{ and } f(z) \equiv 0 \pmod{p} \\ \text{has a solution in } \mathbb{Z}, \end{cases}$$

where D_K denotes the discriminant of K.

Proof. See Cox, Chapter 2, §5(D), Proposition 5.29.[1] □

Proof of Theorem 4.49. The proof is given in Cox, Chapter 2, §5(D),[1] using the three lemmas above and Theorems 4.36 and 4.48. The idea of the proof is as follows. If L is the Hilbert class field of K, then, by Lemma 4.50, the extension $L/\mathbb{Q}$ is Galois, thus, by combining Lemmas 4.51 and 4.52, we have that $L = K(\alpha)$ for some real algebraic integer α. If we let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Q}$ and D_f the discriminant of f, then, for any prime $p \in \mathbb{Z}$ such that $p \nmid D_f$ and $p \nmid n$,

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} \left(\frac{D_K}{p}\right) = 1 \text{ and } f(z) \equiv 0 \pmod{p} \\ \text{has a solution in } \mathbb{Z} \end{cases}.$$

By Proposition 4.22, we have that $D_K = -4n$, since $-n \neq 1 \pmod 4$. It follows that

$$\left(\frac{D_K}{p}\right) = \left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right).$$

By the Artin Reciprocity Theorem for the Hilbert Class Field (Theorem 4.36) and Theorem 4.48,

$$[L : K] = |\mathrm{Gal}(L/K)| = |\mathcal{C}(O_K)| = |\mathcal{C}(D_K)| = h(D_k) = h(-4n).$$ □

4.5 The case $n = 14$

The case $n = 14$ is considered in Cox, Chapter 2, §5(D), and the way the Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-14})$ is applied is explained below.[1] The integer $14 = 2 \cdot 7$ is squarefree and not congruent to 3 modulo 4, hence, by Theorem 4.49, there is a polynomial $f \in \mathbb{Z}[x]$ of degree $h(-4 \cdot 14) = h(-56)$ and is the minimal polynomial of some real algebraic number α such that $L = K(\alpha)$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ given a prime $p \in \mathbb{Z}$ such that $p \neq 2, 7, D_f$ (where D_f denotes the discriminant of f),

$$p = x^2 + 14y^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} \left(\frac{-14}{p}\right) = 1 \text{ and } f(x) \equiv 0 \pmod{p} \\ \text{has a solution in } \mathbb{Z}, \end{cases}$$

It is stated in Cox, Chapter 2, §5(D), Proposition 5.31, that (one such) α is given by $\alpha = \sqrt{2\sqrt{2} - 1}$.[1] We can show that $L = K(\sqrt{2\sqrt{2} - 1})$ is the Hilbert class field of K by showing that it is the maximal unramified abelian extension of K. By Cox, Chapter 1, §2(A), (2.14), the reduced quadratic forms in two variables of discriminant -56 are $x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 + 2xy + 5y^2$, and $3x^2 - 2xy + 5y^2$, thus $h(-56) = 4$.[1] We can determine a basis B for L over K by computing powers of $\alpha = \sqrt{2\sqrt{2} - 1}$ (we assume that $1 \in B$):

$$\left(\sqrt{2\sqrt{2} - 1}\right)^1 = \sqrt{2\sqrt{2} - 1},$$

$$\left(\sqrt{2\sqrt{2} - 1}\right)^2 = 2\sqrt{2} - 1,$$

$$\left(\sqrt{2\sqrt{2} - 1}\right)^3 = \left(\sqrt{2\sqrt{2} - 1}\right)^2 \sqrt{2\sqrt{2} - 1} = (2\sqrt{2} - 1)\sqrt{2\sqrt{2} - 1} = 2\sqrt{2}\sqrt{2\sqrt{2} - 1} - \sqrt{2\sqrt{2} - 1}.$$

