신 용 수 교수지도

석사학위청구논문

Non-unique Factorization Domain, but Factorization Domain.

2008

성신여자대학교 교육대학원

교육학과 수학교육전공

임 선 영

Non-unique Factorization Domain, but Factorization Domain.

신 용 수 교수지도

이 논문을 석사학위논문으로 제출함.

2008년 5월

성신여자대학교 교육대학원
교육학과 수학교육전공
임 선 영

인 준 서

임선영의 석사학위 논문으로 인준함.

심사위원 _____인

심사위원 _____인

심사위원 _____인

성신여자대학교 교육대학원

논문개요

이 논문에서는 factorization domain이지만, unique factorization domain이 아닌 integral domain에 대해 연구하였다. 소수 p에 대해 integral domain인 $D = Z[\sqrt{-p}] = \{a + b\sqrt{-p}\,|\, a, b \in Z\}$이 facto -rization domain이지만 unique factorization domain가 아닌 것을 증명하였다. 그리고 integral domain인 $D = Z\{\sqrt{p}]$와 $D = Z[\sqrt{2p}]$이 factorizat -ion domain이지만 unique factorization domain가 아닌 몇 개의 예를 만들었다.

목차

1. Introduction

$\mathbb{Z}$ and $\mathbb{Q}$ are rings of integers and rational numbers respectively, and let D be an integral domain.

In this thesis, we study an integral domain which is not a unique factorization domain, but a factorization domain.
In Section 2, we prove that an integral domain $D = \mathbb{Z}[\sqrt{-p}] = \{a + b\sqrt{-p} \mid a, b \in \mathbb{Z}\}$, for a prime number p, is not a UFD, but a FD. Furthermore, we make some examples of an integral domain $D = \mathbb{Z}[\sqrt{-p}]$ which is a factorization domain, but not a UFD.

In Section 3, for making some examples of a non-UFD but a FD of type $\mathbb{Z}[\sqrt{2p}]$, we first define the concepts of a quadratic residue and a quadratic nonresidue. Then we introduce the *Legendre symbol*, a notation that tells us whether an integer a is a quadratic nonresidue of p. Also we introduce *Euler's Criterion* so that we can determine whether an integer a is a quadratic nonresidue of p. And using *Euler's Criterion*, we can determine -1 and 2 are quadratic nonresidues of p.
In the end, we make some examples of an integral domain $D = \mathbb{Z}[\sqrt{2p}]$ which is a factorization domain, but not a UFD.

2. Preliminaries Notations and Definitions

Definition 1 ([2], [3]). Let R be a commutative ring with unity 1.

(a) Let $a, b \in R$. If there exists $c \in R$ such that $b = ac$, then a ***divides*** b (or a is a ***factor of*** b), denoted by $a \mid b$.

(b) An element u of R is a ***unit of*** R if u divides 1, that is, if u has a multiplicative inverse in R. Two elements $a, b \in R$ are ***associates in*** R if $a = bu$ where u is a unit in R.

Definition 2 ([2], [3]). (a) A nonzero element p that is not a unit of an integral domain D is an ***irreducible of*** D if in every factorization $p = ab$ in D has the property that either a or b is a unit.

(b) An integral domain D is a ***factorization domain*** (abbreviated FD) if every element in D which is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.

(c) A factorization domain D is a ***unique factorization domain*** (abbreviated UFD) if $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and q_j are associates.

Definition 3 ([2], [3]). 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:

(a) $N(\alpha) = 0$ if and only if $\alpha = 0$.

(b) $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in D$.

Remark 4. (a) Let D be an integral domain with a multiplicative norm N, $N(1) = N(1^2) = N(1)^2$. Thus $N(1) = 1$ since $N(1) \neq 0$. Furthermore, if u is a unit in D, that is, $uu^{-1} = 1$, then $N(uu^{-1}) = N(u)N(u^{-1}) = N(1) = 1$. Therefore $|N(u)| = 1$ for every unit u in D.

(b) Let D and N be as in (a). If 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. In fact, let $\pi = \alpha \cdot \beta$ where $\alpha, \beta \in D$. Then $N(\pi) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$=$p$ is a prime, i.e., $|N(\alpha)| = 1$ or $|N(\beta)| = 1$, and thus either α or β is a unit in D.

