Lecture 27
Euclidean domains and Principal ideal domains
From now on, $R$ is going to be a commutative integral domain. (Some of our theorems can be proven without commutativity or domainness, but we’ll skip nitpicking for the sake of time)
Finishing out the quarter: The many commutative domains

From now on, \( R \) is going to be a commutative integral domain. (Some of our theorems can be proven without commutativity or domainness, but we’ll skip nitpicking for the sake of time)

In order of restrictivity, we also have

**Unique factorization domains (UFDs):** elements factor ‘uniquely’ into primes, where a prime is a non-zero, non-unit \( p \) such that if \( p = ab \), then \( a \) or \( b \) is a unit.

**A domain that’s not a UFD:** \( \mathbb{Z}[\sqrt{-5}] \), because

\[ 6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \text{ and [stuff about units]} \]
Finishing out the quarter: The many commutative domains

From now on, $R$ is going to be a commutative integral domain. (Some of our theorems can be proven without commutativity or domainness, but we’ll skip nitpicking for the sake of time)

In order of restrictivity, we also have

**Unique factorization domains (UFDs):** elements factor ‘uniquely’ into primes, where a prime is a non-zero, non-unit $p$ such that if $p = ab$, then $a$ or $b$ is a unit.

A domain that’s not a UFD: $\mathbb{Z}[\sqrt{-5}]$, because

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \text{ and [stuff about units]}$$

**Principal ideal domains (PIDs):** every ideal is principal.

A UFD that’s not a PID: $\mathbb{Q}[x, y]$, because polynomials factor uniquely, but $(x, y)$ is not principal.
Finishing out the quarter: The many commutative domains

From now on, $R$ is going to be a commutative integral domain.
(Some of our theorems can be proven without commutativity or domainness, but we’ll skip nitpicking for the sake of time)

In order of restrictivity, we also have

**Unique factorization domains (UFDs):** elements factor ‘uniquely’ into primes, where a prime is a non-zero, non-unit $p$ such that if $p = ab$, then $a$ or $b$ is a unit.

*A domain that’s not a UFD:* $\mathbb{Z}[\sqrt{-5}]$, because

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and [stuff about units]

**Principal ideal domains (PIDs):** every ideal is principal.

*A UFD that’s not a PID:* $\mathbb{Q}[x, y]$, because polynomials factor uniquely, but $(x, y)$ is not principal.

**Euclidean domains (EDs):** there’s a division algorithm.

*A PID that’s not a ED:* $\mathbb{Z}[(1 + \sqrt{-19})/2)]$ (see examples on pp 277 and 282)
(Let \( R \) be a commutative integral domain.)

**Definition**

Let \( a, b \in R \) with \( b \neq 0 \).

1. \( a \) is a **multiple** of \( b \) if there exists \( x \in R \) with \( a = bx \). We say \( b \) divides \( a \), denoted \( b \mid a \).
(Let $R$ be a commutative integral domain.)

**Definition**

Let $a, b \in R$ with $b \neq 0$.

1. $a$ is a **multiple** of $b$ if there exists $x \in R$ with $a = bx$. We say $b$ divides $a$, denoted $b \mid a$.

2. A **greatest common divisor** of $a$ and $b$ is a nonzero element $d$ dividing $a$ and $b$ such that $d' \mid a$ and $d' \mid b$ implies $d' \mid d$. 
(Let $R$ be a commutative integral domain.)

**Definition**

Let $a, b \in R$ with $b \neq 0$.

1. *a is a multiple of b* if there exists $x \in R$ with $a = bx$. We say $b$ divides $a$, denoted $b \mid a$.

2. A greatest common divisor of $a$ and $b$ is a nonzero element $d$ dividing $a$ and $b$ such that $d' \mid a$ and $d' \mid b$ implies $d' \mid d$.

*Well-defined?? “a” versus “the”*
(Let \( R \) be a commutative integral domain.)

**Definition**

Let \( a, b \in R \) with \( b \neq 0 \).

