# Lecture 7.7: Euclidean domains, PIDs, and UFDs

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

# The Euclidean algorithm

Around 300 B.C., Euclid wrote his famous book, the *Elements*, in which he described what is now known as the Euclidean algorithm:

**Proposition VII.2 (Euclid's *Elements*)**

Given two numbers not prime to one another, to find their greatest common measure.

The algorithm works due to two key observations:

- If $a \mid b$, then $\gcd(a,b) = a$;
- If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$.

This is best seen by an example: Let $a = 654$ and $b = 360$.

$$\begin{array}{ll} 654 = 360 \cdot 1 + 294 & \gcd(654,360) = \gcd(360,294) \\ 360 = 294 \cdot 1 + 66 & \gcd(360,294) = \gcd(294,66) \\ 294 = 66 \cdot 4 + 30 & \gcd(294,66) = \gcd(66,30) \\ 66 = 30 \cdot 2 + 6 & \gcd(66,30) = \gcd(30,6) \\ 30 = 6 \cdot 5 & \gcd(30,6) = 6. \end{array}$$

We conclude that $\gcd(654,360) = 6$.

# Euclidean domains

Loosely speaking, a Euclidean domain is any ring for which the Euclidean algorithm still works.

## Definition

An integral domain $R$ with 1 is Euclidean if it has a degree function $d \colon R^* \longrightarrow \mathbb{Z}$ satisfying:

(i) non-negativity: $d(r) \geq 0 \quad \forall r \in R^*$.

(ii) monotonicity: $d(a) \leq d(ab)$ for all $a, b \in R$.

(iii) division-with-remainder property: For all $a, b \in R$, $b \neq 0$, there are $q, r \in R$ such that

$$a = bq + r \qquad \text{with} \qquad r = 0 \quad \text{or} \quad d(r) < d(b)\,.$$

Note that Property (ii) could be restated to say: *If $a \mid b$, then $d(a) \leq d(b)$*;

## Examples

- $R = \mathbb{Z}$ is Euclidean. Define $d(r) = |r|$.
- $R = F[x]$ is Euclidean if $F$ is a field. Define $d(f(x)) = \deg f(x)$.

# Euclidean domains

## Proposition

If $R$ is Euclidean, then $U(R) = \{x \in R^* : d(x) = d(1)\}$.

## Proof

$\subseteq$": First, we'll show that associates have the same degree. Take $a \sim b$ in $R^*$:

$$\begin{array}{ccc} a \mid b & \Longrightarrow & d(a) \leq d(b) \\ b \mid a & \Longrightarrow & d(b) \leq d(a) \end{array} \quad \Longrightarrow \quad d(a) = d(b).$$

If $u \in U(R)$, then $u \sim 1$, and so $d(u) = d(1)$. ✓

"$\supseteq$": Suppose $x \in R^*$ and $d(x) = d(1)$.

Then $1 = qx + r$ for some $q \in r$ with either $r = 0$ or $d(r) < d(x) = d(1)$.

If $r \neq 0$, then $d(1) \leq d(r)$ since $1 \mid r$.

Thus, $r = 0$, and so $qx = 1$, hence $x \in U(R)$. ✓ □

# Euclidean domains

## Proposition

If $R$ is Euclidean, then $R$ is a PID.

## Proof

Let $I \neq 0$ be an ideal and pick some $b \in I$ with $d(b)$ minimal.

Pick $a \in I$, and write $a = bq + r$ with either $r = 0$, or $d(r) < d(b)$.

This latter case is impossible: $r = a - bq \in I$, and by minimality, $d(b) \leq d(r)$.

Therefore, $r = 0$, which means $a = bq \in (b)$. Since $a$ was arbitrary, $I = (b)$. $\square$

**Exercises**.

(i) The ideal $I = (3, 2 + \sqrt{-5})$ is not principal in $R_{-5}$.

(ii) If $R$ is an integral domain, then $I = (x, y)$ is not principal in $R[x, y]$.

## Corollary

The rings $R_{-5}$ and $R[x, y]$ are not Euclidean.

# Euclidean domains

The following results are not overly difficult to prove, but they involve checking a number of cases.

**Proposition**

If $m \in \{-11, -7, -3, -2, -1, 2, 3\}$, then $R_m$ is Euclidean with degree function $d(r) = |N(r)|$.

**Proposition**

If $m < 0$ and $m \notin \{-11, -7, -3, -2, -1\}$, then $R_m$ is not Euclidean.

**Corollary**

$R_{-19}$ is a PID that is not Euclidean.

# Unique factorization domains

## Definition

An integral domain is a unique factorization domain (UFD) if

(i) Every nonzero element is a product of irreducible elements;

(ii) Every irreducible element is prime.

## Examples

1. $\mathbb{Z}$ is a UFD: Every integer $n \in \mathbb{Z}$ can be uniquely factored as a product of irreducibles (primes):
$$n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$
This is the *fundamental theorem of arithmetic*.

2. The polynomial ring $\mathbb{Z}[x]$ is a UFD, because every polynomial can be factored into irreducibles polynomials. However, it is not a PID because the ideal
$$(2, x) = \{f(x) : \text{ the constant term is even}\}$$
is not principle.

3. We've shown that (ii) holds for PIDs. Next, we will see that (i) holds as well.

# Unique factorization domains

## Theorem

If $R$ is a PID, then $R$ is a UFD.

## Sketch of proof

We need to show Condition (i) holds: every element is a product of irreducibles. A ring is Noetherian if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilizes, meaning that $I_k = I_{k+1} = I_{k+2} = \cdots$ holds for some $k$.

Suppose $R$ is a PID. It is not hard to show that $R$ is Noetherian. Define

$$X = \{a \in R^* \setminus U(R) : a \text{ can't be written as a product of irreducibles}\}.$$

If $X \neq \emptyset$, then pick $a_1 \in X$, $a_2 \in X \setminus (a_1)$, and $a_3 \in X \setminus (a_1, a_2)$, and so on. We get an ascending chain

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

that does not stabilize. This is impossible in a PID, so $X = \emptyset$. □

# Unique factorization domains

## Facts

1. If $m < 0$, then $R_m$ is a PID iff
$$m \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$
2. If $m > 0$, then $R_m$ is Euclidean (with $d(r) = |N(r)|$) iff
$$m \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$
3. $R_m$ is a PID that is not Euclidean iff $m \in \{-19, -43, -67, -163\}$.

## Open problem

For which $m > 0$ is $R_m$ a PID?

We already proved the following for PIDs. It is also true for UFDs. The proof is not difficult.

## Proposition

If $R$ is a UFD, and $a, b \in R$ not both zero, then $\gcd(a, b)$ exists, and is unique up to associates.

# Summary of ring types