Divisibility

__Definition: Divides__

Let R be an integral domain and $a, b \in R$. To say that a *divides* b, denoted $a \mid b$, means there exists $c \in R$ such that $b = ca$.

__Definition: Associate__

To say that a and b are *associates* means $a \mid b$ and $b \mid a$.

__Theorem__

Let R be a ring and $a, b \in R$ be associates. $\exists\, u \in R^{\times}$ such that $b = ua$ and $a = u^{-1}b$.

Proof

$\exists\, c \in R, b = ca$
$\exists\, d \in R, a = db$
$b = ca = (cd)b$
So $cd = 1$, and thus c and d are units in R
Let $c = u$ and $d = u^{-1}$

$\therefore b = ua$ and $a = u^{-1}b$, where $u \in R^{\times}$.

__Definition: Irreducible__

Let R be an integral domain and $r \in R$. To say that r is *irreducible* in R mean r is non-zero, is not a unit in R, and if $r = ab$ for $a, b \in R$ then either a or b is a unit in R. Such a factorization of p is called *trivial*.

__Definition: Prime__

Let R be an integral domain and $p \in R$. To say that p is *prime* in R means that p is non-zero, p is not a unit in R, and if $p \mid ab$ for $a, b \in R$ then $p \mid a$ or $p \mid b$.

Note that in Z, prime and irreducible are the same thing; however, this is not true in general.

__Theorem__

Let R be an integral domain and $p \in R$:

$$p \text{ prime} \implies p \text{ irreducible}$$

Proof

Assume p is prime in R
Assume $p = ab$ for some $a, b \in R$
$p \mid p$, so $p \mid ab$, and thus $p \mid a$ or $p \mid b$
AWLOG: $p \mid a$

$\exists\, c \in R, a = cp = pc$
$p = ab = pc(b) = p(bc)$
So $bc = 1$ and b is a unit, and thus the factorization of p is trivial

Therefore p is irreducible.

Definition: GCD

Let R be an integral domain and $a, b \in R$. To say that $d \in R$ is a *common divisor* of a and b means $d \mid a$ and $d \mid b$.

To say that d is a *greatest common divisor* (GCD) of a and b, denoted (a, b) or $\gcd(a, b)$, means that d is a divisor of a and b, and every other divisor of a and b also divides d.

Note that GCD is unique up to associates.

Example

$(12, 30) = \pm 6$, but 6 and -6 are associates.