A well-known property of $\gcd'$s in GCD rings

Bill Dubuque

October 28, 2023

We first recall some well-known properties of the greatest common divisors ($\gcd'$s) in GCD rings (also called the *basic gcd laws*), other than the associativity and the commutativity

Lemma 1 *1.* $\gcd(a,b) = a$ *iff* $a \mid b$.
2. $r\gcd(a,b) = \gcd(ra,rb)$ *and* $\gcd(a,b)r = \gcd(ar,br)$ *[distributive]*
3. If $\gcd(ab,c) = 1$, *then* $\gcd(a,c) = 1 = \gcd(b,c)$.
4. If $\gcd(a,b) = 1$ *and* $\gcd(a,c) = 1$, *then* $\gcd(a,bc) = 1$.
5. If $\gcd(a,b) = 1$ *and* $a \mid bc$, *then* $a \mid c$.

There are several proofs for the next proposition, using primes in any UFD, or using Bézout equation in any Bézout ring.

However, the most general proof in any GCD ring is provided below.

Proposition 2 *If* $\gcd(a,b) = 1$ *in a GCD ring then* $\gcd(ab,c) = \gcd(a,c) \cdot \gcd(b,c)$.

Proof. By the above basic gcd laws (associative, commutative, distributive), we indeed have

$$\gcd(a,c)\cdot\gcd(b,c) = \gcd(ab,ac,bc,cc) = \gcd(ab,(\underbrace{a,b,}_{\gcd(a,b)=1}c)c) = \gcd(ab,c).$$

■