Class 20

April 9, 2024

Ideals

A subring I of ring R is called a (two-sided) ideal of R if $\forall r \in R$ and $\forall a \in I$, $ra \in I$ and $ar \in I$.

A few things to note about this definition:

- Ideals are in some sense related to normal subgroups in group theory. These are subrings with important properties for quotient rings (more on them later).
- We will only work with two-sided ideals in this class, so for our purposes we can assume all ideals are two-sided. In general, there are also left and right ideals.
- An ideal "absorbs" elements of R. This means $rI \subseteq I$ and $Ir \subseteq I$.

Ideal Test

Similar to the subring test, there is an ideal test. Let I be a subset of R. Then I is an ideal of R if

1. $a - b \in I$ for all $a, b \in I$
2. $ra, ar \in I \ \forall a \in I, r \in R$

Proof

We can rely on the subring test. As $I \subseteq R$, then axiom 2 of the ideal test implies $ab \in I$ for all $b \in I$, as $b \in R$ as well. As axiom 1 is the same for both tests, then the ideal test implies that I is a subring of R. As I is a subring, and axiom 2 is the definition of an ideal, then the ideal test can tell us if any subset of R is an ideal.

Ex 1

$\forall n \in \mathbb{Z}^+$, the subring $n\mathbb{Z} = \{na | a \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

pf

Let $a, b \in n\mathbb{Z}$ such that $a = nx, b = ny$ for some $x, y \in \mathbb{Z}$. Then using the ideal test,

$$a - b = nx - ny = n(x - y) \in n\mathbb{Z}$$

Suppose $x \in \mathbb{Z}$ and $a = ny \in n\mathbb{Z}$. Then

$$xa = x(ny) = n(xy) \in n\mathbb{Z}$$

$$ax = (ny)x = n(yx) \in n\mathbb{Z}$$

As both axioms are met, then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Ex 2

Let R be a commutative ring, and let the ideal generated by $a \in R$ be given as

$$\langle a \rangle = \{ra | r \in R\}$$

Then $\langle a \rangle$ is an ideal.

pf

First, let $ra, sa \in \langle a \rangle$. Then

$$ra - sa = (r - s)\, a \in \langle a \rangle$$

as $r - s \in R$. Now, suppose $r \in R$, $sa \in \langle a \rangle$. Then

$$r\,(sa) = (rs)\, a \in \langle a \rangle$$

and

$$(sa)\, r = s\,(ar) = s\,(ra) = (sr)\, a \in \langle a \rangle$$

Thus $\langle a \rangle$ satisfies the requirements of the ideal test and $\langle a \rangle$ is an ideal of R.

Ex 3

$R = \mathbb{R}[x]$, and let $I = \left\{\sum_{i=1}^{\infty} c_i x^i | c_i \in \mathbb{R}\right\}$ or in other words, I is the set of all polynomials with real coefficients such that the constant term is 0.

pf

Let's show $I = \langle x \rangle$. Note that $\sum_{i=1}^{\infty} c_i x^i = x \sum_{i=1}^{\infty} c_i x^{i-1}$ as each $c_i \in \mathbb{R}$ then $\sum_{i=1}^{\infty} c_i x^{i-1}$ is an arbitrary element of R, thus

$$I = \langle x \rangle = \{xr | r \in R\} = \left\{x \sum_{i=1}^{\infty} c_i x^{i-1} | c_i \in R\right\} = \left\{\sum_{i=1}^{\infty} c_i x^i | c_i \in \mathbb{R}\right\}$$

As $I = \langle x \rangle$, then I is an ideal by **Ex 2**.

