Chapter 5 Ideals and Quotient Rings

5.1 Ideals and Congruence

Let R and S be rings and $\varphi: R \to S$ a ring homom. Recall we defined $\ker \varphi = \{r \in R : \varphi(r) = 0_S\}$. We showed this is a subring of R, but even more, we showed if $r_1 \in R$ and $r_2 \in \ker\varphi$, then $r_1 r_2 \in \ker\varphi$ since $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) = \varphi(r_1)0_S = 0_S$. Thus, $\ker\varphi$ is not only closed under multiplication of elements in $\ker\varphi$, it is closed under multiplication by the elements of R as well! We give such subrings a name.

Def: Let $I \subseteq R$ be a subring. If given any $r \in R$ and $a \in I$ we have $ra \in I$ and $ar \in I$, we say I is an *ideal*.

Example: Let $R = \mathbb{Z}$ and consider the subring $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ for some $n \in \mathbb{Z}$. (Check this is a subring as an exercise if you don't recall this.) Let $m \in \mathbb{Z}$ and $nt \in n\mathbb{Z}$. Then $m(nt) = n(mt) = (nt)m \in n\mathbb{Z}$. Thus, $n\mathbb{Z}$ is an ideal. Note that $n\mathbb{Z} = \ker\varphi$ where

$$\varphi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$m \longmapsto [m]_n.$$

Example: Let $R = F[x]$ and $I = \{f F[x] = \langle f \rangle$ for $f \in F[x]$ where

$$f \cdot F[x] = \langle f \rangle = \{ g \in F[x] : f \mid g \}.$$

We have $0_F \in \langle f \rangle$. If $g, h \in \langle f \rangle$, then gh and $g+h$ are both clearly seen to be in $\langle f \rangle$ as $\langle f \rangle$ is a subring of $F[x]$. Moreover, if $h \in F[x]$ and $g \in \langle f \rangle$, then we have $hg \in \langle f \rangle$ because $f \mid g$, as $f \mid hg$. Thus, $\langle f \rangle$ is an ideal.

Example: Let $R = \mathbb{Q}$ and $I = \mathbb{Z}$. Then I is a subring, but not an ideal because $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin I$.

Example: Let $R = Mat_2(\mathbb{Q})$ and $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in Mat_2(\mathbb{Q}) \right\}$.

You can check as an exercise that I is a subring of R.

Let $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in I$ and $\begin{pmatrix} c & d \\ e & f \end{pmatrix} \in R$. Then

$$\begin{pmatrix} c & d \\ e & f \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ca + bd & 0 \\ ae + bf & 0 \end{pmatrix} \in I.$$

However, $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$, so if we consider $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin I$. Thus, I is not an ideal. Since it is closed on the left, one sometimes

studies such ideals anyway and refers to them as left ideals.

Theorem 5.1.1: Let $I \subseteq R$ be a nonempty subset. Then I is an ideal iff

1) if $a, b \in I$, then $a - b \in I$
2) if $r \in R$, $a \in I$, then $ra \in I$, and $ar \in I$.

Proof: Exercise. ∎

We saw a couple examples above where given a ring R, we took any element $r \in R$ and considered

$$I = rR = \langle r \rangle = \{ ar \in R : a \in R \}.$$

One had this is an ideal in those cases and the same proof shows that is an ideal in general. We call such an ideal a principal ideal generated by r. In some rings the only ideals are principal ideals.

Theorem 5.1.2: Every ideal in $\mathbb{Z}$ is a principal ideal.

Proof: Let $I \subseteq \mathbb{Z}$ be an ideal. Since I is nonempty, and closed under multiplication by -1, there are positive elements in I as long as $I \neq \{0\}$. Since $\{0\}$ is principal, assume $I \neq \{0\}$. Let $S = \{ n \in I : n > 0 \}$. This is a nonempty

set of positive integers, so the well ordering axiom gives a minimal element $n \in S$. We claim $I = n\mathbb{Z}$. Since $n \in I$ and I is an ideal, $nm \in I$ for all $m \in \mathbb{Z}$, ie, $n\mathbb{Z} \subseteq I$. Let $a \in I$. We need to show $n \mid a$. Write $a = nq + r$ with $0 \leq r < n$. Then $r = a - nq$. Since $a \in I$, $n \in I$, we have $nq \in I$ so $a - nq \in I$. However, this gives $r \in I$. This is a contradiction to n minimal unless $r = 0$, ie, $n \mid a$. Thus, $a \in n\mathbb{Z}$ and so $I = n\mathbb{Z}$. ∎

Not all rings have just principal ideals though. Let R be a commutative ring and $r_1, \ldots, r_n \in R$. Define

$$\langle r_1, \ldots, r_n \rangle = \{ r_1 a_1 + \cdots + r_n a_n : a_i \in R \}.$$

Theorem 6.5.1.3: The collection $\langle r_1, \ldots, r_n \rangle$ is an ideal of R.

Proof: We have $0_R = r_1 0_R + \cdots + r_n 0_R \in \langle r_1, \ldots, r_n \rangle$, so it is a nonempty set. Let $a = r_1 a_1 + \cdots + r_n a_n$, $b = r_1 b_1 + \cdots + r_n b_n$ be elements of $\langle r_1, \ldots, r_n \rangle$ and let $r \in R$. Then

$$a - b = r_1(a_1 - b_1) + \cdots + r_n(a_n - b_n) \in \langle r_1, \ldots, r_n \rangle$$

and

$$ra = r_1(a_1 r) + \cdots + r_n(a_n r) \in \langle r_1, \ldots, r_n \rangle.$$

Thus, by Theorem 3.1.1 we have $\langle r_1, \ldots, r_n \rangle$ is an ideal of R. ∎

We call $\langle r_1, \ldots, r_n \rangle$ the <u>ideal generated by $r_1, \ldots, r_n$</u>. Given an ideal $I \subseteq R$, if there is an $n \in \mathbb{Z}_{\geq 1}$ and elements $r_1, \ldots, r_n \in I$ so that $I = \langle r_1, \ldots, r_n \rangle$ we say I is <u>finitely generated</u>.