Recall that

- a^2 is a *perfect square* when $a \in \mathbb{Z}$ and $a \geq 2$, and
- a *square free integer* is an integer that is not divisible by any perfect squares other than 1.

The following lemma is a straightforward computation.

Lemma 5. *Let p be a prime number and let $D = \mathbb{Z}[\sqrt{-p}]$. Define N on D by*

$$N(a + b\sqrt{-p}) = a^2 + pb^2, \quad a, b \in \mathbb{Z}.$$

Then

(a) *N is a multiplicative norm on D.*
(b) *$\alpha \in D$ is a unit of D if and only if $\alpha = \pm 1$.*

Proof. (a) Let $\alpha = a + b\sqrt{-p}$ with $a, b \in \mathbb{Z}$. Then it is obvious that $N(\alpha) = a^2 + pb^2 = 0$ if and only if $a = b = 0$, that is, $\alpha = 0$.

Now let $\alpha{=}a + b\sqrt{-p}$ and $\beta{=}c + d\sqrt{-p} \in D$ where a, b, c and d in $\mathbb{Z}$. Then

$$\begin{aligned}
N(\alpha \cdot \beta) &= N((a + b\sqrt{-p}) \cdot (c + d\sqrt{-p})) \\
&= N((ac - bdp) + (ad + bc)\sqrt{-p}) \\
&= (ac - bdp)^2 + p(ad + bc)^2 \\
&= a^2c^2 + b^2d^2p^2 + a^2d^2p + b^2c^2p \\
&= a^2c^2 + b^2d^2p^2 + p(a^2d^2 + b^2c^2), \text{ and} \\
N(\alpha) \cdot N(\beta) &= (a^2 + pb^2) \cdot (c^2 + pd^2) \\
&= a^2c^2 + a^2d^2p + b^2c^2p + b^2d^2p^2 \\
&= a^2c^2 + b^2d^2p^2 + p(a^2d^2 + b^2c^2),
\end{aligned}$$

and hence $N(\alpha \cdot \beta){=}N(\alpha) \cdot N(\beta)$.

(b) Let $\alpha = a + b\sqrt{-p}$ be a unit in D with $a, b \in \mathbb{Z}$. Then by Remark 4(b), $|N(\alpha)| = |N(a + b\sqrt{-p})| = |a^2 + pb^2| = a^2 + pb^2 = 1$. Since $p > 1$, we have $a = \pm 1$ and $b = 0$, that is, $\alpha = \pm 1$.
Moreover, it is obvious that $\alpha = \pm 1$ is a unit in D, which completes the proof. □

Lemma 6. *Let D and N be as in Lemma 5. Then D is a FD.*

Proof. We shall prove this by induction on $|N(\alpha)|$. First, assume that $|N(\alpha)| = 2$. Then $|N(\alpha)| = 2$ is a prime in $\mathbb{Z}$, and so α is an irreducible of D by Remark 4 (b).

Now assume $|N(\alpha)| > 2$. If α is an irreducible of D, then we are done. Suppose $\alpha = \beta \cdot \gamma$ with $\beta, \gamma \in D$ and β, γ are non-units. Since

$$\begin{aligned} |N(\alpha)| &= |N(\beta \cdot \gamma)| \\ &= |N(\beta) \cdot N(\gamma)| \\ &= |N(\beta)||N(\gamma)|, \end{aligned}$$

$|N(\beta)| > 1$ and $|N(\gamma)| > 1$, we have $1 < |N(\beta)|, |N(\gamma)| < |N(\alpha)|$ by Lemma 5 (b) (or Remark 4(a)). Hence by induction on $|N(\alpha)|$, $\beta = p_1 \cdots p_r$, $\gamma = q_1 \cdots q_s$ where p_i, q_j are all irreducibles of D. Therefore, $\alpha = \beta \cdot \gamma = (p_1 \cdots p_r) \cdot (q_1 \cdots q_s)$, as we wished. □

Here is a theorem of an integral domain which is not a UFD, but a FD.

Theorem 7. *Let D and N be as in Lemma 5 and let $a \in \mathbb{Z} - \{0\}$. If $1 + a^2 p = qr$ for some distinct prime numbers $q, r \in \mathbb{Z} - \{0\}$ with $q < p$. Then D is not a UFD, but a FD.*

Proof. By Lemma 6, D is a FD. Hence it suffices to show that there is a non-zero and non-unit element $\alpha \in D$ which can be factored by two different products of irreducibles of D. Let $\alpha = 1 + a\sqrt{-p}$.

