On a principal ideal domain that is not a Euclidean domain

Conan Wong
March 15, 2013

Abstract

The ring $\mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right]$ is usually given as a first example of a principal ideal domain (PID) that is not a Euclidean domain. This paper gives an elementary and more direct proof that $\mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right]$ is indeed a PID.

1 Introduction

In a course on abstract algebra, one proves that all Euclidean domains are principal ideal domains (PIDs). The ring $\mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right]$ is then usually given as a “simple” example of a PID that is not a Euclidean domain. However, details of this example are usually omitted. Some textbooks leave it as a series of exercises for the student. There have been efforts to simplify the proof that $\mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right]$ is indeed a PID but not a Euclidean domain, such as [6], [5] and, most recently, [2]. A comparative survey of the various papers can be found in [3].

For ease of notation, let $\omega = \frac{1+\sqrt{-19}}{2}$ henceforth.

It is straightforward to show that $\mathbb{Z}[\omega]$ is not Euclidean and this paper includes an existing proof for completeness. However, the proof that $\mathbb{Z}[\omega]$ is a PID is slightly more difficult. For example, the proofs in [6] and [3] leverage on a theorem due to Dedekind and Hasse, and the ensuing proof requires a breakdown into 5 cases, each corresponding to different elements of $\mathbb{Z}[\omega]$. The proof in [2] is a simplification, intended to make the material more accessible to mathematics students. However, it still requires a partitioning of $\mathbb{Z}[\omega]$ into 7 cases.

This paper provides an elementary and more direct proof that $\mathbb{Z}[\omega]$ is a PID. It is written with the same motivation as [2], utilising only introductory abstract algebra and the absolute value of a complex number, to improve
access to comprehension. By partitioning $\mathbb{Z}[\omega]$ differently, the proof in this paper requires a breakdown into only 3 cases.

2 $\mathbb{Z}[\omega]$ is not a Euclidean Domain

This proof that $\mathbb{Z}[\omega]$ is not a Euclidean domain is similar to the proof in [2] and, as mentioned earlier, is included here for completeness.

Firstly, note that $\omega^2 = \omega - 5$. Thus, $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$. Also, as the minimal polynomial of $\omega$ over $\mathbb{Z}$ is $x^2 - x + 5$, which is Eisenstein and hence irreducible, $\mathbb{Z}[\omega]$ is an integral domain. For any element $\alpha \in \mathbb{Z}[\omega]$, we have the usual absolute value $|\alpha| = \alpha \overline{\alpha}$, where $\overline{\alpha}$ denotes the usual complex conjugate of $\alpha$. It is easy to see that for any $\alpha \in \mathbb{Z}[\omega]$, $\overline{\alpha} \in \mathbb{Z}[\omega]$ as well. We begin by proving some useful properties relating to the absolute values of elements in $\mathbb{Z}[\omega]$.

Lemma 2.1. For $\alpha \in \mathbb{Z}[\omega] \setminus \{0\}$, $|\alpha| \in \mathbb{N}$.

Proof. As $\alpha = a + b\omega$ for some $a, b \in \mathbb{Z}$,

$$|\alpha| = |a + b\left(\frac{1 + \sqrt{-19}}{2}\right)||a + b\left(\frac{1 - \sqrt{-19}}{2}\right)| = a^2 + ab + 5b^2 \in \mathbb{Z}_{\geq 0}.$$ 

Since $\alpha \neq 0$, $|\alpha| \neq 0$. Thus, $|\alpha| \in \mathbb{N}$.

Lemma 2.2. For $\alpha \in \mathbb{Z}[\omega]$, the following statements are equivalent:

(i) $\alpha = -1$ or $1$.

(ii) $\alpha$ is a unit in $\mathbb{Z}[\omega]$.

(iii) $|\alpha| = 1$.

Proof. (i) $\Rightarrow$ (ii) is clear.

For (ii) $\Rightarrow$ (iii), if $\alpha$ is a unit in $\mathbb{Z}[\omega]$, then $\exists \beta \in \mathbb{Z}[\omega]$ such that $\alpha\beta = 1$. Then $1 = |\alpha\beta| = |\alpha||\beta|$. By Lemma 2.1, we must have $|\alpha| = |\beta| = 1$.

