Novi Sad J. Math.
Vol. 38, No. 1, 2008, 137-154

SOME EXAMPLES OF PRINCIPAL IDEAL DOMAIN WHICH ARE NOT EUCLIDEAN AND SOME OTHER COUNTEREXAMPLES

Veselin Perić[1], **Mirjana Vuković**[2]

Abstract. It is well known that every Euclidean ring is a principal ideal ring. It is also known for a very long time that the converse is not valid. Counterexamples exist under the rings R of integral algebraic numbers in quadratic complex fields $\mathbb{Q}\left[\sqrt{-D}\,\right]$, for $D = 19, 43, 67$, and 163. In conection with these counterexamples several results were published in an effort to make them somewhat more accessible. The aim of this note is to present and complete these results.

AMS Mathematics Subject Classification (2000): 13F07, 13F10, 13F15, 11R04

Key words and phrases: Principal ideal domains, Euclidean domains, Unique factorization domains, Rings of algebraic integers in some quadratic field

0. Introduction

It is well known that any Euclidean domain is a principal ideal domain, and that every principal ideal domain is a unique factorization domain.

The main examples of Euclidean domains are the ring $\mathbb{Z}$ of integers and the polynomial ring $K[x]$ in one variable x over a field K. It is known that the polynomial ring $R[x]$ in one variable x over a unique factorization domain R is also a unique factorization domain. So the ring $\mathbb{Z}[x_1, ..., x_n]$ of all polynomials in $n \geq 1$ variables over $\mathbb{Z}$, and the polynomial ring $K[x_1, ...,x_n]$, in $n \geq 1$ variables over K, are also unique factorization domains. But, the ring $\mathbb{Z}[x_1, ...,x_n]$ for $n \geq 1$, and the ring $K[x_1, ..., x_n]$ for $n \geq 2$, are not principal ideal domains. Therefore, we have simple examples of unique factorization domains, that are not principal ideal domains. It is easy to see that any Euclidean domain is a principal ideal domain. But, usually, to show that the converse is not valid, one gives no counterexamples, or one refers to [3]. Unfortunately, for such examples one cannot find all details which could make those examples easy to understand, in [3].

The counterexamples exist under the rings R of integral algebraic numbers in quadratic complex fields $\mathbb{Q}[\sqrt{-D}]$, for $D = 19$, 43, 67, 163, ([6], 1967). Namely,

[1]Department of Mathematics, University of Montenegro, Podgorica, Montenegro, e-mail: vperic@ac.yu

[2]Department of Mathematics, University of Sarajevo, Sarajevo, Bosnia and Herzegovina, e-mail: mirjanav@yahoo.com

H. M. Stark in the mentioned article proved that under the rings R of integral algebraic numbers in complex quadratic fields $\mathbb{Q}[\sqrt{-D}]$, exactly those for $D =$ 1, 2, 3, 7, 11, 19, 43, 67, and 163, are principal ideal domains, and it is well known (see ([2], 1962, Th. 246, p. 213) that the first five of these rings are also Euclidean domains.

Toward the end of the 20th century some articles ([8], 1973; [1], 1988) were published in which for one of the remaining four rings (for that with D=19) it was proved that it is a principal ideal, but not a Euclidean domain. In another article ([7], 1975), taking in account that all remaining rings R (for $D = 19$, 43, 67, and 163) are principal ideal domains, it was proved that none of those rings are Euclidean domains. The last proof is somewhat simpler than the corresponding proof in [8], because in this first proof some non-essential details were omitted.

Both of these proofs are based on a theorem from [3]. The corresponding proof in [1] is not directly based on the cited theorem, but it is essentially not different from the proof in [7].

The proofs in [8] and [1], that, for $D = 19$, the ring R is a principal ideal domain, differ slightly, and are based on a theorem in [7], which is due to *Dedekind* and *Hasse*.

So, in view of [8] and [1], respectively [7], we have one, respectively four, counterexamples of rings which are principal ideals, but not Euclidean domains. Those counterexamples are easier to understand and there are no other such counterexamples under the rings R of integral algebraic numbers in the complex quadratic fields $\mathbb{Q}$ $[\sqrt{-D}]$.

Let us remark that under rings R of integral algebraic numbers in the complex quadratic fields $\mathbb{Q}[\sqrt{-D}]$ there are such rings that are not unique factorization domains (for instance, for $D = 5$).

The aim of this article is to present all of the mentioned results from [8], [7], and [1]. For this purpose we first describe (Section 1) the complex quadratic field $\mathbb{Q}[\sqrt{-D}]$ and the ring R of integral algebraic numbers R in this field. Then we give some basic facts (Section 2) about Euclidean, "almost Euclidean", and principal ideal domains, including the two mentioned theorems from [3] which we will use in the last section (Section 3). The last section contains all mentioned and some other examples and counterexamples, from which those which are well known were only mentioned.

1. The ring R of all integral algebraic numbers in the complex quadratic field $\mathbb{Q}[\sqrt{-D}]$

First we are concerned with the *complex quadratic field* $\mathbb{Q}[\sqrt{-D}]$ and with the *ring R of all algebraic integers* in this field.

Let $\mathbb{Q}$ be the field of rational numbers, and D be a positive integer without square factors greater than 1. Then $\sqrt{-D} = i\sqrt{D}$ is a root of the monic quadratic equation

$$(X - \sqrt{-D})(X - \overline{\sqrt{-D}}) = 0$$

with the rational coefficients:

$$1, -(\sqrt{-D} + \overline{\sqrt{-D}}) = 0, \sqrt{-D} \cdot \overline{\sqrt{-D}} = D,$$

hence, an algebraic number of degree 2.