<u>Exercise:</u> Let $I \subseteq R$ be an ideal. Show $I = R$ if and only if I contains a unit.

<u>Example:</u> Let $R = \mathbb{Z}[x]$ and consider $I = \langle 2, x \rangle$. Our first claim is $1 \notin \langle 2, x \rangle$. Suppose $1 \in \langle 2, x \rangle$. Then $1 = 2f + xg$ for some $f, g \in \mathbb{Z}[x]$. By considering degrees we see $g = 0$ and $f \in \mathbb{Z}$. However, 2 is not invertible in $\mathbb{Z}$ so this is a contradiction. Thus, $1 \notin \langle 2, x \rangle$.

Our next claim is $\langle 2, x \rangle$ is not principal. Suppose $\langle 2, x \rangle = \langle f \rangle$ for some $f \in \mathbb{Z}[x]$. Then we have $2 \in \langle f \rangle$, so there exists $g \in \mathbb{Z}[x]$ so that $fg = 2$. This gives $f = 1$ or 2 by degree argument and the fact 2 is prime in $\mathbb{Z}$. If $f = 1$, then $\langle 2, x \rangle = \langle 1 \rangle = \mathbb{Z}[x]$. This is a contradiction to our first claim. Thus, $f = 2$. We must also have $x \in \langle f \rangle = \langle 2 \rangle$. Thus, there exists $h \in \mathbb{Z}[x]$ so that $x = 2h$. Since $1 = \deg x = \deg h$,

we have $h = ax + b$ for some $a, b \in \mathbb{Z}$. Thus,

$$X = 2ax + 2b.$$

This gives $b = 0$ and $2a = 1$. This is a contradiction to $\mathbb{Z}$ not being invertible in $\mathbb{Z}$. Thus, $\langle 2, X \rangle \neq \langle f \rangle$ and so is not principal.

Our next step is to talk about congruences for general rings. Before we do this, we rephrase our work with $\mathbb{Z}/n\mathbb{Z}$. Recall, we defined $a \equiv b \pmod{n}$ to mean $n \mid (a-b)$. Another way to say this is to say $a - b \in n\mathbb{Z}$. Thus, we could also write $a \equiv b \pmod{I}$ if we write $I = n\mathbb{Z}$ to mean $a - b \in I$. We can generalize this notation to general rings and ideals.

<u>Def:</u> Let R be a ring and $I \subseteq R$ an ideal. We say $a, b \in R$ are <u>congruent modulo I</u> and write $a \equiv b \pmod{I}$ if $a - b \in I$.

<u>Example:</u> 1) Consider $I = \langle x \rangle \subseteq F[x]$. We have $f \equiv g \pmod{I}$ if $f - g \in \langle x \rangle$, ie, if $x \mid (f-g)$. This is equivalent to f and g having the same constant term, i.e. the polynomial functions are equal at 0, $f(0) = g(0)$.

2) Consider $I = \langle x^2 \rangle \subseteq F[x]$. Here we have $f \equiv g \pmod{I}$ if $f - g \in \langle x^2 \rangle$ ie, $x^2 \mid (f-g)$. This is equivalent to $f(0) = g(0)$ and $f'(0) = g'(0)$, ie, They have the same first two terms.

Theorem 5.1.4: Let $I \subseteq R$ be an ideal. The relation congruence modulo I is an equivalence relation, i.e.,

1) reflexive: if $a \in R$, then $a \equiv a \pmod{I}$
2) symmetric: if $a \equiv b \pmod{I}$, then $b \equiv a \pmod{I}$
3) transitive: if $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$, then $a \equiv c \pmod{I}$.

Proof: 1) Since I is a subring, $0_R \in I$. Thus, for any $a \in R$, we have $a - a = 0_R \in I$.

2) Suppose $a - b \in I$. Then since I is an ideal, $-(a-b) \in I$, i.e., $b - a \in I$.

3) Let $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$. Thus, $a - b = i_1 \in I$ and $b - c = i_2 \in I$. Then $a - c = (a-b) + (b-c) = i_1 + i_2 \in I$. ∎

Theorem 5.1.5: Let $I \subseteq R$ be an ideal and $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$. Then:

1) $a + c \equiv b + d \pmod{I}$;
2) $ac \equiv bd \pmod{I}$.

Proof: 1) We have $a - b = i_1 \in I$ and $c - d = i_2 \in I$. We observe that

$$a + c = (b + i_1) + (d + i_2)$$
$$= (b + d) + (i_1 + i_2),$$

i.e.,

$$(a + c) - (b + d) = (i_1 + i_2) \in I.$$

Thus, $a + c \equiv b + d \pmod{I}$.

2) Observe we have

$$ac - bd = ac - bc + bc - bd$$

$$= (a-b)c + b(c-d)$$

$$= i_1 c + b i_2 .$$

Since $i_1, i_2 \in I$ and I is an ideal we have $i_1 c,\ b i_2 \in I$.

