Math 250A Lecture 10 Notes

Daniel Raban

September 28, 2017

1 Prime Ideals and Maximal Ideals

1.1 Fields and integral domains

Definition 1.1. A *field* is a commutative ring where all nonzero elements have multiplicative inverses.

Definition 1.2. An *integral domain* is a ring where $ab = 0$ implies that $a = 0$ or $b = 0$.

Proposition 1.1. *All fields are integral domains.*

Proof. Let R be a field. Then for $a, b \in R$,

$$ab = 0 \implies a^{-1}ab = a^{-1}0 \implies b = 0.$$

□

Definition 1.3. Let I be an ideal of R. I is called *maximal* if R/I is a field.

Definition 1.4. Let I be an ideal of R. I is called *prime* if R/I is an integral domain. Equivalently, I is prime if $ab \in I$ implies that $a \in I$ or $b \in I$.

Why are these definitions equivalent?

$$\begin{aligned} R/I \text{ is an integral domain} &\iff [(a+I)(b+I) = I \implies a \in I \text{ or } b \in I] \\ &\iff [ab + I = I \implies a \in I \text{ or } b \in I] \\ &\iff [ab \in I \implies a \in I \text{ or } b \in I]. \end{aligned}$$

We can see by the previous proposition that all maximal ideals are prime.

Definition 1.5. An ideal $I \neq R$ is *maximal* if for any ideal J, $I \subseteq J$ implies that $I = J$ or $J = R$.

Proposition 1.2. *Let I be an ideal of a ring R. Then R/I is a field iff I is maximal.*

Proof. Suppose I is maximal. Since $I \neq R$, $1 \notin I$, so R/I contains an element $1 + I \neq I$. Letting $x + I \in R/I$, note that $I + Ax = R$, so there exists some $y \in I$ and $a \in R$ such that $y + ax = 1$. Then $ax + I = 1 + I$, so $(a + I)$ is the inverse of $x + I$ in R/I. So R/I is a field.

Conversely, suppose R/I is a field. Then for $x \notin I$, there exists some $a \notin I$ such that $ax + I = 1 + I$. Then $ax + y = 1$ for some $y \in I$, so $(1) \subseteq Ax + I$, which makes $Ax + I = R$. This holds for all $x \notin I$, so I is maximal. $\square$

Example 1.1. Let $R = \mathbb{Z}$. The ideals are of the form (n) for $n = 0, 1, 2, 3, \dots$. The maximal ideals are $(2), (3), (5), (7), \dots$. The prime ideals are $(0), (2), (3), (5), (7), \dots$.

Example 1.2. Let $R = \mathbb{C}[x]$; this is a PID. The ideals are (f) for a polynomial f. The maximal ideals are $(x - a)$ for $a \in \mathbb{C}$ (any polynomial f of degree > 1 factorizes as $f = gh$, so $(f) \subsetneq (g)$, making (f) not maximal). The prime ideals are $(x - a)$ for $a \in \mathbb{C}$, and (0).

Example 1.3. Let $R = \mathbb{C}[x, y]$. The ideal (x, y) is maximal because $R/(x, y) = \mathbb{C}$, which is a field. The ideals $(x - a, y - b)$ are also maximal. These are the only maximal ideals.[1] The prime ideals are $(x - a, y - b)$, (0), and (f) if f is any irreducible polynomial; this is because $\mathbb{C}[x, y]/(f)$ is an integral domain because $\mathbb{C}[x, y]$ is a UFD.

1.2 Maximal ideals and Zorn's lemma

Definition 1.6. A *partial order* is a relation $\leq$ on a set S such that for all $a, b, c \in S$

1. $a \leq a$ (reflexivity).
2. If $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry).
3. If $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity).

Example 1.4. Let S be the set of subsets of some set T. The ordering $\leq$ is inclusion.

Definition 1.7. Let S be a partially ordered set. A *totally ordered* subset T of S is a subset such that for all $a, b \in T$, $a \leq b$ or $b \leq a$.

Definition 1.8. Let S be a partially ordered set. An *upper bound* of a subset T is an element $a \in S$ such that $b \leq a$ for all $b \in T$.

Definition 1.9. Let S be a partially ordered set. An element $a \in S$ is *maximal*[2] if $a \leq b$ implies that $b = a$.

