UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SEDE DI BRESCIA

FACOLTÀ DI SCIENZE MATEMATICHE,
FISICHE E NATURALI

TESI DI LAUREA TRIENNALE IN MATEMATICA

FACTORIZATION PROBLEMS FOR QUADRATIC ALGEBRAIC INTEGERS

Relatore:
Prof.ssa MARIA CLARA TAMBURINI

Correlatore:
Prof. MAXIM VSEMIRNOV

Laureando:
LATTARINI STEFANO
Matricola n. 3103859

ANNO ACCADEMICO 2006/2007

Contents

Introduction **5**

0.1 Prerequisites 5

0.2 Background, scope and goals of this work 5

0.3 Overview of results 6

0.4 Thanks 7

1 Preliminary results **9**

1.1 The concepts of conjugate and norm 9

1.2 Normed Domains 10

1.3 Some notations 12

1.4 Useful results in number theory 13

1.5 Some subrings of $\mathbb{C}$ 16

2 Some UFDs of algebraic integers **19**

2.1 Unique factorization in the ring of Gaussian integers 19

2.2 Exstensions to a class of normed domains 22

2.3 Equivalent forms for our results 25

2.4 Some concrete applications 28

3 Some non-UFDs of algebraic integers **39**

3.1 Some normed complex domains that are not an UFD 39

3.2 Some normed real domains that are not UFD 45

3.3 Deeper results for real domains 47

3.4 More general results for $\mathbb{Z}[\sqrt{m}]$ 51

4 Limits of our methods **55**

4.1 Equivalence between property (1) and property (4) 55

4.2 Complex domains that are not norm-euclidean 57

4.3 Real domains that are not norm-euclidean 58
4.3.1 Introduction 58
4.3.2 Not norm-euclidean $h(\sqrt{m})$ for $m \equiv 2$ or $3 \pmod 4$ 58
4.3.3 Non norm-euclidean $h(\sqrt{m})$ for $m \equiv 1 \pmod 4$ 67

Bibliography **79**

Introduction

0.1 Prerequisites

In this work, we'll assume that the reader has a good knowledge of undergraduate algebra and of elementary number theory, especially the elementary theory of congruences and quadratic residues.

These topics are explained in great details in [HW00], [Chi89] and [Sha85].

0.2 Background, scope and goals of this work

The aim of the present work is to study certain subrings of $\mathbb{C}$ with respect to the property of being (or not being) UFD[1]. We will consider essentially the following classes:

- the rings $\mathbb{Z}\big[\sqrt{m}\,\big]$, where $m \in \mathbb{Z}$ is a non-square in $\mathbb{Z}$;
- the rings $h\big(\sqrt{m}\,\big)$, i.e. the rings of algebraic integers of quadratic extensions of $\mathbb{Q}$.

These issues are part of a broader class of problems, interesting both for their theoretic aspects and their applications, and which (at least in their embrional form) date back to Gauss and Euler.

These problems have been extensively studied in the last two centuries, and have led to many deep and interesting results (some of which are described in [ST87] and in chapters (XII), (XIV) and (XV) of [HW00]).

In this work, we will *not* study the mentioned problems in their full generality; what we will do is to show how it is possible to obtain partial yet interesting results about those problems by means of just elementary methods. For more complete results and more powerful methods the reader can refer to [ST87].

[1] by an UFD we mean a Unique Factorization Domain, i.e. a domain in which every element $\neq 0$ can be written, in an essentialy unique way, as a product of a finite number of irreducibles.

0.3 Overview of results

Overview of chapter 1

In chapter 1, some preliminary concepts, definitions and results will be presented, most of which are classical and well known.
Particularly important are the definition (1.2.1), the lemma (1.4.2) and the whole section 1.5.

Overview of chapter 2

In chapter 2, we will give a simple positive criterion for the uniqueness of factorization, i.e. a sufficient condition that, when satisfied, ensures that a given domain $\mathbb{Z}\big[\sqrt{m}\,\big]$ or $h\big(\sqrt{m}\,\big)$ is an UFD. This criterion will be proved by means of elementary methods, and will be used to find some examples of interesting UFDs, among which is the set $G = \mathbb{Z}\big[\sqrt{-1}\,\big]$ of gaussian integers.
The most significant results of this chapter are the enunciation of properties (1), (3) and (4), the theorem (2.2.1), and the retrieval of the well-known class of norm-euclidean domains through an unusual path.

Overview of chapter 3

In chapter 3, we will give some negative criterions for the uniqueness of factorization, i.e. a set of sufficient conditions such that, when any of them is satisfied, ensure that a given domain $\mathbb{Z}\big[\sqrt{m}\,\big]$ or $h\big(\sqrt{m}\,\big)$ is not an UFD. These criterions will be used to show that a large fraction of the $\mathbb{Z}\big[\sqrt{m}\,\big]$ and $h\big(\sqrt{m}\,\big)$ domains are not UFDs.
The proofs of important results of this chapter will use extensively the lemma (1.4.2) proved in chapter 1 and the law of quadratic reciprocity.
The most outstanding results of this chapter are five "summarizing" results: theorem (3.1.7), theorem (3.1.9), corollary (3.1.11), theorem (3.3.6) and theorem (3.4.7).

Overview of chapter 4

In this chapter, we'll explore some limits of the methods presented in chapter 2.
First and foremost, in theorem (4.1.2) we'll show the equivalence between the property (1) and the apparently stronger property (4) (both defined in chapter 2).
Finally, we'll show (extending a result presented in chapter (XIV) of [HW00]) that the great majority of the domains $h\big(\sqrt{m}\,\big)$ are not norm-euclidean.

0.4 Thanks

The author wishes to thank Professor Maria Clara Tamburini for her helpfulness, continuous support and good advices.
A deep thank is also due to Professor Maxim Vsemirnov, who read, discussed and corrected all the drafts of the present work, and provided a lot of useful suggestions, ideas and improvements.

Chapter 1

Preliminary results

1.1 The concepts of conjugate and norm

Definition 1.1.1. *For all $m \in \mathbb{Z}$ let*

$$\mathbb{Q}\big(\sqrt{m}\,\big) := \big\{a + b\sqrt{m} : a, b \in \mathbb{Q}\big\}. \tag{1.1}$$

It is straightforward to verify that $\mathbb{Q}\big(\sqrt{m}\,\big)$ is a subfield of $\mathbb{C}$ and that $\mathbb{Q}\big(\sqrt{m}\,\big) = \mathbb{Q}$ if and only if m is a perfect square, i.e. $m = h^2$ for an appropriate $h \in \mathbb{Z}$. So, in the rest of this section, we will denote by m a fixed non-square in $\mathbb{Z}$.

Definition 1.1.2. *For each $z \in \mathbb{Q}\big(\sqrt{m}\,\big)$, written $z = x+y\sqrt{m}$ with $x, y \in \mathbb{Q}$, we define $\overline{z} := x - y\sqrt{m}$, and call it the* conjugate *of z.*

The map $z \mapsto \overline{z}$ is an involutory automorphism of $\mathbb{Q}\big(\sqrt{m}\,\big)$, i.e.

$$\forall z_1, z_2 \in \mathbb{Q}\big(\sqrt{m}\,\big): \qquad \overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2, \quad \overline{z_1 z_2} = \overline{z}_1 \overline{z}_2, \quad \overline{1} = 1, \quad \overline{\overline{z_1}} = z_1. \tag{1.2}$$

It follows in particular that:

$$\forall z \in \mathbb{Q}\big(\sqrt{m}\,\big): \qquad \overline{z} = 0 \iff z = 0, \quad z \neq 0 \implies \overline{z^{-1}} = (\overline{z})^{-1}. \tag{1.3}$$

Note that when $m < 0$, the conjugate of $z \in \mathbb{Q}\big(\sqrt{m}\,\big)$ as defined above coincide with the usual complex conjugate of z in $\mathbb{C}$.

Definition 1.1.3. *For $z \in \mathbb{Q}\big(\sqrt{m}\,\big)$ we define*

$$\mathcal{N}(z) := |z\overline{z}|$$

and call it the norm *of z.*

Note that for every $z \in \mathbb{Q}\big(\sqrt{m}\,\big)$ it is $z\overline{z} \in \mathbb{Q}$, and then $\mathcal{N}(z) = |z\overline{z}| = \pm z\overline{z}$.

Lemma 1.1.4. *For all* $z,\ z_1,\ z_2 \in \mathbb{Q}\big(\sqrt{m}\,\big)$*:*

(i) $\mathcal{N}(z) = \mathcal{N}(\overline{z})$

(ii) $\mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\,\mathcal{N}(z_2)$

(iii) $\mathcal{N}(z) = 0 \iff z = 0$

(iv) $z \neq 0 \implies \mathcal{N}\left(z^{-1}\right) = \mathcal{N}(z)^{-1}$

Proof. It results:

- $\mathcal{N}(z) = |z\overline{z}| = \left|\overline{\overline{z}}\ \overline{z}\right| = \left|\overline{z}\ \overline{\overline{z}}\right| = \mathcal{N}(\overline{z})$;
- $\mathcal{N}(z_1 z_2) = |(z_1 z_2)(\overline{z_1 z_2})| = |z_1 z_2 \overline{z}_1 \overline{z}_2| = |(z_1 \overline{z}_1)(z_2 \overline{z}_2)| = \mathcal{N}(z_1)\,\mathcal{N}(z_2)$;
- since $\overline{z} = 0 \iff z = 0$ we have:
  $\mathcal{N}(z) = 0 \iff |z\overline{z}| = 0 \iff z\overline{z} = 0 \iff z = 0$ or $\overline{z} = 0 \iff z = 0$;
- $z \neq 0 \implies \mathcal{N}(z)\,\mathcal{N}\left(z^{-1}\right) = \mathcal{N}\left(zz^{-1}\right) = \mathcal{N}(1) = 1 \implies \mathcal{N}\left(z^{-1}\right) = \mathcal{N}(z)^{-1}$;

and the lemma is proved. □

1.2 Normed Domains

Definition 1.2.1. *Let* D *be a domain. We say that* D *is a* quadratic normed domain *if there exists a fixed non-square integer* m *such that* D *is a subring of* $\mathbb{Q}\big(\sqrt{m}\,\big)$*, and:*

- $\forall \alpha \in D:\ \mathcal{N}(\alpha) \in \mathbb{N}$
- $\forall \alpha \in D:\ \overline{\alpha} \in D$

Equivalently, we can say that D is a *quadratic normed domain* if there exists a fixed non-square intege m such that D is a subring of $\mathbb{Q}\big(\sqrt{m}\,\big)$, and:

$$\forall \alpha \in D:\ \overline{\alpha} \in D \text{ and } \alpha\overline{\alpha} \in \mathbb{Z}$$

From now on, for sake of conciseness, we will write simply *normed domain* instead of *quadratic normed domain*.

In the rest of this section, m will be a fixed non-square integer; moreover, we will denote by D a given normed domain.

Lemma 1.2.2. *Let $\alpha \in D$; then:*

$$\alpha \in D^* \iff \mathcal{N}(\alpha) = 1 \iff \overline{\alpha} \in D^*. \tag{1.4}$$

Proof. We start proving the first double implication of (1.4).

- $\alpha \in D^* \implies \exists\, \beta \in D : \alpha\beta = 1 \implies 1 = \mathcal{N}(1) = \mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta) \implies \mathcal{N}(\alpha) = \mathcal{N}(\beta) = 1$ (since $\mathcal{N}(\alpha)$ and $\mathcal{N}(\beta)$ are natural numbers). We conclude that $\mathcal{N}(\alpha) = 1$.
- $\mathcal{N}(\alpha) = 1 \implies \alpha\overline{\alpha} = \pm\mathcal{N}(\alpha) = \pm 1 \implies (\alpha)(\pm\overline{\alpha}) = 1 \implies \alpha \in D^*$ (since if $\alpha \in D$ then $\overline{\alpha} \in D$ and thus also $\pm\overline{\alpha} \in D$).

Thus we have proved the first double implication of (1.4). The second double implication can easily be deduced from the first, noting that $\forall \gamma \in D : \mathcal{N}(\gamma) = \mathcal{N}(\overline{\gamma})$. □

Lemma 1.2.3. *Let $\alpha, \beta \in D$ be such that $\beta \mid \alpha$. Then β is associate to α if and only if $\mathcal{N}(\beta) = \mathcal{N}(\alpha)$.*

Proof. Assume first that β is associate to α, i.e. $\beta = \epsilon\alpha$, for an appropriate $\epsilon \in D^*$. Thus we get immediatly $\mathcal{N}(\beta) = \mathcal{N}(\alpha)\mathcal{N}(\epsilon) = \mathcal{N}(\alpha)$.
Viceversa, assume now that $\mathcal{N}(\beta) = \mathcal{N}(\alpha)$. We can distinguish two cases.

1. $\beta \neq 0$, i.e. $\mathcal{N}(\beta) \neq 0$.

Write $\alpha = \beta\gamma$, with $\gamma \in D$. It follows:

$$\mathcal{N}(\beta) = \mathcal{N}(\alpha) = \mathcal{N}(\beta)\mathcal{N}(\gamma) \implies \mathcal{N}(\gamma) = 1.$$

We conclude $\gamma \in D^*$, i.e. α and β are associate.

2. $\beta = 0$.

The assumption $\beta \mid \alpha$ implies now $\alpha = 0$. So $\alpha = \beta = 0$ and, a fortiori, α and β are associate.

In both cases, our claim follows. □

The previous two lemmas immediately imply the following useful result:

Corollary 1.2.4. *Let $\alpha \in D \setminus (D^* \cup \{0\})$. Then α is irreducible if and only if*

$$\forall\, \beta \in D : \ 1 < \mathcal{N}(\beta) < \mathcal{N}(\alpha) \implies \beta \nmid \alpha$$

Lemma 1.2.5. *Every $\alpha \in D \setminus \{0\}$ can be written as a product of a finite number of irreducibles of D.*

Proof. By contradiction, let $\alpha \in D \setminus \{0\}$ do not satisfy our claim. Clearly we may assume that $\mathcal{N}(\alpha)$ has the least possible value. Since every unit and every irreducible obviously satisfy our claim, α must be reducible. By the previous Corollary there exists $\beta \in D$ such that $1 < \mathcal{N}(\beta) < \mathcal{N}(\alpha)$ and $\beta \mid \alpha$. Writing $\alpha = \beta\gamma$, $\gamma \in D$, we see that $1 < \mathcal{N}(\gamma) < \mathcal{N}(\alpha)$. By the minimality of $\mathcal{N}(\alpha)$ we have that β and γ can be written a finite product of irreducibles. Hence the same also holds for $\alpha = \beta\gamma$, a contradiction. □

1.3 Some notations

Let D be a domain in which every non-zero element can be written as a product of a finite number of irreducibles.
We denote by I the set of irreducibles in D, by K the set of those elements of D whose factorization into irreducibles is essentially unique, and by H the set of those elements of D which do not have this property, i.e. $H = D \setminus (K \cup \{0\})$.
Noting that every unit can be factorized only into 0 irreducibles, we have $D^* \subseteq K$. On the other hand, because every irreducible element has only trivial factorizations, we easily get $I \subseteq K$. We conclude that $D^* \cup I \subseteq K$.

With this notations the following useful result holds:

Lemma 1.3.1. *Let $\alpha \in K$, $\pi \in I$ such that $\pi \mid \alpha$, and $\alpha_1, \alpha_2 \in D$ such that $\alpha = \alpha_1\alpha_2$. Then $\pi \mid \alpha_1$ or $\pi \mid \alpha_2$.*

Proof. If $\alpha_1 = 0$ or $\alpha_2 = 0$, obiouvsly $\pi \mid \alpha_1$ or $\pi \mid \alpha_2$. So we can suppose $\alpha_1 \neq 0$ and $\alpha_2 \neq 0$; we have then by our hypothesis on D that α_1, α_2 can be written as product of finite number of irreducibles. So $\alpha_1 = \sigma_1 \cdots \sigma_r$, $\alpha_2 = \rho_1 \cdots \rho_s$ for appropriate $r, s \in \mathbb{N}$ and $\sigma_1, \ldots, \sigma_r, \rho_1, \ldots, \rho_s \in I$ (i.e. irreducibles). Since $\alpha = \alpha_1\alpha_2$, and $\alpha \in K$ we have then that:

$$\alpha = \alpha_1\alpha_2 = \sigma_1 \ldots \sigma_r\rho_1 \cdots \rho_s$$

is the *essentially unique factorization* of α as product of irreducibles. Since $\pi \mid \alpha$, we can then say that π must be associated with one of the irreducibles: $\sigma_1, \ldots \sigma_r, \rho_1, \ldots, \rho_s$. If π is associated to a σ_i, then $\pi \mid \alpha_1$, while if π is associated to a ρ_j, then $\pi \mid \alpha_2$, as desired. □

From previous result it immediatly derives by induction the following:

Corollary 1.3.2. *Let $\alpha \in K$, $\pi \in I$ such that $\pi \mid \alpha$, and $\alpha_1, \ldots, \alpha_n \in D$ such that $\alpha = \alpha_1 \ldots \alpha_n$. Then exists $i \in \{1, \ldots n\}$ such that $\pi \mid \alpha_i$*

1.4 Useful results in number theory

In this section we will present, briefly and without proof, some classical results in number theory, that we will use extensively later in our work.
Proofs and background information about these results can be found in [HW00], [Chi89] and [Dav94][1].
We will also state and prove a simple technical lemma, which will be of paramount importance in chapter 3.

Theorem (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots, m_n$ be pairwaise coprime positive integers, and let $a_1, a_2, \ldots, a_n$ be arbitrary integers; then there exists a solution $x = x_0 \in \mathbb{N}$ of the system:*

$$\begin{cases} x \equiv a_1 & (\text{mod } m_1) \\ x \equiv a_2 & (\text{mod } m_2) \\ \quad \vdots & \quad \vdots \\ x \equiv a_n & (\text{mod } m_n) \end{cases}$$

Morever, any other integer solution of this system is given by $x = x_0 + km_1m_2 \cdots m_n$, for arbitrary $k \in \mathbb{Z}$.

Definition (Quadratic residues)**.** *Let p be a prime. Then $x \in \mathbb{Z}$ is said to be a* quadratic residue of p *if there exists $y \in \mathbb{Z}$ such that $a \equiv y^2 \pmod{p}$, and a* quadratic non-residue of p *if no such $y \in \mathbb{Z}$ exists; if x is a quadratic residue of p and $x \not\equiv 0 \pmod{p}$, then x is said to be a* proper quadratic residue of p.
More generally, given an integer $m > 1$, we say that $x \in \mathbb{Z}$ is a quadratic residue of m *if $x \equiv y^2 \pmod{m}$ for a suitable $y \in \mathbb{Z}$; on the contrary, $x \in \mathbb{Z}$ is said to be a* quadratic non-residue of m *if $x \not\equiv y^2 \pmod{m}$ for every $y \in \mathbb{Z}$.*

Definition (Legendre symbol)**.** *Let p be a prime and x an integer; the* Legendre symbol *of x over p is defined as:*

$$\left(\frac{x}{p}\right) := \begin{cases} +1 & \text{if } x \text{ is a proper quadratic residue of } p \\ -1 & \text{if } x \text{ is a quadratic non-residue of } p \\ 0 & \text{if } x \equiv 0 \pmod{p} \end{cases}$$

[1] except for the proof of the Dirichlet's theorem, which is very difficult.

The most important properties of quadratic residues and of the Legendre symbol are summarized in the following proposition:

Theorem. *Let p, q be distinct odd primes, a, b integers. Then:*

(i) $\left(\frac{a^2}{p}\right) = 1$ *if* $p \nmid a$

(ii) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *if* $a \equiv b \pmod{p}$

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(iv) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, *or more explicitly:*

- $\left(\frac{-1}{p}\right) = +1$ *if* $p \equiv 1 \pmod{4}$,
- $\left(\frac{-1}{p}\right) = -1$ *if* $p \equiv 3 \pmod{4}$.

(v) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, *or more explicitly:*

- $\left(\frac{2}{p}\right) = +1$ *if* $p \equiv 1$ *or* $7 \pmod{8}$,
- $\left(\frac{2}{p}\right) = -1$ *if* $p \equiv 3$ *or* $5 \pmod{8}$.

(vi) $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$ (quadratic reciprocity law), *or more explicitly:*

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *if* $p \equiv 1 \pmod{4}$ *or* $q \equiv 1 \pmod{4}$,
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ *if* $p \equiv q \equiv 3 \pmod{4}$.

Here is a simple result on quadratic residues that will be useful in chapter 3:

Lemma 1.4.1. *Let $m > 1$ integer, p a prime such that $p \mid m$, and $x \in \mathbb{Z}$. If x is a quadratic non-residue of p, then it is also a quadratic non-residue of m.*

Proof. Argue by contradiction, assuming that there exists a suitable $y \in \mathbb{Z}$ such that $x \equiv y^2 \pmod{m}$; then, since $p \mid m$, it's also $x \equiv y^2 \pmod{p}$, which contradicts the fact that x is a quadratic non-residue of p. □

We'll need also the classical Dirichlet's theorem on primes in arithmetic progressions:

Theorem (Dirichlet's thorem on primes in arithmetic progressions)**.** *Let a, b be integers with $a > 0$ and* g.c.d. $(a, b) = 1$. *Then the arithmetic progression $\{an + b : n \in \mathbb{N}\}$ contains infinite primes.*

Let's finally see a quite simple and technical lemma that will be very useful in chapter 3.

Lemma 1.4.2. *Suppose given* $n \in \mathbb{N}$ *such that* $n \geq 1$, $p_1, p_2, \ldots, p_n$ *distinct primes,* $t \in \mathbb{Z}$ *such that* $\forall\, i \in \{1, \ldots, n\} : p_i \nmid t$, $a \in \mathbb{Z}$ *such that* g.c.d. $(a, t) = 1$ *and* $m \in \mathbb{N}$ *with* $m \leq n$.
Then there exist infinitely many primes q *such that:*

- q *is a proper quadratic residue of* p_i *for* $i = 1, \ldots m$
- q *is a quadratic non-residue of* p_j *for* $j = m + 1, \ldots n$
- $q \equiv a \pmod{t}$

Proof. As a first step, take $\xi_{m+1}, \xi_{m+2}, \ldots, \xi_n \in \mathbb{Z}$ quadratic non-residue respectively of $p_{m+1}, p_{m+2}, \ldots, p_n$.
Consider then the following system of linear congruences:

$$\begin{cases} x \equiv 1 & (\text{mod } p_1) \\ x \equiv 1 & (\text{mod } p_2) \\ \quad \vdots & \quad \vdots \\ x \equiv 1 & (\text{mod } p_m) \\ x \equiv \xi_{m+1} & (\text{mod } p_{m+1}) \\ \quad \vdots & \quad \vdots \\ x \equiv \xi_n & (\text{mod } p_n) \\ x \equiv a & (\text{mod } t) \end{cases} \tag{1.5}$$

Write $M := p_1 p_2 \cdots p_n t$. Since the p_j are pairwise coprime and all coprime with t, we know from Chinese remainder theorem that system (1.5) is soluble, and that if $x_0 \in \mathbb{N} \setminus \{0\}$ is its minimal positive solution then $x_k := x_0 + kM$ is also a solution for every $k \in \mathbb{Z}$.
Now, g.c.d. $(x_0, M) = 1$, since:

- for every $i \in \{1, 2, \ldots, m\}$, is $x_0 \equiv 1 \pmod{p_i}$, so that g.c.d. $(x_0, p_i) = 1$;
- for every $j \in \{m+1, m+2, \ldots, n\}$, is $x_0 \equiv \xi_j \pmod{p_j}$, so that g.c.d. $(x_0, p_j) = 1$ (since $p_j \nmid \xi_j$ as ξ_j is a quadratic non-residue of p_j);
- $x_0 \equiv a \pmod{t}$ and g.c.d. $(a, t) = 1$, so that g.c.d. $(x_0, t) = 1$.

