# **Section IX.46.** Euclidean Domains

**Note.** Fraleigh comments at the beginning of this section: "Now a modern technique of mathematics is to take some clearly related situations and try to bring them under one roof by abstracting the important ideas common to them." In this section, we take the idea of the division algorithm for integral domain $\mathbb{Z}$ and generalize it to other integral domains.

**Note.** Recall:

1. **Division Algorithm for $\mathbb{Z}$ (Theorem 6.3).**

   If $m$ is a positive integer and $n$ is any integer, then there exist unique integers $q$ and $r$ such that $n = mq + r$ and $0 \leq r < m$.

2. **Division Algorithm for $F[x]$ (Theorem 23.1).**

   Let $F$ be a field and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ be two elements of $F[x]$, with $a_n$ and $b_m$ both nonzero elements of $F$ and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree $m$ of $g(x)$.

**Note.** We now introduce a function which maps an integral domain into the nonnegative integers and use the values of this function to replace the ideas of "remainder" in $\mathbb{Z}$ and "degree" in $F[x]$.

**Definition 46.1.** A *Euclidean norm* on an integral domain $D$ is a function $v$ mapping the nonzero elements of $D$ into the nonnegative integers such that the following conditions are satisfied:

1. For all $a, b \in D$ with $b \neq 0$, there exist $q$ and $r$ in $D$ such that $a = bq + r$ where either $r = 0$ or $v(r) < v(b)$.
2. For all $a, b \in D$ where neither $a$ nor $b$ is 0, we have $v(a) \leq v(ab)$.

An integral domain $D$ is a *Euclidean domain* if there exists a Euclidean norm on $D$.

**Note.** Condition 1 deals with the remainder concept. Condition 2 will let us characterize the units of a Euclidean domain.

**Example 46.2.** The integral domain $\mathbb{Z}$ is a Euclidean domain where we take $v(n) = |n|$ for $n \neq 0$. Condition 1 holds by the Division Algorithm for $\mathbb{Z}$ (Theorem 6.3). Condition 2 holds because $|ab| = |a||b|$ and $|a| \geq 1$ for $a \neq 0$ in $\mathbb{Z}$.

**Example 46.3.** If $F$ is a field, then $F[x]$ is a Euclidean domain where we take $v(f(x)) = (\text{degree } f(x))$ for $f(x) \in F[x]$ and $f(x) \neq 0$ ($v$ is only defined on the nonzero elements by definition). Condition 1 holds by the Division Algorithm for $F[x]$ (Theorem 23.1). Condition 2 holds since the degree of the product of two polynomials is the sum of their degrees.

**Theorem 46.4.** Every Euclidean domain is a PID.

**Corollary 46.5.** Every Euclidean domain is a UFD.

**Proof.** Let $D$ be a Euclidean domain. By Theorem 46.4 $D$ is a PID. By Theorem 45.17 $D$ is a UFD. ∎

**Note.** We now use Condition 2 of a Euclidean norm to characterize the units of a Euclidean domain.

**Theorem 46.6.** For a Euclidean domain with a Euclidean norm $v$, $v(1)$ is minimal among all $v(a)$ for nonzero $a \in D$, and $u \in D$ is a unit if and only if $v(u) = v(1)$.

**Example 46.7.** To illustrate Theorem 46.6, consider the Euclidean domain $\mathbb{Z}$ with $v(n) = |n|$ for $n \neq 0$, we have that $v(1) = 1$ is minimal and the only elements in $\mathbb{Z}$ with $v$ equal to 1 are 1 and $-1$, the units in $\mathbb{Z}$.

**Example 46.8.** For field $F$ and Euclidean domain $F[x]$ where $v(f(x)) = (\text{degree } f(x))$ for nonzero $f(x)$, the minimum value of $v$ is 0 and this is the value of $v$ for the nonzero constant polynomials. As we know, the only units in $F[x]$ are the nonzero constant polynomials (which we associate with the nonzero elements of $F$). We now see the importance of defining $v$ only for the *nonzero* elements! Without this, we could not use Condition 2 to classify units in Theorem 46.6.

**Note.** The next result allows us to find gcd's in a Euclidean domain in a way similar to the approach in $\mathbb{N}$.

**Theorem 46.9. Euclidean Algorithm.**

Let $D$ be a Euclidean domain with a Euclidean norm $v$, and let $a$ and $b$ be nonzero elements of $D$. let $r_1$ be as in Condition 1 for a Euclidean norm, that is $a = bq_1 + r_1$ where either $r_1 = 0$ or $v(r_1) < v(b)$. If $r_1 \neq 0$, let $r_2$ be such that $b = r_1q_2 + r_2$ where either $r_2 = 0$ or $v(r_2) < v(r_1)$. Recursively, let $r_{i+1}$ be such that $r_{i-1} = r_iq_{i+1} + r_{i+1}$ where either $r_{i+1} = 0$ or $v(r_{i+1}) < v(r_i)$. Then the sequence $r_1, r_2, \ldots$ must terminate with some $r_3 = 0$. If $r_1 = 0$, then $b$ is a gcd of $a$ and $b$. If $r_1 \neq 0$ and $r_s = 0$ is the first $r_i = 0$ then a gcd of $a$ and $b$ is $r_{s-1}$. Furthermore, if $d$ is a gcd of $a$ and $b$, then there exist $\lambda$ and $\mu$ in $D$ such that $d = \lambda a + \mu b$.

**Examples 46.10 and 46.11.** We now illustrate the Euclidean Algorithm. The big benefit of it is that it allows us to find a gcd ("algorithmically") without directly factoring the two "numbers." Consider the Euclidean domain $\mathbb{Z}$ with Euclidean norm $v(n) = |n|$ for $n \in \mathbb{Z}$, $n \neq 0$. We find a gcd of $a = 22{,}471$ and $b = 3{,}266$.

Starting with $a = r_{-1}$, $b = r_0$, and the relation $r_{i-1} = r_i q_{i+1} + r_{i+1}$ we get:

| $i$ | $r_{i-1} = r_i q_{i+1} + r_{i+1}$ | $r_{i+1}$ |
|---|---|---|
| 0 | $22{,}471 = (3{,}266)6 + 2{,}875$ | 2,875 |
| 1 | $3{,}266 = (2{,}875)1 + 391$ | 391 |
| 2 | $2{,}875 = (391)7 + 138$ | 138 |
| 3 | $391 = (138)2 + 115$ | 115 |
| 4 | $138 = (115)1 + 23$ | 23 |
| 5 | $115 = (23)5 + 0$ | 0 |

So a gcd of 22,471 and 3,266 if $r_5 = 23$. Notice that we do not have to have positive remainders. Fraleigh shows that we can use negative remainders (remember that $v$ is absolute value) to cut the algorithm down to four steps in this example:

| $i$ | $r_{i-1} = r_i q_{i+1} + r_{i+1}$ | $r_{i+1}$ |
|---|---|---|
| 0 | $22{,}471 = (3{,}266)7 - 391$ | $-391$ |
| 1 | $3{,}266 = (391)8 + 138$ | 138 |
| 2 | $391 = (138)3 - 23$ | $-23$ |
| 3 | $138 = (23)6 + 0$ | 0 |

So a gcd of 22,471 and 3,266 is $r_2 = -23$.

*Revised: 3/22/2024*