Lemma 1.1 (Zorn)**.** *Suppose S is a nonempty partially ordered set such that for any totally ordered subset of S, there is an upper bound. Then S has a maximal element.*

[1] See Hilbert's Nullstellensatz. This word means zero position theorem.

[2] You might think that maximal should mean that $b \leq a$ for all $b \in S$, but this is a very strong condition. This implies a unique maximal element, which is not true for our definition of maximality.

Proof. We will sketch a proof because a full proof requires some set theory. Suppose no maximal element exists; we will find a contradiction.

Step 1: Pick $s_0 \in S$ since S is nonempty. Then $\{s_0\}$ is totally ordered, so it has an upper bound s_1. If s_0 is not maximal, then $s_1 > s_0$.

Step 2: Repeat this with $\{s_0, s_1\}$, which is totally ordered. And repeat this.

Step 3: We do this infinitely many times[3], and find s_ω, which is an upper bound of $\{s_0, s_1, s_2, \ldots\}$.

Step 4. We find an s_α for every ordinal α. But the set of ordinals is a proper class, so it must be bigger than S since S is a set. So we have a contradiction. □

Corollary 1.1. *If I is an ideal of R with $I \neq R$, I is contained in some maximal ideal.*

Proof. Look at the set S of ideals $\neq R$ containing I. It is partially ordered by $\subseteq$ and is nonempty because it contains I. Now suppose I_α is a totally ordered set of ideals; then $\bigcup_\alpha I_\alpha$ is an ideal and is greater than I_α for each α. Why is this an ideal? The total ordering is key. If $a, b \in \bigcup_\alpha I_\alpha$, then $a \in I_{\alpha_1}$ and $b \in I_{\alpha_2}$; without loss of generality, $I_{\alpha_1} \subseteq I_{\alpha_2}$, so $a + b \in I_{\alpha_2}$. This is the upper bound needed to satisfy the conditions of Zorn's lemma. □

Remark 1.1. You may be wondering why we need Zorn's lemma. In general, there exist nonempty ordered sets with no maximal elements. For example, take the open unit interval, $(0, 1)$.[4]

Corollary 1.2. *The intersection of all prime ideals of a ring is the set of elements x with $x^n = 0$ for some n (called nilpotent).*

Proof. Let $\mathfrak{p}$ be a prime ideal. If $x^n = 0$, then $x^{n-1}x = x^n = 0 \in \mathfrak{p}$, so since $\mathfrak{p}$ is prime, $x^{n-1} \in \mathfrak{p}$ or $x \in \mathfrak{p}$, and so on, so $x \in \mathfrak{p}$.

Suppose x is not nilpotent; we need to find a prime ideal P not containing x. Let $M = \left\{1, x, x^2, \ldots\right\}$, which doesn't contain 0 because x is not nilpotent. Let S be the set of ideals disjoint from M. S is partially ordered by inclusion. S is nonempty because $(0) \in S$. Any totally ordered subset $\{I_\alpha\}$ of S has an upper bound $\bigcup_\alpha I_\alpha$. So, by Zorn's lemma, S has a maximal element I; I is maximal in S, not a maximal ideal.

I is prime. Suppose $a, b \notin S$. Then $(I, a) > I$, so it contains an element of M $x^n = i_1 + sa$. Likewise, (I, b) contains an element of M $x^n = i_2 + tb$. So $i_1 i_2 + i_2 sa + i_1 tb + stab = x^{m+n}$ is an element of M, and the first 3 terms on the left hand side are in I. So $ab \notin I$ because otherwise the right hand side of this equation would be an element of I, which is impossible because it is in M. So I is prime, as desired. □

[3]Picking elements in this way requires the axiom of choice. As such, Zorn's lemma was somewhat controversial in the early 20th century.

[4]Assuming that ordered sets always have a maximal element has been the cause of numerous philosophical blunders over the years, such as some attempted proofs of the existence of a god.

2 Localization

2.1 What is localization?

The integers do not have division. This is inconvenient, so we construct the rational numbers $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}, n \neq 0\}$. $\mathbb{Q}$ is a field.

More generally, suppose R is a ring and S is a subset of R. We find a new ring $R[S^{-1}]$ so that all elements of S have inverses. This is localization.

Example 2.1. If R is an integral domain and S is the set of nonzero elements of R, then $R[S^{-1}]$ is a quotient field of R.

