Again on gcd's

Grigore Călugăreanu

November 3, 2023

1 Introduction

When discussing the commutative domain $\mathbb{Z}[\sqrt{-5}]$, *all* Ring Theory texts mention that **this is not UFD** (unique factorization domain) because of

$$3 \cdot 2 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

which are two decompositions not associated in divisibility.

Only *some* of these mention that **this is not GCD** (greatest common divisors exit), the customarily example being the pair $(6, 2(1 + i\sqrt{5}))$ which is proved **not** having a gcd (using the so-called "norm" of elements in $\mathbb{Z}[\sqrt{-5}]$: $N(a + bi\sqrt{5}) = a^2 + 5b^2$. See Example 4 below).

Merely *none* of these mention that **the "well-known" property**

$$a \mid bc, \gcd(a, b) = 1 \Longrightarrow a \mid c$$

fails.

Indeed, as above, 3 (or 2) divides $(1 + i\sqrt{5})(1 - i\sqrt{5})$, $\gcd(3, 1 \pm i\sqrt{5}) = 1$ but $3 \nmid 1 \pm i\sqrt{5}$.

However, if a domain is GCD then the above property holds.

Lemma 1 *(i)* $d_1 \mid a, b$ *implies* $d_1 \mid \gcd(a, b)$.

(ii) $r \gcd(a, b) = \gcd(ra, rb)$ *for every* r*, if both* $\gcd' s$ *exist.*

(iii) $a \mid bc, \gcd(a, b) = 1 \Longrightarrow a \mid c$.

Proof. (i) The definition of the gcd.

(ii) Let $d = \gcd(a, b)$ and $d_1 = \gcd(ra, rb)$. Then rd divides both ra and rb. So it divides d_1. Write $d_1 = rds$. ■

Write $a = da_1$, $b = db_1$, and write $ra = d_1x$, $rb = d_1y$. Then $d_1a_1 = rdsa_1 = ras = d_1xs$ and $d_1b_1 = rdsb_1 = rbs = d_1ys$.

So $a_1 = xs$, $b_1 = ys$. Since $\gcd(a_1, b_1) = 1$, $s = 1$. So $d_1 = rd$.

Proof. (iii) In fact, if both $\gcd'$s exist, $\gcd(a, b) = 1$ implies $\gcd(ac, bc) = c \gcd(a, b) = c$. As a is a common divisor of ac and bc, a divides $\gcd(ac, bc)$. That is, a divides c. ■

By cancellation, it is easy to prove a converse for (ii): $\gcd(ar, br) = r$ implies $\gcd(a, b) = 1$.

From [2].

Proposition 2 *Let D be an integral domain and $a, b \in D$. Then the following are equivalent:*

1. a, b have an lcm,

2. for any $r \in D$, ra, rb have a gcd.

Proof. For arbitrary $x, y \in D$, denote $LCM(x, y)$ and $GCD(x, y)$ the sets of all lcm's and all gcd's of x and y, respectively.

1 $\Rightarrow$ **2**. Let $c \in LCM(a, b)$. Then $c = ax = by$, for some $x, y \in D$. For any $r \in D$, since rab is a multiple of a and b, there is a $d \in D$ such that $rab = cd$. We claim that $d \in GCD(ra, rb)$. There are two steps: showing that d is a common divisor of ra and rb, and that any common divisor of ra and rb is a divisor of d.

1. Since $c = ax$, the equation $rab = cd = axd$ reduces to $rb = xd$, so d divides rb. Similarly, $ra = yd$, so d is a common divisor of ra and rb.

2. Next, let t be any common divisor of ra and rb, say $ra = ut$ and $rb = vt$ for some $u, v \in D$. Then $uvt = rav = rbu$, so that $z := av = bu$ is a multiple of both a and b, and hence is a multiple of c, say $z = cw$ for some $w \in D$. Then the equation $axw = cw = z = av$ reduces to $xw = v$. Multiplying both sides by t gives $xwt = vt$. Since $vt = rb = xd$, we have $xd = xwt$, or $d = wt$, so that d is a multiple of t . As a result, $d \in GCD(ra, rb)$.

