신 용 수 교수지도

석 사 학 위 논 문

A Principal Ideal Domain That Is Not A Euclidean Domain

2008

성신여자대학교 교육대학원

교육학과 수학교육전공

방 지 원

A Principal Ideal Domain That Is Not A Euclidean Domain

신 용 수 교수지도

이 논문을 석사학위논문으로 제출함.

2008월 5월

성신여자대학교 교육대학원
교육학과 수학교육전공
방 지 원

인 준 서

방지원의 석사학위 논문으로 인준함.

심사위원 ________________ 인

심사위원 ________________ 인

심사위원 ________________ 인

성신여자대학교 교육대학원

목 차

1. Introduction 1

2. Preliminary Definitions and Theorem 1

3. Some Example of a Principal Ideal Domain
which is not a Euclidean Domain 12

REFERENCES 21

ABSTRACT(국문초록)

1. **Introduction**

Let D be an integral domain. If D is a Euclidean domain(ED for short see Definition 2.6) then it is a principal ideal domain(PID for short see Definition 2.5). However, the converse is not true in general. Thus in this thesis, we give an example of a principal ideal domain, which is not a Euclidean domain.

More precisely, the domain D is a subset of the complex numbers with the usual operations of addition and multiplication:

$$D = \left\{ a + \frac{b(1+\sqrt{-13})}{2} \;\middle|\; a \text{ and } b \text{ are integers} \right\}.$$

It is easy to show that D is an integral domain with a unit. The goal of this thesis is to show that D is a principal ideal domain(see Theorem 3.1), but it is impossible to define a Euclidean norm on D which makes D a Euclidean domain(see Theorem 3.2).

2. **Preliminary Definitions and Theorem**

Definition 2.1 (Definition 19.2, [1])**.** If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are ***divisors of*** 0 (or ***zero divisors***).

Definition 2.2 (Definition 19.6, [1])**.** An ***integral domain*** D is a commutative ring with unity $1 \neq 0$ and containing no divisors of 0.

Definition 2.3 (Definition 45.4, [1])**.** A nonzero element p that is not a unit of an integral domain D is an ***irreducible*** of D if every factorization $p = ab$ in D has the property that either a or b is a unit.

Definition 2.4 (Definition 27.21, [1])**.** If R is a commutative ring with unity and $a \in R$, the ideal $\{ra \mid r \in R\}$ of all multiples of a is the ***principal ideal generated by*** a and is denoted by $\langle a \rangle$.

An ideal N of R is a ***principal ideal*** if $N = \langle a \rangle$ for some $a \in R$.

Definition 2.5 (Definition 45.7, [1])**.** A integral domain D is a ***principal ideal domain*** (abbreviated **PID**) if every ideal in D is a principal ideal.

Definition 2.6 (Definition 46.1, [1])**.** A ***Euclidean norm*** on an integral domain D is a function ν mapping the nonzero elements of D into nonnegative integers such that the following conditions are satisfied:

1. For all $a, b \in D$ with $b \neq 0$, there exist q and r in D such that $a = bq + r$, where either $r = 0$ or $\nu(r) < \nu(b)$.
2. For all $a, b \in D$ with $b \neq 0$, where neither a nor b is 0, $\nu(a) \leq \nu(ab)$.

An integral domain D is a ***Euclidean domain*** (abbreviated **ED**) if there exists a Euclidean norm on D.

Definition 2.7 (Definition 47.6, [1])**.** Let D be an integral domain. A ***multiplicative norm*** N on D is a function mapping D into the integers $\mathbb{Z}$ such that the following conditions are satisfied:

1. $N(\alpha) = 0$ if and only if $\alpha = 0$.
2. $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha\beta \in D$.

Theorem 2.8. *If D is an integral domain with a multiplicative norm N, then $N(1) = 1$ and $|N(u)| = 1$ for every unit u in D. If, furthermore, every α such that $|N(\alpha)| = 1$ is a unit in D, then an element π in D, with $|N(\pi)| = p$ for a prime $p \in \mathbb{Z}$, is an irreducible of D.*

Proof. Let D be an integral domain with a multiplicative norm N. Then

$$N(1) = N(1 \cdot 1) = N(1)N(1)$$

shows that $N(1) = 1$. Also, if u is a unit in D, then

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}).$$

Since $N(u)$ is an integer, $|N(u)| = 1$.