We see that

$$B = \left\{1, \sqrt{2\sqrt{2} - 1}, \sqrt{2}, \sqrt{2}\sqrt{2\sqrt{2} - 1}\right\}$$

is a basis for L over K. (Note that $\alpha^4 = (2\sqrt{2}-1)^2 = 9 - 4\sqrt{2}$ is a linear combination over K of two other basis elements.) This shows that L has degree 4 over K. Therefore, if L is an unramified abelian extension of K, then, it is the maximal such extension. In Cox, Chapter 2, §5(D), it is shown that this extension is unramified.[1] Since, according to Cox,[1] the minimal polynomial of α is $x^4 + 2x^2 - 7 = (x^2+1)^2 - 8$, we can use Exercise 13(b)(iii) of Dummit and Foote, Chapter 14, Section 14.6,[2] which states that the Galois group of the polynomial $x^4 + ax^2 + b,\ a, b \in \mathbb{Z}$, (which is separable, since it has the four distinct roots $\pm\sqrt{\pm 2\sqrt{2}-1}$) has Galois group isomorphic to D_8, the dihedral group of order 8 (see Dummit and Foote, Chapter 1, Section 1.2[2]) if and only if b and $b(a^2-4b)$ are not squares in $\mathbb{Q}$. In this case $a = 2$ and $b = -7$, which is a non-square in $\mathbb{Q}$, hence,

$$b(a^2 - 4b) = -7(4 + 28) = -7 \cdot 32,$$

which is also a non-square in $\mathbb{Q}$. By Definition 2.19 it follows that the Galois group of the splitting field of $x^4 + 2x^2 - 7$, which must contain $K(\alpha)$, is isomorphic to D_8. Since D_8 has three subgroups of index 2 (see Dummit and Foote, Chapter 2, Section 2.5, Example 4, for the subgroup structure of D_8[2]), the splitting field of $x^4 + 2x^2 - 7$ contains three subfields of degree 2 over $\mathbb{Q}$, by Theorem 2.21 (the Fundamental Theorem of Galois Theory). These quadratic subfields of the splitting field are $K = \mathbb{Q}(\sqrt{-14})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-7})$. Note that D_8 has order $8 = [K : \mathbb{Q}] \cdot [L : K]$, hence, by Proposition 2.2, L is the splitting field of $x^4 + 2x^2 - 7$. An element of $\mathrm{Gal}(L/\mathbb{Q})$ order 4 (two such elements exist in D_8, with one being the inverse of the other, as seen in Dummit and Foote, Chapter 14, Section 14.6[2]) must necessarily map the root $\sqrt{2\sqrt{2}-1}$ to one of $\pm\sqrt{-2\sqrt{2}-1}$, which in turn must be mapped to $-\sqrt{2\sqrt{2}-1}$, since, otherwise, it would have order 2 or 1. It follows that an element of $\mathrm{Gal}(L/\mathbb{Q})$ order 4 does not fix $\mathbb{Q}(\sqrt{2})$ nor $\mathbb{Q}(\sqrt{-7})$, since it maps

$$\sqrt{2} = \left(\left(\sqrt{2\sqrt{2}-1}\right)^2 + 1\right)/2$$

to

$$\left(\left(\pm\sqrt{-2\sqrt{2}-1}\right)^2 + 1\right)/2 = -\sqrt{2},$$

and

$$\sqrt{-7} = \sqrt{-8+1} = \left(\sqrt{2\sqrt{2}-1}\right)\left(\sqrt{-2\sqrt{2}-1}\right)$$

to

$$\left(\pm\sqrt{-2\sqrt{2}-1}\right)\left(\mp\sqrt{2\sqrt{2}-1}\right) = -\sqrt{-8+1} = -\sqrt{-7}.$$

We can conclude that the cyclic subgroup of D_8 of order 4 is isomorphic to $\mathrm{Gal}(L/K)$, thus, the extension L/K is abelian (since cyclic groups are abelian). According to Cox,[1] the polynomial $x^4 + 2x^2 - 7 = (x^2+1)^2 - 8$ has discriminant $-2^{14} \cdot 7$ (which has no other prime factors than 2 and 7), hence, we have the following theorem for the case $n = 14$.

