1-29-1994

Maximal ideals. Prime ideals.

Definition. Let R be a ring. A (left, right, two-sided) ideal I is a (left, right, two-sided) **maximal ideal** if $I \neq R$, and if whenever J is a (left, right, two-sided) ideal and $I \subset J$, either $I = J$ or $J = R$.

An ideal I in a commutative ring is **prime** if $I \neq R$, and if $xy \in I$ implies either $x \in I$ or $y \in I$.

Examples.

1. $R = \mathbb{Z}_{12}$ Ideals are subgroups of the additive group of R, and subgroups of cyclic groups are cyclic, so the (proper) ideals are

$$\begin{aligned} \langle 2 \rangle &= \{0, 2, 4, 6, 8, 10\} \\ \langle 3 \rangle &= \{0, 3, 6, 9\} \\ \langle 4 \rangle &= \{0, 4, 8\} \\ \langle 6 \rangle &= \{0, 6\} \end{aligned}$$

$\langle 2 \rangle$ and $\langle 3 \rangle$ are prime and maximal; $\langle 4 \rangle$ and $\langle 6 \rangle$ are neither prime nor maximal. $\square$

2. $R = \mathbb{Z}[x]$ The ideal $\langle x \rangle$ is prime, since a product of two polynomials is divisible by x if and only if one or the other is divisible by x. It is not maximal, since it is contained in the proper ideal $\langle x, x+2 \rangle$. ($\langle x, x+2 \rangle$ contains constant polynomials divisible by 2, but $1 \notin \langle x, x+2 \rangle$.)

On the other hand, the ideal $\langle x^2 \rangle$ is not prime: $x \cdot x \in \langle x^2 \rangle$, but $x \notin \langle x^2 \rangle$. $\square$

If a ring has ideals, it will have maximal ideals. The proof of this requires an excursion into set theory.

Definition. Let S be a set. A **partial order** on S is a relation $\leq$ on S which satisfies the following axioms:

a. For all $x \in S$, $x \leq x$.

b. For all $x, y \in S$, if $x \leq y$ and $y \leq x$, then $x = y$.

c. For all $x, y, z \in S$, if $x \leq y$ and $y \leq z$, then $x \leq z$.

A partially ordered set is often referred to as a **poset**.

Let S be a partially ordered set. An element $m \in S$ is **maximal** if $m \leq x$ implies $m = x$. If $T \subset S$, an **upper bound** x for T is an element $x \in S$ such that $y \leq x$ for all $y \in T$. Note that an upper bound for T doesn't have to be an element of T.

Examples.

1. The usual $\leq$ relation on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ is a partial order. $\square$

2. Let S be a set, and let T be a collection of subset of S. Then set inclusion partially orders T.

If $X \in \mathcal{T}$, then $X \subset X$. If $X, Y \in \mathcal{T}$, then $X \subset Y$ and $Y \subset X$ imply $X = Y$. Finally, if $X, Y, Z \in \mathcal{T}$, $X \subset Y$, and $Y \subset Z$, then $X \subset Z$. Thus, set inclusion partially orders any collection of subsets of a set. *This situation is one of the most important for the applications which will follow.* $\square$

3. Here is a picture of a partial order on the set $\{1, 2, 3, 4, 5, \text{Calvin}\}$:

$$\begin{tikzcd}
& & 1 & \\
& 2 \arrow[ur] & & \text{Calvin} \arrow[ul] \\
3 \arrow[ur] & & 4 \arrow[ul] & \\
& 5 \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

For example, $5 \leq 3$, $2 \leq 2$ (required by the first axiom for a partial order), and so on. Note that there is no relation between 3 and 4, or between 2, 3, 4, 5 and Calvin. Tough luck for Calvin.

Elements x and y in a partially ordered set are **comparable** if either $x \leq y$ or $y \leq x$. As the example shows, two elements in a poset may not be comparable. $\square$

Zorn's Lemma. Let S be a nonempty poset. If every chain in S has an upper bound, then S has maximal elements. $\square$

Zorn's lemma is (essentially) one of the axioms of set theory. More precisely, Zorn's lemma is equivalent to the **Axiom of Choice**, which is one of the standard axioms of **Zermelo-Fraenkel set theory**. Choice says if X is a set of nonempty pairwise disjoint sets, there is a set Y which contains exactly one element from each set in X. Intuitively, the set Y "chooses" one element from each set in the collection X.