Theorem 1.1. *The set*

$$\mathbb{Q}[\sqrt{-D}] = \{a + b\sqrt{-D} \mid a,\ b \in \mathbb{Q}\}$$

is a subfield of the field $\mathbb{C}$ *of all complex numbers, actually the smalest subfield containing* $\mathbb{Q}$ *and* $\sqrt{-D}$.

Proof. For $a = 0$ and $b = 1$, we have

$$\sqrt{-D} = 0 + 1 \cdot \sqrt{-D} \in \mathbb{Q}[\sqrt{-D}],$$

and for $a \in \mathbb{Q}$ and $b = 0$,

$$a = a + 0 \cdot \sqrt{-D} \in \mathbb{Q}[\sqrt{-D}],\ i.e.\ \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-D}].$$

Obviously, $\mathbb{Q}[\sqrt{-D}]$ is closed under addition and conjugation. Since

$$\sqrt{-D} \cdot \sqrt{-D} = -D \in \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-D}],$$

the set $\mathbb{Q}[\sqrt{-D}]$ is also closed under multiplication. Therefore, $\mathbb{Q}[\sqrt{-D}]$ is a commutative ring with unity element 1.

In particular, $\mathbb{Q}[\sqrt{-D}]$ is a vector space over the field $\mathbb{Q}$. This space has a basis $\{1, \sqrt{-D}\}$, hence the dimension

$$dim_{\mathbb{Q}}\ \mathbb{Q}[\sqrt{-D}] = 2.$$

An element

$$\alpha = a + b\sqrt{-D} \in \mathbb{Q}[\sqrt{-D}]\backslash\{0\}$$

has in $\mathbb{C}$ an inverse

$$\alpha^{-1} = (\alpha\overline{\alpha})^{-1}\overline{\alpha}.$$

But,

$$\alpha\overline{\alpha} = a^2 + b^2 D \in \mathbb{Q},\ \alpha\overline{\alpha} \neq 0,$$

i.e.

$$(\alpha\overline{\alpha})^{-1} \in \mathbb{Q},\ \text{hence}\ (\alpha\overline{\alpha})^{-1} \cdot \overline{\alpha} \in \mathbb{Q}[\sqrt{-D}].$$

This means $\alpha^{-1} \in \mathbb{Q}[\sqrt{-D}]$, and so $\mathbb{Q}[\sqrt{-D}]$ is a field. □

Definition 1.1. *The field* $\mathbb{Q}\ [\sqrt{-D}]$ *is called the complex quadratic field of algebraic numbers.*

Definition 1.2. *For an element $\alpha \in \mathbb{Q}\ [\sqrt{-D}]$ we say that it is an algebraic integer if the monic quadratic equation*

$$(x-\alpha)\cdot(x-\overline{\alpha})=0$$

has all coefficients in $\mathbb{Z}$:

$$1, -(\alpha+\overline{\alpha}),\ \alpha\overline{\alpha}\in\mathbb{Z}.$$

That is true for

$$\alpha = a+b\sqrt{-D},\ (a,b\in\mathbb{Z}),$$

since

$$\alpha+\overline{\alpha}=2a\in\mathbb{Z},\ \alpha\overline{\alpha}=a^2+b^2D\in\mathbb{Z}.$$

But, in the case that

$$(*) \qquad D\equiv -1(mod\,4),\ i.e.\ D=4k-1\ (k\geq 1)$$

an algebraic number

$$\alpha = a+b\sqrt{-D}\ \in\mathbb{Q}[\sqrt{-D}]$$

can be an algebraic integral number also when

$$a\notin\mathbb{Z}\ \ and/or\ \ b\notin\mathbb{Z}.$$

In this case we must have

$$\alpha+\overline{\alpha}=2a\in\mathbb{Z},\ i.e.\ a=\frac{2a_1+1}{2}\ \ (a_1\in\mathbb{Z}),$$

and

$$\alpha\overline{\alpha}=a^2+b^2D=a_1^2+a_1+\frac{1}{4}+b^24k-b^2\in\mathbb{Z},$$

hence

$$a=a_1+\frac{1}{2},\ b=b_1+\frac{1}{2},\ \ (a_1,b_1\in\mathbb{Z}).$$

Under the additional condition $(*)$, the algebraic number

$$\begin{aligned}\alpha = &\ a_1+\tfrac{1}{2}+(b_1+\tfrac{1}{2})\sqrt{-D}\\ = &\ (a_1-b_1)+(2b_1+1)(1+\sqrt{-D})/2,\quad (a_1,b_1\in\mathbb{Z}),\end{aligned}$$

is also an integral algebraic number. In particular, for $a_1=b_1=0$,

$$\theta=\frac{1}{2}(1+\sqrt{-D})\in\mathbb{Q}[\sqrt{-D}]$$

is an algebraic integer.

Thus, the following theorem is true:

Theorem 1.2. *If the condition (*) is fulfilled, then for the set of all algebraic integers in* $\mathbb{Q}[\sqrt{-D}]$

$$R = \{a + b\theta \mid a, b \in \mathbb{Z}\},$$

holds, and otherwise, only

$$R = \{a + b\sqrt{-D} \mid a,\ b \in \mathbb{Z}\}$$

holds. In both cases R is an integral domain with unity element 1. In the first case

$$\theta = (1 + \sqrt{-D})/2$$

is a root of the monic quadratic equation

$$X^2 - X + k = 0,$$

where k is the rational integer in (*), and $\sqrt{-D}$ *is a root of the monic quadratic equation*

$$X^2 + D = 0.$$

Definition 1.3. *The ring R in Theorem 1.2. is called the ring of algebraic integers in the complex quadratic field* $\mathbb{Q}[\sqrt{-D}]$.