Thus, from Dirichlet theorem, we have that the set:

$$\Gamma := \{x_k : k \in \mathbb{N}\} = \{x_0 + kM : k \in \mathbb{N}\} \subseteq \mathbb{N}$$

contains infinitely many primes q; each of this primes satisfies system (1.5), so that:

- $q \equiv a \pmod{t}$;
- $\forall\, i \in \{1, 2, \dots m\} : \; q \equiv 1^2 \pmod{p_i}$, so that q is a quadratic residue of p_i;
- $\forall\, j \in \{m+1, m+2, \dots n\} : \; q \equiv \xi_j \pmod{p_i}$ with ξ_j quadratic non-residue of p_j, so that q is a quadratic non-residue of p_j;

and our claim follows. □

1.5 Some subrings of $\mathbb{C}$

We are now going to define the subrings of $\mathbb{C}$ which will be considered in this work. They can be subdivided into two classes, namely:

1. the rings of the form $\mathbb{Z}\big[\sqrt{m}\,\big]$, with m a non-square in $\mathbb{Z}$;
2. the rings of algebraic integers of quadratic extensions of $\mathbb{Q}$.

Definition 1.5.1. *Given m in $\mathbb{Z}$ we define $\mathbb{Z}\big[\sqrt{m}\,\big] := \{a + b\sqrt{m} : \; a, b \in \mathbb{Z}\}$.*

More attention is deserved by the rings which belong to the above class (2), whose definition is somehow more elaborate and complex. All definitions and preliminar properties which we are now going to explain (quite schematically and without proofs) are analyzed in a more complete and organic form in chapter XIV of [HW00].
We begin recalling the definitions of "algebraic number", "algebraic integer", "algebraic field" and "quadratic field".

- A complex number $z \in \mathbb{C}$ is said to be an *algebraic number* if there exist $n \in \mathbb{N} \setminus \{0\}$ and $a_0, a_1, \dots, a_n \in \mathbb{Z}$ such that $a_n \neq 0$ and $a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = 0$. Equivalently, $z \in \mathbb{C}$ is algebraic if an only if there exists a non-costant polynomial $P(x) \in \mathbb{Z}[x]$ such that $P(z) = 0$.
- A complex number $z \in \mathbb{C}$ is said to be an *algebraic integer* if there exist $n \in \mathbb{N} \setminus \{0\}$ and $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$ such that $z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = 0$. Equivalently, $z \in \mathbb{C}$ is an algebraic integer if an only if there exists a non-costant monic polynomial $P(x) \in \mathbb{Z}[x]$ such that $P(z) = 0$. It can be proved with standard algebraic methods that $z \in \mathbb{C}$ is an algebraic integer if and only if it is algebraic over $\mathbb{Q}$ and its minimal polynomial over $\mathbb{Q}$ has rational integer coefficients (see for example Theorem (236) in chapter XIV of [HW00][2]).

[2] which, as a matter of fact, is given in a slighty different but equivalent form.

- For every $\vartheta \in \mathbb{C}$, we define

$$\mathbb{Q}(\vartheta) := \left\{ \frac{P(\vartheta)}{Q(\vartheta)} : \ P(x),\, Q(x) \in \mathbb{Q}[x] \ \text{ and } \ Q(\vartheta) \neq 0 \right\}$$

  and call it the simple extension of $\mathbb{Q}$ by ϑ.

  This definition is consistent, since it can easily be proved that $\mathbb{Q}(\vartheta)$ is the smallest subfield of $\mathbb{C}$ which contains ϑ. If ϑ is algebraic, we call it the *algebraic field* on ϑ.

- If $\xi \in \mathbb{C}$ is an irrational algebraic number which satisfies an equation of degree two with coefficients in $\mathbb{Z}$, then ξ is said to be *quadratic*. A *quadratic field* (or *quadratic estension of* $\mathbb{Q}$) is an algebraic field of the form $\mathbb{Q}(\xi)$, with $\xi \in \mathbb{C}$ quadratic.

Definition 1.5.2. *For every squarefree $m \in \mathbb{Z} \setminus \{0\}$ we define:*

$$h\big(\sqrt{m}\big) := \begin{cases} \{x + y\sqrt{m} : \ x, y \in \mathbb{Z}\} & \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \\ \left\{ \frac{x+y\sqrt{m}}{2} : \ x, y \in \mathbb{Z} \ \text{ and } \ x \equiv y \pmod 2 \right\} & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

For each algebraic number $\xi \in \mathbb{C}$ we define:

$$A_\xi := \{ z \in \mathbb{C} : \ z \text{ algebraic integer and } z \in \mathbb{Q}(\xi) \}.$$

According to the terminology introduced above, it can be proved that the collection of sets:

$$\{ A_\xi : \ \xi \in \mathbb{C} \text{ quadratic } \}$$

is precisely the collection of all the rings of the form $h\big(\sqrt{m}\big)$ for $m \in \mathbb{Z} \setminus \{0\}$ squarefree.

Finally we have:

Theorem 1.5.3. *For every $m \in \mathbb{Z} \setminus \{h^2 : h \in \mathbb{Z}\}$, $\mathbb{Z}\big[\sqrt{m}\big]$ is a normed domain. Moreover, for every squarefree $m \in \mathbb{Z} \setminus \{0\}$, $h\big(\sqrt{m}\big)$ is a normed domain.*

Proof. First, it is easy to prove that $\mathbb{Z}\big[\sqrt{m}\big]$ is a normed domain.
From the equality $h\big(\sqrt{m}\big) = \mathbb{Z}\big[\sqrt{m}\big]$, holding for $m \equiv 2 \text{ or } 3 \pmod 4$, we immediately have that $h\big(\sqrt{m}\big)$ is a normed domain if $m \equiv 2 \text{ or } 3 \pmod 4$.
Hence we have only to deal with the case $m \equiv 1 \pmod 4$, when it results:

$$h\big(\sqrt{m}\big) = \left\{ \frac{x + y\sqrt{m}}{2} : \ x,\, y \in \mathbb{Z} \ \text{ and } \ x \equiv y \pmod 2 \right\}.$$

Let $x, y, X, Y \in \mathbb{Z}$ such that $x \equiv y \pmod 2$ and $X \equiv Y \pmod 2$; we have:

- $\left(\frac{x+y\sqrt{m}}{2}\right)+\left(\frac{X+Y\sqrt{m}}{2}\right)=\frac{(x+X)+(y+Y)\sqrt{m}}{2}\in h\big(\sqrt{m}\,\big)$, since $x+X\equiv y+Y \pmod 2$;
- $\left(\frac{x+y\sqrt{m}}{2}\right)\left(\frac{X+Y\sqrt{m}}{2}\right)=\frac{(xX+myY)+(xY+Xy)\sqrt{m}}{4}=$
  $=\frac{a+b\sqrt{m}}{2}\in h\big(\sqrt{m}\,\big)$, since:
  (1) $xY+Xy\equiv xX+xX=2xX\equiv 0 \pmod 2$, so that:
  $b=\frac{xY+Xy}{2}\in\mathbb{Z}$;
  (2) $xX+myY\equiv xX+yY\equiv xX+Xx=2Xx\equiv 0 \pmod 2$, so that:
  $a=\frac{xX+myY}{2}\in\mathbb{Z}$;
  (3) $2a-2b=(xX+myY)-(xY+Xy)=xX+myY-xY-Xy\equiv xX+yY-xY-Xy \pmod 4 \implies 2a-2b\equiv x(X-Y)-y(X-Y)=(x-y)(X-Y)\equiv 0 \pmod 4$ (since $2\mid(x-y)$ and $2\mid(X-Y)$), so that:
  $2a\equiv 2b \pmod 4 \implies a\equiv b \pmod 2$;
- $1=\frac{2+0\sqrt{m}}{2}\in h\big(\sqrt{m}\,\big)$ (as obiouvsly $2\equiv 0 \pmod 2$);
- if $\alpha\in h\big(\sqrt{m}\,\big)$, then $\alpha=\frac{x+y\sqrt{m}}{2}$, for $x,y\in\mathbb{Z}$ such that $x\equiv y \pmod 2$; so $\overline{\alpha}=\frac{x-y\sqrt{m}}{2}\in h\big(\sqrt{m}\,\big)$ since $x\equiv y\equiv -y \pmod 2$, and also $\alpha\overline{\alpha}=\left(\frac{x^2-my^2}{4}\right)\in\mathbb{Z}$, since:

$$x\equiv y \pmod 2 \implies x^2\equiv y^2 \pmod 4 \implies x^2-my^2\equiv x^2-y^2\equiv 0 \pmod 4.$$

The first three points of the precedent list prove that $h\big(\sqrt{m}\,\big)$ is a subring of $\mathbb{Q}\big(\sqrt{m}\,\big)$, while the last point proves that $h\big(\sqrt{m}\,\big)$ is normed. □

Chapter 2

Some UFDs of algebraic integers

2.1 Unique factorization in the ring of Gaussian integers

Definition 2.1.1. *The ring G of Gaussian integers consists of all complex numbers $x+iy$ where x, y are rational integers, i.e.*

$$G := \mathbb{Z}[i] = \{x + iy : \ x, y \in \mathbb{Z}\} \tag{2.1}$$

Clearly G is a normed domain in the sense of definition (1.2.1), with $G^* = \{1, -1, i, -i\}$.

First we make an important remark: in the rest of this section we will denote by $\mathcal{N}(\cdot)$ the usual complex norm $\mathcal{N} : \mathbb{C} \longrightarrow [\,0, +\infty[$; however this will cause no confusion since, as $G = \mathbb{Z}[i] \subseteq \mathbb{Q}\big(\sqrt{-1}\,\big)$, we easily have that the complex norm and the norm in the sense of definition (1.1.3) coincide for G.

The aim of this Section is to prove that G is a UFD, without using the well known fact that G is an euclidean domain. To this purpose it will be useful the following result.

Lemma 2.1.2. *Let $\tau \in \mathbb{C} \setminus \{0\}$ be such that $\mathcal{N}(\tau) \leq 1$. Then there exists $\epsilon \in G^*$ such that $\mathcal{N}(\tau + \epsilon) < 1$.*

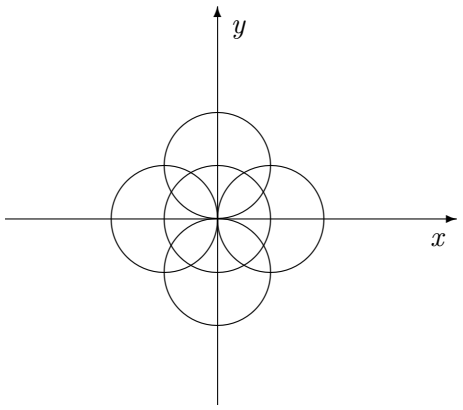
Proof. First note that, for every $\epsilon_1, \epsilon_2 \in G^*$, it results $\mathcal{N}(\epsilon_1\tau) \leq 1$ (since $\mathcal{N}(\epsilon_1\tau) = \mathcal{N}(\tau)$ and $\mathcal{N}(\tau) \leq 1$); moreover, if $\mathcal{N}(\epsilon_1\tau + \epsilon_2) < 1$, we have then:
$\mathcal{N}(\tau + \epsilon) < 1$, with $\epsilon := \epsilon_1^{-1}\epsilon_2 \in G^*$.
So we need to prove our assert only for $\epsilon\tau$, where $\epsilon \in G^*$ is an arbitrary unit of G.
We can now use this observation to simplify our problem. Let $\tau = a + ib$. Multiplying τ by $i \in G^*$, if necessary, we may assume $|a| \geq |b|$. Moreover, with a further multiplication by $\pm 1 \in G^*$ (with sign appropriatly chosen), we may assume $a \geq 0$. Summarizing we can assume without loss of generality that $a \geq |b|$.

We distinguish now 2 cases:

Case 1: $a > |b|$. Clearly $a \neq 0$, and $a \leq 1$ (since $a^2 + b^2 = \mathcal{N}(\tau) \leq 1$); hence, letting $\epsilon := -1 \in G^*$, we have: $\mathcal{N}(\tau + \epsilon) - 1 = \mathcal{N}(a + ib - 1) - 1 = (a-1)^2 + b^2 - 1 = a^2 + b^2 - 2a < 2a^2 - 2a = 2a(a-1) \leq 0$. Thus $\mathcal{N}(\tau + \epsilon) < 1$.

Case 2: $a = |b|$. We have then $a^2 = b^2$, and so $2a^2 = a^2 + b^2 = \mathcal{N}(\tau)$ with $\mathcal{N}(\tau) \leq 1$ and $\mathcal{N}(\tau) \neq 0 \Longrightarrow 0 < a \leq \frac{1}{\sqrt{2}} < 1 \Longrightarrow a(a-1) < 0$. Hence, letting $\epsilon := -1 \in G^*$, we have: $\mathcal{N}(\tau + \epsilon) - 1 = \mathcal{N}(a + ib - 1) - 1 = (a-1)^2 + b^2 - 1 = a^2 + b^2 - 2a = 2a^2 - 2a = 2a(a-1) < 0$. Thus $\mathcal{N}(\tau + \epsilon) < 1$. □

The following picture provides a geometric interpretation of the previous lemma, as it shows visually that the union of the four unitary *open* circles with center respectively $(-1, 0)$, $(0, -1)$, $(1, 0)$, $(0, 1)$ covers completely the unitary *closed* circle centered in $(0, 0)$, deprived of the center (i.e. the point $(0, 0)$).



Now we return to our main topic. Our central theorem may be enunciated as follows:

Theorem 2.1.3. *The ring G is an UFD.*

To prove this theorem, we need some preliminary observations and one further lemma.
First, in the notation of section 1.3, our aim is to show that $H = \emptyset$, i.e. the set of elements of G which do not admit an essentially unique factorization is empty.
We will argue by contradiction assuming that $H \neq \emptyset$.
Recalling that $I \cup G^* \subseteq K$, we have that any factorization into irreducible of an arbitrary element of H consists of at least two (not necessarily distinct) factors.
As G is a normed domain, we know from lemma (1.2.5) that every $\alpha \in G \setminus \{0\}$ can be written as a product of a finite number of irreducible.

By the assumption $H \neq \emptyset$, we may choose $\xi_0 \in H$ such that $\mathcal{N}(\xi_0) = \min \mathcal{N}(H)$, where (of course) $\mathcal{N}(H) := \{\mathcal{N}(h) : \ h \in H\}$.
By definition of H we have, in particular,

$$\xi_0 = \pi_1 \pi_2 \cdots \pi_r = \sigma_1 \sigma_2 \cdots \sigma_s \tag{2.2}$$

with $r, s \geq 2$, for suitable $\pi_k, \sigma_h \in I$ which make the two factorizations essentially distinct.
Our proof will be based on the following two Lemmas.

Lemma 2.1.4. *Referring to the equation* (2.2)*, we have that for every* $i, j \in \mathbb{N}$ *with* $1 \leq i \leq r$ *and* $1 \leq j \leq s$*,* π_i *and* σ_j *are not associated.*

Proof. Assume that our claim is false. Then, up to a reordering of the factors, we may suppose that σ_1 is associate to π_1, i.e. $\sigma_1 = \epsilon \pi_1$, with $\epsilon \in G^*$. Letting $\xi := \pi_2 \cdots \pi_r$ and simplifing (2.2) by π_1, we get:

$$\xi = \pi_2 \cdots \pi_r = (\epsilon \sigma_2) \cdots \sigma_s. \tag{2.3}$$

Since the two factorizations of ξ_0 in (2.2) are essentially distinct, and since ϵ is a unit of G, it can easily be shown that also the two factorizations of ξ in (2.3) are essentially distinct, i.e. that $\xi \in H$. Noting that we have also $\mathcal{N}(\xi) < \mathcal{N}(\xi_0)$ (since $\xi_0 = \pi_1 \xi$ and $\mathcal{N}(\pi_1) > 1$) and $\mathcal{N}(\xi_0) = \min \mathcal{N}(H)$ (by definition of ξ_0), we get the desired contradiction. □

It's also clear that we may suppose without loss of generality that $\mathcal{N}(\pi_1) \leq \mathcal{N}(\sigma_1)$; at this stage we can finally give:

Proof of theorem (2.1.3). Let $\tau := \frac{\pi_1}{\sigma_1}$; clearly $\mathcal{N}(\tau) \leq 1$ and $\tau \neq 0$, so we have by lemma (2.1.2) that:

$$\exists\, \epsilon \in G^* : \ \mathcal{N}(\tau + \epsilon) < 1, \quad \text{i.e. such that:} \quad \mathcal{N}(\epsilon \sigma_1 + \pi_1) < \mathcal{N}(\sigma_1).$$

Define now $\psi := \epsilon \xi_0 + \pi_1 \sigma_2 \cdots \sigma_s$; from equation (2.2) it derives:

- $\psi = \pi_1 (\epsilon \pi_2 \cdots \pi_r + \sigma_2 \cdots \sigma_s) = \pi_1 \omega, \ \omega \in G \implies \pi_1 \mid \psi$
- $\psi = (\epsilon \sigma_1 + \pi_1)(\sigma_2 \cdots \sigma_s)$

From the last equality it follows in particular that $\psi \neq 0$, since $\epsilon \sigma_1 + \pi_1 \neq 0$ as π_1, σ_1 not associate.

Moreover:

$$\mathcal{N}(\psi) = \mathcal{N}(\epsilon\sigma_1 + \pi_1)\mathcal{N}(\sigma_2 \cdots \sigma_s) < \mathcal{N}(\sigma_1)\mathcal{N}(\sigma_2 \cdots \sigma_s) = \mathcal{N}(\sigma_1 \cdots \sigma_s) = \mathcal{N}(\xi_0)$$

so that:

$$\mathcal{N}(\psi) < \mathcal{N}(\xi_0) = \min \mathcal{N}(H) \implies \psi \notin H \implies \psi \in K$$

Thus ψ has an essentially unique factorization into irreducibles. Since:

- $\pi_1 \mid \psi$, and:
- $\psi = (\epsilon\sigma_1 + \pi_1)(\sigma_2 \cdots \sigma_s)$, and:
- π_1 is not associate with any σ_j,

it follows from corollary (1.3.2) that $\pi_1 \mid (\epsilon\sigma_1 + \pi_1)$, and then $\pi_1 \mid \epsilon\sigma_1$.
Since π_1, σ_1 are irreducible and ϵ is a unit of G, this means that π_1 and σ_1 are associate, which, according to lemma (2.1.4), gives us the desired contradiction. □

2.2 Exstensions to a class of normed domains

In this section we will extend and generalize the methods and concepts seen so far, and use them to show that some well-known real and complex normed domains are UFDs.[1]

In the rest of this section, we'll limit our attention to that normed domains D which satisfy an analogue of lemma (2.1.2); more precisely, from now on and until the end of this section, we will denote by $D \subseteq \mathbb{Q}(\sqrt{m})$ a normed domain which satisfies the following:

Property 1. $\forall \tau \in \mathbb{Q}(\sqrt{m}) \setminus \{0\}$ *such that* $\mathcal{N}(\tau) \leq 1$ *and* $\tau \notin D^*$, $\exists\, \theta \in D$ *such that* $\mathcal{N}(\theta\tau + 1) < 1$.

Our aim is to prove that, in such hypothesis, D is an UFD, i.e. in the notation of section (1.3) of chapter (1), that $K = D \setminus \{0\}$, or equivalently that $H = \emptyset$ (note that we have no need to prove that every $\alpha \in D$ can be written as a finite product of irreducibles, since, being D is a normed domain, this fact already assured by lemma (1.2.5)).
Here is our proposition in a precise form:

[1] Regarding the domains we're going to analyze, we must say that it's known that all them are, in fact, *euclidean domains*, and so, a fortiori, UFDs. But we won't make direct use of this fact; instead, we will retrieve this well-known class of domains in an original way, and only later we will find, state and prove the well-known result asserting that their norm is an euclidean function. More observation about these facts will be given later.

Theorem 2.2.1. *Let $D \subseteq \mathbb{Q}\left(\sqrt{m}\right)$ be a normed domain such that:*

$$\forall \tau \in \mathbb{Q}\left(\sqrt{m}\right) \setminus \{0\} \text{ with } \mathcal{N}(\tau) \leq 1 \text{ and } \tau \notin D^*,\ \exists\, \theta \in D :\ \mathcal{N}(\theta\tau + 1) < 1$$

(i.e. D satisfies property (1)). Then D is an UFD.

Proof. The proof is very similar to that seen in the previous section for the theorem (2.1.3).
Argue by contradiction, supposing $H \neq \emptyset$. By this assumption we may choose $\xi_0 \in H$ such that $\mathcal{N}(\xi_0) = \min \mathcal{N}(H)$.
Since $\xi_0 \in H$, by definition of H we have in particular:

$$\xi_0 = \pi_1\pi_2 \cdots \pi_r = \sigma_1\sigma_2 \cdots \sigma_s \tag{2.4}$$

with $r, s \geq 2$, for suitable $\pi_k, \sigma_h \in I$ which make the two factorizations essentially distinct.
Exactly as seen in the proof of lemma (2.1.4), it can be proved that, in the two factorizations given by equation (2.4), no π_k is associate with any σ_h. Moreover, we can clearly assume without loss of generality that $\mathcal{N}(\pi_1) \leq \mathcal{N}(\sigma_1)$.
Let now $\tau := \frac{\pi_1}{\sigma_1} \in \mathbb{Q}\left(\sqrt{m}\right)$; clearly $\mathcal{N}(\tau) \leq 1$, and, since π_1 and σ_1 are not associate, $\tau \notin D^*$; so we have by property (1) that:

$$\exists\, \theta \in D \text{ such that } \mathcal{N}(\tau\theta + 1) < 1, \text{ i.e. such that } \mathcal{N}(\sigma_1 + \theta\pi_1) < \mathcal{N}(\sigma_1).$$

Define now $\psi := \xi_0 + \theta\pi_1\sigma_2 \cdots \sigma_s$; from (2.4) it derives:

- $\psi = \pi_1(\pi_2 \cdots \pi_r + \theta\sigma_2 \cdots \sigma_s) = \pi_1\omega,\ \omega \in G \implies \pi_1 \mid \psi$
- $\psi = (\sigma_1 + \theta\pi_1)(\sigma_2 \cdots \sigma_s)$

From the last equality it follows in particular that $\psi \neq 0$, since $\sigma_1 + \theta\pi_1 \neq 0$ (as $\pi_1 \nmid \sigma_1$ because π_1, σ_1 are irreducible and not associate).
Moreover:

$$\mathcal{N}(\psi) = \mathcal{N}(\sigma_1 + \theta\pi_1)\mathcal{N}(\sigma_2 \cdots \sigma_s) < \mathcal{N}(\sigma_1)\mathcal{N}(\sigma_2 \cdots \sigma_s) = \mathcal{N}(\sigma_1 \cdots \sigma_s) = \mathcal{N}(\xi_0)$$

so that:

$$\mathcal{N}(\psi) < \mathcal{N}(\xi_0) = \min \mathcal{N}(H) \implies \psi \notin H \implies \psi \in K$$

Thus ψ has an essentially unique factorization into irreducibles. Since:

- $\pi_1 \mid \psi$, and:
- $\psi = (\sigma_1 + \theta\pi_1)(\sigma_2 \cdots \sigma_s)$, and:
- π_1 is not associate with any σ_j,

it follows from corollary (1.3.2) that $\pi_1 \mid (\sigma_1 + \theta\pi_1)$, and so $\pi_1 \mid \sigma_1$.

