PIDs that are not EDs

Swayam Chube

December 8, 2024

Abstract

It is known that every Euclidean Domain (ED) is a Principal Ideal Domain (PID). We present two exammples of PIDs that are not EDs, namely, $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ and $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

§1 $\mathbb{R}[X,Y]/(X^2+Y^2+1)$

We first begin with two important lemmas.

LEMMA 1.1. Let A be a commutative ring in which every prime ideal is principal. Then, A is a principal ring.

Proof. Suppose not and let Σ denote the poset of all proper ideals that are not principal. Let $\mathscr{C}$ denote a chain in Σ and let $\mathfrak{a} = \bigcup \mathscr{C}$. If $\mathfrak{a} = (a)$ is principal, then there is an ideal $\mathfrak{b} \in \mathscr{C}$ that contains a, consequently, $\mathfrak{b} = (a)$, a contradiction. Thus, $\mathfrak{a} \in \Sigma$ and is an upper bound for $\mathscr{C}$. Due to Zorn's Lemma, Σ contains a maximal element, say $\mathfrak{p}$.

We contend that $\mathfrak{p}$ is prime. Suppose not. Then, there are $a, b \notin \mathfrak{p}$ with $ab \in \mathfrak{p}$. Note that $(\mathfrak{p} : b)$ is an ideal properly containing $\mathfrak{p}$ (since it also contains a) and hence, must be principal, say (c). Next, $\mathfrak{p} + (b)$ properly contains $\mathfrak{p}$ and hence, must be principal, say (d). Clearly, $\mathfrak{p} \supseteq (\mathfrak{p} : b)(\mathfrak{p} + (b)) = (cd)$. On the other hand, if $x \in \mathfrak{p}$, then $x = \alpha d$ for some $\alpha \in A$. Since $\alpha d \in \mathfrak{p}$, we have $\alpha \in (\mathfrak{p} : b) = (c)$. Thus, $\mathfrak{p} \subseteq (\mathfrak{p} : b)(\mathfrak{p} + (b))$ and $\mathfrak{p} = (cd)$ is principal, a contradiction. Hence, $\mathfrak{p}$ is prime, and must be principal, again, a contradiction. This completes the proof. ■

LEMMA 1.2. Let A be a Euclidean Domain with Euclidean function $\delta : A \backslash \{0\} \to \mathbb{N}_0$. Then, there is a non-zero prime $p \in A$ such that $\pi : A \twoheadrightarrow A/p$ restricts to a surjective group homomorphism $\pi : A^\times \to (A/p)^\times$.

Proof. Let $p \in A$ be a non-zero element in $A \backslash A^\times$ that minimizes δ. Then, p must be irreducible, for if $p = ab$ with a non-unit, then

$$\delta(p) = \delta(ab) \geqslant \delta(a) \geqslant \delta(p),$$

consequently, $\delta(a) = \delta(ab)$ whence b must be a unit. This shows that p is prime.

Now, let $\overline{a} \in A/p$ be invertible. Then, there is a non-zero $a \in A$ with $\pi(a) = \overline{a}$. Thus, there are q and r with $a = pq + r$. Since $r \neq 0$, we must have $\delta(r) < \delta(p)$, whereby, $r \in A^\times$. Note that $\pi(r) = \pi(a) = \overline{a}$ and hence, the restriction of π to $A^\times \to (A/p)^\times$ is surjective. ■

We are now ready to prove the main of this section. Let $A = R[X,Y]/(X^2+Y^2+1)$ and let x and y denote the images of X and Y in A.

PROPOSITION 1.3. Every non-zero prime ideal in A is of the form $(ax+by+c)$ where $(a,b) \neq 0$.

