Introduction to Rings and Modules

Lecture 6, Monday May 1 2023
Ari Feiglin

6.1 Prime Ideals

Definition 6.1.1:

Let R be a commutative ring, a proper ideal $I \triangleleft R$ is **prime** if for every $a, b \in R$ if $ab \in I$ then $a \in I$ or $b \in I$.

Example 6.1.2:

(1) Notice then that if p is prime, then $p\mathbb{Z}$ is a prime ideal. This is because if $nm \in p\mathbb{Z}$ then p divides nm and therefore divides n or m and so one is in $p\mathbb{Z}$.
And if n is not prime then suppose p is a prime which divides n, then $p \cdot \frac{n}{p} \in n\mathbb{Z}$ but neither p nor $\frac{n}{p}$ are in $n\mathbb{Z}$, so $n\mathbb{Z}$ is not prime. So the only prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$.

(2) And $\{0\}$ is a prime ideal if and only if R is an integral domain. This is because $ab = 0$ if and only if $ab \in I$.

Proposition 6.1.3:

Let R be a commutative ring, and $I \trianglelefteq R$. The following are equivalent:

(1) I is a prime ideal.

(2) For any $J, J' \trianglelefteq R$, if $JJ' \subseteq I$ then $J \subseteq I$ or $J' \subseteq I$.

(3) ${}^{R}\!/_{I}$ is an integral domain.

Proof:

We show the first equivalence. Suppose that there is an $a \in J$ which isn't in I and a $b \in J'$ which isn't in I. But $ab \in JJ' \subseteq I$ and since I is prime, $a \in I$ or $b \in I$.
Now we show the second equivalence. Suppose that

$$(r + I)(r' + I) = I \implies rr' + I = I$$

then $rr' \in I$ so one must be in I, so one of $r + I$ or $r' + I$ is 0, so ${}^{R}\!/_{I}$ is an integral domain.
We show that the third implies the first. Suppose $ab \in I$ then $(a + I)(b + I) = ab + I = 0_{{}^{R}\!/_{I}}$. But since ${}^{R}\!/_{I}$ is an integral domain, $a + I$ or $b + I$ must be 0 so either $a \in I$ or $b \in I$ as required. ∎

Example 6.1.4:

Let $R = \mathbb{Z}[x]$ and $I = (2) = \{2f(x) \mid f(x) \in \mathbb{Z}[x]\}$. Then we can form a ring homomorphism $\varphi\colon \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$ by

$$\varphi\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} [a_k] x^k$$

This is obviously a group homomorphism, and it preserves multiplication as

$$\varphi\left(\left(\sum_{k=0}^{n} a_k x^k\right) \cdot \left(\sum_{k=0}^{n} b_k x^k\right)\right) = \varphi\left(\sum_{k=0}^{2n} x^k \sum_{i=0}^{k} a_i b_{k-i}\right) = \sum_{k=0}^{2n} x^k \sum_{i=0}^{k} [a_i b_{k-i}]$$

which is equal to the product of the images of the polynomials under φ.

The kernel of this homomorphism is the set of polynomials with even coefficients, $\{p \in \mathbb{Z}[x] \mid p_k \in 2\mathbb{Z}\} = (2)$. So by the first isomorphism theorem

$$\mathbb{Z}[x] \big/ (2) \cong \mathbb{Z}_2[x]$$

Since $\mathbb{Z}_2$ is an integral domain, so is $\mathbb{Z}_2[x]$ and therefore $\mathbb{Z}[x]/(2)$ is an integral domain so (2) is prime.

Example 6.1.5:

Since we showed that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, (x) is also a prime ideal.
And $(2, x)$ (the ideal generated by 2 and x, which is $(2) + (x)$) then we can map elements of $f \in \mathbb{Z}[x]$ to $[f(0)] \in \mathbb{Z}_2$. Then the kernel of this is are polynomials with even free coefficients, which is $(2) + (x)$. Thus $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}_2$ by the first isomorphism theorem, so $(2, x)$ is prime.

Notice then that we have the following proper chain of prime ideals:

$$(0) \subset (x) \subset (2, x)$$

Definition 6.1.6:

Let R be a ring, and I a proper (left/right/bidirectional) ideal. I is **maximal** if it is not contained in any other proper (left/right/bidirectional) ideal.

We recall Zorn's Lemma:

Lemma 6.1.7:

Let $(P, \leq)$ be a non-empty partial-ordered set. If every chain in P ($p_1 \leq p_2 \leq p_3 \leq \dots$) has an upper bound (an $M \in P$ such that for every n, $p_n \leq M$), then S has a maximal element (an element $s \in P$ such that for every $t \neq s$, $s \not\leq t$).

(This is equivalent to the axiom of choice).

