A Principal Ideal Domain which does not allow for a Euclidean function

Francesco Vercellesi
francesco.vercellesi@sns.it

Abstract
A proof that the integral domain $\mathbb{Z}\left[\left(1+i\sqrt{19}\right)/2\right]$ has principal ideals but does not allow for any Euclidean function.

Contents

From now on we will denote:

$$\omega = \frac{1}{2} + i\frac{\sqrt{19}}{2}, \quad D = \mathbb{Z}[\omega]$$

We will first prove that D is not Euclidean and then that its ideals are principal. First, we characterise the elements of D.

Lemma 0.1: The elements of D are all and only the complex numbers of the form:

$$\frac{\alpha}{2} + i\frac{\beta}{2}\sqrt{19}, \quad a \equiv_2 b$$

Proof: Just by summing integer multiples of ω^0 and ω^1 we can obtain all numbers of the given form, so all of them must be in D.
If we now show that numbers of the given form are closed under addition and multiplication we would be done, since:
1. closedness under multiplication would give that powers of ω and all monomials of the forms $k\omega^n$ for $k \in \mathbb{Z}$ and $n \in \mathbb{N}$ are in D;
2. closedness under addition would then give that all integer polynomials evaluated at ω are in D.

Let us prove closedness under addition. Let:

$$z_1 = \frac{\alpha}{2} + i\frac{\beta}{2}\sqrt{19}, \quad z_2 = \gamma + i\frac{\delta}{2}\sqrt{19}, \quad \alpha \equiv_2 \beta, \quad \gamma \equiv_2 \delta$$

then:

$$z_1 + z_2 = \frac{\alpha+\gamma}{2} + i\frac{\beta+\delta}{2}\sqrt{19}, \quad \alpha+\gamma \equiv_2 \beta+\delta$$

which shows that the sum is also of the given form.

Let us prove closedness under multiplication. Let:

$$z_1 = \frac{\alpha}{2} + i\frac{\beta}{2}\sqrt{19}, \quad z_2 = \gamma + i\frac{\delta}{2}\sqrt{19}, \quad \alpha \equiv_2 \beta, \quad \gamma \equiv_2 \delta$$

then:

$$z_1 z_2 = \frac{\alpha\gamma - 19\beta\delta}{4} + \frac{\alpha\delta + \beta\gamma}{4} i\sqrt{19}$$

Obviously:

$$\alpha\gamma \underset{2}{\equiv} 19\beta\delta, \quad \alpha\delta \underset{2}{\equiv} \beta\gamma$$

so the numerators in the two fractions are even. Then we can write:

$$z_1 z_2 = \frac{(\alpha\gamma - 19\beta\delta)/2}{2} + \frac{(\alpha\delta + \beta\gamma)/2}{2} i\sqrt{19}$$

where the numerators are integers. Now showing that they also have the same parity amounts to showing that:

$$\alpha\gamma - 19\beta\delta \underset{4}{\equiv} \alpha\delta + \beta\gamma$$

but since:

$$\begin{aligned}
& 2 \mid (\alpha - \beta) \wedge 2 \mid (\gamma - \delta) \\
\Longrightarrow\ & (\alpha - \beta)(\gamma - \delta) \underset{4}{\equiv} 0 \\
\Longrightarrow\ & \alpha\gamma - \alpha\delta - \beta\gamma + \beta\delta \underset{4}{\equiv} 0 \\
\Longrightarrow\ & \alpha\gamma - 19\beta\delta \underset{4}{\equiv} \alpha\delta + \beta\gamma
\end{aligned}$$

as we wanted. ■

1. D is not Euclidean

Definition 1.1: Given a domain R we say that $x \in R$ is a *universal side divisor* if and only if it is not zero, not a unit and one can write:

$$y = \gamma x + \delta$$

for some $\gamma \in R$, $\delta \in \{0\} \cup R^*$.

