JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **30**, No. 4, November 2017
http://dx.doi.org/10.14403/jcms.2017.30.4.449

GENERALIZATIONS OF GREATEST COMMON DIVISORS OF GCD DOMAINS

Sang-Cho Chung*

Abstract. In this paper we study several generalizations of greatest common divisor of GCD domain with always the greatest common divisor.

1. Introduction and preliminaries

In the ring of integers, the greatest common divisor (gcd) of two or more integers, which are not all zero, always uniquely exist. But in an integral domain without an order relation, the largest common divisor is not unique.

Throughout this paper, D is an integral domain. Let a and b be elements in D. We say that a *divides* b, and write $a|b$, if there exists an element $c \in D$ such that $b = ac$. A *unit* in D is an element with a multiplicative inverse. The elements a and b in D are *associates* if $a = ub$ for some unit u in D.

Let A be a nonempty subset of D. The element d is a *greatest common divisor* (gcd) of A if $d|a$ for each a in A, and whenever $e|a$ for each a in A, we have $e|d$.

In general, the greatest common divisor is not unique, so we denote the set of all greatest common divisors of A by $\mathrm{GCD}(A)$.

The elements of A are said to be *relatively prime* (or the set A is said to be *relatively prime*) if 1 is a greatest common divisor of A.

The element m is a *least common multiple* (lcm) of A if $a|m$ for each a in A, and whenever $a|e$ for each a in A, we have $m|e$.

In general, the least common multiple is not unique, so we denote the set of all greatest common divisors of A by $\mathrm{LCM}(A)$.

In case $\mathrm{GCD}(\{a,\ b\}) = \mathrm{GCD}(a,\ b)$ and $\mathrm{LCM}(\{a,\ b\}) = \mathrm{LCM}(a,\ b)$

Received September 23, 2017; Accepted Octorber 23, 2017.
2010 Mathematics Subject Classification: Primary 13G05; Secondary 11A05.
Key words and phrases: integral domain, greatest common divisor, least common multiple, GCD-domain.

For non-empty subsets $A,\ B \subset D$, a *set multiplication* AB is a set $AB = \{ab \mid a \in A,\ b \in B\}$.

EXAMPLE 1.1. In the ring of integers $\mathbb{Z}$, the set of all greatest common divisors and the set of all least common multiples of two integers $6,\ 8$ are $\mathrm{GCD}(6,\ 8) = \{2,\ -2\}$ and $\mathrm{LCM}(6,\ 8) = \{24,\ -24\}$

By the ordinary definition of the greatest common divisor and the least common multiple, $\gcd(6,\ 8) = 2$ and $\mathrm{lcm}(6,\ 8) = 24$. Obviously, $\gcd(6,\ 8) \in \mathrm{GCD}(6,\ 8)$ and $\mathrm{lcm}(6,\ 8) \in \mathrm{LCM}(6,\ 8)$.

EXAMPLE 1.2. In an euclidean domain $\mathbb{Z}[i]$, the set of all greatest common divisors and the set of all least common multiples of two elements $1+i,\ 2 \in \mathbb{Z}[i]$ are $\mathrm{GCD}(1+i,\ 2) = \{1+i,\ -1-i,\ -1+i,\ 1-i\}$ and $\mathrm{LCM}(1+i,\ 2) = \{2,\ -2,\ 2i,\ -2i\}$.

An integral domain D is a *GCD-domain* if any two elements admit at least one greatest common divisor.

In general, an integral domain D is not a GCD-domain([3, see Theorem 4] or Theorem 2.1). An integral domain is a UFD(unique factorization domain) if and only if it is a GCD domain satisfying the ascending chain condition on principal ideals [4].

Therefore for finite subsets of a UFD, greatest common divisors and least common multiples always exist [3, see p. 75].

In this paper we study several generalizations of greatest common divisor of GCD domain where the greatest common divisor is always present for both elements.

2. Generalized greatest common divisors

Let's investigate an integral domain that does not have greatest common divisors.

