GCD domains

Wikipedia, PlanetMath

March 12, 2020

A *GCD domain* is an integral domain R with the property that any two elements have a greatest common divisor (GCD); i.e., there is a unique minimal principal ideal containing the ideal generated by two given elements. Equivalently, any two elements of R have a least common multiple (LCM).

A GCD domain generalizes a *unique factorization domain* (UFD) to a non-Noetherian setting in the following sense: an integral domain is a UFD if and only if it is a GCD domain satisfying the ascending chain condition on *principal ideals* (and in particular if it is Noetherian).

GCD domains appear in the following chain of class inclusions:

commutative rings $\supset$ integral domains $\supset$ integrally closed domains $\supset$ GCD domains $\supset$ unique factorization domains $\supset$ principal ideal domains $\supset$ Euclidean domains $\supset$ fields $\supset$ finite fields.

PlanetMath.

Let D be a GCD domain. For any $a \in D$, denote $[a]$ the set of all elements in D that are associates of a, $GCD(a, b)$ the set of all gcd's of elements a and b in D, and any $S \subseteq D$, $mS := \{ms \mid s \in S\}$. Then

Lemma 1 *1.* $GCD(a, b) = [a]$ *iff* $a \mid b$.

2. $mGCD(a, b) = GCD(ma, mb)$.

3. If $GCD(ab, c) = [1]$, *then* $GCD(a, c) = [1]$.

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* $a \mid c$.

Proof. To aid in the proof of these properties, let us denote, for $a \in D$ and $S \subseteq D$, $a \mid S$ to mean that every element of S is divisible by a, and $S \mid a$ to mean that every element in S divides a. We take the following five steps:

1. One direction is obvious from the definition. So now suppose $a \mid b$. Then $a \mid GCD(a,b)$. But by definition, $GCD(a,b) \mid a$, so $[a] = GCD(a,b)$.

2. Pick $d \in GCD(a,b)$ and $x \in GCD(ma,mb)$. We want to show that md and x are associates. By assumption, $d \mid a$ and $d \mid b$, so $md \mid ma$ and $md \mid mb$, which implies that $md \mid x$. Write $x = mn$ for some $n \in D$. Then $mn \mid ma$ and $mn \mid mb$ imply that $n \mid a$ and $n \mid b$, and therefore $n \mid d$ since d is a gcd of a and b. As a result, $mn \mid md$, or $x \mid md$, showing that x and md are associates. As a result, the map $f : mGCD(a,b) \to GCD(ma,mb)$ given by $f(d) = md$ is a bijection.

3. If $d \mid a$ and $d \mid c$, then $d \mid ab$ and $d \mid c$. So $d \mid GCD(ab,c) = [1]$, hence d is a unit and the result follows.

4. Suppose $d \mid a$ and $d \mid bc$. Then $d \mid ab$ and $d \mid bc$ and hence $d \mid GCD(ab,bc) = bGCD(a,c) = [b]$. But $d \mid a$ also, so $d \mid GCD(a,b) = [1]$ and d is a unit.

5. $GCD(a,b) = [1]$ implies $[c] = GCD(ac,bc)$. Now, $a \mid ac$ and by assumption, $a \mid bc$. Therefore, $a \mid GCD(ac,bc) = [c]$. ■

The second property above can be generalized to arbitrary integral domain: let D be an integral domain, $a,b \in D$, with $GCD(a,b) \neq \emptyset \neq GCD(ma,mb)$, then $d \in GCD(a,b)$ iff $md \in GCD(ma,mb)$.

Proposition 2 *Every GCD domain is integrally closed.*

Proof. Let D be a GCD domain. For any $a,b \in D$, let $GCD(a,b)$ be the collection of all gcd's of a and b. For this proof, we need (2) and (5) in the above lemma.

For convenience, let $\gcd(a,b)$ be any one of the representatives in $GCD(a,b)$.

Let K be the field of fraction of D, and $a/b \in K$ ($a,b \in D$ and $b \neq 0$) is a root of a monic polynomial $p(x) \in D[x]$. We may, from property (1) above, assume that $\gcd(a,b) = 1$. Write

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0.$$

So we have

$$0 = (a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_0.$$

Multiply the equation by b^n then rearrange, and we get

$$-a^n = c_{n-1}ba^{n-1} + \cdots + c_0b^n = b(c_{n-1}a^{n-1} + \cdots + c_0b^{n-1}).$$

Therefore, $b \mid a^n$. Since $\gcd(a, b) = 1$, $1 = \gcd(a^n, b) = b$, by repeated applications of property (4), and one application of property (2) above. Therefore b is an associate of 1, hence a unit and we have $a/b \in D$. ■

Recall the following

Definitions. A *Schreier* domain, named after Otto Schreier, is an integrally closed domain where every nonzero element is *primal*; i.e., whenever x divides yz, x can be written as $x = x_1x_2$ so that x_1 divides y and x_2 divides z. An integral domain is said to be *pre-Schreier* if every nonzero element is primal. A GCD domain is an example of a Schreier domain. The term "Schreier domain" was introduced by P. M. Cohn in [1]. The term "pre-Schreier domain" is due to Muhammad Zafrullah (see [2]).

In general, an irreducible element is primal if and only if it is a prime element. Consequently, in a Schreier domain, every irreducible is prime. In particular, an atomic Schreier domain is a unique factorization domain; this generalizes the fact that an atomic GCD domain is a UFD.

Finally

Proposition 3 *Every GCD domain is a Schreier domain.*

Proof. That a GCD domain is *integrally closed* is clear from the previous proposition. We need to show that D is *pre-Schreier*, that is, every non-zero element is primal. Suppose c is non-zero in D, and $c \mid ab$ with $a, b \in D$. Let $r = \gcd(a, c)$ and $rt = a$, $rs = c$. Then $1 = \gcd(s, t)$ by property (2) above. Next, since $c \mid ab$, write $cd = ab$ so that $rsd = rtb$. This implies that $sd = tb$. So $s \mid tb$ together with $\gcd(s, t) = 1$ show that $s \mid b$ by property (5). So we have just shown the existence of $r, s \in D$ with $c = rs$, $r \mid a$ and $s \mid b$. Therefore, c is primal and D is a Schreier domain. ■

References

[1] P. M. Cohn *Bezout rings and their subrings*. Proc. Camb. Phil. Soc. **64** (1968), 251-264.

[2] M. Zafrullah *On a property of pre-Schreier domains*. Comm. Algebra **15** (9) (1987), 1895-1920.