A Ring that is a PID but not an ED

Bajtek Rogue

October 29, 2025

Motivation

When studying rings, we encounter the fact that all Euclidean domains are principal ideal domains. A natural question arises: is the converse true? In this paper, we prove that it is not. Specifically, the converse fails for the ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. To establish this result, we require two useful lemmas.

Lemmas

Lemma 1. *Let R be a ring. A function $N : R \to \mathbb{N}$ is called a **Dedekind–Hasse norm** if*

$$\forall a, b \in R \setminus \{0\} \quad b \nmid a \implies \exists s, t \in R \quad 0 < N(sa - tb) < N(b).$$

If R has a Dedekind–Hasse norm, then R is a principal ideal domain.

Proof. Suppose R is a ring with Dedekind–Hasse norm $N : R \to \mathbb{N}$. Let $I \lhd R$ be any ideal of R. Take $g = \arg\min_{i \in I \setminus \{0\}} N(i)$. Since $\varnothing \neq \{N(i) : i \in I \setminus \{0\}\} \subseteq \mathbb{N}$, such a g exists by the well-ordering principle on $\mathbb{N}$. Now let $i \in I$.

Case 1: $g \mid i$.
Then $i = gx$ for some $x \in R$, and thus $i \in \langle g \rangle$.

Case 2: $g \nmid i$.
Since N is a Dedekind–Hasse norm, there exist $s, t \in R$ such that $0 < N(si - tg) < N(g)$. We have $si - tg \in \langle i, g \rangle \subseteq I$ since $i \in I$, so $si - tg \in I$. But this contradicts the minimality of the norm of g, so this case is impossible.

Thus $i \in \langle g \rangle$, but i was arbitrary, so $I \subseteq \langle g \rangle$. Since $g \in I$, we have $\langle g \rangle \subseteq I$, and therefore $I = \langle g \rangle$. Hence R is a principal ideal domain. □

Lemma 2. *Let R be a ring. An element $u \in R \setminus (R^* \cup \{0\})$ is called a **universal side divisor** if*

$$\forall x \in R \; \exists y \in R^* \cup \{0\} \quad u \mid x - y.$$

If R is a Euclidean domain, then R has a universal side divisor.

Proof. Suppose R is a Euclidean domain with norm $N : R \to \mathbb{N}$. Take $u = \underset{a \in R \setminus (R^* \cup \{0\})}{\arg\min} N(a)$. Since $\varnothing \neq \{N(a) : a \in R \setminus (R^* \cup \{0\})\} \subseteq \mathbb{N}$, such a u exists by the well-ordering principle on $\mathbb{N}$. Let $x \in R$. By the division algorithm, we can write $x = uq + r$ where $q, r \in R$.

Case 1: $r = 0$.

Then $u \mid x$, so $u \mid x - 0$. Since $0 \in R^* \cup \{0\}$, we have that u is a universal side divisor.

Case 2: $r \neq 0$.

Then $N(r) < N(u)$, and by the minimality of $N(u)$, we know that $r \in R^* \cup \{0\}$. Moreover, $u \mid x - r$, so u is a universal side divisor. $\square$

Constructing a Dedekind–Hasse Norm

Consider the ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ and the function $N : \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \to \mathbb{N}$ given by

$$N\left(a + b\frac{1+\sqrt{-19}}{2}\right) = \left(a + b\frac{1+\sqrt{-19}}{2}\right) \cdot \left(a + b\frac{1-\sqrt{-19}}{2}\right).$$

We can easily verify that $N\left(a + b\frac{1+\sqrt{-19}}{2}\right) = a^2 + ab + 5b^2$. Since N is the norm map from complex numbers, N is multiplicative. Moreover, $N(a + b\sqrt{-19}) = a^2 + 19b^2$.