Theorem 4.53. Let $p \in \mathbb{Z}$ such that $p \neq 2, 7$. Then

$$p = x^2 + 14y^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} \left(\frac{-14}{p}\right) = 1 \text{ and } (x^2+1)^2 \equiv 8 \pmod{p} \\ \text{has a solution in } \mathbb{Z}. \end{cases}$$

5 General n and the ring class field

In this section we will briefly look at the theory of the ring class field and state how it relates to the problem of primes of the form $x^2 + ny^2$. In this Sections, all proofs are omitted. For details, we refer to Cox, Chapter 2, §7–9.[1]

5.1 The ring class field

Definitions and Propositions 5.1–5.10 below are stated in Cox, Chapter 2, §7(A).[1]

Definition 5.1. A subset $\mathcal{O}$ of a quadratic field K is called an *order in* K if

(i) $\mathcal{O}$ is a ring containing 1

(ii) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module, i.e., there exists a finite subset $\{\alpha_1, \cdots, \alpha_r\}$ $(r \in \mathbb{Z}_{\geq 1})$ of $\mathcal{O}$ such that $\mathcal{O} = \{z_1\alpha_1 + \cdots + z_r\alpha_r \mid z_1, \cdots, z_r \in \mathbb{Z}\}$

(iii) $\mathcal{O}$ contains a $\mathbb{Q}$-basis for K, i.e., there exists a finite subset $\{\beta_1, \cdots, \beta_s\}$ $(s \in \mathbb{Z}_{\geq 1})$ of $\mathcal{O}$ such that every element in K can be written as a linear combination $q_1\beta_1 + \cdots + q_s\beta_s$, where $q_1, \cdots, q_s \in \mathbb{Q}$.

Proposition 5.2. Let K be a quadratic field and let $\mathcal{O} \subset K$ be an order in K. Then $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2.

Proposition 5.3. Let K be a quadratic field and let $\mathcal{O} \subset K$ be an order in K. Then K is the field of fractions of O.

Proposition 5.4. Let K be a quadratic field. Then $\mathcal{O}_K$ is an order in K, and $\mathcal{O} \subset \mathcal{O}_K$, for every order $\mathcal{O}$ in K, that is, $\mathcal{O}_K$ is the maximal order in K

As in the case of $\mathcal{O}_K$ (or any Dedekind domain), the notion of a fractional ideal can be extended, in accordance with Cox, Chapter 2, §7(A),[1] to an arbitrary order in K in the following way.

Definition 5.5. Let K be a quadratic field and let $\mathcal{O} \subset K$ be an order in K. Although $\mathcal{O}$ need not be a Dedekind domain, we can still define the notion of a fractional ideal of $\mathcal{O}$ in a similar way. We call a subset of $\mathcal{O}$ a *fractional ideal of* $\mathcal{O}$ if it is of the form αI, where I is an ideal of $\mathcal{O}$ and $\alpha \in K \setminus \{0\}$. (This definition is stated as one of two equivalent versions given in Cox, Chapter 2, §7(A)[1]) An ideal I of $\mathcal{O}$ is called *proper* if

$$\mathcal{O} = \{\alpha \in K \mid \alpha I \subset I\}.$$

Similarly, a fractional ideal J of $\mathcal{O}$ is called *proper* if

$$\mathcal{O} = \{\beta \in K \mid \beta J \subset J\}.$$

A fractional ideal of $\mathcal{O}$ is called *principal* if it is of the form $\beta\mathcal{O}$, where $\beta \in K \setminus \{0\}$.

Definition 5.6. Let K be a quadratic field and let $\mathcal{O} \subset K$ be an order in K. We denote by $I(\mathcal{O})$ the set of proper fractional ideals in $\mathcal{O}$, and by $P(\mathcal{O})$ the set of principal fractional ideals in $\mathcal{O}$.

Proposition 5.7. Let K be a quadratic field and let $\mathcal{O} \subset K$ be an order in K. Then a fractional ideal of $\mathcal{O}$ is proper if and only if it is invertible.

Remark 5.8. Every principal fractional ideal $\alpha\mathcal{O}$ of $\mathcal{O}$ is invertible, with inverse $\alpha^{-1}\mathcal{O}$. By Proposition 5.9, it follows that $P(\mathcal{O}) \subset I(\mathcal{O})$.

Proposition 5.9. Let K be a quadratic field and let $\mathcal{O} \subset K$ be an order in K. Then $I(\mathcal{O})$ is a group and $P(\mathcal{O})$ is a subgroup.