For (iii) $\Rightarrow$ (i), we write $\alpha = a + b\omega$ for some $a, b \in \mathbb{Z}$. Then $1 = |\alpha| = a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{9}{4}b^2$. As $a, b \in \mathbb{Z}$, we must have $b = 0$, which in turn implies that $a^2 = 1$. □

Our proof that $\mathbb{Z}[\omega]$ is not Euclidean features some “special elements” of $\mathbb{Z}[\omega]$, namely $\pm 1, \pm 2$ and $\pm 3$. Lemma 2.2 showed that $\pm 1$ are the only units in $\mathbb{Z}[\omega]$. The following lemma shows that $\pm 2$ and $\pm 3$ are irreducible in $\mathbb{Z}[\omega]$. Recall that an element of a ring is irreducible if it satisfies the following properties:

(i) It is a nonzero non-unit in the ring; and
(ii) If it is written as a product of 2 elements of the ring, exactly 1 of them is a unit.

**Lemma 2.3.** $± 2$ and $± 3$ are irreducible in $\mathbb{Z}[\omega]$.

**Proof.** As $± 1$ are units, it suffices to prove that 2 and 3 are irreducible.

2 is clearly a nonzero non-unit in $\mathbb{Z}[\omega]$, since $\frac{1}{2} \not\in \mathbb{Z}[\omega]$. Suppose we write $2 = \alpha \beta$ for some $\alpha, \beta \in \mathbb{Z}[\omega]$. Then $4 = |2| = |\alpha| |\beta|$. By Lemma 2.1, this implies that $(|\alpha|, |\beta|) = (1, 4), (2, 2)$ or $(4, 1)$. By Lemma 2.2, the first and the last cases would imply that either $\alpha$ or $\beta$ is a unit respectively and, hence, 2 is irreducible.

For the case $(|\alpha|, |\beta|) = (2, 2)$, writing $\alpha = a + b\omega$ for some $a, b \in \mathbb{Z}$, we would get $2 = |\alpha| = a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2$. But then $a, b \in \mathbb{Z}$ means that $b = 0$, which in turn implies that $a^2 = 2$, a contradiction.

The proof that 3 is irreducible is similar.

**Theorem 2.4.** $\mathbb{Z}[\omega]$ is not a Euclidean domain.

**Proof.** Assume the contrary, i.e. that $\mathbb{Z}[\omega]$ is a Euclidean domain. Then there exists a Euclidean degree function $D : \mathbb{Z}[\omega] \setminus \{0\} \to \mathbb{N}$ satisfying the Euclidean Division Algorithm:

For $\alpha, \beta \in \mathbb{Z}[\omega]$ where $\beta \neq 0$, there exist $q, r \in \mathbb{Z}[\omega]$ such that $\alpha = \beta q + r$ and either $r = 0$ or $D(r) < D(\beta)$.

As the range of $D$ is $\mathbb{N}$, we can choose $m \in \mathbb{Z}[\omega]$ such that $D(m)$ is as small as possible subject to $m$ not being zero or a unit. Then let $q, r \in \mathbb{Z}[\omega]$ be the quotient and remainder, respectively, when we divide 2 by $m$ in $\mathbb{Z}[\omega]$, i.e.

$$2 = mq + r,$$

where $r = 0$ or $D(r) < D(m)$.

$D(m)$ is already as small as possible subject to $m$ being a nonzero non-unit. So either $r = 0$, or else $D(r) < D(m)$ implies that $r$ is a unit in $\mathbb{Z}[\omega]$, i.e.

$$r = -1 \text{ or } 1 \text{ (by Lemma 2.2).}$$

If $r = 0$, then $m$ divides 2. Since $m$ is not a unit and 2 is irreducible in $\mathbb{Z}[\omega]$ (by Lemma 2.3), this means that $m = -2$ or 2. (Again, we have used the fact that the only units in $\mathbb{Z}[\omega]$ are -1 and 1.)

If $r = -1$, then $m$ divides 3. By a similar line of reasoning as in the case above, $m = -3$ or 3.

If $r = 1$, then $m$ divides 1, which is a contradiction since $m$ is not a unit by assumption.
Thus, we have shown that the possible choices for \( m \) (i.e. the nonzero non-unit elements of \( \mathbb{Z}[\omega] \) with minimal degree \( D \)) are \( \pm 2 \) and \( \pm 3 \).