First, note that if $\beta = c + d\sqrt{-p}$ with $c, d \in \mathbb{Z}$, $d \neq 0$, then

$$N(\beta) = c^2 + d^2 p \geq p > q. \tag{1}$$

Note that if $\beta = c + d\sqrt{-p}$ with $c, d \in \mathbb{Z}$, β devides α, and $d = 0$, then β is a unit in D. In fact, if $\beta = c \in \mathbb{Z}$, then $c \mid 1$, which means that β is a unit of D. In other words, if β devides α, $\beta \in D$ and β is not a unit in D, then β is the form of $c + d\sqrt{-p}$ with $c, d \in \mathbb{Z}$, $d \neq 0$.

Let $\alpha = \beta \cdot \gamma$ with $\beta, \gamma \in D$. If β is not a unit of D, then β is the form of $c + d\sqrt{-p}$ with $c, d \in \mathbb{Z}$, $d \neq 0$ by the above argument.
Furthermore, since

$$\begin{aligned} |N(\alpha)| &= |N(\beta)||N(\gamma)| \\ &= 1 + a^2 p \\ &= q \cdot r, \text{ and} \end{aligned}$$

by equation (1), $|N(\beta)| > q$ we have $|N(\gamma)| = 1$, that is, γ is a unit of D by Remark 4(b). This means that α is an irreducible of D.
Similarly, one can show that $\alpha' = 1 - a\sqrt{-p}$ is an irreducible of D.
Now suppose $q = q_1 \cdot q_2$ where q_1, q_2 are non-units in D. Then

$$q^2 = N(q) = N(q_1 \cdot q_2) = N(q_1)N(q_2) \Rightarrow N(q_1) = q$$

by Remark 4(b). Let $q_1 = e + f\sqrt{-p}$ where $e, f \in \mathbb{Z}$. Then

$$q = N(q_1) = e^2 + f^2 p \Rightarrow e^2 = q \text{ and } f = 0,$$

for $p > q$, which is a contradiction since q is a prime in $\mathbb{Z}$. In other words, q is an irreducible of D.
Furthermore, since D has only units ± 1, it is obvious that $1 + a\sqrt{-p}$ and q cannot be associates in D. Therefore, $\alpha = 1 + a^2 p$ can be factored by two different products of irreducibles in D, and hence D is not a UFD, as we desired. □

Here are some examples of a factorization domain, but not UFD. Furthermore one can make many examples as in Example 8.

Example 8. (a) Let $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Choose $p = 5$ and $a = 3$ in Theorem 7.

$$\begin{aligned} N(1 + 3\sqrt{-5}) &= 1 + 3^2 \cdot 5 \\ &= 46 \\ &= 2 \cdot 23 \end{aligned}$$

for distinct prime numbers $2, 23 \in \mathbb{Z} - \{0\}$ with $2 < 5$.

(b) Let $\mathbb{Z}[\sqrt{-13}] = \{a + b\sqrt{-13} \mid a, b \in \mathbb{Z}\}$. Choose $p = 13$ and $a = 3$ in Theorem 7.

$$\begin{aligned} N(1 + \sqrt{-13}) &= 1 + 3^2 \cdot 13 \\ &= 118 \\ &= 2 \cdot 59 \end{aligned}$$

for distinct prime numbers $2, 29 \in \mathbb{Z} - \{0\}$ with $2 < 13$.

(c) Let $\mathbb{Z}[\sqrt{-17}] = \{a + b\sqrt{-17} \mid a, b \in \mathbb{Z}\}$. Choose $p = 17$ and $a = 2$ in Theorem 7.

$$\begin{aligned} N(1 + 2\sqrt{-17}) &= 1 + 2^2 \cdot 17 \\ &= 69 \\ &= 3 \cdot 23 \end{aligned}$$

for distinct prime numbers $3, 23 \in \mathbb{Z} - \{0\}$ with $3 < 17$.

(d) Let $\mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} \mid a, b \in \mathbb{Z}\}$. Choose $p = 19$ and $a = 2$ in Theorem 7.

$$\begin{aligned} N(1 + 2\sqrt{-19}) &= 1 + 2^2 \cdot 19 \\ &= 77 \\ &= 7 \cdot 11 \end{aligned}$$

for distinct prime numbers $7, 11 \in \mathbb{Z} - \{0\}$ with $7 < 11$.

