LECTURE 6: PROPERTIES OF IDEALS (§7.4 of D&F)

Assume R is a ring with identity $1 \neq 0$ for this lecture. We do not generally assume R is commutative.

Def^n/ Let $A \subseteq R$.

(1.) Let (A) denote smallest ideal of R containing A. We say (A) is the <u>ideal generated</u> by A.

(2.) $RA = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\}$

$AR = \{a_1r_1 + a_2r_2 + \cdots + a_nr_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\}$

$RAR = \{r_1a_1r_1' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{N}\}$

Also, if $A = \emptyset$ then $RA = AR = RAR = 0$

(3.) An ideal generated by a single element is called a <u>principal ideal</u>

(4.) An ideal generated by a finite set is <u>finitely generated ideal</u>

We can prove RA is a left ideal, AR is a right ideal and RAR is a two-sided ideal all of which contain A. When R is commutative $RA = AR = RAR = (A)$.

<u>Proposition</u>: If R is commutative then (a) is an ideal

<u>Proof</u>: Let $a \in R$ then for commutative R consider $r \in R$ and let $x \in (a) = \{as \mid s \in R\}$ so $x = as$ and hence $xr = asr \in (a)$ since $sr \in R$ thus $r(a) \subseteq (a)$.

Let $x, y \in (a)$ then $\exists r_x, r_y \in R$ s.t. $x = r_xa$ and $y = r_ya$ thus $xy = (r_xa)(r_ya) = (r_xar_y)a \in (a)$ and $x - y = (r_x - r_y)a \in (a)$ since $r_xar_y, r_x - r_y \in R$ thus (a) is subring with $R(a) \subseteq (a)$ $\therefore$ (a) is ideal.

Let's think a little about how principal ideals interact with the concept of divisibility.

Def^n/ For R a commutative ring, we say $a \mid b$ or "a divides b" if $\exists r \in R$ such that $b = ra$ in which case we also say b is a multiple of a.

Thus observe for commutative ring R,

$$(a) = \{ra \mid r \in R\} = \text{set of multiples of } a.$$

$$b \in (a) \iff \left(\begin{array}{c} b = ra \\ \text{for some} \\ r \in R \end{array} \right) \iff a \mid b$$

E1 For $R = \mathbb{Z}$, $x \in (10) = 10\mathbb{Z} \Rightarrow 10 \mid x$.

Notice, $10\mathbb{Z} \subset 2\mathbb{Z}$ and $10\mathbb{Z} \subseteq 5\mathbb{Z}$ that is $(10) \subset (2)$ and $(10) \subset (5)$ and $2 \mid 10$ and $5 \mid 10$.

Th^m/ For commutative ring R containing a, b, $(a) \subseteq (b) \iff b \mid a$.

Proof: suppose $(a) \subseteq (b)$ then notice $a \cdot 1 = a \in (a)$ hence $a \in (b)$ thus $a = br \Rightarrow b \mid a$.

Conversely, suppose $b \mid a$ then $\exists r \in R$ s.t. $a = br$. Let $x \in (a)$ then $\exists s \in R$ s.t. $x = as = brs \in (b)$ as $rs \in R$. Thus $(a) \subseteq (b)$. //

Proposition: Let I be an ideal of R.

(1.) $I = R$ iff I contains a unit

(2.) Given R commutative, R is a field $\Leftrightarrow$ only ideals of R are R and 0

Proof: (1.) If $I = R$ then $1 \in R = I$ thus I contains a unit.

conversely, if I contains unit u with $uv = vu = 1$

then for $r \in R$ notice $r = rvu \in rvI = I$

thus $r \in I$ hence $R = I$ since $I \subseteq R$ is given.

(2.) Suppose R is commutative.

$\Rightarrow$ Assume R is a field and I is an ideal.

If $I \neq 0$ then $a \in I$ where $a \neq 0$

~~hence $a^{-1} \in R$ and $a^{-1}a = 1 \in I$~~

thus a is a unit and by (1), $I = R$.

$\Leftarrow$ Suppose the only ideals of R are R and 0.

