In the previous lecture we defined prime and maximal ideals.

The following lemma gives us the connection between these proper ideals and the corresponding factor ring.

**Lemma.** Suppose $A$ is a unital commutative ring and $I \triangleleft A$.

1. $I$ is prime $\iff$ $A/I$ is an integral domain.

2. $I$ is maximal $\iff$ $A/I$ is a field.

**Proof.** (1) ($\implies$) Since $I$ is prime, it is proper. And so $A/I$ is not the trivial ring.

   $(a+I)(b+I) = 0+I \Rightarrow ab+I = 0+I \Rightarrow ab \in I$

   $\Rightarrow a \in I$ or $b \in I$

   $\Rightarrow a+I = 0$ or $b+I = 0$

   So $A/I$ has no zero-divisor.

(\iff) $A/I$ is an integral domain $\Rightarrow A/I$ is not the trivial ring

$\Rightarrow I \neq A$.

- $ab \in I \Rightarrow (a+I)(b+I) = 0 \Rightarrow a+I = 0$ or $b+I = 0$

  $\Rightarrow a \in I$ or $b \in I$.

(2) ($\implies$) Since $I$ is maximal, it is a proper ideal; and so $A/I$ is
not the trivial ring. Suppose \( \alpha + I \neq 0 \). Then \( \alpha \notin I \). So
\( I \not\subseteq \langle \alpha \rangle + I \triangleleft A \). By maximality of \( I \), we deduce that
\( \langle \alpha \rangle + I = A \); and so \( \exists \beta \in A \) and \( c \in I \) s.t. \( ab + c = 1 \).
This implies \( (a + I)(b + I) = 1 + I \); and that means \( a + I \) is
a unit; and so \( A/I \) is a field.

(\( \Leftarrow \)) Since \( A/I \) is a field, it is a non-trivial ring. And so \( I \) is
a proper ideal. Suppose \( I \not\subseteq J \triangleleft A \). Let \( a \in A \setminus I \). Then
\( a + I \) is a unit in \( A/I \). So \( \exists \beta \in A \) s.t. \( (a + I)(b + I) = 1 + I \).
Therefore \( \exists c \in I \) s.t. \( ab + c = 1 \), which implies
\( 1 = ab + c \in \langle \alpha \rangle + I \subseteq J \); and so \( J = A \). Thus \( I \) is
a maximal ideal. \( \blacksquare \)

Corollary. \( \text{Max}(A) \subseteq \text{Spec}(A) \).

\( \text{Pr.} \) \( \text{The Max}(A) \Rightarrow A/I_{\alpha} \) is a field \( \Rightarrow A/I_{\alpha} \) is an integral domain
\( \Rightarrow \alpha \in \text{Spec}(A) \). \( \blacksquare \)

Cor. \( \forall \mathfrak{p} \in \text{Spec}(A) \) and \( |A/I_{\mathfrak{p}}| < \infty \) \( \Rightarrow \mathfrak{p} \in \text{Max}(A) \).
Lecture 17: Zorn's lemma

Thursday, December 6, 2018 11:09 PM

Proposition: \( \text{Spec}(A) \Rightarrow A_{\mathfrak{p}} \) is an integral domain \( \Rightarrow \)
\( |A_{\mathfrak{p}}| < \infty \)

Next we will find lots of prime and maximal ideals. To show this we use Zorn’s lemma. This result is equivalent to axiom of choice.

Definition: A non-empty set \( \Sigma \) with a relation \( \leq \) is called a Partially Ordered Set (\( \text{POSet} \)) if

\[-a \leq a, \ a \leq b, b \leq c \Rightarrow a \leq c.\]

Definition: Suppose \((\Sigma, \leq)\) is a poset. A non-empty subset \( C \) of \( \Sigma \) is called a chain if \( \forall a, b \in C \), either \( a \leq b \) or \( b \leq a \).

(H is also called a totally ordered set.)

Definition: Suppose \((\Sigma, \leq)\) is a poset, and \( \Delta \) is a non-empty subset of \( \Sigma \). We say \( a \in \Sigma \) is an upper bound of \( \Delta \) if \( \forall b \in \Delta, b \leq a \).
Def. Suppose \((\Sigma, \preceq)\) is a poset, \(a \in \Sigma\) is called a maximal element of \(\Sigma\) if \(a \preceq b\) implies \(a = b\).

Zorn’s lemma. Suppose \((\Sigma, \preceq)\) is a poset. If any chain \(C \subseteq \Sigma\) has an upper bound, then \(\Sigma\) has a maximal element.