3. Some Example of Non-UFD but FD of Type $\mathbb{Z}[\sqrt{p}]$

In the previous section, we gave some examples of an integral domain which is not a UFD but a FD of type $\mathbb{Z}[\sqrt{-p}]$ for some prime p. In this section, we shall give some examples of a non-UFD but a FD of type $\mathbb{Z}[\sqrt{p}]$ for a prime number p.

Lemma 9. *Let p be a prime number and let $D := \mathbb{Z}[\sqrt{p}] = \{a+b\sqrt{p} \mid a, b \in \mathbb{Z}\}$. Define $N(a + b\sqrt{p}) = a^2 - pb^2$. Then*

(a) *$N : D \to \mathbb{Z}$ is a multiplicative norm.*
(b) *$\alpha \in D$ is a unit if and only if $N(\alpha) = \pm 1$*

Proof. (a) Let $\alpha = a + b\sqrt{p}$ with $a, b \in \mathbb{Z}$. Then it is obvious that $N(\alpha) = a^2 - pb^2 = 0$ if and only if $a = b = 0$, that is, $\alpha = 0$.

Now let $\alpha = a + b\sqrt{p}$, and $\beta = c + d\sqrt{p} \in \mathbb{Z}$ where a, b, c and d in $\mathbb{Z}$. Then

$$\begin{aligned} N(\alpha \cdot \beta) &= N((a + b\sqrt{p}) \cdot (c + d\sqrt{p})) \\ &= N((ac + bdp) + (ad + bc)\sqrt{p}) \\ &= (ac + bdp)^2 - p(ad + bc)^2 \\ &= a^2c^2 + b^2d^2p^2 - a^2d^2p - b^2c^2p \\ &= a^2c^2 + b^2d^2p^2 - p(a^2d^2 + b^2c^2), \text{ and} \\ N(\alpha) \cdot N(\beta) &= N(a + b\sqrt{p}) \cdot N(c + d\sqrt{p}) \\ &= (a^2 - pb^2)(c^2 - pd^2) \\ &= a^2c^2 - a^2d^2p - b^2c^2p + b^2d^2p^2 \\ &= (a^2c^2 + b^)2d^2p^2) - p(a^2d^2 + b^2c^2), \end{aligned}$$

and hence $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

(b) Let $\alpha = a + b\sqrt{p}$ be a unit in D with $a, b \in \mathbb{Z}$. Then by Remark 4(b), $|N(\alpha)| = |N(a + b\sqrt{p})| = |a^2 - pb^2| = 1$, that is, $N(\alpha) = \pm 1$.
Conversely, assume $N(\alpha) = \pm 1$, where $\alpha = a + b\sqrt{p}$ in D with $a, b \in \mathbb{Z}$.
Then $N(\alpha) = a^2 - pb^2 = (a + b\sqrt{p})(a - b\sqrt{p}) = \pm 1$, that is, $\alpha = a + b\sqrt{p}$ is a unit of D, which completes the proof. □

Lemma 10. *Let p be a prime integer and let $D := \mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Z}\}$. Then D is a FD.*

Proof. We shall prove this by induction on $|N(\alpha)|$. First, assume that $|N(\alpha)| = 2$. Then $|N(\alpha)| = 2$ is a prime in $\mathbb{Z}$, and so α is an irreducible of D by Remark 4 (b).

Now assume $|N(\alpha)| > 2$. If α is an irreducible of D, then we are done. Suppose $\alpha = \beta \cdot \gamma$ with $\beta, \gamma \in D$ and β, γ are non-units. Since

$$\begin{aligned} |N(\alpha)| &= |N(\beta \cdot \gamma)| \\ &= |N(\beta) \cdot N(\gamma)| \\ &= |N(\beta)||N(\gamma)|, \end{aligned}$$

$|N(\beta)| > 1$ and $|N(\gamma)| > 1$, we have $1 < |N(\beta)|, |N(\gamma)| < |N(\alpha)|$ by Lemma 9 (b) (or Remark 4(a)). Hence by induction on $|N(\alpha)|$, $\beta = p_1 \cdots p_r$, $\gamma = q_1 \cdots q_s$ where $p_\imath$, $q_\jmath$ are all irreducibles of D. Therefore, $\alpha = \beta \cdot \gamma = (p_1 \cdots p_r) \cdot (q_1 \cdots q_s)$, as we wished. □

Recall that if m is a positive integer, we say that the integer a is a ***quadratic residue of*** m if $(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. If the congruence $x^2 \equiv a \pmod{m}$ has no solution, we say that a is a ***quadratic nonresidue of*** m.

