Section 27 – Prime and maximal ideals

Instructor: Yifan Yang

Spring 2007
Overview

- In Exercise 12 of Section 26, we show that a factor ring of an integral domain may be a field. For example, if $p$ is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

- Also, in Exercise 13 of the same section, we show that a factor ring of an integral domain may have a zero divisor. For example, if $n$ is composite, then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors.

- In this section, we will determine when a factor ring of an integral domain is again an integral, and when it becomes a field.

- We will then apply the results to the polynomial rings $F[x]$, where $F$ is a field.
Proper/improper and trivial/nontrivial ideals

Definition
Let \( R \) be a nonzero ring. The ideal \( \{0\} \) is the trivial ideal, and the ring \( R \) itself is the improper ideal. Any other ideal is a proper nontrivial ideal.
Theorem (27.5)
Let $R$ be a ring with unity. If an ideal $I$ contains a unit, then $I = R$.

Proof.
Let $u$ be a unit contained in $I$. Then $1 = u^{-1}u \in I$. It follows that $r = r1 \in I$ for all $r \in R$. □

Corollary (27.6)
A field contains no proper nontrivial ideals.

Proof.
Any nontrivial ideal of a field contains a unit. Then Theorem 27.5 says that the ideal must be the whole field. □
Maximal ideals

Definition (27.7)
A proper ideal $M$ of a ring $R$ is a maximal ideal such that there is no proper ideal $N$ of $R$ properly containing $M$. (That is, if $N$ is an ideal such that $M \subset N \subset R$, then $N = M$ or $N = R$.)

Example
Let $p$ be a prime. Then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.
When is $R/I$ a field?

**Theorem (27.9)**

Let $R$ be a commutative ring with unity. Then $M$ is a maximal ideal if and only if $R/M$ is a field.

**Corollary (27.11)**

A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

**Key observation**

Let $\phi : R \mapsto R'$ be a ring homomorphism with kernel $\text{Ker}(\phi)$. If $I'$ is a proper nontrivial ideal of $\phi(R)$, then $I = \phi^{-1}(I')$ is a proper ideal of $R$ with $\text{Ker}(\phi) \subsetneq I$. 
Proof of $M$ maximal $\iff R/M$ a field

- Let $M$ be a maximal ideal. We need to show that if $a + M \neq M$, then there exists $b + M$ such that $(a + M)(b + M) = 1 + M$.
- Equivalently, we need to show that the principal ideal $\langle a + M \rangle$ of $R/M$ is the whole ring $R/M$.
- Consider the canonical homomorphism $\gamma : R \to R/M$ defined by $\gamma(r) = r + M$.
- Now $\langle a + M \rangle$ is a nontrivial ideal since $a + M \neq M$.
- If $\langle a + M \rangle$ is also a proper ideal, then by the remark on the previous page, $\gamma^{-1}(\langle a + M \rangle)$ is a proper ideal containing properly $\ker(\gamma) = M$. This contradicts to the assumption that $M$ is a maximal ideal.
- Therefore, $\langle a + M \rangle = R/M$. This concludes the proof. $\square$
Proof of $R/M$ field $\iff M$ maximal

- Assume that $R/M$ is a field, and $N$ be an ideal of $R$ such that $M \subset N \subset R$. We need to prove that either $N = M$ or $N = R$.
- Consider the canonical homomorphism $\gamma : R \to R/M$ given by $\gamma : a \mapsto a + M$.
- Since $N$ is an ideal of $R$, $N/M = \gamma(N)$ is an ideal of $\phi(R) = R/M$.
- Since $R/M$ is a field, by Corollary 27.6, $N/M$ is either the trivial ideal $\{0 + M\}$ or the whole field $R/M$.
- The first case yields $N = M$, while the second case gives $N = R$. □
Prime ideals

Definition (27.13)
An ideal $P \neq R$ in a commutative ring is a prime ideal if $ab \in P$ implies $a \in P$ or $b \in P$.

Example

1. If $R$ is an integral domain, then $\{0\}$ is a prime ideal.
2. $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$.
3. Let $R = \mathbb{Z}$, and $n$ be a positive integer. If $n$ is composite, say $n = ab$ with $a, b > 1$, then $ab = n \in n\mathbb{Z}$, but $a, b \notin n\mathbb{Z}$, and $n\mathbb{Z}$ is not a prime ideal.
4. If $n = p$ is a prime and $ab \in p\mathbb{Z}$, then $p|ab$, which implies $p|a$ or $p|b$. Thus, $ab \in p\mathbb{Z}$ does imply $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. Therefore, $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. 
When is $R/I$ an integral domain?

**Theorem (27.15)**

Let $R$ be a commutative ring with unity. Then $P$ is a prime ideal of $R$ if and only if $R/P$ is an integral domain.

**Proof.**

$R/P$ is an integral domain

$\iff (a + P)(b + P) = 0 + P \Rightarrow a + P = 0 + P$ or $b + P = 0 + P$

$\iff ab \in P \Rightarrow a \in P$ or $b \in P$

$\iff P$ is a prime ideal.

$\square$
Maximal implies prime

Corollary (27.16)
Every maximal ideal in a commutative ring with unity is a prime ideal.

Example
The trivial ideal \{0\} of \( \mathbb{Z} \) is a prime ideal, but not a maximal ideal.
Examples of prime ideals

1. Let $R$ be an integral domain. Then $\{0\}$ is a prime ideal. We find $R/\{0\} \simeq R$ is indeed an integral domain.

2. Let $\mathbb{Z} \times \{0\}$ be a prime ideal of $\mathbb{Z} \times \mathbb{Z}$. Then we have $\mathbb{Z} \times \mathbb{Z}/(\mathbb{Z} \times \{0\}) \simeq \mathbb{Z}$, which is an integral domain.