Let $\pi \in D$ such that $|N(\pi)| = p$, where p is a prime in $\mathbb{Z}$.
If $\pi = \alpha\beta$ where α, $\beta \in D$, then we have

$$p = |N(\pi)| = |N(\alpha\beta)| = |N(\alpha)N(\beta)| = |N(\alpha)||N(\beta)|,$$

so either $|N(\alpha)| = 1$ or $|N(\beta)| = 1$.
By assumption, either α or β is a unit of D. Thus π is an irreducible of D, as expected. ∎

Lemma 2.9. *Let* $D = \mathbb{Z}\left[\frac{1+\sqrt{-13}}{2}\right]$ *be an integral domain and* U *be the set of all units of* D*. Then* $U = \{\pm 1\}$*.*

Proof. Let $\alpha = a + \frac{b(1+\sqrt{-13})}{2}$ in U where a, b are integers. Then

$$\begin{aligned} N(\alpha) &= N\left(a + \frac{b(1+\sqrt{-13})}{2}\right) \\ &= N\left(\left(a+\frac{b}{2}\right) + \frac{b\sqrt{-13}}{2}\right) \\ &= \left(a+\frac{b}{2}\right)^2 + \frac{13b^2}{4} \\ &= 1. \end{aligned}$$

If $b \neq 0$, then $N(\alpha) \geq \frac{13b^2}{4} > 1$, and so $b = 0$. Hence $a^2 = 1$, i.e., $a = \pm 1$, and thus $U = \{\pm 1\}$, as we desired. □

Lemma 2.10. *Let* D *and* U *be as above. Then* 2 *and* 3 *are irreducibles of* D*.*

Proof. Let $2 = \alpha \cdot \beta$, where α, $\beta \in D$. Then

$$4 = N(2) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

so $N(\alpha) = 1$, 2, or 4.

If $N(\alpha) = 1$, then α is a unit in D, and if $N(\alpha) = 4$ such that $N(\beta) = 1$, so β is a unit in D.

Suppose that $N(\alpha) = 2$. If $\alpha = a + \dfrac{b(1+\sqrt{-13})}{2}$ in D where a, b are integers, then

$$\begin{aligned} N(\alpha) &= N\left(a + \frac{b(1+\sqrt{-13})}{2}\right) \\ &= N\left(\left(a + \frac{b}{2}\right) + \frac{b\sqrt{-13}}{2}\right) \\ &= \left(a + \frac{b}{2}\right)^2 + \left(\frac{\sqrt{13}b}{2}\right)^2 \\ &= \left(a + \frac{b}{2}\right)^2 + \frac{13b^2}{4} \\ &= 2. \end{aligned}$$

If $b \neq 0$, then $N(\alpha) \geq \dfrac{13b^2}{4} > 2$, which implies that $b = 0$. Thus, $N(\alpha) = a^2 = 2$, which is impossible because a is integer. Therefore 2 is an irreducible of D.

Now we shall show that 3 is an irreducible of D.

If $\alpha \cdot \beta = 3$, where α, $\beta \in D$, then

$$9 = N(3) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta),$$

so $N(\alpha) = 1$, 3, or 9.

If $N(\alpha) = 1$, then α is a unit in D, and if $N(\alpha) = 9$, then $N(\beta) = 1$, so β is a unit in D.