Thus $ac - bd = i_1 c + b i_2 \in I$, i.e. $ac \equiv bd \pmod{I}$. ∎

<u>Exercise:</u> Let $a \in R$. Given $k \in \mathbb{Z}_{\geq 1}$, define

$$a^k = \underbrace{a \cdots a}_{k\text{-copies}}$$

and

$$ka = \underbrace{a + \cdots + a}_{k\text{-copies}}.$$

Prove that if $a \equiv b \pmod{I}$, then

$$ka \equiv kb \pmod{I}$$

and

$$a^k \equiv b^k \pmod{I}.$$

Recall that we defined congruence classes modulo n as $[a]_n = \{ b \in \mathbb{Z} : a \equiv b \pmod{n} \}$. This could be rewritten as $[a]_n = \{ a + nk : k \in \mathbb{Z} \}$. We can denote this by $a + n\mathbb{Z}$.

In this context, we would write

$$[a]_n + [b]_n = (a+n\mathbb{Z}) + (b+n\mathbb{Z}).$$

Since we defined $[a]_n + [b]_n = [a+b]_n$, we have $(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$.

And similarly, $(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}$. Note there is nothing new here; it is just new notation for what we have already done!

We now define this for general rings and ideals. Given $I \subseteq R$ an ideal and $a \in R$, we set

$$\begin{aligned} a+I &= \{ b \in R : a \equiv b \pmod{I} \} \\ &= \{ b \in R : a-b \in I \} \\ &= \{ b \in R : b = a+i \text{ for some } i \in I \} \\ &= \{ a+i : i \in I \}. \end{aligned}$$

Theorem 5.1.6: Let I be an ideal in R, and $a, b \in R$. Then

$a \equiv b \pmod{I}$ iff $a+I = b+I$.

Proof: Suppose $a \equiv b \pmod{I}$. Then there exists $i \in I$ so that $a = b+i$. Thus, given any $j \in I$ we have $a+j = b+i+j \in b+I$.

Thus, $a+I \subseteq b+I$. Similarly, $b+I \subseteq a+I$ and so $a+I = b+I$.

Now suppose $a+I = b+I$. Since $0_R \in I$, $a+0_R = a$ is in $a+I = b+I$. Thus, $a = b+i$ for some $i \in I$, i.e., $a \equiv b \pmod{I}$. ∎

Theorem 5.1.7: Let $I \subseteq R$ be an ideal and $a, b \in R$. Then either

$$(a+I) \cap (b+I) = \emptyset \quad \text{or} \quad a+I = b+I.$$

Proof: If $(a+I) \cap (b+I) = \emptyset$ we are done so assume there exists $r \in (a+I) \cap (b+I)$. Thus, there exist $i_1, i_2 \in I$ so that $r = a + i_1 = b + i_2$. This gives $a - b = i_2 - i_1 \in I$, i.e., $a \equiv b \pmod{I}$. The previous theorem now gives $a+I = b+I$. ∎

As in the case of $\mathbb{Z}$, this shows the classes $a+I$ partition R, i.e., each element of R is contained in exactly one $a+I$. We call the congruence classes $a+I$ the **cosets of I**.

We set

$$R/I = \{a+I : a \in R\}$$

i.e., R/I is the collection of cosets. We can define addition and multiplication on these; which we will do in the next section.

Example: Let $I = \langle x \rangle \overset{c}{\subseteq} F[x]$, i.e., I is the collection of polynomials with no constant term. Consider the case of $F = \mathbb{Q}$ for simplicity first. $2 + I = \{2 + f : f \in I\}$

$= \{\text{polynomials with constant term } 2\}$

What about $x^2 + I$? Observe that $x^2 \in I$, so

$x^2 + I = 0_R + I$ because $x^2 - 0_R \in I$; thus $x^2 + I = 0_R + I = I$.

Example: Let $R = \mathbb{Z}$ and $I = 5\mathbb{Z}$. Then for $a \in R$ we have

$a + I = a + 5\mathbb{Z} = [a]_5$. Thus, in this case there

are only 5 cosets: $0 + I = 5\mathbb{Z}$, $1 + 5\mathbb{Z}$, $2 + 5\mathbb{Z}$,

$3 + 5\mathbb{Z}$, $4 + 5\mathbb{Z}$.

Example: Consider $F = \mathbb{Z}/3\mathbb{Z}$ and $R = F[x]$. Consider the

ideal $\langle x^2 \rangle = I$. Let $f, g \in R$; write

$$f = \sum_{j=0}^{n} a_j x^j$$

$$g = \sum_{j=0}^{m} b_j x^j.$$

Note that if $a_0 = b_0$ and $a_1 = b_1$, then

$$f - g = \sum_{j \geq 2}^{\max(m,n)} (a_j - b_j) x^j$$

where we set $a_j = 0$ for $j > n$ and $b_j = 0$ for $j > m$.

Thus, if $a_0 = b_0$ and $a_1 = b_1$ then $x^2 \mid (f - g)$,

which means $f - g \in I$, i.e., $f + I = g + I$.

This shows that the coset $f + I$ is completely determined by

the first two terms of f. Moreover, if $a_0 \neq b_0$ or $a_1 \neq b_1$, then $x^2 \nmid (f-g)$ so $f+I \neq g+I$. Thus, the cosets $f+I$ are in 1-1 correspondence with the set $\{a+bx : a, b \in \mathbb{Z}/3\mathbb{Z}\}$. (Note this set is NOT a ring!) by sending $(\sum_{j=0}^{n} a_j x^j) + I$ to $a_0 + a_1 x$. Since there are 3 choices for a_0 and 3 choices for a_1, there are 9 different cosets:

$$R/I = (\mathbb{Z}/3\mathbb{Z})[x]/\langle x^2 \rangle = \{ 0+0x, 0+1x, 0+2x,$$

$$1+0x, 1+x, 1+2x, 2+0x, 2+x, 2+2x \}.$$

Exercise: Write down all the elements of $(\mathbb{Z}/2\mathbb{Z})[x]/\langle x^2-1 \rangle$.