In fact, both Choice and Zorn are equivalent to other statements, such as Hausdorff Maximality and the Well-Ordering Principle. The latter, for example, says that every set can be well-ordered. (A set is **well-ordered** if it can be partially ordered in such a way that every two elements are comparable, and every nonempty subset has a least element.)

In the early part of this century, the Axiom of Choice was a source of controversy. Since the choice set Y above is not specified constructively, many mathematicians felt that the axiom was dubious. Even today, **constructivists** feel that Choice is philosophically unsatisfying, and try to do mathematics without it. While they represent a small minority of practicing mathematicians, they have made important contributions by coming up with constructive proofs of many results.

Nowadays, Choice is accepted and used by the vast majority of mathematicians. I will use Zorn's lemma (and the Axiom of Choice) without much discussion, since I don't consider their use terribly controversial.

Theorem. Let R be a ring with 1, and let I be a proper (left, right, two-sided) ideal. There exists a (left, right, two-sided) ideal M containing I.

Proof. Let S be the set of (left, right, two-sided) proper ideals of R which contain I. Since $I \subset I$, $I \in \mathcal{S}$, and $\mathcal{S} \neq \emptyset$.

Partially order S by inclusion. I'll show that every chain in S has an upper bound. Let T be a chain in S. Thus, T is a collection of ideals of R which contain I, and such that any two elements of T are comparable. Define

$$M = \bigcup_{J \in \mathcal{T}} J.$$

I claim that M is an upper bound for T.

First, I must show that M is an ideal. Since $I \subset M$, M is nonempty. Let $x, y \in M$. Say $x \in J$ and $y \in K$, where J and K are ideals which contain I. Since elements of T are comparable, either $J \subset K$ or $K \subset J$. In the first case, $x, y \in K$, so $x - y \in K$; in the second case, $x, y \in J$, so $x - y \in J$. In either case, $x - y \in M$. Hence, M is a subgroup of the additive group of R.

Next, let $x \in M$ and $r \in R$. I'll give the proof for left ideals; the right ideal and two-sided ideal cases are similar. Suppose $x \in J$, where J is an ideal containing I. Then $rx \in J$, so $rx \in M$. This shows that M is an ideal.

Next, observe that M must be proper. For if $M = R$, then $1 \in M$, so $1 \in J$ for some $J \in \mathcal{T}$, so $J = R$. This contradicts our assumption that the elements of S were *proper* ideals.

Since $I \subset M$, M is an ideal containing I. Finally, M contains every element of T by construction, so M is an upper bound for T.

The hypotheses of Zorn's lemma are satisfied. Therefore, S has maximal elements. A maximal element of S will be a proper ideal containing I which is not contained in any other proper ideal containing I. Such an element is clearly a maximal ideal. $\square$

Lemma. Let $\phi : R \to S$ be a ring map.

a. If I is an ideal in R and ϕ is surjective, then $\phi(I)$ is an ideal in S.

b. If J is an ideal in S, then $\phi^{-1}(J)$ is an ideal in R.

Proof. I'll do the case where I and J are left ideals; the right and two-sided cases are minor variations.

a. Suppose I is an ideal in R, and suppose ϕ is surjective. Let $x, y \in I$. Then

$$\phi(x) - \phi(y) = \phi(x - y) \in \phi(I),$$

so $\phi(I)$ is an additive subgroup.

Let $x \in I$, and let $s \in S$. Write $s = \phi(r)$, where $r \in R$ (surjectivity of ϕ). Then

$$s \cdot \phi(x) = \phi(r)\phi(x) = \phi(rx) \in \phi(I).$$

Therefore, $\phi(I)$ is an ideal.

b. Let J be an ideal in S. Let $x, y \in \phi^{-1}(J)$, so $\phi(x), \phi(y) \in J$. Then

$$\phi(x - y) = \phi(x) - \phi(y) \in J,$$

so $x - y \in \phi^{-1}(J)$. Therefore, $\phi^{-1}(J)$ is an additive subgroup.