This ring is closed under conjugation, since

$$\overline{\theta} = k - \theta, \text{ respectively } \overline{\sqrt{-D}} = -\sqrt{-D}.$$

In the ring R of algebraic integers in $\mathbb{Q}[\sqrt{-D}]$ we have the mapping

$$\varphi : R \to \mathbb{Z}, \quad \varphi(\alpha) = \alpha\overline{\alpha}, (\alpha \in R)$$

with the properties:

i) $$\varphi(\alpha) \geq 0, \quad \varphi(\alpha) = 0 \Leftrightarrow \alpha = 0;$$

ii) $$\varphi(\alpha\beta) = \varphi(\alpha) \cdot \varphi(\beta), \quad (\alpha,\ \beta \in R).$$

From *ii*), it follows

ii') $$\varphi(\alpha\beta) \geq \varphi(\alpha), \quad (\alpha, \beta \in R, \beta \neq 0).$$

Using the mapping φ, which has the first two properties of the Euclidean norm in the definition of the Euclidean domain, we can determine the set $\mathcal{U}$ of all *unities* in R.

For the unity element 1 of R we have obviously, $\varphi(1) = 1$. Therefore, for $u \in \mathcal{U}$, from

$$u \mid 1 \ \text{ and } \ 1 \mid u, \ (u \neq 0),$$

we have, taking ii') into account, $\varphi(u) = 1$.
If

$$R = \{a + b\sqrt{-D} \mid a,\ b \in \mathbb{Z}\},$$

from $\varphi(u) = 1$, it follows:

$$u = a + b\sqrt{-D} \Leftrightarrow a^2 + b^2 D = 1,$$

i.e. for $D > 1$,

$$a^2 = 1, b^2 = 0, \text{ hence } a = \pm 1,\ b = 0,$$

and, for $D = 1$, i.e. in the case of the ring $R = \{a + bi \,|\, a,\, b \in \mathbb{Z}\}$, of *Gaussian integers* it follows

$$a^2 = 1,\ b^2 = 0 \vee a^2 = 0,\ b^2 = 1,$$

hence

$$a = \pm 1, b = 0 \vee a = 0, b = \pm 1.$$

That means

$$\mathcal{U} = \{1, -1\},\ (D > 1),$$
$$\mathcal{U} = \{1, -1, i, -i\},\ (D = 1).$$

Now let

$$D \equiv -1 (mod\, 4),\ i.e.\ D = 4k - 1\ (k \geq 1),$$

i.e.

$$R = \{a + b\theta \,|\, a, b \in \mathbb{Z}\}.$$

Then for

$$u = a + b\theta,\ (a, b \in \mathbb{Z}),$$

we have

$$1 = \varphi(u) = (a + b/2)^2 + b^2 D/4 = a^2 + ab + b^2 k,$$

respectively

$$1 = \varphi(\overline{u}) = \varphi(a + b - b\theta) = (a + b)^2 - ab + b^2(k - 1).$$

If $k > 1$, then for $a \cdot b \geq 0$, it follows

$$b^2 = 0,\ a^2 = 1,\ \ i.e.\ \ a = \pm 1,\ b = 0,$$

respectively for $a \cdot b \leq 0$,

$$b = 0,\ (a + b)^2 = 1,\ \ i.e.\ \ a = \pm 1,\ b = 0,$$

since (for $k \geq 2$) we can not have

$$b^2 = 1,\ (a + b)^2 = 0,\ \ ab = 0,$$

in view of the contradiction

$$a = -b, \text{ and } a = 0.$$

It remains to check the case when $k = 1$. In this case, for $a \cdot b \geq 0$, we have

$$a^2 + ab + b^2 = 1,$$

i.e.

$$a^2 = 1, b = 0 \vee a^2 = 0, b^2 = 1,$$

hence

$$a = \pm 1, b = 0 \vee a = 0, b = \pm 1.$$

For $a \cdot b \leq 0$, we have

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

hence

$$(a+b)^2 = 1,\ ab = 0 \vee (a+b)^2 = 0,\ ab = -1.$$

That means

$$a = \pm 1,\ b = 0 \vee a = 0,\ b = \pm 1 \vee a = \pm 1,\ b = \mp 1.$$

The unities of R essentially determine the structure of the ring R. Therefore, the foregoing (known) results we state in the form of the following theorem:

Theorem 1.3. *The ring R of all algebraic integers in the complex quadratic field $\mathbb{Q}[\sqrt{-D}]$ has the following unities:*

1) If $D \not\equiv -1 \,(mod\, 4)$,

$$u = \pm 1 \vee u = \pm i,\ (D = 1);$$

$$u = \pm 1,\ (D > 1).$$

2) If $D \equiv -1 (mod\, 4)$, *i.e.* $D = 4k - 1,\ (k \geq 1)$,

$$u = a + b\theta,$$

where:

i) $a = \pm 1, b = 0 \ \vee \ a = 0, b = \pm 1 \ \vee \ a = \pm 1, b = \mp 1,\ (k = 1)$;

ii) $a = \pm 1, b = 0,\ (k > 1)$.