THEOREM 2.1. [3, Theorem 4] *In an integral domain* $\mathbb{Z}[\sqrt{-d}],\ d \geq 3$ *a nonsquare integer, we have the following.*

(1) *In case* $d+1$ *is not a prime number, let* $d+1 = pk$ *where* p *is a prime and* $k \geq 2$. *Then* $1 \in \mathrm{GCD}(p,\ 1+\sqrt{-d})$ *exists but* $\mathrm{GCD}(pk,\ (1+\sqrt{-d})k)$ *does not exist.*
(2) *In case* $d+1$ *is a prime number, let* $d+4 = 2k$ *for some* $k \geq 2$. *Then* $1 \in \mathrm{GCD}(2,\ 2+\sqrt{-d})$ *exists but* $\mathrm{GCD}(2k,\ (2+\sqrt{-d})k)$ *does not exist.*

The following Theorem shows that in a GCD-domain any two elements admit at least one least common multiple.

THEOREM 2.2. [2, Corollary 43] *For an integral domain D, The followings are equivalent.*

(1) *Any two elements of D have a greatest common divisor.*
(2) *Any two elements of D have a least common multiple.*

THEOREM 2.3. [2, refer to Lemma 33] *Let D be an integral domain. For $a,\ b \in D$, assume that there exist $d \in \mathrm{GCD}(a,\ b)$ and $m \in \mathrm{LCM}(a,\ b)$. Then we have the following.*

(1) *$d' \in \mathrm{GCD}(a,\ b)$ if and only if d and d' are associates.*
(2) *$m' \in \mathrm{LCM}(a,\ b)$ if and only if m and m' are associates.*
(3) *$1 \in \mathrm{GCD}(a,\ b)$ if and only if $\mathrm{GCD}(a,\ b) = \{u \mid u \text{ is a unit in } D\}$.*
(4) *$1 \in \mathrm{LCM}(a,\ b)$ if and only if a and b are units in D.*

In special, the cardinality of element of $\mathrm{GCD}(a,\ b)$ and that of element of $\mathrm{LCM}(a,\ b)$ are the same. That is, the cardinality is of the set of all units.

Proof. (1) ($\Rightarrow$) Since d and d' are elements of $\mathrm{GCD}(a,\ b)$, by the definition of the greatest common divisor, $d|d'$ and $d'|d$. Therefore there exist $x,\ x' \in D$ such that $d = d'x'$ and $d' = dx$.

At first if $d = 0$, then $d' = 0$ and hence $0 = d = d' = d'1$. Therefore d and d' are associative elements.

Next if $d \neq 0$, then since D is an integral domain,

$$d = (dx)x' = d(xx') \quad \Longrightarrow \quad 1 = xx' \quad \Longrightarrow \quad x \text{ and } x' \text{ are units.}$$

Therefore d and d' are associative elements.

($\Leftarrow$) Let d and d' be associative elements. Then there exists a unit $u \in D$ such that

$$d = ud'.$$

Since $d|a$ and $d|b$, we have

$$d|a,\ d|b \quad \Longrightarrow \quad ud'|a,\ ud'|b \quad \Longrightarrow \quad d'|a,\ d'|b.$$

Next if $e|a,\ e|b$, then for some $x \in D$

$$e|d \implies d = ex \implies ud' = ex \implies d' = e(xu^{-1}) \implies e|d'.$$

Hence $d' \in \mathrm{GCD}(a,\ b)$.

(2) From the similar method as above in (1), we can get the conclusion.

(3) It follows from (1).

(4) It follows from (2). □

THEOREM 2.4. *Let D be a GCD-domain. Then for $x,\ y,\ x',\ y'$ in D, we have the followings.*

(1) *If* $\mathrm{GCD}(x,\ y) \cap \mathrm{GCD}(x',\ y') \neq \emptyset$, *then* $\mathrm{GCD}(x,\ y) = \mathrm{GCD}(x',\ y')$.
(2) *If* $\mathrm{LCM}(x,\ y) \cap \mathrm{LCM}(x',\ y') \neq \emptyset$, *then* $\mathrm{LCM}(x,\ y) = \mathrm{LCM}(x',\ y')$.

