Principle Ideal Domain

Definition: PID

Let R be an integral domain. To say that R is a *principal ideal domain* means that every $I \trianglelefteq R$ is ideal - there exists $a \in R$ such that:

$$I = (a) = aR$$

Example

The following are PIDs:

1). $\mathbb{Z}$

2). $\mathbb{Z}[i]$

3). $\mathbb{Z}[\omega]$

4). $F[x]$ for a field F

The following are not PIDs:

1). $\mathbb{Z}[x]$ because $(2, x)$ is not principal

2). $F[x, y]$ because (x, y) is not principal

3). $\mathbb{Z}[\sqrt{-5}]$ because it contains irreducibles that are not prime

Lemma

Let R be a PID and $a, b \in R$. $(a, b) \in R$ and $\exists\, x, y \in R$ such that:

$$(a, b) = xa + yb$$

In other words, the GCD can be represented as a linear combination of a and b in R.

Proof

Since R is a PID, $(a, b) = (a) + (b)$ should still be principal
So $\exists\, d \in R$ such that $(a, b) = (d)$
$(d) = (a) + (b) \supseteq (a)$, and so $d \mid a$ (to contain is to divide)
Likewise, $d \mid b$
Thus, d is a common divisor of a and b

Assume c is some other common divisor of a and b
$(c) \supseteq (a)$ and $(c) \supseteq (b)$
But (d) is the smallest ideal containing (a, b)

So $(c) \supseteq (a, b) = (d)$ and therefore $c \mid d$.

Moreover, since $(d) = (a) + (b)$, there exists $x, y \in R$ such that $d = xa + yb$.

Theorem

Let R be a PID and $p \in R$:

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

Proof

Assume p is irreducible
Assume $p \mid ab$ for some $a, b \in R$
AWLOG: $p \nmid a$
Since p is irreducible, the only divisors of p are associates of p and 1, and hence the only common divisors of p and a are units, which are associates of 1
In particular, $(p, a) = 1$
So, by the previous lemma, $\exists\, x, y \in R$ such that $1 = ax + py$
$b = bax + bpy = abx + pby$
But $p \mid ab$ and $p \mid pby$, so $p \mid b$

Therefore, p is prime.

Thus, is a PID, prime and irreducible are the same thing.