Suppose that $N(\alpha) = 3$. If $\alpha = a + \dfrac{b(1+\sqrt{-13})}{2}$ in D, where a, b are integers, then

$$\begin{aligned} N(\alpha) &= N\left(a + \frac{b(1+\sqrt{-13})}{2}\right) \\ &= N\left(\left(a + \frac{b}{2}\right) + \frac{b\sqrt{-13}}{2}\right) \\ &= \left(a + \frac{b}{2}\right)^2 + \left(\frac{\sqrt{13}b}{2}\right)^2 \\ &= \left(a + \frac{b}{2}\right)^2 + \frac{13b^2}{4} \\ &= 3. \end{aligned}$$

If $b \neq 0$, then $N(\alpha) \geq \dfrac{13b^2}{4} > 3$, which implies that $b = 0$. Thus, $N(\alpha) = a^2 = 3$, which is impossible because a is integer. Therefore 3 is an irreducible of D, which completes the proof. □

Definition 2.11 (Definition [3]). Let D be an integral domain and let $D^* := D - \{0\}$. A non-empty subset P of D^* is called a ***product ideal*** of D if $xy \in P$ for all $x \in P$ and $y \in D^*$.

Notice that D^* is a product ideal.

Definition 2.12 (Definition [3]). Let S be a nonempty subset of an integral domain D. The ***derived set*** of S, denoted by S_0, is defined by

$$S_0 := \{x \in S \mid y + xD \subset S, \text{ for some } y \text{ in } D\}.$$

Definition 2.13 (Definition 45.1, [1])**.** Let R be a commutative ring with unity and let $a, b \in R$. If there exists $c \in R$ such that $b = ac$, then a ***divides*** b (or a is a ***divisor*** of b), denoted by $a \mid b$.

Definition 2.14 (Definition [3])**.** Let D be an integral domain.
An element x of $(D^*)_0 := D_0^*$ is said to be a ***side divisor*** of y in D provided there is a z in D that is not in D_0^* such that $x \mid (y + z)$.

Definition 2.15 (Definition [3])**.** Let D be an integral domain. An element x of D^* is a ***universal side divisor*** if it is a side divisor of every element of D.

Theorem 2.16. *Let D be an integral domain with a multiplicative norm N. If for all pairs of non-zero elements x and y in I with $N(y) \leq N(x)$, either $y \mid x$ or there exist z and w in D with $0 < N(xz - yw) < N(y)$, then I is a principal ideal of D.*

Proof. Let $I \neq \{0\}$ be an ideal in D. Let y be an element of I with minimal nonzero norm, and let x be any other element of I, i.e., $N(y) \leq N(x)$. In particular, for all z, $w \in D$, we have $xz - yw = 0$ or $xz - yw \neq 0$.

Note that $N(y) \leq N(x)$ and $xz - yw \in I$ for any z, $w \in D$. However, if $y \nmid x$, then there exists z and w in D with $0 < N(xz - yw) < N(y)$ means that $xz - yw \neq 0$. Hence we have $0 \neq xz - yw \in I$ and $N(y) \leq N(xz - yw)$, then

$$0 < N(xz - yw) \lneq N(y) \leq N(xz - yw),$$

which is a contradiction. Thus $y \mid x$.

Therefore, $I = \langle y \rangle$, i.e., I is a principal ideal of D, as we wished. □

Lemma 2.17. *Let D be as above. If S is a product ideal in D, then S_0 is a product ideal in D.*

Proof. If x is in S_0, then x is in S and there exists y in D such that $y + xD \subset S$. Let z be in D^*. Since S is a product ideal and x is in S, xz is in S. Further, $y + (xz)D \subset y + xD \subset S$.

This shows that $S_0 D^* \subset S_0$; i.e., S_0 is a product ideal. □

Lemma 2.18. *Let D be as above. If $S \subset T \subseteq D$, then $S_0 \subset T_0$.*

Proof. If x is in S_0, then x is in S and hence in T, and there exists a y in D such that $y + xD \subset S \subset T$. Therefore, x is in T_0, and $S_0 \subset T_0$. □

Theorem 2.19. *If D is a Euclidean domain, then there exists a sequence, $\{P_n\}$, of product ideals with the following properties:*

(i) $D^* = P_0 \supset P_1 \supset P_2 \supset \cdots \supset P_n \supset \cdots$,