Next, let $x \in \phi^{-1}(J)$ and let $r \in R$. Now $\phi(x) \in J$, so $\phi(rx) = \phi(r)\phi(x) \in J$. Hence, $rx \in \phi^{-1}(J)$. Hence, $\phi^{-1}(J)$ is an ideal. $\square$

Theorem. Let R be a commutative ring with 1. Let I be an ideal.

a. I is prime if and only if R/I is an integral domain.

b. I is maximal if and only if R/I is a field.

Proof. Observe that since R is commutative, so is R/I. For

$$(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I).$$

a. ($\Rightarrow$) Suppose I is prime. I want to show that R/I is a domain. This amounts to showing that R/I has no zero divisors.

Let $(a+I)(b+I) = 0 \in R/I$. I must show that $a+I = 0$ or $b+I = 0$. Now $(a+I)(b+I) = 0 \in R/I$ means $ab + I = 0 \in R/I$, or $ab \in I$. Since I is prime, either $a \in I$ or $b \in I$. In the first case, $a + I = I = 0 \in R/I$, whereas in the second case, $b + I = I = 0 \in R/I$. This proves that R/i is a domain.

($\Leftarrow$) Suppose R/I is a domain. I want to show that I is prime. Let $ab \in I$. I must show $a \in I$ or $b \in I$.

Now $ab \in I$ implies $ab + I = I$, or $(a + I)(b + I) = I = 0 \in R/I$. Since R/I is a domain, either $a + I = I = 0 \in R/I$, or $b + I = I = 0 \in R/I$. In the first case, $a \in I$, and in the second case, $b \in I$. Therefore, I is prime.

b. ($\Rightarrow$) Suppose I is maximal. I want to show that R/I is a field. I must show that every nonzero element is invertible.

Suppose that $a + I \in R/I$, where $a \notin I$ (so $a + I \neq 0 \in R/I$). Consider the ideal $\langle a, I\rangle$. It contains I, and is larger than I, since $a \in \langle a, I\rangle$ while $a \notin I$. Therefore, $\langle a, I\rangle = R$.

I claim that every element of $\langle a, I\rangle$ can be written in the form $ra + x$, where $r \in R$ and $x \in I$. Indeed, consider the set

$$S = \{ra + x \mid r \in R, x \in I\}.$$

By closure, $S \subset \langle a, I\rangle$.

On the other hand, S is an ideal. For

$$(ra + x) - (r'a + x') = (r - r')a + (x - x') \in S,$$

so S is an additive subgroup.

If $s \in R$ and $ra + x \in S$, then $s(ra + x) = (sr)a + sx$. Now $sx \in I$, since I is an ideal, so $(sr)a + sx \in S$. This proves that S is an ideal. Since S is an ideal containing a and I, it follows that $\langle a, I\rangle \subset S$. Hence, $S = \langle a, I\rangle$.

Now $1 \in R = \langle a, I\rangle$, so write $1 = ra + x$, where $r \in R$ and $x \in I$. Then

$$1 + I = ra + x + I = ra + I = (r + I)(a + I).$$

Therefore, $r + I$ is the inverse of $a + I$ in R/I. Hence, R/I is a field.

($\Leftarrow$) Suppose that R/I is a field. I want to show that I is maximal. Let J be an ideal, and suppose that $I \subset J$ but $I \neq J$. I'll show that $J = R$.

The quotient map $\pi : R \to R/I$ is a surjective ring map. By the lemma, $\pi(J)$ is an ideal in R/I. However, the only ideals in a field are the zero ideal and the whole field. Since $I \neq J$, there is an $x \in J$, $x \in R - I$, and then $\pi(x) \neq 0 \in R/I$. Thus, $\pi(J)$ is not the zero ideal, so it's R/I.

Find $x \in J$ such that $\pi(x) = 1 + I$. Then $x + I = 1 + I$. If $r \in R$, then $rx + I = r + I$, so $r - rx = y \in I$. Now $x \in J$, so $rx \in J$. Write $r = rx + y$. $rx \in J$, and $y \in I \subset J$, so $r \in J$. Since r was arbitrary, $R \subset J$, i.e. $R = J$. This proves that I is maximal. $\square$

Corollary. In a commutative ring, maximal ideals are prime.

Proof. If I is maximal, R/I is a field. Hence, R/I is a domain, so I is prime. $\square$

Examples.