Proof. (1) Take an element $a \in \mathrm{GCD}(x,\ y) \cap \mathrm{GCD}(x',\ y')$. Then there are elements $a_x,\ a_y,\ a_{x'},\ a_{y'} \in D$ such that

$$x = aa_x,\ y = aa_y,\ x' = aa_{x'},\ y' = aa_{y'}.$$

($\subset$) For all $b \in \mathrm{GCD}(x,\ y)$, since $a \in \mathrm{GCD}(x,\ y)$, by Theorem 2.3 there is a unit $u \in D$ such that

$$a = bu.$$

Then

$$x' = aa_{x'} = (bu)a_{x'} \quad \text{and} \quad y' = aa_{y'} = (bu)a_{y'}.$$

Therefore

$$b|x' \quad \text{and} \quad b|y'.$$

Next assume that $e|x'$ and $e|y'$ for some element $e \in D$. Since $a \in \mathrm{GCD}(x',\ y')$, we have $e|a$. Hence $a = ee'$ for some $e' \in D$. Therefore $bu = a = ee'$, and then

$$b = e(e'u^{-1}).$$

That is $e|b$, and $b \in \mathrm{GCD}(x',\ y')$. Hence

$$\mathrm{GCD}(x,\ y) \subset \mathrm{GCD}(x',\ y').$$

($\supset$) Using the similar method as above,

$$\mathrm{GCD}(x',\ y') \subset \mathrm{GCD}(x,\ y).$$

Thus we have $\mathrm{GCD}(x',\ y') = \mathrm{GCD}(x,\ y)$.

(2) From the similar method as above in (1), we can get the conclusion. □

THEOREM 2.5. [2, Proposition 39 and Proposition 44] *Let D be an integral domain. Then for $a,\ b \in D$, we have the followings.*

(1) *If there exists an element $m \in \mathrm{LCM}(a,\ b)$, then $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$.*
(2) *Moreover, if D is a PID(principal ideal domain), then there exists an element $d \in \mathrm{GCD}(a,\ b)$ such that $d = ax+by$ for some $x,\ y \in D$.*

Proof. (1) Since $m \in \mathrm{LCM}(a,\ b)$, there are $x,\ y \in D$ such that

$$m = ax = by \in \langle a \rangle \cap \langle b \rangle\,.$$

Hence $\langle m \rangle \subset \langle a \rangle \cap \langle b \rangle$.

On the other hands, since for all $c \in \langle a \rangle \cap \langle b \rangle$, $a|c$ and $b|c$, we have $m|c$. Therefore $c \in \langle m \rangle$. That is $\langle m \rangle = \langle a \rangle \cap \langle b \rangle$.

(2) Let $\langle a,\ b\rangle = \{ax + by \mid x,\ y \in D\}$. Then since D is PID, there exists an element $d \in D$ such that $\langle a,\ b\rangle = \langle d\rangle$. Therefore

$$d \in \langle d\rangle = \langle a,\ b\rangle\,.$$

Hence there exist elements $x,\ y \in D$ such that

$$d = ax + by.$$

On the other hands, since $a,\ b \in \langle a,\ b\rangle = \langle d\rangle$,

$$d|a, \quad d|b.$$

Furthermore, if $e|a,\ e|b$, then since $d = ax + by$, we have $e|d$. Therefore $d \in \mathrm{GCD}(a,\ b)$. □

Corollary 2.6. *Let D be an integral domain and $a,\ b \in D$. Suppose that* $\mathrm{GCD}(a,\ b)$ *is a non-emptyset. Then we have the following.*

(1) *If there are $x,\ y \in D$ such that $ax + by = 1$, then a and b are relatively prime.*
(2) *Moreover, D is a PID and $a,\ b$ are relatively prime, then $ax+by = 1$ for some $x,\ y \in D$.*

Proof. (1) Suppose that there are $x,\ y \in D$ such that $ax + by = 1$. Let $d \in \mathrm{GCD}(a,\ b)$. Then $d|a$ and $d|b$, and $d|ax + by = 1$. Therefore $d|1$, that is, d is a unit. Hence a and b are relatively prime.

(2) If a and b are relatively prime, then since $1 \in \mathrm{GCD}(a,\ b)$, by Theorem 2.5 there are elements $x,\ y \in D$ such that $ax + by = 1$. □

Theorem 2.7. [3, Theorem 2] *or* [2, Proposition 40] *Let D be a GCD-domain. Then for $a,\ b \in D$, we have the followings.*

(1) *There exist $d \in \mathrm{GCD}(a,\ b)$, $m \in \mathrm{LCM}(a,\ b)$ such that*

$$ab = dm \in \mathrm{GCD}(a,\ b) \cdot \mathrm{LCM}(a,\ b).$$

In particular, for all $d' \in \mathrm{GCD}(a,\ b)$, $m' \in \mathrm{LCM}(a,\ b)$, ab and $d'm'$ are associates.