If $n, m \in \mathbb{Z}$, then $n + m\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ since

$$n + m\sqrt{-19} = (n - m) + 2m \cdot \frac{1+\sqrt{-19}}{2}.$$

Take $\alpha, \beta \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ with $\alpha, \beta \neq 0$ and $\beta \nmid \alpha$. Thus $\frac{\alpha}{\beta} \notin \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. However, $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{-19})$ since $\mathbb{Q}(\sqrt{-19})$ is the smallest field containing $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Hence we can write $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{c}$ where $a, b, c \in \mathbb{Z}$. Without loss of generality, we may assume that $\gcd(a, b, c) = 1$ and $c > 0$. Also, $c \geq 2$ since if $c = 1$, then $\frac{\alpha}{\beta} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, which contradicts our assumption.

Note that the condition $0 < N(s\alpha - t\beta) < N(\beta)$ is equivalent to $0 < N\left(s \cdot \frac{\alpha}{\beta} - t\right) < N(1) = 1$ by the multiplicativity of N.

Case 1: $c \geq 6$

By Bézout's identity, we can write $ax + by + cz = 1$ for some $x, y, z \in \mathbb{Z}$. Now perform division with remainder in integers of $ay - 19bx$ by c to get $ay - 19bx = qc + r$, where r is chosen so that $|r| \leq \frac{c}{2}$. Put $s = y + x\sqrt{-19}$

and $t = q - z\sqrt{-19}$. We obtain

$$
\begin{aligned}
s \cdot \frac{\alpha}{\beta} - t &= (y + x\sqrt{-19}) \cdot \frac{a + b\sqrt{-19}}{c} - (q - z\sqrt{-19}) \\
&= \frac{(ay - 19bx) + (ax + by)\sqrt{-19}}{c} + \frac{-qc + cz\sqrt{-19}}{c} \\
&= \frac{(ay - 19bx - qc) + (ax + by + cz)\sqrt{-19}}{c}.
\end{aligned}
$$

Recall that $ax+by+cz = 1$ and $ay-19bx-qc = r$. We get $s \cdot \frac{\alpha}{\beta} - t = \frac{r+\sqrt{-19}}{c}$, and

$$
N\left(\frac{r + \sqrt{-19}}{c}\right) = \frac{r^2 + 19}{c^2} \leq \frac{\frac{c^2}{4} + 19}{c^2} = \frac{1}{4} + \frac{19}{c^2}.
$$

If $c \geq 6$, then $\frac{1}{4} + \frac{19}{c^2} < 1$, so N satisfies the Dedekind–Hasse norm property. It remains to check the values $c \in \{2, 3, 4, 5\}$.

Case 2: $c = 2$

Let $c = 2$. Then $a \not\equiv b \pmod 2$, because if $a \equiv b \equiv 0 \pmod 2$, then $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Put $s = 1$ and $t = \frac{a-b-1}{2} + b \cdot \frac{1+\sqrt{-19}}{2}$. Note that $\frac{a-b-1}{2} \in \mathbb{Z}$ because $a \not\equiv b \pmod 2$. We get

$$
s \cdot \frac{\alpha}{\beta} - t = 1 \cdot \frac{a + b\sqrt{-19}}{2} - \left(\frac{a - b - 1}{2} + b \cdot \frac{1 + \sqrt{-19}}{2}\right) = \frac{1}{2},
$$

and $0 < N\left(\frac{1}{2}\right) = \frac{1}{4} < 1$, as needed.

Case 3: $c = 3$

Let $c = 3$. If $a \equiv b \equiv 0 \pmod 3$, then $\gcd(a, b, c) = 3 > 1$, which is impossible. Recall that $\forall n \in \mathbb{Z}$, we have $n^2 \equiv 0$ or $1 \pmod 3$. Thus $a^2+b^2 \equiv 0 \pmod 3$ if and only if $a \equiv b \equiv 0 \pmod 3$. But we know this is not true, so $a^2 + b^2 \not\equiv 0 \pmod 3$. Also, $a^2 + 19b^2 \equiv a^2 + b^2 \pmod 3$, so $a^2 + 19b^2 \not\equiv 0 \pmod 3$.