Lemma 1.1: An Euclidean Domain R which is not a field always has a universal side divisor.

Proof: Let us consider the set $R' = (R \setminus R^*) \setminus \{0\}$. Since R is not a field, R' is nonempty and therefore the Euclidean function g has a minimum on it. Let $x \in R'$ be an element that minimizes g.

Then for all $y \in R$ we can perform Euclidean division and write:

$$y = \gamma x + \delta$$

where $g(\delta) < g(x)$. But since x minimizes g over the non invertibles, δ must be invertible or zero. ■

Theorem 1.2: D has no universal side divisor.

Proof: Let N be the square of the complex norm. Note that:

$$N\left(\frac{\alpha}{2} + i\frac{\beta}{2}\sqrt{19}\right) = \frac{1}{4}(\alpha^2 + 19\beta^2)$$

Let us list the lowest values attained by N on D.
When $\beta^2 = 0$, α and α^2 must be even. To have $N \leq 9$ we must have $\alpha^2 \leq 36$.
When $\beta^2 = 1$, α and α^2 must be odd. To have $N \leq 9$ we must have $\alpha^2 \leq 9$.
When $\beta^2 > 1$, no value of α^2 can verify $N \leq 9$.

We can list this values:
- $N(x) = 0 \Longleftrightarrow x = 0$;
- $N(x) = 1 \Longleftrightarrow x = \pm 1$;
- $N(x) = 4 \Longleftrightarrow x = \pm 2$;
- $N(x) = 5 \Longleftrightarrow x = \pm 1/2 \pm i\sqrt{19}/2$;
- $N(x) = 7 \Longleftrightarrow x = \pm 3/2 \pm i\sqrt{19}/2$;
- $N(x) = 9 \Longleftrightarrow x = \pm 3$;
- $N(x) > 9$ for all other x.

Since N is multiplicative and assumes no values between 0 and 1 the only units in D are ± 1.

Aiming for a contradiction, we now assume D has a universal side divisor ξ. This would mean that for all $y \in D$ we could write either of:

$$y = k\xi, \quad y = k\xi + 1, \quad y = k\xi - 1$$

We will now analyze multiple cases.

Case 1: If $N(\xi) > 9$ we take any $y \in D$ such that $N(y) = 4$. If we could write $y = k\xi$, that would mean $N(k) = N(y)/N(\xi) = 4/9$ which we have already seen is not a value N can attain.

Therefore it must hold that $y = k\xi \pm 1$. But now the triangular inequality gives:

$$3 = |y| + 1 \geq |y \pm 1| = |k\xi| > 3$$

↯

Case 2: If instead $N(\xi) \in \{5, 7, 9\}$ we would have to write all y such that $N(y) \in \{4, 5, 7, 9\}$ as

$$y = k\xi \text{ or } y = k\xi \pm 1$$

where $k \in \{-1, 0, 1\}$. If that were not the case, we would have $N(k) \geq 4$ and the triangular inequality would give either of:

$$4 \geq |y| + 1 \geq |y \pm 1| = |k\xi| \geq \sqrt{4 \cdot 5} > 4$$
$$3 \geq |y| = |k\xi| \geq \sqrt{4 \cdot 5} > 4$$

Then we only have 9 possible combinations to write the 12 elements $y \in D$ such that $N(y) \in \{4, 5, 7, 9\}$. ↯

Case 3: If $N(\xi) = 4$, it would be enough to have $y \in D$ such that $N(y) = 5$ and $y \neq \xi \pm 1$. Obviously we can't have either $y = 0\xi$, $y = 0\xi \pm 1$, or $y = \xi$ since:

$$N(0\xi) = 0, \quad N(0\xi \pm 1) = 1, \quad N(\xi) = 4$$

and instead $N(y) = 5$.