Since π_1, σ_1 are irreducible, this means that π_1 and σ_1 are associate, which, according to what proved previously, gives us the desired contradiction. □

Now we consider a concrete exemple of normed domain which satisfies theorem (2.2.1).

What we want to prove here is that the real normed domain $h\big(\sqrt{2}\,\big) = \mathbb{Z}\big[\sqrt{2}\,\big]$ is an UFD, showing that it satisfies property (1).

Suppose that $\tau = a + b\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}\,\big) \setminus \big(\mathbb{Z}\big[\sqrt{2}\,\big]^* \cup \{0\}\big) \subseteq \mathbb{R} \setminus \{0\}$ (with $a, b \in \mathbb{Q}$ not both zero, since $\tau \neq 0$) and such that $\mathcal{N}(\tau) \leq 1$ (i.e. $\big|a^2 - 2b^2\big| \leq 1$).

Since $a, b \in \mathbb{Q}$ are not both zero, it results $a^2 - 2b^2 \neq 0$. So we can find $x, y \in \mathbb{Z}$ such that:

$$(2.5) \qquad \begin{cases} \left| x + \frac{a}{a^2-2b^2} \right| \leq \frac{1}{2} \\ \left| y - \frac{b}{a^2-2b^2} \right| \leq \frac{1}{2} \end{cases}$$

Let now $\theta := x + y\sqrt{2} \in \mathbb{Z}\big[\sqrt{2}\,\big]$; we want to show that: $\mathcal{N}(\theta\tau + 1) < 1$.

This follows from simple (yet tedious) calculations:

$$\begin{aligned}
&\mathcal{N}(\theta\tau + 1) = \mathcal{N}\left((x + y\sqrt{2})(a + b\sqrt{2}) + 1\right) = \\
&\left|(ax + 2by + 1)^2 - 2(ay + bx)^2\right| = \\
&\left|a^2x^2 + 4b^2y^2 + 1 + 4abxy + 2ax + 4by - 2a^2y^2 - 2b^2x^2 - 4abxy\right| = \\
&\left|x^2(a^2 - 2b^2) - 2y^2(a^2 - 2b^2) + 1 + 2(ax + 2by)\right| = \\
&\left|a^2 - 2b^2\right| \cdot \left| x^2 - 2y^2 + \frac{1}{a^2 - 2b^2} + \frac{2(ax + 2by)}{a^2 - 2b^2} \right| \leq \\
&\left| x^2 - 2y^2 + \frac{1}{a^2 - 2b^2} + \frac{2(ax + 2by)}{a^2 - 2b^2} \right| = \\
&\left| \left(x^2 + 2 \cdot \frac{ax}{a^2 - 2b^2} + \frac{a^2}{(a^2 - 2b^2)^2} \right) - 2\left(y^2 - 2 \cdot \frac{by}{a^2 - 2b^2} + \frac{b^2}{(a^2 - 2b^2)^2} \right) \right| = \\
&\left| \left(x + \frac{a}{a^2 - 2b^2} \right)^2 - 2\left(y - \frac{a}{a^2 - 2b^2} \right)^2 \right| \leq \\
&\left(x + \frac{a}{a^2 - 2b^2} \right)^2 + 2\left(y - \frac{a}{a^2 - 2b^2} \right)^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4} < 1.
\end{aligned}$$

So property (1) is valid for $h\big(\sqrt{2}\,\big)$, which then is an UFD.

2.3 Equivalent forms for our results

In this section we'll give two altenative equivalent forms for property (1). Then, we'll see how it is possible to express such property in a slighty stronger way, which is however much more manageable. In this weaker form it will be easy to recognize the fundamental property of those normed domains which are "euclidean with respect to the norm" (or, more briefly, "norm-euclidean"). So we see as it's possibile to retrieve by an unusual way the well-known class of euclidean real or complex domains of quadratic numbers.

In what follows, m is of course a non-square integer and D is a normed domain with $D \subseteq \mathbb{Q}\left(\sqrt{m}\right)$.

Property 2. $\forall\, \tau \in \mathbb{Q}\left(\sqrt{m}\right)$ *such that* $\mathcal{N}(\tau) \geq 1$, $\exists\, \theta \in D$ *such that* $\mathcal{N}(\tau - \theta) < \mathcal{N}(\tau)$.

We have immediatly:

Theorem 2.3.1. *If* $D \subseteq \mathbb{Q}\left(\sqrt{m}\right)$ *is a normed domain, then it satisfies property (1) if and only if it satisfies property (2).*

Proof. We'll prove the two implication separately.

1. Let us prove that property (1) implies property (2).

   Suppose $\tau \in \mathbb{Q}\left(\sqrt{m}\right)$ such that $\mathcal{N}(\tau) \geq 1$. If $\tau \in D^*$, than *a fortiori* $\tau \in D$; so, letting $\theta := \tau \in D$, we obtain $\mathcal{N}(\tau - \theta) = 0 < \mathcal{N}(\tau)$. If $\tau \notin D^*$, then is also $\tau_1 := (-\tau)^{-1} \notin D^*$, and moreover is $\mathcal{N}(\tau_1) = (\mathcal{N}(\tau))^{-1} \leq 1$, so that we obtain from property (1) that $\exists\, \theta \in D : \mathcal{N}(\theta\tau_1 + 1) < 1 \implies \mathcal{N}(\tau - \theta) = \mathcal{N}(\tau)\mathcal{N}\left(1 - \theta\tau^{-1}\right) = \mathcal{N}(\tau)\left(\mathcal{N}(1 + \theta\tau_1)\right) < \mathcal{N}(\tau)$.

2. Let us prove that property (2) implies property (1).

   Suppose $\tau \in \mathbb{Q}\left(\sqrt{m}\right) \setminus (D^* \cup \{0\})$ such that $\mathcal{N}(\tau) \leq 1$. Letting $\tau_1 := -\left(\tau^{-1}\right)$, it results $\mathcal{N}(\tau_1) = \mathcal{N}\left(-\left(\tau^{-1}\right)\right) = \mathcal{N}\left(\tau^{-1}\right) = (\mathcal{N}(\tau))^{-1} \geq 1$, so that we immediately obtain from property (2) that $\exists\, \theta \in D : \mathcal{N}(\theta - \tau_1) < \mathcal{N}(\tau_1) \implies \mathcal{N}(\tau\theta + 1) = \mathcal{N}(\tau)\mathcal{N}\left(\theta + \tau^{-1}\right) = \mathcal{N}(\tau)\mathcal{N}(\theta - \tau_1) < \mathcal{N}(\tau)\mathcal{N}(\tau_1) = \mathcal{N}(\tau\tau_1) = \mathcal{N}(-1) = 1$.

The two implications prove the theorem. □

Let's now see another property which is (almost) equivalent to property (1):

Property 3. $\forall\, \alpha, \beta \in D\backslash\{0\}$ *such that* $\mathcal{N}(\alpha) \geq \mathcal{N}(\beta)$, $\exists\, \theta, \rho \in D$ *such that* $\alpha = \beta\theta + \rho$ *and* $\mathcal{N}(\rho) < \mathcal{N}(\alpha)$.

The following result holds:

Theorem 2.3.2. *If* $D \subseteq \mathbb{Q}\big(\sqrt{m}\,\big)$ *is a normed domain such that* $D \not\subseteq \mathbb{Q}$, *then it satisfies property (1) if and only if it satisfies property (3).*

Proof. First, since $D \not\subseteq \mathbb{Q}$, there exist $r, s \in \mathbb{Q} :\ r + s\sqrt{m} \in D,\ s \neq 0$. From this, it's quite easy to deduce that the field of quotients of D is $\mathbb{Q}\big(\sqrt{m}\,\big)$, so that:

$$\forall \xi \in \mathbb{Q}\big(\sqrt{m}\,\big) :\ \exists\, \lambda_1, \lambda_2 \in D \text{ such that } \lambda_2 \neq 0 \text{ and } \xi = \frac{\lambda_1}{\lambda_2}$$

At this point, note that thanks to the theorem (2.3.1) we need only to prove that:

$$(\text{property (2) holds for } D) \iff (\text{property (3) holds for } D).$$

We'll do this in two steps.

1. Let us prove that property (2) implies property (3).

   Let $\alpha, \beta \in D \setminus \{0\}$ with $\mathcal{N}(\alpha) \geq \mathcal{N}(\beta)$, and put $\tau := \frac{\alpha}{\beta} \in \mathbb{Q}\big(\sqrt{m}\,\big)$, so that $\mathcal{N}(\tau) \geq 1$. Then for property (2) we have that $\exists\, \theta \in D$ with $\mathcal{N}(\tau - \theta) < \mathcal{N}(\tau)$, i.e. $\mathcal{N}(\alpha - \theta\beta) = \mathcal{N}(\beta)\mathcal{N}(\tau - \theta) < \mathcal{N}(\beta)\mathcal{N}(\tau) = \mathcal{N}(\beta\tau) = \mathcal{N}(\alpha)$. So it's enough to put $\rho := (\alpha - \beta\theta) \in D$ to get the desired result.

2. Let us prove that property (3) implies property (2).

   Let $\tau \in \mathbb{Q}\big(\sqrt{m}\,\big)$ such that $\mathcal{N}(\tau) \geq 1$; we know that τ can be written as $\tau = \frac{\alpha}{\beta}$ for suitable $\alpha, \beta \in D$ with $\beta \neq 0$. So by our hypotesis it results:

   $$\mathcal{N}(\tau) \geq 1 \implies \mathcal{N}(\alpha) \geq \mathcal{N}(\beta)$$

   and thus, from property (3):

   $$\exists\, \theta, \rho \in D \text{ such that } \mathcal{N}(\rho) < \mathcal{N}(\alpha) \text{ and } \alpha = \beta\theta + \rho$$

   so that:

   $$\begin{aligned} \mathcal{N}(\tau - \theta) &= \mathcal{N}\left(\beta^{-1}\right)\mathcal{N}(\beta\tau - \beta\theta) = \left(\mathcal{N}(\beta)\right)^{-1}\mathcal{N}(\alpha - \beta\theta) = \\ &= \frac{\mathcal{N}(\rho)}{\mathcal{N}(\beta)} < \frac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)} = \mathcal{N}\left(\frac{\alpha}{\beta}\right) = \mathcal{N}(\tau)\,. \end{aligned}$$

   Thus $\mathcal{N}(\tau - \theta) < \mathcal{N}(\tau)$, as required.

The two implications prove the theorem. □

Let's finally see a stonger but handier form of property (1)[2]:

Property 4. $\forall\, \psi \in \mathbb{Q}\big(\sqrt{m}\big)$, $\exists\, \theta \in D$ *such that* $\mathcal{N}(\psi - \theta) < 1$.

The following useful result holds:

Theorem 2.3.3. *If* $D \subseteq \mathbb{Q}\big(\sqrt{m}\big)$ *is a normed domain which satisfies property (4), then it also satisfies property (1). In particular, every normed domain* D *which satisfies property (4) is an UFD.*

Proof. Since property (1) is equivalent to property (2), it's enough to prove that property (2) follows from property (4).
Let $\tau \in \mathbb{Q}\big(\sqrt{m}\big)$ such that $\mathcal{N}(\tau) \geq 1$; then, from property (4) we can say that $\exists\, \theta \in D$ such that $\mathcal{N}(\tau - \theta) < 1 \implies \mathcal{N}(\tau - \theta) < \mathcal{N}(\tau)$ since $1 \leq \mathcal{N}(\tau)$. So D satisfies property (2). □

Finally we see that property (4) is equivalent to the fact that the domain D is *norm-euclidean* (at least in the case $D \not\subseteq \mathbb{Q}$).
Obiouvsly, we say that a normed domain D is norm-euclidean if its norm $\mathcal{N} : D \longrightarrow \mathbb{N}$ is an euclidean function, i.e. if:

$$\forall \alpha, \beta \in D,\ \beta \neq 0 : \exists\, \theta, \rho \in D \text{ such that } \alpha = \beta\theta + \rho \text{ and } (\rho = 0 \text{ or } \mathcal{N}(\rho) < \mathcal{N}(\beta))$$

The following result holds:

Theorem 2.3.4. *If* $D \subseteq \mathbb{Q}\big(\sqrt{m}\big)$ *is a normed domain such that* $D \not\subseteq \mathbb{Q}$*, then it satisfies property (4) if and only if it is norm-euclidean.*

Proof. Again, from $D \not\subseteq \mathbb{Q}$ we can immediatly conclude that the field of quotients of D is $\mathbb{Q}\big(\sqrt{m}\big)$, so that:

$$\forall \xi \in \mathbb{Q}\big(\sqrt{m}\big) : \exists\, \lambda_1, \lambda_2 \in D \text{ such that } \lambda_2 \neq 0 \text{ and } \xi = \frac{\lambda_1}{\lambda_2}$$

Suppose first that D is norm-euclidean. Then, given $\psi \in \mathbb{Q}\big(\sqrt{m}\big)$ and writing $\psi = \frac{\alpha}{\beta}$ for suitable $\alpha, \beta \in D$ with $\beta \neq 0$, we have that there exist $\theta, \rho \in D$ such that $\alpha = \beta\theta + \rho$,

[2]but we'll see in chapter 4 that property (4) is only apparently stronger than property (1), the two being essentially equivalent.

with $\mathcal{N}(\rho) < \mathcal{N}(\beta)$[3]. We have then:

$$\mathcal{N}(\psi - \theta) = \mathcal{N}\left(\frac{\alpha - \theta\beta}{\beta}\right) = \mathcal{N}\left(\frac{\rho}{\beta}\right) = \frac{\mathcal{N}(\rho)}{\mathcal{N}(\beta)} < \frac{\mathcal{N}(\beta)}{\mathcal{N}(\beta)} = 1$$

so that D satisfies property (4).

Conversely, suppose now that D satisfies property (4). Then, given $\alpha, \beta \in D$ with $\beta \neq 0$, letting $\psi := \frac{\alpha}{\beta} \in \mathbb{Q}\big(\sqrt{m}\,\big)$, we can find $\theta \in D$ such that $\mathcal{N}(\psi - \theta) < 1$, i.e. such that $\mathcal{N}(\alpha - \beta\theta) < \mathcal{N}(\beta)$. Thus, defining $\rho := \alpha - \beta\theta$, we obtain:

$$\alpha = \beta\theta + \rho, \quad \mathcal{N}(\rho) < \mathcal{N}(\beta)$$

and so *a fortiori*:

$$\alpha = \beta\theta + \rho, \quad \mathcal{N}(\rho) < \mathcal{N}(\beta) \ \text{ or } \ \rho = 0.$$

so that D satisfies property (4). □

2.4 Some concrete applications

At this point we can retrieve the classical:

Theorem 2.4.1. *The complex normed domains:*

$$h\big(\sqrt{-1}\,\big) = \mathbb{Z}[\,i\,],\ h\big(\sqrt{-2}\,\big) = \mathbb{Z}\big[\sqrt{-2}\,\big],\ h\big(\sqrt{-3}\,\big),\ h\big(\sqrt{-7}\,\big),\ h\big(\sqrt{-11}\,\big)$$

and the real normed domains:

$$h\big(\sqrt{2}\,\big) = \mathbb{Z}\big[\sqrt{2}\,\big],\ h\big(\sqrt{3}\,\big) = \mathbb{Z}\big[\sqrt{3}\,\big],\ h\big(\sqrt{5}\,\big),\ h\big(\sqrt{13}\,\big)$$

are UFDs.

Proof. We want to show that the domains listed in the statement of the theorem all satisfy property (4), so from theorem (2.3.3) it will follow immediately that all these domains are UFDs.

We distinguish two cases.

Case 1: $D = \mathbb{Z}\big[\sqrt{m}\,\big]$, for $m = -1,\ -2,\ +2,\ +3$.

This case comprises all the m such that $m \equiv 2$ or $3 \pmod 4$.

Given $\psi \in \mathbb{Q}\big(\sqrt{m}\,\big)$, it results $\psi = a + b\sqrt{m}$ for appropriate $a, b \in \mathbb{Q}$. If we take $x, y \in \mathbb{Z}$ such that $|a - x| \leq \frac{1}{2}$ and $|b - y| \leq \frac{1}{2}$, and define $\theta := x + y\sqrt{m}$, then we have clearly $\theta \in D$.

[3] in principle, there is also the separate case $\rho = 0$, which however still implies $\mathcal{N}(\rho) = 0 < \mathcal{N}(\beta)$, since $\beta \neq 0$.

Moreover:

$$\mathcal{N}(\psi-\theta)=\mathcal{N}\left((a-x)+(b-y)\sqrt{m}\right)=\left|(a-x)^2-m(b-y)^2\right|.$$

If $m=-1,\ -2,\ +2$ we have then:

$$\mathcal{N}(\psi-\theta)\leq(a-x)^2+|m|\,(b-y)^2\leq\frac{1}{4}+|m|\cdot\frac{1}{4}=\frac{1+|m|}{4}\leq\frac{1+2}{4}=\frac{3}{4}<1$$

i.e. $\mathcal{N}(\psi-\theta)<1$.

If $m=3$, we must reason in a slighty different way. There are the two following possibilities:

$$\left|(a-x)^2-m(b-y)^2\right|=(a-x)^2-m(b-y)^2\leq(a-x)^2\leq\frac{1}{4}<1$$

or:

$$\left|(a-x)^2-m(b-y)^2\right|=m(b-y)^2-(a-x)^2\leq m(b-y)^2\leq\frac{m}{4}=\frac{3}{4}<1$$

In both these cases we have:

$$\mathcal{N}(\psi-\theta)=\left|(a-x)^2-m(b-y)^2\right|<1$$

as required.

Case 2: $D=h\left(\sqrt{m}\right)$, for $m=-3,\ -7,\ -11,\ +5,\ +13$.

This case comprises all the m such that $m\equiv 1\pmod 4$.

Given $\psi\in\mathbb{Q}\left(\sqrt{m}\right)$, we can obviously find $a,\,b\in\mathbb{Q}$ such that $\psi=\frac{a+b\sqrt{m}}{2}$. If we take $y\in\mathbb{Z}$ such that $|b-y|\leq\frac{1}{2}$, and then $x\in\mathbb{Z}$ such that $\left|\frac{a-y}{2}-x\right|\leq\frac{1}{2}$ and define $\theta:=\frac{(2x+y)+y\sqrt{m}}{2}$, then we have $\theta\in D$ (since $2x+y\equiv y\pmod 2$).

Moreover:

$$\mathcal{N}(\psi-\theta)=\mathcal{N}\left(\frac{(a-y-2x)+(b-y)\sqrt{m}}{2}\right)=\left|\frac{1}{4}(a-y-2x)^2-\frac{1}{4}m(b-y)^2\right|$$

If $m=-3,\ -7,\ -11,\ +5$ we have then:

$$\begin{aligned}\mathcal{N}(\psi-\theta)\ &\leq\ \left(\frac{a-y-2x}{2}\right)^2+\frac{1}{4}\,|m|\,(b-y)^2\leq\left(\frac{1}{2}\right)^2+\frac{|m|}{4}\left(\frac{1}{2}\right)^2=\\ &=\ \frac{1}{4}+|m|\cdot\frac{1}{16}=\frac{4+|m|}{16}\leq\frac{4+11}{16}=\frac{15}{16}<1\end{aligned}$$

i.e. $\mathcal{N}(\psi-\theta)<1$.

If $m = 13$, we must reason in a slighty different way.
In this case, we can have either:

$$\begin{aligned}\left|\frac{1}{4}(a-y-2x)^2 - \frac{1}{4}m(b-y)^2\right| &= \frac{1}{4}(a-y-2x)^2 - \frac{1}{4}m(b-y)^2 \leq \\ &\leq \frac{1}{4}(a-y-2x)^2 = \left(\frac{a-y-2x}{2}\right)^2 \leq \frac{1}{4} < 1\end{aligned}$$

or:

$$\begin{aligned}\left|\frac{1}{4}(a-y-2x)^2 - \frac{1}{4}m(b-y)^2\right| &= \frac{1}{4}m(b-y)^2 - \frac{1}{4}(a-y-2x)^2 \leq \\ &\leq \frac{1}{4}m(b-y)^2 \leq \frac{m}{4}\cdot\left(\frac{1}{2}\right)^2 = \frac{m}{16} = \frac{13}{16} < 1\end{aligned}$$

In both cases it results:

$$\mathcal{N}(\psi - \theta) = \left|\frac{1}{4}(a-y-2x)^2 - \frac{1}{4}m(b-y)^2\right| < 1$$

as required. □

More information about normed domains D of the form $h\big(\sqrt{m}\,\big)$ which satisfy (or do not satisfy) property (4) (which is effectively equivalent to say that the domain D is euclidean with respect to the norm) can be found in Chapter XIV of [HW00]. In particular, see theorems (246) – (247) – (248) – (249).

Now we see two results that, taken together, give a slighty stronger version of theorem (248) of [HW00]. They also improve theorem (2.4.1), at least for positive values of m.