Let $a \in R$ with $a \neq 0$ then $(a) = R$

hence, as we assume $1 \in R$, $ar = 1$ for

some $r \in R$ $\Rightarrow$ a is a unit $\therefore$ R is field.

Corollary: If R is a field then any nonzero ring homomorphism from R into another ring is an injection

Proof: $f : R \to A$ has $\ker(f)$ an ideal of R. If f is nonzero then $\ker(f) \neq R$ $\Rightarrow$ $\ker(f) = 0$ $\therefore$ f injective. //

Def^{n}/ An ideal M in an arbitrary ring S is called a <u>maximal ideal</u> if $M \neq S$ and the only ideals containing M are M and S.

E2 An example of a ring without a maximal ideal can be constructed with $\mathbb{Q}$ given the usual addition but a nonstandard multiplication $\times : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$

$$a * b = 0$$

for all $a, b \in \mathbb{Q}$. This makes $(\mathbb{Q}, +, *)$ a ring. It can be shown (<u>SIDE QUEST, 10pts</u>) that $\mathbb{Q}$ has no maximal subgroups (this rabbit trail $\Rightarrow$ §6.1#16, §3.2#21, §1.6#21 and §1#15 & §1.6#20)

$\therefore (\mathbb{Q}, +, *)$ has no maximal ideals.

Note the ring in **E2** is not unital. It turns out that if R has a multiplicative identity $1 \neq 0$ then maximal ideals must exist.

<u>PROPOSITION</u>: In a ring containing 1 every proper ideal is contained in a maximal ideal.

<u>PROOF</u>: (following Dummit & Foote p. 254 we look to use Zorn's Lemma)

Let R be a ring with $1 \in R$ and let I be a proper ideal. Notice $R = 0$ is forbidden. Let

$$S = \{ J \mid J \neq R,\ J \text{ ideal with } I \subseteq J \}$$

Observe $I \in S$ hence $S \neq \emptyset$. Notice S is partially ordered via inclusion. If C is a chain in S then let

$$J = \bigcup_{A \in C} A$$

Observe $J \neq \emptyset$ since $0 \in A \Rightarrow 0 \in J$. Suppose $a, b \in J$ then $\exists\ A, B \in C$ s.t. $a \in A$ and $b \in B$. But note either $A \subseteq B$ or $B \subseteq A$ and thus $a - b \in J$

Proof continued

Working to show $J = \bigcup_{A \in \mathcal{C}} A$ is an ideal, we shown J is subring. Notice J is closed under mult. by R since $RA \subseteq A$ and $AR \in A$ for each $A \in \mathcal{C}$ hence $RJ \subseteq J$ and $JR \subseteq J$ by def^n of union. Thus J is an ideal. If J is not proper then $J = R$ thus $1 \in J$. Thus $1 \in A$ for some $A \in \mathcal{C}$ which is $\rightarrow\leftarrow$ since $A \in \mathcal{C} \subseteq \mathcal{S}$.

Therefore, each chain has an upper bound in $\mathcal{S}$. By Zorn's Lemma $\mathcal{S}$ has maximal element which serves as a maximal proper ideal containing I. //

ZORN'S LEMMA: If $\mathcal{X}$ is a nonempty partially ordered set in which every chain has an upper bound then $\mathcal{X}$ has maximal element

Def^n A partial order on a nonempty set $\mathcal{X}$ is a relation on $\mathcal{X}$ denoted $\leq$ satisfying

(1.) $x \leq x$
(2.) if $x \leq y$ and $y \leq x$ then $x = y$, $\forall x, y \in \mathcal{X}$
(3.) if $x \leq y$ and $y \leq z$ then $x \leq z$, $\forall x, y, z \in \mathcal{X}$.

Def^n Let the nonempty set $\mathcal{X}$ be partially ordered by $\leq$

(1.) A subset $\mathcal{B}$ of $\mathcal{X}$ is called a chain if for all $x, y \in \mathcal{B}$ either $x \leq y$ or $y \leq x$.
(2.) An upper bound for the subset $\mathcal{B}$ of $\mathcal{X}$ is an element $x \in \mathcal{X}$ s.t. $b \leq x$ $\forall b \in \mathcal{B}$.
(3.) A maximal element of $\mathcal{X}$ is $m \in \mathcal{X}$ s.t. if $m \leq x$ for any $x \in \mathcal{X}$ then $m = x$.

