properties of a gcd domain

Canonical name	PropertiesOfAGcdDomain
Date of creation	2013-03-22 18:18:44
Last modified on	2013-03-22 18:18:44
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	9
Author	CWoo (3771)
Entry type	Result
Classification	msc 13G05

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, $\mathrm{GCD}(a,b)$ 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

1. $\mathrm{GCD}(a,b) = [a]$ iff $a \mid b$.
2. $m\,\mathrm{GCD}(a,b) = \mathrm{GCD}(ma, mb)$.
3. If $\mathrm{GCD}(ab,c) = [1]$, then $\mathrm{GCD}(a,c) = [1]$
4. If $\mathrm{GCD}(a,b) = [1]$ and $\mathrm{GCD}(a,c) = [1]$, then $\mathrm{GCD}(a,bc) = [1]$.
5. If $\mathrm{GCD}(a,b) = [1]$ 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 $S \subseteq D$, $a|S$ to mean that every element of S is divisible by a, and $S|a$ to mean that every element in S divides a. We take the following four steps:

1. One direction is obvious from the definition. So now suppose $a \mid b$. Then $a \mid \mathrm{GCD}(a,b)$. But by definition, $\mathrm{GCD}(a,b) \mid a$, so $[a] = \mathrm{GCD}(a,b)$.
2. Pick $d \in \mathrm{GCD}(a,b)$ and $x \in \mathrm{GCD}(ma,mb)$. 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 $f : m\,\mathrm{GCD}(a,b) \to \mathrm{GCD}(ma,mb)$ 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 $d \mid \mathrm{GCD}(ab,c) = [1]$, 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 $d \mid \mathrm{GCD}(ab,bc) = b\,\mathrm{GCD}(a,c) = [b]$. But $d \mid a$ also, so $d \mid \mathrm{GCD}(a,b) = [1]$ and d is a unit.
5. $\mathrm{GCD}(a,b) = [1]$ implies $[c] = \mathrm{GCD}(ac,bc)$. Now, $a \mid ac$ and by assumption, $a \mid bc$. Therefore, $a \mid \mathrm{GCD}(ac,bc) = [c]$.

$\square$

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