(think remainders here.).

§5.2 Quotient Rings and Homomorphisms:

Let R be a ring and $I \subseteq R$ an ideal. As was mentioned in the last section, we can put an addition and multiplication on R/I; namely, given $a+I, b+I \in R/I$ we define

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

The first thing we must do is check these are well-defined. Let

$a+I = c+I$ and $b+I = d+I$, i.e., there exists $i_1, i_2 \in I$ so that

$a-c = i_1$ and $b-d = i_2$. Then $(a+b)-(c+d) = (a-c)+(b-d) = i_1+i_2 \in I$.

Thus, $(a+b)+I = (c+d)+I$ (here we are using $a+b \in (a+b)+I \cap (c+d)+I$

so the intersection is nonempty, hence the cosets are equal.) Similarly,

we have $ab-cd = ab-cb+cb-cd$

$= (a-c)b + c(b-d)$

$= i_1 b + c i_2 \in I$

because I is an ideal. Thus, $ab \equiv cd \pmod{I}$, i.e.,

$ab+I = cd+I$. This gives multiplication and addition of cosets is

well-defined.

<u>Exercise</u>: Show that R/I is a ring. Note the proof that $\mathbb{Z}/n\mathbb{Z}$

is a ring works here if you change $[a]_n$ to $a+I$.

<u>Example</u>: Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$. Then R/I is exactly the

ring $\mathbb{Z}/n\mathbb{Z}$. Note this is the reason that $\mathbb{Z}/n\mathbb{Z}$ is the correct

notation for this ring and $\mathbb{Z}_n$ is rubbish.

Example: Consider the ring $R = (\mathbb{Z}/2\mathbb{Z})[x]$ and $I = \langle x^2 \rangle$

The elements of R/I are ~~$0, 1, x, x+1$~~ $0+I,\ 1+I,\ x+I,\ (x+1)+I$. Note the only possible coefficients are 0 and 1, and since $I = \langle x^2 \rangle$, any term that is divisible by x^2 is congruent to 0 modulo I, i.e., if $f \in R$ is given by $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, then $f \equiv a_0 + a_1 x \pmod{I}$. This is why the only elements of R/I are $0+I = I,\ 1+I,\ x+I,\ (x+1)+I$. We can write out addition and multiplication tables for R/I:

$+$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$1+I$	$1+I$	$0+I$	$(x+1)+I$	$x+I$
$x+I$	$x+I$	$(x+1)+I$	$0+I$	$1+I$
$(x+1)+I$	$(x+1)+I$	$x+I$	$1+I$	$0+I$

While the addition is straightforward, for multiplication we make use of the fact that $x^2 + I = 0 + I$:

$\cdot$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$x+I$	$0+I$	$x+I$	$0+I$	$x+I$
$(x+1)+I$	$0+I$	$(x+1)+I$	$x+I$	$1+I$

Some features here to point out: Note $x+I$ is a zero divisor.

Note that $((x+1)+I)((x+1)+I) = (x^2+2x+1)+I$

$= 1+I.$

Thus, $(x+1)+I$ is a unit and is its own inverse.

We call the ring R/I a quotient ring: it is easy to see (check as an exercise) that if R is commutative, so is R/I. If R has an identity, 1_R, then $1_R + I$ is the identity of R/I.

Example: Let $R = \mathbb{Z}[x]$ and consider the set

$$I = \{ f \in \mathbb{Z}[x] : f \text{ has even constant term} \}.$$

One can check (and should as an exercise) that I is a subring of $\mathbb{Z}[x]$. Moreover, it is an ideal because if $f \in I$, $g \in \mathbb{Z}[x]$ with writing $f = 2a_0 + a_1 x + \cdots + a_n x^n$ and $g = b_0 + b_1 x + \cdots + b_m x^m$ with $a_i, b_i \in \mathbb{Z}$, then

$$fg = \sum_{j=0}^{m+n} c_j x^j$$

where $c_j = \sum_{k=0}^{j} \tilde{a}_k b_{j-k}$ and so $c_0 = \sum 2a_i b_0$. ($\tilde{a}_0 = 2a_0$, $\tilde{a}_k = a_k$ for $k > 0$.)

Thus, we can consider R/I. Let $f \in R$. Then if the constant term of f is even, $f \in I$ so $f + I = 0 + I$. If f has an odd constant term, say $2k+1$, then if $f = (2k+1) + a_1 x + \cdots + a_n x^n$, we have

$f = 1 + (2k + a_1 x + \cdots + a_n x^n)$ and $2k + a_1 x + \cdots + a_n x^n \in I$,

so $f + I = 1 + I$. Thus, $R/I = \{0+I, 1+I\}$. The

addition and multiplication tables show this is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

(Write them out to see this; they are easy!)

Example: Let $R = \mathbb{R}[x]$ and $I = \langle x^2+1 \rangle$. Note that $(x^2+1) + I = 0 + I$,

i.e. $x^2 + I = -1 + I$ in R/I. Let $f \in \mathbb{R}[x]$. Then using

the division algorithm we have $f = (x^2+1)q + r$ with $r = 0$ or

$\deg r < 2$. Thus, $f + I = (ax+b) + I$ for $f = b + ax + x^2(\text{stuff})$.