4.3 Lecture 23: prime and maximal ideals

The definition below is very important. We need to remember and absorb these terms for the remainder of our study of rings.

Definition 4.3.1. *Let R be a commutative ring and A a proper ideal of R,*

(i.) *A is a* **prime ideal** *of R if $a, b \in R$ and $ab \in A$ implies $a \in A$ or $b \in A$.*

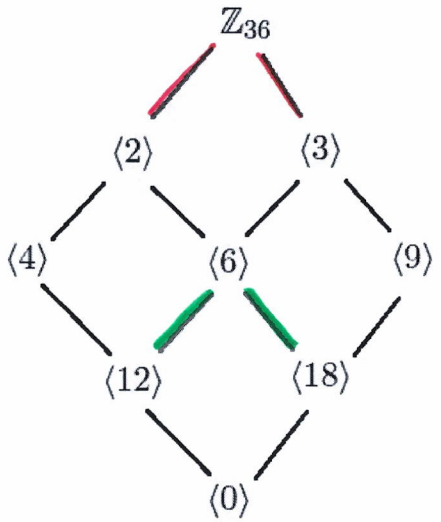
(ii.) *A is a* **maximal ideal** *of R if any ideal B of R with $A \subseteq B \subseteq R$ has $B = A$ or $B = R$.*

The terminology of prime naturally ties into the concept of prime we know from our work in $\mathbb{Z}$. Recall that Euclid's Lemma states that if a prime $p \mid ab$ then $p \mid a$ or $p \mid b$.

Example 4.3.2. *Let p be a prime and consider the ideal $p\mathbb{Z}$. If $a, b \in \mathbb{Z}$ and $ab \in p\mathbb{Z}$ then $ab = pk$ for some $k \in \mathbb{Z}$ hence $p \mid ab$ and thus $p \mid a$ or $p \mid b$ by Euclid's Lemma. If $p \mid a$ then $a = pn$ for some $n \in \mathbb{Z}$ and hence $a \in p\mathbb{Z}$. Likewise, $p \mid b$ then $b \in p\mathbb{Z}$. In summary, if p is prime then $p\mathbb{Z}$ is a prime ideal.*

I suppose I should mention, there is another way of defininining a prime ideal which helps make the correspondence between containment of ideals and divisibility of integers a bit more clear. See Lecture 22 of my Math 307 notes if you're interested.

Example 4.3.3. *Consider $\mathbb{Z}_{36}$ the ideals $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals in $\mathbb{Z}_{36}$. On the other hand, we also note $\langle 12 \rangle$ and $\langle 18 \rangle$ are maximal ideals in $\langle 6 \rangle$. You can see the maximality in the lattice diagram below:*



You might notice $\mathbb{Z}_{36}/2\mathbb{Z}_{36} \cong \mathbb{Z}_2$ and $\mathbb{Z}_{36}/3\mathbb{Z}_{36} \cong \mathbb{Z}_3$ are both fields. What about $\langle 6 \rangle / \langle 12 \rangle$? I'll be explicit,

$$\langle 6 \rangle = \{0, 6, 12, 18, 24, 30\} \qquad \& \qquad \langle 12 \rangle = \{0, 12, 24\}$$

So, you can see,

$$\langle 6 \rangle / \langle 12 \rangle = \{\langle 12 \rangle, 6 + \langle 12 \rangle\} \cong \mathbb{Z}_2$$

Showing $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$ requires some careful calculation:

we do find easier arguments later.

