Properties of ideals

For this section, let R be a ring w/ identity $1 \neq 0$.

Usually we define specific ideals of R by describing a generating set.

Def: Let $A \subseteq R$ be a subset.

1.) Let (A) be the smallest ideal of R containing A, called the ideal generated by A. i.e. $(A) = \bigcap_{I \supseteq A \text{ an ideal}} I$ (Exercise: this is an ideal!)

2.) If $A = \{a\}$, i.e. it consists of a single element, write $(A) = (a)$. If $I = (a)$, for some $a \in R$, it's called a principal ideal. e.g. $(1) = R$.

3) If A is finite, i.e. $A = \{a_1, \ldots, a_n\}$, write $(A) = (a_1, \ldots, a_n)$. If I has a finite generating set, it's called a finitely generated ideal.

4.) Define $RA := \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R, a_i \in A\}$

Similarly, $AR := \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R, a_i \in A\}$,

and $RAR := \{r_1 a_1 s_1 + \cdots + r_n a_n s_n \mid r_i, s_i \in R, a_i \in A\}$

Note that all the sums are finite sums.

Remark: By construction, RA is closed under subtraction.

If $s \in R$ and $r_1 a_1 + \cdots + r_n a_n \in RA$, then

$$s(r_1 a_1 + \cdots + r_n a_n) = (sr_1)a_1 + \cdots + (sr_n)a_n \in R.$$

Thus, RA is a left ideal. Similarly, AR is a right ideal, and RAR is an ideal.

Claim: $RAR = (A)$. i.e. RAR is the ideal generated by A.

Pf: By definition, $(A) = \bigcap_{\substack{I \text{ an ideal} \\ A \subseteq I}} I$. If $a \in A$, then $a = 1 \cdot a \cdot 1 \in RAR$.

Thus, $A \subseteq RAR$, so $(A) \subseteq RAR$.

If $\sum_{i=1}^{n} r_i a_i s_i \in RAR$, then since (A) is an ideal, $r_i a_i s_i \in (A)$, so the sum is as well. $\Rightarrow RAR = (A)$. $\square$

If R is commutative, then $RA = AR = RAR = (A)$.

Remark: If R is commutative, $a \in R$, then any element of (a) is of the form $r_1 a + \cdots + r_n a = (r_1 + \cdots + r_n)a$.
That is, $(a) = \{ra \mid r \in R\}$ (This doesn't necessarily work in a noncommutative ring.)

In this case, $b \in (a) \iff b = ra$, some $r \in R \iff (b) \subseteq (a)$.
"a divides b"

Ex: In $\mathbb{Z}$, $(n) = n\mathbb{Z}$, and $4 = 2 \cdot 2 \Rightarrow 4 \in (2) \Rightarrow (4) \subseteq (2)$.

Ex: Consider the ideal $(2, x) \subseteq \mathbb{Z}[x]$. Is this a principal ideal? i.e. does $(f(x)) = (2, x)$, for some $f(x) \in \mathbb{Z}[x]$?

If so, $2 = fg$, some $g \in \mathbb{Z}[x]$. Thus, f has degree 0, and is thus either ± 1 or ± 2. But $x \notin (2)$ and $(\pm 1) = \mathbb{Z}[x]$, so $(2, x)$ is not principal.

Def: Let I and J be ideals of R.

1.) The sum of I and J is $I + J := \{a + b \mid a \in I, b \in J\}$

2.) The product of I and J is IJ, the set of finite sums of elements of the form ab, with $a \in I$, $b \in J$.

Note that $I, J \subseteq I + J$. In fact, $I + J$ is the ideal generated by elements of I and J.

Note that if $x = \sum a_i b_i \in IJ$, then $x \in I \cap J$. That is $IJ \subseteq I \cap J$.
($a_i \in I$, $b_i \in J$)

They can be equal, but not always.

Ex: Let $I = (6)$, $J = (10)$ in $\mathbb{Z}$.

Then $I + J = \{6a + 10b \mid a, b \in \mathbb{Z}\}$.

Since $6a + 10b = 2(3a + 5b) \in (2)$ $\forall$ a, b, we know $I + J \subseteq (2)$.

Moreover, $2 = -6\cdot 3 + 10\cdot 2 \in I + J$. Thus, $(2) \subseteq I + J$, so $I + J = (2)$.

$$IJ = \{\Sigma 6a_i 10 b_i \mid a_i, b_i \in \mathbb{Z}\} = \{60c \mid c \in \mathbb{Z}\} = (60).$$

As mentioned above, if an ideal is generated by 1, it is all of R. In fact, we have the following:

Prop: Let I be an ideal of R. Then $I = R \iff I$ contains a unit.

