J. Appl. Math. & Informatics Vol. 26(2008), No. 3 - 4, pp. 779 - 784
Website: http://www.kcam.biz

NON-UNIQUE FACTORIZATION DOMAINS

YONG SU SHIN

ABSTRACT. We show that $\mathbb{Z}[\sqrt{-p}]$ is not a unique factorization domain (UFD) but a factorization domain (FD) with a condition $1 + a^2p = qr$, where a and p are positive integers and q and r are positive primes in $\mathbb{Z}$ with $q < p$. Using this result, we also construct several specific non-unique factorization domains which are factorization domains. Furthermore, we prove that an integral domain $\mathbb{Z}[\sqrt{p}]$ is not a UFD but a FD for some positive integer p.

AMS Mathematics Subject Classification : 13D40, 14M10
Key words and Phrases : Factorization domains, unique factorization domains.

1. Introduction

Let D be an integral domain with an arbitrary characteristic. It is well-known that the ring of integers $\mathbb{Z}$ and the polynomial rings $F[x]$ over a field F are principal ideal domains (see [1], [2], and [3]). The chief result is that every Euclidean domain is a principal ideal domain and every principal ideal domain is a unique factorization domain.

In [4], Wilson proved that the ring $D = \left\{a + b(1 + \sqrt{-19})/2 \mid a, b \in \mathbb{Z}\right\}$ is a principal ideal domain, but not a Euclidean domain. Moreover there is a simple example $\mathbb{Z}[x]$ (the ring of polynomials with integer coefficients) of a unique factorization domain, but not a principal ideal domain. In this paper, we construct a factorization domain, but not a unique factorization domain.

In Section 2, we introduce some preliminary notations and definitions. We also prove that the subring $\mathbb{Z}[\sqrt{-p}]$ of the complex number field $\mathbb{C}$ cannot be a unique factorization domain (UFD) but a factorization domain (FD) for some square free positive integer $p \in \mathbb{Z}$ (see Theorem 7).

Received September 28, 2007.
This paper was supported by a grant from Sungshin Women's University in 2008.

In Section 3, we construct some different integral domains which are not a UFD but a FD of type $\mathbb{Z}[\sqrt{p}]$ for some $p \in \mathbb{Z}^+$ such that p is square free.

2. Non-unique factorization domains of type $\mathbb{Z}[\sqrt{-p}]$

Definition 1. 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. (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 that 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 numbered so that p_i and q_j are associates.

Definition 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 safisfied:

(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 is an integral domain with a multiplicative norm N, then $N(1) = 1$ and $N(u) = \pm 1$ for every unit u in D.

(b) Let D be as in (a). If every α such that $N(\alpha) = \pm 1$ 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.

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 straightforwrad computation that we leave to the reader.

Lemma 5. *Let p be a positive integer with $\sqrt{p} \notin \mathbb{Z}$ 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 $\alpha = \pm 1$.*

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

Proof. Assume $\alpha \in D$ is neither 0 nor a unit.

We shall prove this lemma by induction on $N(\alpha)$. Since α is neither 0 nor a unit, we have that $N(\alpha) \geq 2$ by Remark 4 (a). If $N(\alpha) = 2$, then α is an irreducible of D by Remark 4 (b).

Now suppose that $N(\alpha) > 2$. If α is an irreducible of D, then we are done. If α is not an irreducible, then $\alpha = \beta\gamma$ where $\beta, \gamma \in D$ and neither β nor γ is a unit of D. The fact that $1 < N(\beta), N(\gamma) < N(\alpha)$ indicate that there exist irreducibles $p_1, \ldots, p_t$ and $q_1, \ldots, q_s$ of D such that

$$\beta = p_1 \cdots p_t \quad \text{and} \quad \gamma = q_1 \cdots q_s$$

by induction on $N(\alpha)$. Therefore

$$\alpha = \beta\gamma = p_1 \cdots p_t q_1 \cdots q_s$$

is a product of irreducibles of D, as we desired. □

Using the following theorem, we can construct several kinds of examples of an integral domain which is not a UFD, but a FD (see Example 8).

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

Proof. Note that $(1 + a\sqrt{-p})(1 - a\sqrt{-p}) = 1 + a^2p$ and $N(\alpha) > p$ for every non-unit α in $D - \{0\}$. Let $1 + a\sqrt{-p} = \alpha\beta$ where $\alpha, \beta \in D$. Then $N(1 + a\sqrt{-p}) = N(\alpha\beta) = N(\alpha)N(\beta) = qr$, and so $N(\alpha) = 1, q, r$, or qr. Since $q < p$, it is impossible that either $N(\alpha)$ or $N(\beta)$ is q or r, and hence $N(\alpha) = 1$ or $N(\beta) = 1$, that is, either α or β is a unit of D. Thus $1 + a\sqrt{-p}$ is an irreducible of D. A similar argument shows that $1 - a\sqrt{-p}$ is also an irreducible of D.

If $q = \gamma\delta$ where $\gamma, \delta \in D$, then $N(q) = N(\gamma)N(\delta) = q^2$. However, since $q < p$, we have either $N(\gamma) = 1$ or $N(\delta) = 1$. In other words, either γ or δ is a unit of D. Thus q is an irreducible of D. Furthermore, since

$$(1 + a\sqrt{-p})(1 - a\sqrt{-p}) = qr$$

and q is not associate to both $1 + a\sqrt{-p}$ and $1 - a\sqrt{-p}$, $1 + aq^2$ can be factored into products of irreducibles of D by two different ways. Therefore, D is not a UFD, but a FD by Lemma 6, as we wished. □

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. Then $1 + a^2p = 1 + 3^2 \cdot 5 = 46 = 2 \cdot 23$ and $2 < 5$. Hence $\mathbb{Z}[\sqrt{-5}]$ is an integral domain which is not a UFD, but a FD by Theorem 7.

