GCD Domains

Definition 1. *Let R be a domain, with $a, b \in R$. We say $d \in R$ is a* greatest common divisor *of a and b if*

1. *$d|a$ and $d|b$, and*
2. *If $c \in R$ such that $c|a$ and $c|b$, then $c|d$.*

We denote the set of all greatest common divisors of a and b by $\mathsf{gcd}(a, b)$. We say that a and b are relatively prime *if $1 \in \mathsf{gcd}(a, b)$.*

It is important to note that in a general domain, gcds need not exist, and if they do, they need not be unique.

Proposition 1. *Let R be a domain.*

1. *In fact, given $a, b \in R$, either $\mathsf{gcd}(a, b) = \varnothing$ or $\mathsf{gcd}(a, b)$ is an associate class.*
2. *If $a|b$ then $a \in \mathsf{gcd}(a, b)$.*
3. *$a \in \mathsf{gcd}(a, 0)$ for all $a \in R$.*
4. *If u is a unit, then $1 \in \mathsf{gcd}(u, a)$ for all $a \in R$.*

For example, in $\mathbb{Z}$, $\mathsf{gcd}(4, 6) = \{2, -2\}$.

Proposition 2. *Let R be a domain. Provided all the appropriate gcds exist, we have the following.*

- $\mathsf{gcd}(a, b) = \mathsf{gcd}(b, a)$
- $\mathsf{gcd}(a, \mathsf{gcd}(b, c)) = \mathsf{gcd}(\mathsf{gcd}(a, b), c)$
- $\mathsf{gcd}(ab, ac) = a\mathsf{gcd}(b, c)$
- *(Euclid's Lemma) If a and b are relatively prime and $a|bc$, then $a|c$.*
- *If a and b are relatively prime, then $\mathsf{gcd}(a, bc) = \mathsf{gcd}(a, c)$.*
- *If $d \in \mathsf{gcd}(a, b)$ and we write $a = da'$ and $b = db'$, then $1 \in \mathsf{gcd}(a', b')$.*
- *If $1 \in \mathsf{gcd}(a, b)$ then $\mathsf{gcd}(ab, c) = \mathsf{gcd}(a, c)\mathsf{gcd}(b, c)$.*
- *If a and b are relatively prime and a and c are relatively prime, then a and bc are relatively prime.*

Definition 2. *Let R be a domain. We say that R is a* GCD domain *if any two elements of R have a greatest common divisor.*

Proposition 3. *If R is a GCD domain, then every irreducible element of R is also prime.*

Proof. Let p be irreducible and suppose $p|ab$. Let $d \in \mathsf{gcd}(a, p)$, and write $a = da'$ and $p = dp'$. Since p is irreducible, either d or p' is a unit. If d is a unit, then we have $p|b$ by Euclid's lemma. If p' is a unit, then $p|a$. $\square$

A Domain which is not a GCD domain

Here we outline a proof that $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ is a domain but not a GCD domain.

1. Show that the equation $a^2 + ab + b^2 = 2$ has no solutions in $\mathbb{Z}$.
2. Show that $\mathbb{Z}[\sqrt{-3}]$ is a subring of $\mathcal{O}(\sqrt{-3})$ and thus a domain, and that no element of this subring has norm 2 (using the usual norm on $\mathcal{O}(\sqrt{-3})$).
3. Show that 2 is irreducible in $\mathbb{Z}[\sqrt{-3}]$.
4. Show that 2 divides $(1 + \sqrt{-3})(1 - \sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$, but that 2 does not divide $1 + \sqrt{-3}$ or $1 - \sqrt{-3}$. In particular, 2 is not prime in $\mathbb{Z}[\sqrt{-3}]$.
5. Because $\mathbb{Z}[\sqrt{-3}]$ contains irreducible elements which are not prime, it cannot be a GCD domain.