1. *a* is a **multiple** of *b* if there exists \( x \in R \) with \( a = bx \). We say \( b \) divides \( a \), denoted \( b \mid a \).

2. A greatest common divisor of \( a \) and \( b \) is a nonzero element \( d \) dividing \( a \) and \( b \) such that \( d' \mid a \) and \( d' \mid b \) implies \( d' \mid d \).

*Well-defined?? “a” versus “the”*

**Proposition**

Let \( a, b, d, d' \in R \).

1. **Abusing parentheses:** If the ideal generated by \( \{a, b\} \) is the same as the ideal generated by \( d \), then \( d = \gcd(a, b) \), i.e.

\[
(a, b) = (d) \quad \implies \quad (a, b) = d.
\]
(Let \( R \) be a commutative integral domain.)

**Definition**

Let \( a, b \in R \) with \( b \neq 0 \).

1. *a is a multiple of* \( b \) if there exists \( x \in R \) with \( a = bx \). We say \( b \) divides \( a \), denoted \( b \mid a \).

2. A greatest common divisor of \( a \) and \( b \) is a nonzero element \( d \) dividing \( a \) and \( b \) such that \( d' \mid a \) and \( d' \mid b \) implies \( d' \mid d \).

**Proposition**

Let \( a, b, d, d' \in R \).

1. Abusing parentheses: If the ideal generated by \( \{a, b\} \) is the same as the ideal generated by \( d \), then \( d = \gcd(a, b) \), i.e.
   \[
   (a, b) = (d) \implies (a, b) = d.
   \]

2. Uniqueness: If \( d \) and \( d' \) generate the same ideal, then
   \[
   d' = ud \quad \text{for some unit} \ u \in R^\times.
   \]
   In particular, if \( d \) and \( d' \) are both greatest common divisors of \( a \) and \( b \), then \( d' = ud \).
Finding and using greatest common divisors

The previous proposition said

\[ if \ (a, b) = (d) \ then \ d = \gcd(a, b). \]

Careful! Not every ideal is principal! So the converse is not always true! Ex: \((x, y) \in \mathbb{Q}[x, y]\).
Finding and using greatest common divisors

The previous proposition said

\[ \text{if } (a, b) = (d) \text{ then } d = \gcd(a, b). \]

Careful! Not every ideal is principal! So the converse is not always true! Ex: \((x, y)\) in \(\mathbb{Q}[x, y]\).

(\text{Corollary})

However, if \(R\) is a \textbf{principal ideal domain} (an integral domain where every ideal is principal), we have

1. the ideal \((a, b)\) is the same as the ideal \((\gcd(a, b))\), for any \(\gcd(a, b)\), and so

2. since \((a, b) = \{ar + bs \mid r, s \in R\}\), this means that

\[ ar + bs = \gcd(a, b) \quad \text{for some } r, s \in R. \]
Finding and using greatest common divisors

The previous proposition said

\[ \text{if } (a, b) = (d) \text{ then } d = \gcd(a, b). \]

Careful! Not every ideal is principal! So the converse is not always true! Ex: \((x, y)\) in \(\mathbb{Q}[x, y]\).

(Corollary)

However, if \(R\) is a principal ideal domain (an integral domain where every ideal is principal), we have

1. the ideal \((a, b)\) is the same as the ideal \((\gcd(a, b))\), for any \(\gcd(a, b)\), and so
2. since \((a, b) = \{ar + bs \mid r, s \in R\}\), this means that

\[ ar + bs = \gcd(a, b) \quad \text{ for some } r, s \in R. \]

But what are \(r\) and \(s\)? To calculate, we need a division algorithm! Euclidean domains is where that happens.
Euclidean Domains

Recall the quadratic field $\mathbb{Q}(\sqrt{D})$ and its ring of integers $\mathbb{Z}[\omega]$ (where $D$ is a square-free integer and $\omega = \sqrt{D}$ or $(1 + \sqrt{D})/2$).
Euclidean Domains