Proof of the next theorem is a good example of how Zorn’s lemma can be used in algebra.

Def. Suppose \(A\) is a unital commutative ring. A subset \(S \subseteq A\) is called \textit{multiplicatively closed} if \(1 \in S\) and
\[ s_1, s_2 \in S \implies s_1 s_2 \in S. \]

Theorem. Suppose \(A\) is a unital commutative ring, \(S \subseteq A\) is multiplicatively closed, \(\mathcal{U} \triangleleft A\), and \(\mathcal{U} \cap S = \emptyset\). Let
\[ \sum_{\mathcal{U}, S} := \{ b \in A \mid \alpha \in \mathcal{U} \cdot b \in \mathcal{U} \cap S = \emptyset \} . \]

1. \(\sum_{\mathcal{U}, S}\) has a maximal element \( \alpha \) s.t. \( \mathcal{U} \subseteq \langle \alpha \rangle \).
2. If \( \alpha \in \sum_{\mathcal{U}, S}\) is a maximal element of \(\sum_{\mathcal{U}, S}\), then \( \alpha \) is prime.

In particular, \( \text{Spec}(A) \cap \sum_{\mathcal{U}, S} \neq \emptyset \).
Cor. Suppose \( \mathfrak{A} \neq \emptyset \). Then \( \exists \mathfrak{a} \in \text{Max} A \) s.t. \( \mathfrak{A} \subseteq \mathfrak{a} \).

\textbf{Pf.} of Cor. Since \( \mathfrak{A} \neq \emptyset \), \( \exists \mathfrak{a} \cap \emptyset = \emptyset \). By part (1) of the previous theorem, \( \sum_{\mathfrak{A}, \mathfrak{S}} \) has a maximal element \( \mathfrak{a} \).

\textbf{Claim.} \( \mathfrak{a} \in \text{Max}(A) \).

\textbf{Pf.} of Claim. Suppose \( \mathfrak{a} \subseteq \mathfrak{a}' \neq \emptyset \). Then \( \emptyset \subseteq \mathfrak{a} \subseteq \mathfrak{a}' \subseteq \mathfrak{a} \) and \( \mathfrak{a}' \cap \emptyset = \emptyset \). Hence \( \mathfrak{a}' \in \sum_{\mathfrak{A}, \mathfrak{S}} \) since \( \emptyset \) is a maximal element of \( \sum_{\mathfrak{A}, \mathfrak{S}} \), we deduce that \( \mathfrak{a} = \mathfrak{a}' \).

\textbf{Pf.} of Theorem. (a) By Zorn's lemma it is enough to show any chain \( C \subseteq \sum_{\mathfrak{A}, \mathfrak{S}} \) has an upper bound.

\textbf{Claim1.} \( U \) \( \mathfrak{b} \) is an ideal of \( A \). (This is true for any chain \( \{ \mathfrak{b} \} \) of ideals, and usually this is how Zorn's lemma is used in ring theory.)

\textbf{Pf.} of Claim1. \( a_1, a_2 \in U \mathfrak{b} \Rightarrow \exists b_1, b_2 \in C \) s.t. \( a_1 \in b_1 \) \( \cap \mathfrak{b} \Rightarrow a_2 \in b_2 \), \( C \) is a chain \( \Rightarrow \) either \( b_1 \subseteq b_2 \) or \( b_2 \subseteq b_1 \) either \( a_1, a_2 \in b_1 \) or \( a_1, a_2 \in b_2 \Rightarrow a_1 + a_2 \in b_1 \cup b_2 \Rightarrow a_1 + a_2 \in U \mathfrak{b} \).
Lecture 17: Existence of prime ideals
Friday, December 7, 2018  8:14 AM

\[ \text{Claim 1.} \quad \text{Let } A \subseteq \mathfrak{A}, a \in A. \] 
\[ \exists b \in \mathfrak{A} \text{ s.t. } a \in b. \] 
\[ \Rightarrow a \in \bigcup_{b \in \mathfrak{A}} b. \] 
\[ \Rightarrow \exists b \in \mathfrak{A} \text{ s.t. } a \in b. \] 
\[ \quad \text{Claim 2. If } C \subseteq \bigcup_{\mathfrak{A}, \mathfrak{S}} \text{ is a chain, then } \bigcup_{b \in \mathfrak{A}} b \in C. \] 
\[ \text{Proof of Claim 2.} \quad \text{By Claim 1, } U \supseteq A. \] 
\[ \text{For any } b \in C, \quad U \supseteq b. \] 
\[ \text{And } \bigcup_{b \in \mathfrak{A}} (b \cap S) = \emptyset; \text{ and claim follows.} \] 
\[ \text{Claim 2.} \] 

