planetmath.org

Math for the people, by the people.

gcd domain

Canonical name	GcdDomain
Date of creation	2013-03-22 14:19:51
Last modified on	2013-03-22 14:19:51
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	26
Author	CWoo (3771)
Entry type	Definition
Classification	msc 13G05
Related topic	GreatestCommonDivisor
Related topic	BezoutDomain
Related topic	DivisibilityInRings
Defines	gcd
Defines	greatest common divisor
Defines	relatively prime
Defines	lcm domain

Throughout this entry, let D be a commutative ring with $1 \neq 0$.

A gcd (greatest common divisor) of two elements $a, b \in D$, is an element $d \in D$ such that:

1. $d \mid a$ and $d \mid b$,
2. if $c \in D$ with $c \mid a$ and $c \mid b$, then $c \mid d$.

For example, 0 is a gcd of 0 and 0 in any D. In fact, if d is a gcd of 0 and 0, then $d \mid 0$. But $0 \mid 0$, so that $0 \mid d$, which means that, for some $x \in D$, $d = 0x = 0$. As a result, 0 is the unique gcd of 0 and 0.

In general, however, a gcd of two elements is not unique. For example, in the ring of integers, 1 and -1 are both gcd's of two relatively prime elements. By definition, any two gcd's of a pair of elements in D are associates of each other. Since the binary relation "being associates" of one anther is an equivalence relation (*not* a congruence relation!), we may define *the* gcd of a and b as the set

$$\operatorname{GCD}(a, b) := \{c \in D \mid c \text{ is a gcd of } a \text{ and } b\},$$

For example, as we have seen, $\operatorname{GCD}(0, 0) = \{0\}$. Also, for any $a \in D$, $\operatorname{GCD}(a, 1) = \operatorname{U}(D)$, the group of units of D.

If there is no confusion, let us denote $\gcd(a, b)$ to be any element of $\operatorname{GCD}(a, b)$.

If $\operatorname{GCD}(a, b)$ contains a unit, then a and b are said to be *relatively prime*. If a is irreducible, then for any $b \in D$, a, b are either relatively prime, or $a \mid b$.

An integral domain D is called a *gcd domain* if any two elements of D, not both zero, have a gcd. In other words, D is a gcd domain if for any $a, b \in D$, $\operatorname{GCD}(a, b) \neq \varnothing$.

Remarks

- A unique factorization domain, or UFD is a gcd domain, but the converse is not true.
- A Bezout domain is always a gcd domain. A gcd domain D is a Bezout domain if $\gcd(a, b) = ra + sb$ for any $a, b \in D$ and some $r, s \in D$.
- In a gcd domain, an irreducible element is a prime element.
- A gcd domain is integrally closed. In fact, it is a Schreier domain.

- Given an integral domain, one can similarly define an lcm of two elements a, b: it is an element c such that $a \mid c$ and $b \mid c$, and if d is an element such that $a \mid d$ and $b \mid d$, then $c \mid d$. Then, a *lcm domain* is an integral domain such that every pair of elements has a lcm. As it turns out, the two notions are equivalent: an integral domain is lcm iff it is gcd.

The following diagram indicates how the different domains are related:

$$\begin{array}{ccccc} \texttt{http://planetmath.org/EuclideanRing}\text{Euclidean domain} & \Longrightarrow & \text{PID} & \Longrightarrow & \text{U} \\ & & \Downarrow & & \\ & & \text{Bezout domain} & \Longrightarrow & \text{gcd c} \end{array}$$

References

[1] D. D. Anderson, *Advances in Commutative Ring Theory: Extensions of Unique Factorization, A Survey*, 3rd Edition, CRC Press (1999)

[2] D. D. Anderson, *Non-Noetherian Commutative Ring Theory: GCD Domains, Gauss' Lemma, and Contents of Polynomials*, Springer (2009)

[3] D. D. Anderson (editor), *Factorizations in Integral Domains*, CRC Press (1997)