Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 42 (2001), No. 1, 219-233.

Generalized GCD Rings

Majid M. Ali **David J. Smith**

Department of Mathematics, University of Auckland
Private Bag 92019, Auckland, New Zealand
e-mail: majid@math.auckland.ac.nz
e-mail: smith@math.auckland.ac.nz

Abstract. All rings are assumed to be commutative with identity. A generalized GCD ring (G-GCD ring) is a ring (zero-divisors admitted) in which the intersection of every two finitely generated (f.g.) faithful multiplication ideals is a f.g. faithful multiplication ideal. Various properties of G-GCD rings are considered. We generalize some of Jäger's and Lüneburg's results to f.g. faithful multiplication ideals.

MSC 2000: 13A15 (primary), 13F05 (secondary)
Keywords: multiplication ideal, Prüfer domain, greatest common divisor, least common multiple

0. Introduction

Let R be a commutative ring with identity. An ideal I in R is a multiplication ideal if every ideal contained in I is a multiple of I. In this paper we generalize G-GCD domains, introduced by Anderson and Anderson [5] as follows: Let $S(R)$ be the multiplicative semigroup of f.g. faithful multiplication ideals in R. A ring R is a G-GCD ring if $S(R)$ is closed under intersection. Important examples of G-GCD rings are principal ideal rings, Bezout rings, Von Neumann regular rings, arithmetical rings, Prüfer domains and of course G-GCD domains.

Our interest in G-GCD rings results from our attempt to extend Jäger's results [9] to f.g. faithful multiplication ideals and to generalize Lüneburg's results concerning Prüfer domains [11].

In §2 we study the existence of $\gcd(A, B)$ and $\mathrm{lcm}(A, B)$ and their relationships where $A, B \in S(R)$. We prove that the existence of $\mathrm{lcm}(A, B)$ implies that of $\gcd(A, B)$ and $AB = \gcd(A, B)\mathrm{lcm}(A, B)$ [Theorem 2.1]. The converse is not true in general. Ohm type properties are studied and we show that if $\mathrm{lcm}(A, B)$ exists, then $\mathrm{lcm}(A, B)^k = \mathrm{lcm}(A^k, B^k)$ and $\gcd(A, B)^k = \gcd(A^k, B^k)$ for each positive integer k [Theorem 2.6]. However, the existence of $\gcd(A, B)$ does not imply these properties.

In §3, equivalent conditions for G-GCD rings are given [Theorem 3.1]. Following Helmer [8], we define $\Phi_{A,B}$ as the associative lattice of ideals of R which divide A and are relatively prime to B. The lattice $\Phi_{A,B}$ contains a smallest element if R is a ring with unique prime power factorization. We show that $M \in \Phi_{A,B}$ is a smallest element of $\Phi_{A,B}$ if and only if $\Phi_{[A:M],B}$ is trivial [Theorem 3.7]. All rings considered in this paper are commutative with identity. Consult [6], [7], [10] and [13] for the basic concepts used.

1. Preliminaries

Let R be a commutative ring with identity. An ideal I in R is called a *multiplication ideal* if every ideal contained in I is a multiple of I, see [7]. Let I and J be ideals in R. Following [13, p.113], the *conductor* of J into I, $[I : J]$, is the set of all elements $x \in R$ such that $xJ \subseteq I$. In [10], $[I : J]$ is called the *residual* of I by J. The *annihilator* of I is denoted by $\mathrm{ann}(I)$ and equals to $[0 : I]$. I is *faithful* if $\mathrm{ann}(I) = 0$. Suppose that I is a multiplication ideal in R and $J \subseteq I$. There exists an ideal K in R such that $J = KI$. Note that $K \subseteq [J : I]$ and therefore

$$J = KI \subseteq [J : I]I \subseteq J,$$

so that $J = [J : I]I$.

The proofs of the following lemmas can be found in [12], [14] and [2].

Lemma 1.1. *Let R be a ring. Then a multiplication ideal I in R is finitely generated if and only if* $\mathrm{ann}(I) = \mathrm{ann}(J)$ *for some finitely generated ideal J contained in I.*

Lemma 1.2. *Let R be a ring and J an ideal contained in a finitely generated faithful multiplication ideal I. Then*

(i) *J is a multiplication ideal if and only if $[J : I]$ is a multiplication ideal.*

(ii) *J is finitely generated if and only if $[J : I]$ is finitely generated.*

The following lemma shows that finitely generated faithful multiplication ideals are cancellation ideals.

Lemma 1.3. *Let R be a ring and $I \in S(R)$. Then $[IJ : I] = J$ for every ideal J in R. Consequently, for all ideals J and K in R, if $IJ = IK$, then J=K.*

We remark that for a finitely generated ideal I, the following conditions are equaivalent:

(1) I is a faithful multiplication ideal.

(2) I is a locally principal ideal.

(3) I is a cancellation ideal.

According to [13, p. 109] if R is a ring and I, J two ideals in R, we say that I *divides* J, denoted by $I|J$, if there exists an ideal C in R such that $J = IC$. Hence $J \subseteq I$. It is clear now that if I is a multiplication ideal in R then $I|J$ if and only if $J \subseteq I$.

Let I and J be two ideals in R. An ideal G in R is called a *greatest common divisor* of I and J, or $\gcd(I, J)$, if and only if :

(i) $G|I$ and $G|J$,

(ii) If G' is an ideal with $G'|I$ and $G'|J$, then $G'|G$.

Similarly, an ideal K in R is called *a least common multiple of* I and J, or $\mathrm{lcm}(I, J)$, if and only if:

(i) $I|K$ and $J|K$,

(ii) If K' is an ideal with $I|K'$ and $J|K'$ then $K|K'$.