The first result is:

Theorem 2.4.2. *The domain $h\big(\sqrt{m}\,\big)$ is norm-euclidean for the following values of m:*

$$m = 2,\ 3,\ 6,\ 7,\ 11.$$

Proof. Note that in what follows is $h\big(\sqrt{m}\,\big) = \mathbb{Z}\big[\sqrt{m}\,\big]$ since every m here is $\not\equiv 1 \pmod 4$. Argue by contradiction, assuming that $h\big(\sqrt{m}\,\big)$ is not norm-euclidean. Then it's easy to see that there must exist $r, s \in \mathbb{Q}$ such that:

$$\forall\, x, y \in \mathbb{Z}: \quad \big|(r-x)^2 - m(s-y)^2\big| \geq 1 \tag{2.6}$$

First, note that the expression $E(x,y,r,s) := \left|(r-x)^2 - m(s-y)^2\right|$ is unaltered by the substitution:

$$\varrho : \begin{cases} r \mapsto \epsilon_1 r + u \\ x \mapsto \epsilon_1 x + u \\ s \mapsto \epsilon_2 s + v \\ y \mapsto \epsilon_2 y + v \end{cases} \tag{2.7}$$

where $\epsilon_1, \epsilon_2 \in \{+1, -1\}$ and u, v are arbitrary integers, Moreover (and this is a fundamental fact), if x, y run over all the rational integers, $\varrho(x)$ and $\varrho(y)$ do the same.
At this point it's clear that we can suppose without loss of generality that $0 \le r \le \frac{1}{2}$ and $0 \le s \le \frac{1}{2}$ (since for every $q \in \mathbb{Q}$ there exist $\epsilon \in \{+1, -1\}$ and $z \in \mathbb{Z}$ such that $0 \le z + \epsilon q \le \frac{1}{2}$).
Now, from (2.6) it derives that for every $x, y \in \mathbb{Z}$ one of the following statements must hold:

$$[P(x,y)] : \quad (r-x)^2 \ge 1 + m(s-y)^2 \tag{2.8}$$

$$[N(x,y)] : \quad m(s-y)^2 \ge 1 + (r-x)^2 \tag{2.9}$$

Some particular inequalities which we shall use are:

$$\begin{array}{llll} [P(0,0)] : & r^2 \ge 1 + ms^2 & [N(0,0)] : & ms^2 \ge 1 + r^2 \\ [P(1,0)] : & (1-r)^2 \ge 1 + ms^2 & [N(1,0)] : & ms^2 \ge 1 + (1-r)^2 \\ [P(-1,0)] : & (1+r)^2 \ge 1 + ms^2 & [N(-1,0)] : & ms^2 \ge 1 + (1+r)^2 \end{array}$$

We know that one inequality at least in each of these pair of inequalities is true; we also know that $0 \le r \le \frac{1}{2}$ and $0 \le s \le \frac{1}{2}$.
First, if $r = s = 0$, then $P(0,0)$ and $N(0,0)$ are both false, so this possibility is excluded. Moreover we have:

$$1 \le 1 + ms^2 \quad \text{and} \quad r^2 \le \frac{1}{4}$$

so that $P(0,0)$ is false. But also $P(0,1)$ is false, because from it derives:

$$1 \ge (1-r)^2 \ge 1 + ms^2 \ge 1 \implies \begin{cases} 1 + ms^2 = 1 \\ (1-r)^2 = 1 \end{cases} \implies r = s = 0$$

a possibility already excluded.
Thus it's assured that $P(0,0)$ and $P(1,0)$ are both false, so that $N(0,0)$ and $N(1,0)$ are true. If $P(-1,0)$ were true, then $N(1,0)$ and $P(-1,0)$ combined would give:

$$(1+r)^2 \ge 1 + ms^2 \ge 2 + (1-r)^2 \implies 4r \ge 2 \implies r \ge \frac{1}{2}$$

so that $r = \frac{1}{2}$, and consequentely:

$$\frac{9}{4} = (1+r)^2 \geq 1 + ms^2 \geq 2 + (1-r)^2 = \frac{9}{4} \implies 1 + ms^2 = \frac{9}{4} \implies ms^2 = \frac{5}{4}$$

But this is impossible, since writing $s = \frac{p}{q}$, for $p, q \in \mathbb{N}$ coprime, it would give:

$$4mp^2 = 5q^2 \implies p^2 \mid 5 \implies p = 1 \implies 5q^2 = 4m \implies 5 \mid m$$

with $m = 2$, 3, 6, 7 or 11, a contradiction.

We have thus proved that $P(-1,0)$ is false, so that $N(-1,0)$ holds. This gives:

$$ms^2 \geq 1 + (1+r)^2 \geq 2 \tag{2.10}$$

and so, since $s^{-2} \geq 4$:

$$m \geq 2s^{-2} \geq 8$$

so that the only case we have to deal with from now on is $m = 11$.

Let us consider the inequalities:

$$[P(2,0)] \ : \ (2-r)^2 \geq 1 + 11s^2 \qquad [N(2,0)] \ : \ 11s^2 \geq 1 + (2-r)^2$$

We know that at least one of them must hold. But $N(2,0)$ is false, since it implies:

$$11s^2 \geq 1 + (2-r)^2 \geq 1 + \left(2 - \frac{1}{2}\right)^2 = 1 + \left(\frac{3}{2}\right)^2 = \frac{13}{4} \implies 11 \geq s^{-2} \cdot \frac{13}{4} \geq 13,$$

a contradiction. So $P(2,0)$ is true, i.e. : $(2-r)^2 \geq 1 + ms^2$.

From this and from (2.10) we deduce $(2-r)^2 \geq 1 + 11s^2 \geq 2 + (1+r)^2$, and so:

$$2 \leq (2-r)^2 - (1+r)^2 = 3 - 6r \implies -6r \geq -1$$

i.e. :

$$r \leq \frac{1}{6} \tag{2.11}$$

Let us now consider the inequalities:

$$[P(-2,1)] \ : \ (2+r)^2 \geq 1 + 11(1-s)^2 \qquad [N(-2,1)] \ : \ 11(1-s)^2 \geq 1 + (2+r)^2$$

We know that at least one of them must hold. If this were $N(-2,1)$, we would have:

$$11(1-s)^2 \geq 1 + (2+r)^2 \geq 5 \implies 1 - s \geq \sqrt{\frac{5}{11}} \implies s \leq 1 - \sqrt{\frac{5}{11}} < \frac{1}{3}.$$

But then, from (2.10) would derive:

$$1+\frac{11}{9}=1+11\cdot\left(\frac{1}{3}\right)^2>1+11s^2\geq 2+(1+r)^2\geq 3\implies \frac{20}{9}\geq 3,$$

a contradiction.

Thus $N(-2,1)$ is false, so that $P(-2,1)$ must hold, i.e. :

$$(2+r)^2\geq 1+11(1-s)^2 \tag{2.12}$$

Now we must consider the two following further inequalities:

$$[P(2,1)]\ :\ (2-r)^2\geq 1+11(1-s)^2 \qquad [N(2,1)]\ :\ 11(1-s)^2\geq 1+(2-r)^2$$

Again, we know that at least one of them must hold. If $N(2,1)$ were hold, we'd get from (2.12):

$$(2+r)^2\geq 1+11(1-s)^2\geq 2+(2-r)^2\implies 4+4r+r^2\geq 2+4-4r+r^2\implies 8r\geq 2$$

and so $r\geq\frac{1}{4},$ which contradicts (2.11).

Thus $P(2,1)$ holds, and so, being $1-s\geq\frac{1}{2}\,,$ we obtain:

$$(2-r)^2\geq 1+11(1-s)^2\geq 1+\frac{11}{4}=\frac{15}{4}\implies 2-r\geq\frac{\sqrt{15}}{2}\implies r\leq\frac{4-\sqrt{15}}{2}<\frac{1}{15}.$$

So we have a further upper bound for r:

$$r<\frac{1}{15} \tag{2.13}$$

From (2.12) we deduce now:

$$1+11(1-s)^2\leq(2+r)^2<(2+\frac{1}{15})=\left(\frac{31}{15}\right)^2\implies(1-s)^2<\frac{1}{11}\left(\left(\frac{31}{15}\right)^2-1\right)$$

so that, since $(0.55)^2\geq\left(\frac{\left(\frac{31}{15}\right)^2-1}{11}\right),$ we have the following lower bound for s:

$$1-s<0.55\implies s>0.45 \tag{2.14}$$

Finally, let us consider the following pairs of inequalities:

$$[P(5,-1)]\ :\ (5-r)^2\geq 1+11(1+s)^2 \qquad [N(5,-1)]\ :\ 11(1+s)^2\geq 1+(5-r)^2$$

If $P(5,-1)$ were true, we would get from (2.14):

$$20.25=\frac{81}{4}=\left(5-\frac{1}{2}\right)^2\geq(5-r)^2\geq 1+11(1+s)^2>1+11\cdot(1.45)^2=24.1275,$$

a contradiction. So $N(5,-1)$ must hold. Using (2.13), we get then:

$$\frac{99}{4} = 11\left(1+\frac{1}{2}\right)^2 \geq 11(1+s)^2 \geq 1+(5-r)^2 > 1+\left(5-\frac{1}{15}\right)^2 = \frac{5701}{225}$$

so that $22275 = 99 \cdot 225 > 4 \cdot 5701 = 22804,$ a contradiction.

Thus we can eventually conclude that also $h\big(\sqrt{11}\,\big) = \mathbb{Z}\big[\sqrt{11}\,\big]$ is norm-euclidean, and the theorem is proved. □

Now we can see an analogue of the previous theorem for the case $m \equiv 1 \pmod 4$. The argumentations will be very similar.

Theorem 2.4.3. *The domain $h\big(\sqrt{m}\,\big)$ is norm-euclidean for the following values of m:*

$$m \;=\; 5,\ 13,\ 17,\ 21,\ 29,\ 33,\ 37,\ 41.$$

Proof. First note that here every m here is $\equiv 1 \pmod 4$, so that:

$$h\big(\sqrt{m}\,\big) = \left\{ \frac{(2x+y)+y\sqrt{m}}{2} \,:\, x,y \in \mathbb{Z} \right\}.$$

We'll argue by contradiction, assuming that $h\big(\sqrt{m}\,\big)$ is not norm-euclidean.
Then it's easy to see that, written $n := \frac{1}{4}m,$ must exist $r,s \in \mathbb{Q}$ such that:

$$\forall\, x,y \in \mathbb{Z}: \quad \left| \left(r-x-\frac{y}{2}\right)^2 - n(s-y)^2 \right| \geq 1 \tag{2.15}$$

(to prove this, write the generic element $\tau \in \mathbb{Q}\big(\sqrt{m}\,\big)$ as $\tau = r + \frac{1}{2}s\sqrt{m},$ with $r,s \in \mathbb{Q}$)
First, note that the expression $E(x,y,r,s) := \left|\left(r-x-\frac{y}{2}\right)^2 - n(s-y)^2\right|$ is unaltered by any of the following four substitutions:

$$\varrho_1 : \begin{cases} r \mapsto \epsilon r + u \\ x \mapsto \epsilon x + u \\ s \mapsto s \\ y \mapsto y \end{cases} \tag{2.16}$$

$$\varrho_2 : \begin{cases} r \mapsto r \\ x \mapsto x - v \\ s \mapsto s + 2v \\ y \mapsto y + 2v \end{cases} \tag{2.17}$$

$$\varrho_3 : \begin{cases} r \mapsto r \\ x \mapsto x + y \\ s \mapsto -s \\ y \mapsto -y \end{cases} \tag{2.18}$$

$$\varrho_4 : \begin{cases} r \mapsto \frac{1}{2} - r \\ x \mapsto -x \\ s \mapsto 1 - s \\ y \mapsto 1 - y \end{cases} \tag{2.19}$$

where $\epsilon \in \{+1, -1\}$ and u, v are arbitrary integers. Moreover (and this is a fundamental fact), for any of the transormations σ_i given above, if x, y run over all the rational integers, $\varrho_i(x)$ and $\varrho_i(y)$ do the same.

Now, using this observation, we're going now to prove that it can be assumed without loss of generality that $0 \leq r \leq \frac{1}{2}$ and $0 \leq s \leq \frac{1}{2}$.

We firt use ϱ_1 to make $0 \leq r \leq \frac{1}{2}$, then ϱ_2 to make $-1 \leq s \leq 1$; and then, if necessary, ϱ_3 to make $0 \leq s \leq 1$. If $0 \leq s \leq \frac{1}{2}$, the reduction is completed. On the other hand, if $\frac{1}{2} \leq s \leq 1$, we end by using ϱ_4, as we can do because $\frac{1}{2} - r$ lies between 0 and $\frac{1}{2}$ if r does so.

Now, from (2.15) it derives that for every $x, y \in \mathbb{Z}$ one of the following statements must hold:

$$[P(x,y)] \; : \quad \left(r - x - \frac{y}{2}\right)^2 \geq 1 + n(s-y)^2 \tag{2.20}$$

$$[N(x,y)] \; : \quad n(s-y)^2 \geq 1 + \left(r - x - \frac{y}{2}\right)^2 \tag{2.21}$$

Some particular inequalities which we shall use are:

$$\begin{array}{llll} [P(0,0)] \; : & r^2 \geq 1 + ns^2 & [N(0,0)] \; : & ns^2 \geq 1 + r^2 \\ [P(1,0)] \; : & (1-r)^2 \geq 1 + ns^2 & [N(1,0)] \; : & ns^2 \geq 1 + (1-r)^2 \\ [P(-1,0)] \; : & (1+r)^2 \geq 1 + ns^2 & [N(-1,0)] \; : & ns^2 \geq 1 + (1+r)^2 \end{array}$$

We know that one inequality at least in each of these pair of inequalities is true; we also know that $0 \leq r \leq \frac{1}{2}$ and $0 \leq s \leq \frac{1}{2}$.

First, if $r = s = 0$, then $P(0,0)$ and $N(0,0)$ are both false, so this possibility is excluded. Moreover we have:

$$1 \leq 1 + ns^2 \quad \text{and} \quad r^2 \leq \frac{1}{4}$$

so that $P(0,0)$ is false. But also $P(1,0)$ is false, because from it derives:

$$1 \geq (1-r)^2 \geq 1 + ns^2 \geq 1 \implies \begin{cases} 1 + ns^2 &= 1 \\ (1-r)^2 &= 1 \end{cases} \implies r = s = 0$$

a possibility already excluded.

Thus it's assured that $P(0,0)$ and $P(1,0)$ are both false, so that $N(0,0)$ and $N(1,0)$ are true. If $P(-1,0)$ were true, then $N(1,0)$ and $P(-1,0)$ combined would give:

$$(1+r)^2 \geq 1 + ns^2 \geq 2 + (1-r)^2 \implies 4r \geq 2 \implies r \geq \frac{1}{2}$$

so that $r = \frac{1}{2}$, and consequentely:

$$\frac{9}{4} = (1+r)^2 \geq 1 + ns^2 \geq 2 + (1-r)^2 = \frac{9}{4} \implies 1 + ns^2 = \frac{9}{4} \implies ns^2 = \frac{5}{4}$$

But this is impossible, since writing $s = \frac{p}{q}$, for $p, q \in \mathbb{N}$ coprime, it would give:

$$mp^2 = 4np^2 = 5q^2 \implies p^2 \mid 5 \implies p = 1 \implies 5q^2 = m \implies 5 \mid m$$

with $m = 5$, 13, 17, 21, 29, 33, 37 or 41, so that:

$$m = 5 \implies q^2 = 1 \implies p = q = 1 \implies s = \frac{p}{q} = 1,$$

a contradiction.

We have thus proved that $P(-1,0)$ is false, so that $N(-1,0)$ holds. This gives:

$$ns^2 \geq 1 + (1+r)^2 \geq 2 \tag{2.22}$$

and so, since $s^{-2} \geq 4$:

$$\frac{1}{4}m = n \geq 2s^{-2} \geq 8 \implies m \geq 4 \cdot 8 = 32,$$

Thus, from now on, we have only to deal with the cases $m = 33$ or $m = 37$ or $m = 41$, so that it is surely:

$$33 \leq m \leq 41 \quad \text{i.e.} \quad \frac{33}{4} \leq n \leq \frac{41}{4} \tag{2.23}$$

From the inequality (2.22) we immediately get:

$$\frac{41}{4}s^2 \geq ns^2 \geq 1 + (1+r)^2 \geq 2 \implies s^2 \geq \frac{8}{41} \implies s \geq \sqrt{\frac{8}{41}} > 0.4417$$

so that:

$$s > 0.4417 \tag{2.24}$$

and:

$$(1+r)^2 \leq ns^2 - 1 \leq \frac{41}{4} \cdot \left(\frac{1}{2}\right)^2 - 1 = \frac{25}{16} \implies 1 + r \leq \frac{5}{4}$$

so that:

$$r \leq \frac{1}{4} = 0.25 \tag{2.25}$$

Consider now the inequality:

$$[P(-1,1)] \; : \; \left(1 - \frac{1}{2} - r\right)^2 \geq 1 + n(1-s)^2$$

If it were true, we would get:

$$\left(\frac{1}{2} + r\right)^2 \geq 1 + n(1-s)^2 \geq 1 + n\left(\frac{1}{2}\right)^2 = 1 + \frac{1}{4}n \geq 1 + \frac{1}{4} \cdot \frac{33}{4} = \frac{49}{16} = \left(\frac{7}{4}\right)^2$$

so that:

$$1 = \frac{1}{2} + \frac{1}{2} \geq \frac{1}{2} + r \geq \frac{7}{4}$$

a contradiction.

Then $N(-1,1)$ must hold, i.e. :

$$n(1-s)^2 \geq 1 + \left(\frac{1}{2} + r\right)^2 \tag{2.26}$$

Consider then the following inequality:

$$[P(1,1)] \; : \; \left(1 + \frac{1}{2} - r\right)^2 \geq 1 + n(1-s)^2$$

If it were true as a strict inequality, we would get from (2.26):

$$\left(\frac{3}{2} - r\right)^2 > 1 + n(1-s)^2 \geq 2 + \left(\frac{1}{2} + r\right)^2 \implies \frac{9}{4} - 3r + r^2 > 2 + \frac{1}{4} + r + r^2$$

so that:

$$-4r > 2 + \frac{1}{4} - \frac{9}{4} = 0 \implies r < 0$$

a contradiction. Then, if $P(1,1)$ holds, it must be $\left(\frac{3}{2} - r\right)^2 = 1 + n(1-s)^2$. Moreover, if (2.26) were true as a strict inequality, we would have:

$$\left(\frac{3}{2} - r\right)^2 = 1 + n(1-s)^2 > 2 + \left(\frac{1}{2} + r\right)^2$$

from which can be deduced exactly as above that $r < 0$, a contradiction. So, if $P(1,1)$ holds, it must be:

$$\left(\frac{3}{2} - r\right)^2 = 1 + n(1-s)^2 \quad \text{and} \quad n(1-s)^2 = 1 + \left(\frac{1}{2} + r\right)^2$$

so that:

$$\left(\frac{3}{2}-r\right)^2 = 2+\left(\frac{1}{2}+r\right)^2 \implies r=0 \implies n(1-s)^2 = 1+\left(\frac{1}{2}+r\right)^2 = \frac{5}{4}$$

from which we can finally deduce, using also (2.23):

$$(1-s)^2 = \frac{5}{4n} = \frac{5}{m} \leq \frac{5}{33} \implies 1-s = \sqrt{\frac{5}{33}} < 0.4 \implies s > 1-0.4 = 0.6 > \frac{1}{2}$$

again a contradiction.

Thus is now proved that $P(1,1)$ can't hold, so that $N(1,1)$ certainly holds, i.e. :

$$n(1-s)^2 \geq 1+\left(\frac{3}{2}-r\right)^2 \tag{2.27}$$

Finally, consider the inequality:

$$[P(-2,1)] \ : \ \left(2-\frac{1}{2}-r\right)^2 \geq 1+n(1-s)^2$$

If it were true, we would get from (2.27):

$$\left(\frac{3}{2}+r\right)^2 = \left(2-\frac{1}{2}-r\right)^2 \geq 1+n(1-s)^2 \geq 2+\left(\frac{3}{2}-r\right)^2$$

so that:

$$\frac{9}{4}+3r+r^2 \geq 2+\frac{9}{4}-3r+r^2 \implies 6r \geq 2 \implies r \geq \frac{1}{3} > \frac{1}{4}$$

which contradicts (2.25). Thus $N(-2,1)$ must hold, i.e. :

$$n(1-s)^2 \geq 1+\left(\frac{3}{2}+r\right)^2 \tag{2.28}$$

From this inequality we finally deduce:

$$\frac{m}{4}(1-s)^2 = n(1-s)^2 \geq 1+\left(\frac{3}{2}+r\right)^2 \geq 1+\frac{9}{4} = \frac{13}{4}$$

which, togheter with (2.24), lead us to the conclusive desired contradiction:

$$13 \leq m(1-s)^2 \leq 41(1-s)^2 < 41(1-0.4417)^2 = 12.77965449$$

□

Chapter 3

Some non-UFDs of algebraic integers

3.1 Some normed complex domains that are not an UFD

In this section, we'll give a quite general condition on $m > 0$ which ensure that $h\left(\sqrt{-m}\right)$ or $\mathbb{Z}\left[\sqrt{-m}\right]$ is not an UFD.