2 $\Rightarrow$ **1**. Suppose $k \in GCD(a, b)$. Write $ki = a$, $kj = b$ for some $i, j \in D$. Set $l = kij$, so that $ab = kl$. We want to show that $l \in LCM(a, b)$. First, notice that $l = aj = bi$, so that $a \mid l$ and $b \mid l$. Now, suppose $a \mid t$ and $b \mid t$, we want to show that $l \mid t$ as well. Write $t = ax = by$. Then $ta = aby$ and $tb = abx$, so that $ab \mid ta$ and $ab \mid tb$. Since $GCD(ta, tb) \neq \varnothing$, we have $tk \in GCD(ta, tb)$, implying $ab \mid tk$. In other words $tk = abz$ for some $z \in D$. As a result, $tk = abz = klz$, or $t = lz$. In other words, $l \mid t$, as desired. ■

Corollary 3 *Let D be an integral domain. Then D is a lcm domain iff it is a gcd domain.*

Moreover, [Bill Dubuque] (to avoid introducing several new letters, formally fractions are used)

Theorem 4 $\gcd(a, b) = ab/\mathrm{lcm}(a, b)$ *if* $\mathrm{lcm}(a, b)$ *exists.*

Proof. $d \mid a, b \iff a, b \mid \frac{ab}{d} \iff [a, b] \mid \frac{ab}{d} \iff d \mid \frac{ab}{[a,b]}$. ■

Examples. 1) $\gcd(a, b) = 1$ implies $\gcd(ac, bc) = c$, fails.

A counterexample appears already above: $\gcd(3, 1 \pm i\sqrt{5}) = 1$ but $\gcd(2 \cdot 3, 2(1 \pm i\sqrt{5}))$ (not only is not 2 but) **does not exist**.

2) In $\mathbb{Z}[\sqrt{-3}]$ consider $a = 2$, $b = 1 - i\sqrt{3}$. We have $\gcd(a, b) = 1$ but $\gcd(2a, 2b) = \gcd(4, 2 - 2i\sqrt{3})$ doesn't exist, so $l := \mathrm{lcm}(a, b)$ doesn't exist (by the equivalence in the previous section). More explicitly, if the lcm l existed then

$2, b \mid 4, 2b \Rightarrow l \mid 4, 2b \Rightarrow \frac{l}{2} \mid 2, b \Rightarrow \frac{l}{2} = 1 \Rightarrow l = 2 \Rightarrow b \mid 2 \Rightarrow b \mid a$, a contradiction.

3) $\gcd(3, 1 \pm i\sqrt{5}) = 1$.

As $N(3) = 9$, $N(1 \pm i\sqrt{5}) = 6$ if d is a common divisor, then $N(d) \mid \gcd(9,6) = 3$ so $N(d) \in \{1,3\}$. The equation $a^2 + 5b^2 = 3$ has no solution.

4) $\gcd(2 \cdot 3, 2(1 \pm i\sqrt{5}))$ does not exist.

Note that both 2 and $1 \pm i\sqrt{5}$ are divisors of 6. Hence, if $\delta = \gcd(2 \cdot 3, 2(1 \pm i\sqrt{5}))$ exists then $N(2) = 4$ and $N(1 \pm i\sqrt{5}) = 6$ would divide $N(\delta)$. Consequently, $\operatorname{lcm}(4,6) = 12$ would divide $N(\delta)$.

On the other hand, since $\delta \mid 6, 2(1 \pm i\sqrt{5})$ it follows that $N(\delta) \mid 36, 24$ and so $N(\delta) \mid \gcd(36,24) = 12$.

Therefore $N(\delta) = 12$. Finally, δ does not exist as the equation $a^2 + 5b^2 = 12$ has no (integer) solutions.

5) $\gcd(8, 6 + 2i\sqrt{5})$ does not exist

Since $\gcd(4, 3+i\sqrt{5}) = 1$, cancellation by 2 in $8 \cdot (-7) = (6+2i\sqrt{5})(-6+2i\sqrt{5})$ gives $4 \cdot (-7) = (3 + i\sqrt{5})(-6 + 2i\sqrt{5})$.

If the gcd above exists, it should follow that 4 divides $-6 + 2i\sqrt{5}$. Since $N(4) = 16$, $N(-6 + 2i\sqrt{5}) = 56$ we derive $16 \mid 56$, a contradiction.

References

[1] Bill Dubuque https://math.stackexchange.com/questions/235139

[2] C. Woo https://planetmath.org/anintegraldomainislcmiffitisgcd (2013).