ZORN'S LEMMA AND MAXIMAL IDEALS

RUSS WOODROOFE

We showed in class that a commutative ring with identity R is a field if and only if 0 is the only proper ideal of R. Herstein discusses this in Chapter 3.5. The result led us to define a *maximal ideal* as a maximal proper ideal, i.e., maximal ideal $\neq R$. With only a bit of work, we saw that:

Corollary 1. *If R is a commutative ring with 1, and M is an ideal, then R/M is a field if and only if M is a maximal ideal.*

In this note, I will give a proof that rings always have maximal ideals.

1. Zorn's Lemma

As a tool, we will need Zorn's Lemma. Zorn's Lemma is equivalent to the Axiom of Choice, which mathematicians are occasionally skeptical about: for an account see Eric Schecter's page at:
http://www.math.vanderbilt.edu/~schectex/ccc/choice.html
We summarize this discussion briefly. A set can *be made well-ordered* if there is a total ordering of the set where every subset contains a minimal element. Zorn's Lemma, the Axiom of Choice, and that any set can be well-ordered, are all equivalent statements.

But well-ordering is usually thought of as being a property of the natural numbers! We repeat a waggish quotation from the above web page:

> The Axiom of Choice is obviously true; the Well Ordering Principle is obviously false; and who can tell about Zorn's Lemma?
>
> Jerry Bona

Zorn's Lemma is nonetheless very useful in algebra, and finding maximal ideals is an excellent example of how it is used.

We give a couple of definitions.

Definition 2. A *partially ordered set* is a set P with an order $\leq$ satisfying some basic properties:

(1) $a \leq x$ (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)

More helpful are examples. The set of all subsets of $[n]$ is a partially ordered set under the order of set inclusion; as is the subgroup lattice of any group. The integers $\mathbb{Z}$ are a partially ordered set under the normal meaning of $\leq$. Similarly with $\mathbb{Q}$ and $\mathbb{R}$.

Definition 3. A *totally ordered set* L is a partially ordered set, where if a and b are in L, then either $a \leq b$ or $b \leq a$.

The integers $\mathbb{Z}$ are an example of a totally ordered set, but the subgroup lattice is (usually) not.

Example 4. Consider $L(S_3)$. This is not a totally ordered set, since S_3 has three subgroups of order 2: H_1, H_2, and H_3. None of the three are contained in any other, e.g., $H_1 \not\subseteq H_2$. Thus, $L(S_3)$ is not a totally ordered set.

A word on notation. I'll usually use L for totally ordered sets, since in the countable case, they are actually "linearly" ordered. That is, the elements form a chain

$$\cdots \leq x_{-1} \leq x_0 \leq x_1 \leq x_2 \leq \dots$$

by sorting them from greatest to least.

We now state Zorn's Lemma:

Lemma 5. (Zorn's Lemma) *Let P be a nonempty partially ordered set, such that for every totally ordered subset L, there exists some "upper bound" u for L so that $u \geq x$ for every $x \in L$. Then P has a maximal element.*

Note that some posets do not have any maximal element – $\mathbb{Z}$ (under the usual ordering) does not, for example.

Exercise 6. (Easy) Why does $\mathbb{Z}$ not meet the criteria for Zorn's Lemma?

2. Maximal Ideals

In the introduction, we said that we'd find maximal ideals of a commutative ring with 1. More specifically, we'll prove the following theorem:

Theorem 7. *Let R be a commutative ring with 1, and $I \subset R$ be a proper ideal. Then I is contained in a maximal ideal M.*

So not only does R have a maximal ideal, but we have a "development" theorem, that every ideal is contained in a maximal one!

Proof. (Of Theorem) We can see that Zorn's Lemma may be useful, because the Theorem calls for finding a maximal element. We need to define a poset where the maximal element is a maximal ideal containing I. So we take

$$\mathcal{P} = \{\text{proper ideals of } R \text{ that contain } I\}.$$

A maximal element of $\mathcal{P}$ will finish the proof, so we need only show that $\mathcal{P}$ satisfies the condition of Zorn's Lemma.

Let $\mathcal{L}$ be a totally ordered subset of $\mathcal{P}$. This means that $\mathcal{L}$ is a set of proper ideals, where if $A, B \in \mathcal{L}$, then either $A \subseteq B$ or $B \subseteq A$. Let

$$M_{\mathcal{L}} = \bigcup_{J \in \mathcal{L}} J.$$

Since $M_{\mathcal{L}}$ is the union of every $J \in \mathcal{L}$, we have that $M_{\mathcal{L}} \supseteq J$ for every $J \in \mathcal{L}$. That is, $M_{\mathcal{L}}$ is an upper bound for $\mathcal{L}$. To satisfy Zorn's Lemma, we need only show that $M_{\mathcal{L}}$ is in $\mathcal{P}$. There are three things that we need to check: "proper", "ideal of R", and "contains I".

(1) $M_{\mathcal{L}}$ is proper, i.e., $M_{\mathcal{L}} \neq R$:
Since $1 \notin J$ for each $J \in L$, we have that $1 \notin M_{\mathcal{L}}$, hence that $M_{\mathcal{L}} \neq R$.

(2) $M_{\mathcal{L}}$ is an ideal:
Suppose that $r \in R$, and $a \in M_{\mathcal{L}}$. If $a \in M_{\mathcal{L}}$, then it must be contained in some $J \in \mathcal{L}$. Thus, $ra \in J$, and so $ra \in M_{\mathcal{L}}$. Taking $r = -1$, we get that $-a \in M_{\mathcal{L}}$.
Now suppose that $a, b \in M_{\mathcal{L}}$. Then there is some $J_a, J_b \in \mathcal{L}$ with $a \in J_a$ and $b \in J_b$. But since $\mathcal{L}$ is totally ordered, either $J_a \subseteq J_b$ or else $J_b \subseteq J_a$. Without loss of generality, suppose that $J_b \subseteq J_a$. Then both $a, b \in J_a$, hence $a + b \in J_a$, and so $a + b \in M_{\mathcal{L}}$.

(3) $M_{\mathcal{L}}$ contains I:
This is obvious, since $I \subseteq J \subseteq M_{\mathcal{L}}$ for any $J \in \mathcal{L}$.

Since $\mathcal{P}$ satisfies the condition for Zorn's Lemma, it has a maximal element, which is a maximal proper ideal of R containing I as desired. □

We pause to notice again how we found the upper bound for $\mathcal{L}$: we simply took the union of all the elements of $\mathcal{L}$. This is a pretty good trick, and frequently how applications of Zorn's Lemma in algebra work. The only 'hard' step is checking that the union is in $\mathcal{P}$.

We note one corollary of Theorem 7.

Corollary 8. *If R is a nontrivial commutative ring with identity, then there is a surjective homorphism of R onto some field.*