Let's start with a proposition about $\mathbb{Z}\left[\sqrt{-m}\right]$:

Theorem 3.1.1. *If $m \in \mathbb{Z}$ a composite number such that $m > 1$, then $\mathbb{Z}\left[\sqrt{-m}\right]$ is not an UFD.*

Proof. Let p the smallest prime number with $p \mid m$, and let $m = ph$, with $h \in \mathbb{N} \setminus \{0\}$. Since m is composite, of course $p < m \implies h > 1 \implies m = ph \geq p^2$ (as follows easily from the minimality of p).
Now, in $\mathbb{Z}\left[\sqrt{-m}\right]$ we clarly have:

$$\left(\sqrt{-m}\right)^2 = -m = p \cdot (-h)$$

so that in $\mathbb{Z}\left[\sqrt{-m}\right]$ is $p \mid \left(\sqrt{-m}\right)^2$ but $p \nmid \sqrt{-m}$ (as one can immediately check observing that the equality $\sqrt{-m} = p(a + b\sqrt{-m})$, $a, b \in \mathbb{Z}$ would imply $pb = 1 \implies p \mid 1$, a contradiction).
So if we prove that p is irreducible in $\mathbb{Z}\left[\sqrt{-m}\right]$ we also immediately get that $\mathbb{Z}\left[\sqrt{-m}\right]$ is not an UFD.
Argue by contradiction, assuming that $p = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}\left[\sqrt{-m}\right]$ not units (i.e. such that $\mathcal{N}(\alpha) > 1$ and $\mathcal{N}(\beta) > 1$). Then, writing $\alpha = \left(a + b\sqrt{-m}\right)$ and $\beta = \left(c + d\sqrt{-m}\right)$ for $a, b, c, d \in \mathbb{Z}$, we obtain:

$$m \geq p^2 = \mathcal{N}(p) = \mathcal{N}(\alpha)\mathcal{N}(\beta) > \mathcal{N}(\alpha) = a^2 + b^2 m \geq b^2 m$$

so that:

$$b^2 m < m \implies b = 0.$$

It can also be proved in an identical manner that $d = 0$, so that $p = ac$, with $a, c \in \mathbb{Z}$, which implies $a = \pm 1$ or $c = \pm 1$ since p is prime in $\mathbb{Z}$.
But then also $\alpha = \pm 1$ or $\beta = \pm 1$, a contradiction as α and β are not units. □

Since $h\big(\sqrt{-m}\big) = \mathbb{Z}\big[\sqrt{-m}\,\big]$ if $m \equiv 1$ or $2 \pmod 4$, we immediately have the following result:

Corollary 3.1.2. *If $m > 1$ is a composite squarefree integer with $m \equiv 1$ or $2 \pmod 4$, then $h\big(\sqrt{-m}\big)$ is not an UFD.*

A similar result holds also for $m \equiv 3 \pmod 4$:

Theorem 3.1.3. *If $m > 1$ is a composite squarefree integer with $m \equiv 3 \pmod 4$, then $h\big(\sqrt{-m}\big)$ is not an UFD.*

Proof. As in the proof of previous theorem, let p the smallest prime number such that $p \mid m$, and write $m = pH$ for $H \in \mathbb{N} \setminus \{0\}$; then we easily get $p^2 \geq m$.
Again, in $h\big(\sqrt{-m}\big)$ we have:

$$\big(\sqrt{-m}\big)^2 = -m = p \cdot (-H)$$

so that in $h\big(\sqrt{-m}\big)$ is $p \mid \big(\sqrt{-m}\big)^2$. But in $h\big(\sqrt{-m}\big)$ is also $p \nmid \sqrt{-m}$, since the assumption $p \mid \sqrt{-m}$ would imply that for suitable $a, b \in \mathbb{Z}$ is[1]:

$$\sqrt{-m} = p\left(\frac{a + b\sqrt{-m}}{2}\right) \implies 2 = pb \implies b = 1 \text{ and } p = 2$$

so that, since $p \mid m$, m must be even, which contradicts the hypothesis that $m \equiv 3 \pmod 4$.
So our aim is now to show that p is irreducible in $h\big(\sqrt{-m}\big)$.
Let

$$p = \left(\frac{a + b\sqrt{-m}}{2}\right)\left(\frac{c + d\sqrt{-m}}{2}\right) \tag{3.1}$$

for $a, b, c, d \in \mathbb{Z}$ with $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$. We want first to show that $b = 0$ or $d = 0$. Argue by contradiction assuming $b \neq 0 \neq d$. If we write $A := |bd|$, it results then $A \geq 1$, and:

$$A^2 m^2 = 16m^2 \cdot \frac{b^2}{4} \cdot \frac{d^2}{4} \leq 16\left(\frac{a^2 + b^2 m}{4}\right)\left(\frac{c^2 + d^2 m}{4}\right) = 16\mathcal{N}(p) = 16p^2 \tag{3.2}$$

[1] in fact, it must be also $a \equiv b \pmod 2$, but this is of no importance here.

from which, being $p^4 \leq A^2p^4 \leq A^2m^2$, derives immediately:

$$p^4 \leq 16p^2 \implies p^2 \leq 16 \implies p \leq 4 \implies p = 2 \text{ or } 3.$$

Finally, since $p \mid m$ and m odd, we have $p = 3$.
From inequality (3.2), recalling that $m = pH = 3H$, we have now:

$$16 \cdot 3^2 = 16p^2 \geq A^2m^2 = A^2 \cdot 3^2H^2 \implies (AH)^2 \leq 16 \implies H \leq AH \leq 4$$

from which the possibilities: $H = 1, 2, 3$ or 4.
But since m is odd it is $2 \neq H \neq 4$, since m is squarefree it is $H \neq p = 3$ and since m is composite it is $H \neq 1$, so that we get the desired contradiction which lead us to deduce that $b = 0$ or $d = 0$.
At this point it's clear that we can suppose without loss of generality that $b = 0$; thus, since $a \equiv b \pmod 2$, it results $a = 2r$, $r \in \mathbb{Z} \setminus \{0\}$.
The equation (3.1) becomes now:

$$2p = cr + dr\sqrt{-m}$$

from which, since $r \neq 0$, immediatly derives that $d = 0$ and so, being $c \equiv d \pmod 2$, that $c = 2s$ for an appropriate $s \in \mathbb{Z}$
Thus we finally have:

$$2p = cr = 2sr \implies p = sr \implies r = \pm 1 \text{ or } s = \pm 1$$

and then:

$$\frac{a + b\sqrt{-m}}{2} = r = \pm 1 \quad \text{or} \quad \frac{c + d\sqrt{-m}}{2} = s = \pm 1$$

which proves that p is irreducible in $h\big(\sqrt{-m}\big)$, so that we can conclude that $h\big(\sqrt{-m}\big)$ is not an UFD. □

Summarizing the two propositions (3.1.2) and (3.1.3) we get the following:

Theorem 3.1.4. *If $m > 1$ is a composite squarefree integer then $h\big(\sqrt{-m}\big)$ is not an UFD.*

For the domains $\mathbb{Z}\big[\sqrt{-m}\,\big]$ there is another severe limitation to the possibility of being UFD:

Theorem 3.1.5. *If $m > 1$ is an odd integer, then $\mathbb{Z}\big[\sqrt{-m}\,\big]$ is not an UFD.*

Proof. Let us first show that 2 is irreducible in $\mathbb{Z}\left[\sqrt{-m}\right]$. Argue by contradiction, assuming that: $2 = \alpha\beta = \left(a + b\sqrt{-m}\right)\left(c + d\sqrt{-m}\right)$ with α, β not units in $\mathbb{Z}\sqrt{-m}$ (i.e. such that $\mathcal{N}(\alpha) > 1$ and $\mathcal{N}(\beta) > 1$). We get immediately:

$$4 = \mathcal{N}(\alpha)\mathcal{N}(\beta) \implies \mathcal{N}(\alpha) = \mathcal{N}(\beta) = 2 \implies a^2 + mb^2 = 2$$

If would be $b \neq 0$, then we should have $b^2 \geq 1$ and so $2 = a^2 + mb^2 \geq mb^2 \geq m \geq 3$, contradiction. So it is $b = 0 \implies a^2 = 2$, again a contradiction. Thus we can conclude that 2 is irreducible in $\mathbb{Z}\left[\sqrt{-m}\right]$.
Since m is odd, we have now that in $\mathbb{Z}\left[\sqrt{-m}\right]$ is:

- $2 \nmid \left(1 + \sqrt{-m}\right)$
- $2 \nmid \left(1 - \sqrt{-m}\right)$
- $2 \mid (1 + m) = \left(1 + \sqrt{-m}\right) \cdot \left(1 - \sqrt{-m}\right)$

which, together with the irreducibility of 2, proves that $\mathbb{Z}\left[\sqrt{-m}\right]$ is not an UFD. □

Again, since $h\left(\sqrt{-m}\right) = \mathbb{Z}\left[\sqrt{-m}\right]$ for $m \equiv 1 \pmod 4$, we immediately get:

Corollary 3.1.6. *If $m > 1$ is a squarefree odd integer such that $m \equiv 1 \pmod 4$, then $h\left(\sqrt{-m}\right)$ is not an UFD.*

We can give now a "definitive" result on the complex normed domains of the form $\mathbb{Z}\left[\sqrt{-m}\right]$:

Theorem 3.1.7. *If m is a positive integer, then $\mathbb{Z}\left[\sqrt{-m}\right]$ is an UFD if and only if $m = 1$ or $m = 2$.*

Proof. From theorem (2.4.1) of chapter 2 we know that $\mathbb{Z}\left[\sqrt{-1}\right]$ and $\mathbb{Z}\left[\sqrt{-2}\right]$ are UFDs.
On the contrary, if $m > 2$, it can be:

- m even and $m > 2$, so that m is composite and then $\mathbb{Z}\left[\sqrt{-m}\right]$ is not UFD by theorem (3.1.1), or:
- $m > 1$ and m odd, so that $\mathbb{Z}\left[\sqrt{-m}\right]$ not an UFD by theorem (3.1.6),

and $\mathbb{Z}\left[\sqrt{-m}\right]$ can't be an UFD in either case. □

Since $h\left(\sqrt{-m}\right) = \mathbb{Z}\left[\sqrt{-m}\right]$ when $m \equiv 1$ or $2 \pmod 4$, a trivial implication of the previous result is:

Corollary 3.1.8. *If $m > 2$ is a squarefree integer such that $m \equiv 1$ or $2 \pmod 4$, then $h\big(\sqrt{-m}\big)$ is not an UFD.*

The following proposition is very easy to prove too, using the previous corollary and the theorem (3.1.4):

Theorem 3.1.9. *If $m > 1$ is a squarefree integer such that $h\big(\sqrt{-m}\big)$ is an UFD, then $m = 2$ or m is prime and $m \equiv 3 \pmod 4$.*

The previous theorem can be greatly strengthened, leading to the following result:

Theorem 3.1.10. *Let $p > 3$ be an odd prime with $p \equiv 3 \pmod 4$, and suppose that there exist a prime $q < \frac{p}{4}$ such that $-p$ is a quadratic residue of $4q$; then $h\big(\sqrt{-p}\big)$ is not an UFD.*

Proof. Let $z \in \mathbb{Z}$ such that:

$$z^2 \equiv -p \pmod{4q}. \tag{3.3}$$

Then it's clearly $z \equiv 1 \pmod 2$, so that we have $\alpha := \left(\frac{1+z\sqrt{-p}}{2}\right) \in h\big(\sqrt{-p}\big)$. From (3.3) we have $\mathcal{N}(\alpha) = \frac{1}{4}(z^2+p) \in \mathbb{Z}$ and $q \mid \mathcal{N}(\alpha)$ in $\mathbb{Z}$, and thus, *a fortiori*, $q \mid \mathcal{N}(\alpha) = \alpha\overline{\alpha}$ in $h\big(\sqrt{-p}\big)$. But since $1 \not\equiv 0 \pmod q$, we immediately have $q \nmid \alpha$ and $q \nmid \overline{\alpha}$. Then, to prove that $h\big(\sqrt{-p}\big)$ is not an UFD, we have only to show that q is irreducible in $h\big(\sqrt{-p}\big)$.
Argue by contradiction, assuming that $q = \beta\gamma$ for $\beta, \gamma \in h\big(\sqrt{-p}\big)$ not units, i.e. such that $\mathcal{N}(\beta) > 1, \mathcal{N}(\gamma) > 1$. From this, since q is prime, we deduce:

$$q^2 = \mathcal{N}(q) = \mathcal{N}(\beta\gamma) = \mathcal{N}(\beta)\mathcal{N}(\gamma) \implies \mathcal{N}(\beta) = \mathcal{N}(\gamma) = q$$

Writing now $\beta = \frac{a+b\sqrt{-p}}{2}$ for suitable $a, b \in \mathbb{Z}$ with $a \equiv b \pmod 2$, it results, supposing $b \neq 0$:

$$4q = 4\mathcal{N}(\beta) = a^2 + pb^2 \geq pb^2 > 4qb^2 \implies b^2 < 1 \implies b = 0$$

so that we surely have $b = 0$. But then $a^2 = 4q$, which, being q prime, is a contradiction. □

As consequence of previous theorem we have:

Corollary 3.1.11. *Let $p > 3$ be an odd prime such that $p \equiv 3 \pmod 4$ and such that $h\big(\sqrt{-p}\big)$ is an UFD; then there exists a prime q such that $p = 4q - 1$. In particular, it must be $p = 7$ (if $q = 2$) or $p \equiv 3 \pmod 8$ (if q odd).*

Proof. Argue by contradiction, assuming that $\frac{1}{4}(p+1)$ – which is an integer since $p \equiv 3 \pmod 4$ and greater than 1 since $p > 3$ – is composite, and let r be one of its prime divisors. Then we can write $\frac{1}{4}(p+1) = rA$ for $A \in \mathbb{N}$, $A > 1$, from which we deduce:

- $\frac{1}{4}(p+1) = rA \geq 2r \implies r \leq \frac{1}{8}(p+1) < \frac{1}{8} \cdot 2p \implies r < \frac{1}{4}p$
- $r \,\big|\, \frac{1}{4}(p+1) \implies 4r \mid (p+1)$

We have then:

$$-p \equiv 1^2 \pmod{4r}, \quad 1 < r < \frac{1}{4}p, \quad r \text{ prime}$$

so that, by theorem (3.1.10), we have immediately that $h\big(\sqrt{-p}\big)$ is not an UFD, a contradiction. □

Finally, we can see an immediate consequence of previous result:

Corollary 3.1.12. *Let $1 < p < 200$ be a prime such that $h\big(\sqrt{-p}\big)$ is an UFD; then p must be one of the following numbers:*

$$2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163$$

Proof. The only p primes with $p < 200$ such that $p \leq 7$ or $p \equiv 3 \pmod 8$ are:

$$2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 59,\ 67,\ 83,\ 107,\ 131,\ 139,\ 163,\ 179$$

Moreover:

- $\frac{59+1}{4} = 15 = 3 \cdot 5$
- $\frac{83+1}{4} = 21 = 3 \cdot 7$
- $\frac{107+1}{4} = 27 = 3^3$
- $\frac{131+1}{4} = 33 = 3 \cdot 11$
- $\frac{139+1}{4} = 35 = 5 \cdot 7$
- $\frac{179+1}{4} = 45 = 3^2 \cdot 5$

Thus our claim follows immediately from corollary (3.1.11). □

3.2 Some normed real domains that are not UFD

In this section, we'll give a quite general condition on $m > 0$ ensuring that $h\big(\sqrt{m}\big)$ or $\mathbb{Z}\big[\sqrt{m}\big]$ is not an UFD.
The results that we'll can obtain about real domains will be weaker then those found about complex domains, and our proofs will be obiouvsly more elaborated.

Let's start with a proposition about $\mathbb{Z}\big[\sqrt{m}\big]$:

Theorem 3.2.1. *Let $m > 1$ be a non-square integer, and suppose that there exists a prime p such that:*

- *$\pm p$ are both quadratic non-residues of m;*
- *m is a quadratic residue of p.*

Then $\mathbb{Z}\big[\sqrt{m}\big]$ is not an UFD.

Proof. By hypothesis we can find $t \in \mathbb{Z}$ such that $t^2 \equiv m \pmod{p} \implies p \mid (t^2 - m) = (t + \sqrt{m})(t - \sqrt{m})$, but $p \nmid (t + \sqrt{m})$ and $p \nmid (t - \sqrt{m})$ (as one can immediately check observing that the equality: $t \pm \sqrt{m} = p(a + b\sqrt{m})$, $a, b \in \mathbb{Z}$ would imply $pb = \pm 1 \implies p \mid 1$, a contradiction). So, if p is irreducible in $\mathbb{Z}\big[\sqrt{m}\big]$, this domain can't be an UFD.
Argue by contradiction, assuming that $p = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}\big[\sqrt{m}\big]$ not units, i.e. such that $\mathcal{N}(\alpha) > 1$, $\mathcal{N}(\beta) > 1$. If $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$, we get then, for an appropriate choice of sign:

$$p^2 = \mathcal{N}(\alpha)\mathcal{N}(\beta) \implies \mathcal{N}(\alpha) = \mathcal{N}(\beta) = p \implies \pm p = \pm\mathcal{N}(\alpha) = a^2 - mb^2 \equiv a^2 \pmod{m},$$

a contradiction, as $\pm p$ are both quadratic non-residues of m. □

From previous result and from the equality $h\big(\sqrt{m}\big) = \mathbb{Z}\big[\sqrt{m}\big]$, holding for $m \equiv 2$ or $3 \pmod 4$, we immediately get:

Corollary 3.2.2. *Let $m > 1$ be a squarefree integer such that $m \equiv 2$ or $3 \pmod 4$, and suppose that there exists a prime p such that:*

- *$\pm p$ are both quadratic non-residues of m;*
- *m is a quadratic residue of p.*

Then $h\big(\sqrt{m}\big)$ is not an UFD.

A similar result holds also for $m \equiv 1 \pmod 4$:

Theorem 3.2.3. *Let $m > 1$ be a squarefree integer such that $m \equiv 1 \pmod 4$, and suppose that there exists a prime $p > 2$ such that:*

- *$\pm p$ are both quadratic non-residues of m;*
- *m is a quadratic residue of p.*

Then $h\big(\sqrt{m}\big)$ is not an UFD.

Proof. By hypothesis we can find $t \in \mathbb{Z}$ such that:

$$t^2 \equiv m \pmod p \implies p \mid (t^2 - m) = (t + \sqrt{m})(t - \sqrt{m}),$$

but $p \nmid (t+\sqrt{m})$ and $p \nmid (t-\sqrt{m})$, since the assumption $p \mid (t \pm \sqrt{m})$ would imply that for suitable $a, b \in \mathbb{Z}$ is[2]:

$$t \pm \sqrt{m} = p\left(\frac{a + b\sqrt{m}}{2}\right) \implies \pm 2 = pb \implies p \mid 2$$

which contradicts our assumption that $p > 2$.
So, in order to prove that $h\big(\sqrt{m}\big)$ is not an UFD, we have only to show that p is irreducible in $h\big(\sqrt{m}\big)$.
Argue by contradiction, assuming that $p = \alpha\beta$ with $\alpha, \beta \in h\big(\sqrt{m}\big)$ not units, i.e. such that $\mathcal{N}(\alpha) > 1$, $\mathcal{N}(\beta) > 1$. Writing $\alpha = \frac{a+b\sqrt{m}}{2}$, with $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$, we get then, for an appropriate choice of sign:

$$\begin{aligned} p^2 = \mathcal{N}(\alpha)\mathcal{N}(\beta) &\implies \mathcal{N}(\alpha) = \mathcal{N}(\beta) = p \\ &\implies \pm 4p = \pm 4\,\mathcal{N}(\alpha) = a^2 - mb^2 \equiv a^2 \pmod m \end{aligned}$$

Since $\text{g.c.d.}\,(m, 4) = 1$ (as m is odd), from the last congruence it immediately derives that at least one between $+p$ and $-p$ is a quadratic residue of m, which gives us the desired contradiction. □

Let's now see another useful general result about $\mathbb{Z}\big[\sqrt{m}\,\big]$:

Theorem 3.2.4. *If $m > 1$ is a non-square integer such that $m \equiv 1 \pmod 4$, then $\mathbb{Z}\big[\sqrt{m}\,\big]$ is not an UFD.*

Proof. Since m is odd, it results:

$$2 \mid (1 - m) = (1 + \sqrt{m})(1 - \sqrt{m})$$

while obiouvsy $2 \nmid (1 + \sqrt{m})$ and $2 \nmid (1 - \sqrt{m})$ in $\mathbb{Z}\big[\sqrt{m}\,\big]$. So, by proving that 2 is irreducible in $\mathbb{Z}\big[\sqrt{m}\,\big]$, we'll also prove that this domain is not an UFD.

[2] in fact, it must be also $a \equiv b \pmod 2$, but this is of no importance here.

Argue by contradiction, assuming that $2 = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}\left[\sqrt{m}\right]$ not units. Then $\mathcal{N}(\alpha) > 1$, $\mathcal{N}(\beta) > 1$, so that, writing $\alpha = a + b\sqrt{m}$ for $a, b \in \mathbb{Z}$, we obtain:

$$4 = \mathcal{N}(2) = \mathcal{N}(\alpha)\mathcal{N}(\beta) \implies \mathcal{N}(\alpha) = \mathcal{N}(\beta) = 2 \implies \pm 2 = a^2 - mb^2$$

From this equality, since m is odd, follows immediately that $a \equiv b \pmod 2$, and so that $a^2 \equiv b^2 \pmod 4$. But then:

$$2 \equiv \pm 2 = a^2 - mb^2 \equiv a^2 - b^2 \equiv 0 \pmod 4$$

a contradiction. □

Now we want to apply the results seen so far to three simple but concrete examples.

Example 1. Let $m = 10$, which is obiouvsly squarefree; since $10 \equiv 2 \pmod 4$, is

$$h\left(\sqrt{10}\right) = \mathbb{Z}\left[\sqrt{10}\right] = \left\{a + b\sqrt{10} : a, b \in \mathbb{Z}\right\}.$$

Moreover, $10 \equiv 0^2 \pmod 2$, while ± 2 are both quadratic non-residues of 10 (as one can immediatly check by direct calculations).
Since 2 is prime, by theorem (3.2.1), $h\left(\sqrt{10}\right) = \mathbb{Z}\left[\sqrt{10}\right]$ isn't an UFD.

Example 2. Let $m = 85$, which is obiouvsly squarefree; since $85 \equiv 1 \pmod 4$, is

$$h\left(\sqrt{85}\right) = \left\{\frac{a + b\sqrt{85}}{2} : a, b \in \mathbb{Z} \text{ and } a \equiv b \pmod 4\right\}.$$

Moreover, $85 \equiv 1^2 \pmod 3$, while ± 3 are both quadratic non-residues of 85 (as they are both quadratic non-residue of 5). Since 3 is a prime > 2, by theorem (3.2.3), $h\left(\sqrt{85}\right)$ isn't an UFD.

Example 3. Let $m = 41$; since $41 \equiv 1 \pmod 4$, the domain $\mathbb{Z}\left[\sqrt{41}\right]$ is not an UFD by thorem (3.2.4)

3.3 Deeper results for real domains

Using the results (3.2.2) – (3.2.3) seen in the previos section, we can now see some general and quite strong results for the real domains of the form $h\left(\sqrt{m}\right)$ and $\mathbb{Z}\left[\sqrt{m}\right]$.
In our proofs we will heavily use the lemma (1.4.2) seen in chapter 1.

Theorem 3.3.1. *Let $q_1, q_2, \ldots, q_n$ $(n \geq 2)$ be pairwise distinct odd primes such that $q_1 \equiv 1 \pmod 4$, and let $m = q_1 q_2 \cdots q_n$. Then $h\big(\sqrt{m}\big)$ and $\mathbb{Z}\big[\sqrt{m}\big]$ are not UFDs.*

Proof. Since the primes q_i are pairwise distinct and all odd, we easily deduce from lemma (1.4.2) that there exists a prime p such that:

- $p \equiv 1 \pmod 4$
- p is a quadratic non-residue (mod q_1) and (mod q_2)
- p is a proper quadratic residue (mod q_i), $\forall\, i \in \{3, \ldots, n\}$

So, as $q_1 \equiv 1 \pmod 4$, we obtain:

$$\left(\frac{\pm p}{q_1}\right) = \left(\frac{\pm 1}{q_1}\right)\left(\frac{p}{q_1}\right) = (+1)\cdot(-1) = -1$$

But $q_1 \mid m$, so that, *a fortiori*, $+p$ and $-p$ are both quadratic non-residues of m; moreover, since $p \equiv 1 \pmod 4$, using quadratic reciprocity law, we get:

$$\left(\frac{m}{p}\right) = \left(\frac{q_1 q_2 q_3 \cdots q_n}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\left(\frac{q_3}{p}\right)\cdots\left(\frac{q_n}{p}\right) =$$

$$= \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\left(\frac{p}{q_3}\right)\cdots\left(\frac{p}{q_n}\right) = (-1)(-1)(+1)\cdots(+1) = +1$$

so that m is a quadratic residue of p.
Since $p > 2$ (as p is an odd prime), from theorems (3.2.1) and (3.2.3) and corollary (3.2.2), we conclude that $h\big(\sqrt{m}\big)$ and $\mathbb{Z}\big[\sqrt{m}\big]$ are not UFDs. □

Theorem 3.3.2. *Let $q_1, q_2, \ldots, q_n$ $(n \geq 1)$ be pairwise distinct odd primes such that $q_1 \equiv 1 \pmod 4$, and let $m = 2q_1 q_2 \cdots q_n$. Then $h\big(\sqrt{m}\big)$ and $\mathbb{Z}\big[\sqrt{m}\big]$ are not UFDs.*

Proof. Since the primes q_i are pairwise distinct and all odd, we easily deduce from lemma (1.4.2) that there exists a prime p such that:

- $p \equiv 5 \pmod 8$
- p is a quadratic non-residue (mod q_1)
- p is a proper quadratic residue (mod q_i), $\forall\, i \in \{2, \ldots, n\}$

So, as $q_1 \equiv 1 \pmod 4$, we obtain:

$$\left(\frac{\pm p}{q_1}\right) = \left(\frac{\pm 1}{q_1}\right)\left(\frac{p}{q_1}\right) = (+1)\cdot(-1) = -1$$

But $q_1 \mid m$, so that, *a fortiori*, $+p$ and $-p$ are both quadratic non-residues of m; moreover, since $p \equiv 1 \pmod 4$, using quadratic reciprocity law, we get:

$$\left(\frac{m}{p}\right) = \left(\frac{2q_1q_2\cdots q_n}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_n}{p}\right) =$$

$$= \left(\frac{2}{p}\right)\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_n}\right) = (-1)(-1)(+1)\cdots(+1) = +1$$

so that m is a quadratic residue of p.
Since $p > 2$ (as p is an odd prime), from theorems (3.2.1) and (3.2.3) and corollary (3.2.2), we conclude that $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ are not UFDs. □

The two previous results can immediately be unified in the following theorem:

Theorem 3.3.3. *Let $m > 1$ be a squarefree composite integer that has a prime factor of the form $4k+1$, $k \in \mathbb{N}$. Then $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ are not UFDs.*

Theorems (3.3.1) – (3.3.2) can easily be extended to analogous cases. This is what we'll do in the two following propositions.