Example 4.3.4. *Let A be an ideal of $\mathbb{R}[x]$ for which $\langle x^2+1\rangle \subseteq A \subseteq \mathbb{R}[x]$ and $A \neq \langle x^2+1\rangle$. In other words, suppose $\langle x^2+1\rangle$ is properly contained in A. There exists $f(x) \in A$ and $f(x) \notin \langle x^2+1\rangle$. By the division of polynomials, there exists $q(x), r(x) \in \mathbb{R}[x]$ for which*

$$f(x) = q(x)(x^2+1) + r(x)$$

and $r(x) \neq 0$ and $r(x) = ax+b$. Note $r(x) \neq 0$ indicates at least one of a, b is nonzero. Furthermore,

$$ax + b = f(x) - q(x)(x^2+1) \in A$$

since $f(x) \in A$ and $q(x)(x^2+1) \in \langle x^2+1\rangle \subseteq A$ and A is an ideal. Moreover,

$$a^2x^2 - b^2 = (ax+b)(ax-b) \in A$$

since the produce of $ax+b \in A$ and $ax-b \in \mathbb{R}[x]$ must be in A again as A is an ideal. As $\langle x^2+1\rangle$ is contained in A we also may note $a^2(x^2+1) \in A$. Therefore,

$$0 \neq a^2 + b^2 = (a^2x^2 + a^2) - (a^2x^2 - b^2) \in A$$

But, $1 = \frac{1}{a^2+b^2}(a^2+b^2) \in A$ hence $\langle 1\rangle \subset A$ and $\langle 1\rangle = \{(1)f(x) \mid f(x) \in \mathbb{R}[x]\} = \mathbb{R}[x]$. Therefore, $\langle x^2+1\rangle$ is a maximal ideal.

I followed Gallian on page 258-259 for the most part in the example above. Likewise, the next example is Gallian's Example 16 on page 259.

Example 4.3.5. *In $\mathbb{Z}_2[x]$ the ideal $\langle x^2+1\rangle$ is not a prime ideal as $(x+1)^2 = x^2+2x+1 = x^2+1 \in \langle x^2+1\rangle$ yet $x+1 \notin \langle x^2+1\rangle$. To elaborate on the noncontainment claim, suppose $x+1 \in \langle x^2+1\rangle$ for some $f(x) \in \mathbb{Z}_2[x]$ we need*

$$x + 1 = f(x)(x^2+1)$$

why can we not solve the above for appropriate $f(x) \in \mathbb{Z}_2[x]$?

Theorem 4.3.6. *Let R be a commutative ring with unity and let A be an ideal of R. The quotient ring R/A is an integral domain if and only if A is prime.*

Proof: suppose R is a unital commutative ring with ideal A in R. Suppose R/A is an integral domain. Let $a, b \in R$ and $ab \in A$. Note,

$$A = ab + A = (a+A)(b+A)$$

thus $a+A = A$ or $b+A = A$ as R/A has no zero divisors (here A serves as zero in R/A). Hence $a \in A$ or $b \in A$.

Conversely, suppose A is a prime ideal. We need to show R/A has no zero divisors. Suppose $(a+A)(b+A) = A$ then $ab+A = A$ hence $ab \in A$. But, A is prime hence $a \in A$ or $b \in A$ thus $a+A = A$ or $b+A = A$. Furthermore, denoting the unity of R as 1 we note that $(1+A)(r+A) = 1r+A = r+A$ for each $r+A \in R/A$. Also, calculate $(r+A)(s+A) = rs+A = sr+A = (s+A)(r+A)$ hence R/A is a commutative ring. Therefore, R/A is an integral domain. □

Theorem 4.3.7. *Let R be a commutative ring with unity and let A be an ideal of R. The quotient ring R/A is a field if and only if A is maximal.*

Proof: suppose R is a commutative ring with unity $1 \in R$ and suppose A is an ideal of R. Assume R/A is a field. Consider an ideal B of R for which $A \subseteq B \subseteq R$ with $A \neq B$. It follows there exists $x \in B$ for which $x \notin A$ hence $x + A \neq A$ which means $x + A$ is a nonzero element in R/A. Since R/A is a field and $1 + A$ serves as the unity we have the existence of $y + A$ for which $(x + A)(y + A) = 1 + A$. Thus, $xy + A = 1 + A$ and we find $1 - xy \in A$. However, $x \in B$ implies $xy \in B$ as B is an ideal. Since $A \subseteq B$ we find $1 - xy \in B$. Thus,

$$xy + (1 - xy) = 1 \in B$$

But, $x = 1(x) \in B$ for each $x \in R$ hence $B = R$ and we find A is a maximal ideal.