Proposition 6.1.8:

Let R be a ring and I be a proper (left/right/bidirectional) ideal, then there exists a maximal (left/right/bidirectional) ideal M such that $I \subseteq M$.

Proof:

We will prove this for left ideals. Let

$$P = \{J \triangleleft R \mid I \subseteq J\}$$

be a partially ordered set under the partial order of inclusion ($\subseteq$). Let $J_1 \subseteq J_2 \subseteq \cdots$ be a chain in P, then let

$$M = \bigcup_{n=1}^{\infty} J_n$$

M is a group (the union of an ascending chain of subgroups is a group) since if $a, b \in M$ then there exists a J_n such that $a, b \in J_n$ (since we can take the maximum between the indexes of the ideals where we find a and b), so $a + b \in J_n$ and so $a + b \in M$ and so M is closed under addition. And if $a \in M$, then $a \in J_n$ for some n and so $-a \in J_n \subseteq M$.
And M is closed under left multiplication by R since if $a \in M$, there exists some n where $a \in J_n$ so $Ra \subseteq J_n \subseteq M$.
Now we must also show that M is proper, that is $M \neq R$. If $M = R$ then $1 \in M$ so there would exist a J_n with $1 \in J_n$ which means that $J_n = R$ and so J_n is not proper, which is a contradiction (since P is a set of proper ideals).
And since $I \subseteq M$, $M \in P$ and M is clearly an upper bound for the chain.
So every chain in P has an upper bound, and so P has a maximal element M. This maximal element is clearly a maximal ideal containing I as for any proper ideal J, if $M \subseteq J$ then $J \in P$ so $M = J$ since M is maximal in P. ■

Example 6.1.9:

This claim is not true for rngs. Let $(G, +)$ be an abelian group and define $g \cdot h = 0$, then $(G, +, \cdot)$ is an rng. Since any subgroup of G is an ideal (since it contains 0, so it is closed under multiplication by G), and any ideal of G is necessarily a subgroup. So we can look for an abelian group G which has no maximal (proper) subgroups.
We can choose $(\mathbb{Q}, +)$ as our group. Suppose $H < \mathbb{Q}$ is a maximal proper subgroup. Then there exists an $x \notin \mathbb{Q}$ and $0 \neq y \in \mathbb{Q}$, then let $\frac{y}{x} = \frac{a}{b}$ for integers a, b. Then $a \neq 0$ and $\frac{x}{a} \notin H + \langle x \rangle$ since if it were then $x = ah + anx = ah + bny \in H$ which contradicts that $x \notin H$. So $H \subset H + \langle x \rangle \subset \mathbb{Q}$, so H is not maximal.

Theorem 6.1.10 (The Correspondence Theorem):

Suppose I is some ideal of R, let $\mathcal{G} = \{J \trianglelefteq R \mid I \subseteq J\}$ and $\mathcal{N} = \left\{ {}^{J}\!/_{I} \trianglelefteq {}^{R}\!/_{I} \right\}$, then there is an inclusion-preserving bijection between $\mathcal{G}$ and $\mathcal{N}$.

Proof:

We will focus on left ideals.
We define the mapping

$$\varphi\colon \mathcal{G} \longrightarrow \mathcal{N}, \qquad \varphi(J) = {}^{J}\!\Big/_{I}$$

This is well defined since I is an ideal of J's, and if $j + I \in {}^{J}\!/_{I}$ and $r + I \in {}^{R}\!/_{I}$:

$$(r + I)(j + I) = rj + I = j' + I \in {}^{J}\!\Big/_{I}$$

Since J is an ideal of R's.
Note that since an ideal of ${}^{R}\!/_{I}$ is a subgroup of ${}^{R}\!/_{I}$, it must have the form ${}^{J}\!/_{I}$ for some $I \leq J \leq R$ ($\leq$ meaning subgroup here) by the correspondence theorem for groups. We now claim that J is an ideal, let $r \in R$ and $j \in J$, since

$$(r + I)(j + I) \in {}^{J}\!\Big/_{I} \implies rj \in J$$

So J is indeed an ideal. So we can explicitly find the inverse of φ:

$$\varphi^{-1}\left({}^{J}\!\Big/_{I}\right) = J$$

This is well-defined as explained above and obviously the inverse of φ.
So φ is a bijection, and it is obviously inclusion-preserving. ∎

Notice that we showed that J is an ideal of R containing I if and only if ${}^{J}\!/_{I}$ is an ideal of ${}^{R}\!/_{I}$.

Proposition 6.1.11:

Let R be a commutative ring and $I \triangleleft R$ a proper ideal. Then I is maximal if and only if ${}^{R}\!/_{I}$ is a field.