Recall the quadratic field \( \mathbb{Q}(\sqrt{D}) \) and its ring of integers \( \mathbb{Z}[\omega] \) (where \( D \) is a square-free integer and \( \omega = \sqrt{D} \) or \((1 + \sqrt{D})/2\)). To calculate the units of \( \mathbb{Z}[\omega] \), we defined a “norm”

\[
N : \mathbb{Q}(\sqrt{D}) \rightarrow \mathbb{Q} \quad \text{defined by} \quad N(a + b\sqrt{D}) = a^2 - b^2D.
\]
Euclidean Domains

Recall the quadratic field \( \mathbb{Q}(\sqrt{D}) \) and its ring of integers \( \mathbb{Z}[\omega] \) (where \( D \) is a square-free integer and \( \omega = \sqrt{D} \) or \( (1 + \sqrt{D})/2 \)). To calculate the units of \( \mathbb{Z}[\omega] \), we defined a “norm”

\[
N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q} \quad \text{defined by} \quad N(a + b\sqrt{D}) = a^2 - b^2 D.
\]

When restricted to \( \mathbb{Z}[\omega] \subseteq \mathbb{Q}(\sqrt{D}) \), we had

\[
N(n + m\omega) \in \mathbb{Z} \quad \text{and} \quad N(x) = 0 \text{ iff } x = 0.
\]
Euclidean Domains

Recall the quadratic field $\mathbb{Q}(\sqrt{D})$ and its ring of integers $\mathbb{Z}[\omega]$ (where $D$ is a square-free integer and $\omega = \sqrt{D}$ or $(1 + \sqrt{D})/2$).

To calculate the units of $\mathbb{Z}[\omega]$, we defined a “norm”

$$N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$$

defined by

$$N(a + b\sqrt{D}) = a^2 - b^2D.$$

When restricted to $\mathbb{Z}[\omega] \subseteq \mathbb{Q}(\sqrt{D})$, we had

$$N(n + m\omega) \in \mathbb{Z} \quad \text{and} \quad N(x) = 0 \iff x = 0.$$

**Definition.** Let $R$ be an ID. A **norm** is a function

$$N : R \to \mathbb{Z}_{\geq 0} \quad \text{with} \quad N(0) = 0.$$

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a **positive norm**.
Euclidean Domains

Recall the quadratic field $\mathbb{Q}(\sqrt{D})$ and its ring of integers $\mathbb{Z}[\omega]$ (where $D$ is a square-free integer and $\omega = \sqrt{D}$ or $(1 + \sqrt{D})/2$).

To calculate the units of $\mathbb{Z}[\omega]$, we defined a “norm”

$$N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q} \quad \text{defined by} \quad N(a + b\sqrt{D}) = a^2 - b^2D.$$ 

When restricted to $\mathbb{Z}[\omega] \subseteq \mathbb{Q}(\sqrt{D})$, we had

$$N(n + m\omega) \in \mathbb{Z} \quad \text{and} \quad N(x) = 0 \text{ iff } x = 0.$$

**Definition.** Let $R$ be an ID. A norm is a function

$$N : R \to \mathbb{Z}_{\geq 0} \quad \text{with} \quad N(0) = 0.$$

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a **positive norm**.

*Uh oh!*
Euclidean Domains

Recall the quadratic field $\mathbb{Q}(\sqrt{D})$ and its ring of integers $\mathbb{Z}[\omega]$ (where $D$ is a square-free integer and $\omega = \sqrt{D}$ or $(1 + \sqrt{D})/2$).

To calculate the units of $\mathbb{Z}[\omega]$, we defined a “norm”

$$N : \mathbb{Q}(\sqrt{D}) \rightarrow \mathbb{Q}$$
defined by

$$N(a + b\sqrt{D}) = a^2 - b^2 D.$$

When restricted to $\mathbb{Z}[\omega] \subseteq \mathbb{Q}(\sqrt{D})$, we had

$$N(n + m\omega) \in \mathbb{Z} \quad \text{and} \quad N(x) = 0 \text{ iff } x = 0.$$

**Definition.** Let $R$ be an ID. A norm is a function

$$N : R \rightarrow \mathbb{Z}_{\geq 0} \quad \text{with} \quad N(0) = 0.$$

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a positive norm.