(2) *If $1 \in \mathrm{GCD}(a,\ b)$, then $ab \in \mathrm{LCM}\,(a,\ b)$.*

Proof. (1) By Theorem 2.2, there is a least common multiple $m \in \mathrm{LCM}(a,\ b)$ of a and b. Let $d = ab/m$. Then

$$a = \frac{ab}{m} \cdot \frac{m}{b} = d \cdot \frac{m}{b} \text{ and } b = \frac{ab}{m} \cdot \frac{m}{a} = d \cdot \frac{m}{a}.$$

Hence $d|a$ and $d|b$. Next suppose that $e|a$ and $e|b$. Then

$$a\left|\frac{ab}{e} \text{ and } b\right|\frac{ab}{e}.$$

Hence $m|\frac{ab}{e}$. Therefore $e|\frac{ab}{m} = d$. Thus $d \in \mathrm{GCD}(a,\ b)$. Then $ab = dm \in \mathrm{GCD}(a,\ b) \cdot \mathrm{LCM}(a,\ b)$.

Since $d,\ d'$ are associates and so are $m,\ m'$ by Theorem 2.3, obviously $ab = dm$ and $d'm'$ are associates.

(2) Since $1 \in \mathrm{GCD}(a,\ b)$, by (1) we can get the following; $ab \in \mathrm{GCD}\,(a,\ b) \cdot \mathrm{LCM}\,(a,\ b) = \mathrm{LCM}\,(a,\ b)$. □

Theorem 2.8. [2, Proposition 34] *Let D be a GCD-domain. Then for $a,\ b,\ c \in D$ and $d \in \mathrm{GCD}(a,\ b)$, we have the followings.*

(1) $\mathrm{GCD}(ab,\ ac) = a\mathrm{GCD}(b,\ c)$.
(2) *If $d \neq 0$, then $1 \in \mathrm{GCD}\left(\frac{a}{d},\ \frac{b}{d}\right)$. This means that $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.*
(3) $1 \in \mathrm{GCD}(a,\ b) \cap \mathrm{GCD}(a,\ c)$ *if and only if* $1 \in \mathrm{GCD}(a,\ bc)$.

Proof. (1) Let $x \in \mathrm{GCD}(ab,\ ac)$. Then $a|ab$ and $a|ac$, so $a|x$. That is, there is $y \in D$ such that $ay = x$. Since $x|ab$ and $x|ac$, we have

$$y|b \text{ and } y|c.$$

Next if $z|b$ and $z|c$, then $az|ab$ and $az|ac$, so $az|x = ay$ and $z|y$. Therefore $y \in \mathrm{GCD}(b,\ c)$, and hence

$$ay = x \in \mathrm{GCD}(ab,\ ac) \cap a\mathrm{GCD}(b,\ c).$$

Then $\mathrm{GCD}(ab,\ ac) = a\mathrm{GCD}(b,\ c)$ by Theorem 2.4 (1).

(2) It follows immediately by (1).

(3) ($\Rightarrow$) Suppose $1 \in \mathrm{GCD}(a,\ b) \cap \mathrm{GCD}(a,\ c)$, and let $d \in \mathrm{GCD}(a,\ bc)$. Then $d|a$ and $d|bc$, so $d|ab$ and $d|bc$.

On the other hands, by (1)

$$b = b \cdot 1 \in b\mathrm{GCD}(a,\ c) = \mathrm{GCD}(ab,\ bc).$$

Hence we have $d|b$. Since $1 \in \mathrm{GCD}(a,\ b)$, we have $d|1$. Then d is a unit, and by Theorem 2.3 we have $1 \in \mathrm{GCD}(a,\ bc)$.

($\Leftarrow$) Let $d \in \mathrm{GCD}(a,\ c)$. Then $d|a,\ d|c$. Therefore $d|ab$. Hence $d|1$. That is, by Theorem 2.3 d is a unit, and $1 \in \mathrm{GCD}(a,\ c)$.

Similarly, we have $1 \in \mathrm{GCD}(b,\ c)$. □

Theorem 2.9. *Let D be a GCD-domain. Then for $a,\ b,\ c \in D$, we have the followings.*

(1) $\mathrm{LCM}(ab,\ ac) = a\mathrm{LCM}(b,\ c)$.
(2) $1 \in \mathrm{LCM}(a,\ b) \cap \mathrm{LCM}(a,\ c)$ *if and only if* $1 \in \mathrm{LCM}(a,\ bc)$.