Thus, the elements of $\mathbb{R}[x]/(x^2+1)$ are linear terms. Moreover,

given $(a_0 + a_1 x) + I$, $(b_0 + b_1 x) + I$, we have

$$\begin{aligned}((a_0 + a_1 x) + I)((b_0 + b_1 x) + I) &= a_0 b_0 + (a_0 b_1 + b_0 a_1) x + a_1 b_1 x^2 + I \\ &= (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0) x + I\end{aligned}$$

where we have used $x^2 + I = -1 + I$. We will return to this

example in a bit.

Let R be a ring and $I \subseteq R$ an ideal. We have a natural

map $\pi : R \to R/I$ defined by $\pi(r) = r + I$. We have already

encountered this map when $R = \mathbb{Z}$ and $I = n\mathbb{Z}$. ie

$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $m \longmapsto [m]_n$.

Theorem 5.2.1: Let $I \leq R$ be an ideal. The map $\pi : R \to R/I$ given by $r \longmapsto r + I$ is a ring homomorphism with kernel I. Moreover, the map is surjective.

Proof: Let $r_1, r_2 \in R$. Then

$$\pi(r_1 + r_2) = (r_1 + r_2) + I = (r_1 + I) + (r_2 + I)$$
$$= \pi(r_1) + \pi(r_2)$$

and

$$\pi(r_1 r_2) = r_1 r_2 + I = (r_1 + I)(r_2 + I)$$
$$= \pi(r_1)\pi(r_2).$$

Thus, π is a ring homomorphism.

Let $r + I \in R/I$. Then $\pi(r) = r + I$ so the map is surjective. It only remains to prove $\ker(\pi) = I$. Let $i \in I$.

Then $\pi(i) = i + I = 0 + I$. Thus, $i \in \ker \pi$ so $I \leq \ker \pi$. Now let $r \in \ker \pi$. Then $\pi(r) = 0 + I$, ie, $r + I = 0 + I$. This is equivalent to $r \in I$. Thus, $\ker \pi = I$. ∎

Observe this shows that given any ideal $I \leq R$, there is a ring

homomorphism π so that $I = \ker \pi$, namely, take $\pi : R \to R/I$. This is often referred to as the projection map.

The next theorem is extremely useful in studying the structure of rings.

Theorem 5.2.2: (First Isomorphism Thm): Let $\varphi : R \to S$ be a homomorphism of rings. Then $R/\ker\varphi \cong \text{Im}(\varphi)$.

Proof: Let $K = \ker\varphi$. We define a map $\Phi : R/K \to S$ by setting $\Phi(r+K) = \varphi(r)$. The most important part here is to show this map is well-defined. Suppose $r_1 + K = r_2 + K$. Then $r_1 - r_2 \in K = \ker\varphi$, so $\varphi(r_1 - r_2) = 0_S$, i.e. $\varphi(r_1) = \varphi(r_2)$. Thus, if $r_1 + K = r_2 + K$, then $\Phi(r_1+K) = \varphi(r_1) = \varphi(r_2) = \Phi(r_2+K)$ and so the map is well-defined.

Let $r_1 + K, r_2 + K \in R/K$. Then

$$\Phi((r_1+K) + (r_2+K)) = \Phi((r_1+r_2)+K)$$
$$= \varphi(r_1+r_2) = \varphi(r_1) + \varphi(r_2)$$
$$= \Phi(r_1+K) + \Phi(r_2+K)$$

and

$$\Phi((r_1+K)(r_2+K)) = \Phi(r_1 r_2 + K)$$
$$= \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$$
$$= \Phi(r_1+K)\,\Phi(r_2+K).$$

Thus, $\bar{\varphi}$ is a homomorphism.

Let $r+K \in \ker \bar{\varphi}$. Then $\bar{\varphi}(r+K) = 0_S$, i.e., $\varphi(r) = 0_S$. Thus, $r \in \ker \varphi = K$. But then $r+K = 0_R + K = 0_{R/K}$, so $\bar{\varphi}$ is injective.

Finally, let $s \in \operatorname{im}(\varphi)$. Then there exists $r \in R$ so that $\varphi(r) = s$. However, we then have $\bar{\varphi}(r+K) = \varphi(r) = s$ so $\bar{\varphi}$ surjects onto $\operatorname{im}(\varphi)$, i.e. $\operatorname{im}(\bar{\varphi}) = \operatorname{im}(\varphi)$.

Combining all of these we have $R/K \xrightarrow{\simeq} \operatorname{im}(\varphi)$. ∎

The easiest way to apply the previous theorem is when φ is surjective.

Example: Let $R = \mathbb{Z}[x]$ and $S = \mathbb{Z}/2\mathbb{Z}$ and define

$$\varphi : R \to S \quad \text{by} \quad \varphi(a_0 + a_1 x + \cdots + a_n x^n) = [a_0]_2.$$

