Ring Theory Independent Study

Torey Hilbert

April 2018

1 Maximal and Prime Ideals

1.1 Motivation

Many of the common uses of ring theory involve attacking problems that seem impossible in their current state. Often times these challenging problems can be translated into far simpler, but equivalent, problems when posed in terms of a "different language". However, in order to take advantage of this, we need to come up with natural generalizations for familiar concepts.

1.2 Background

For all of the following, let R be a commutative ring with unity.
Ideals: An ideal I of the ring R is a subset $I \subseteq R$ that is closed under addition, negatives, and multiplication. Additionally, it "absorbs products" meaning that if $i \in I$, then for any $a \in R$, $ai \in R$. An ideal I is **proper** if $I \neq R$. For any $x \in R$, the ideal "generated by x" is $\{ax \mid x \in R\}$ and is denoted by (x). If there exists some $x \in R$ such that $I = (x)$, we say that I is **principal**. Every element of the ring R/I is of the form $x+I = \bar{x} = \{x+i \mid i \in I\}$ for some $x \in R$. A **principal ideal domain** (P.I.D.) is a ring where every ideal is principal.

The first thing we define is a generalization of prime integers, extending the property that if n is prime, and $n|ab$, then either $n|a$ or $n|b$. In fact, one could even define primes as the positive integers such that $n|ab$ implies either $n|a$ or $n|b$.

Suppose n is prime, and $n = ab$. Then either $n|a$ or $n|b$. Let $n|a$. Then $n = a$, so $b = 1$, and vice versa if $n|b$. Hence n has only two divisors (1 and n), which is the usual definition. This makes the following definition of a prime ideal a very natural extension.
Prime Ideals: A (proper) ideal P of the ring R is prime if $ab \in P$ only if either $a \in P$ or $b \in P$.

Examples of prime ideals include $p\mathbb{Z}$ in $\mathbb{Z}$ for any prime p, and the zero ideal of any integral domain is prime.
Maximal Ideals: A (proper) ideal M of a ring R is maximal if it is not contained in a larger ideal of R. This is equivalent to M being maximal if for any proper ideal $A \subset R$, $M \subseteq A$ implies $M = A$.

Theorem: If R is commutative, then for any ideal M of R, R/M is a field if and only if M is maximal. Also, for any ideal P of R, R/P is an integral domain if and only if P is prime.
Proof: $(\rightarrow)$ Suppose M is a maximal ideal of R, and let A be a subring of R such that $M \subseteq A$. Since M is maximal, A is an ideal if and only if $A = R$ or $A = M$, so that $A/M = R/M$ or $A/M = 0$. But by the fourth isomorphism theorem, A is an ideal if and only if A/M is an ideal of R/M, so the only ideals of R/M are $A/M = R/M$ and $A/M = 0$. Recall that F is a field if the only ideals of F are the zero ideal and F, and hence R/M is a field.
$(\leftarrow)$ Suppose R/M is a field. Then notice, by the fourth isomorphism theorem, a subring A of R such that $M \subseteq A$ is an ideal if and only if f A/M is an ideal of R/M. However, since R/M is a field, its only ideals are R/M and $0 = M/M$, which correspond to $A = R$ or $A = M$. Hence the only ideals of R which contain M are R and M, so it follows that M is maximal.
$(\rightarrow)$ Suppose P is prime. Then for any $a, b \in R$, $\bar{a}\bar{b} = \bar{0}$ if and only if $ab \in P$, so either $a \in P$ or $b \in P$. Hence either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, which in turn implies that R/P has no zero divisors, so it is an integral domain.
$(\leftarrow)$ Suppose R/P is an integral domain, and suppose $ab \in P$. Then $\bar{a}\bar{b} = \overline{ab} = \bar{0}$, and since R/P has no zero divisors, either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, which means precisely that either $a \in P$ or $b \in P$. Hence P is prime.

1.3 Problems and Examples

Claim: The following hold true in any commutative ring R with unity:

1. 0 is a maximal ideal of R if and only if R is a field.
2. If R is an integral domain, then for any $p, q \in R$, $(p) = (q)$ if and only if $p = uq$ for some unit $u \in R$.
3. If P is an integral domain and P is also a prime ideal of R, then R is an integral domain.

Proof:

1. $(\rightarrow)$ In any field R, there are only two ideals: 0 and R. R is not a proper ideal, so 0 is maximal since it is not the subset of any proper ideal of R other than itself.

   $(\leftarrow)$ Conversely, for any ideal I of R, $0 \subseteq I$, so if 0 is maximal, then $0 = I$. Hence 0 is the only proper ideal of R, and thus R is a field.

2. $(\rightarrow)$ Suppose $(p) = (q)$. Then $(p) \subseteq (q)$, so $p \in (q)$ and thus, for some $a \in R$, $p = aq$. Similarly, $(q) \subseteq (p)$, so for some $b \in R$, $q = bp = b(aq) = (ba)q$. Now R is an integral domain, and we can assume q is nonzero (because if $q = 0$, then $(0) = 0 = (p)$, so $p = 0 = 1q$). Hence $1 = ba$, and thus a and b are units in R, so $p = aq$, for some unit $a \in R$.

   $(\leftarrow)$ Conversely, suppose $p = uq$ for some unit $u \in R$. Then clearly $p \in (q)$, so $(p) \subseteq (q)$. Since u is a unit, there exists $v \in R$ such that $vu = 1$, so $vp = vuq = q$, so $q \in (p)$, so $(q) \subseteq (p)$. Thus $(p) = (q)$.

