Contents

Last update: 2024 August 20

1 Euclidean Domains, PIDs, UFDs

1.1 Euclidean Domains

Definition 1.1.1. Let R be an integral domain. Any function $N : R \to \mathbf{Z}^+ \cup \{0\}$ 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 1.1.2. 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 is called the *remainder* of the division.

Example 1.1.1 (Euclidean Algorithm)**.** Let a and b be any two elements of the Euclidean domain R. By successive "divisions" (these actually are divisions in the field of fractions of R) we can write

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where r_n is the last nonzero remainder. Such an r_n exists since $N(b) > N(r_0) > N(r_1) > ... > N(r_n)$ is a decreasing sequence of nonnegative integers if the remainders are nonzero, and such a sequence cannot continue indefinitely. Note also that there is no guarentee that these elements are unique.

Example 1.1.2.

(1) Fields are trivial examples of Euclidean Domains where any norm will satisfy the defining condition (e.g., $N(a) = 0$ for all a). This is because for every a, b with $b \neq 0$ we have $a = qb + 0$, where $q = ab^{-1}$.

(2) The integers $\mathbf{Z}$ are a Euclidean Domain with norm given by $N(a) = |a|$, the usual absolute value.

(3) If F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain with norm given by $N(p(x)) = \deg p(x)$. The Division Algorithm for polynomials is simply "long division" of polynomials. The proof is very similar to that for $\mathbf{Z}$ and is given in the next chapter. We will prove in Section **??** that $R[x]$ is not a Euclidean Domain if R is not a field.

Proposition 1.1.1. *Every ideal in a Euclidean Domain is principle. 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 minimum norm.*

Proof. If I is the zero ideal there is nothing to prove. Otherwise let $d \in I$ be any nonzero element of minimum norm (such a d exists since the set $\{N(a) \mid a \in I\}$ has a minimum element by the well-ordering of **Z**). Clearly $(d) \subseteq I$ since d is an element of I. To show the reverse inclusion let $a \in I$ and use the Division Algorithm to write $a = qd + r$ with $r = 0$ or $N(r) < N(d)$. Then $r = a - qd$ and note that $a \in I$ and $qd \in I$, so r is an element of I. By the minimality of the norm of d, it must be the case that $r = 0$. Hence $a = qd \in (d)$, showing $I \subseteq (d)$ which establishes the proposition that $I = (d)$. □

Example 1.1.3. Let $R = \mathbf{Z}[x]$. Since the ideal $(2, x)$ is not principle, it follows that the ring $\mathbf{Z}[x]$ of polynomials with integer coefficients is not a Euclidean Domain.

Definition 1.1.3. 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 $b \mid a$.

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

  (i) $d \mid a$ and $d \mid b$, and

  (ii) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

A greatest common divisor of a and b will be denoted by $\gcd(a, b)$, or (abusing the notation) simply (a, b).

Definition 1.1.4. If I is the ideal of R generated by a and b (that is, $I = (a, b)$), then d is the greatest common divisor of a and b if

(i) I is contained in the principial ideal (d), and

(ii) if (d') is any principical ideal containing I then $(d) \subseteq (d')$.

Proposition 1.1.2. *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 a greatest common divisor of a and b.*

Proof. This follows directly from the previous definition. □

Proposition 1.1.3. *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.*

Proof. If either d or d' are 0 then we are done. Assume d and d' are nonzero. Since $d \in (d')$ there is some $x \in R$ such that $d = xd'$. Since $d' \in (d)$ there is some $y \in R$ such that $d' = yd$. Thus $d = xyd$ and so $d(1 - xy) = 0$. Since $d \neq 0$, it must be the case that $xy = 1$, that is, both x and y are units. This proves the first assertion.

The second assertion follows from the first since any two greatest common divisors of a and b generate the same principle ideal (they divide eachother). □

Theorem 1.1.4. *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 described in Example 1.1.1. Then*

(1) d is the 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

$$d = ax + by.$$

Proof. By Proposition 1.1.1, the ideal generated by a and b is principal so a, b do have a greatest common divisor, namely any element which generates the (principal) ideal (a, b). Both parts of the theorem will follow once we show $d = r_n$ generates this ideal; i.e., once we show that

(i) $d \mid a$ and $d \mid b$ (which means $(a, b) \subseteq (d)$)

(ii) d is an R-linear combination of a and b (which means $(d) \subseteq (a, b)$.)

To prove that d divides both a and b, simply keep track of the divisibilities in the Euclidean Algorithm. Recall the following set of equations from Example 1.1.1

$$\begin{aligned}
a &= q_0 b + r_0 && (0)\\
b &= q_1 r_0 + r_1 && (1)\\
r_0 &= q_2 r_1 + r_2 && (2)\\
&\vdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1} && (k+1)\\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && (n)\\
r_{n-1} &= q_{n+1} r_n && (n+1)
\end{aligned}$$

We proceed with induction with n as the base case. Equation $(n+1)$ gives $r_n \mid r_{n-1}$ and clearly $r_n \mid r_n$. Assume $r_n \mid r_{k+1}$ and $r_n \mid r_k$ as our inductive hypothesis. By Equation $(k+1)$ we see that r_n divides both terms on the right hand side —hence $r_n \mid r_{k-1}$. From Equation (1) $r_n \mid b$ and from Equation (0) $r_n \mid a$, which establishes (i). □