This is clearly surjective, and is easily checked to be a homomorphism. The kernel is precisely the polynomials with even constant terms. Thus, we recover the isomorphism given before that

$$\mathbb{Z}[x]/(\text{polys with even constant term}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Example: Let $R = F[x]$ and $S = F$. Define $\varphi: R \to S$ by sending f to its constant term, i.e. by sending f to the polynomial function evaluated at 0. Thus, $\varphi(f) = f(0)$. It is easy to see this is a surjective homom and $\ker(\varphi) = \langle x \rangle$. Thus,

$$F[x]/\langle x \rangle \cong F.$$

Example: Let $R = \mathbb{R}[x]$ and $S = {}^*\mathbb{C}$. Define $\varphi: R \to S$ by sending f to $f(i)$. Note we have to explain this a bit. Since f is a polynomial in $\mathbb{R}[x]$, it induces a polynomial function $f: \mathbb{R} \to \mathbb{R}$. However, since $\mathbb{R} \subseteq \mathbb{C}$, we can view the polynomial f as an element of $\mathbb{C}[x]$. When we do this, f induces a polynomial function $f: \mathbb{C} \to \mathbb{C}$. When we write $f(i)$, it is the image of i under this polynomial map. For example, if $f = x^3 + x^2 + 1$, then

$$\varphi(f) = i^3 + i^2 + 1 = -i.$$

Let $a + bi \in \mathbb{C}$. Then $\varphi(a + bx) = a + bi$, so φ is surjective. Let $f, g \in \mathbb{R}[x]$. Then

$$\varphi(f+g) = (f+g)(i) = f(i) + g(i) = \varphi(f) + \varphi(g)$$

and

$$\varphi(fg) = (fg)(i) = f(i)\,g(i) = \varphi(f)\varphi(g).$$

Thus, φ is a surjective homomorphism. We claim $\ker \varphi = \langle x^2+1 \rangle$. It is clear that if $x^2+1 \mid f$, then since $f = (x^2+1)g$ for some $g \in \mathbb{R}[x]$ we have

$$\varphi(f) = (i^2+1)g(i) = 0,$$

so $\langle x^2+1 \rangle \subseteq \ker \varphi$. Let $f \in \ker \varphi$. Then $f(i) = 0$, so i is a root of f. Thus, $(x+i) \mid f$ when f is considered as an element of $\mathbb{C}[x]$. This gives $g \in \mathbb{C}[x]$ so that $f = (x+i)g$. We can apply complex conjugation to the coefficients of f and since f is defined over $\mathbb{R}$, this does not change f, i.e. if we let $f = a_0 + a_1 x + \cdots + a_n x^n$, then $\overline{f} = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n$

$$= a_0 + a_1 x + \cdots + a_n x^n = f.$$

This means that $f = \overline{(x+i)}\,\overline{g}$ as well, i.e., $f = (x-i)\overline{g}$, so $-i$ is also a root of f, i.e. $(x^2+1) \mid f$. Thus, $f \in \langle x^2+1 \rangle$.

Thus, $\ker \varphi = \langle x^2+1 \rangle$. Using the 1st isom theorem gives

$$\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}.$$

More generally, let $\varphi : R \to R$ be an isomorphism. (An isomorphism from a ring to itself is often called an automorphism.)

Define a map $\Phi : R[x] \to R[x]$ by $\Phi\left(\sum_{j=0}^{n} a_j x^j\right) = \sum_{j=0}^{n} \varphi(a_j) x^j$.

We claim this is an automorphism of $R[x]$. The fact it is a homomorphism follows from φ being a homom:

$$\Phi\left(\sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{m} b_j x^j\right) = \Phi\left(\sum_{j=0}^{\max(n,m)} (a_j + b_j) x^j\right)$$

$$= \sum_{j=0}^{\max(n,m)} \varphi(a_j + b_j) x^j = \sum_{j=0}^{n} \varphi(a_j) x^j + \sum_{j=0}^{m} \varphi(b_j) x^j$$

$$= \Phi\left(\sum_{j=0}^{n} a_j x^j\right) + \Phi\left(\sum_{j=0}^{m} b_j x^j\right).$$

And

$$\Phi\left(\sum_{j=0}^{n} a_j x^j \sum_{j=0}^{m} b_j x^j\right) = \Phi\left(\sum_{j=0}^{n+m} c_j x^j\right) \qquad (*)$$

Observe $\varphi(c_j) = \varphi\left(\sum_{k=0}^{j} a_k b_{j-k}\right) = \sum_{k=0}^{j} \varphi(a_k)\varphi(b_{j-k})$

because φ is a homom. Thus,

$$(*) = \sum_{j=0}^{n+m} \varphi(c_j) x^j = \left(\sum_{j=0}^{n} \varphi(a_j) x^j\right)\left(\sum_{j=0}^{m} \varphi(b_j) x^j\right)$$

$$= \Phi\left(\sum_{j=0}^{n} a_j x^j\right) \Phi\left(\sum_{j=0}^{m} b_j x^j\right).$$

To see injectivity, observe that if $\Phi\left(\sum_{j=0}^{n} a_j x^j\right) = 0$,

then $\varphi(a_j) = 0$ for all $j \in \{0, \ldots, n\}$. But φ is injective, so

this gives $a_j = 0$ for all $j \in \{0, \ldots, n\}$. Thus, $\sum_{j=0}^{n} a_j x^j = 0$.

Let $\sum_{j=0}^{n} b_j x^j \in R[x]$. Since φ is surjective, for each b_j there exists $a_j \in R$ so that $\varphi(a_j) = b_j$. Thus $\Phi\left(\sum_{j=0}^{n} a_j x^j\right) = \sum_{j=0}^{n} b_j x^j$, so Φ is surjective as well.

The last example used this for φ the complex conjugation map from $\mathbb{C}$ to $\mathbb{C}$.

Example

Example: Show that $\mathbb{Q}[x]/(x^2-3) \cong \mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3} : a, b \in \mathbb{Q}\}$.

It might help in the example exercise to note the following fact.

Let $f \in F[x]$ with root α. If $\varphi: F \to F$ is an isomorphism, then $\varphi(\alpha)$ is a root of $\Phi(f)$ as well. To see this, observe that if α is a root of f, then $f = (x-\alpha)g$ for some $g \in F[x]$.