(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. Then $1 + a^2p = 1 + 3^2 \cdot 13 = 118 = 2 \cdot 59$ and $2 < 13$. Hence $\mathbb{Z}[\sqrt{-13}]$ is another example of an integral domain which is not a UFD, but a FD by Theorem 7 again.

3. Non-unique factorization domains of type $\mathbb{Z}[\sqrt{p}]$

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

Lemma 9. *Let p be a square free integer and let $D := \mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Z}\}$. Define N on D by*

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

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 $\alpha = a + b\sqrt{p} \in D$ with $a, b \in \mathbb{Z}$. If $N(\alpha) = a^2 - pb^2 = 0$, then $a^2 = pb^2$. Since p is a square free integer, we have that $a = b = 0$, that is, $\alpha = 0$. In other words, $N(\alpha) = 0$ if and only if $\alpha = 0$.

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

$$N(\alpha) = a^2 - pb^2 \quad \text{and} \quad N(\beta) = c^2 - pd^2.$$

Hence,

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

So N is a multiplicative norm on D.

(b) Let α be a unit in D. Then there exists an element $\beta \in D$ such that $\alpha\beta = 1$. Hence $N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1$, and so $N(\alpha) = \pm 1$. Conversely, let $\alpha = a + b\sqrt{p} \in D$ with $a, b \in D$ and assume $N(\alpha) = \pm 1$. Then

$$N(\alpha) = N(a + b\sqrt{p}) = a^2 - pb^2 = (a + b\sqrt{p})(a - b\sqrt{p}) = \pm 1,$$

and thus, $\alpha = a + b\sqrt{p}$ is a unit in D, as we desired. □

By the same method as in the proof of Lemma 6 with Lemma 9, one can easily prove the following lemma, and so we omit the proof here.

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

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.

Theorem 11. *Let p and q be positive integers such that pq is square free. Let $D := \mathbb{Z}[\sqrt{pq}] = \{a + b\sqrt{pq} \mid a, b \in \mathbb{Z}\}$. Assume that $\pm r$ is a quadratic nonresidue of q where r is a prime number in $\mathbb{Z}$. Then $\pm r$ is an irreducible of D.*

Proof. Let $a + b\sqrt{pq}$ with $a, b \in \mathbb{Z}$. Define N on D by

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

Note, by Lemma 9, that

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

Let $\alpha\beta = \pm r$ where $\alpha, \beta \in D$. Then $N(\pm r) = N(\alpha\beta) = N(\alpha)N(\beta) = r^2$ implies $N(\alpha) = \pm 1$, $\pm r$, or $\pm r^2$. If $N(\alpha) = \pm r$, then $N(\alpha) = a^2 - b^2pq = \pm r$, that is, $a^2 \equiv \pm r \pmod{q}$, which is a contradiction since $\pm r$ is a quadratic nonresidue of q by our assumption. In other words, $N(\alpha) \neq \pm r$ for any $\alpha \in D$. If $N(\alpha) = \pm 1$, then α is a unit of D by (b). If $N(\alpha) = \pm r^2$, then $N(\beta) = \pm 1$, i.e., β is a unit in D. Therefore, $\pm r$ is an irreducible of D, as we desired. □

Example 12. (a) Now consider an integral domain $D := \mathbb{Z}[\sqrt{26}]$ and let $q = 13$. Note that $a^2 \equiv 0, 1, 3, 4, 9, 10, 12 \pmod{13}$ for every integer $a \in \mathbb{Z}$. Hence ± 2 and ± 5 are quadratic nonresidues of 13, i.e., by Theorem 11, ± 2 and ± 5 are irreducibles of D. Moreover, since $N(6 \pm \sqrt{26}) = 2 \cdot 5$, we know that $6 \pm \sqrt{26}$ are also irreducibles of D. So, $(6 + \sqrt{26})(6 - \sqrt{26}) = 10 = 2 \cdot 5$, that is, 10 is factored into two different products of irreducibles of D. Therefore, D is not a UFD but a FD by Lemma 10.

(b) Consider an integral domain $D := \mathbb{Z}[\sqrt{39}]$ and let $q = 13$. Note that, by (a), ± 2 and ± 5 are quadratic nonresidues of 13, i.e., ± 2 and ± 5 are irreducibles of D. Moreover, since $N(7 \pm \sqrt{39}) = 10 = 2 \cdot 5$, we see that $7 \pm \sqrt{39}$ are also irreducibles of D. Therefore, $(7 + \sqrt{39})(7 - \sqrt{39}) = 10 = 2 \cdot 5$, that is, 10 is factored into two different products of irreducibles of D. Therefore, D is not a UFD but a FD by Lemma 10.

References

1. J.B. Fraleigh, *A First Course in Abstract Algebra.* 7th Ed. Addison and Wesley, (2003).
2. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers.* 4th Ed. Oxford:Clarendon Press, (1960).

3. K.H. Rosen, *Elementary Number Theory and Its Application*. 5th Ed. Addison and Wesley, (2005).
4. J.C. Wilson, *A Principal Ideal Ring that is not a Euclidean Ring*, Math. Mag. **46**:34–38, (1973).

Yong Su Shin received his MS and Ph.D at Seoul National University. On 1997, he became an assistant Professor at Sungshin Women's University, where he is a Professor. His research interest is the Hilbert functions of sets of finite points in $\mathbb{P}^n$, Gorenstein and Level algebras, and integral domains.

Department of Mathematics, Sungshin Women's University, Seoul, Korea, 136-742
email: ysshin@sungshin.ac.kr