Theorem 3.3.4. *Let $q_1, q_2, \ldots, q_n$ $(n \geq 3)$ be pairwise distinct odd primes such that $q_1 \equiv 3 \pmod 4$, and let $m = q_1q_2\cdots q_n$. Then $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ are not UFDs.*

Proof. Since the primes q_i are pairwise distinct and all odd, we easily deduce from lemma (1.4.2) that there exists a prime p such that:

- $p \equiv 1 \pmod 4$
- p is a quadratic non-residue (mod q_2) and (mod q_3)
- p is a proper quadratic residue (mod q_i), $\forall\, i \in \{1, 4, \ldots, n\}$

So, as $q_1 \equiv 3 \pmod 4$, we obtain:

$$\left(\frac{p}{q_2}\right) = -1 \quad \text{and} \quad \left(\frac{-p}{q_1}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{p}{q_1}\right) = (-1)\cdot(+1) = -1$$

But $q_1 \mid m$, $q_2 \mid m$, so that, *a fortiori*, $+p$ and $-p$ are both quadratic non-residues of m; moreover, since $p \equiv 1 \pmod 4$, using quadratic reciprocity law, we get:

$$\left(\frac{m}{p}\right) = \left(\frac{q_1q_2q_3q_4\cdots q_n}{p}\right) = \left(\frac{q_2}{p}\right)\left(\frac{q_3}{p}\right)\left(\frac{q_1}{p}\right)\left(\frac{q_4}{p}\right)\cdots\left(\frac{q_n}{p}\right) =$$

$$= \left(\frac{p}{q_2}\right)\left(\frac{p}{q_3}\right)\left(\frac{p}{q_1}\right)\left(\frac{p}{q_4}\right)\cdots\left(\frac{p}{q_n}\right) = (-1)(-1)(+1)(+1)\cdots(+1) = +1$$

so that m is a quadratic residue of p.
Since $p > 2$ (as p is an odd prime), from theorems (3.2.1) and (3.2.3) and corollary (3.2.2), we conclude that $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ are not UFDs. □

Theorem 3.3.5. *Let $q_1, q_2, \ldots, q_n$ $(n \geq 2)$ be pairwise distinct odd primes such that $q_1 \equiv 3 \pmod 4$, and let $m = 2q_1q_2\cdots q_n$. Then $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ are not UFDs.*

Proof. Since the primes q_i are pairwise distinct and all odd, we easily deduce from lemma (1.4.2) that there exists a prime p such that:

- $p \equiv 5 \pmod 8$
- p is a quadratic non-residue (mod q_2)
- p is a proper quadratic residue (mod q_i), $\forall\, i \in \{1, 3, \ldots, n\}$

So, as $q_1 \equiv 3 \pmod 4$, we obtain:

$$\left(\frac{p}{q_2}\right) = -1 \quad \text{and} \quad \left(\frac{-p}{q_1}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{p}{q_1}\right) = (-1)\cdot(+1) = -1$$

But $q_1 \mid m$, $q_2 \mid m$, so that, *a fortiori*, $+p$ and $-p$ are both quadratic non-residues of m; moreover, since $p \equiv 1 \pmod 4$, using quadratic reciprocity law, we get:

$$\left(\frac{m}{p}\right) = \left(\frac{2q_1q_2\cdots q_n}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{q_2}{p}\right)\left(\frac{q_1}{p}\right)\left(\frac{q_3}{p}\right)\cdots\left(\frac{q_n}{p}\right) =$$

$$= \left(\frac{2}{p}\right)\left(\frac{p}{q_2}\right)\left(\frac{p}{q_1}\right)\left(\frac{p}{q_3}\right)\cdots\left(\frac{p}{q_n}\right) = (-1)(-1)(+1)(+1)\cdots(+1) = +1$$

so that m is a quadratic residue of p.
Since $p > 2$ (as p is an odd prime), from theorems (3.2.1) and (3.2.3) and corollary (3.2.2), we conclude that $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ are not UFDs. □

Theorems (3.3.3) – (3.3.4) – (3.3.5) can be now unified, leading to the following result:

Theorem 3.3.6. *Let $m > 1$ be a squarefree integer such that at least one between $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ is an UFD; then there exist two distinct primes p, q such that $m = p$, or $m = 2p$ and $p \equiv 3 \pmod 4$, or $m = pq$ and $p \equiv q \equiv 3 \pmod 4$.*

Proof. If m is prime, there is nothing to prove. So let's suppose m composite.
From theorem (3.3.3) it derives that m has no factors of the form $4k + 1$. From this statement we immediately conclude that one of the two following possibilities holds:

- m has only two prime factors, no one of the form $4k+1$, i.e. $m = 2p$ for p prime such that $p \equiv 3 \pmod 4$, or $m = pq$ for p, q primes such that $p \equiv q \equiv 3 \pmod 4$.
- m has one of the form indicated in theorems (3.3.4) and (3.3.5).

But if the second case hold, we could deduce from theorems (3.3.4) and (3.3.5) themselves that both $h\big(\sqrt{m}\big)$ and $\mathbb{Z}\big[\sqrt{m}\big]$ aren't UFD, which contradicts our hypothesis. So, if m is composite, the first case must hold, and this proves the thoerem. □

3.4 More general results for $\mathbb{Z}[\sqrt{m}]$

At this stage, we can reinforce theorem (3.3.6) if we limit our attention to the domains $\mathbb{Z}\big[\sqrt{m}\big]$, for $m > 1$ squarefree.
This fact is expressed in the following result:

Theorem 3.4.1. *Let $m > 1$ be a squarefree integer such that $\mathbb{Z}\big[\sqrt{m}\big]$ is an UFD; then there exists a prime $p \equiv 3 \pmod 4$ such that $m = 2$ or $m = p$ or $m = 2p$.*

Proof. From theorem (3.3.6) we know that, if $\mathbb{Z}\big[\sqrt{m}\big]$ is an UFD, then either m has one of forms listed in our statement, or $m = p \equiv 1 \pmod 4$ (p prime) or $m = pq$ for p, q primes and $p \equiv q \equiv 3 \pmod 4$.
But in both these latter situations is $m \equiv 1 \pmod 4$, so that $\mathbb{Z}\big[\sqrt{m}\big]$ can't be an UFD by thorem (3.2.4). □

Now, it would be a good thing to generalize further theorem (3.4.1), and see what we can say about the domains $\mathbb{Z}\big[\sqrt{m}\big]$, for $m > 1$ non-square but not necessarily also squarefree. As a first step, we can easily adjust theorems (3.3.1) – (3.3.2) and obtain the two following propositions (3.4.2) and (3.4.3):

Theorem 3.4.2. *Let A be a positive integer, $q_1, q_2, \ldots, q_n$ ($n \geq 2$) be pairwise distinct odd primes such that $q_1 \equiv 1 \pmod 4$, and let $m = q_1 q_2 \cdots q_n A^2$. Then $\mathbb{Z}\big[\sqrt{m}\big]$ is not an UFD.*

Proof. We easily deduce from lemma (1.4.2) that there exists a prime p such that:

- $p \equiv 1 \pmod 4$
- $p > A \implies A \not\equiv 0 \pmod p$
- p is a quadratic non-residue (mod q_1) and (mod q_2)

- p is a proper quadratic residue (mod q_i), $\forall\, i \in \{3, \dots, n\}$

So, as $q_1 \equiv 1 \pmod 4$, we obtain:

$$\left(\frac{\pm p}{q_1}\right) = \left(\frac{\pm 1}{q_1}\right)\left(\frac{p}{q_1}\right) = (+1)\cdot(-1) = -1$$

But $q_1 \mid m$, so that, *a fortiori*, $+p$ and $-p$ are both quadratic non-residues of m; moreover, since $p \equiv 1 \pmod 4$, using quadratic reciprocity law, we get:

$$\left(\frac{m}{p}\right) = \left(\frac{q_1 q_2 q_3 \cdots q_n A^2}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\left(\frac{q_3}{p}\right)\cdots\left(\frac{q_n}{p}\right)\left(\frac{A^2}{p}\right) =$$

$$= \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\left(\frac{p}{q_3}\right)\cdots\left(\frac{p}{q_n}\right)\left(\frac{A^2}{p}\right) = (-1)(-1)(+1)\cdots(+1)(+1) = +1$$

so that m is a quadratic residue of p.
From theorem (3.2.1), we conclude that $\mathbb{Z}\big[\sqrt{m}\,\big]$ is not an UFD. □

Theorem 3.4.3. *Let A be a positive integer, $q_1, q_2, \dots, q_n$ $(n \geq 1)$ be pairwise distinct odd primes such that $q_1 \equiv 1 \pmod 4$, and let $m = 2q_1q_2\cdots q_nA^2$.*
Then $h\big(\sqrt{m}\,\big)$ and $\mathbb{Z}\big[\sqrt{m}\,\big]$ are not UFD.

Proof. The proof is essentially identical to the proofs of theorems (3.3.2) – (3.4.1), with the difference that the conditions on the prime p have to be substituted with the following ones:

- $p \equiv 5 \pmod 8$
- $p > A$ (so that $A \not\equiv 0 \pmod p$)
- p is a quadratic non-residue (mod q_1)
- p is a proper quadratic residue (mod q_i), $\forall\, i \in \{2, \dots, n\}$

The argumentation proceeds in the usual way and quickly lead to the proof of our claim. □

Theorems (3.3.4) – (3.3.5) can be adjusted similarly, leading to the two following propositions, whose proofs are now quite obvious:

Theorem 3.4.4. *Let A be a positive integer, $q_1, q_2, \dots, q_n$ $(n \geq 3)$ be pairwise distinct odd primes such that $q_1 \equiv 3 \pmod 4$, and let $m = q_1q_2\cdots q_nA^2$. Then $\mathbb{Z}\big[\sqrt{m}\,\big]$ is not an UFD.*

Theorem 3.4.5. *Let A be a positive integer, $q_1, q_2, \ldots, q_n$ $(n \geq 2)$ be pairwise distinct odd primes such that $q_1 \equiv 1 \pmod 4$, and let $m = 2q_1q_2 \cdots q_nA^2$. Then $\mathbb{Z}\left[\sqrt{m}\right]$ is not an UFD.*

Another step towards generalization is to improve theorem (3.2.4):

Theorem 3.4.6. *Let $m = 4^k m_1$, with $k \in \mathbb{N}$, $m_1 \in \mathbb{N} \setminus \{0\}$ not a perfect square, and $m_1 \equiv 1 \pmod 4$. Then $\mathbb{Z}\left[\sqrt{m}\right]$ is not an UFD.*

Proof. In virtue of theorem (3.2.4), we have only to analize the case $k \geq 1$.
In $\mathbb{Z}\left[\sqrt{m}\right]$ we have then:

$$2 \mid (4 - 4^k m_1) = (4 - m) = (2 + \sqrt{m})(2 - \sqrt{m})$$

but $2 \nmid (2+\sqrt{m})$ and $2 \nmid (2-\sqrt{m})$, so that if we prove the irreducibility of 2 in $\mathbb{Z}\left[\sqrt{m}\right]$ we can immediately conclude that this domanin is not an UFD.
But obiouvsly it results $\mathbb{Z}\left[\sqrt{m}\right] \subseteq \mathbb{Z}\left[\sqrt{m_1}\right]$, and 2 is irreducible in $\mathbb{Z}\left[\sqrt{m_1}\right]$ (as shown in the proof of theorem (3.2.4)), so that it is *a fortiori* irreducible in $\mathbb{Z}\left[\sqrt{m}\right]$. □

We can finally summarize theorems (3.4.2) – (3.4.3) – (3.4.4) – (3.4.5) – (3.4.6) into the following result, which generalizes theorem (3.4.1):

Theorem 3.4.7. *Let $m = m_1A^2$, with A positive integer, $m_1 > 1$ squarefree integer, and assume that $\mathbb{Z}\left[\sqrt{m}\right]$ is an UFD. Then there exists a prime $p \equiv 3 \pmod 4$ such that $m_1 = 2$ or $m_1 = p$ or $m_1 = 2p$.*

Proof. If $m_1 = 2$, there is nothing to prove. Suppose now $m_1 > 2$ prime. If $m_1 \equiv 1 \pmod 4$, writing $A = 2^k A_1$ for $k \in \mathbb{N}$, $A_1 \in \mathbb{N}$ odd, and putting $m_2 := m_1{A_1}^2$, we get:

$$m = m_1A^2 = 4^k m_2$$

where m_2 is not a perfect square and $m_2 = m_1{A_1}^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4$. But then we deduce from theorem (3.4.6) that $\mathbb{Z}\left[\sqrt{m}\right]$ is not an UFD, a contradiction.
So we can conclude that if $m_1 > 2$ is prime, it must be $m_1 \equiv 3 \pmod 4$.
Suppose now m_1 composite. From theorems (3.4.2) – (3.4.3), we immediately deduce that m_1 has no prime factors of the form $4h+1$. Then, of the following two possibilities one must hold: either m_1 has only two prime factors (and no one of this of the form $4h + 1$), or m has one of the forms indicated in theorems (3.4.2) – (3.4.3). But in the

latter case, these theorems themselves say us that $\mathbb{Z}\left[\sqrt{m}\right]$ is not an UFD, against our hypothesis.

So, if m_1 is composite, it results $m_1 = 2p$ or $m_1 = pq$, for suitable distinct primes p, q such that $p \equiv q \equiv 3 \pmod 4$.

But if the second equality holds, writing $A = 2^k A_1$, we deduce:

$$m = m_1 A^2 = 4^k {A_1}^2 pq = 4^k m_2$$

where

$$m_2 = pq{A_1}^2 \equiv 3 \cdot 3 \cdot 1 = 9 \equiv 1 \pmod 4$$

so that, since m_2 is not a perfect square, $\mathbb{Z}\left[\sqrt{m}\right]$ can't be an UFD in virtue of theorem (3.4.6), a contradiction.

Thus, if m_1 is prime, it must be $m_1 = 2$ or $m_1 = p \equiv 3 \pmod 4$, while if m is composite it must be $m = 2p$ for p prime with $p \equiv 3 \pmod 4$, and the theorem is proved. □

Chapter 4

Limits of our methods

4.1 Equivalence between property (1) and property (4)

While reading chapter 2, you have probably noted that, in order to show that property (1) (defined at page 22) holds for the rings $h\big(\sqrt{m}\,\big)$ of our interest, we have shown, as a matter of fact, that a (apparently) stronger property holds, i.e. property (4) (defined at page 27).
Thus, a question that arises naturally is:
"Is property (4) truly stronger than property (1), i.e. does there exist a squarefree integer m such that $h\big(\sqrt{m}\,\big)$ satisfies property (1) but not property (4)?"
In this section we'll prove that the answer to this question is "no"[1].

Let's begin with the following:

Definition 4.1.1. *Let D a domain, and let $\Psi : D \setminus \{0\} \to \mathbb{N}$ a function such that:*

$$\forall\, \alpha, \beta \in D \setminus \{0\} \;\; with \;\; \Psi(\alpha) \geq \Psi(\beta), \;\; \exists\, \theta, \rho \in D : \; \alpha = \beta\theta + \rho, \; \rho = 0 \;\; or \;\; \Psi(\rho) < \Psi(\alpha)$$

Then Ψ is said to be a quasi-euclidean function *and D a* quasi-euclidean domain.

By theorems (2.3.2) and (2.3.4), we have that for every normed domain $D \subseteq \mathbb{Q}\big(\sqrt{m}\,\big)$ such that $D \not\subseteq \mathbb{Q}$, subsistence of property (4) is equivalent to the fact that D is norm-euclidean, while subsistence of property (1) is equivalent to the fact that D is a norm-quasi-euclidean, i.e. that its norm is a quasi-euclidean function.
Our main result can now be enunciated as follows:

Theorem 4.1.2. *Let D a domain and let $\Psi : D \setminus \{0\} \to \mathbb{N}$. Then Ψ is quasi-euclidean if and only if it is euclidean.*

[1] as a matter of fact, we will prove a more general result.

Proof. We will prove separately the two implications.

Implication 1 : Ψ euclidean $\implies$ Ψ quasi-euclidean
Suppose given $\alpha, \beta \in D \setminus \{0\}$ such that $\Psi(\alpha) \geq \Psi(\beta)$. Since $\beta \neq 0$ and since Ψ is an euclidean function, there exist $\theta, \rho \in D$ with $\alpha = \beta\theta + \rho$, $\rho = 0$ or $\Psi(\rho) < \Psi(\beta)$. Since $\Psi(\beta) \leq \Psi(\alpha)$, we have then:

$$\alpha = \beta\theta + \rho, \quad \rho = 0 \text{ or } \Psi(\rho) < \Psi(\alpha)$$

so that Ψ is quasi-euclidean.

Implication 2 : Ψ quasi-euclidean $\implies$ Ψ euclidean
Suppose given $\alpha, \beta \in D$ such that $\beta \neq 0$. We want to prove that there exist $\theta, \rho \in D$ such that $\alpha = \beta\theta + \rho$, for $\rho = 0$ or $\Psi(\rho) < \Psi(\beta)$.
Obiouvsly, if $\beta \mid \alpha$, we can choose $\theta := \frac{\alpha}{\beta}$ and $\rho := 0$. So we can suppose $\beta \nmid \alpha$.
From this point on, we will argue by contradiction, assuming that:

$$\forall\, \theta \in D : \ \Psi(\alpha - \beta\theta) \geq \Psi(\beta) \tag{4.1}$$

(obiouvsly we have $\alpha - \beta\theta \neq 0$, since $\beta \nmid \alpha$, so that the expression $\Psi(\alpha - \beta\theta)$ makes sense).
Defining:

$$\mathcal{A} := \{\alpha - \beta\theta : \ \theta \in D\} \subseteq D \setminus \{0\},$$

we have $\Psi(\mathcal{A}) = \{\Psi(\alpha - \beta\theta) : \ \theta \in D\} \subseteq \mathbb{N} \implies \exists\, \theta_0 \in D : \ \Psi(\alpha - \beta\theta_0) = \min \Psi(\mathcal{A})$, and so:

$$\forall\, \theta \in D : \ \Psi(\alpha - \beta\theta_0) \leq \Psi(\alpha - \beta\theta) \tag{4.2}$$

But from (4.1) we get $\Psi(\alpha - \beta\theta_0) \geq \Psi(\beta)$, and so, since Ψ is quasi-euclidean, we have that there exist θ_1, ρ_1 such that:

$$(\alpha - \beta\theta_0) = \beta\theta_1 + \rho_1, \quad \rho_1 = 0 \text{ or } \Psi(\rho_1) < \Psi(\alpha - \theta_0\beta).$$

Since $\beta \nmid \alpha$, we have also $\beta \nmid (\alpha - \beta\theta_0)$, so that $\rho_1 \neq 0$. Thus we get:

$$\Psi(\alpha - \theta_0\beta) > \Psi(\rho_1) = \Psi\left(\alpha - \beta(\theta_0 + \theta_1)\right) = \Psi(\alpha - \beta\overline{\theta}), \quad \overline{\theta} \in D$$

which, according with (4.2), gives us the desired contradiction. □

4.2 Complex domains that are not norm-euclidean

The basic result of this section is the following:

Theorem 4.2.1. *If $m \geq 15$ is a squarefree integer, then $h\big(\sqrt{-m}\big)$ is not norm-euclidean*

Proof. First, it's obvious that $\forall m \in \mathbb{Z}$ squarefree is:

$$h\big(\sqrt{-m}\big) \subseteq T(m) := \left\{ \frac{x + y\sqrt{-m}}{2} \ : \ x, y \in \mathbb{Z} \right\}$$

Suppose now by contradiction that $h\big(\sqrt{-m}\big)$ is norm-euclidean; then for every $\psi \in \mathbb{Q}\big(\sqrt{-m}\big)$ we can find a $\theta \in h\big(\sqrt{-m}\big)$ (and so *a fortiori* a $\theta \in T(m)$) such that $\mathcal{N}(\psi - \theta) < 1$.
So, letting $\psi := \frac{1}{4} + \frac{1}{4}\sqrt{-m}$ and $\theta = \frac{x}{2} + \frac{y}{2}\sqrt{-m}$ $(x, y \in \mathbb{Z})$, we get:

$$(2x-1),\ (2y-1) \ \in \mathbb{Z} \setminus \{0\} \implies \begin{cases} (2x-1)^2 \geq 1 \\ (2y-1)^2 \geq 1 \end{cases}$$

and:

$$\begin{aligned} 1 > \mathcal{N}(\psi - \theta) &= \left(\frac{x}{2} - \frac{1}{4}\right)^2 + m\left(\frac{y}{2} - \frac{1}{4}\right)^2 = \frac{1}{16}\left((2x-1)^2 + m(2y-1)^2\right) \geq \\ &\geq \frac{1}{16}(1+m) = \frac{1+m}{16} \geq \frac{1+15}{16} = 1 \implies 1 > 1 \end{aligned}$$

which give us the desired contradiction. □

Using the previous result, it's easy to classify completely the complex norm-euclidean domains:

Theorem 4.2.2. *If m is a squarefree integer, then $h\big(\sqrt{-m}\big)$ is norm-euclidean if and only if*

$$m = 1,\ 2,\ 3,\ 7 \text{ or } 11.$$

Proof. First, we know by theorem (2.4.1) that $h\big(\sqrt{-m}\big)$ is norm-euclidean if $m = 1, 2, 3, 7$ or 11. On the other hand, from theorem (3.1.7) and from the fact that $\mathbb{Z}\big[\sqrt{-m}\big] = h\big(\sqrt{-m}\big)$ if $m \equiv 1$ or $2 \pmod 4$, we know that for every $m > 2$ with $m \equiv 1$ or $2 \pmod 4$, $h\big(\sqrt{-m}\big)$ is not an UFD, and so *a fortiori* it is not norm-euclidean. Moreover, from the previous theroem, we know that if $m \geq 15$ is a squarefree integer, then $h\big(\sqrt{-m}\big)$ is not norm-euclidean. Hence, apart from 1 and 2, the only values of m that can make $h\big(\sqrt{-m}\big)$ norm-euclidean are 3, 7 and 11, and the result follows. □

4.3 Real domains that are not norm-euclidean

4.3.1 Introduction

In this section we will give a partial classification of those real normed domains $h\big(\sqrt{m}\big)$ that are or are not norm-euclidean.
Unfortunately, we can't give a theorem such simple as theorem (4.2.2), but only more limited results whose proofs will be more elaboreted and complex.