Proof. By Theorem 2.2, for all $x,\ y \in D$, $\mathrm{LCM}(x,\ y)$ always exists.

(1) Let $m \in \mathrm{LCM}(ab,\ ac)$. Then $a|ab$ and $a|ac$ so $a|m$. That is, there is $y \in D$ such that $ay = m$. Since $ab|m$ and $ac|m$, we have

$$b|y \text{ and } c|y.$$

Next if $b|z$ and $c|z$, then $ab|az$ and $ac|az$, so $ay = m|az$ and $y|z$. Therefore $y \in \mathrm{LCM}(b,\ c)$, and hence

$$ay = m \in \mathrm{LCM}(ab,\ ac) \cap a\mathrm{LCM}(b,\ c).$$

Then $\mathrm{LCM}(ab,\ ac) = a\mathrm{LCM}(b,\ c)$ by Theorem 2.4 (2).

(2) Since $a,\ b,\ c$ are units, it is clear. □

THEOREM 2.10. *Suppose an integral domain D is a PID. Then for $a,\ b,\ c \in D$, we have the following.*

(1) *If $1 \in \mathrm{GCD}(a,\ b)$, $a|bc$, then $a|c$.*
(2) *If $1 \in \mathrm{GCD}(a,\ b)$, $a|c,\ b|c$, then $ab|c$.*

Proof. (1) Suppose that $1 \in \mathrm{GCD}(a,\ b)$. Then by Corollary 2.6 (2), there are $x,\ y \in D$ such that

$$ax + by = 1.$$

Thus $acx + bcy = c$. Since $a|bc$, there is an element $a' \in D$ such that $bc = aa'$ Hence

$$c = acx + bcy = acx + (aa')y = a(cx + a'y).$$

Therefore $a|c$.

(2) Suppose that $1 \in \mathrm{GCD}(a,\ b)$. Then by Corollary 2.6(2), there are $x,\ y \in D$ such that

$$ax + by = 1 \text{ and } acx + bcy = c.$$

Since $a|c$ and $b|c$, there are $a',\ b' \in D$ such that $c = aa'$ and $c = bb'$ Thus

$$c = a(bb')x + b(aa')y = ab(b'x + a'y).$$

Therefore $ab|c$. □

DEFINITION 2.11. Let D be a GCD domain D and $a,\ b \in D$. We define a *relation* R on D as follows: aRb if there exist elements $x,\ y \in D$ such that $a,\ b \in \mathrm{GCD}(x,\ y)$.

THEOREM 2.12. *Let D be a GCD domain. Then for the relation R on D in the above Definition 2.11, we have the followings.*

(1) *For all $a \in D$, aRa*
(2) *If aRb, then bRa.*
(3) *If aRb and bRc, then aRc.*

That is, the relation R on D is an equivalent relation.

Proof. (1) For all $a \in D$, since $a \in \mathrm{GCD}(a,\ a)$, we have aRa.

(2) Suppose that aRb. Then there are elements $x,\ y \in D$ such that $a,\ b \in \mathrm{GCD}(x,\ y)$. Obviously $b,\ a \in \mathrm{GCD}(x,\ y)$. Hence bRa.

(3) Suppose that aRb and bRc. Then there are elements $x,\ y,\ x',\ y' \in D$ such that $a,\ b \in \mathrm{GCD}(x,\ y)$ and $b,\ c \in \mathrm{GCD}(x',\ y')$.

Since $b \in \mathrm{GCD}(x,\ y) \cap \mathrm{GCD}(x',\ y')$, by Theorem 2.4 $\mathrm{GCD}(x,\ y) = \mathrm{GCD}(x',\ y')$. Thus

$$a,\ c \in \mathrm{GCD}(x,\ y) = \mathrm{GCD}(x',\ y').$$

Hence aRc. □

THEOREM 2.13. *Let D be a GCD domain. Then for non-empty subsets $A,\ B$ of D, we have the following.*

(1) $\mathrm{GCD}(A) \cdot \mathrm{GCD}(B) = \mathrm{GCD}(AB)$.
(2) $\mathrm{GCD}(A) \cdot \mathrm{GCD}(\{1\}) = \mathrm{GCD}(\{1\}) \cdot \mathrm{GCD}(A) = \mathrm{GCD}(A)$.
(3) $1 \in \mathrm{GCD}(A) \cdot \mathrm{GCD}(B)$ *if and only if* $1 \in \mathrm{GCD}(A)$ *and* $1 \in \mathrm{GCD}(B)$.
(4) *The set of all equivalent classes* $D/R = \{\mathrm{GCD}(A) \mid \emptyset \neq A \subset D\}$ *is a commutative monoid under the above set multiple operation* $(\cdot)$ *with an identity* $\mathrm{GCD}(\{1\})$.