1. $R = \mathbb{Z}_{12}$ By an earlier example, the (proper) ideals are

$$\begin{aligned}\langle 2\rangle &= \{0, 2, 4, 6, 8, 10\}\\ \langle 3\rangle &= \{0, 3, 6, 9\}\\ \langle 4\rangle &= \{0, 4, 8\}\\ \langle 6\rangle &= \{0, 6\}\end{aligned}$$

$R/\langle 2\rangle \approx \mathbb{Z}_2$ is a field, so $\langle 2\rangle$ is maximal (and prime). $R/\langle 3\rangle \approx \mathbb{Z}_3$ is a field, so $\langle 3\rangle$ is maximal (and prime). $R/\langle 4\rangle \approx \mathbb{Z}_4$; it certainly has order 4, and you can check that $1 + \langle 4\rangle$ has order 4. Since $\mathbb{Z}_4$ is not a domain, $\langle 4\rangle$ isn't prime (and hence, isn't maximal). $R/\langle 6\rangle \approx \mathbb{Z}_6$ (there is only one abelian group of order 6); since $\mathbb{Z}_6$ is not a domain, $\langle 6\rangle$ is not prime nor maximal. $\square$

2. Consider the ideal $I = \langle x - y^2\rangle$ in $\mathbb{Q}[x, y]$. I claim that I is prime.

The map $\phi : \mathbb{Q}[x, y] \to \mathbb{Q}[t]$ given by

$$\phi(x) = t^2, \qquad \phi(y) = t,$$

is a surjective ring homomorphism. $\phi(x - y^2) = t^2 - t^2 = 0$, so $I \subset \ker\phi$. I'll show that $I = \ker\phi$.

Consider $R = \mathbb{Q}[x, y]/I$. I claim that every coset in R can be written in the form

$$f(x) + g(x)y + I, \quad f, g \in \mathbb{Q}[x].$$

Take an arbitrary coset $p(x, y) + I$. Then

$$p(x, y) + I = q(x) + (\text{terms with odd powers of } y) + (\text{terms with even powers of } y) + I =$$

$$q(x) + y \cdot (\text{terms with even powers of } y) + (\text{terms with even powers of } y) + I.$$

A typical term with an even power of y looks like $h(x)y^{2k}$. However, $x - y^2 \in I$, so $x + I = y^2 + I$, so $x^k + I = y^{2k} + I$. Therefore,

$$h(x)y^{2k} + I = h(x)x^k + I.$$

Thus, modulo I, a term with an even power of y can be replaced by a term in x.

Therefore,

$$q(x) + y \cdot (\text{terms with even powers of } y) + (\text{terms with even powers of } y) + I = q(x) + y \cdot r(x) + s(x) + I.$$

Setting $f(x) = q(x) + s(x)$ and $g(x) = r(x)$ proves the claim.

Now I'll prove that $\ker \phi \subset I$. Suppose then that $\phi\left(p(x, y)\right) = 0$. I must show that $p \in I$. By the claim,

$$p(x, y) = f(x) + y \cdot g(x) + \text{junk},$$

where junk $\in I$.

Apply ϕ to both sides:

$$\phi\left(f(x) + y \cdot g(x)\right) = 0.$$

I'll show that $f = 0$ and $g = 0$.

The previous equation gives

$$f(t^2) + t \cdot g(t^2) = 0.$$

Write

$$f(x) = \sum_{i=0}^{m} a_i x^i, \qquad g(x) = \sum_{j=0}^{n} b_j y^j.$$

Then

$$0 = \sum_{i=0}^{m} a_i t^{2i} + t \cdot \sum_{j=0}^{n} b_j t^{2j} = \sum_{i=0}^{m} a_i t^{2i} + \sum_{j=0}^{n} b_j t^{2j+1}.$$

The first sum has even powers of t, while the second sum has odd powers of t. Therefore, *all* the coefficients are 0: $a_i = 0$ for all i, $b_j = 0$ for all j. Thus, $f = 0$ and $g = 0$.

Finally, it follows that $p(x, y) = \text{junk} \in I$. This shows that $\ker \phi \subset I$, so $\ker \phi = I$.

By the First Isomorphism Theorem,

$$\frac{\mathbb{Q}[x, y]}{I} = \frac{\mathbb{Q}[x, y]}{\ker \phi} \approx \operatorname{im} \phi = \mathbb{Q}[t].$$

Now $\mathbb{Q}[t]$ is a domain (to be proved later!). Hence, I is prime. $\square$