(ii) $\bigcap P_n = \varnothing$,

(iii) $(P_n)_0 \subset P_{n+1}$, *for each n, and*

(iv) *Let $(D^*)_{(0)} := D^*_0$ and $(D^*)_{(n)} := D^*_n = (D^*_{n-1})_0$ for every positive n, the n-th derived set D^*_n of D^*. Then $D^*_n \subset P_n$*

Proof. Let ν be a Euclidean variation on D. For each nonnegative integer n, define $P_n = \{x \in D^* \mid \nu(x) \geq n\}$. This defines the sequence which obviously has properties (i) and (ii). Suppose that x is in P_n and y is in D^*, $\nu(xy) \geq \nu(x) \geq n$ which implies that xy is in P_n.

This shows that $P_n D^* \subset P_n$; i.e., for each n, P_n is a product ideal.

For property (iii), let x be in $(P_n)_0$; i.e., x is in P_n and there exists a y in D such that $y + xD \subset P_n$. Applying the Euclidean algorithm, there exist elements q and r in D with $y = xq + r$ and $r = 0$ or $\nu(x) > \nu(r)$. Hence, $r = y + x(-q)$ is in $y + xD \subset P_n$, which implies that $\nu(r) \geq n$ and in turn, $\nu(x) > \nu(r) \geq n$, so that $\nu(x) \geq n + 1$ and x is in P_{n+1}.

This proves property (iii), $(P_n)_0 \subset P_{n+1}$.

For property (iv), clearly $D^* = P_0 = \{x \in D^* \mid \nu(x) \geq 0\}$ and application of (iii) gives $D_0^* = (P_0)_0 \subset P_1$. Assuming that $D_n^* \subset P_n$, Lemma 2.18 and (iv) yield $D_{n+1}^* = (D_n^*)_0 \subset (P_n)_0 \subset P_{n+1}$, as we desired. □

Corollary 2.20. *If $D_0^* = (D_0^*)_0 \neq \varnothing$, then D is not a Euclidean domain.*

Proof. The hypotheses of this corollary implies $D_n^* = D_0^*$ for all n. If D is a Euclidean domain, by Theorem 2.19, we have $\varnothing \neq D_0^* = \bigcap D_n^* = \varnothing$, which is a contradiction. Therefore, if $D_0^* = (D_0^*)_0 \neq \varnothing$, then D is not a Euclidean domain. □

Lemma 2.21. *Let D and U be as above. Then*

(a) $D_0^* = D^* - U$

(b) $D_0^* - (D_0^*)_0 =$ *the set of all universal side divisors in* D_0^*

Proof. (a) If x is a unit in D, say $xy = 1$ for some $y \in D$, and z is any element of D, then $z + x(-yz) = 0$ is not in D^*, that is, $z + xD \not\subset D^*$ for any $z \in D$. This shows that units are not in D_0^*.

If x is not a unit in D, then using $z = -1$, $z + xy \neq 0$ for all y in D, that is, $-1 + xD \subset D^*$. Which shows that if x is not a zero and not a unit, then x is in D_0^*.

(b) If x is in $(D_0^*)_0$, then x is in D_0^*, and so there is a y in D such that $y + xD \subset D_0^* = D^* - U$.

Case 1. If $z = 0$, then for any $w \in D$,

$$\begin{aligned} y + xw \neq 0 = z \quad &\iff \quad y \neq x(-w) = x(-w) + 0 = x(-w) + z \\ &\iff \quad x \nmid y = y + 0 \\ &\iff \quad x \nmid y + z. \end{aligned}$$

Case 2. If z is unit, then for any $w \in D$,

$$\begin{aligned} y + xw \neq (-z) \quad &\iff \quad x(-w) \neq y + z \\ &\iff \quad x \nmid y + z. \end{aligned}$$

By Cases 1 and 2, x never divides $y + z$ if z is zero or a unit. Thus, x is not a side divisor of y, and therefore, not a universal side divisor.