With these definitions gcd and lcm are unique if they exist, but in examples we show that they do not necessarily exist.

The following two lemmas play a main role in our work. The first one shows any divisor of a f.g. faithful multiplication ideal is a f.g. faithful multiplication ideal, while the second one shows that the least common multiple of two f.g. faithful multiplication ideals, if it does exist, is also a f.g. faithful multiplication ideal.

Lemma 1.4. *Let R be a ring and $I \in S(R)$. If G is an ideal in R and $G|I$, then $G \in S(R)$.*

Proof. As $G|I$, we have $I \subseteq G$, and hence $\mathrm{ann}(G) \subseteq \mathrm{ann}(\mathrm{I}) = 0$, i.e. $\mathrm{ann}(G) = 0$. To show that G is multiplication, suppose $H \subseteq G$. Since $G|I$, there exists an ideal K in R with $I = KG$. It follows that $HK \subseteq KG$, and hence $HK \subseteq I$. But I is multiplication. Thus there exists an ideal F in R such that $HK = IF$, and hence $HKG = IFG$. This implies that $HI = FGI$. From Lemma 1.3, we get $H = FG$. Finally, since $I \subseteq G$ and $\mathrm{ann}(G) = 0 = \mathrm{ann}(I)$, we infer from Lemma 1.1, G is f.g.

Lemma 1.5. *Let R be a ring and $I, J \in S(R)$. If $K = \mathrm{lcm}(I, J)$ exists, then $K \in S(R)$.*

Proof. IJ is a multiplication ideal [4, Theorem 2, Corollary 1] and also $\mathrm{ann}(IJ) = 0$. Since IJ is a common multiple of I and J, we have $K|IJ$, and by Lemma 1.4, $K \in S(R)$.

We mention three further lemmas which will be used later. Their proofs are clear.

Lemma 1.6. *Let R be a ring and A,B ideals in R such that $\gcd(A, B)$ exists. Let $C, D \in S(R)$ such that $\gcd(C, D)$ exists. If $A \subseteq C$ and $B \subseteq D$, then*

$$\gcd(A, B) \subseteq \gcd(C, D).$$

If, moreover, $\mathrm{lcm}(A, B)$ and $\mathrm{lcm}(C, D)$ exist, then

$$\mathrm{lcm}(A, B) \subseteq \mathrm{lcm}(C, D).$$

The following lemmas generalize Gauss's Lemma to f.g. faithful multiplication ideals in a ring R.

Lemma 1.7. *Let R be a ring and $A_i (1 \leq i \leq n)$ a finite collection of ideals in $S(R)$ such that* $\gcd(A_1, A_2, \dots, A_n)$ *and* $\gcd(A_1, A_2, \dots, A_{n-1})$ *exist. If* $G = \gcd(A_1, A_2, \dots, A_{n-1})$*, then* $\gcd(A_1, A_2, \dots, A_n) = \gcd(G, A_n)$.

Lemma 1.8. *Let R be a ring and $A_i (1 \leq i \leq n)$ a finite collection of ideals in $S(R)$ such that* $\operatorname{lcm}(A_1, A_2, \dots, A_n)$ *and* $\operatorname{lcm}(A_1, A_2, \dots, A_{n-1})$ *exist. If* $K = \operatorname{lcm}(A_1, A_2, \dots A_{n-1})$*, then*

$$\operatorname{lcm}(A_1, A_2, \dots, A_n) = \operatorname{lcm}(K, A_n).$$

2. gcd and lcm of multiplication ideals

In this section we generalize to ideals some results in a paper by Jäger [9] concerning the greatest common divisor and least common multiple of two elements in an integral domain. Compare the following theorem with [9, Theorem 4].

Theorem 2.1. *Let R be a ring and $A, B \in S(R)$. If* $\operatorname{lcm}(A, B)$ *exists, then so too does* $\gcd(A, B)$ *and in particular*

$$AB = \gcd(A, B)\operatorname{lcm}(A, B).$$

Proof. Let $K = \operatorname{lcm}(A, B)$. Then $K|AB$, and hence there exists an ideal G in R with $AB = KG$. Since $K \in S(R)$ (Lemma 1.5), we infer from Lemma 1.3

$$[AB : K] = [KG : K] = G.$$

We shall prove that $G = \gcd(A, B)$. As $A|K$, there exists an ideal C in R such that $K = AC$. It follows that

$$AB = KG = ACG,$$

and by Lemma 1.3, $B = CG$. Hence $G|B$. Similarly, $G|A$. Assume that G' is an ideal in R such that $G'|A$, $G'|B$. Hence there exist ideals D_1 and D_2 in R such that $A = D_1G'$ and $B = D_2G'$. Therefore $AB = D_1D_2G'^2$. We have from Lemma 1.4 that $G' \in S(R)$ and hence from Lemma 1.3 we get

$$[AB : G'] = [D_1D_2G'^2 : G'] = D_1D_2G'.$$

It follows that

$$[AB : G'] = D_1B = D_2A,$$

and hence $[AB : G']$ is a common multiple of A and B. Therefore $K|[AB : G']$, and hence there exists an ideal M in R such that

$$[AB : G'] = KM.$$

But $AB \subseteq G'$ and G' is a multiplication ideal. Thus $[AB : G']G' = AB$, and hence $AB = KMG'$. It follows that $KG = KMG'$ and from Lemma 1.3 we have $G = MG'$, i.e. $G'|G$, and the proof is complete.

The next result should be compared with [9, Theorem 2].