By Claim 2, for any chain \( C \subseteq \bigcup_{\mathfrak{A}, \mathfrak{S}} \), \( \bigcup_{b \in C} b \) is an upper bound of \( C \). And so by Zorn’s lemma \( \bigcup_{\mathfrak{A}, \mathfrak{S}} \) has a maximal element. 

\[ \text{(part c1)} \]

(2) Suppose \( \mathfrak{p} \in \bigcup_{\mathfrak{A}, \mathfrak{S}} \) is maximal in \( \bigcup_{\mathfrak{A}, \mathfrak{S}} \). And suppose to the contrary \( \mathfrak{p} \) is not prime. So \( \exists a, b \in \mathfrak{A} \) s.t.
\[ a, b \notin \mathfrak{p} \] and \( ab \in \mathfrak{p} \). Hence \( \mathfrak{p} \not\subset \langle a \rangle \) and \( \mathfrak{p} \not\subset \langle b \rangle \).

By maximality of \( \mathfrak{p} \), we deduce that \( \mathfrak{p} + \langle a \rangle, \mathfrak{p} + \langle b \rangle \notin \bigcup_{\mathfrak{A}, \mathfrak{S}} \).

Since \( \mathfrak{p} + \langle a \rangle, \mathfrak{p} + \langle b \rangle \) are ideals of \( A \) that contain \( \mathfrak{p} \), we have
a subset, we deduce that \( p + \langle a \rangle \cap S \neq \emptyset \) and \( p + \langle b \rangle \cap S \neq \emptyset \).

Say \( s_1 \in p + \langle a \rangle \) and \( s_2 \in p + \langle b \rangle \). Then

\[
\exists p_1, r_1 \in A, \quad s_1 = p_1 + ar_1 \implies S \ni s_2 = p_1(p_2 + br_2) + (ar_1)p_2 + (ar_1)(br_2) \in p.
\]

\[
\implies s_1 s_2 \in p \cap S \text{ which contradicts } p \in \sum_{a, s}. \quad \text{as above}
\]

**Def.** \( \text{Nil}(A) := \{ a \in A \mid a^n = 0 \text{ for some } n \in \mathbb{Z}^+ \} \)

is called the nilradical of \( A \); and \( a \in A \) is called nilpotent if \( a^n = 0 \) for some \( n \in \mathbb{Z}^+ \). (So \( \text{Nil}(A) \) consists of nilpotent elements of \( A \).)

**Theorem.**

1. \( \text{Nil}(A) \subseteq A \)
2. \( \text{Nil}(A) = \bigcap_{p \in \text{Spec } A} p \).

**Proof.**

1. \( a, b \in \text{Nil}(A) \implies \exists n, m \in \mathbb{Z}^+, a^n = b^m = 0 \)

\[
\implies (a + b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} = 0.
\]

Either \( i \geq n \) or \( n+m-i \geq m \),

\[a^i = 0 \quad \text{or} \quad b^{n+m-i} = 0\]

\[\implies a + b \in \text{Nil}(A)\]
\[ a \in \text{Nil}(A), \; \text{re} A \Rightarrow \begin{cases} a^n = 0 \quad \text{for some } n \in \mathbb{Z}^+ \Rightarrow (ra)^n = 0 \\ r \in A \end{cases} \]

\[ \Rightarrow ra \in \text{Nil}(A). \]

(2) \( a \in \text{Nil}(A) \Rightarrow \exists n \in \mathbb{Z}^+, \; a^n = 0 \]

\[ \Rightarrow \forall p \in \text{Spec } A, \; a^n \in p \]

\[ \Rightarrow \text{By induction on } n, \; a \in p \]

\[ a^n = a \cdot a^{n-1} \in p \Rightarrow \text{either } a \in p \text{ or } a^{n-1} \in p. \]

\[ \Rightarrow a \in \bigcap_{p \in \text{Spec } A} p. \]

\[ \text{Suppose to the contrary that } \exists a \in \bigcap_{p \in \text{Spec } A} p \setminus \text{Nil}(A). \]

Then \( S_a := \{1, a, a^2, \ldots, a^n \} \) is a multiplicatively closed set that does not contain 0. So by the previous theorem \( \exists p_0 \in \text{Spec } A \cap \bigcup_{a} S_a \)

but this means \( p_0 \cap S_a = \emptyset \), which implies \( a \notin p_0 \). And this

contradicts (2). \[ \square \]