Lecture 26
Properties of Ideals
Last time: Maximal ideals

Definition
An ideal $M$ in the ring $S$ is a maximal ideal if $M \neq S$ and the only ideals containing $M$ are $M$ and $S$. 
Last time: Maximal ideals

Definition
An ideal $M$ in the ring $S$ is a maximal ideal if $M \neq S$ and the only ideals containing $M$ are $M$ and $S$.

Proposition
In a ring with identity every proper ideal is contained in a maximal ideal.

Theorem (Zorn’s Lemma)
If $A$ is a non-empty partially ordered set in which every chain has an upper bound, then $A$ has a maximal element.
Last time: Maximal ideals

Definition
An ideal $M$ in the ring $S$ is a maximal ideal if $M \neq S$ and the only ideals containing $M$ are $M$ and $S$.

Proposition
In a ring with identity every proper ideal is contained in a maximal ideal.

Theorem (Zorn’s Lemma)
If $A$ is a non-empty partially ordered set in which every chain has an upper bound, then $A$ has a maximal element.

Proposition
Let $R$ be a commutative ring. The ideal $M$ is maximal if and only if $R/M$ is a field.
Generalizing the integers: Prime ideals

Ring theory in Number theory. For example, read about the reduction homomorphism (p. 245), and its role in finding integer solutions to equations like

\[ x^2 + y^2 = 3z^2 \quad \text{or} \quad x^n + y^n = z^n \]
Generalizing the integers: Prime ideals

Ring theory in Number theory. For example, read about the reduction homomorphism (p. 245), and its role in finding integer solutions to equations like

\[ x^2 + y^2 = 3z^2 \quad \text{or} \quad x^n + y^n = z^n \]

Definition
Let \( R \) be a commutative ring. An ideal \( P \) is a prime ideal if \( P \neq R \) and whenever \( ab \in P \), either \( a \in P \) or \( b \in P \).
Generalizing the integers: Prime ideals

Ring theory in Number theory. For example, read about the reduction homomorphism (p. 245), and its role in finding integer solutions to equations like

\[ x^2 + y^2 = 3z^2 \quad \text{or} \quad x^n + y^n = z^n \]

Definition

Let \( R \) be a commutative ring. An ideal \( P \) is a prime ideal if \( P \neq R \) and whenever \( ab \in P \), either \( a \in P \) or \( b \in P \).

Proposition

Let \( R \) be a commutative ring. The ideal \( P \) is a prime ideal if and only if \( R/P \) is an integral domain.
Generalizing the integers: Prime ideals

Ring theory in Number theory. For example, read about the reduction homomorphism (p. 245), and its role in finding integer solutions to equations like

\[ x^2 + y^2 = 3z^2 \quad \text{or} \quad x^n + y^n = z^n \]

Definition
Let \( R \) be a commutative ring. An ideal \( P \) is a **prime ideal** if \( P \neq R \) and whenever \( ab \in P \), either \( a \in P \) or \( b \in P \).

Proposition
Let \( R \) be a commutative ring. The ideal \( P \) is a prime ideal if and only if \( R/P \) is an integral domain.

Corollary
Let \( R \) be a commutative ring. Every maximal ideal of \( R \) is a prime ideal.
The many kinds of rings

Assume all rings $R$ have 1 for a moment.
We already know.

Commutative rings:
The many kinds of rings

Assume all rings $R$ have 1 for a moment.
We already know.

Commutative rings: multiplication is commutative.
Division rings:
The many kinds of rings

Assume all rings $R$ have 1 for a moment.
We already know.

- **Commutative rings:** multiplication is commutative.
- **Division rings:** $(R - \{0\}, \times)$ is a group.
- **Fields:**
The many kinds of rings

Assume all rings $R$ have 1 for a moment.
We already know.

Commutative rings: multiplication is commutative.
Division rings: $(R - \{0\}, \times)$ is a group.
Fields: $(R - \{0\}, \times)$ is an abelian group.