Next, we divide \( \omega \) by \( m \) in \( \mathbb{Z}[\omega] \), getting
\[
\omega = mq' + r',
\]
for some \( q', r' \in \mathbb{Z}[\omega] \) where \( r' = 0 \) or \( D(r') < D(m) \).

By the same argument as above, this implies that \( r' = -1, 0 \) or \( 1 \).

If \( r' = -1 \), then \( m \) divides \( 1 + \omega \) in \( \mathbb{Z}[\omega] \). But as \( m \in \{ \pm 2, \pm 3 \} \), \( \frac{1}{m}(1 + \omega) \notin \mathbb{Z}[\omega] \), a contradiction.

If \( r' = 0 \), then \( m \) divides \( \omega \) in \( \mathbb{Z}[\omega] \). But as \( m \in \{ \pm 2, \pm 3 \} \), \( \frac{1}{m}\omega \notin \mathbb{Z}[\omega] \), a contradiction.

If \( r' = 1 \), then \( m \) divides \( -1 + \omega \) in \( \mathbb{Z}[\omega] \). But as \( m \in \{ \pm 2, \pm 3 \} \), \( \frac{1}{m}(-1 + \omega) \notin \mathbb{Z}[\omega] \), a contradiction. \( \square \)

3 \( \mathbb{Z}[\omega] \) is a Principal Ideal Domain

This proof is based on a combination of ideas from [1] and [7]. Importantly, it hinges on the absolute values of elements in \( \mathbb{Z}[\omega] \) and, thus, uses Lemma 2.1 from the previous section.

**Theorem 3.1.** \( \mathbb{Z}[\omega] \) is a principal ideal domain.

**Proof.** Let \( I \) be any nonzero ideal in \( \mathbb{Z}[\omega] \). As Lemma 2.1 showed that the absolute values of nonzero elements in \( \mathbb{Z}[\omega] \) are natural numbers, we can pick a nonzero \( \beta \in I \) such that \( |\beta| \) is as small as possible among the nonzero elements of \( I \). We seek to show that \( I = (\beta) \), i.e. \( I \) is a principal ideal generated by \( \beta \).

Assume the contrary. Then there exists a nonzero \( \alpha \in I \setminus (\beta) \). Consider \( \frac{\alpha}{\beta} \in \mathbb{C} \). As \( \omega = \frac{1}{2} + \frac{\sqrt{19}}{2}i \in \mathbb{C} \), we can pick \( m \in \mathbb{Z} \) such that
\[
-\frac{\sqrt{19}}{2} < Im(\frac{\alpha}{\beta} + m\omega) \leq \frac{\sqrt{19}}{2}
\]
where \( Im \) refers to the imaginary part of a complex number. We now split up the argument into 2 cases, depending on the value of \( Im(\frac{\alpha}{\beta} + m\omega) \).

**Case 1.** \( -\frac{\sqrt{3}}{2} < Im(\frac{\alpha}{\beta} + m\omega) < \frac{\sqrt{3}}{2} \)

In this more straightforward case, we can pick \( n \in \mathbb{Z} \) such that
\[
-\frac{1}{2} < Re(\frac{\alpha}{\beta} + m\omega + n) \leq \frac{1}{2}
\]

4
where $Re$ refers to the real part of a complex number. Since $Im(\frac{a}{\beta} + m\omega + n) = Im(\frac{a}{\beta} + m\omega)$, we also have

$$-\frac{\sqrt{3}}{2} < Im(\frac{a}{\beta} + m\omega + n) < \frac{\sqrt{3}}{2}.$$ 

Thus, $|\frac{a}{\beta} + m\omega + n| < (\frac{1}{2})^2 + (\frac{\sqrt{3}}{2})^2 = 1$, and $|\alpha + (m\omega + n)\beta| = |\frac{a}{\beta} + m\omega + n||\beta| < |\beta|$. But as $\alpha, \beta \in I$ and $m, \omega \in \mathbb{Z}[\omega]$, it follows that $\alpha + (m\omega + n)\beta \in I$. Since $|\beta|$ is as small as possible among the absolute values of nonzero elements in $I$, $|\alpha + (m\omega + n)\beta| < |\beta|$ implies that $\alpha + (m\omega + n)\beta = 0$. Thus, $\alpha \in (\beta)$, which contradicts our assumption.