3. Let $n$ be a composite number, then $n\mathbb{Z}$ is not a prime ideal, and $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ is not an integral domain.

4. Let $p$ be a prime, then $p\mathbb{Z}$ is a prime ideal, and $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ is an integral domain (actually a field).
Principal ideals

Definition (27.21)
Let $R$ be a commutative ring with unity, and $a \in R$. The ideal $\{ra : r \in R\}$ is the principal ideal generated by $a$, and is denoted by $\langle a \rangle$. An ideal $I$ of $R$ is a principal ideal if $I = \langle a \rangle$ for some $a \in R$.

Observations

- If $\langle a \rangle = R$, then $a$ is a unit since $1 \in R \Rightarrow ra = 1$ for some $r \in R$.
- Assume that $R$ is an integral domain. Then $\langle a \rangle = \langle b \rangle$ if and only if $b = ua$ for some unit $u \in R$. 
Ideals in $F[x]$

Theorem (27.24)

Let $F$ be a field. Then every ideal $I$ in $F[x]$ is principal.

Proof.

- If $I = \{0\}$, then $I = \langle 0 \rangle$ is principal.
- If $I \neq \{0\}$, let $g(x)$ be a nonzero element of $I$ of minimal degree. We claim that $I = \langle g(x) \rangle$.
- Let $f(x) \in I$. Using the division algorithm (Theorem 23.1), we find $f(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
- Now $r(x) = f(x) - q(x)g(x) \in I$. By the minimality of $\deg g(x)$, we must have $r(x) = 0$, instead of $\deg r(x) < \deg g(x)$.
- Thus, $f(x) = q(x)g(x) \in \langle g(x) \rangle$, and $I = \langle g(x) \rangle$. □
Maximal ideals in $F[x]$

**Theorem (27.25)**

An ideal $\langle p(x) \rangle \neq \{0\}$ in $F[x]$ is maximal if and only if $p(x)$ is irreducible over $F$.

**Corollary**

The factor ring $F[x]/\langle p(x) \rangle$ is a field if and only if $p(x)$ is irreducible over $F$.

**Remark**

Theorem 27.25 is extremely important in our study of the field theory.
Proof of $\Rightarrow$ in Theorem 27.25

- Let $\langle p(x) \rangle$ be a maximal ideal. We need to prove that
  - $p(x)$ is not a constant polynomial,
    - if $p(x) = f(x)g(x)$ then either $f(x)$ or $g(x)$ is a unit in $F[x]$.
  - If $p(x)$ is a nonzero constant polynomial, then $p(x)$ is a unit in $F[x]$ and by Theorem 27.5 $\langle p(x) \rangle = F[x]$, contradicting to the assumption. Thus, $p(x)$ is not a constant polynomial.
- Now suppose that $p(x) = f(x)g(x)$. Then $\langle p(x) \rangle \subset \langle f(x) \rangle$.
- Since $\langle p(x) \rangle$ is a maximal ideal, either $\langle f(x) \rangle = F[x]$ or $\langle f(x) \rangle = \langle p(x) \rangle$.
  - If $\langle f(x) \rangle = F[x]$, then $f(x)$ is a unit.
  - If $\langle f(x) \rangle = \langle p(x) \rangle$, then $f(x) \in \langle p(x) \rangle$ and $f(x) = p(x)h(x)$ for some $h(x) \in F[x]$.
- Then $p(x) = f(x)g(x) = p(x)[h(x)g(x)]$, and $h(x)g(x) = 1$. Thus, $g(x)$ is a unit. □
Proof of \( \Rightarrow \) in Theorem 27.25

- Assume that \( p(x) \) is irreducible over \( F \). We need to prove that
  - \( \langle p(x) \rangle \neq F[x] \),
  - if \( I \) is an ideal such that \( \langle p(x) \rangle \subset I \subset F[x] \), then either \( I = \langle p(x) \rangle \) or \( I = F[x] \).
- If \( \langle p(x) \rangle = F[x] \), then \( p(x) \) is a unit in \( F[x] \). By definition, a unit is not an irreducible. Thus, \( \langle p(x) \rangle \neq F[x] \).
- Assume that \( \langle p(x) \rangle \subset I \subset F[x] \). We have \( I = \langle f(x) \rangle \) for some \( f(x) \in F[x] \).
- Since \( \langle p(x) \rangle \subset \langle f(x) \rangle \), we have \( p(x) = f(x)g(x) \) for some \( g(x) \in F[x] \).
- Because \( p(x) \) is irreducible, either \( f(x) \) or \( g(x) \) is a unit.
- If \( f(x) \) is a unit, then \( I = \langle f(x) \rangle = F[x] \). If \( g(x) \) is a unit, then \( \langle f(x) \rangle = \langle p(x) \rangle \).
\[ \square. \]
Unique factorization in $F[x]$

Theorem (27.27)

Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)|r(x)s(x)$ for some $r(x), s(x) \in F[x]$, then $p(x)|r(x)$ or $p(x)|s(x)$.

Proof.

If $p(x)|r(x)s(x)$, then $r(x)s(x) \in \langle p(x) \rangle$. By Theorem 27.25, $\langle p(x) \rangle$ is a maximal ideal, which by Corollary 27.16, is a prime ideal. Thus, $r(x) \in \langle p(x) \rangle$ or $s(x) \in \langle p(x) \rangle$, which in turn implies that $p(x)|r(x)$ or $p(x)|s(x)$. 

□
Homework

1. Problems 4, 8, 15–18, 30, 34, 35 of Section 27.
2. Give an example where $I$ and $J$ are ideals of a ring $R$, but the set
   \[ \{ ab : a \in I, \; b \in J \} \]
   is not an ideal of $R$. (Compare this with Problem 35.)