1 Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

All rings in this chapter are commutative

1.1 Euclidean Domains

Definition. Any function $N\colon R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a *norm* on the integral domain R. If $N(a) > 0$ for $a \neq 0$ define N to be a *positive norm*.

Definition. The integral domain R is said to be a *Euclidean Domain* (or possess a *Division Algorithm*) if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$ there exist elements q and r in R with

$$a = qb + r \quad \text{with } r = 0 \text{ or } N(r) < N(b).$$

The element q is called the *quotient* and the element r the *remainder* of the division.

Proposition 1. Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R then $I = (d)$, where d is any nonzero element of I of minimal norm.

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

1. a is said to be a *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 $b|a$.

2. A *greatest common divisor* of a and b is a nonzero element d such that

   (a) $d|a$ and $d|b$, and

   (b) if $d'|a$ and $d'|b$ then $d'|d$.

   A greatest common divisor of a and b will be denoted by g.c.d(a, b), or (abusing the notation) simply (a, b)

Note.

1. $b|a$ in R if and only if $a \in (b)$ if and only if $(a) \subseteq (b)$.

2. The above definition of greatest common divisor can be restated in terms of ideals as such. If I is the ideal of R generated by a and b, then d is a greatest common divisor of a and b if

   (a) I is contained in the principal ideal (d), and

   (b) if (d') is any principal ideal containing I then $(d) \subseteq (d')$.

Proposition 2. If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.

Proposition 3. Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$ for some unit u in R. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.

Theorem 4. Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then

1. d is a greatest common divisor of a and b, and

2. the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an R-linear combination of a and b, i.e., there are elements x and y in R such that
$$d = ax + by.$$

1.2 Principal Ideal Domains (P.I.D.s)

Definition. A *Principal Ideal Domain* (P.I.D) is an integral domain in which every ideal is principal.

Note. By Proposition 1 every Euclidean Domain is a Principal Ideal Domain. So every result about P.I.D.s automatically holds for Euclidean Domains.

Proposition 6. Let R be a Principal Ideal Domain and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

1. d is a greatest common divisor of a and b

2. d can be written as an R-linear combination of a and b

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

Proposition 7. Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Corollary 8. If R is any commutative ring such that the ring $R[x]$ is a Principal Ideal Domain (or Euclidean Domain), then R is necessarily a field.

Definition. Define N to be a *Dedekind-Hasse norm* if N is a positive norm and for every nonzero $a, b \in R$ either a is an element of the ideal (b) or there is a nonzero element of the ideal (a, b) of norm strictly smaller then the norm of b (i.e., either b divides a in R or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$).

Proposition 9. The integral domain R is a P.I.D if and only if R has a Dedekind-Hasse norm.

1.3 Unique Factorization Domains (U.F.D.s)

Definition. Let R be an integral domain.

1. Suppose $r \in R$ is nonzero and is not a unit. Then r is called *irreducible* in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise r is said to be *reducible*.

2. The nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated by p is a prime ideal. In other words, a nonzero p is prime if it is not a unit and whenever $p|ab$ for any $a, b \in R$, then either $p|a$ or $p|b$.

3. Two elements a and b of R differing by a unit are said to be *associate* in R (i.e., $a = ub$ for some unit u in R).

Proposition 10. In an integral domain a prime element is always irreducible.

Proposition 11. In a Principal Ideal Domain a nonzero element is a prime if and only if it is irreducible.

Definition. A *Unique Factorization Domain* (U.F.D.) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

1. r can be written as a finite product of irreducibles p_i in R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$ and
2. the decomposition in 1. is unique up to associates: namely if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of factors so that p_i is associate to q_i for $i = 1, 2, \dots, n$.

Proposition 12. In a Unique Factorization Domain a nonzero element is a prime if and only if it is irreducible.

Proposition 13. Let a and b be two nonzero elements of the Unique Factorization Domain R and suppose

$$a = u p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \qquad \text{and} \qquad b = v p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units and the primes $p_1, p_2, \dots, p_n$ are distinct and the exponents e_i and f_i are ≥ 0. Then the element

$$d = p_1^{min(e_1,f_1)} p_2^{min(e_2,f_2)} \cdots p_n^{min(e_n,f_n)}$$

(where $d = 1$ if all exponents are 0) is the greatest common divisor of a and b.

Theorem 14. Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.

Corollary 15. (Fundamental Theorem of Arithmetic) The integers $\mathbb{Z}$ are a Unique Factorization Domain.

Corollary 16. Let R be a P.I.D. Then there exists a multiplicative Dedekind-Hasse norm on R.

Note. We have the following inclusions among classes of commutative rings with identity:

$$fields \subset Euclidean\ Domains \subset P.I.D.s \subset U.F.D.s \subset integral\ domains$$

with all containments being proper.