If $N(k) > 1$ then by the triangular inequality we would have either:

$$4 > |y| + 1 \geq |y \pm 1| = |k\xi| \geq \sqrt{4 \cdot 4} = 4$$
$$3 > |y| = |k\xi| \geq \sqrt{4 \cdot 4} = 4$$

But now since $N(\xi) = 4$ implies $\xi \in \mathbb{R}$, and all $y \in D$ such that $N(y) = 5$ are not real, it's easy to see that we can choose y with the desired properties. ↯

■

Corollary 1.2.1: D is not an Euclidean Domain.

Proof: Aiming for a contradiction we assume D is an Euclidean Domain. Then by Lemma 1.1 D would have a universal side divisor. But by Theorem 1.2 we know D has no universal side divisor. ↯

■

2. D has principal ideals

Definition 2.1: Given an integral domain R, we say that $H : R \to \mathbb{N}$ is a *Dedekind-Hasse norm* if for all $u, v \in R$ the following hold:
- $H(u) = 0 \iff u = 0$;
- $u \mid v$ or there are $s, t \in R$ such that $0 < H(su + tv) < H(u)$.

Lemma 2.1: If a ring R has a Dedekind-Hasse norm H, then R has principal ideals.

Proof: Let $I \subseteq R$ be an ideal. If $I = \{0\}$ then it is generated by 0, so we can assume $I \setminus \{0\}$ is nonempty and therefore take $x \in I \setminus \{0\}$ which minimizes H.

We want to show that $I = (x)$. Obviously, since $x \in I$ we have $(x) \subseteq I$ so we only have to prove $I \subseteq (x)$.
Given $y \in I$ either:
- $x \mid y$ and therefore $y \in (x)$;
- $x \nmid y$ and we can choose $s, t \in R$ such that $0 < H(sx + ty) < H(x)$. But $sx + ty \in I$ so this would contradict the fact that x was chosen to minimize H in $I \setminus \{0\}$.

■

Theorem 2.2: On the domain D, the square of the complex norm N is a Dedekind-Hasse norm.

Proof: We want to show that given $u, v \in D$ such $u \nmid v$ there are $s, t \in D$ such that:

$$|su - tv| < |u|, \quad su \neq tv$$

We will now embed D in $\mathbb{C}$ to be able to perform divisions and rewrite the previous condition as:

$$0 < \left|s - t\frac{v}{u}\right| < 1$$

It is now useful to note that the elements of D are placed on the horizontal lines $\mathfrak{I}(z) = k\sqrt{19}/2$ in the complex plane, and that on these lines they are evenly spaced, 1 unit apart from each other.

Let us now consider two cases:

Case 1: If for some integer k:

$$\mathfrak{I}\left(\frac{v}{u}\right) \in \left(k\frac{\sqrt{19}}{2} - \frac{\sqrt{3}}{2}, k\frac{\sqrt{19}}{2} + \frac{\sqrt{3}}{2}\right)$$

From our previous observation we know that we can choose an element $s \in D$ such that:

$$\mathfrak{I}(s) = k\frac{\sqrt{19}}{2}, \quad \left|\mathfrak{R}(s) - \mathfrak{R}\left(\frac{v}{u}\right)\right| \leq \frac{1}{2}$$

which in turn means that choosing $t = 1$ yields:

$$\left|s - t\frac{v}{u}\right| = \sqrt{\left(\mathfrak{R}(s) - \mathfrak{R}\left(\frac{v}{u}\right)\right)^2 + \left(\mathfrak{I}(s) - \mathfrak{I}\left(\frac{v}{u}\right)\right)^2} < \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = 1$$

If now we had:

$$\left|s - t\frac{v}{u}\right| = 0$$

that would mean:

$$su = v$$

which contradicts the hypothesis that $u \nmid v$.

