planetmath.org

Math for the people, by the people.

an integral domain is lcm iff it is gcd

Canonical name	AnIntegralDomainIsLcmIffItIsGcd
Date of creation	2013-03-22 18:19:38
Last modified on	2013-03-22 18:19:38
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	10
Author	CWoo (3771)
Entry type	Derivation
Classification	msc 13G05

Proposition 1. *Let D be an integral domain. Then D is a lcm domain iff it is a gcd domain.*

This is an immediate consequence of the following

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 $\mathrm{LCM}(x, y)$ and $\mathrm{GCD}(x, y)$ the sets of all lcm's and all gcd's of x and y, respectively.

$(1 \Rightarrow 2)$. Let $c \in \mathrm{LCM}(a, b)$. 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 $d \in \mathrm{GCD}(ra, rb)$. 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 $k \in \mathrm{GCD}(a, b)$. Write $ki = a$, $kj = b$ for some $i, j \in D$. Set $\ell = kij$, so that $ab = k\ell$. We want to show that $\ell \in \mathrm{LCM}(a, b)$. First, notice that $\ell = aj = bi$, so that $a \mid \ell$ and $b \mid \ell$. Now, suppose $a \mid t$ and $b \mid t$, we want to show that $\ell \mid t$ as well. Write $t = ax = by$. Then $ta = aby$ and $tb = abx$, so that $ab \mid ta$ and $ab \mid tb$. Since $\mathrm{GCD}(ta, tb) \neq \varnothing$, we have $tk \in \mathrm{GCD}(ta, tb)$ (see `http://planetmath.org/PropertiesOfAGCDDomain`proof of this here), implying $ab \mid tk$. In other words $tk = abz$ for some $z \in D$. As a result, $tk = abz = k\ell z$, or $t = \ell z$. In other words, $\ell \mid t$, as desired. ∎

Since the first statement is equivalent to D being an lcm domain, and the second statement is equivalent to D being a gcd domain, Proposition 1 follows.

Another way of stating Proposition 1 is the following: let L be the set of equivalence classes on the integral domain D, where $a \sim b$ iff a and b are associates. Partial order L so that $[a] \leq [b]$ iff $ac = b$ for some $c \in D$. Then L is a semilattice (upper or lower) implies that L is a lattice.