Theorem 2.2. *Let R be a ring and $A, B, C \in S(R)$. Then*

(i) $\operatorname{lcm}(A, B)$ *exists if and only if* $\operatorname{lcm}(CA, CB)$ *exists, in which case*

$$\operatorname{lcm}(CA, CB) = C\operatorname{lcm}(A, B).$$

(ii) *If* $\gcd(CA, CB)$ *exists, then so too does* $\gcd(A, B)$, *and*

$$\gcd(CA, CB) = C\gcd(A, B).$$

Proof. (i) Suppose that $\operatorname{lcm}(A, B) = K$ exists. Then $A|K$ and $B|K$ and hence $CA|CK$, $CB|CK$. Let V be an ideal in R such that $CA|V$, $CB|V$. There exist ideals D_1 and D_2 in R such that

$$V = CAD_1 = CBD_2.$$

It follows from Lemma 1.3 that

$$[V : C] = AD_1 = BD_2,$$

and hence $[V : C]$ is a common multiple of A and B. Thus $K|[V : C]$ and hence $CK|[V : C]C$. Since $CA|V$, we have $V \subseteq C$ and $[V : C]C = V$. This implies that $CK|V$ and $CK = \operatorname{lcm}(CA, CB)$.

Conversely, suppose that $\operatorname{lcm}(CA, CB) = L$ exists. Then $CA|L$, $CB|L$ and hence there exist ideals D_1 and D_2 in R such that

$$L = CAD_1 = CBD_2.$$

By Lemma 1.3,

$$[L : C] = AD_1 = BD_2,$$

and hence $[L : C]$ is a common multiple of A and B. Assume that L' is an ideal in R such that $A|L'$, $B|L'$. Then $CA|CL'$, $CB|CL'$ and therefore $L|CL'$. There exists an ideal I in R such that $CL' = IL$ and from Lemma 1.3 we infer that $L' = [IL : C]$. We observe that

$$[IL : C] = I[L : C].$$

In fact, let $x \in [IL : C]$. Then $xC \subseteq IL$, and hence $xCAD_1 \subseteq ILAD_1$. But $L = CAD_1$ and $L \in S(R)$. Thus, by Lemma 1.3, $x \in IAD_1 = I[L : C]$. The other inclusion is obvious. It follows that

$$[L : C] = \operatorname{lcm}(A, B).$$

Since C is a multiplication ideal and $L \subseteq C$, $L = [L : C]C$ and we have shown that

$$\operatorname{lcm}(CA, CB) = C\operatorname{lcm}(A, B).$$

(ii) Let $G = \gcd(CA, CB)$. Then $CA, CB \subseteq G$ and from Lemma 1.3, $A, B \subseteq [G : C]$. Since $C|CA$ and $C|CB$, we get $C|G$ and hence $G \subseteq C$. But $G \in S(R)$ (Lemma 1.4). Therefore, from Lemma 1.2, we infer that $[G : C] \in S(R)$ and hence $[G : C]$ is a common divisor of A and B. Suppose that D is an ideal in R such that $D|A$, $D|B$. Then $CD|CA$, $CD|CB$ and therefore $CD|G$. It follows that $G \subseteq CD$ and from Lemma 1.3, we have $[G : C] \subseteq [CD : C] = D$.

Finally, since D is a multiplication ideal (Lemma 1.4), we get $D|[G:C]$, and we conclude that $[G:C]=\gcd(A,B)$. Moreover

$$\gcd(CA,CB)=G=[G:C]C=C\gcd(A,B),$$

and this finishes the proof of the theorem.

The converses of Theorems 2.1 and 2.2 (ii) are not true. let $R=k[X^2,X^3]$, k a field. Then $\gcd(X^2R,X^3R)=R$ but $\operatorname{lcm}(X^2R,X^3R)$ does not exist. Also it is easily seen that $\gcd(X^5R,X^6R)$ does not exist.

Compare the following generalization of Euclid's Lemma with [9, Theorem 7].

Proposition 2.3. *Let R be a ring and $A,B,C\in S(R)$ such that $\gcd(BA,BC)$ exists and $\gcd(A,C)=R$. Then*

$$\gcd(A,BC)=\gcd(A,B).$$

Proof. As $\gcd(BA,BC)$ exists, we infer from Theorem 2.2 that

$$\gcd(BA,BC)=B\gcd(A,C)=B.$$

It follows from Lemma 1.7 that

$$\begin{aligned}\gcd(A,B)&=\gcd(A,\gcd(BA,BC))\\&=\gcd(\gcd(A,BA),BC)\\&=\gcd(A,BC).\end{aligned}$$

We now prove that with an additional condition, the converse of Theorem 2.1 is true. Compare with [9, Theorem 5]. First we prove a lemma.

Lemma 2.4. *Let R be a ring and $A,B\in S(R)$. If $G=\gcd(A,B)$ then*

$$\gcd([A:G],[B:G])=R.$$

Proof. As $A,B\subseteq G$ and G is a multiplication ideal, we have $A=[A:G]G$, $B=[B:G]G$, and hence by Theorem 2.2 (ii),

$$G=\gcd([A:G]G,[B:G]G)=G\ \gcd([A:G],[B:G]).$$

From Lemma 1.3, we conclude

$$\gcd([A:G],[B:G])=R.$$

Theorem 2.5. *For any ring R, $\gcd(A,B)$ exists for all $A,B\in S(R)$ if and only if $\operatorname{lcm}(A,B)$ exists for all $A,B\in S(R)$.*

Proof. Let $A, B \in S(R)$. By Theorem 2.2 (i) we may assume

$$\gcd(A, B) = R.$$

(In fact, if $\gcd(A, B) = D$, then $A = [A : D]D$, $B = [B : D]D$ and $\mathrm{lcm}(A, B)$ exists if and only if $\mathrm{lcm}([A : D], [B : D])$ exists, and $\gcd([A : D], [B : D]) = R$ by Lemma 2.4). We show that $\mathrm{lcm}(A, B) = AB$. Clearly AB is a common multiple of A and B. If V is any common multiple of A and B, say $V = AM = BN$, then $A|BN$ so by Proposition 2.3,

$$A = \gcd(A, BN) = \gcd(A, N),$$

and hence $A|N$, so that $AB|V$ (recall that $BN = V$). The converse follows from Theorem 2.1.