2. Euclidean, almost Euclidean, principal ideal, and unique factorization domains

First we recall the following well-known definitions:

Definition 2.1. *A domain $\mathbb{D}$ with unity element e is said to be a principal ideal domain if every ideal A of $\mathbb{D}$ is a principal ideal, i.e. if it is generated by one element $\alpha \in \mathbb{D}$,*

$$A = (\alpha) = \mathbb{D} \cdot \alpha.$$

Definition 2.2. *For a domain $\mathbb{D}$ we say it is a Euclidean domain if on $\mathbb{D}$ we can define a mapping $\varphi : \mathbb{D} \to \mathbb{Z}$, with the following three properties:*

i) $\varphi(\alpha) \geq 0, \quad \varphi(\alpha) = 0 \Leftrightarrow \alpha = 0$;

ii) $\varphi(\alpha\beta) = \varphi(\alpha) \cdot \varphi(\beta), (\alpha, \beta \in \mathbb{D})$;

iii) *for each* $\alpha, \beta \in \mathbb{D}, \beta \neq 0, \quad$ *there exist* $\gamma, \rho \in \mathbb{D}$ *such that*

$$\alpha = \beta\gamma + \rho, \quad \varphi(\rho) < \varphi(\beta),$$

called the Euclidean norm.

Let us remark that from ii) follows

ii') $\varphi(\alpha\beta) \geq \varphi(\alpha), (\alpha, \beta \in \mathbb{D}, \beta \neq 0)$.

The condition ii') is usually taken instead of ii) in the definition of the Euclidean domain.
Since in iii),

$$\rho = 0 \Leftrightarrow \beta \,|\, \alpha,$$

and

$$\rho \neq 0 \Leftrightarrow 0 < \varphi(\alpha - \beta\gamma) < \varphi(\beta),$$

we can replace the condition iii) in definition 2.2. by

iii') *for all* $\alpha, \beta \in \mathbb{D}, \beta \neq 0, \varphi(\alpha) \geq \varphi(\beta), \beta \,|\, \alpha$ or there is $\gamma \in \mathbb{D}$ such that

$$0 < \varphi(\alpha - \beta\gamma) < \varphi(\beta).$$

Thereby, the assumption $\varphi(\alpha) \geq \varphi(\beta)$ is not essential since for $\varphi(\alpha) < \varphi(\beta)$, we can take $\gamma = 0$ and $\rho = \alpha$, to get iii).
Usually, in the definition of the Euclidean domain it is explicitly assumed that $\mathbb{D}$ has a unity element. This is not necessary, since it is well-known that the existence of a unity element follows automatically. Namely, (in view of $\mathbb{D} \neq \{0\}$) the set

$$\{\varphi(\alpha) \,|\, \alpha \in \mathbb{D}, \alpha \neq 0\}$$

is a non-empty subset of $\mathbb{N}$, and therefore there exists a minimal element

$$\varphi(\lambda) = min\{\varphi(\alpha) \,|\, \alpha \in \mathbb{D}, \alpha \neq 0\}.$$

From this it follows that

$$\varphi(\alpha) \geq \varphi(\lambda), (\alpha \in \mathbb{D}, \alpha \neq 0),$$

and therefore, then there exists no element $\gamma \in \mathbb{D}$ with

$$0 < \varphi(\alpha - \lambda\gamma) < \varphi(\lambda),$$

hence we have

$$\lambda \,|\, \alpha,\ i.e.\ \alpha = \lambda\gamma.$$

In particular,

$$\lambda \,|\, \lambda,\ i.e.\ \lambda = e\lambda,\ (\text{for some } e \in \mathbb{D}).$$

But, then

$$\alpha e = e\lambda\gamma = \lambda\gamma = \alpha,$$

and $e \in \mathbb{D}$ is the unity element of $\mathbb{D}$.
The idea arises to replace the condition iii') by the somewhat weaker condition iii") for all $\alpha, \beta \in \mathbb{D},\ \beta \neq 0, \varphi(\alpha) \geq \varphi(\beta), \beta \,|\, \alpha$ or there exist $\delta, \gamma \in \mathbb{D}$ such that

$$0 < \varphi(\alpha\delta - \beta\gamma) < \varphi(\beta).$$

In this way we can generalize the notion of a Euclidean domain:

Definition 2.3. *For a domain $\mathbb{D}$ with a unity element we say that it is an almost Euclidean domain, if it is possible to define on $\mathbb{D}$ a mapping $\varphi : \mathbb{D} \to \mathbb{Z}$, with the properties i), ii'), and iii"), called the Dedekind-Hassean norm.*

The following theorem is well known:

Theorem 2.1. *Every Euclidean domain is a principal ideal domain.*

Proof. The well-known proof of this theorem we will adapt a little to the condition iii').
Let A be an ideal of $\mathbb{D}$. If $A = \{0\}$, then $A = (0)$ is a principal ideal. If $A \neq \{0\}$, then there exists

$$\varphi(\beta) = min\{\varphi(\alpha) \,|\, \alpha \in A, \alpha \neq 0\}.$$

Since $\mathbb{D}\beta \subseteq A$, it suffices to prove that for all $\alpha \in A$, $\alpha \neq 0$ we have

$$\beta \,|\, \alpha,\ i.e.\ \alpha \in \mathbb{D}\beta,\ \text{since surely } 0 \in \mathbb{D}\beta.$$

By the choice of the element β , $\beta \neq 0$ and $\varphi(\alpha) \geq \varphi(\beta)$.
If $\beta \not| \alpha$, then according to iii') there exists $\gamma \in \mathbb{D}$, such that

$$0 < \varphi(\alpha - \beta\gamma) < \varphi(\beta).$$

This is not possible, since $\alpha - \beta\gamma \in A$ and $\alpha - \beta\gamma \neq 0$. □

From the above proof we derive the proof of the following theorem, which in view of the condition *iii"*), differs only in taking

$$0 < \varphi(\alpha\delta - \beta\gamma) < \varphi(\beta),$$

instead of

$$0 < \varphi(\alpha - \beta\gamma) < \varphi(\beta),$$

and thereby $\alpha\delta - \beta\gamma \in A$. That means, the following theorem is also true.