As a first step, we see a simple lemma that will be useful later:

Lemma 4.3.1. *If $\alpha, \beta \in [0, +\infty[$ and $\beta > \alpha + 1$, then there exists $n \in \mathbb{N}$ such that $\alpha < n < \beta$.*

Proof. Define $n := \lfloor \alpha \rfloor + 1$; then it results:

$$\alpha < \lfloor \alpha \rfloor + 1 \leq \alpha + 1 < \beta \implies \alpha < n < \beta$$

as desired. □

We will separate the study of the cases $m \equiv 2$ or $3 \pmod 4$ and $m \equiv 1 \pmod 4$ in two distinct subsections.

4.3.2 Not norm-euclidean $h\big(\sqrt{m}\big)$ for $m \equiv 2$ or $3 \pmod 4$

We begin analyzing three particular cases, namely $m = 23$, $m = 14$ and $m = 35$.

Theorem 4.3.2. *The domain $h\big(\sqrt{23}\big) = \mathbb{Z}\big[\sqrt{23}\big]$ isn't norm-euclidean.*[2]

Proof. We're going to prove our claim by showing that $\mathbb{Z}\big[\sqrt{23}\big]$ can't satisfy property (2). Define $\tau := 1 + \frac{7}{23}\sqrt{23} \in \mathbb{Q}\big(\sqrt{23}\big)$, so that $\mathcal{N}(\tau) = \frac{26}{23} > 1$, and let $\theta = x + y\sqrt{23},\ x, y \in \mathbb{Z}$. If $\mathcal{N}(\tau - \theta) < \mathcal{N}(\tau)$, then:

$$\left|(1-x)^2 - 23 \cdot \left(\frac{7}{23} - y\right)^2\right| < \left|1^2 - 23 \cdot \left(\frac{7}{23}\right)^2\right|$$

so that

$$\left|23(x-1)^2 - (7 - 23y)^2\right| < 26$$

Let now $N := 23(x-1)^2 - (7-23y)^2$; then $N \equiv -3 \pmod{2)3}$ and $|N| < 26$, so that N must then be -3 or 20.
Thus, letting $X := x - 1$, $Y := 7 - 23y$, we have the possibilities:

[2] this example is an adaptation of one that is presented chapter XIV of [HW00].

1. $N = -3$ i.e. $23X^2 - Y^2 = -3$.

   Clearly neither X nor Y can be divisible by 3, so that $X^2 \equiv Y^2 \equiv 1 \pmod 3 \implies N \equiv 22 \equiv 1 \pmod 3$, a contradiction.

2. $N = 20$ i.e. $23X^2 - Y^2 = 20$.

   Clearly neither X nor Y can be divisible by 5, so that $X^2 \equiv \pm 1$, $Y^2 \equiv \pm 1 \pmod 5$; moreover $Y^2 = 23X^2 - 20 \equiv 3X^2 \pmod 5$, and so:

   $$3 \equiv Y^2 \left(X^2\right)^{-1} \equiv (\pm 1) \cdot (\pm 1)^{-1} \equiv \pm 1 \pmod 5,$$

   a contradiction.

Thus $h\big(\sqrt{23}\big) = \mathbb{Z}\big[\sqrt{23}\big]$ doesn't satisfy property (2), so it doesn't satisfy property (4), i.e. it isn't norm-euclidean. □

Theorem 4.3.3. *The domain* $h\big(\sqrt{14}\big) = \mathbb{Z}\big[\sqrt{14}\big]$ *isn't norm-euclidean*

Proof. Take

$$\psi := \frac{1}{2} + \frac{1}{2}\sqrt{14} \in \mathbb{Q}\big(\sqrt{14}\big),$$

and suppose that there exists $\theta = x + y\sqrt{14} \in \mathbb{Z}\big[\sqrt{14}\big]$, with $x, y \in \mathbb{Z}$, such that $\mathcal{N}(\psi - \theta) < 1$. We get then:

$$\begin{aligned} 1 > \mathcal{N}(\psi - \theta) &= \mathcal{N}\left(\left(x - \frac{1}{2}\right) + \left(y - \frac{1}{2}\right)\sqrt{14}\right) = \\ &= \left|\left(x - \frac{1}{2}\right)^2 - 14\left(y - \frac{1}{2}\right)^2\right| = \left|\frac{1}{4}\left((2x-1)^2 - 14(2y-1)^2\right)\right| \end{aligned}$$

so that, letting $X := 2x - 1$, $Y := 2y - 1$ and $U := X^2 - 14Y^2$, we have:

- $|U| < 4$
- $U \equiv 1 - 14 \equiv -13 \equiv 3 \pmod 8$
  (since X, Y are odd and $z^2 \equiv 1 \pmod 8$ $\forall\, z \in \mathbb{Z}$ odd)

Then:

$$U = 3 \implies X^2 - 14Y^2 = 3 \implies X^2 \equiv 3 \pmod 7$$

which, as can be easily seen by direct calculation, is a contradiction. □

By reasoning in an almost identical way, we obtain:

Theorem 4.3.4. *The domain* $h\big(\sqrt{35}\big) = \mathbb{Z}\big[\sqrt{35}\big]$ *isn't norm-euclidean*

Proof. Take

$$\psi := \frac{1}{2} + \frac{1}{2}\sqrt{35} \in \mathbb{Q}\big(\sqrt{35}\big),$$

and suppose that there exists $\theta = x + y\sqrt{35} \in \mathbb{Z}\big[\sqrt{35}\big]$, with $x, y \in \mathbb{Z}$, such that $\mathcal{N}(\psi - \theta) < 1$. We get then:

$$\begin{aligned} 1 > \mathcal{N}(\psi - \theta) &= \mathcal{N}\left(\left(x - \frac{1}{2}\right) + \left(y - \frac{1}{2}\right)\sqrt{35}\right) = \\ &= \left|\left(x - \frac{1}{2}\right)^2 - 35\left(y - \frac{1}{2}\right)^2\right| = \left|\frac{1}{4}\left((2x-1)^2 - 35(2y-1)^2\right)\right| \end{aligned}$$

so that, letting $X := 2x - 1$, $Y := 2y - 1$ and $U := X^2 - 35Y^2$, we have:

- $|U| < 4$
- $U \equiv 1 - 35 \equiv -2 \pmod 8$
  (since X, Y are odd and $z^2 \equiv 1 \pmod 8$ $\forall\, z \in \mathbb{Z}$ odd)

Then:

$$U = -2 \implies X^2 - 35Y^2 = -2 \implies X^2 \equiv 5 \pmod 7$$

which, as can be easily seen by direct calculation, is a contradiction. □

Note that the main interest of the theorems (4.3.2) and (4.3.3) depends on the fact that both $h\big(\sqrt{14}\big)$ and $h\big(\sqrt{23}\big)$ are UFDs[3] (as one can deduce from table (10.4), chapter 10 of [ST87]).

Now we are going to prove a more general and systematic result. But first we need three technical yet simple lemmas.

Lemma 4.3.5. *If* $t, m, \mu \in \mathbb{Z}$ *satisfy* $t \equiv 1 \pmod 2$ *and* $m \equiv 2 \pmod 4$ *and* $\mu = 2$ *or* 3*, then* $\nexists\, X, Y \in \mathbb{Z}$ *such that*

$$X^2 - mY^2 \equiv t^2 - \mu m \pmod 8 \tag{4.3}$$

Proof. If (4.3) holds, we have:

$$X^2 - t^2 \equiv m(Y^2 - \mu) \pmod 8 \implies X^2 - t^2 \equiv 0 \pmod 2 \text{ (as } m \text{ is even)} \implies$$

$$\implies X, t \text{ odd} \implies X^2 - t^2 \equiv 1 - 1 \equiv 0 \pmod 8,$$

[3] this statement will not be proved here.

so that, writing $m = 2M$ (with M odd integer), we get:

$$0 \equiv 2M(Y^2 - \mu) \pmod 8 \implies (Y^2 - \mu)M \equiv 0 \pmod 4 \implies Y^2 \equiv \mu \pmod 4,$$

which is a contradiction since $\mu = 2$ or 3. □

Lemma 4.3.6. *If $t, m, \mu \in \mathbb{Z}$ satisfy, $t \equiv 1 \pmod 2$ and $m \equiv 3 \pmod 4$ and $\mu = 5$ or 6, then $\nexists\, X, Y \in \mathbb{Z}$ such that*

$$X^2 - mY^2 \equiv t^2 - \mu m \pmod 8 \tag{4.4}$$

Proof. If (4.4) holds, we have that $m(Y^2 - \mu) \equiv X^2 - t^2 \pmod 8$, and so, being $t^2 \equiv m^2 \equiv 1 \pmod 8$ (as m and t are odd):

$$Y^2 - \mu \equiv m^2(Y^2 - \mu) \equiv m(X^2 - t^2) \equiv m(X^2 - 1) \pmod 8$$

i.e.

$$Y^2 \equiv \mu + m(X^2 - 1) \pmod 8.$$

But, since $m \equiv 3$ or $7 \pmod 8$ and $X^2 \equiv 0$, 1 or $4 \pmod 8$, it must be $m(X^2-1) \equiv 0$, 1 or $5 \pmod 8$, so that, since $\mu = 5$ or 6:

$$Y^2 \equiv \mu + m(X^2 - 1) \equiv 2,\ 3,\ 5,\ 6 \text{ or } 7 \pmod 8,$$

a contradiction. □

Lemma 4.3.7. *Let m, A, U, t be integers with $m > 1$, $|U| < m$, $U \equiv t \pmod m$ and $Am < t < (A+1)m$; then $U = t - Am$ or $U = t - (A+1)m$.*

Proof. Define:

$$U_1 := t - Am \quad \text{and} \quad U_2 := t - (A+1)m$$

From our hypotheses, we immediately get:

$$-m < U_2 < 0 < U_1 < m \quad \text{and} \quad U_1 \equiv U_2 \equiv t \pmod m$$

so that, being $U \equiv t \pmod m$ and $|U| < m$, it's easy to deduce that $U = U_1$ or $U = U_2$, i.e. $U = t - Am$ or $U = t - (A+1)m$. □

Now we can state and prove our theorem, which is a generalization of theorem (249) in chapter XIV of [HW00] (as will become clear after the statement of theorem (4.3.9)).

Theorem 4.3.8. *Suppose that $m > 1$ is a squarefree integer such that:*

(a) $m \equiv 2 \pmod 4$ *and* $\exists\, t \in \mathbb{N}$ *odd,* $\exists\, k \in \mathbb{N}$ *such that* $(4k+2)m < t^2 < (4k+3)m$,

or:

(b) $m \equiv 3 \pmod 4$ *and* $\exists\, t \in \mathbb{N}$ *odd,* $\exists\, k \in \mathbb{N}$ *such that* $(8k+5)m < t^2 < (8k+6)m$.

Then $h\big(\sqrt{m}\big) = \mathbb{Z}\big[\sqrt{m}\big]$ *can't be norm-euclidean.*

Proof. Argue by contradiction, assuming that $h\big(\sqrt{m}\big) = \mathbb{Z}\big[\sqrt{m}\big]$ is norm-euclidean. Then, defining $\psi := \frac{t}{m}\sqrt{m} \in \mathbb{Q}\big(\sqrt{m}\big)$, we can say that $\exists\ \theta \in h\big(\sqrt{m}\big)$ such that $\mathcal{N}(\psi - \theta) < 1$, i.e. writing $\theta = x + y\sqrt{m}$ for suitable $x, y \in \mathbb{Z}$:

$$\big|(t - my)^2 - mx^2\big| < m$$

Write now $U := (t - my)^2 - mx^2$; we immediately deduce that:

$$|U| < m \quad \text{and} \quad U \equiv t^2 \pmod m$$

Assuming now that there exists $A \in \mathbb{N}$ such that $Am < t^2 < (A+1)m$, from lemma (4.3.7) we get:

$$U = t^2 - Am \quad \text{or} \quad U = t^2 - (A+1)m \tag{4.5}$$

Now we must distinguish two cases.

Case 1 : $m \equiv 2 \pmod 4$.
Then we have from hypothesis (a) that $A = 4k + 2$, so that from (4.5) the two following possibilities follow[4]:

- $(t - my)^2 - mx^2 = U = t^2 - 2m - 4km \equiv t^2 - 2m \pmod 8$
- $(t - my)^2 - mx^2 = U = t^2 - 3m - 4km \equiv t^2 - 3m \pmod 8$

which, since t is odd, give us a contradiction in virtue of lemma (4.3.5).

Case 2 : $m \equiv 3 \pmod 4$.
Then we have from hypothesis (b) that $A = 8k + 5$, so that from (4.5) the two following possibilities follow:

- $(t - my)^2 - mx^2 = U = t^2 - 5m - 8km \equiv t^2 - 5m \pmod 8$
- $(t - my)^2 - mx^2 = U = t^2 - 6m - 8km \equiv t^2 - 6m \pmod 8$

[4] recall that m is even, so that $4km \equiv 0 \pmod 8$.

which, since t is odd, give us a contradiction in virtue of lemma (4.3.6). □

Theorem (4.3.8) can immediately be used to prove the following strong and interesting result:

Theorem 4.3.9. *If $m > 1$ is a squarefree integer such that:*

- $m \equiv 2 \pmod 4$ *and* $m \geq 42$, *or:*
- $m \equiv 3 \pmod 4$ *and* $m \geq 91$,

then $h\big(\sqrt{m}\,\big)$ isn't norm-euclidean.

Proof. In virtue of theorem (4.3.8), to prove our theorem it's enough to prove that:

- $\forall\, m \geq 42 :\ m \equiv 2 \pmod 4,\ \exists\, t \in \mathbb{Z}$ odd such that $2m < t^2 < 3m$
- $\forall\, m \geq 91 :\ m \equiv 3 \pmod 4,\ \exists\, t \in \mathbb{Z}$ odd such that $5m < t^2 < 6m$

We can distingush two cases.

Case 1. $m \equiv 2 \pmod 4$ and $m \geq 42$.

It results:

$$m \geq 42 > 40 = 4 \cdot (5+5) > 4 \cdot \left(5 + 2\sqrt{6}\right) = 4 \cdot \left(\sqrt{3} + \sqrt{2}\right)^2$$

so that $\sqrt{m} > 2(\sqrt{3}+\sqrt{2}) \implies \sqrt{m}(\sqrt{3}-\sqrt{2}) > 2$, and then:

$$\left(\frac{\sqrt{3m}-1}{2}\right) - \left(\frac{\sqrt{2m}-1}{2}\right) = \frac{\sqrt{3m}-\sqrt{2m}}{2} = \frac{1}{2}\sqrt{m}\left(\sqrt{3}-\sqrt{2}\right) > 1.$$

Thus, putting $\beta := \frac{1}{2}\left(\sqrt{3m}-1\right)$ and $\alpha := \frac{1}{2}\left(\sqrt{2m}-1\right)$, and using lemma (4.3.1), we obtain:

$$\begin{aligned} \beta - \alpha > 1 \quad &\implies \beta > \alpha + 1 \implies \exists\, u \in \mathbb{N} \text{ such that } \alpha < u < \beta \\ &\implies \sqrt{2m} = 2\alpha + 1 < 2u + 1 < 2\beta + 1 = \sqrt{3m}. \end{aligned}$$

Finally, writing $t := 2u+1$, we have $t \in \mathbb{N}$ odd and $2m < t^2 < 3m$, as desired.

Case 2. $m \equiv 3 \pmod 4$ and $m \geq 91$.

It results:

$$m \geq 91 > 88 = 4 \cdot (11+11) > 4 \cdot \left(11 + 2\sqrt{30}\right) = 4 \cdot \left(\sqrt{6} + \sqrt{5}\right)^2$$

so that $\sqrt{m} > 2(\sqrt{6}+\sqrt{5}) \implies \sqrt{m}(\sqrt{6}-\sqrt{5}) > 2,$ and then:

$$\left(\frac{\sqrt{6m}-1}{2}\right) - \left(\frac{\sqrt{5m}-1}{2}\right) = \frac{\sqrt{6m}-\sqrt{5m}}{2} = \frac{1}{2}\sqrt{m}\left(\sqrt{6}-\sqrt{5}\right) > 1.$$

Thus, putting $\beta := \frac{1}{2}\left(\sqrt{6m}-1\right)$ and $\alpha := \frac{1}{2}\left(\sqrt{5m}-1\right)$, and using lemma (4.3.1), we obtain:

$$\begin{aligned} \beta - \alpha > 1 \quad &\implies \beta > \alpha + 1 \implies \exists\, u \in \mathbb{N} \text{ such that } \alpha < u < \beta \\ &\implies \sqrt{5m} = 2\alpha + 1 < 2u + 1 < 2\beta + 1 = \sqrt{6m}. \end{aligned}$$

Finally, writing $t := 2u+1,$ we have $t \in \mathbb{N}$ odd and $5m < t^2 < 6m,$ as desired. □

The previous theorem gives a severe limitation to the possibility for a given domain $h\left(\sqrt{m}\right)$ (with $m \equiv 2$ or $3 \pmod 4$) of being norm-euclidean. Moreover, the result can be reinforced again, leading to the following theorem:

Theorem 4.3.10. *If $m \equiv 2$ or $3 \pmod 4$ is a squarefree positive integer such that the domain $h\left(\sqrt{m}\right)$ is norm-euclidean, then it must be:*

$$m = 2,\ 3,\ 6,\ 7,\ 11 \text{ or } 19$$

Proof. Of course, if $m \equiv 2 \pmod 4$ and $m \geq 42,$ or if $m \equiv 3 \pmod 4$ and $m \geq 91,$ then $h\left(\sqrt{m}\right)$ isn't norm-euclidean in virtue of the previous theorem (4.3.9). Thus we have only to show that $h\left(\sqrt{m}\right)$ is not norm-euclidean in the finitely many cases:

1) $m \equiv 2 \pmod 4,$ $2 \leq m < 42,$ m squarefree, $m \neq 2$ and $m \neq 6$

2) $m \equiv 3 \pmod 4,$ $3 \leq m < 91,$ m squarefree, $m \neq 3,$ $m \neq 7,$ $m \neq 11,$ and $m \neq 19$

For sake of simplicity, we'll break down our analysis into two parts, separating the cases $m \equiv 2 \pmod 4$ and $m \equiv 3 \pmod 4$.

Part 1. $m \equiv 2 \pmod 4$.

Then m has one of the following values:

$$m = 10,\ 14,\ 22,\ 26,\ 30,\ 34 \text{ or } 38$$

For each such m, we must show that $h\left(\sqrt{m}\right)$ is not norm-euclidean.

This is done in the following calculations.

- ***m* = 10 :** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 5,$ as $5^2 = 25$ and:

$$10 \cdot 2 = 20 < 25 < 30 = 10 \cdot 3$$

- $\boldsymbol{m = 14}$**:** $h\big(\sqrt{14}\big)$ isn't norm-euclidean by theorem (4.3.3).
- $\boldsymbol{m = 22}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 7$, as $7^2 = 49$ and:
$$22 \cdot 2 = 44 < 49 < 66 = 22 \cdot 3$$
- $\boldsymbol{m = 26}$**:** It suffices to apply by theorem (4.3.8) with $k = 1$ and $t = 13$, as $6 = 4 \cdot 1 + 2$ and $13^2 = 169$ and:
$$26 \cdot 6 = 156 < 169 < 182 = 26 \cdot 7$$
- $\boldsymbol{m = 30}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 9$, as $9^2 = 81$ and:
$$30 \cdot 2 = 60 < 81 < 90 = 30 \cdot 3$$
- $\boldsymbol{m = 34}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 9$, as $9^2 = 81$ and:
$$34 \cdot 2 = 68 < 81 < 102 = 34 \cdot 3$$
- $\boldsymbol{m = 38}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 9$, as $9^2 = 81$ and:
$$38 \cdot 2 = 76 < 81 < 114 = 38 \cdot 3$$

Part 2. $m \equiv 3 \pmod 4$.

Since by hypotesis Then m has one of the following values:

$$m = 15,\ 19,\ 23,\ 31,\ 35,\ 39,\ 43,\ 47,\ 51,\ 55,\ 59,\ 67,\ 71,\ 79,\ 83,\ \text{or } 87$$

For each such m, we must show that $h\big(\sqrt{m}\big)$ is not norm-euclidean.

This is done in the following calculations.

- $\boldsymbol{m = 15}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 9$, as $9^2 = 81$ and:
$$15 \cdot 5 = 75 < 81 < 90 = 15 \cdot 6$$
- $\boldsymbol{m = 23}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 11$, as $11^2 = 121$ and:
$$23 \cdot 5 = 115 < 121 < 138 = 23 \cdot 6$$

- $\boldsymbol{m = 31}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 13$, as $13^2 = 169$ and:

$$31 \cdot 5 = 155 < 169 < 186 = 31 \cdot 6$$

- $\boldsymbol{m = 35}$**:** $h\big(\sqrt{35}\big)$ isn't norm-euclidean by theorem (4.3.4).