Let R be a ring and $A, B \in S(R)$. Then it is easily verified that $\mathrm{lcm}(A, B)$ exists in $S(R)$ if and only if $A \cap B \in S(R)$ and in this case $\mathrm{lcm}(A, B) = A \cap B$. If $\mathrm{lcm}(A, B)$ exists, it follows from Theorem 2.1 that $\gcd(A, B)$ exists and is $[AB : (A \cap B)]$. If A, B and $A + B \in S(R)$, then $A \cap B \in S(R)$, hence

$$\gcd(A, B) = [AB : (A \cap B)] = [AB : A] + [AB : B] = B + A.$$

As $\mathrm{lcm}(X^2R, X^3R)$ in $R = k[X^2, X^3]$ does not exist, we conclude that $X^2R \cap X^3R$ is not a multiplication ideal. Also, it is shown in [15] that $2\mathbb{Z}[\sqrt{5}] \cap (-1 + \sqrt{5})\mathbb{Z}[\sqrt{5}]$ is not a multiplication ideal in $\mathbb{Z}[\sqrt{5}]$, so $\mathrm{lcm}(2\mathbb{Z}[\sqrt{5}], (-1 + \sqrt{5})\mathbb{Z}[\sqrt{5}]$ does not exist.

It is also useful to remark that if R is a ring and $A, B \in S(R)$ have a lcm, then

$$\mathrm{lcm}(A, B) = A \cap B = [A : B]B,$$

and hence

$$[\mathrm{lcm}(A, B) : B] = [A : B].$$

But Theorem 2.1 says that $\gcd(A, B)$ exists and

$$AB = \gcd(A, B)\mathrm{lcm}(A, B).$$

It follows that

$$[A : \gcd(A, B)] = [A : B] = [\mathrm{lcm}(A, B) : B],$$

and hence by Lemma 2.4, $\gcd([A : B], [B : A]) = R$.

Compare the following theorem with [1, Propositions 2.1 and 3.1].

Theorem 2.6. *Let R be a ring and $A, B \in S(R)$ such that $\mathrm{lcm}(A, B)$ exists. Then the following statements are true:*

(i) $\mathrm{lcm}(A, B)^k = \mathrm{lcm}(A^k, B^k)$ *for each positive integer k.*
(ii) $\gcd(A, B)^k = \gcd(A^k, B^k)$ *for each positive integer k.*
(iii) $[A : B]^k = [A^k : B^k]$ *for each positive integer k.*

Proof. We shall prove (i) by induction on k. The result is trivial for $k = 1$. Assume that $k \geq 1$ and that

$$\mathrm{lcm}(A, B)^k = \mathrm{lcm}(A^k, B^k).$$

Notice that it follows from Theorem 2.2 (i) and Lemma 1.8 that if $C, D \in S(R)$ such that $\mathrm{lcm}(C, D)$ exists, then

$$\mathrm{lcm}(A, B)\mathrm{lcm}(C, D) = \mathrm{lcm}(AC, AD, BC, BD).$$

Hence

$$\mathrm{lcm}(A^k, B^k) = \mathrm{lcm}(A, B)^k = \mathrm{lcm}(A^k, A^{k-1}B, \ldots, B^k).$$

It follows that

$$\mathrm{lcm}(A^k, B^k) \subseteq A^{k-1}B, AB^{k-1}.$$

Now, by Theorem 2.2 and Lemma 1.8,

$$\begin{aligned}
\mathrm{lcm}(A, B)^{k+1} &= \mathrm{lcm}(A, B)^k \mathrm{lcm}(A, B) \\
&= \mathrm{lcm}(A^k, B^k)\mathrm{lcm}(A, B) \\
&= \mathrm{lcm}(\mathrm{lcm}(A^{k+1}, B^{k+1}), A^k B, AB^k)).
\end{aligned}$$

It is enough to show that

$$\mathrm{lcm}(A^{k+1}, B^{k+1}) \subseteq A^k B, AB^k.$$

From Theorem 2.1, Lemma 1.6, Theorem 2.2 (i) and Lemma 1.8, we have

$$\begin{aligned}
A^k B &= A^{k-1}AB \\
&= A^{k-1}\mathrm{lcm}(A, B)\,\mathrm{gcd}(A, B) \\
&= A^{k-1}\mathrm{lcm}(A\,\mathrm{gcd}(A, B), B\,\mathrm{gcd}(A, B)) \\
&\supseteq A^{k-1}\mathrm{lcm}(A^2, B\,\mathrm{gcd}(A, B)) \\
&= \mathrm{lcm}(A^{k+1}, A^{k-1}B\,\mathrm{gcd}(A, B)) \\
&\supseteq \mathrm{lcm}(A^{k+1}, \mathrm{lcm}(A^k, B^k)\,\mathrm{gcd}(A, B)) \\
&= \mathrm{lcm}(A^{k+1}, \mathrm{lcm}(A^k\,\mathrm{gcd}(A, B), B^k\,\mathrm{gcd}(A, B)) \\
&\supseteq \mathrm{lcm}(A^{k+1}, \mathrm{lcm}(A^{k+1}, B^{k+1})) \\
&= \mathrm{lcm}(A^{k+1}, B^{k+1}).
\end{aligned}$$