Definition 11 ([1])**.** Let p be an odd prime and a be an integer not divisible by p. The ***Legendre symbol*** $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p. \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Example 12. The previous example shows that the Legendre symbols

$\left(\frac{a}{17}\right)$, $a = 1, 2, \ldots, 16$ have the following values:

$$\begin{aligned} & \left(\frac{1}{17}\right) = \left(\frac{2}{17}\right) = \left(\frac{4}{17}\right) = \left(\frac{8}{17}\right) = \left(\frac{9}{17}\right) = \left(\frac{13}{17}\right) \\ = \ & \left(\frac{15}{17}\right) = \left(\frac{16}{17}\right) = 1, \end{aligned}$$

$$\begin{aligned} & \left(\frac{3}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{11}{17}\right) \\ = \ & \left(\frac{12}{17}\right) = \left(\frac{14}{17}\right) = -1. \end{aligned}$$

Theorem 13 (Theorem 11.3 (Euler's Criterion), [1])**.** *Let p be an odd prime and let a be a positive integer not divisible by p. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Theorem 14 (Theorem 11.4, [1])**.** *Let p be an odd prime and a and b be integers not divisible by p. Then*

(a) *if* $a \equiv b \pmod{p}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(c) $\left(\frac{a^2}{p}\right) = 1$.

Theorem 15 (Theorem 11.5, [1])**.** *If p is an odd prime, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}. \\ -1 & \text{if } p \equiv -1 \pmod{4}. \end{cases}$$

Example 16. Let $p = 29$. By Theorem 15, since $29 \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = 1$. Hence -1 is a quadratic residue of 29.

Theorem 17 (Theorem 11.6, [1])**.** *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Hence, 2 is a quadratic residue of all primes $p \equiv \pm 1 \pmod 8$ and a quadratic nonresidue of all primes $p \equiv \pm 3 \pmod 8$.

Example 18. (a) Let $p = 31$. By Theorem 17,

$$\left(\frac{2}{p}\right) = (-1)^{(31^2-1)/8} = 1,$$

that is, 2 is a quadratic residue of 31.

(b) Let $p = 29$. By Theorem 17,

$$\left(\frac{2}{p}\right) = (-1)^{(29^2-1)/8} = -1,$$

that is, 2 is a quadratic nonresidue of 29.

Theorem 19. *Let p be a prime number and let $D := \mathbb{Z}[\sqrt{2p}] = \{a + b\sqrt{2p} \mid a, b \in \mathbb{Z}\}$. Assume that ± 2 is quadratic nonresidues of p. Then ± 2 is an irreducible of D. Furthermore, if $\alpha \in D$ and $N(\alpha) = 2q$ for some odd prime number $q \in \mathbb{Z}$, then α is an irreducible of D.*

Proof. Define N on D as follows:

$$N(a + b\sqrt{2p}) = a^2 - 2pb^2 \text{ with } a, b \in \mathbb{Z}$$

Note that N is a multiplicative norm on D by Lemma 9. Moreover, α is a unit of D if and only if $N(\alpha) = \pm 1$.
Now suppose $\pm 2 = \alpha \cdot \beta$ where $\alpha, \beta \in D$. Then $N(\pm 2) = N(\alpha \cdot \beta) =$

$N(\alpha) \cdot N(\beta) = 4$, that is, $N(\alpha) = \pm 1,\ \pm 2,\ \pm 4$. If $N(\alpha) = \pm 1$, then α is a unit of D. If $N(\alpha) = \pm 4$, then $N(\beta) = \pm 1$, that is, β is a unit of D.
Assume $N(\alpha) = \pm 2$. Let $\alpha = a + b\sqrt{2p}$ where $a, b \in \mathbb{Z}$. Then

$$N(\alpha) = a^2 - 2pb^2 = \pm 2 \Rightarrow a^2 \equiv \pm 2 \pmod{p},$$

which means that ± 2 is a quadratic residue of p, a contradiction. Thus $N(\alpha) \neq \pm 2$ for any non-unit in $D^* = D - \{0\}$. Hence ± 2 is an irreducible of D.