Now perform division with remainder in integers of $a^2 + 19b^2$ by 3 to get $a^2 + 19b^2 = 3q + r$, where $r \in \{1, 2\}$ by the previous argument. Put $s = a - b\sqrt{-19}$ and $t = q$. We get

$$
s \cdot \frac{\alpha}{\beta} - t = (a - b\sqrt{-19}) \cdot \frac{a + b\sqrt{-19}}{3} - q = \frac{a^2 + 19b^2 - 3q}{3} = \frac{r}{3},
$$

and $0 < N\left(\frac{r}{3}\right) = \frac{r^2}{9} < 1$ because $r \neq 0$. Hence N satisfies the Dedekind–Hasse norm property.

Case 4: $c = 4$

Let $c = 4$. If $a \equiv b \equiv 0 \pmod 2$, then $\gcd(a,b,c) \geq 2 > 1$, which is impossible.

Subcase 4.1: $a \equiv 0 \pmod 2$ or $b \equiv 0 \pmod 2$ (but not both).

Either way, we have $a^2 + 19b^2 \equiv 1 \pmod 2$. Now perform division with remainder in integers of $a^2 + 19b^2$ by 4 to get $a^2 + 19b^2 = 4q + r$, where $r \in \{1, 3\}$. Note that if $r \in \{0, 2\}$, then we would have $a^2 + 19b^2 \equiv 0 \pmod 2$, a contradiction. Put $s = a - b\sqrt{-19}$ and $t = q$. We get

$$s \cdot \frac{\alpha}{\beta} - t = (a - b\sqrt{-19}) \cdot \frac{a + b\sqrt{-19}}{4} - q = \frac{a^2 + 19b^2 - 4q}{4} = \frac{r}{4},$$

and $0 < N\left(\frac{r}{4}\right) = \frac{r^2}{16} < 1$ because $r \neq 0$.

Subcase 4.2: $a \equiv b \equiv 1 \pmod 2$.

Recall that for $n \in \{1, 3, 5, 7\}$, we have $n^2 \equiv 1 \pmod 8$. Hence $a^2+19b^2 \equiv 1+3\cdot 1 \equiv 4 \pmod 8$. Thus we have $a^2+19b^2 = 8q+4$. Put $s = \frac{a-b}{2}+b\cdot\frac{1+\sqrt{-19}}{2}$ and $t = q$. Note that $\frac{a-b}{2} \in \mathbb{Z}$ because $a \equiv b \equiv 1 \pmod 2$. We get

$$s \cdot \frac{\alpha}{\beta} - t = \left(\frac{a-b}{2} + b \cdot \frac{1+\sqrt{-19}}{2}\right) \cdot \frac{a + b\sqrt{-19}}{4} - q = \frac{a^2 + 19b^2 - 8q}{8} = \frac{4}{8}.$$

Obviously $\frac{4}{8} = \frac{1}{2}$, and $0 < N\left(\frac{1}{2}\right) = \frac{1}{4} < 1$. Hence for $c = 4$, the Dedekind–Hasse norm property holds.

Case 5: $c = 5$

Let $c = 5$. Then $a \not\equiv 0 \pmod 5$ or $b \not\equiv 0 \pmod 5$, because otherwise $\gcd(a,b,c) = 5 > 1$. Perform division with remainder in integers of $a^2 + 19b^2$ by 15 to get $a^2 + 19b^2 = 15q + r$. Note that

$$a^2 + 19b^2 \equiv a^2 + 4b^2 \pmod{15}.$$

We have $a^2 + 4b^2 \equiv 0 \pmod{15}$ if and only if $a \equiv b \equiv 0 \pmod{15}$ or $(ab^{-1})^2 \equiv -4 \equiv 11 \pmod{15}$. We know that the first case is impossible. However, for all $n \in \mathbb{Z}$, we have $n^2 \equiv 0, 1, 4, 6, 9,$ or $10 \pmod{15}$. Thus $r \neq 0$.