*Uh oh! Fix the field norm by taking the absolute value.*
Euclidean Domains

Definition. Let $R$ be an integral domain. A norm is a function

$$N : R \rightarrow \mathbb{Z}_{\geq 0}$$

with

$$N(0) = 0.$$ 

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a positive norm.
Euclidean Domains

Definition. Let $R$ be an integral domain. A norm is a function

$$N : R \to \mathbb{Z}_{\geq 0} \quad \text{with} \quad N(0) = 0.$$ 

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a positive norm.

Definition. An integral domain $R$ is a Euclidean Domain if there is a norm $N$ on $R$ satisfying

for all $a, b \in R$, $b \neq 0$, there exists $q, r \in R$

with

$$a = qb + r,$$

where $r = 0$ or $N(r) < N(b)$. We call $q$ the quotient and $r$ the remainder of the division.
Euclidean Domains

Definition. Let $R$ be an integral domain. A norm is a function

$$N : R \rightarrow \mathbb{Z}_{\geq 0}$$

with $N(0) = 0$.

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a positive norm.

Definition. An integral domain $R$ is a Euclidean Domain if there is a norm $N$ on $R$ satisfying

for all $a, b \in R$, $b \neq 0$, there exists $q, r \in R$

with

$$a = qb + r,$$

where $r = 0$ or $N(r) < N(b)$.

We call $q$ the quotient and $r$ the remainder of the division.

Ex: (i) $\mathbb{Z}[\omega]$ with $N(n + m\omega) = |n^2 - m^2\omega|$ only sometimes!!
Euclidean Domains

Definition. Let $R$ be an integral domain. A norm is a function

$$N : R \rightarrow \mathbb{Z}_{\geq 0} \quad \text{with} \quad N(0) = 0.$$ 

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a positive norm.

Definition. An integral domain $R$ is a Euclidean Domain if there is a norm $N$ on $R$ satisfying

for all $a, b \in R, \quad b \neq 0, \quad$ there exists $q, r \in R$

with

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

We call $q$ the quotient and $r$ the remainder of the division.

Ex: (i) $\mathbb{Z}[\omega]$ with $N(n + m\omega) = |n^2 - m^2\omega|$ only sometimes!!
(ii) Fields $F$ with $N(a) = 0$ for all $a \in F$. 
Euclidean Domains

Definition. Let $R$ be an integral domain. A **norm** is a function

$$N : R \rightarrow \mathbb{Z}_{\geq 0} \quad \text{with} \quad N(0) = 0.$$  

If $N(a) > 0$ for all $a \neq 0$, say $N$ is a **positive norm**.

Definition. An integral domain $R$ is a **Euclidean Domain** if there is a norm $N$ on $R$ satisfying

for all $a, b \in R, \quad b \neq 0$, there exists $q, r \in R$

with

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

We call $q$ the **quotient** and $r$ the **remainder** of the division.

Ex:  
(i) $\mathbb{Z}[\omega]$ with $N(n + m\omega) = |n^2 - m^2\omega|$ **only sometimes!!**
(ii) Fields $F$ with $N(a) = 0$ for all $a \in F$.
(iii) Integers with $N(n) = |n|$ (read ex 1 on p271).
Euclidean Domains

Definition. Let \( R \) be an integral domain. A norm is a function

\[
N : R \to \mathbb{Z}_{\geq 0} \quad \text{with} \quad N(0) = 0.
\]

If \( N(a) > 0 \) for all \( a \neq 0 \), say \( N \) is a positive norm.