Conversely, if x is not in $(D_0^*)_0$, and it is in D_0^*, then for every y in D there exists a w in D with $y + xw$ not in D_0^*; i.e., $y + xw$ is a zero or a unit, and thus $x \mid (y + z)$ where $z \notin D_0^* = D^* - U$, i.e., x is a side divisor of y. Since this holds for every y in

D, x is a universal side divisor.

Therefore, these two arguments show that $(D_0^*)_0$ is the set D_0^* exclusive of the universal side divisors, that is, $x \mid (y+0)$, $x \mid (y + \text{unit})$. □

If D has no universal side divisors, then $D_0^* = (D_0^*)_0 \neq \varnothing$. Therefore the corollary will complete the proof that D is not a Euclidean domain.

Corollary 2.20 and Lemma 2.21 are now used to show that D is not a Euclidean domain.

Lemma 2.22. *Let D and U be as above. A side divisor of 2 in D is a non-unit divisor of 2 or 3.*

Proof. Let x be a side divisor of 2 in D. Then $x \in D_0^* = D^* - U$, i.e., x is a non-unit, and there is an element $z \notin D_0^*$, that is, by Lemma 2.21, $z \in \{0\} \bigcup U = \{0, \pm 1\}$. Thus $x \mid (2+z)$, i.e.,

$$x \mid (2+0), \quad x \mid (2+1) = 3, \quad x \mid (2-1) = 1,$$

and so $x \mid 2$ or $x \mid 3$, as we wished. □

Lemma 2.23. *Let D and U be as above. Then a side divisor of $\dfrac{1+\sqrt{-13}}{2}$ in D is a divisor of*

$$\frac{1+\sqrt{-13}}{2}, \quad \frac{3+\sqrt{-13}}{2}, \quad \textit{or} \quad \frac{-1+\sqrt{-13}}{2}.$$

Proof. Let x be a side divisor of $\dfrac{1+\sqrt{-13}}{2}$ in D.
Then, by Lemma 2.21, there exists $z \in \{0\} \bigcup U = \{0, \pm 1\}$, such that

$$x \;\Big|\; \left(\frac{1+\sqrt{-13}}{2}\right) + z,$$

and hence

$$\left(\frac{1+\sqrt{-13}}{2}\right) + z \quad = \quad \frac{1+\sqrt{-13}}{2}, \quad \frac{3+\sqrt{-13}}{2}, \quad \text{or} \quad \frac{-1+\sqrt{-13}}{2}$$

which completes the proof. □

Theorem 2.24 (Theorem 3.22, [2])**.** *If a_1, a_2, ... , a_n are nonzero integers, then the equation*

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c$$

has an integral solution if and only if

$$(a_1, a_2, ..., a_n) = d \mid c.$$

3. Some Example of a Principal Ideal Domain which is not a Euclidean Domain

Theorem 3.1. *The domain*

$$D = \left\{ a + \frac{b(1+\sqrt{-13})}{2} \;\Bigg|\; a \text{ and } b \text{ are integers} \right\}$$

is a principal ideal domain.

Proof. We will show that the domain D under consideration satisfies the hypotheses of Theorem 2.16.

Recall that N is a multiplicative norm on $\mathbb{C}$. Note that N is also a multiplicative norm on D. Let x, y, z and w be in D. Then we observe that

$$\begin{aligned} & 0 < N(xz - yw) < N(y) \\ \text{iff} \quad & 0 < \frac{N(xz - yw)}{N(y)} < 1 \\ \text{iff} \quad & 0 < N\left(\frac{xz - yw}{y}\right) < 1 \\ \text{iff} \quad & 0 < N\left(\frac{x}{y} \cdot z - w\right) < 1, \end{aligned}$$

for all z and w in D.