Similarly

$$AB^k \supseteq \mathrm{lcm}(A^{k+1}, B^{k+1}),$$

and this finishes the proof of (i). For (ii), we have

$$AB = \mathrm{lcm}(A, B)\,\mathrm{gcd}(A, B),$$

and hence

$$\begin{aligned}
A^k B^k &= \mathrm{lcm}(A, B)^k\,\mathrm{gcd}(A, B)^k \\
&= \mathrm{lcm}(A^k, B^k)\,\mathrm{gcd}(A, B)^k.
\end{aligned}$$

Since $\mathrm{lcm}(A^k, B^k) = \mathrm{lcm}(A, B)^k \in S(R)$, it follows from Lemma 1.3 that

$$[A^k B^k : \mathrm{lcm}(A^k, B^k)] = \gcd(A, B)^k.$$

Finally, from Theorem 2.1, we have

$$[A^k B^k : \mathrm{lcm}(A^k, B^k)] = \gcd(A^k, B^k).$$

Part (ii) of the theorem is thus concluded. For (iii), we have

$$[A : B]^k B^k = \mathrm{lcm}(A, B)^k = \mathrm{lcm}(A^k, B^k) = [A^k : B^k]B^k.$$

But $B^k \in S(R)$, hence by Lemma 1.3 we get the result, and the proof is complete.

It is useful to mention that even if $A, B \in S(R)$ such that $\gcd(A, B)$ exists, the conclusion of Theorem 2.6 (ii) is not always true. For example, again let $R = k[X^2, X^3]$. Then $\gcd(X^2R, X^3R) = R$, and hence $\gcd(X^2R, X^3R)^2 = R$. But

$$\gcd(X^4R, X^6R) = X^4R \neq R.$$

3. Generalized GCD rings

Anderson [3] and [5] introduced and investigated a class of domains called generalized greatest common divisor (G-GCD) domains for which the set of invertible ideals is closed under intersection. These include Prüfer domains, π-domains and of course principal ideal domains. We generalize this as follows: A ring R (zero-divisors admitted) is called a *generalized GCD ring* (*G-GCD ring*) if the intersection of every two f.g. faithful multiplication ideals in R is also a f.g. faithful multiplication ideal. Important examples of G-GCD rings include principal ideal rings, Bezout rings, von Neumann regular rings, arithmetical rings, Prüfer domains and of course G-GCD domains. $Z[\sqrt{5}]$ and $k[X^2, X^3]$ are example of rings which are not G-GCD rings.

The following theorem is now straightforward.

Theorem 3.1. *Let R be a ring and $S(R)$ the multiplicative semigroup of f.g. faithful multiplication ideals. Then the following statements are equivalent:*

(i) *R is a* G-GCD *ring.*

(ii) *For all $A, B \in S(R)$, $\mathrm{lcm}(A, B)$ exists in $S(R)$.*

(iii) *For all $A, B \in S(R)$, $\gcd(A, B)$ exists in $S(R)$.*

(iv) *For all $A, B \in S(R)$, $[A : B] \in S(R)$.*

Theorem 3.1 has two corollaries which we wish to mention. The first generalizes two properties that characterize Prüfer domains. The second is a version of the Chinese Remainder Theorem.

Corollary 3.2. *Let R be a* G-GCD *ring. For all $A, B, C \in S(R)$,*

(i) $[\gcd(A, B) : C] = \gcd([A : C], [B : C])$.

(ii) $[C : \mathrm{lcm}(A, B)] = \gcd([C : A], [C : B])$.

Proof. (i) Let $G = \gcd(A, B)$. By Theorem 3.1, $\gcd([A : C], [B : C])$ exists and $[G : C] \in S(R)$. Also it is obvious that

$$\gcd([A : C], [B : C]) \subseteq [G : C].$$

Using Lemmas 1.6 and 2.4 and Theorem 2.2, we get

$$\begin{aligned} [G : C] &= [G : C] \gcd([A : G], [B : G]) \\ &= \gcd([A : G][G : C], [B : G][G : C]) \\ &\subseteq \gcd([A : C], [B : C]). \end{aligned}$$

For (ii), let $K = \mathrm{lcm}(A, B)$. Again by Theorem 3.1, $\gcd([C : A], [C : B])$ exists and $[C : K] \in S(R)$. Clearly,

$$\gcd([C : A], [C : B]) \subseteq [C : K].$$

On the other hand, we have

$$R = \gcd([A : G], [B : G]) = \gcd([K : A], [K : B])$$

and hence by Lemma 1.6 and Theorem 2.2 we infer that

$$\begin{aligned} [C : K] &= [C : K] \gcd([K : A], [K : B]) \\ &= \gcd([C : K][K : A], [C : K][K : B]) \\ &\subseteq \gcd([C : A], [C : B]). \end{aligned}$$

Corollary 3.3. *Let R be a* G-GCD *ring. For all $A, B, C \in S(R)$,*

(i) $\mathrm{lcm}(\gcd(A, B), C) = \gcd(\mathrm{lcm}(A, C), \mathrm{lcm}(B, C))$.

(ii) $\gcd(\mathrm{lcm}(A, B), C) = \mathrm{lcm}(\gcd(A, C), \gcd(B, C))$.