Theorem 2.2. *Every almost Euclidean domain $\mathbb{D}$ is a principal ideal domain.*

This generalization of *Euclidean* to *almost Euclidean domain* has its own reason. Theorem 2.2 is known (ev. without the term "*almost Euclidean domain*"), and is due to *Dedekind* and *Hasse* (see [3], p. 100 and [1], pp. 868, 870). This theorem will be used in the proof of Theorem 3.4 (Section 3.).

It is known that the following theorem is valid.

Theorem 2.3. *Every principal ideal domain $\mathbb{D}$ is a unique factorization domain.*

Therefore in any principal ideal domain $\mathbb{D}$ we can define a mapping $\varphi : \mathbb{D} \to \mathbb{Z}$ with the properties i) and ii) given in Definition 2.3. It is sufficient to take

$$\varphi(\alpha) = 0, (\alpha = 0);$$

$$\varphi(\alpha) = 2^{n_1+\cdots+n_i}, \quad (\alpha = p_1^{n_1} \cdots p_i^{n_i}), \ (\alpha \neq 0).$$

But such a mapping φ also has the property iii"). Actually, if for $\alpha, \beta \in \mathbb{D}, \ \beta \neq 0, \ \varphi(\alpha) \geq \varphi(\beta)$, we have $\beta \,|\, \alpha$, and in this case there is nothing to prove. On the other hand, if $\beta \not| \alpha$:

$$(\alpha, \beta) = (\alpha\delta - \beta\gamma), \quad (\text{for some } \delta, \gamma \in \mathbb{D}),$$

and

$$0 < \varphi(\alpha\delta - \beta\gamma) < \varphi(\beta)$$

follows. Namely,

$$\alpha\delta - \beta\gamma \neq 0, \text{ in view of } \beta \neq 0,$$

and

$$\varphi(\alpha\delta - \beta\gamma) < \varphi(\beta),$$

since

$$(\alpha\delta - \beta\gamma) \,|\, \alpha, \beta,$$

and if

$$\varphi(\alpha\delta - \beta\gamma) = \varphi(\beta),$$

then

$$\alpha\delta - \beta\gamma \sim \beta,$$

hence

$$\beta \,|\, \alpha, \quad \text{since} \quad (\alpha\delta - \beta\gamma) \,|\, \alpha.$$

That means the converse of Theorem 2.2 is valid too, i.e.

Theorem 2.4. *A domain $\mathbb{D}$ is an almost Euclidean domain if and only if $\mathbb{D}$ is a principal ideal domain.*

We close this section with the following theorem needed in the last section.

Theorem 2.5. *Let $\mathbb{D}$ be a domain that is not a field (hence $\mathbb{D}\backslash(\mathcal{U}\cup\{0\}) \neq \emptyset$). If there exists no $\beta \in \mathbb{D}\backslash(\mathcal{U}\cup\{0\})$, such that for all $\alpha \in \mathbb{D}, \beta \,|\, (\alpha - \rho)$ for some $\rho \in \mathcal{U}\cup\{0\}$, then $\mathbb{D}$ is not a Euclidean domain.*

Proof. Suppose on the contrary, that the domain $\mathbb{D}$ satisfying the conditions of the theorem is a Euclidean domain. Then there exists

$$\varphi(\beta) = min\{\varphi(\alpha) \,|\, \alpha \in \mathbb{D}\backslash(\mathcal{U}\cup\{0\})\}.$$

Since $\beta \neq 0$, then for every $\alpha \in \mathbb{D}$, there exist $\delta, \gamma \in \mathbb{D}$ such that

$$\alpha = \beta\gamma + \rho,\ \varphi(\rho) < \varphi(\beta).$$

But, then, by choosing $\beta \in \mathbb{D}$, we have $\rho \in \mathcal{U}\cup\{0\}$, i.e.

$$\beta \,|\, (\alpha - \rho) \text{ for some } \rho \in \mathcal{U}\cup\{0\},$$

a contradiction. □

3. Some counterexamples

The most important examples of Euclidean domains are the ring $\mathbb{Z}$ of rational integers and the polynomial ring $K[x]$ in one variable x over a field K.

The following theorem is well-known:

Theorem 3.1. *If $\mathbb{D}$ is a unique factorization domain, then the polynomial ring $\mathbb{D}[x]$ in one variable (and therefore in finitely many variables) over $\mathbb{D}$ is a unique factorization domain too.*

In particular, the ring $\mathbb{Z}[x_1, \ldots, x_n]$, $(n \geq 1)$ as well as the ring $K[x_1, \ldots, x_n]$, $(n \geq 1)$ is a unique factorization domain. But, for $n \geq 1$, the ring $\mathbb{Z}[x_1, \ldots, x_n]$, and for $n \geq 2$, the ring $K[x_1, \ldots, x_n]$ are not principal ideal domains.