Let x and y be in D^* and $y \nmid x$, then we can write

$$\begin{aligned} \frac{x}{y} &= \frac{s + \dfrac{t(1+\sqrt{-13})}{2}}{u + \dfrac{v(1+\sqrt{-13})}{2}} = \frac{2s + t(1+\sqrt{-13})}{2u + v(1+\sqrt{-13})} = \frac{(2s+t) + t\sqrt{-13}}{(2u+v) + v\sqrt{-13}} \\ &= \frac{((2s+t) + t\sqrt{-13}) \times ((2u+v) - v\sqrt{-13})}{((2u+v) + v\sqrt{-13}) \times ((2u+v) - v\sqrt{-13})} \\ &= \frac{((2s+t)(2u+v) + 13tv) + ((2s+t)(-v) + (2u+v)t)\sqrt{-13}}{(2u+v)^2 + 13v^2} \end{aligned}$$

where s, t, u, v are integers.

Let

$$\begin{aligned} a' &= (2s+t)(2u+v) + 13tv, \\ b' &= (2s+t)(-v) + (2u+v)t, \\ c' &= (2u+v)^2 + 13v^2. \end{aligned}$$

Then we can rewrite

$$\frac{x}{y} = \frac{(a' + b'\sqrt{-13})}{c'} = \frac{(a + b\sqrt{-13})}{c}$$

where a, b, c are integers with $(a, b, c) = 1$.

Note that

$$\begin{aligned} a + b\sqrt{-13} &= a + \frac{2b(1 + \sqrt{-13})}{2} - b \\ &= (a - b) + \frac{2b(1 + \sqrt{-13})}{2} \in D. \end{aligned}$$

If $c = 1$, then

$$x = (a + b\sqrt{-13})y,$$

that is, $y \mid x$, a contradiction. Hence, $c > 1$.

(i) First of all, assume that $c \geq 5$.

By Theorem 2.24, there exist integers d, e, f such that

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

and by Division Algorithm, there exist q and r in $\mathbb{Z}$ such that

$$ad - 13be = cq + r,$$

and $|r| \leq \frac{c}{2}$.

Set $z = d + e\sqrt{-13}$ and $w = q - f\sqrt{-13}$. Then

$$\begin{aligned}
\left(\frac{x}{y}\right)\cdot z - w &= \frac{(a+b\sqrt{-13})}{c}\cdot(d+e\sqrt{-13})-(q-f\sqrt{-13})\\
&= \frac{(ad+ae\sqrt{-13}+bd\sqrt{-13}-13be)}{c}-\frac{(cq-cf\sqrt{-13})}{c}\\
&= \frac{ad-13be-cq+\sqrt{-13}(ae+bd+cf)}{c}\\
&= \frac{(cq+r-cq+\sqrt{-13})}{c}\\
&= \frac{r}{c}+\frac{\sqrt{-13}}{c}\\
&= \frac{r}{c}+\frac{\sqrt{13}}{c}i.
\end{aligned}$$

This complex number is not zero and has a nonzero norm

$$N\left(\frac{x}{y}\cdot z - w\right) = \left(\frac{r}{c}\right)^2 + \left(\frac{\sqrt{13}}{c}\right)^2 = \frac{r^2+13}{c^2},$$

which is less than 1. In fact, since $r^2 \leq \dfrac{c^2}{4}$, $c \geq 5$,

$$\frac{r^2+13}{c^2} \leq \frac{\frac{c^2}{4}+13}{c^2} = \frac{1}{4}+\frac{13}{c^2} \leq \frac{1}{4}+\frac{13}{5^2} = \frac{77}{100} < 1.$$

The remaining possibilities are $c = 2$, 3, or 4.

Consider these in order.

(ii) If $c = 2$, then $y \nmid x$ and $(a, b, 2) = 1$, then both a and b are not even. If both a and b are odd, then

$$\begin{aligned} \frac{x}{y} &= \frac{a + b\sqrt{-13}}{2} \\ &= \frac{(a-b) + b(1+\sqrt{-13})}{2} \\ &= \left(\frac{a-b}{2}\right) + \frac{b(1+\sqrt{-13})}{2}. \end{aligned}$$

Since both a and b are odd, then $a - b$ is even and $\frac{a-b}{2}$ is a integer, that is, $\frac{x}{y} \in D$, a contradiction. Thus it is impossible that both a and b are odd.

Then we shall show that $a^2 + 13b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 2$.