Apply Φ: $\Phi(f) = \Phi((x-\alpha)g) = \Phi(x-\alpha)\,\Phi(g)$

$= (x - \varphi(\alpha))\,\Phi(g)$,

so $\varphi(\alpha)$ is a root of $\Phi(f)$. For our case, let $\varphi: \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3})$ be defined by $a+b\sqrt{3} \mapsto a-b\sqrt{3}$. It is easy to check this is an isomorphism (do it as an exercise.)

Just as in the last example, we define $\psi: \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{3})$ by sending $f \mapsto f(\sqrt{3})$ where we view f as in $\mathbb{Q}(\sqrt{3})[x]$ to

obtain the polynomial function $f: \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3})$. As above, it is easy to check this is a surjective homom and that $\langle x^2-3 \rangle \subseteq \ker \Psi$. Let $g \in \ker \Psi$. Then $g(\sqrt{3}) = 0$, so $g = (x-\sqrt{3})h$ for some $h \in \mathbb{Q}(\sqrt{3})[x]$. Since g is defined with coefficients in $\mathbb{Q}$, we have $\overline{\Phi}(g) = g$. Thus,

$$g = \overline{\Phi}(g) = \overline{\Phi}(x-\sqrt{3})\,\overline{\Phi}(h)$$
$$= (x+\sqrt{3})\,\overline{\Phi}(h),$$

so $-\sqrt{3}$ is a root of g as well. Thus, $x^2-3 \mid g$ and so $\ker \Psi \subseteq \langle x^2-3 \rangle$. Thus,

$$\mathbb{Q}[x]/\langle x^2-3 \rangle \cong \mathbb{Q}(\sqrt{3}).$$

5.3 Prime and maximal ideals:

Recall that when studying integers we showed an equivalent definition for $p \in \mathbb{Z}$ to be prime was to require if $p \mid ab$, then $p \mid a$ or $p \mid b$. We use this as motivation for defining when an ideal is prime. Consider the ideal $p\mathbb{Z}$. Suppose $ab \in p\mathbb{Z}$. This is equivalent to $p \mid ab$, so necessarily $p \mid a$ or $p \mid b$. However, this is equivalent to $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. We use this to define prime ideals.

Def: Let $I \subseteq R$ be an ideal. We say I is a *prime ideal* if whenever $rs \in I$, then $r \in I$ or $s \in I$.

Example: From above it is easy to see the prime ideals in $\mathbb{Z}$ are precisely those ideals $p\mathbb{Z}$ for p a prime number and $0\mathbb{Z}$. Observe $0\mathbb{Z} = \{0\}$ and if $ab \in 0\mathbb{Z}$, ie, if $ab = 0$, then $a = 0$ or $b = 0$. So we obtain one extra "prime" by considering ideals.

Example: Consider $R = F[x]$. Let f be an irreducible polynomial in $F[x]$ and consider $I = \langle f \rangle$. This is a prime ideal because we saw before if $f \mid gh$, then $f \mid g$ or $f \mid h$.

Example: Let R be an abstract integral domain. Then $\langle 0_R \rangle$ is prime because if $ab = 0_R$, then $a = 0_R$ or $b = 0_R$.

Theorem 5.3.1: Let R be a commutative ring with identity. An ideal $\wp \subseteq R$ is a prime ideal if and only if $R/\wp$ is an integral domain.

Proof: We know $R/\wp$ is automatically a commutative ring with identity,

so this really comes down to considering zero divisors.

"⇒" Suppose $\wp$ is a prime ideal and let $a+\wp, b+\wp \in R/\wp$ be nonzero elements so that $(a+\wp)(b+\wp) = 0+\wp$. Then $ab+\wp = 0+\wp$, i.e. $ab \in \wp$. This gives $a \in \wp$ or $b \in \wp$. This contradicts $a+\wp$ and $b+\wp$ being nonzero so no zero divisors exist.

"⇐" Suppose $R/\wp$ is an integral domain. Let $ab \in \wp$. Then $ab+\wp = 0+\wp$. Thus, $(a+\wp)(b+\wp) = 0+\wp$. Since $R/\wp$ is an integral domain, we have $a+\wp = 0+\wp$ or $b+\wp = 0+\wp$, i.e., $a \in \wp$ or $b \in \wp$. Thus, $\wp$ is prime. ∎

Example: Observe that in $\mathbb{Z}$ if we take a prime ideal $p\mathbb{Z}$, we have any other ideal containing $p\mathbb{Z}$ must be all of $\mathbb{Z}$. To see this, consider $I \supsetneq p\mathbb{Z}$. We say before all ideals in $\mathbb{Z}$ are principal, so $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Since $n\mathbb{Z} \supsetneq p\mathbb{Z}$, we have $p \in n\mathbb{Z}$, i.e., $n \mid p$. But since $n\mathbb{Z} \neq p\mathbb{Z}$, $n \neq p$. Thus, $n = 1$ and so $I = \mathbb{Z}$. Thus, there are no ideals between $p\mathbb{Z}$ and $\mathbb{Z}$ in terms of containment, i.e., if $p\mathbb{Z} \subsetneq I \subseteq \mathbb{Z}$, then $I = \mathbb{Z}$.

Example: Consider $R = \mathbb{Z}[x]$. We have $\langle x \rangle$ is a prime ideal because $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ via the 1st isom. theorem using the map $\Phi: \mathbb{Z}[x] \to \mathbb{Z}$ by $f \mapsto f(0)$. Since $\mathbb{Z}$ is an integral domain, $\mathbb{Z}[x]/\langle x \rangle$ is an integral domain so $\langle x \rangle$ is prime. This differs from the previous case because we saw before that $\langle x \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x]$. We claim $\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Define $\Psi: \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ by $f \mapsto f(0) \bmod 2 = [f(0)]_2$.