**Case 2.** Either $-\frac{\sqrt{19}}{4} < Im(\frac{a}{\beta} + m\omega) \leq -\frac{\sqrt{3}}{2}$, or $\frac{\sqrt{3}}{2} \leq Im(\frac{a}{\beta} + m\omega) \leq \frac{\sqrt{19}}{4}$

If $-\frac{\sqrt{19}}{4} < Im(\frac{a}{\beta} + m\omega) \leq -\frac{\sqrt{3}}{2}$, then let $\alpha' = -\alpha - m\omega\beta$.

If $\frac{\sqrt{3}}{2} \leq Im(\frac{a}{\beta} + m\omega) \leq \frac{\sqrt{19}}{4}$, then let $\alpha' = \alpha + m\omega\beta$.

In both instances, since $\alpha, \beta \in I$ and $m, \omega \in \mathbb{Z}[\omega]$, we see that $\alpha' \in I$. But if $\alpha' \in (\beta)$, then $\alpha = \pm(\alpha' - m\omega\beta) \in (\beta)$ as well, which contradicts our assumption that $\alpha \notin (\beta)$. Thus, in both instances, we have found an element $\alpha' \in I \setminus (\beta)$ such that

$$\frac{\sqrt{3}}{2} \leq Im(\frac{\alpha'}{\beta}) \leq \frac{\sqrt{19}}{4}.$$ 

Now, as in **Case 1**, we can find $n \in \mathbb{Z}$ such that

$$-\frac{1}{2} < Re(\frac{\alpha'}{\beta} + n) \leq \frac{1}{2}.$$ 

Let $\alpha'' = \alpha' + n\beta \in I$. Note that $Im(\frac{\alpha''}{\beta}) = Im(\frac{\alpha'}{\beta})$. As before, if $\alpha'' \in (\beta)$, then $\alpha' = \alpha'' - n\beta \in (\beta)$ as well, which is a contradiction. Thus, we have found an element $\alpha'' \in I \setminus (\beta)$ such that

$$\frac{\sqrt{3}}{2} \leq Im(\frac{\alpha''}{\beta}) \leq \frac{\sqrt{19}}{4}, \text{ and } -\frac{1}{2} < Re(\frac{\alpha''}{\beta}) \leq \frac{1}{2}.$$ 

To finish the proof, we consider the element $\frac{2\alpha''}{\beta} - \omega \in \mathbb{C}$, which will give us the desired contradictions via 2 subcases. Since $\omega = \frac{1}{2} + \frac{\sqrt{19}}{2}i$, we get that

$$-\frac{3}{2} < Re(\frac{2\alpha''}{\beta} - \omega) \leq \frac{1}{2}.$$ 

5
Noting that \( \sqrt{19} < \sqrt{27} = 3\sqrt{3} \), we get \( \sqrt{3} - \frac{\sqrt{19}}{2} > \sqrt{3} - \frac{3\sqrt{3}}{2} = -\frac{\sqrt{3}}{2} \). Thus,

\[ -\frac{\sqrt{3}}{2} < \sqrt{3} - \frac{\sqrt{19}}{2} \leq \text{Im}(\frac{2\alpha''}{\beta} - \omega) \leq 0. \]

**Case 2(a).** \(-\frac{1}{2} < \text{Re}(\frac{2\alpha''}{\beta} - \omega) \leq \frac{1}{2}\)

In this sub-case, since \( |\frac{2\alpha''}{\beta} - \omega| < (\frac{1}{2})^2 + (-\frac{\sqrt{3}}{2})^2 = 1 \), we see that \( |2\alpha'' - \omega\beta| = |\frac{2\alpha''}{\beta} - \omega||\beta| < |\beta| \). Since \( \alpha'', \beta \in I \), it follows that \( 2\alpha'' - \omega\beta \in I \) as well. But as \( |\beta| \) is as small as possible among the absolute values of nonzero elements in \( I \), \( |2\alpha'' - \omega\beta| < |\beta| \) implies that \( 2\alpha'' - \omega\beta = 0 \). This means that \( \frac{\omega\beta}{2} = \alpha'' \in I \).

