Principal Ideal Domains

This section of notes roughly follows Sections 8.1-8.2 in Dummit and Foote.

Throughout this whole section, we assume that R is a commutative ring.

Definition 55. Let R b a commutative ring and let $a, b \in R$ with $b \neq 0$.

(1) a is said to be **multiple** of b if there exists an element $x \in R$ with $a = bx$. In this case, b is said to **divide** a or be a **divisor** of a, written $b \mid a$.

(2) A **greatest common divisor** of a and b is a nonzero element d such that
   (a) $d \mid a$ and $d \mid b$, and
   (b) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

   A greatest common divisor of a and b will be denoted $\gcd(a, b)$ (or possibly (a, b)).

Note 56. Note that $b \mid a$ in a ring R iff $a \in (b)$ iff $(a) \subseteq (b)$. In particular, if d is any divisor of both a and b, then (d) must contain both a and b, and hence must contain (a, b). Moreover, if $d = \gcd(a, b)$ iff $(a, b) \subseteq (d)$ and if (d') is any principal ideal containing (a, b), then $(d) \subseteq (d')$.

The note above immediately proves the following result.

Theorem 57. If a and b are nonzero elements in the commutative ring R such that $(a, b) = (d)$, then $d = \gcd(a, b)$.

Note 58. It is important to point out that the theorem above is giving us a sufficient condition, but it is not necessary. For example, $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$ that is not principal. Then $\mathbb{Z}[x] = (1)$ is the unique principal ideal containing both 2 and x, and so $\gcd(2, x) = 1$.

Theorem 59. Let R be an integral domain. If $(d) = (d')$, then $d' = ud$ for some unit $u \in R$. In particular, if $d = \gcd(a, b) = d'$, then $d' = ud$ for some unit $u \in R$.

Proof. Easy exercise. □

Definition 60. A **principal ideal domain** (PID) is an integral domain in which every ideal is principal.

Example 61. Here are some short examples.

(1) $\mathbb{Z}$ is a PID.

(2) $\mathbb{Z}[x]$ is not a PID since $(2, x)$ is not principal.

Theorem 62. Let R be a PID, $a, b \in R \setminus \{0\}$, and $(d) = (a, b)$. Then

(1) $d = \gcd(a, b)$

(2) $d = ax + by$ for some $x, y \in R$

(3) d is unique up to multiplication by a unit of R.

Proof. The result follows from Theorems 57 and 62. $\square$

Theorem 63. Every nonzero prime ideal in a PID is a maximal ideal.

Corollary 64. If R is a commutative ring such that the polynomial ring $R[x]$ is a PID, then R is necessarily a field.

Example 65. Here are a few quick examples.

(1) We already know that $\mathbb{Z}[x]$ is not a PID, but the above corollary tells us again that it isn't since $\mathbb{Z}$ is not a field.

(2) The polynomial ring $\mathbb{Q}[x]$ is an eligible PID and it turns out that it is. In fact, $F[x]$ ends up being a PID for every field F.

(3) The polynomial ring $\mathbb{Q}[x,y]$ turns out not to be a PID. The reason for this is that $\mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$ and $\mathbb{Q}[x]$ is not a field.