This is a surjective homom. because the map Ψ is a composition of surjective homomorphisms $\Psi = \Psi_1 \circ \Psi_2$ where $\Psi_2: \mathbb{Z}[x] \to \mathbb{Z}$ by $f \mapsto f(0)$ and $\Psi_1: \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by $[m] \mapsto [m]_2$. Since the composition of homoms is a homom and the composition of surjective maps is surjective, Ψ is a surjective homom. If $f \in \langle 2, x \rangle$, then $f = 2g + xh$ for some $g, h \in F[x]$. Then $\Psi(f) = \Psi(2g) + \Psi(xh) = [0]_2$, thus, $\langle 2, x \rangle \subseteq \ker \Psi$.

Let $f \in \ker \Psi$. Then $[f(0)]_2 = [0]_2$, so $2 \mid f(0)$. Write $f = a_0 + a_1 x + \cdots + a_n x^n$. Then we have $a_0 = 2b_0$ for some $b_0 \in \mathbb{Z}$ so $f = 2b_0 + x(a_1 + a_2 x + \cdots + a_n x^{n-1}) \in \langle 2, x \rangle$. Thus, $\ker \Psi = \langle 2, x \rangle$ and so $\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Proof: "$\Rightarrow$" Assume m is a maximal ideal. Since R is commutative, R/m is commutative as well. Moreover, since m is maximal we have $1_R \notin m$, so $0_R + m \neq 1_R + m$. Thus, $1_R + m$ is the identity in R/m. It remains to show any nonzero element in R/m has an inverse. Let $a + m \in R/m$ be a nonzero element, i.e., $a \notin m$. Consider the set

$$J = \{m + ra : r \in R, m \in m\}.$$

We claim this is an ideal. Note $0_R = 0_R + 0_R \cdot a \in J$.

Let $m_1 + r_1 a$, $m_2 + r_2 a \in J$. Then

$$(m_1 + r_1 a) - (m_2 + r_2 a) = (m_1 - m_2) + (r_1 - r_2)a \in J.$$

Let $r \in R$. Then $r(m_1 + r_1 a) = rm_1 + rr_1 a \in J$ because m is an ideal. Thus, J is an ideal. Moreover, we have $m \subseteq J$ because given $m \in m$, $m = m + 0_R a \in J$. We also have $a = 0_R + 1_R a \in J$. Since $a \notin m$, we have $m \subsetneq J$. Since m is maximal, we must have $J = R$.

Thus, there exists $r_1 \in R$, $m \in m$ so that $m + ra = 1_R$, i.e., $(a + m)(r + m) = 1_R + m$. Thus, $a + m$ is invertible. This gives R/m is a field.

"$\Leftarrow$" Now suppose R/m is a field. Let J be an ideal so that $m \subseteq J \subseteq R$. If $m = J$ we are done, so assume $m \subsetneq J$. So there exists $a \in J$ with $a \notin m$. Thus, $a + m \neq 0_R + m$. Since R/m is a field, there exists $b \in R$

The previous example leads to the following definition.

Def: Let $I \subsetneq R$ be an ideal. We say I is a maximal ideal if whenever there is an ideal J so that $I \subseteq J \subseteq R$, then $I = J$ or $R = J$. (In other words, there are no ideals between the maximal ideal and the entire ring.)

Example: Let $R = \mathbb{Z}$. The ideals $p\mathbb{Z}$ are maximal ideals for p prime as we saw above.

Example: Let $R = F[x]$ and $f \in R$ an irreducible polynomial. Consider the ideal $I = \langle f \rangle$. Suppose there is an ideal $I \subsetneq J \subseteq R$. If $J \neq I$, then exists $g \in J$ so that $f \nmid g$. ~~Thus, $g = fq + r$ with $q, r \in R$ and $r \neq 0_F$, $\deg r < \deg f$.~~ Note that since f is irred and $f \nmid g$, we must have $\gcd(g, f) = 1_F$. Thus there exist $a, b \in R$ so that $1_F = fa + gb$. However, since $f \in J$ and $g \in J$, we must have $fa + gb \in J$ because it is an ideal, i.e., $1_F \in J$. This implies $J = R$. Thus, $\langle f \rangle$ is maximal since the only ideal properly containing $\langle f \rangle$ is R.

Theorem 5.3.2: Let $M \subseteq R$ be an ideal with R a commutative ring with identity. Then M is maximal iff R/M is a field.

so that $(a+m)(b+m) = 1_R + m$, i.e., $ab+m = 1_R + m$. This gives $ab - 1_R = m$ for some $m \in \mathfrak{m}$, i.e., $1_R = ab - m$. However, since $a \in J$, $ab \in J$ and since $\mathfrak{m} \subsetneq J$, we have $m \in J$. Thus, $ab - m \in J$. This gives $1_R \in J$ and so $J = R$. Thus, $\mathfrak{m}$ is maximal. ∎

Example: We saw above that $\mathbb{Z}[x]/\langle 2, x\rangle \cong \mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field, we have $\mathbb{Z}[x]/\langle 2, x\rangle$ is a field and so $\langle 2, x\rangle$ is a maximal ideal.

Cor 5.3.3: Let R be a commutative ring with identity. Then every maximal ideal is a prime ideal.

Proof: Let $\mathfrak{m}$ be a maximal ideal. This gives $R/\mathfrak{m}$ is a field. Since every field is an integral domain we have $R/\mathfrak{m}$ is an integral domain. Thus, $\mathfrak{m}$ is a prime ideal. ∎