- $\boldsymbol{m = 39}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 15$, as $15^2 = 225$ and:

$$39 \cdot 5 = 195 < 225 < 234 = 39 \cdot 6$$

- $\boldsymbol{m = 43}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 15$, as $15^2 = 225$ and:

$$43 \cdot 5 = 215 < 225 < 258 = 43 \cdot 6$$

- $\boldsymbol{m = 47}$**:** It suffices to apply by theorem (4.3.8) with $k = 1$ and $t = 25$, as $13 = 8 \cdot 1 + 5$ and $25^2 = 625$ and:

$$47 \cdot 13 = 611 < 625 < 658 = 47 \cdot 14$$

- $\boldsymbol{m = 51}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 17$, as $17^2 = 289$ and:

$$51 \cdot 5 = 255 < 289 < 306 = 51 \cdot 6$$

- $\boldsymbol{m = 55}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 17$, as $17^2 = 289$ and:

$$55 \cdot 5 = 275 < 289 < 330 = 55 \cdot 6$$

- $\boldsymbol{m = 59}$**:** It suffices to apply by theorem (4.3.8) with $k = 4$ and $t = 47$, as $37 = 8 \cdot 4 + 5$ and $47^2 = 2209$ and:

$$59 \cdot 37 = 2183 < 2209 < 2242 = 59 \cdot 38$$

- $\boldsymbol{m = 67}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 19$, as $19^2 = 361$ and:

$$67 \cdot 5 = 335 < 361 < 402 = 67 \cdot 6$$

- $\boldsymbol{m = 71}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 19$, as $19^2 = 361$ and:

$$71 \cdot 5 = 355 < 361 < 426 = 71 \cdot 6$$

- $\boldsymbol{m = 79}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 21$, as $21^2 = 441$ and:
$$79 \cdot 5 = 395 < 441 < 474 = 79 \cdot 6$$

- $\boldsymbol{m = 83}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 21$, as $21^2 = 441$ and:
$$83 \cdot 5 = 415 < 441 < 498 = 83 \cdot 6$$

- $\boldsymbol{m = 87}$**:** It suffices to apply by theorem (4.3.8) with $k = 0$ and $t = 21$, as $21^2 = 441$ and:
$$87 \cdot 5 = 435 < 441 < 522 = 87 \cdot 6$$

All the possible cases have been analyzed, and the theorem is proved. □

4.3.3 Non norm-euclidean $h\left(\sqrt{m}\right)$ for $m \equiv 1 \pmod 4$

Let's start seeing a domain of the form $h\left(\sqrt{m}\right)$, with $m \equiv 1 \pmod 4$, which is not norm-euclidean.

Theorem 4.3.11. *The domain $h\left(\sqrt{53}\right)$ isn't norm-euclidean.*

Proof. Argue by contradiction, assuming that $h\left(\sqrt{53}\right) = \left\{\frac{2x+y}{2} + \frac{y}{2}\sqrt{53} : \ x, y \in \mathbb{Z}\right\}$ is norm-euclidean, i.e. that:

$$\forall r, s \in \mathbb{Q} \quad \exists\, x, y \in \mathbb{Z} : \quad \left|\left(\frac{2x+y}{2} - r\right)^2 - 53\left(\frac{y}{2} - s\right)^2\right| < 1 \tag{4.6}$$

Let now $r := 0$ and $s := \frac{12}{53}$. Then (4.6) becomes:

$$\left|\frac{(2x+y)^2}{4} - \frac{53}{4}\left(y - \frac{24}{53}\right)^2\right| < 1$$

i.e.

$$\left|(53y - 24)^2 - 53\,(2x+y)^2\right| < 212 \tag{4.7}$$

Write now $X := 53y - 24$, $Y := 2x + y$, $U := X^2 - 53Y^2$. We have then $X^2 \equiv 24^2 \equiv 46 \pmod{53} \implies U \equiv 46 \pmod{53}$, and $X \equiv Y \equiv y \pmod 2 \implies U = X^2 - 53Y^2 \equiv X^2 - Y^2 \equiv 0 \pmod 4$. Thus, using also (4.7), we get:

- $U \equiv 46 \pmod{53}$ and $U \equiv 0 \pmod 4 \implies U \equiv 152 \pmod{212}$.

- $|U| < 212 \implies U = 152$ or $U = -60$.

We now will show that both this cases are impossible.

1. $U = -60 = -4 \cdot 3 \cdot 5$.
Then $9 \nmid U = X^2 - 53Y^2 \implies 3 \nmid X$ and $3 \nmid Y \implies X^2 \equiv Y^2 \equiv 1 \pmod 3$ $\implies 0 \equiv -60 = U = X^2 - 53Y^2 \equiv 1 - 53 \cdot 1 \equiv -52 \equiv 2 \pmod 3$, a contradiction.

2. $U = 152 = 8 \cdot 19$.
Then $X^2 - 53Y^2 = U \equiv 0 \pmod 8$. Obiouvsly is $X \equiv Y \pmod 2$; if it were $X \equiv Y \equiv 1 \pmod 2$, we would get:

$$0 \equiv X^2 - 53Y^2 \equiv 1 - 53 = -52 \equiv 4 \pmod 8,$$

a contradiction. Thus it must be $X = 2a$, $Y = 2b$ for suitable $a, b \in \mathbb{Z} \implies a^2 - 53b^2 = \frac{U}{4} = 38 \implies a \equiv b \pmod 2$. But then:

$$a^2 \equiv b^2 \pmod 4 \implies 38 = a^2 - 53b^2 \equiv a^2 - b^2 \equiv 0 \pmod 4,$$

which gives us the final contradiction. □

Now were going to prove a generalization of the previous result, which will enable us to build an infinite class of domains $h\big(\sqrt{m}\big)$ with $m \equiv 1 \pmod 4$ which are all not norm-euclidean.
Here is our result[5]:

Theorem 4.3.12. *Let $m > 1$ be a squarefree integer with $m \equiv 5 \pmod{24}$, and assume that there exist A, $t \in \mathbb{N}$ such that $A \equiv 6,\ 11,\ 23$ or $30 \pmod{36}$, $t \equiv 3 \pmod 6$ and $Am < t^2 < (A+1)m$. Then $h\big(\sqrt{m}\big)$ isn't norm-euclidean.*

Proof. Argue by contradiction, assuming that

$$h\big(\sqrt{m}\big) = \left\{ \frac{2x+y}{2} + \frac{y}{2}\sqrt{m} : \ x, y \in \mathbb{Z} \right\}$$

is norm-euclidean. Then, defining $\psi := \frac{t}{m}\sqrt{m} \in \mathbb{Q}\big(\sqrt{m}\big)$, we can say that $\exists\, \theta \in h\big(\sqrt{m}\big)$ such that $\mathcal{N}(\psi - \theta) < 1$, i.e. writing $\theta = \frac{2x+y}{2} + \frac{y}{2}\sqrt{m}$ for suitable $x, y \in \mathbb{Z}$:

$$\left| \frac{(2x+y)^2}{4} - \frac{(my - 2t)^2}{4m^2} \cdot m \right| < 1$$

[5]note that this result is unfortunately much weaker than those obtained for $m \equiv 2$ or $3 \pmod 4$.

or better:

$$\left|(2t - my)^2 - m(2x + y)^2\right| < 4m. \tag{4.8}$$

Writing now:

$$U := (2t - my)^2 - m(2x + y)^2 \tag{4.9}$$

we immediately deduce that $U \equiv 4t^2 \pmod{m}$ and $U \equiv m^2y^2 - my^2 = m(m-1)y^2 \equiv 0 \equiv 4t^2 \pmod{4}$ (as $4 \mid (m-1)$), so that, using also inequality (4.8) and our hypothesis on A we get:

$$U \equiv 4t^2 \pmod{4m} \quad \text{and} \quad |U| < 4m \quad \text{and} \quad A \cdot (4m) < 4t^2 < (A+1) \cdot (4m).$$

At this point we can apply lemma (4.3.7) to deduce that $U = 4t^2 - A \cdot (4m)$ or $U = 4t^2 - (A+1) \cdot (4m)$, i.e. that:

$$U = 4\left(t^2 - Am\right) \quad \text{or} \quad U = 4\left(t^2 - (A+1)m\right) \tag{4.10}$$

Now, since $A \equiv 6,\ 11,\ 23$ or $30 \pmod{36}$, from (4.10) easily derives[6] that must exist $B, C \in \mathbb{N}$ with $B \equiv 3 \pmod 4$ and $C \equiv 3$ or $6 \pmod 9$ such that $U = 4(t^2 - Bm)$ or $U = 4(t^2 - Cm)$; moreover, from (4.9) easily derives that $U = X^2 - mY^2$ with $X, Y \in \mathbb{Z},\ X \equiv Y \pmod 2$.

Thus, summarizing what has been obtained so far, we can state that there exist X, Y, B, C, t, $m \in \mathbb{Z}$ such that:

$$\begin{cases} X \equiv Y \pmod 2 \\ m \equiv 5 \pmod{24} \\ t \equiv 3 \pmod 6 \\ B \equiv 3 \pmod 4 \\ C \equiv 3 \text{ or } 6 \pmod 9 \end{cases} \tag{4.11}$$

and:

$$X^2 - mY^2 = 4(t^2 - Bm) \quad \text{or} \quad X^2 - mY^2 = 4(t^2 - Cm) \tag{4.12}$$

Now we are going to show that, with the (4.11) holding, both the (4.12) are impossible. To this purpose, we'll divide the rest of our proof into two cases.

Case 1. Assume first that:

$$X^2 - mY^2 = 4(t^2 - Bm). \tag{4.13}$$

[6] it's enough to set $B = A$ and $C = A + 1$ if $A \equiv 11$ or $23 \pmod{36}$, $B = A + 1$ and $C = A$ if $A \equiv 6$ or $30 \pmod{36}$.

If $X \equiv Y \equiv 1 \pmod 2$, it follows that $X^2 - mY^2 \equiv 1 - m \equiv 4 \pmod 8 \implies 8 \nmid (X^2 - mY^2) = 4(t^2 - Bm) \implies 2 \nmid (t^2 - Bm)$, which is a contradiction since t, B and m are all odd.
Thus it must be $X \equiv Y \equiv 0 \pmod 2$, and writing $X = 2W$, $Y = 2Z$ for suitable W, $Z \in \mathbb{Z}$ we obtain:

$$4\left(W^2 - mZ^2\right) = 4\left(t^2 - Bm\right) \implies W^2 - mZ^2 = t^2 - Bm.$$

Now $t^2 - Bm \equiv 1 - 3 \cdot 5 \equiv 2 \pmod 4$, so that $2 \mid \left(W^2 - mZ^2\right)$ and thus $W \equiv Z \pmod 2$; but then:

$$2 \equiv t^2 - Bm \equiv W^2 - Z^2 \equiv 0 \pmod 4$$

again a contradiction.

Case 2. Assume now that

$$X^2 - mY^2 = 4(t^2 - Cm). \tag{4.14}$$

Since $3 \mid t$ and $C \equiv 3$ or $6 \pmod 9$, equality (4.14) can be rewritten as:

$$X^2 - mY^2 = 4(9r - 3sm) \tag{4.15}$$

for suitable $r \in \mathbb{Z}$ and $s \in \{1, 2\}$.
As $3 \nmid s$ and $3 \nmid m$, from (4.15) we get X, $Y \not\equiv 0 \pmod 3$, thus $X^2 \equiv Y^2 \equiv 1 \pmod 3$. But then, since $m \equiv 2 \pmod 3$:

$$0 \equiv 4\,(9r - 3ms) = X^2 - mY^2 \equiv 1 - 2 \equiv -1 \pmod 3,$$

which is plainly impossible.

In both cases we reached a contradiction, and the result follows. □

As stated previously, the result just proven can be used to build an infinite class of domains $h\left(\sqrt{m}\right)$ with $m \equiv 1 \pmod 4$ which are all not norm-euclidean.

Corollary 4.3.13. *If $m \equiv 5 \pmod{24}$ and $m \geq 941$ $(= 39 \cdot 24 + 5)$, then $h\left(\sqrt{m}\right)$ isn't norm-euclidean.*

Proof. We will show that for every $m \geq 941$ there exists an $u \in \mathbb{N}$ such that $6m < (6u + 3)^2 < 7m$, from which our claim will follow immediately in virtue of the previous theorem (4.3.12).

First, it's easy to see that $941 > 36(13 + 2\sqrt{42})$, so that if $m \geq 941$ it's also

$$m > 36\left(13 + 2\sqrt{42}\right) = 6^2\left(\sqrt{7} + \sqrt{6}\right)^2$$

and then:

$$\sqrt{m} > 6\left(\sqrt{7} + \sqrt{6}\right) = \frac{6}{\sqrt{7} - \sqrt{6}} \implies \sqrt{7m} - \sqrt{6m} > 6$$

or equivalently:

$$\frac{\sqrt{6m} - 3}{6} + 1 < \frac{\sqrt{7m} - 3}{6}$$

From this last inequality and from lemma (4.3.1) we deduce that $\exists\, u \in \mathbb{N}$ such that:

$$\frac{\sqrt{6m} - 3}{6} < u < \frac{\sqrt{7m} - 3}{6}$$

i.e. such that:

$$6m < (6u + 3)^2 < 7m$$

and our claim follows. □

We conclude by an elegant result which reinforce the previous corollary (4.3.13):

Theorem 4.3.14. *Let $m > 1$ squarefree such that $m \equiv 5 \pmod{24}$; then the domain $h\left(\sqrt{m}\right)$ is norm-euclidean if and only if $m = 5$ or $m = 29$.*

Proof. It was already shown in theorem (2.4.3) that $h\left(\sqrt{5}\right)$ and $h\left(\sqrt{29}\right)$ are norm-euclidean, and in the previous corollary (4.3.13) that $h\left(\sqrt{m}\right)$ isn't norm-euclidean for any m squarefree such that $m \geq 941$ and $m \equiv 5 \pmod{24}$; thus, to prove our claim, we only need to show that $h\left(\sqrt{m}\right)$ isn't norm-euclidean for all m squarefree with $m \equiv 5 \pmod{24}$ and $53 \leq m < 941$, i.e. for:

$$\begin{aligned} m \;=\; & 53,\ 77,\ 101,\ 149,\ 173,\ 197,\ 221,\ 269,\ 293,\ 317,\ 341,\ 365,\ 389,\ 413,\ 437,\\ & 461,\ 485,\ 509,\ 533,\ 557,\ 581,\ 629,\ 653,\ 677,\ 701,\ 749,\ 773,\ 797,\ 821,\ 869,\\ & 893,\ \text{or}\ 917. \end{aligned}$$

This easily follows from theorem (4.3.12) and the following calculations.

- $\boldsymbol{m = 53}$**:** It suffices to apply theorem (4.3.12) with $A = 258$ and $t = 117$, as:
  - $117 = 19 \cdot 6 + 3$
  - $258 = 36 \cdot 7 + 6$
  - $117^2 = 13689$
  - $53 \cdot 258 = 13674 < 13689 < 13727 = 53 \cdot 259$

- $\boldsymbol{m = 77}$**:** It suffices to apply theorem (4.3.12) with $A = 42$ and $t = 57$, as:
  - $57 = 9 \cdot 6 + 3$
  - $42 = 36 \cdot 1 + 6$
  - $57^2 = 3249$
  - $77 \cdot 42 = 3234 < 3249 < 3311 = 77 \cdot 43$
- $\boldsymbol{m = 101}$**:** It suffices to apply theorem (4.3.12) with $A = 47$ and $t = 69$, as:
  - $69 = 11 \cdot 6 + 3$
  - $47 = 36 \cdot 1 + 11$
  - $69^2 = 4761$
  - $101 \cdot 47 = 4747 < 4761 < 4848 = 101 \cdot 48$
- $\boldsymbol{m = 149}$**:** It suffices to apply theorem (4.3.12) with $A = 210$ and $t = 177$, as:
  - $177 = 29 \cdot 6 + 3$
  - $210 = 36 \cdot 5 + 30$
  - $177^2 = 31329$
  - $149 \cdot 210 = 31290 < 31329 < 31439 = 149 \cdot 211$
- $\boldsymbol{m = 173}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 33$, as:
  - $33 = 5 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $33^2 = 1089$
  - $173 \cdot 6 = 1038 < 1089 < 1211 = 173 \cdot 7$
- $\boldsymbol{m = 197}$**:** It suffices to apply theorem (4.3.12) with $A = 138$ and $t = 165$, as:
  - $165 = 27 \cdot 6 + 3$
  - $138 = 36 \cdot 3 + 30$
  - $165^2 = 27225$
  - $197 \cdot 138 = 27186 < 27225 < 27383 = 197 \cdot 139$

- $\boldsymbol{m = 221}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 39$, as:
  - $39 = 6 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $39^2 = 1521$
  - $221 \cdot 6 = 1326 < 1521 < 1547 = 221 \cdot 7$
- $\boldsymbol{m = 269}$**:** It suffices to apply theorem (4.3.12) with $A = 150$ and $t = 201$, as:
  - $201 = 33 \cdot 6 + 3$
  - $150 = 36 \cdot 4 + 6$
  - $201^2 = 40401$
  - $269 \cdot 150 = 40350 < 40401 < 40619 = 269 \cdot 151$
- $\boldsymbol{m = 293}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 45$, as:
  - $45 = 7 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $45^2 = 2025$
  - $293 \cdot 6 = 1758 < 2025 < 2051 = 293 \cdot 7$
- $\boldsymbol{m = 317}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 45$, as:
  - $45 = 7 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $45^2 = 2025$
  - $317 \cdot 6 = 1902 < 2025 < 2219 = 317 \cdot 7$
- $\boldsymbol{m = 341}$**:** It suffices to apply theorem (4.3.12) with $A = 11$ and $t = 63$, as:
  - $63 = 10 \cdot 6 + 3$
  - $11 = 36 \cdot 0 + 11$
  - $63^2 = 3969$
  - $341 \cdot 11 = 3751 < 3969 < 4092 = 341 \cdot 12$

- $\boldsymbol{m = 365}$**:** It suffices to apply theorem (4.3.12) with $A = 23$ and $t = 93$, as:
  - $93 = 15 \cdot 6 + 3$
  - $23 = 36 \cdot 0 + 23$
  - $93^2 = 8649$
  - $365 \cdot 23 = 8395 < 8649 < 8760 = 365 \cdot 24$
- $\boldsymbol{m = 389}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 51$, as:
  - $51 = 8 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $51^2 = 2601$
  - $389 \cdot 6 = 2334 < 2601 < 2723 = 389 \cdot 7$
- $\boldsymbol{m = 413}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 51$, as:
  - $51 = 8 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $51^2 = 2601$
  - $413 \cdot 6 = 2478 < 2601 < 2891 = 413 \cdot 7$
- $\boldsymbol{m = 437}$**:** It suffices to apply theorem (4.3.12) with $A = 66$ and $t = 171$, as:
  - $171 = 28 \cdot 6 + 3$
  - $66 = 36 \cdot 1 + 30$
  - $171^2 = 29241$
  - $437 \cdot 66 = 28842 < 29241 < 29279 = 437 \cdot 67$
- $\boldsymbol{m = 461}$**:** It suffices to apply theorem (4.3.12) with $A = 23$ and $t = 105$, as:
  - $105 = 17 \cdot 6 + 3$
  - $23 = 36 \cdot 0 + 23$
  - $105^2 = 11025$
  - $461 \cdot 23 = 10603 < 11025 < 11064 = 461 \cdot 24$

- $\boldsymbol{m = 485}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 57$, as:
  - $57 = 9 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $57^2 = 3249$
  - $485 \cdot 6 = 2910 < 3249 < 3395 = 485 \cdot 7$
- $\boldsymbol{m = 509}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 57$, as:
  - $57 = 9 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $57^2 = 3249$
  - $509 \cdot 6 = 3054 < 3249 < 3563 = 509 \cdot 7$
- $\boldsymbol{m = 533}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 57$, as:
  - $57 = 9 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $57^2 = 3249$
  - $533 \cdot 6 = 3198 < 3249 < 3731 = 533 \cdot 7$
- $\boldsymbol{m = 557}$**:** It suffices to apply theorem (4.3.12) with $A = 11$ and $t = 81$, as:
  - $81 = 13 \cdot 6 + 3$
  - $11 = 36 \cdot 0 + 11$
  - $81^2 = 6561$
  - $557 \cdot 11 = 6127 < 6561 < 6684 = 557 \cdot 12$
- $\boldsymbol{m = 581}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 63$, as:
  - $63 = 10 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $63^2 = 3969$
  - $581 \cdot 6 = 3486 < 3969 < 4067 = 581 \cdot 7$

- $\boldsymbol{m = 629}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 63$, as:
  - $63 = 10 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $63^2 = 3969$
  - $629 \cdot 6 = 3774 < 3969 < 4403 = 629 \cdot 7$
- $\boldsymbol{m = 653}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 63$, as:
  - $63 = 10 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $63^2 = 3969$
  - $653 \cdot 6 = 3918 < 3969 < 4571 = 653 \cdot 7$
- $\boldsymbol{m = 677}$**:** It suffices to apply theorem (4.3.12) with $A = 11$ and $t = 87$, as:
  - $87 = 14 \cdot 6 + 3$
  - $11 = 36 \cdot 0 + 11$
  - $87^2 = 7569$
  - $677 \cdot 11 = 7447 < 7569 < 8124 = 677 \cdot 12$
- $\boldsymbol{m = 701}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 69$, as:
  - $69 = 11 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $69^2 = 4761$
  - $701 \cdot 6 = 4206 < 4761 < 4907 = 701 \cdot 7$
- $\boldsymbol{m = 749}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 69$, as:
  - $69 = 11 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $69^2 = 4761$
  - $749 \cdot 6 = 4494 < 4761 < 5243 = 749 \cdot 7$

- $\boldsymbol{m = 773}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 69$, as:
  - $69 = 11 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $69^2 = 4761$
  - $773 \cdot 6 = 4638 < 4761 < 5411 = 773 \cdot 7$
- $\boldsymbol{m = 797}$**:** It suffices to apply theorem (4.3.12) with $A = 42$ and $t = 183$, as:
  - $183 = 30 \cdot 6 + 3$
  - $42 = 36 \cdot 1 + 6$
  - $183^2 = 33489$
  - $797 \cdot 42 = 33474 < 33489 < 34271 = 797 \cdot 43$
- $\boldsymbol{m = 821}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 75$, as:
  - $75 = 12 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $75^2 = 5625$
  - $821 \cdot 6 = 4926 < 5625 < 5747 = 821 \cdot 7$
- $\boldsymbol{m = 869}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 75$, as:
  - $75 = 12 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $75^2 = 5625$
  - $869 \cdot 6 = 5214 < 5625 < 6083 = 869 \cdot 7$
- $\boldsymbol{m = 893}$**:** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 75$, as:
  - $75 = 12 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $75^2 = 5625$
  - $893 \cdot 6 = 5358 < 5625 < 6251 = 893 \cdot 7$

- ***m* = 917 :** It suffices to apply theorem (4.3.12) with $A = 6$ and $t = 75$, as:
  - $75 = 12 \cdot 6 + 3$
  - $6 = 36 \cdot 0 + 6$
  - $75^2 = 5625$
  - $917 \cdot 6 = 5502 < 5625 < 6419 = 917 \cdot 7$

All the possible cases have been analyzed, and the theorem is proved.

□

Bibliography

[Chi89] Lindsay Childs. *Algebra: un'introduzione concreta*. ETS Editrice, 1989. Italian translation by Carlo Traverso.

[Dav94] Harold Davenport. *Aritmetica superiore*. Zanichelli, 1994. Italian translation by Umberto Zannier.

[HW00] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers*. Clarendon Press, fifth edition, 2000.

[Sha85] Daniel Shanks. *Solved and unsolved problems in number theory*. Chelsea Publishing Company, third edition, 1985.

[ST87] Ian Stewart and David Tall. *Algebraic number theory*. Chapman & Hall, second edition, 1987.