2.2 Construction

We may as well assume $1 \in S$ and S is closed under multiplication. If a, b have inverses, then ab should, as well. First, Assume S has no zero divisors. We basically copy the construction of $\mathbb{Q}$ from $\mathbb{Z}$.

Take all pairs (r, s) with $r \in R$ and $s \in S$. Call this r/s. We have an equivalence relation $r_1/s_1 \equiv r_2/s_2$ means $r_1s_2 = r_2s_1$. The subtle point of this construction is that we need to check that this equivalence relation is transitive.

We first assume that S has no zero divisors. Suppose $r_1/s_1 \equiv r_2/s_2$ and $r_2/s_2 \equiv r_3/s_3$. We have $r_1s_2 = r_2s_1$ and $r_2s_3 = r_3s_2$. So $r_1s_2s_3 = r_2s_1s_3 = s_1r_3s_2$. This makes $s_2(r_1s_3 = r_3s_1) = 0$, and since s_2 is not a zero divisor, $r_1s_3 = r_3s_1$; i.e. $r_1/s_1 \equiv r_3/s_3$. The remaining step is to check that the equivalence classes form a ring. We leave this as an exercise.

In this case, we have the map $R \to R[S^{-1}]$ sending $r \mapsto r/1$. This map is injective because it has trivial kernel; $r/1 = 0/1$ means $1r = 0 \cdot 1 = 0$, which makes $r = 0$.

What if S has zero divisors? Then $r_1/s_1 \equiv r_2/s_2$ is not an equivalence relation. So let I be the ideal of all elements with $xs = 0$ for some $s \in S$. Check that this is an ideal. Now form R/I, and let $\bar{S}$ be the image of S in R/I. Then $\bar{S}$ has no zero divisors in R/I, so we can form $(R/I)[\bar{S}^{-1}]$ as before.

So we get a ring $R[S^{-1}]$ with the following properties:

1. There is a homomorphism from $R \to R[S^{-1}]$.
2. The images of all elements of S are invertible in $R[S^{-1}]$.
3. $R[S^{-1}]$ is the universal ring with these properties.

$$\begin{tikzcd} R \arrow[r] \arrow[dr] & R[S^{-1}]s \arrow[d, dashed] \\ & X \end{tikzcd}$$

The kernel of the map $R \to R[S^{-1}]$ is I, the set of elements killed by something in S. Then $r_1/s_1 \equiv r_2/s_2$ can be defined as $\exists s_3$ such that $s_3(r_1s_2 - r_2s_1) = 0$.

2.3 Examples

Why is localization called localization?

Example 2.2. Let $R = \mathbb{C}[x]$, the set of polynomial functions on $\mathbb{C}$. Suppose we want to examine $0 \in \mathbb{C}$. What do the functions near 0 look like? An example is the rational functions that are nonsingular at 0; this is an approximation to all holomorphic functions in a neighborhood of 0. This is equal to $R[S^{-1}]$, where S is the set of polynomials that are nonzero at 0. The map $R \to R[S^{-1}]$ is injective but not surjective.

Example 2.3. Let R be the set of continuous functions on $\mathbb{R}$. Focus on the point $0 \in \mathbb{R}$. Look at the germs, functions that are equivalent in a neighborhood of 0. The ring of germs is $R[S^{-1}]$, where S is the set of functions that are nonzero at 0. Here, the map $R \to R[S^{-1}]$ is surjective but not injective.

You may have noticed that in these two examples, S was the complement of a prime ideal. In general, if p is any prime ideal, then the complement of p is multiplicatively closed.

Example 2.4. Let $R = \mathbb{Z}$, and suppose we are interested in (2). Let $S = \mathbb{Z} \setminus (2)$, the odd numbers. So we get a ring $\mathbb{Z}_{(2)}$, the rationals a/b with b odd. In general, let $R_p = R[S^{-1}]$, where S is the complement of a prime ideal p. The units of $\mathbb{Z}_{(2)}$ are rationals of the form a, b with a, b odd. 2 is a prime element of $Z_{(2)}$. Anly element of $Z_{(2)}$ equals $2^n u$ for some unit u and a unique $n \in \mathbb{N}$. So this is a UFD with only one prime: 2. We see that localizing at 2 "kills off" all primes other than 2.