Ex 4

Let $R = M_2[\mathbb{Z}]$ and $I = M_2[2\mathbb{Z}]$. Then using the ideal test:

Let $A, B \in I$ such that $A = \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}, B = \begin{pmatrix} 2e & 2f \\ 2g & 2h \end{pmatrix}$. Then

$$A - B = \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix} - \begin{pmatrix} 2e & 2f \\ 2g & 2h \end{pmatrix} = \begin{pmatrix} 2a - 2e & 2b - 2f \\ 2c - 2g & 2d - 2h \end{pmatrix} = \begin{pmatrix} 2\,(a-e) & 2\,(b-f) \\ 2\,(c-g) & 2\,(d-h) \end{pmatrix} \in I$$

Now, suppose $C = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in R$. Then

$$AR = \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 2ax + 2bz & 2ay + 2bw \\ 2cx + 2dz & 2cy + 2dw \end{pmatrix} = \begin{pmatrix} 2\,(ax+bz) & 2\,(ay+bw) \\ 2\,(cx+dz) & 2\,(cy+dw) \end{pmatrix} \in I$$

Similarly,

$$RA = \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix} = \begin{pmatrix} x2a + y2c & x2b + y2d \\ z2a + w2c & z2b + w2d \end{pmatrix} = \begin{pmatrix} 2\,(xa+yc) & 2\,(xb+yd) \\ 2\,(za+wc) & 2\,(zb+wd) \end{pmatrix} \in I$$

Thus I is an ideal.

Quotient Rings

Let R be a ring and I be a subring of R. The set of cosets $R/I = \{r + I | r \in R\}$ is a ring under the operations $(s+I)+(t+I) = (s+t)+I$ and $(s+I)\,(t+I) = st+I$
if and only if I is an ideal.

pf

Suppose I is a subring of R. Then I is a subgroup of R under addition. Furthermore, since R is commutative under addition, this implies that I is a normal subgroup. (As every subgroup of an abelian group is normal). As I is normal, then R/I will be an abelian group under addition of cosets, as R/I is a group when I is normal, and R/I is abelian when R is abelian (As shown in previous lectures and homework assignments). Now, for the multiplication property, we will consider two cases:

First, suppose I is an ideal. Then

$$(s+I)(t+I) = st + I \in R/I$$

as $st \in R$. To show this is well defined, let's multiply explicitly:

$$(s+I)(t+I) = st + sI + tI + II = st + I + I + I = st + I$$

so multiplication is well defined. Now, to show associativity: let $s+I, t+I, u+I \in R/I$. Then

$$((s+I)(t+I))(u+I) = (st+I)(u+I) = (st)u + I$$

$$= s(tu) + I = (s+I)(tu+I) = (s+I)((t+I)(u+I))$$

Finally, let's show the distributive laws: let $s+I, t+I, u+I \in R/I$. Then

$$(s+I)((t+I)+(u+I)) = (s+I)((t+u)+I)$$

$$= s(t+u) + I = st + su + I = st + I + su + I$$

$$(s+I)(t+I) + (s+I)(u+I)$$

Similarly, we can show the right distribution law:

$$((t+I)+(u+I))(s+I) = ((t+u)+I)(s+I)$$

$$= (t+u)s + I = ts + us + I = ts + I + us + I$$

$$(t+I)(s+I) + (u+I)(s+I)$$

Suppose that I is not an ideal. Then there exists elements $r \in R$, $a \in I$ such that

$$ra \notin I \text{ or } ar \notin I$$

WLOG suppose

$$ra \notin I$$

then

$$a + I = 0 + I$$

$$(r+I)(a+I) = (r+I)(0+I)$$

$$ra + I = r0 + I = I$$

but $ra \notin I$ so $ra + I \neq I$! Thus multiplication is not well defined if I is not an ideal.

Ex 1

$R = \mathbb{Z}$, $I = n\mathbb{Z}$ then

$$R/I = \{I, 1+I, \ldots, (n-1)+I\}$$

Ex 2

$R = \mathbb{R}[x]$, and $I = \left\{\sum_{i=1}^{\infty} c_i x^i | c_i \in \mathbb{R}\right\}$

$$R/I = \{a + I | a \in \mathbb{R}\}$$

Ex 3

$R = M_2[\mathbb{Z}]$ and $I = M_2[2\mathbb{Z}]$

$$R/I = \left\{\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) + I | a, b, c, d \in \{0,1\}\right\}$$

Prime and Maximal Ideals

An ideal I of a ring R is a prime ideal if $I \neq R$ and for all $a, b \in R$ such that $ab \in I$, either $a \in I$ or $b \in I$. An ideal I of a ring R is a maximal ideal if $I \neq R$ and for any ideal B of R such that $I \subset B$, $B = R$.