Case 1. $a = 2k$, $b = 2l + 1$. Then

$$\begin{aligned} a^2 + 13b^2 &\equiv a^2 + b^2 \pmod 2 \\ &= (2k)^2 + (2l+1)^2 \\ &= 4k^2 + 4l^2 + 4l + 1 \\ &= 2(2k^2 + 2l^2 + 2l) + 1 \\ &\not\equiv 0 \pmod 2. \end{aligned}$$

Case 2. $a = 2k + 1$, $b = 2l$. In this case, $a^2 + 13b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 2$ by the same idea as in Case 1.

Let $a^2 + 13b^2 = 2q + r$ where q, $r \in \mathbb{Z}$ and $0 \le r < 2$. Then, by Cases 1 and 2, $r = 1$. Set $z = a - b\sqrt{-13}$ and $w = q$.

Thus,

$$\begin{aligned}\left(\frac{x}{y}\right)\cdot z - w &= \frac{(a+b\sqrt{-13})}{2}\cdot(a-b\sqrt{-13}) - q\\ &= \frac{a^2+13b^2}{2} - q = \frac{2q+r}{2} - q\\ &= \frac{r}{2} \neq 0,\end{aligned}$$

and so

$$0 < N\left(\frac{x}{y}\cdot z - w\right) = \frac{r^2}{4} < 1.$$

(iii) Let $c = 3$. Then we shall show that $a^2 + 13b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 3$ using $(a, b, 3) = 1$. Thus it is impossible that both a and b are multiple of 3.

Case 1. $a = 3k$, $b = 3l \pm 1$. Then

$$\begin{aligned}a^2 + 13b^2 &\equiv a^2 + b^2 \pmod 3\\ &= (3k)^2 + (3l \pm 1)^2\\ &= 9k^2 + 9l^2 \pm 6l + 1\\ &= 3(3k^2 + 3l^2 \pm 2l) + 1\\ &\not\equiv 0 \pmod 3.\end{aligned}$$

Case 2. $a = 3k \pm 1$, $b = 3l$. In this case, $a^2 + 13b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 3$ by the same idea as in Case 1.

Case 3. $a = 3k \pm 1$, $b = 3l \pm 1$. Then

$$\begin{aligned} a^2 + 13b^2 &\equiv a^2 + b^2 \pmod 3 \\ &= (3k \pm 1)^2 + (3l \pm 1)^2 \\ &= 9k^2 \pm 6k + 1 + 9l^2 \pm 6l^2 + 1 \\ &= 3(3k^2 \pm 2k + 3l^2 \pm 2l) + 2 \\ &\not\equiv 0 \pmod 3. \end{aligned}$$

Let $a^2 + 13b^2 = 3q + r$ where q, $r \in \mathbb{Z}$ and $0 \le r < 3$. Then, by the above three cases, $r = 1$ or 2. Set $z = a - b\sqrt{-13}$ and $w = q$.

Thus,

$$\begin{aligned} \left(\frac{x}{y}\right) \cdot z - w &= \frac{(a + b\sqrt{-13})}{3} \cdot (a - b\sqrt{-13}) - q \\ &= \frac{a^2 + 13b^2}{3} - q = \frac{3q + r}{3} - q \\ &= \frac{r}{3} \ne 0, \end{aligned}$$

and so

$$0 < N\left(\frac{x}{y} \cdot z - w\right) = \frac{r^2}{9} < 1.$$

(iv) If $c = 4$, $(a, b, 4) = 1$, then both a and b are not even.

Then we shall show that $a^2 + 13b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 4$.

Case 1. $a = 2k$, $b = 2l + 1$. Then

$$\begin{aligned} a^2 + 13b^2 &\equiv a^2 + b^2 \pmod 4 \\ &= (2k)^2 + (2l + 1)^2 \\ &= 4k^2 + 4l^2 + 4l + 1 \\ &= 4(k^2 + l^2 + l) + 1 \\ &\not\equiv 0 \pmod 4. \end{aligned}$$

Case 2. $a = 2k+1$, $b = 2l$. In this case, $a^2 + 13b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 4$ by the same idea as in Case 1.