Thus, there are simple counterexamples proving that the converse of Theorem 3.1 is not true.
On the contrary, as we mentioned in the introduction, for a very long time, we have not had any simple counterexample that could prove in an understandable manner that there exist principal ideal domains which are not Euclidean domains.
For the ring R of algebaraic integers in the complex quadratic field $\mathbb{Q}[\sqrt{-D}]$ *Stark* ([6], 1967) proved that R is a principal ideal domain, exactly in the cases when:

$$D = 1, 2, 3, 7, 11, 19, 43, 67, \text{ and } 163.$$

Otherwise, it is known (see [2], Th. 246, p. 213) that the first five of these domains are also Euclidean domains. For the sake of completness we will prove now this known result:

Theorem 3.2. *For $D = 1, 2, 3, 7$, and 11, the ring R of algebraic integers in the field $\mathbb{Q}[\sqrt{-D}]$ is a Euclidean domain with the Euclidean norm φ, $\varphi(\alpha) = \alpha\overline{\alpha}$.*

Proof. For nonzero elements α, β in R, we have $\alpha \cdot \beta^{-1} = x + iy\sqrt{D}$ in $\mathbb{Q}[\sqrt{-D}]$. Let x and y belong to the unit intervals $[u_1, u_2]$ and $[v_1, v_2]$, respectively, where u_i, v_j are rational integers.
If $D = 2$, then we can choose $u + iv\sqrt{2}$ in R such that $|x - u| \leq 1/2$ and $|y - v| \leq 1/2$, and so

$$\alpha = (x + iy\sqrt{2})\beta = (u + iv\sqrt{2})\beta + ((x - u) + i(y - v)\sqrt{2})\beta$$

with

$$\varphi(((x - u) + i(y - v)\sqrt{2})\beta) < \varphi(\beta).$$

If $D = 1, 3, 7$ or 11, then we can find $u + iv\sqrt{D}$ in R such that $|x - u| \leq 1/2$ and $|y - v| \leq 1/4$.
Namely, if x belongs to the first, respectively to the second, half of $[u_1, u_2]$, and y belongs to the first, respectively to the fourth, quarter of $[v_1, v_2]$, then we can choose $u = u_1$, respectively $u = u_2$, and $v = v_1$, respectively $v = v_2$. Finally, if y belongs to the second or to the third quarter of $[v_1, v_2]$, we can take $u = (u_1 + u_2)/2$ and $v = (v_1 + v_2)/2$. Then we have

$$\alpha = (x + iy\sqrt{D}) \cdot \beta = (u + iv\sqrt{D}) \cdot \beta + ((x - u) + i(y - v)\sqrt{D}) \cdot \beta$$

with

$$\begin{aligned} \varphi(((x - u) + i(y - v)\sqrt{D}) \cdot \beta) &= (\,|\,x - u\,|\,^2 + \,|\,y - v\,|\,^2 D) \cdot \varphi(\beta) \\ &= (4 + D)/16 \cdot \varphi(\beta) < \varphi(\beta). \end{aligned}$$

□

For the ring R with $D = 19$ (with $D = 19, 43, 67$, and 163) it is not difficult to prove that it is a principal ideal, but not a Euclidean domain. The proofs in [8] and [1] that R, for $D = 19$, is a principal ideal domain are based on Theorem 2.3 and differ only in the proof of the following theorem:

Theorem 3.3. *The ring R of algebraic integers in the complex quadratic field $\mathbb{Q}[\sqrt{-19}]$ is an almost Euclidean domain.*

Proof. Since $D = 4 \cdot 5 - 1$,

$$R = \{a + b\theta \mid \ a, b \in \mathbb{Z}\},$$

and R has the set of all unities

$$\mathcal{U} = \{1, -1\}.$$

Moreover, on R we define the mapping

$$\varphi : R \to \mathbb{Z}, \quad \varphi(\alpha) = \alpha\overline{\alpha}, (\alpha \in R),$$

with properties i) *and* ii) from Definition 2.2. We prove that φ has the property iii) too. Let $\alpha, \beta \in R$, $\beta \neq 0$ and $\varphi(\alpha) \geq \varphi(\beta)$. If $\beta \,|\, \alpha$, we have nothing to prove. Otherwise, we have to prove that there exist $\delta, \gamma \in R$, such that

$$0 < \varphi(\alpha\delta - \beta\gamma) < \varphi(\beta).$$

This is equivalent to

$$0 < \varphi((\alpha/\beta)\delta - \gamma) < \varphi(1).$$

In the proof of the last relation, we will follow the proof from [8]. For

$$\alpha, \beta \in R, \alpha \neq 0, \beta \neq 0, \beta \not| \alpha,$$

we have

$$\alpha/\beta = (a + b\sqrt{-19})/c, \quad (a, b, c \in \mathbb{Z},\ (a, b, c) = 1).$$

Therefore $c > 1$, since for $c = 1$, $\alpha/\beta \in R$, i.e. $\beta \,|\, \alpha$.
Suppose that $c \geq 5$, and choose the rational integers d, e, f, q, r so that

$$ae + bd + cf = 1,$$

$$ad - 19bc = cq + r, \ |\, r \,| \ < c/2.$$

This is possible, since $\mathbb{Z}$ is a Euclidean domain, hence also a principal ideal domain, and $(a, b, c) = 1$. We set now

$$\delta = d + e\sqrt{-19}, \gamma = q - f\sqrt{-19}.$$

Then

$$(\alpha/\beta)\delta - \gamma = (a + b\sqrt{-19})(d + e\sqrt{-19})/c - (q - f\sqrt{-19}) = r/c + \sqrt{-19}/c.$$

The complex number

$$r/c + \sqrt{-19}/c \neq 0,$$

and moreover

$$\varphi((r + \sqrt{-19})/c) = (r^2 + 19)/c^2 < 1,$$

in view of

$$|\, r \,| \ \leq c/2 \ \text{ and } \ c \geq 5.$$

Namely, for $c \geq 6$,

$$\begin{aligned} (r^2 + 19)/c^2 \leq & \quad (c^2/4 + 19)/c^2 = 1/4 + 19/c^2 \\ \leq & \quad 1/4 + 19/36 = 112/144 < 1, \end{aligned}$$

and for $c = 5$, $|\, r \,| \ \leq 2$, i.e.

$$(r^2 + 19)/c^2 \leq (4 + 19)/c^2 = 23/25 < 1.$$

It remains to check the cases $c = 2, c = 3$, and $c = 4$, which will be considered separately:

i) $\underline{c = 2}$. From $\beta \not| \alpha$ and $(a, b, c) = 1$ it follows that a, b are of different parities.