Pf: If $I = R$, then $1 \in I$. Conversely, if $u \in I$, a unit, then $uv = 1$, some v, so $uv = 1 \in I$. $\Rightarrow \forall\ r \in R$, $r = 1\cdot r \in I$. Thus $I = R$. □

Since all the nonzero elements of a field are units, we get the following:

Cor: Let R be commutative. R is a field $\iff$ its only ideals are 0 and R.

Pf: If R is a field, $I \subseteq R$ an ideal, then if I contains some nonzero element, it's R. Otherwise it's 0.

Conversely, if the only ideals are 0 and R, consider $a \in R$ some nonzero element. Then $(a) = R$. Thus $1 = ab$, some $b \in R$.

Thus a is a unit. $\square$

Since kernels of homomorphisms are ideals, if F is a field, R a ring, then any homomorphism $\varphi: F \to R$ has to have kernel 0 or F. If the kernel is 0, it's injective. If the kernel is F, it's the zero map. That is...

Cor: Any nonzero homomorphism from a field is injective.

Maximal ideals

We talked a little about "maximal groups" in group theory. In ring theory, maximal ideals play a very important role.

Def: An ideal M in a ring R is a maximal ideal if $M \neq R$ and the only ideals containing M are M and R.

Ex: If F is a field, then 0 is the only maximal ideal.

In general, it can be difficult to check directly using the definition whether an ideal is maximal. Luckily, for commutative rings, we have the following criterion:

Prop: Assume R is commutative. The ideal M is maximal if and only if R/M is a field.

Pf: Suppose M is maximal. By the lattice isomorphism Theorem (!!), the only ideals of R/M are those of the form I/M, where $I \supseteq M$. Thus, R/M has ideals $M/M = 0$, and R/M. Thus, R/M is a field.

If R/M is a field, then, just as above, the only ideals containing M are R and M. Thus M is maximal. □

Remark: If R is a ring w/ 1, then any ideal I is contained in at least one maximal ideal. The proof (which we won't give) uses Zorn's Lemma.

Ex: As mentioned in the last section, the only ideals of $\mathbb{Z}$ are those of the form $n\mathbb{Z}$ $(= (n))$. $n\mathbb{Z}$ is maximal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field. This is the case if and only if n is prime.

Ex: $(2, x) \subseteq \mathbb{Z}[x]$ is maximal: If $f \in \mathbb{Z}[x]$, then $\overline{f} = \overline{0}$ or $\overline{1}$, depending on whether the constant term is odd or even.

So $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/2\mathbb{Z}$ is a field.

Prime ideals

We've been thinking about many of the definitions/properties

relating to ring as generalizations of $\mathbb{Z}$. Similarly, we can generalize the notion of "primeness".

More specifically, a prime integer p can be characterized by the property that if p divides mn, then p divides m or n.

Def: If R is commutative, $P \subseteq R$ an ideal, P is a prime ideal if $P \neq R$ and if $m, n \in R$ s.t. $mn \in P$, then $m \in P$ or $n \in P$.

Ex: Which ideals $n\mathbb{Z}$ of $\mathbb{Z}$ are prime? Suppose $ab \in n\mathbb{Z}$. Then n divides ab. We can conclude a or $b \in n\mathbb{Z}$ if and only if n is prime. That is, the prime ideals of $\mathbb{Z}$ are exactly those generated by a prime element. Note that in this case, the nonzero prime ideals are exactly the maximal ideals.

An important property of prime ideals is that if we mod out by them, the condition translates to the ring having no zero divisors. That is:

Theorem: Let R be a commutative ring, $P \subseteq R$ an ideal. Then P is prime if and only if R/P is an integral domain.

Pf: Let $\bar{a}$ denote $a + P \in R/P$. Let $r \in R$.

Note that $\bar{r} = 0 \iff r + P = 0 + P \iff r \in P$

Thus, if P is prime, $\overline{ab} = \bar{0} \Rightarrow a \in P$ or $b \in P \Rightarrow \bar{a} = 0$ or $\bar{b} = 0$.

$\bar{1} \neq 0$, since $P \neq R$, so R/P is an integral domain.

If R/P is an integral domain, then if $ab \in P$, $\bar{a}\bar{b} = 0$, so $\bar{a} = 0$ or $\bar{b} = 0$, so $a \in P$ or $b \in P$. $R/P \neq 0$, so $P \neq R$. Thus P is prime. □

We saw that in the case of the integers, $0 \neq I \subseteq \mathbb{Z}$ is prime $\iff$ I is maximal. While this is not usually the case in an arbitrary ring, one implication always holds:

Corollary: If R is commutative, every maximal ideal is prime.

Pf: If M is maximal, then R/M is a field and thus an integral domain. Thus M is prime. □

Ex: Consider $(x) \subseteq \mathbb{Z}[x]$. $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, so (x) is prime, but not maximal.

However $(x) \subseteq \mathbb{Q}[x]$ is maximal.

More generally, $(x) \subseteq R[x]$ is prime $\iff$ R is an integral domain, and maximal $\iff$ R is a field.