Lecture 7.5: Euclidean domains and algebraic integers

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 $b = 360$.

\[
\begin{align*}
654 &= 360 \cdot 1 + 294 \\
360 &= 294 \cdot 1 + 66 \\
294 &= 66 \cdot 4 + 30 \\
66 &= 30 \cdot 2 + 6 \\
30 &= 6 \cdot 5
\end{align*}
\]

\[
\begin{align*}
\gcd(654, 360) &= \gcd(360, 294) \\
\gcd(360, 294) &= \gcd(294, 66) \\
\gcd(294, 66) &= \gcd(66, 30) \\
\gcd(66, 30) &= \gcd(30, 6) \\
\gcd(30, 6) &= 6
\end{align*}
\]

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 $R$ is **Euclidean** if it has a degree function $d : R^* \rightarrow \mathbb{Z}$ 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

\[ a = bq + r \quad \text{with} \quad r = 0 \text{ or } d(r) < d(b). \]

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 $d(f(x)) = \deg f(x)$.
- The **Gaussian integers** $R_{-1} = \mathbb{Z}[\sqrt{-1}] = \{a + bi : a, b \in \mathbb{Z}\}$ is Euclidean with degree function $d(a + bi) = a^2 + b^2$. 
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 $R^*$:

$$a | b \implies d(a) \leq d(b)$$

$$b | a \implies d(b) \leq d(a) \implies d(a) = d(b).$$

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 $1 | r$.

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 \( R_{-5} \) (not a PID or UFD) and \( R[x, y] \) (not a PID) are not Euclidean.
Algebraic integers

The algebraic integers are the roots of monic polynomials in \( \mathbb{Z}[x] \). This is a subring of the algebraic numbers (roots of all polynomials in \( \mathbb{Z}[x] \)).

Assume \( m \in \mathbb{Z} \) is square-free with \( m \neq 0, 1 \). Recall the quadratic field

\[
\mathbb{Q}(\sqrt{m}) = \left\{ p + q\sqrt{m} \mid p, q \in \mathbb{Q} \right\}.
\]

**Definition**

The ring \( R_m \) is the set of algebraic integers in \( \mathbb{Q}(\sqrt{m}) \), i.e., the subring consisting of those numbers that are roots of monic quadratic polynomials \( x^2 + cx + d \in \mathbb{Z}[x] \).

**Facts**

- \( R_m \) is an integral domain with 1.
- Since \( m \) is square-free, \( m \not\equiv 0 \pmod{4} \). For the other three cases:

\[
R_m = \begin{cases} 
\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} & m \equiv 2 \text{ or } 3 \pmod{4} \\
\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \{a + b\left(\frac{1+\sqrt{m}}{2}\right) : a, b \in \mathbb{Z}\} & m \equiv 1 \pmod{4}
\end{cases}
\]

- \( R_{-1} \) is the Gaussian integers, which is a PID. (easy)
- \( R_{-19} \) is a PID. (hard)
**Definition**

For $x = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, define the norm of $x$ to be

$$N(x) = (r + s\sqrt{m})(r - s\sqrt{m}) = r^2 - ms^2.$$ 

$R_m$ is norm-Euclidean if it is a Euclidean domain with $d(x) = |N(x)|$.

Note that the norm is multiplicative: $N(xy) = N(x)N(y)$.

**Exercises**

Assume $m \in \mathbb{Z}$ is square-free, with $m \neq 0, 1$.

- $u \in U(R_m)$ iff $|N(u)| = 1$.
- If $m \geq 2$, then $U(R_m)$ is infinite.
- $U(R_{-1}) = \{\pm 1, \pm i\}$ and $U(R_{-3}) = \{\pm 1, \pm \frac{1 \pm \sqrt{-3}}{2}\}$.
- If $m = -2$ or $m < -3$, then $U(R_m) = \{\pm 1\}$. 

M. Macauley (Clemson)
Euclidean domains and algebraic integers

**Theorem**

\( R_m \) is norm-Euclidean iff

\[ m \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}. \]

**Theorem (D.A. Clark, 1994)**

The ring \( R_{69} \) is a Euclidean domain that is *not* norm-Euclidean.

Let \( \alpha = (1 + \sqrt{69})/2 \) and \( c > 25 \) be an integer. Then the following degree function works for \( R_{69} \), defined on the prime elements:

\[
d(p) = \begin{cases} 
|N(p)| & \text{if } p \neq 10 + 3\alpha \\
c & \text{if } p = 10 + 3\alpha 
\end{cases}
\]

**Theorem**

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

**Open problem**

Classify which \( R_m \)'s are PIDs, and which are Euclidean.
Theorem
If $m < 0$, then $R_m$ is a PID iff
$$m \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$  

Recall that $R_m$ is norm-Euclidean iff
$$m \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$  

Corollary
If $m < 0$, then $R_m$ is a PID that is not Euclidean iff $m \in \{-19, -43, -67, -163\}$.  

M. Macauley (Clemson)
Algebraic integers

Figure: Algebraic numbers in the complex plane. Colors indicate the coefficient of the leading term: **red** = 1 (algebraic integer), **green** = 2, **blue** = 3, **yellow** = 4. Large dots mean fewer terms and smaller coefficients. Image from Wikipedia (made by Stephen J. Brooks).
Figure: Algebraic integers in the complex plane. Each red dot is the root of a monic polynomial of degree $\leq 7$ with coefficients from $\{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$. From Wikipedia.
Summary of ring types

- **Fields**
  - \( \mathbb{Q} \)
  - \( \mathbb{R} \)
  - \( \mathbb{C} \)

- **Integral Domains**
  - \( \mathbb{Z} \)
  - \( \mathbb{Z}[x, y] \)
  - \( \mathbb{Z}[x] \)
  - \( \mathbb{Z}[x^2, x^3] \)

- **Unique Factorization Domains (UFDs)**
  - \( \mathbb{R} \)
  - \( \mathbb{Z}_p \)
  - \( \mathbb{Q} \)
  - \( \mathbb{F}_p^n \)
  - \( \mathbb{R}(\sqrt{-\pi}, i) \)

- **Principal Ideal Domains (PIDs)**
  - \( \mathbb{R}_{-1} \)
  - \( \mathbb{R}_{-19} \)
  - \( \mathbb{R}_{-43} \)
  - \( \mathbb{R}_{-67} \)
  - \( \mathbb{R}_{-163} \)

- **Euclidean Domains**
  - \( \mathbb{Z} \)
  - \( \mathbb{Z}_6 \)
  - \( \mathbb{Z}_{-5} \)
  - \( \mathbb{Z}_{-19} \)
  - \( \mathbb{Z}_{-43} \)

- **Commutative Rings**
  - \( \mathbb{R} \times \mathbb{R} \)

- **All Rings**
  - Field extensions
  - Matrices

- **Additional Rings**
  - \( M_n(\mathbb{R}) \)

M. Macauley (Clemson)