Note that in general not every maximal ideal is prime and not every prime ideal is maximal.

Ex 1

For $R = \mathbb{Z}$, $I = n\mathbb{Z}$ is a prime ideal if and only if n is prime. Suppose n is prime. Then if $ab = nx$ for some integer x, then either a or b has n as a prime factor, thus a or b will be in I. I is also maximal.

Ex 2

Let $R = \mathbb{Z}_{12}$. The possible proper ideals of $\mathbb{Z}_{12}$ are $\langle 0 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle$. Here, $\langle 2 \rangle, \langle 3 \rangle$ are both prime and maximal. The other ideals are neither.

Ex 3

With non-commutative rings, these can be quite difficult to determine. For $R = M_2[\mathbb{Z}]$, $I = M_2[2\mathbb{Z}]$, I is not prime as

$$\left(\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array}\right)\left(\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array}\right) = \left(\begin{array}{cc} 2 & 2 \\ 2 & 2 \end{array}\right) \in I$$

even though $\left(\begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array}\right) \notin I$. Despite this I is maximal (The proof is outside of the scope of this course). We will derive a couple of theorems to help related these special types of ideals.

Thm

For a commutative ring with unity R with ideal I, R/I is an integral domain if and only if I is prime.

Pf

First, suppose R/I is an integral domain. Suppose $a, b \in R$ satisfy

$$(a + I)(b + I) = ab + I = 0 + I$$

Thus if $ab \in I$, then either $a + I = 0 + I$ or $b + I = 0 + I$ so $a \in I$ or $b \in I$ and I is prime. Now, suppose I is prime. Then $ab \in I$ implies that $a \in I$ or $b \in I$, thus if

$$0 + I = ab + I = (a + I)(b + I)$$

then either $a + I = 0 + I$ (if $a \in I$) or $b + I = 0 + I$ (if $b \in I$). Thus R/I is an integral domain.

Thm

For a commutative ring with unity R, R/I is a field if and only if I is maximal.

Pf

Suppose R/I is a field and B is an ideal of R such that $I \subset B$. We will show $B = R$ (and thus I is maximal). Let $b \in B$ such that $b \neq I$. Then $\exists c \in R$ such that

$$(b+I)(c+I) = bc + I = 1 + I$$

Subtracting from both sides

$$1 - bc + I = I$$

thus $1 - bc \in I \subset B$. As $bc \in B$, then

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

As $1 \in B$, then for any $r \in R$, $1r = r \in B$ so $B = R$, thus I is maximal. Now, suppose I is maximal. Then let $b \in R$ such that $b \notin I$. We want to show that $b + I$ has an inverse. We do not need to check for any elements of R that are in I as for all $a \in I$, $a + I = 0 + I$ and fields require that the non-zero elements have multiplicative inverses. Before we show this, let's start by showing there exists an ideal B such that $I \subset B$ of the form

$$B = \{br + a | r \in R, a \in I\}$$

Using the ideal test

$$(br_1 + a_1) - (br_2 + a_2) = br_1 - br_2 + a_1 - a_2$$

$$= b(r_1 - r_2) + (a_1 - a_2) \in B$$

as $r_1 - r_2 \in R$ and $a_1 - a_2 \in I$. Now for the product, let $s \in R$. As R is commutative

$$s(br + a) = (br + a)s = brs + as \in B$$

as $rs \in R, as \in I$. Now that we have shown B is an ideal, we can prove the original statement. As $I \subset B$, then $B = R$, as I is maximal. Suppose $1 = bc + a'$ for some $a' \in I$. Then

$$1 + I = (bc + a') + I = bc + a' + I = bc + I = (b + I)(c + I)$$

Thus every nonzero element $b + I \in R/I$ has an inverse, so R/I is a field.