Definition. An integral domain \( R \) is a Euclidean Domain if there is a norm \( N \) on \( R \) satisfying for all \( a, b \in R, \ b \neq 0 \), there exists \( q, r \in R \) with

\[
a = qb + r, \quad \text{where } r = 0 \text{ or } N(r) < N(b).
\]

We call \( q \) the quotient and \( r \) the remainder of the division.

Ex: (i) \( \mathbb{Z}[\omega] \) with \( N(n + m\omega) = |n^2 - m^2\omega| \) only sometimes!!
(ii) Fields \( F \) with \( N(a) = 0 \) for all \( a \in F \).
(iii) Integers with \( N(n) = |n| \) (read ex 1 on p271).
(iv) \( F[x] \) with \( N(p(x)) = \deg(p(x)) \).
$a(x) = x^5 - 3x^2 + 2$ and $b(x) = b = x^3 - 2x + 1$
Proposition

Every ideal in a Euclidean Domain is principal, generated by an element of minimum norm.
Proposition

Every ideal in a Euclidean Domain is principal, generated by an element of minimum norm.

Example: \( \mathbb{Z}[x] \) has a non-principal ideal, and therefore has no ‘good’ norm.
**Proposition**

Every ideal in a Euclidean Domain is principal, generated by an element of minimum norm.

**Example:** $\mathbb{Z}[x]$ has a non-principal ideal, and therefore has no ‘good’ norm.

**Theorem (Computing GCD’s in Euclidean domains)**

Let $R$ be a Euclidean Domain and $a, b \in R$. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for $a$ and $b$. Then

1. $d$ is the g.c.d. of $a$ and $b$, and
2. $(d)$ is the ideal generated by $a$ and $b$.

In particular, there exist $x, y \in R$ such that $d = ax + by$. 
Seeing the difference between PIDs and EDs is subtle
Seeing the difference between PIDs and EDs is subtle

A universal side divisor is a non-zero, non-unit $a \in R$ such that every $x \in R$ can be written as

$$x = qa + z$$

where $z = 0$ or is a unit.
A universal side divisor is a non-zero, non-unit \( a \in R \) such that every \( x \in R \) can be written as
\[
x = qa + z \quad \text{where } z = 0 \text{ or is a unit.}
\]

The existence of universal side divisors is a way of getting around finding a norm. Namely (see prop 8.5 on p. 277)

*if \( R \) is a Euclidean domain (but not a field), then \( R \) has universal side divisors*
Seeing the difference between PIDs and EDs is subtle

A universal side divisor is a non-zero, non-unit \( a \in R \) such that every \( x \in R \) can be written as
\[
x = qa + z \quad \text{where } z = 0 \text{ or is a unit.}
\]

The existence of universal side divisors is a way of getting around finding a norm. Namely (see prop 8.5 on p. 277)

*if \( R \) is a Euclidean domain (but not a field),
then \( R \) has universal side divisors*

(\( \star \)) Example: Fix \( D = -19 \). Can show that \( \mathbb{Z}[\omega] \) does not have usd’s.
A universal side divisor is a non-zero, non-unit \( a \in R \) such that every \( x \in R \) can be written as
\[
x = qa + z \quad \text{where} \quad z = 0 \text{ or is a unit}.
\]

The existence of universal side divisors is a way of getting around finding a norm. Namely (see prop 8.5 on p. 277)

\textit{if } R \textit{ is a Euclidean domain (but not a field), then } R \textit{ has universal side divisors}

\((*)\) Example: Fix \( D = -19 \). Can show that \( \mathbb{Z}[\omega] \) does not have usd’s.

A Dedekind-Hasse norm is a positive norm \( N \) on \( R \) such that for all \( a, b \in R - \{0\} \) either
\[
a \in (b) \quad \text{or} \quad \exists \text{ non-zero } s \in (a, b) \text{ with } N(s) < N(b).
\]
Seeing the difference between PIDs and EDs is subtle

A universal side divisor is a non-zero, non-unit $a \in R$ such that every $x \in R$ can be written as

$$x = qa + z$$

where $z = 0$ or is a unit.