Now as \( \bar{\omega} \in \mathbb{Z}[\omega] \) and \( \bar{\omega}\omega = 5 \), we have \( \frac{5}{2}\beta = \bar{\omega}(\frac{\omega\beta}{2}) \in I \). And since \( \beta \in I \), we see that \( \frac{1}{2}\beta = \frac{5}{2}\beta - 2\beta \in I \) as well. But then \( 0 < |\frac{1}{2}\beta| = \frac{1}{4}|\beta| < |\beta| \) contradicts the minimality of \( |\beta| \) among the absolute values of nonzero elements in \( I \), which completes the proof of this sub-case.

**Case 2(b).** \(-\frac{3}{2} < \text{Re}(\frac{2\alpha''}{\beta} - \omega) \leq -\frac{1}{2}\)

In this sub-case, we “shift by 1” to get a proof similar to Case 2(a), i.e. we consider \( \frac{2\alpha''}{\beta} - \omega + 1 \in \mathbb{C} \). Clearly,

\[ -\frac{1}{2} < \text{Re}(\frac{2\alpha''}{\beta} - \omega + 1) \leq \frac{1}{2}, \text{ and } -\frac{\sqrt{3}}{2} < \text{Im}(\frac{2\alpha''}{\beta} - \omega + 1) \leq 0 \]

since \( \text{Im}(\frac{2\alpha''}{\beta} - \omega + 1) = \text{Im}(\frac{2\alpha''}{\beta} - \omega) \).

Thus, \( |\frac{2\alpha''}{\beta} - \omega + 1| < (\frac{1}{2})^2 + (-\frac{\sqrt{3}}{2})^2 = 1 \), and we see that \( |2\alpha'' - \omega\beta + \beta| = |\frac{2\alpha''}{\beta} - \omega + 1||\beta| < |\beta| \). Since \( \alpha'', \beta \in I \), it follows that \( 2\alpha'' - \omega\beta + \beta \in I \) as well. But as \( |\beta| \) is as small as possible among the absolute values of nonzero elements in \( I \), \( |2\alpha'' - \omega\beta + \beta| < |\beta| \) implies that \( 2\alpha'' - \omega\beta + \beta = 0 \). This means that \( \frac{\omega - 1}{2}\beta = \alpha'' \in I \).

Now as \( \frac{1}{2} \in \mathbb{Z}[\omega] \) and \( (\omega - 1)(\omega - 1) = 5 \), we have \( \frac{5}{2}\beta = (\omega - 1)(\frac{\omega - 1}{2}\beta) \in I \). By an argument identical to that in Case 2(a), \( \frac{1}{2}\beta \in I \) as well, contradicting the minimality of \( |\beta| \) among the absolute values of nonzero elements in \( I \) and completing the proof. \( \square \)
4 Concluding Remarks

The ring \( \mathbb{Z}[\omega] \) is an example of a quadratic integer ring. In general, for a square-free integer \( D \), let

\[
\theta = \begin{cases} 
\sqrt{D} & \text{if } D \equiv 2, 3 \pmod{4} \\
\frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod{4}
\end{cases}
\]

Then, \( \mathbb{Z}[\theta] \) is a quadratic integer ring (the ring of integers in the quadratic number field, \( \mathbb{Q}(\sqrt{D}) \)).

It is known that \( \mathbb{Z}[\theta] \) is a PID but not a Euclidean domain exactly when \( D = -19, -43, -67 \) or \(-163 \) (see [3], [4] and [5]). This paper dealt with the case \( D = -19 \). Perhaps a possible next step would be to find a unifying proof (for all 4 cases) that is equally accessible to students in mathematics.

References

[1] Bergman, G.M. A principal ideal domain that is not Euclidean. [George M. Bergman’s website, accessed on 21 January 2013] Available at: math.berkeley.edu/~gbergman/grad.hndts/nonEucPID.ps


[7] Wilson, R.A. An example of a PID which is not a Euclidean domain. [Robert A. Wilson’s website, accessed on 21 January 2013] Available at: www.maths.qmul.ac.uk/~raw/MTH5100/PIDnotED.pdf