Proof. (i) By Theorem 3.1 and Corollary 3.2, we have

$$\begin{aligned} \mathrm{lcm}(\gcd(A, B), C) &= \gcd(A, B) \cap C = [\gcd(A, B) : C]C \\ &= C \gcd([A : C], [B : C]) \\ &= \gcd([A : C]C, [B : C]C) \\ &= \gcd(A \cap C, B \cap C) \\ &= \gcd(\mathrm{lcm}(A, C), \mathrm{lcm}(B, C)), \end{aligned}$$

and hence (i) is clear. Now, using (i) twice and by Lemma 1.7 we get

$$\begin{aligned} \mathrm{lcm}(\gcd(A, C), \gcd(B, C)) &= \gcd(\mathrm{lcm}(A, \gcd(B, C)), \mathrm{lcm}(C, \gcd(B, C)) \\ &= \gcd(\mathrm{lcm}(A, \gcd(B, C)), C) \\ &= \gcd(\gcd(\mathrm{lcm}(A, B), \mathrm{lcm}(A, C)), C) \\ &= \gcd(\mathrm{lcm}(A, B), \gcd(\mathrm{lcm}(A, C), C)) \\ &= \gcd(\mathrm{lcm}(A, B), C). \end{aligned}$$

G-GCD rings are a generalization of G-GCD domains and Prüfer domains. We extend methods used by Lüneburg [11] to this more general case. In particular, let R be a G-GCD ring and $A, B \in S(R)$. Define

$$\Phi_{A,B} = \{I \ : \ I \text{ is an ideal of } R, \quad I|A, \quad \gcd(I, B) = R\}.$$

Lüneburg showed that if R is a Dedekind domain then $\Phi_{A,B}$ always has a smallest element, and that if R is a Prüfer domain, an element $M \in \Phi_{A,B}$ is smallest if and only if for all f.g. ideals S of R, if $AM^{-1} \subseteq S$ and $S + B = R$ then $S = R$. Ali [2] has extended some of Lüneburg's results and methods to arithmetical rings.

We note that by Lemma 1.4, $\Phi_{A,B} \subseteq S(R)$ and $\Phi_{A,B}$ is non-empty since $R \in \Phi_{A,B}$.

The following observation will be useful later. It follows easily from Proposition 2.3 and Corollary 3.2.

Lemma 3.4. *Suppose R is a* G-GCD *ring and that $A, B, J \in S(R)$. If* $\gcd(A, J) = \gcd(B, J) = R$, *then*

$$\gcd(\mathrm{lcm}(A, B), J) = R = \gcd(AB, J).$$

Theorem 3.5. *Let R be a* G-GCD *ring and $A, B \in S(R)$. Then $\Phi_{A,B}$ forms a lattice of ideals. Moreover, if $\Phi_{A,B}$ contains a minimal element, then it is unique.*

Proof. Let $X, Y \in \Phi_{A,B}$. Then $X, Y \in S(R)$ and $\gcd(X, Y) = G$ and $\mathrm{lcm}(X, Y) = L$ exist. Cleary $G|A$ and by Lemma 1.7 $\gcd(G, B) = R$, and hence $G \in \Phi_{A,B}$. As $X|A$ and $Y|A$, we infer that $L|A$ and hence, from Corollary 3.2 $\gcd(L, B) = R$. This shows that $L \in \Phi_{A,B}$ and the first assertion follows. Suppose now that M is a minimal element in $\Phi_{A,B}$. Let $X \in \Phi_{A,B}$. Then $\mathrm{lcm}(M, X) \in \Phi_{A,B}$. But $\mathrm{lcm}(M, X) \subseteq M$. It follows that $\mathrm{lcm}(M, X) = M$ and hence $M \subseteq X$. Therefore, M is the smallest element in $\Phi_{A,B}$.

Notice that if the G-GCD ring R has ACC on elements of $S(R)$, then the conditions of Theorem 3.5 are satisfied, and $\Phi_{A,B}$ has a unique minimal element for all $A, B \in S(R)$.

Corollary 3.6. *Let R be a* G-GCD *ring and $X, Y \in \Phi_{A,B}$. Then $[X : Y] \in \Phi_{A,B}$.*

Proof. By Theorem 3.1, $[X : Y]$ is in $S(R)$. As $[X : Y]|X$, the corollary is now clear.

Theorem 3.7. *Let R be a* G-GCD *ring and $A, B \in S(R)$. Then $M \in \Phi_{A,B}$ is smallest if and only if the only ideal dividing $[A : M]$ and relatively prime to B is R.*

Proof. Suppose first that M is the smallest element in $\Phi_{A,B}$. Let S be an ideal in R such that $S|[A : M]$. $[A : M] \in S(R)$ by Theorem 3.1 and hence $S \in S(R)$ by Lemma 1.4. Now as $A = [A : M]M$, we have $MS|A$. Also, we have

$$\gcd(S, B) = R = \gcd(M, B),$$

so by Lemma 3.4, $\gcd(MS, B) = R$, and this implies that $MS \in \Phi_{A,B}$. It follows that $M \subseteq MS \subseteq M$, and hence $M = MS$. By Lemma 1.3, $S = R$. Conversely, let M be an ideal

in R satisfying the condition of the Theorem. Suppose $X \in \Phi_{A,B}$. Then $X|A, M|A$ and hence $\text{lcm}(X, M)|A$. It follows that
$$[\text{lcm}(X, M) : M]|[A : M],$$
and hence $[X : M]|[A : M]$. Furthermore
$$R = \gcd(X, B) \subseteq \gcd([X : M], B) \subseteq R,$$
so that $[X : M] = R$ and hence $M \subseteq X$, and M is the smallest element in $\Phi_{A,B}$.

Theorem 3.8. *Let R be a* G-GCD *ring and $A, B, J \in S(R)$. Then the following are equivalent:*

(i) *$J|A$ and $\gcd(J, B) = R$.*

(ii) *$J|[A : G]$ and $\gcd(J, G) = R$ where $G = \gcd(A, B)$.*

In particular, $\Phi_{A,B} = \Phi_{[A:G],G}$.