The existence of universal side divisors is a way of getting around finding a norm. Namely (see prop 8.5 on p. 277)

*if $R$ is a Euclidean domain (but not a field),
then $R$ has universal side divisors*

(*) Example: Fix $D = -19$. Can show that $\mathbb{Z}[w]$ does not have usd’s.

A Dedekind-Hasse norm is a positive norm $N$ on $R$ such that for all $a, b \in R - \{0\}$ either

$$a \in (b) \quad \text{or} \quad \exists \text{ non-zero } s \in (a, b) \text{ with } N(s) < N(b).$$

We care because (see prop 8.9 and cor 8.16)

*an integral domain is a PID if and only if it has a D-H norm*
Seeing the difference between PIDs and EDs is subtle

A **universal side divisor** is a non-zero, non-unit \( a \in R \) such that every \( x \in R \) can be written as
\[
x = qa + z \quad \text{where } z = 0 \text{ or is a unit.}
\]

The existence of universal side divisors is a way of getting around finding a norm. Namely (see prop 8.5 on p. 277)

*if \( R \) is a Euclidean domain (but not a field), then \( R \) has universal side divisors*

\((*)\) **Example:** Fix \( D = -19 \). Can show that \( \mathbb{Z}[\omega] \) does not have usd’s.

A **Dedekind-Hasse norm** is a positive norm \( N \) on \( R \) such that for all \( a, b \in R - \{0\} \) either
\[
a \in (b) \quad \text{or} \quad \exists \text{ non-zero } s \in (a, b) \text{ with } N(s) < N(b).
\]

We care because (see prop 8.9 and cor 8.16)

*an integral domain is a PID if and only if is has a D-H norm*

\((*)\) **Example:** Can show that the standard field norm on \( \mathbb{Z}[\omega] \) is a Dedekind-Hasse norm (p. 282).
Seeing the difference between PIDs and EDs is subtle

A universal side divisor is a non-zero, non-unit \( a \in R \) such that every \( x \in R \) can be written as
\[
x = qa + z \quad \text{where } z = 0 \text{ or is a unit.}
\]

The existence of universal side divisors is a way of getting around finding a norm. Namely (see prop 8.5 on p. 277)

*if \( R \) is a Euclidean domain (but not a field),
then \( R \) has universal side divisors*

(\(\ast\) Example: Fix \( D = -19 \). Can show that \( \mathbb{Z}[\omega] \) does not have usd’s.

A Dedekind-Hasse norm is a positive norm \( N \) on \( R \) such that for all \( a, b \in R - \{0\} \) either
\[
a \in (b) \quad \text{or} \quad \exists \text{ non-zero } s \in (a, b) \text{ with } N(s) < N(b).
\]

We care because (see prop 8.9 and cor 8.16)

*an integral domain is a PID if and only if it has a D-H norm*

(\(\ast\) Example: Can show that the standard field norm on \( \mathbb{Z}[\omega] \) is a Dedekind-Hasse norm (p. 282). So \( \mathbb{Z}[\omega] \) is a PID but not a ED.
Some more facts about PID’s

Recall that a prime ideal $P$ is an ideal satisfying

$$ab \in P,$$

then $a \in P$ or $b \in P$.

Also, recall that maximal ideals are all prime ideals.
Some more facts about PID’s

Recall that a prime ideal $P$ is an ideal satisfying

if $ab \in P$, then $a \in P$ or $b \in P$.

Also, recall that maximal ideals are all prime ideals.

**Proposition**

*In a PID, every non-zero prime ideal is a maximal ideal.*
Some more facts about PID’s

Recall that a prime ideal $P$ is an ideal satisfying
if $ab \in P$, then $a \in P$ or $b \in P$.
Also, recall that maximal ideals are all prime ideals.

Proposition

In a PID, every non-zero prime ideal is a maximal ideal.

Corollary

If $R[x]$ is a PID, then $R$ is a field.
So all polynomial rings that are PIDs are also Euclidean domains!