Suppose α is reducible in D. Let $\alpha = \beta \cdot \gamma$ where $\beta,\ \gamma \in D$ and $\alpha = a + b\sqrt{2p}$ with $a, b \in \mathbb{Z}$. Then

$$\begin{aligned} N(\alpha) &= N(\beta \cdot \gamma) \\ &= N(\beta) \cdot N(\gamma) \\ &= a^2 - 2pb^2 \\ &= 2q, \end{aligned}$$

which follows that $N(\beta) = \pm 1, \pm 2, \pm q, \pm 2q$. However, by the above argument, we know that $N(\beta) \neq \pm 2$ for any β in D. In other words, for any non-zero divisor β of α, $N(\beta) = \pm 1, \pm 2q$. Thus if $N(\beta) = \pm 1$, then β is a unit in D, and if $N(\beta) = \pm 2q$, that is, $N(\gamma) = \pm 1$, then γ is a unit in D. Hence, α is an irreducible of D, as we wished. □

Example 20. (a) Consider an integral domain $D := \mathbb{Z}[\sqrt{10}]$. Then we have $p = 5$ in Theorem 19. Let $p = 5$ and $a = 1, 2, 3, 4$.
By Theorem 13,

$$\left(\frac{1}{5}\right) \equiv 1^{(5-1)/2} = 1^2 = 1 \equiv 1 \pmod{5},$$

$$\left(\frac{2}{5}\right) \equiv 2^{(5-1)/2} = 2^2 = 4 \equiv -1 \pmod{5},$$

$$\left(\frac{3}{5}\right) \equiv 3^{(5-1)/2} = 3^2 = 9 \equiv -1 \pmod{5}, \text{ and}$$

$$\left(\frac{4}{5}\right) \equiv 4^{(5-1)/2} = 4^2 = 16 \equiv 1 \pmod{5}.$$

Hence, the integers ± 2 are quadratic nonresidues of 5.
Thus by Theorem 19, ± 2 and ± 3 are irreducibles of D. In particular,

2 and 3 are irreducibles of D.

Let $\alpha = 4 + \sqrt{10} \in D$. Then

$$\begin{aligned} N(\alpha) &= N(4+\sqrt{10}) \\ &= N(4+\sqrt{2\cdot 5}) \\ &= (4+\sqrt{10})(4-\sqrt{10}) \\ &= 6 \\ &= 2\cdot 3. \end{aligned}$$

Thus, if we apply $q = 3$ in Theorem 19, then we know that $4 + \sqrt{10}$ is an irreducible of D.

Furthermore, if 2 and $4 + \sqrt{10}$ are associate in D, then

$$2 \cdot (a + b\sqrt{10}) = 4 + \sqrt{10},$$

for some $a, b \in \mathbb{Z}$, $a + b\sqrt{10}$ is a unit in D. Then $2b = 1$, which is impossible. Therefore, 2 and $4 + \sqrt{10}$ are not associates in $D = \mathbb{Z}[\sqrt{10}]$. In other words, 6 can be factored into two different products of irreducibles of D. Therefore, $\mathbb{Z}[\sqrt{10}]$ is not a UFD, but FD by Lemma 10.

(b) Now consider another integral domain $D := \mathbb{Z}[\sqrt{26}]$. Let $p = 13$ and $a = 1, 2, \ldots, 12$.
By Theorem 13,

$$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1.$$

$$\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1.$$

Hence, the quadratic nonresidue of 13 are $\pm 2, \pm 5, \pm 6$.
Thus by Theorem 19, ± 2 is an irreducible of D.

Consider $\alpha = 8 + \sqrt{26} \in D$. Then

$$\begin{aligned} N(\alpha) &= N(8+\sqrt{26}) \\ &= N(8+\sqrt{2\cdot 13}) \\ &= (8+\sqrt{26})(8-\sqrt{26}) \\ &= 38 \\ &= 2\cdot 19. \end{aligned}$$

Thus, if we choose $q = 19$ in Theorem 19, then we know that $8 + \sqrt{26}$ is an irreducible of D.