3. Suppose $a, b \in R$ and $ab = 0$. Since P is prime and $0 \in P$, either $a \in P$ or $b \in P$. But P has no zero divisors, so $a = 0$ or $b = 0$. Thus for any product $ab = 0$ in R, either $a = 0$ or $b = 0$, so R is an integral domain.

Claim: Let R be a commutative ring with unity. Then the following is true:

1. R is a field if and only if (x) is maximal in the ring $R[x]$. Also, R is an integral domain if and only if (x) is prime in the ring $R[x]$.

2. Let $f(x) \in R[x]$ have a leading coefficient $a_n = 1$. Then every element of $R[x]/(f(x))$ is the image of some polynomial $p(x) \in R[x]$ such that $deg(p) < n$.

Proof:

1. Notice $R[x]/(x) \cong R$. Since $R[x]/(x)$ is a field if and only if (x) is maximal, it follows that R is a field if and only if (x) is maximal. Similarly, $R[x]/(x)$ is an integral domain if and only if (x) is prime, so R is and integral domain if and only if (x) is prime.

2. Let $deg(f) = n$ such that $f(x) = x^n + c_{n-1}x^{n-1} + ... + c_0$. Firstly,

$$\begin{aligned} \overline{x_n} &= \overline{x^n + (c_{n-1}x^{n-1} + ... + c_0) - (c_{n-1}x^{n-1} + ... + c_0)} \\ &= \overline{f(x) - (c_{n-1}x^{n-1} + ... + c_0)} \\ &= \overline{-(c_{n-1}x^{n-1} + ... + c_0)}. \end{aligned}$$

Let $\overline{q(x)} \in R[x]/(f(x))$. Suppose $deg(q) = m \geq n$, such that $q(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_0$. Then

$$\begin{aligned} \overline{q(x)} &= \overline{a_m x^m + a_{m-1}x^{m-1} + ... + a_0} \\ &= \overline{a_m x^m} + \overline{a_{m-1}x^{m-1} + ... + a_0} \\ &= \overline{a_m x^{m-n} x^n} + \overline{a_{m-1}x^{m-1} + ... + a_0} \\ &= \overline{-a_m x^{m-n}(c_{n-1}x^{n-1} + ... + c_0)} + \overline{a_{m-1}x^{m-1} + ... + a_0} \\ &= \overline{(a_{m-1} - a_m c_{n-1})x^{m-1} + ... + (a_{m-n} - a_m c_0)x^{m-n} + a_{m-n-1}x^{m-n-1} + ... + a_0} \\ &= \overline{q'(x)}, \end{aligned}$$

where $q'(x) \in R[x]$ has a degree of at most $m - 1$. Since, we can always decrease the degree of $q(x)$ by one whenever $deg(q) \geq n$, this implies that there exists some $p(x) \in R[x]$ with a degree of at most $n - 1$ such that $\overline{p(x)} = \overline{q(x)}$.

Claim: Let R be a P.I.D. Then the following is true:

1. For any nonzero $a, b \in R$, there exists a least common multiple of a and b in R, namely there exists $c \in R$ such that c is a multiple of a and b, and that any other multiple of a and b is a multiple of c.

2. If P is a prime ideal of R, then R/P is a P.I.D.

Proof:

1. Let $a, b \in R$ be nonzero, and consider $(a) \cap (b)$. To show that $(a) \cap (b)$ is an ideal in R, let $x, y \in (a) \cap (b)$ and $z \in R$. Then $x, y \in (a)$ and $x, y \in (b)$, so $x - y \in (a)$ and $x - y \in (b)$, so $x - y \in (a) \cap (b)$ (meaning $(a) \cap (b)$ is closed under subtraction). Likewise, $xz \in (a)$ and $xz \in (b)$, so $xz \in (a) \cap (b)$ (meaning $(a) \cap (b)$ absorbs products), hence $(a) \cap (b)$ is an ideal of R. But any ideal of R is principal, so there exists $c \in R$ such that $(c) = (a) \cap (b)$. Notice then, $c \in (a)$ and $c \in (b)$, so c is a common multiple of a and b. Take any other common multiple d. Then $d \in (a) \cap (b) = (c)$, so d is a multiple of c. It follows that c is a least common multiple of a and b.

2. We immediately see that R/P is an integral domain, so it just remains to show that every ideal of R/P is principal. By the Third Isomorphism Theorem, every ideal of R/P is of the form I/P, where I is an ideal of R that contains P. But since R is a P.I.D., that implies that $I = (c)$ for some $c \in I$. Consider any $\overline{x} \in I/P$. Then $x \in I$, $x = cy$ for some $c \in R$. Hence $\overline{x} = \overline{cy} = \overline{c} \cdot \overline{y}$, which implies $I/P = (\overline{c})$. So every ideal of R/P principal.

   Another way to prove this is simply that if $P = 0$, then $R/P = R$ which is a P.I.D., and if $P \neq 0$, then P is maximal so R/P is a field. All fields are P.I.D.s, so R/P is a P.I.D.

<u>Claim:</u>

1. $\mathbb{Z}[i]/(1+i)$ is a field.

Proof:

1. $\mathbb{Z}[i]$ is a P.I.D., and notice that $1+i$ is irreducible (since $N(1+i) = 2$, which is prime). This implies that $1+i$ is prime, so that $(1+i)$ is a prime ideal of $\mathbb{Z}[i]$. But in a P.I.D., any prime ideal is a maximal ideal as well, so $(1+i)$ is maximal, and it follows that $\mathbb{Z}[i]/(1+i)$ is a field.