Proof. Let (i) be satisfied. Then
$$R = \gcd(J, B) \subseteq \gcd(J, G) \subseteq R.$$
Let $K = \text{lcm}(A, B)$. Then $K \subseteq A \subseteq J$, and hence
$$[A : G] = [K : B] = [K : B] \gcd(J, B) = \gcd(J[K : B], [K : B]B) \subseteq \gcd(J, K) = J.$$
But $J \in S(R)$. Thus $J|[A : G]$ and hence (ii) is satisfied. Conversely, let (ii) be satisfied. Then, obviously, $A \subseteq [A : G] \subseteq J$, and hence $J|A$. From Lemma 1.7 and since $A \subseteq J$, we have
$$R = \gcd(J, G) = \gcd(J, \gcd(A, B)) = \gcd(\gcd(J, A), B) = \gcd(J, B)$$
This proves the theorem.

Let R be a G-GCD ring and $A, B \in S(R)$. Define two sequences of ideals in R recursively as follows: $M_0 = A$, $N_0 = B$, $N_{i+1} = \gcd(M_i, N_i)$ and $M_{i+1} = [M_i : N_{i+1}]$ for all $i \geq 0$. As a consequence of Theorem 3.8, the following are satisfied.

(i) $M_i \subseteq M_{i+1}$, $N_i \subseteq N_{i+1}$ for all $i \geq 0$.

(ii) $M_i, N_i \in S(R)$ for all $i \geq 0$.

(iii) $\Phi_{A,B} = \Phi_{M_i,N_i}$ for all $i \geq 0$.

Theorem 3.9. *Let R be a* G-GCD *ring and $A, B \in S(R)$ with the sequences M_i, N_i as above. The following statements are equivalent:*

(i) *$\cup_{i=i}^{\infty} M_i$ is the smallest element in $\Phi_{A,B}$.*

(ii) *$\cup_{i=1}^{\infty} M_i \in \Phi_{A,B}$.*

(iii) *$\cup_{i=1}^{\infty} M_i \in S(R)$.*

(iv) *$\exists\, n \in N$ with $\cup_{i=1}^{\infty} M_i = M_n$.*

(v) *$\exists\, n \in N$ with $M_n = M_{n+1}$.*

(vi) *$\exists\, n \in N$ with $N_{n+1} = R$.*

Proof. (i)⇒(ii)⇒(iii)⇒(iv)⇒(v) is clear. We show (v)⇒(vi). Let $G_i = \gcd(M_i, N_i)$, $K_i = \operatorname{lcm}(M_i, N_i)$. Then $M_{i+1} = [M_i : G_i] = [K_i : N_i]$ for all $i \geq 0$. If $M_n = M_{n+1}$, then

$$M_n = [M_n : G_n] = [K_n : N_n],$$

and hence

$$M_n N_n = [K_n : N_n] N_n = K_n.$$

But Theorem 2.1 says that $M_n N_n = G_n K_n$, and hence $K_n = K_n G_n$. By Lemma 1.3, $G_n = N_{n+1} = R$. To complete the proof of the corollary, we have to show that (vi)⇒(i). Suppose that $R = N_{n+1} = \gcd(M_n, N_n) = G_n$. Then $M_{n+1} = [M_n : G_n] = [M_n : R] = M_n$. Also $R = N_{n+1} \subseteq N_{n+k}$ and hence $N_{n+k} = R$ for all $k \geq 1$ and hence

$$R = N_{n+k} \subseteq N_{n+k+1} = G_{n+k} \quad \text{for all } k \geq 1.$$

It follows that

$$M_{n+k+1} = [M_{n+k} : G_{n+k}] = [M_{n+k} : R] = M_{n+k}$$

for all $k \geq 1$. Therefore $\cup_{i=1}^{\infty} M_i = M_n$. Finally since $M_n | M_n$ and $\gcd(M_n, N_n) = N_{n+1} = R$, it follows that $M_n \in \Phi_{M_n, N_n}$, and hence from Theorem 3.8, M_n is the smallest element in $\Phi_{A,B}$.

If R is a G-GCD ring which has ACC on elements of $S(R)$, then Theorem 3.9 and the remark before it, give us the possibility of finding M_n which satisfies $M_n = M_{n+1}$, and hence the smallest element of $\Phi_{A,B}$.

We conclude with the following application which should be compared with [11, Theorem 10].

Theorem 3.10. *Let R be a* G-GCD *ring and $A, B \in S(R)$. Let $K = \operatorname{lcm}(A, B)$. Let M_A and M_B be the smallest elements of $\Phi_{A,[K:A]}$ and $\Phi_{B,[K:B]}$ respectively. Then the following statements are satisfied:*

(i) $\operatorname{lcm}(M_A, M_B) = \operatorname{lcm}(A, B)$.

(ii) $\gcd([A : M_A], [B : M_B] \gcd(M_A, M_B)) = R = \gcd([B : M_B], [A : M_A] \gcd(M_A, M_B))$

(iii) $\gcd(M_A, [\operatorname{lcm}(M_A, M_B) : M_A]) = R = \gcd(M_B, [\operatorname{lcm}(M_A, M_B) : M_B])$.