Put $s = a - b\sqrt{-19}$ and $t = 3q$. We get

$$s \cdot \frac{\alpha}{\beta} - t = (a - b\sqrt{-19}) \cdot \frac{a + b\sqrt{-19}}{5} - 3q = \frac{a^2 + 19b^2 - 15q}{5} = \frac{r}{5},$$

and so $0 < N\left(\frac{r}{5}\right) = \frac{r^2}{25} < 1$ because $r \neq 0$.

This completes all cases, so the function N is a Dedekind–Hasse norm on $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. By Lemma 1, we conclude that $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a principal ideal domain.

No Universal Side Divisor

Recall that since N is multiplicative, if $x \mid y$, then $N(x) \mid N(y)$ for any $x, y \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Let us find the units in $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Take $v \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]^*$ with $v = a + b \cdot \frac{1+\sqrt{-19}}{2}$. We have

$$N(v) = a^2 + ab + 5b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4}b^2 \geq 5$$

if $b \neq 0$. Since $v \mid 1$ and $N(1) = 1$, we have $N(v) = 1$. Hence $b = 0$, and then $a^2 = 1$, which implies $a = \pm 1$. Thus $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]^* = \{-1, 1\}$.

Also, we have $N(z) < 5 \implies z \in \{\pm 1, \pm 2\}$ for $z \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Suppose $u \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \setminus \{-1, 0, 1\}$ is a universal side divisor. We have $N(u) \neq 1$. Also, there exists $y \in \{-1, 0, 1\}$ such that $u \mid 2 - y$ since $2 \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

Case 1: $y = 1$.

Then $u \mid 1$, so $u \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]^*$, which is impossible.

Case 2: $y = 0$.

Then $u \mid 2$, so $N(u) \mid N(2) = 4$. That means $N(u) = 4$, which yields $u = \pm 2$.

Case 3: $y = -1$.

Then $u \mid 3$, so $N(u) \mid N(3) = 9$. Since $N(u) \neq 3$, we have $N(u) = 9$. Let $u = n + m \cdot \frac{1+\sqrt{-19}}{2}$. Then $N(u) = n^2 + nm + 5m^2 = 9$, so $3 \mid n^2 + nm + 5m^2$. Note that $n^2 + nm + 5m^2 \equiv 0 \pmod 3$ if and only if $n \equiv m \equiv 0 \pmod 3$. Hence we can write $n = 3k$ and $m = 3\ell$ for $k, \ell \in \mathbb{Z}$. The equation becomes $9k^2 + 9k\ell + 45\ell^2 = 9$, and so $k^2 + k\ell + 5\ell^2 = 1$. By previous calculations, we know that $\ell = 0$ and $k = \pm 1$. Thus $u = \pm 3$.

Hence the only possible universal side divisors of $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ are ± 2 and ± 3. If u is a universal side divisor, then so is $-u$. Thus we only need to consider 2 and 3.

Take $\frac{1+\sqrt{-19}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. There must exist a $z \in \{-1, 0, 1\}$ such that $2 \mid \frac{1+\sqrt{-19}}{2} - z$ or $3 \mid \frac{1+\sqrt{-19}}{2} - z$. Thus we need 2 or 3 to divide one of $\frac{1+\sqrt{-19}}{2}$, $\frac{-1+\sqrt{-19}}{2}$, or $\frac{3+\sqrt{-19}}{2}$. However, $N(2) = 4$ and $N(3) = 9$, but

$$N\left(\frac{1+\sqrt{-19}}{2}\right) = 5, \quad N\left(\frac{-1+\sqrt{-19}}{2}\right) = 5, \quad N\left(\frac{3+\sqrt{-19}}{2}\right) = 7.$$

Since divisibility implies divisibility of norms, neither 2 nor 3 divides any of these elements, so they are not universal side divisors of $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Since these were the only possible candidates, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ has no universal side divisors. Hence it is not a Euclidean domain by Lemma 2.