Proof. Let $\mathfrak{p}$ be a non-zero prime ideal of A. Note first that

$$\dim A = \dim R[X,Y] - \operatorname{ht}((X^2+Y^2+1)) = 1,$$

whence $\mathfrak{p}$ is maximal. Further, $A/\mathfrak{p}$ is a finitely generated $\mathbb{R}$-algebra and also a field, and due to Zariski's Lemma, must be a finite extension of $\mathbb{R}$. Thus, $[A/\mathfrak{p} : \mathbb{R}] \leqslant 2$. Let $\overline{x}, \overline{y}$ denote the images of x and y in $A/\mathfrak{p}$. Since $1, \overline{x}, \overline{y}$ cannot be linearly independent over $\mathbb{R}$, we must have a non-trivial linear combination $a\overline{x} + b\overline{y} + c = 0$ in $A/\mathfrak{p}$. Hence, $ax+by+c \in \mathfrak{p}$. If $(a,b) = 0$, then $\mathfrak{p}$ would contain a unit which is impossible.

Note that $(aX+bY+c)$ was a maximal ideal in $R[X,Y]$. Hence, $(ax+by+c)$ is a maximal ideal in A. Further, the quotient $A/(ax+by+c)$ strictly contains $\mathbb{R}$ and due to Zariski's Lemma, must be a finite extension of it, whence is isomorphic to $\mathbb{C}$. This shows that $\mathfrak{p} = (ax+by+c)$ and $A/\mathfrak{p} \cong \mathbb{C}$ thereby completing the proof. ■

PROPOSITION 1.4. A is a PID but not an ED.

Proof. Due to Proposition 1.3 and Lemma 1.1, A is a PID. Suppose A were an ED. According to Lemma 1.2, there is a non-zero prime $p \in A$ and a group surjection $\pi : A^\times \to (A/p)^\times$. Note that $A^\times \cong \mathbb{R}^\times$ and $(A/p)^\times \cong \mathbb{C}^\times$. But there is no surjective group homomorphism $\mathbb{R}^\times \twoheadrightarrow \mathbb{C}^\times$, a contradiction. ■

§2 $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

Let $K = \mathbb{Q}[\sqrt{-19}]$ be a number field and let $\mathcal{O}_K$ denote the ring of integers in K. It is well known that $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ and that it has class number 1. Hence, every fractional ideal over $\mathcal{O}_K$ is principal. In particular, every integral ideal of $\mathcal{O}_K$ is principal and $\mathcal{O}_K$ is a PID.

We shall now argue that $\mathcal{O}_K$ is not an ED. Suppose $\delta : \mathcal{O}_K \backslash \{0\} \to \mathbb{N}_0$ is a Euclidean function and let $p \in \mathcal{O}_K$ be a non-zero, non-invertible element that minimizes δ. Consider the canonical projection $\pi : \mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/(p)$.

If $0 \neq \overline{a} \in \mathcal{O}_K/(p)$, then there is an $a \in \mathcal{O}_K$ that maps to it under π. We may write $a = pq + r$ where $q \in \mathcal{O}_K$, $0 \neq r$ and $\delta(r) < \delta(p)$. Due to the minimality of $\delta(p)$, we must have that r is a unit. Note that the only units in $\mathcal{O}_K$ are ± 1. Indeed, if $x \in \mathcal{O}_K$ is a unit, then there are integers m and n such that

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

Since x is a unit, we have $N_{K/\mathbb{Q}}(x) = \pm 1$, that is,

$$(2m+n)^2 + 19n^2 = 4.$$

It is not hard to see, from the above equation, that the only solutions are $x = \pm 1$.

Hence, $r \in \{\pm 1\}$, in particular, $\mathcal{O}_K/(p)$ can have atmost 3 elements and at least 2 elements. Thus, the *ideal norm* of (p) is either 2 or 3. Hence, $N_{K/\mathbb{Q}}(p) \in \{2, 3\}$.

We may suppose $p = m + n\frac{1+\sqrt{-19}}{2}$. The equation involving norm gives us

$$(2m+n)^2 + 19n^2 \in \{8, 12\}.$$

Due to size reasons, $n = 0$. And we are left with $m^2 \in \{2, 3\}$, which is impossible. Thus, $\mathcal{O}_K$ cannot be an ED. This completes the proof.