Integral domains (or domains, or IDs):

Principal ideal domains (PIDs): every ideal is principal.
Unique factorization domains (UFDs): elements factor uniquely into primes.
Euclidean domains (EDs): there's a division (i.e. Euclidean) algorithm.

You can show that $\text{ID's} \subseteq \text{UFDs} \subseteq \text{PIDs} \subseteq \text{EDs} \subseteq \text{Fields}$
The many kinds of rings

Assume all rings $R$ have 1 for a moment.
We already know.

Commutative rings: multiplication is commutative.
Division rings: $(R - \{0\}, \times)$ is a group.
Fields: $(R - \{0\}, \times)$ is an abelian group.
Integral domains (or domains, or IDs): no zero divisors (cancellation works).
The many kinds of rings

Assume all rings $R$ have 1 for a moment.

We already know.

- **Commutative rings:** multiplication is commutative.
- **Division rings:** $(R - \{0\}, \times)$ is a group.
- **Fields:** $(R - \{0\}, \times)$ is an abelian group.
- **Integral domains (or domains, or IDs):** no zero divisors (cancellation works).

**New:** the many kinds of (integral) domains.

- **Principal ideal domains (PIDs):** every ideal is principal.
- **Unique factorization domains (UFDs):** elements factor uniquely into primes.
- **Euclidean domains (EDs):** there's a division (i.e. Euclidean) algorithm.
The many kinds of rings

Assume all rings $R$ have 1 for a moment.

We already know.

- **Commutative rings**: multiplication is commutative.

- **Division rings**: $(R - \{0\}, \times)$ is a group.

- **Fields**: $(R - \{0\}, \times)$ is an abelian group.

- **Integral domains (or domains, or IDs)**: no zero divisors (cancellation works).

New: the many kinds of (integral) domains.

- **Principal ideal domains (PIDs)**: every ideal is principal.
The many kinds of rings

Assume all rings $R$ have 1 for a moment.

We already know.

- **Commutative rings:** multiplication is commutative.
- **Division rings:** $(R - \{0\}, \times)$ is a group.
- **Fields:** $(R - \{0\}, \times)$ is an abelian group.
- **Integral domains (or domains, or IDs):** no zero divisors (cancellation works).

New: the many kinds of (integral) domains.

- **Principal ideal domains (PIDs):** every ideal is principal.
- **Unique factorization domains (UFDs):** elements factor uniquely into primes.
The many kinds of rings

Assume all rings $R$ have 1 for a moment.

We already know.

- **Commutative rings:** multiplication is commutative.
- **Division rings:** $(R - \{0\}, \times)$ is a group.
- **Fields:** $(R - \{0\}, \times)$ is an abelian group.
- **Integral domains (or domains, or IDs):** no zero divisors (cancellation works).

**New: the many kinds of (integral) domains.**

- **Principal ideal domains (PIDs):** every ideal is principal.
- **Unique factorization domains (UFDs):** elements factor uniquely into primes.
- **Euclidean domains (EDs):** there's a division (i.e. Euclidean) algorithm.
The many kinds of rings

Assume all rings $R$ have 1 for a moment.

We already know.

**Commutative rings:** multiplication is commutative.

**Division rings:** $(R - \{0\}, \times)$ is a group.

**Fields:** $(R - \{0\}, \times)$ is an abelian group.

**Integral domains (or domains, or IDs):** no zero divisors (cancellation works).

**New: the many kinds of (integral) domains.**

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

**Unique factorization domains (UFDs):** elements factor uniquely into primes.

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

You can show that

$$\{ \text{ID’s} \} \subseteq \{ \text{UFDs} \} \subseteq \{ \text{PIDs}\} \subseteq \{ \text{EDs} \} \subseteq \{ \text{Fields}\}$$
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”

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

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

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

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

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

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”

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

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

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

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”

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

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

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

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

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

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

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

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

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

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

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!!
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

$$a = qb + r$$

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

with

$$N(r) < N(b).$$

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

with

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

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!!
(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

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

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 $a, b \in R$, $b \neq 0$, 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) $\mathbb{Z}[x]$ with $N(p(x)) = \deg(p(x))$. 