Proof:

Notice that I is maximal if and only if the set of ideals containing I is $\mathcal{G} = \{I, R\}$ and by **The Correspondence Theorem** this is if and only if the ideals of ${}^{R}\!/_{I}$ are $\mathcal{N} = \left\{0, {}^{R}\!/_{I}\right\}$.
And so we will show that F is a field if and only if it has trivial ideals. If F is a field, then if $\{0\} \neq I$ is an ideal of F, then there is a non-zero $x \in I$, since $x^{-1} \in F$ this means $xx^{-1} = 1 \in I$ so $I = F$. And if F is not a field then there exists an $x \in F$ without a multiplicative inverse. Then if $1 \in (x)$ this means that there exists a $y \in F$ with $yx = 1$, and since R is commutative this means $yx = xy = 1$ so y is x's multiplicative inverse in contradiction. So $1 \notin (x)$ so $\{0\} \neq (x) \neq F$, so if F is not a field there exist non-trivial ideals.
Thus since I is maximal if and only if ${}^{R}\!/_{I}$ only has trivial ideals, I is maximal if and only if ${}^{R}\!/_{I}$ is a field. ∎

We showed in our proof that a commutative ring is a field if and only if it has trivial ideals, which is important as well.

Corollary 6.1.12:

If R is a commutative ring then every maximal ideal is prime.

Proof:

We know that I is a maximal ideal if and only if ${}^{R}\!/_{I}$ is a field, which means ${}^{R}\!/_{I}$ is an integral domain, which means that I is a prime ideal. ∎

Definition 6.1.13:

We call ideals generated by a single element **principal ideals**. If R is a ring in which every (left/right/bidirectional) ideal is principal is a **principal (left/right/bidirectional) ideal ring** If a principle ideal ring is also an integral domain, it is called a **principle ideal domain** (PID).

Note that the trivial ideals are principal:

$$\{0\} = (0), \quad R = (1)$$

Example 6.1.14:

(1) Since the ideals of a field are trivial, all fields are principal ideal domains.

(2) $\mathbb{Z}$ is also a principal ideal domain since all of its ideals are of the form $n\mathbb{Z} = (n)$.

Proposition 6.1.15:

Let R be a principal ideal domain, and let P be a non-zero prime ideal. Then P is maximal.

Proof:

We know that there exists a maximal ideal M such that $P \subseteq M$. Since R is a principal ideal domain, $P = (p)$ and $M = (m)$, and so $p = rm \in P$. Thus $r \in P$ or $m \in P$. If $r \in P$ then $r = tp$, and since $p = rm = tpm = ptm$ (R is an integral domain), this means $p(1 - tm) = 0$. And since R is an integral domain, $1 - tm = 0$ (since $P \neq 0$ so $p \neq 0$). So $tm = 1$ and so $1 \in (m) = M$ which means $M = R$ which is a contradiction since M is a proper ideal.
Therefore $m \in P$ and so $M = (m) \subseteq P$ which means $P = M$ so P is maximal. ∎

Notice that during this proof we showed the following:

Proposition 6.1.16:

Let R be an integral domain and $P \trianglelefteq R$ a non-zero prime ideal. Then if $M \triangleleft R$ is a proper principal ideal such that $P \subseteq M$, then $M = P$.
That is, proper principal ideals do not (properly) contain any non-zero prime ideals.

Since we showed $(x) \subset (2, x) \subset \mathbb{Z}[x]$ in $\mathbb{Z}[x]$, and (x) and $(2, x)$ are non-zero prime ideals, $\mathbb{Z}[x]$ is not a principal ideal domain since (x) is not maximal.
And furthermore $(2, x)$ is not a principal ideal since $(x) \subset (2, x)$, so it contains a non-zero prime ideal (x).

Definition 6.1.17:

Let R be a commutative ring. The **dimension** of R is the largest number d such that there exists a proper chain of prime ideals

$$P_0 \subset P_1 \subset \cdots \subset P_{d-1} \subset P_d$$

(The dimension of R is one less than the length of the chain.)
If there doesn't exist a largest d, then R has infinite dimension.

Thus R is a field if and only if $\dim R = 0$. This is because R is a field if and only if it has trivial ideals, and since if R has a non-trivial ideal it has a prime ideal (since maximal ideals are prime), R is a field if and only if its only prime ideal is $\{0\}$, and so the only chain in a field is a chain of length 1.

Proposition 6.1.18:

If R is a prime ideal domain, $\dim R \leq 1$.

Proof:

Since if $P \trianglelefteq R$ is a non-zero prime ideal, P is maximal, the only prime ideal chains we can form are of the form

$$\{0\} \subseteq P$$

Which has length 2 or 1 depending on whether P is zero or not. So $\dim R$ is 1 or 0. ■