Conversely, suppose A is a maximal ideal. Suppose $x \in R$ yet $x \notin A$. In other words, we consider a nonzero element $x + A$ in R/A. Construct,

$$B = \{xr + a \mid r \in R, a \in A\}$$

I'll leave it to the reader to verify that B is indeed an ideal of R. Moreover, if $a \in A$ then note $a = x(0) + a \in B$ thus $A \subseteq B$. By maximality of A we have $B = R$. Therefore, $1 \in B$ and we find there exists $r \in R, a \in A$ for which $xr + a = 1$ or $1 - xr = a \in A$. Observe, $(x+A)(r+A) = xr+A = 1+A$. Thus $x+A$ has multiplicative inverse $r+A$ in R/A. Furthermore, we note that $(1+A)(r+A) = 1r+A = r+A$ for each $r+A \in R/A$. Also, calculate $(r+A)(s+A) = rs+A = sr+A = (s+A)(r+A)$ hence R/A is a commutative ring with unity where every nonzero element has a multiplicative inverse. That is, R/A forms a field. □

Example 4.3.8. *Since a field is an integral domain it follows that a maximal ideal must be a prime ideal in view of Theorems 4.3.6 and 4.3.7. On the other hand, we can exhibit an ideal which is prime, but, not maximal. Consider* $\langle x \rangle$ *in* $\mathbb{Z}[x]$ *if* $f(x), g(x) \in \mathbb{Z}[x]$ *and* $f(x)g(x) \in \langle x \rangle$ *then* $f(x)g(x) = xh(x)$ *for some* $h(x) \in \mathbb{Z}[x]$. *It follows that* x *must be a factor in* $f(x)$ *or* $g(x)$ *thus* $f(x) \in \langle x \rangle$ *or* $g(x) \in \langle x \rangle$ *and we find* $\langle x \rangle$ *is a prime ideal of* $\mathbb{Z}[x]$. *Consider,* $\langle x, 2 \rangle$ *contains* $\langle x \rangle$ *since* $\langle x, 2 \rangle = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ *so to obtain* $\langle x \rangle$ *simply select elements with* $g(x) = 0$. *On the other hand,* $2 \in \langle x, 2 \rangle$ *and* $2 \notin \langle x \rangle$. *Also,* $1 \in \mathbb{Z}[x]$ *and* $1 \notin \langle 2, x \rangle$ *hence* $\langle x \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x]$. *This proves* $\langle x \rangle$ *is not maximal.*

PROPOSITION: Assume R is commutative ring with $1 \in R$. The ideal M is maximal ideal $\Leftrightarrow$ R/M is a field.

($\Rightarrow$) Suppose M is a maximal ideal. Suppose $x \in R$ yet $x \notin M$. In other words, we consider a nonzero element $x + M \in R/M$. Construct,

$$B = \{ xr + m \mid r \in R,\ m \in M \}$$

We can prove B is an ideal of R. Let

$xr_1 + m_1,\ xr_2 + m_2 \in B$ then

$$(xr_2 + m_2) - (xr_1 + m_1) = x(r_2 - r_1) + m_2 - m_1 \in B$$

$$(xr_2 + m_2)(xr_1 + m_1) = x(r_2 x r_1 + m_2 r_1 + m_1 r_2) + m_1 m_2 \in B$$

thus B is a subring and if $r \in R$ then

$$r(xr_1 + m_1) = x(rr_1) + rm_1 \in B$$

since $m_1 \in M$, $r \in R \Rightarrow rm_1 \in M$ as M is an ideal.

Hence B is an ideal of R. Let $z \in M$ then $z = x(0) + z \in B$ thus $M \subseteq B$. By maximality we find $B = R$. Consequently, $1 \in B$ and $\exists\, r \in R, m \in M$ for which $xr + m = 1 \Rightarrow 1 - xr = m \in M$. Thus

$$(x + M)(r + M) = xr + M = 1 + M$$

Thus $(x + M)^{-1} = r + M \in R/M$ $\therefore$ R/M is a commutative ring with every nonzero element a unit. That is, R/M is a field. //