Proof. Let $G = \gcd(A, B)$. We have

$$R = \gcd([K : A], [K : B]) = \gcd([A : G], [B : G]).$$

It follows that

$$\begin{aligned} \gcd([A : M_A], [B : M_B], [A : G], [B : G]) &= \gcd([A : M_A], [B : M_B], \gcd([A : G], [B : G]) \\ &= \gcd([A : M_A], [B : M_B], R) = R. \end{aligned}$$

As $\gcd([A : M_A], [B : M_B], [A : G]) | [A : G]$, we infer from Theorem 3.7 that

$$\gcd([A : M_A], [B : M_B], [A : G]) = R.$$

Also, since $\gcd([A:M_A],[B:M_B])|[B:M_B]$, we have from Theorem 3.7 that

$$\gcd([A:M_A],[B:M_B]) = R.$$

Now, $[B:G]|B$ and $\gcd([A:G],[B:G]) = R$, then $[B:G] \in \Phi_{B,[A:G]} = \Phi_{B,[K:B]}$. But M_B is the smallest element in $\Phi_{B,[K:B]}$. Thus $M_B \subseteq [B:G] = [K:A]$, and hence

$$\operatorname{lcm}(M_A, M_B) \subseteq \operatorname{lcm}(M_A, [K:A]).$$

Also, since $M_A \in \Phi_{A,[K:A]}$, we infer that $R = \gcd(M_A, [K:A])$. It follows from Theorem 2.1 that

$$\operatorname{lcm}(M_A, [K:A]) = M_A[K:A],$$

and hence

$$\operatorname{lcm}(M_A, M_B) \subseteq M_A[K:A].$$

Similarly, $\operatorname{lcm}(M_A, M_B) \subseteq M_B[K:B]$. Since $A \subseteq M_A$ and $B \subseteq M_B$, we have that $A = [A:M_A]M_A$ and $B = [B:M_B]M_B$. It follows that

$$\begin{aligned}
\operatorname{lcm}(M_A, M_B) &= \operatorname{lcm}(M_A, M_B)R \\
&= \operatorname{lcm}(M_A, M_B)\gcd([A:M_A],[B:M_B]) \\
&= \gcd([A:M_A]\operatorname{lcm}(M_A, M_B), [B:M_B]\operatorname{lcm}(M_A, M_B)) \\
&\subseteq \gcd([A:M_A]M_A[K:A], [B:M_B]M_B[K:B]) \\
&= \gcd([K:A]A, [K:B]B) = \gcd(K,K) = K = \operatorname{lcm}(A,B).
\end{aligned}$$

On the other hand $A \subseteq M_A, B \subseteq M_B$ and by Lemma 1.6, $\operatorname{lcm}(A,B) \subseteq \operatorname{lcm}(M_A, M_B)$. This finishes the proof of (i). To prove (ii), as $M_A \in \Phi_{A,[K:A]}$, we have $\gcd(M_A, [K:A]) = R$, and hence $\gcd([A:M_A], M_A, [K:A]) = R$. This implies that $\gcd(\gcd([A:M_A], M_A), [K:A]) = R$. But $\gcd([A:M_A], M_A)|[A:M_A]$ and $[A:M_A]|A$. Thus by Theorem 3.7,

$$\gcd([A:M_A], M_A) = R.$$

It follows that

$$\gcd([A:M_A], \gcd(M_A, M_B)) = R.$$

As noted earlier we have

$$\gcd([A:M_A],[B:M_B]) = R,$$

So by Lemma 3.4,

$$\gcd([A:M_A],[B:M_B]\gcd(M_A, M_B)) = R.$$

Similarly,

$$\gcd([B:M_B],[A:M_A]\gcd(M_A, M_B)) = R.$$

For (iii), we have $M_A \in \Phi_{A,[K:A]}$, and hence $\gcd(M_A, [K:A]) = R$. But $\gcd(M_A, [A:M_A]) = R$. It follows from Lemma 3.4 that $\gcd(M_A, [K:A][A:M_A]) = R$. It is clear that

$$[K:A][A:M_A] \subseteq [K:M_A] = [\operatorname{lcm}(M_A, M_B):M_A].$$

Hence

$$\gcd(M_A, [\mathrm{lcm}(M_A, M_B) : M_A]) = R.$$

Similarly

$$\gcd(M_B, [\mathrm{lcm}(M_A, M_B) : M_B]) = R,$$

and this concludes the proof of the Theorem.

References

[1] Ali, M. M.: *The Ohm Type properties for multiplication ideals.* Beiträge Algebra Geom. **37**(2) (1996), 399–414.

[2] Ali, M. M.: *A generalization of Lüneburg's results to arithmetical rings.* Ricerche di Matematica **44**(1) (1995), 91–108.

[3] Anderson, D. D.: *π-domains, divisiorial ideals and overings.* Glasgow Math J. **19** (1978), 199–203.

[4] Anderson, D. D.: *Some remarks on multiplication ideals.* Math. Japonica **25** (1980), 463–469.

[5] Anderson, D. D.; Anderson, D. F: *Generalized GCD domains.* Comment. Math. Univ. St. Paul. **2** (1979), 215–221.

[6] Fontana, M.; Huckaba, J.; Papick, I.: *Prüfer domains.* Marcel Dekker 1997.

[7] Gilmer, R.: *Multiplicative Ideal Theory.* Queen's, Kingston 1992.

[8] Helmer, O.: *The elementary divisor theorem for certain rings without chain conditions.* Bull. Amer. Math. Soc. **49** (1943), 225–236.

[9] Jäger, J.: *Zur Existenz und Berechnung von ggT und kgV in Integritätsringen und deren Quotientenkörpern.* Math.-phys. Sem. ber. **26** (1979), 230–243.

[10] Larsen, M. D.; McCarthy, P. J.: *Multiplicative theory of ideals.* Academic Press, New York 1971.

[11] Lüneburg, H: *Introno ad una questione aritmetica in un dominio di Prüfer.* Ricerche di Matematica **38** (1989), 249–259.

[12] Low, G. M.; Smith, P. F.: *Multiplication modules and ideals.* Comm. Algebra **18**(12) (1990), 4353–4375.

[13] Ribenboim, P.: *Algebraic Numbers.* Wiley, New York 1972.

[14] Smith, P. F.: *Some remarks on multiplication modules.* Arch. Math. **50** (1988), 223–235.

Received November 15, 1999