Case 2: Otherwise we would have:

$$\begin{aligned}
&\mathfrak{I}\left(\frac{v}{u}\right) \in \left[k\frac{\sqrt{19}}{2} + \frac{\sqrt{3}}{2}, (k+1)\frac{\sqrt{19}}{2} - \frac{\sqrt{3}}{2}\right] \\
\Longrightarrow\ &\mathfrak{I}\left(2\frac{v}{u}\right) \in \left[k\sqrt{19} + \sqrt{3}, (k+1)\sqrt{19} - \sqrt{3}\right] \\
\Longrightarrow\ &\mathfrak{I}\left(2\frac{v}{u}\right) \in \left[(2k+1)\frac{\sqrt{19}}{2} - \frac{\sqrt{19} - 2\sqrt{3}}{2}, (2k+1)\frac{\sqrt{19}}{2} + \frac{\sqrt{19} - 2\sqrt{3}}{2}\right] \\
\Longrightarrow\ &\mathfrak{I}\left(2\frac{v}{u}\right) \in \left((2k+1)\frac{\sqrt{19}}{2} - \frac{\sqrt{3}}{2}, (2k+1)\frac{\sqrt{19}}{2} + \frac{\sqrt{3}}{2}\right)
\end{aligned}$$

which means that just like before we can choose $s \in D$ such that:

$$\mathfrak{I}(s) = (2k+1)\frac{\sqrt{19}}{2}, \quad \left|\mathfrak{R}(s) - \mathfrak{R}\left(2\frac{v}{u}\right)\right| \leq \frac{1}{2}$$

which immediately gives:

$$\left|s - 2\frac{v}{u}\right| < 1$$

If $s - 2v/u \neq 0$ we are done. Otherwise we have $(s/2)u = v$.
If $s/2 \in D$ again we contradict the hypothesis that $u \nmid v$. So we are left to consider the case where $(s/2) \notin D$.

Our goal is now to show that in this case we can choose: $t' = 2\overline{v/u}$ and an integer s' such that:

$$0 < \left|s' - t'\frac{v}{u}\right| < 1$$

First of all, let us show that $t' \in D$:

$$t' = 2\overline{\left(\frac{v}{u}\right)} = 2\overline{\left(\frac{s}{2}\right)} = \overline{s}$$

and since D is closed by conjugation and $s \in D$ this shows our goal.

Furthermore we notice that:

$$t'\frac{v}{u} = 2\overline{\left(\frac{v}{u}\right)}\left(\frac{v}{u}\right) = 2\left|\frac{v}{u}\right|^2 = 2\left|\frac{s}{2}\right|^2$$

is a real number. If it is not an integer, we can choose s' to be the closest integer to it and immediately obtain our goal.

After writing:

$$s = \frac{\alpha}{2} + i\frac{\beta}{2}\sqrt{19}, \quad \alpha \underset{2}{\equiv} \beta$$

the following cases cover all the cases where $s/2 \notin D$.
Subcase 1: If α and β are odd we have:

$$2\left|\frac{s}{2}\right|^2 = \frac{\alpha^2 + 19\beta^2}{8}$$

But we have:

$$\alpha^2 \underset{8}{\equiv} \beta^2 \underset{8}{\equiv} 1 \Longrightarrow \alpha^2 + 19\beta^2 \underset{8}{\equiv} 4$$

which means that the above fraction can't be an integer.
Subcase 2: If α and β are even and:

$$\alpha \underset{4}{\not\equiv} \beta$$

we have:

$$\frac{s}{2} = \frac{\alpha'}{2} + i\frac{\beta'}{2}\sqrt{19}$$

where either $\alpha' = \alpha/2$ is even and $\beta' = \beta/2$ is odd or viceversa. Then:

$$2\left|\frac{s}{2}\right|^2 = \frac{\alpha'^2 + 19\beta'^2}{2}$$

but $\alpha'^2 + 19\beta'^2$ is odd and the above fraction can't be an integer.

■

Corollary 2.2.1: D has principal ideals.

Proof: By Theorem 2.2 we know D has a Dedekind-Hasse norm and by Lemma 2.1 we know this implies having principal ideals. ■