Furthermore, if 2 and $8 + \sqrt{26}$ are associates in D, then

$$2 \cdot (a + b\sqrt{26}) = 8 + \sqrt{26}$$

for some $a, b \in \mathbb{Z}$, $a + b\sqrt{26}$ is a unit in D. Then $2b = 1$, which is impossible. Therefore, 2 and $8 + \sqrt{26}$ are not associates in D. In other words, 38 can be factored into two different products of irreducibles of D. Therefore, $\mathbb{Z}[\sqrt{26}]$ is not a UFD, but FD by Lemma 10.

(c) Now consider another integral domain $D := \mathbb{Z}[\sqrt{58}]$. Let p=29 and a=1,2,...,28.
By Theorem 13,

$$\begin{aligned} & \left(\frac{1}{29}\right) = \left(\frac{4}{29}\right) = \left(\frac{5}{29}\right) = \left(\frac{6}{29}\right) = \left(\frac{7}{29}\right) = \left(\frac{9}{29}\right) = \left(\frac{13}{29}\right) \\ = \quad & \left(\frac{16}{29}\right) = \left(\frac{20}{29}\right) = \left(\frac{22}{29}\right) = \left(\frac{23}{29}\right) = \left(\frac{24}{29}\right) = \left(\frac{25}{29}\right) = \left(\frac{28}{29}\right) = 1. \end{aligned}$$

$$\begin{aligned} & \left(\frac{2}{29}\right) = \left(\frac{3}{29}\right) = \left(\frac{8}{29}\right) = \left(\frac{10}{29}\right) = \left(\frac{11}{29}\right) = \left(\frac{12}{29}\right) = \left(\frac{14}{29}\right) \\ = \quad & \left(\frac{15}{29}\right) = \left(\frac{17}{29}\right) = \left(\frac{18}{29}\right) = \left(\frac{19}{29}\right) = \left(\frac{21}{29}\right) = \left(\frac{26}{29}\right) = \left(\frac{27}{29}\right) = -1. \end{aligned}$$

Hence, the quadratic nonresidues of 29 are $\pm 2, \pm 3, \pm 8, \pm 10, \pm 11, \pm 12, \pm 14$. Thus, by Theorem 19, ± 2 is an irreducible of D.

Consider $\alpha = 8 + \sqrt{58} \in D$. Then

$$\begin{aligned} N(\alpha) &= N(8 + \sqrt{58}) \\ &= N(8 + \sqrt{2 \cdot 29}) \\ &= (8 + \sqrt{58})(8 - \sqrt{58}) \\ &= 6 \\ &= 2 \cdot 3. \end{aligned}$$

Thus, if we choose $q = 3$ in Theorem 19, then we know that $8 + \sqrt{58}$

is an irreducible of D.

Furthermore, if 2 and $8+\sqrt{58}$ are associates in D, then

$$2 \cdot (a + b\sqrt{58}) = 8 + \sqrt{58}$$

for some $a, b \in \mathbb{Z}$, $a + b\sqrt{58}$ is a unit in D. Then $2b = 1$, which is impossible. Therefore, 2 and $8+\sqrt{58}$ are not associates in $D = \mathbb{Z}[\sqrt{58}]$. In other words, 6 can be factored into two different products of irreducibles of D. Therefore, $\mathbb{Z}[\sqrt{58}]$ is not a UFD, but FD by Lemma 10, again.

References

[1] K.H. Rosen, *Elementary Number Theory 4th.*, Addison-Wesley (1999).
[2] T.W. Hungerford , *Algebra*, Springer-Verlag (1973).
[3] John B. Fraleigh, *A first course Abstract Algebra 7th.*, Addison-Wesley (2003).

ABSTRACT

Non-unique Factorization Domain, but Factorization Domain.

Im, Sun-Young
Mathematics Education Major
Department of Education
The Graduate School of Education
Sungshin Women's University

In this thesis, we study an integral domain which is not a unique factorization domain, but a factorization domain.

We prove that an integral domain $D = Z[\sqrt{-p}] = \{a + b\sqrt{-p} \mid a, b \in Z\}$, for a prime p, is not a unique factorization domain, but a factorization domain. Furthermore, we make some examples of an integral domain $D = Z[\sqrt{-p}]$ and an integral domain $D = Z[\sqrt{2p}]$ which are factorization domains, but not unique factorization domains.