We set

$$\delta = 1, \text{ and } \gamma = [(a-1) + b\sqrt{-19}]/2 = [(a-1) - b]/2 + b\theta.$$

Surely, $\delta, \gamma \in R$. Moreover,

$$(\alpha/\beta)\delta - \gamma = 1/2 \neq 0$$

and has the norm

$$\varphi((\alpha/\beta)\delta - \gamma) = \varphi(1/2) = 1/4 < 1.$$

ii) $\underline{c = 3}$. Then $(a, b, c) = 1$ implies

$$a^2 + 19b^2 \equiv a^2 + b^2 \not\equiv 0 \ (mod\, 3).$$

Let

$$\delta = a - b\sqrt{-19}, \quad \gamma = q,$$

where

$$a^2 + 19b^2 = 3q + r, \quad r = 1 \text{ or } r = 2.$$

Then

$$(\alpha/\beta)\delta - \gamma = r/3 \neq 0$$

and has the norm

$$\varphi((\alpha/\beta)\delta - \gamma) < 1.$$

iii) $\underline{c= 4}$. In this case a and b are not both even. If they are elements of different parities

$$a^2 + 19b^2 \equiv a^2 - b^2 \not\equiv 0 \ (mod\, 4).$$

Let

$$\delta = a - b\sqrt{-19}, \quad \gamma = q,$$

where

$$a^2 + 19b^2 = 4q + r, \quad 0 < r < 4.$$

Then

$$(\alpha/\beta)\delta - \gamma = r/4 \neq 0$$

and has the norm

$$\varphi((\alpha/\beta)\delta - \gamma) < 1.$$

If a, b are both odd, then

$$a^2 + 19b^2 \equiv a^2 + 3b^2 \not\equiv 0 \ (mod\, 8).$$

Let

$$\delta = (a - b\sqrt{-19})/2 = (a+b)/2 - b\theta \in R, \quad \gamma = q,$$

where

$$a^2 + 19b^2 = 8q + r, \quad 0 < r < 8.$$

Then

$$(\alpha/\beta)\delta - \gamma = r/8 \neq 0,$$

and

$$\varphi((\alpha/\beta)\delta - \gamma) < 1.$$

So, Theorem 3.3. has been proved. □

The proofs of the theorems in [8], [7], and [1], asserting that certain R in $\mathbb{Q}[\sqrt{-D}]$ are not Euclidean domains differ slightly, but only those in [8] and [7] are directly based on Theorem 2.5.

Following [7] we will now prove the theorem:

Theorem 3.4. *The ring R of algebraic integers in the complex quadratic field $\mathbb{Q}[\sqrt{-D}]$ is not a Euclidean domain for $D = 19, 43, 67,$ and 163.*

Proof. Since

$$D \equiv -1 (mod\, 4), \ i.e.\ D = 4k - 1, (k = 5, 11, 17, 41),$$

in view of Section 2.

$$R = \{a + b\theta \,|\, a, b \in \mathbb{Z}\}$$

is an integral domain with unity element 1 and the set of unities

$$\mathcal{U} = \{1, -1\}.$$

Moreover, the mapping

$$\varphi : R \to \mathbb{Z}, \quad \varphi(\alpha) = \alpha\overline{\alpha}, \quad (\alpha \in R),$$

has the properties i) and ii) of the Euclidean norm.
Here we modify somewhat the proof from [7]. If R were a Euclidean domain with a Euclidean norm ψ, then there would exist

$$\psi(\beta) = min\{\psi(\alpha) \,|\, \alpha \in R\backslash(\mathcal{U} \cup \{0\})\}, \quad (\beta \in R, \beta \neq 0),$$

and for every $\alpha \in R$, we would have

$$\alpha = \beta\gamma + \rho, \text{ for some } \gamma, \rho \in R, \rho = 0 \vee \psi(\rho) < \psi(\beta),$$

i.e.

$$\beta \,|\, (\alpha - \rho), \rho \in \mathcal{U} \cup \{0\} = \{1, -1, 0\}.$$

In particular, this would be true for $\alpha = 2$, and so we would have

$$\beta \,|\, 2 \text{ or } \beta \,|\, 3, \text{ since } \beta \not| 2 - 1 = 1.$$

From now on we follow again the proof from [7].
But, 2 and 3 are not reducible in R. Namely, if

$$2 = (a + b\theta)(c + d\theta), (a + b\theta \notin \mathcal{U}, c + d\theta \notin \mathcal{U}),$$

then

$$4 = \varphi(2) = \varphi(a + b\theta)\varphi(c + d\theta),$$

i.e.

$$2 = \varphi(a + b\theta) = \varphi(c + d\theta),$$

since

$$1 \neq \varphi(a + b\theta) \in \mathbb{Z}, 1 \neq \varphi(c + d\theta) \in \mathbb{Z}.$$