Case 3. $a = 2k+1$, $b = 2l+1$. Then

$$\begin{aligned} a^2 + 13b^2 &\equiv a^2 + b^2 \pmod 4 \\ &= (2k+1)^2 + (2l+1)^2 \\ &= 4k^2 + 4k + 1 + 4l^2 + 4l + 1 \\ &= 4(k^2 + k + l^2 + l) + 2 \\ &\not\equiv 0 \pmod 4. \end{aligned}$$

Let $a^2 + 13b^2 = 4q + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < 4$. Then, by the above three cases, $r = 1$, 2 or 3. Set $z = a - b\sqrt{-13}$ and $w = q$. Thus,

$$\begin{aligned} \left(\frac{x}{y}\right) \cdot z - w &= \frac{(a + b\sqrt{-13})}{4} \cdot (a - b\sqrt{-13}) - q \\ &= \frac{a^2 + 13b^2}{4} - q = \frac{4q + r}{4} - q \\ &= \frac{r}{4} \neq 0. \end{aligned}$$

and so

$$0 < N\left(\frac{x}{y} \cdot z - w\right) = \frac{r^2}{16} < 1.$$

Therefore, by Theorem 2.16, the integral domain D is a principal ideal domain, as we desired. □

Theorem 3.2. *The domain D with usual norm is not a Euclidean domain.*

Proof. Using Theorem 2.19, Corollary 2.20, and Lemma 2.21, it can now be shown that D has no universal side divisor.

If $x = a + \dfrac{b(1+\sqrt{-13})}{2}$ is a universal side divisor where a, $b \in \mathbb{Z}$, then x is a side divisor of 2.

A side divisor of 2 in D must be a non-unit divisor of 2 or 3, by Lemma 2.22.

Note that, by Lemma 2.10, 2 and 3 are irreducible in D. In other words, any side divisor of 2 are 2, -2, 3, and -3, by Lemma 2.9. Then x is one of the element 2, -2, 3, or -3.

On the other hand, by Lemma 2.23, a side divisor of $\dfrac{(1+\sqrt{-13})}{2}$ must be a non-unit divisor of

$$\frac{(1+\sqrt{-13})}{2}, \quad \frac{(3+\sqrt{-13})}{2}, \quad \text{or} \quad \frac{(-1+\sqrt{-13})}{2},$$

and these elements of D have norms of $\dfrac{7}{2}$, $\dfrac{11}{2}$, and $\dfrac{7}{2}$ respectively, while the norms of ± 2 and ± 3 are 4 and 9, respectively.

As a result, any side divisor of 2 cannot be a side divisor of $\dfrac{(1+\sqrt{-13})}{2}$, and thus there are no universal side divisors in D.

Therefore, the domain D with usual norm is not a Euclidean domain. $\square$

References

[1] John B. Fraleigh, *A First Course In Abstract Algebra*, Seventh Edition, *Addison Wesley*, (2003)

[2] Kenneth H. Rosen, *Elementary Number Theory and its applications*, Fourth Edition, *Addison Wesley Longman*, (2000)

[3] Wilson, J. C., *A Principal Ideal Ring That Is Not a Euclidean Ring*, *Math. Mag.*, **Vol 46** (1973), 34–38.

국 문 초 록

유클리드 정역이 아닌 주아이디얼 정역

성신여자대학교 교육대학원

교육학과 수학교육전공

방 지 원

[유클리드 정역이면 주아이디얼 정역이다] 라는 명제는 성립한다. 하지만, 그 역은 성립하지 않는다. 즉, 주아이디얼 정역이면서 유클리드 정역이라 할 수 없는 예는 얼마든지 존재할 수 있다.

이 논문에서는 주아이디얼 정역이지만, 유클리드 정역이 될 수 없는 예를

$$D=\left\{a+\frac{b(1+\sqrt{-13})}{2} \mid a,b\text{는 정수}\right\}$$

이것을 이용하여 몇 개의 정의와 정리를 사용해서 증명하였다.