Definition 5.10. Given a quadratic field K and an order $\mathcal{O}$ in K, the quotient group $I(\mathcal{O})/P(\mathcal{O})$ is called the *ideal class group of* $\mathcal{O}$, and is denoted $\mathcal{C}(\mathcal{O})$. Furthermore, if $\mathcal{O} = \mathcal{O}_K$, then, this definition agrees with Definition 4.13.

Definitions 5.11–5.12 below are stated in Cox, Chapter 2, §8(A), as is Theorem 5.13.[1] Definition

Definition 5.11. Let K be a number field. A *modulus of* K is a product

$$M \;:=\; \prod_{P \text{ prime of } K} P^{n_P}.$$

such that

- $n_P \geq 0$ for all P, and only finitely many n_P's are nonzero,
- if P is a complex infinite prime, then $n_P =$, and
- if P is a real infinite prime, then $n_P = 0$ or $n_P = 1$.

Definition 5.12. Let K be a number field and let M be a modulus of K. By $I_K(M)$, we denote the subgroup of the I_K (see Definition 4.11) which are relatively prime to M, and by $P_{K,1}(M)$ the subgroup of $I_K(M)$ generated by P_K. A subgroup H of $I_K(M)$ satisfying that

$$P_{K,1} \subset H \subset I_K(M)$$

is called a *congruence subgroup for M*

The following theorem states the existence of the ring class field, and it is stated without a proof (giving a reference to the book *Algebraic Number Fields* by G. Janusz) as Theorem 8.6 i n Cox, Chapter 2, §8(A).[1] Definition 5.14 is according to Cox, Chapter 2, §9(A).[1]

Theorem 5.13. Let K be a number field, let M be a modulus of K, and let H be a congruent subgroup for M. Then there exists a unique abelian extension L/K satisfying that all primes in K that ramify in L divide M, and H is the kernel or the artin map of K/L restricted to $I_K(M)$.

Definition 5.14. The field L of Theorem 5.13 is called the *ring class field of K*

5.2 Theorem for primes of the form $x^2 + ny^2$ for general n

The following theorem is a generalization of Theorem 4.49, and is stated as Theorem 9.2 in Cox, Chapter 2, §9(A).[1]

Theorem 5.15. Let n be any positive integer and let $p \in \mathbb{Z}$ be a prime such that $p \nmid n$ and $p \neq 2$. Let $K = \mathbb{Q}(\sqrt{-n})$ and let $\alpha \in R$ be a real algebraic number such that $L = K(\alpha)$ is the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ of K. Then, there exists a monic irreducible $f \in \mathbb{Z}[x]$ of degree $h(-4n)$, which is the minimal polynomial of α, such that, for a prime $p \in \mathbb{Z}$ not dividing 2 nor the order of f

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and } f(z) \equiv 0 \pmod{p} \\ \text{has a solution in } \mathbb{Z} \end{cases}$$

Proof. See Cox, Chapter 2, §9(A).[1] □

Remark 5.16. In Cox, Chapter 2, §5(B),[1] the Theorem 5.15 is applied to the orders $\mathbb{Z}[\sqrt{-27}]$ and $\mathbb{Z}[\sqrt{-64}]$ of $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-1})$ respectively. This way, Cox provides alternative proofs of Theorems 3.1 and 3.2.[1]

References

[1] Cox, D. A. (1997). *Primes of the Form $x^2 + ny^2$*. Hoboken, New Jersey: John Wiley & Sons, Inc.

[2] Dummit, D. S., Foote, R. M. (2004). *Abstract Algebra.* 3rd ed. Hoboken, New Jersey: John Wiley & Sons, Inc.

[3] Ireland, K., Rosen, M. (2010). *A Classical Introduction to Modern Number Theory.* 2nd ed. New York, New York: Springer-Verlag.

[4] Marcus, D. A. (2018). *Number Fields.* 2nd ed. Cham, Switzerland: Springer International Publishing AG.

[5] Samuel, P. (1971). *Algebraic Theory of Numbers.* Translated from French by A. J. Silberger. London, England: Kershaw Publishing Company LTD, pp.27–28.