From this it follows that

$$\begin{aligned} 2 = &\quad \varphi(a + b\theta) = (a + b/2 + \sqrt{-D}b/2)(a + b/2 - \sqrt{-D}b/2) \\ = &\quad a^2 + ab + b^2/4 + (4k - 1)b^2/4 = a^2 + ab + b^2k. \end{aligned}$$

Hence, for $ab \geq 0$, in view of $k \geq 5, b = 0$, and for $ab \leq 0$,

$$\begin{aligned} 2 = &\quad \varphi(a + b\theta) = \varphi(a + b\overline{\theta}) = \varphi(a + b - b/2 - \sqrt{-D}b/2) \\ = &\quad (a + b - b/2)^2 + (4k - 1)b^2/4 = (a + b)^2 - ab + b^2(k - 1), \end{aligned}$$

hence, $b = 0$ also.
Similarly, we could prove $d = 0$, and hence $2 = ab$, would be a nontrivial presentation of 2 in $\mathbb{Z}$ as a product of primes, which is impossible.
Similarly one can prove that 3 is not reducible in R.
We have had

$$\beta \,|\, 2 \text{ or } \beta \,|\, 3,$$

and so

$$\beta = \pm 2 \text{ or } \beta = \pm 3.$$

But, none of these four numbers can divide

$$\theta, \ \theta + 1, \ \theta - 1,$$

for otherwise

$$\begin{aligned} \beta \,|\, \theta &\quad \Rightarrow \quad \varphi(\beta) \,|\, \varphi(\theta), \\ \beta \,|\, (\theta + 1) &\quad \Rightarrow \quad \varphi(\beta) \,|\, \varphi(\theta + 1), \\ \beta \,|\, (\theta - 1) &\quad \Rightarrow \quad \varphi(\beta) \,|\, \varphi(\theta - 1). \end{aligned}$$

This is impossible, since

$$\varphi(\beta) = 4 \text{ or } \varphi(\beta) = 9,$$

and

$$\begin{aligned} \varphi(\theta) &= (1/2+\sqrt{-D}/2)(1/2-\sqrt{-D}/2) = 1/4+(4k-1)/4 = k, \\ \varphi(\theta+1) &= (3/2+\sqrt{-D}/2)(3/2-\sqrt{-D}/2) = 9/4+k-1/4 = k+2, \\ \varphi(\theta-1) &= (-1/2+\sqrt{-D}/2)(-1/2-\sqrt{-D}/2) = 1/4+(4k-1)/4 = k. \end{aligned}$$

□

Let us remark, that in this proof we have not used Theorem 2.5. Why was this theorem then used in [7]? In the proof given in [7] one takes an arbitrary element $\beta \in R\backslash(\mathcal{U} \cup \{0\})$ with the property

$$\beta \,|\, (\alpha - \rho) \text{ for each } \alpha \in R \text{ and some } \rho \in (\mathcal{U} \cup \{0\}).$$

For such an element β all remaining arguments in the above proof are valid, and thus such $\beta \in R\backslash(\mathcal{U} \cup \{0\})$ does not exist.

In view of Theorem 2.5 R is not a Euclidean domain.
It is clear that this small modification of the proof of Theorem 3.4. used later in [1], was not used in [7]. By this modification one cannot get much more, since the proof that for

$$\varphi(\beta) = min\{\varphi(\alpha) \,|\, \alpha \in R\backslash(\mathcal{U} \cup \{0\})\}, (\beta \in R, \beta \neq 0),$$

we have

$$\beta \,|\, (\alpha - \rho) \quad \text{for all} \quad \alpha \in R, \alpha \neq 0 \quad \text{and some} \quad \rho \in (\mathcal{U} \cup \{0\}),$$

is actually equivalent to the proof of Theorem 3.5.

We will close this article with another well-known counterexample.
In view of the mentioned result of Stark there are not many rings R of algebraic integers in the complex quadratic field $\mathbb{Q}[\sqrt{-D}]$ which are principal ideal domains. It is known that the ring R for $D = 5$ is not a unique factorization domain. Namely, in this ring

$$\mathcal{U} = \{1, -1\} \text{ and the numbers } 3, 2+\sqrt{5}, 2-\sqrt{5}$$

are not irreducible, and

$$9 = 3 \cdot 3 = (2+\sqrt{5})(2-\sqrt{5})$$

are nonequivalent presentations of 9 as a product of non-reducible elements.

References

[1] Campoli, O. A., A Principal Ideal Domain that is not a Euclidean Domain. American Math. Monthly 95 No. 9 (1988), 868-871.

[2] Hardy, G. H., Wright, E. M., An Introduction to the Theory of Numbers. Oxford, New York (1962), Theorem 246, p. 213.

[3] Motzkin, T., The Euclidean Algorithm, Bull. Amer. Math. Soc. 55 (1949), 1142-1146.

[4] Perić, V., Algebra Vol. 1, third edition. IGKRO Svjetlost, Sarajevo, 1991.

[5] Pollard, H., The Theory of Algebraic Numbers. Carus Monograph 9, MAA, Wiley, New York, 1950.

[6] Stark, H. M., A Complete Determination of the Complex Quadratic Fields of Class - Number One. Michigan Math. J. 14 (1967), 1-27.

[7] Williams, K. S., Note on Non-Euclidean Principal Ideal Domains. Math. Mag. Vol. 48, No. 3 (1975), 176-177.

[8] Wilson, J. C., A Principal Ideal Ring That is Not a Euclidean Ring. Math. Mag. 46 No. 1 (1973), 34-38.

Received by the editors May 7, 2008