Proof. (1) Let $a \in \mathrm{GCD}(A)$, $b \in \mathrm{GCD}(B)$ and $A = aA'$, $B = bB'$ for some $A',\ B' \subset D$. Then $1 \in \mathrm{GCD}(A')$ and $1 \in \mathrm{GCD}(B')$ by Theorem 2.8 (2). Therefore

$$\begin{aligned}\mathrm{GCD}(A) \cdot \mathrm{GCD}(B) &= \mathrm{GCD}(aA') \cdot \mathrm{GCD}(bB') \\ &= a\mathrm{GCD}(A') \cdot b\mathrm{GCD}(B') \text{ by Theorem 2.8 (1)} \\ &= ab\mathrm{GCD}(A'B') \text{ by Theorem 2.8 (3)} \\ &= \mathrm{GCD}(abA'B') = \mathrm{GCD}(AB).\end{aligned}$$

(2) By (1) it is clear.

(3) When $1 \in \mathrm{GCD}(A) \cdot \mathrm{GCD}(B)$, assume that $1 \notin \mathrm{GCD}(A)$ or $1 \notin \mathrm{GCD}(B)$. Say $1 \notin \mathrm{GCD}(A)$. Then if $d \in \mathrm{GCD}(A)$, d is not a unit by Theorem 2.3 (1). Let $A = dA'$. Then

$$\begin{aligned}1 \in \mathrm{GCD}(A) \cdot \mathrm{GCD}(B) &= \mathrm{GCD}(dA') \cdot \mathrm{GCD}(B) \\ &= d\mathrm{GCD}(A') \cdot \mathrm{GCD}(B)\end{aligned}$$

Thus d is a unit. This is a contradiction. Therefore $1 \in \mathrm{GCD}(A)$. Similarly we have $1 \in \mathrm{GCD}(B)$.

The converse is clear.

(4) If it shows that the operation $(\cdot)$ is well-defined, then by (1), (2), the conclusion holds.

Assume that $\mathrm{GCD}(A) = \mathrm{GCD}(A')$ and $\mathrm{GCD}(B) = \mathrm{GCD}(B')$ for non-empty subsets $A,\ A',\ B,\ B' \subset D$. Let $a \in \mathrm{GCD}(A) = \mathrm{GCD}(A')$ and $b \in \mathrm{GCD}(B) = \mathrm{GCD}(B')$. Then by (1)

$$ab \in \mathrm{GCD}(AB) \cap \mathrm{GCD}(A'B').$$

Hence by Theorem 2.4(1)

$$\mathrm{GCD}(AB) = \mathrm{GCD}(A'B').$$

Therefore the operation $(\cdot)$ is well-defined. □

Theorem 2.13(3) shows that the monoid D/R is not a group.

Example 2.14. In the ring of integers $\mathbb{Z}$, for $\mathrm{GCD}(6,\ 8) = \{2,\ -2\}$ and $\mathrm{GCD}(8,\ 12) = \{4,\ -4\}$, we have

$$\mathrm{GCD}(6,\ 8) \cdot \mathrm{GCD}(8,\ 12) = \{2,\ -2\}\{4,\ -4\} = \{8,\ -8\}$$
$$\mathrm{GCD}(48,\ 72,\ 64,\ 96) = \{8,\ -8\}.$$

Hence we have

$$\mathrm{GCD}(6,\ 8) \cdot \mathrm{GCD}(8,\ 12) = \mathrm{GCD}(\{6,\ 8\}\{8,\ 12\}).$$

References

[1] R. B. Ash, *Abstract Algebra: The Basic Graduate Year*, electronic copies, 2000.
[2] P. L. Clark, *Factorization in integral domains*, http://alpha.math.uga.edu/∼pete/factorization2010.pdf, preprint.
[3] D. Khurana, *On GCD and LCM in domains: A Conjecture of Gauss*, Resonance, **8** (2003), 72–79.
[4] https://en.wikipedia.org/wiki/GCD_domain

*
Department of Mathematics Education
Mokwon University
Daejeon 35349, Republic of Korea
E-mail: math888@naver.com