NOTES ON RINGS, MATH 369.101

Kernels of ring homomorphisms and Ideals

Recall the definition of a ring homomorphism.

Some new examples:

(1) Complex conjugation: $z = a + bi \mapsto \overline{z} = a - bi$ (where $i^2 = -1$). This gives a ring homomorphism $\mathbb{C} \to \mathbb{C}$, since we can check that $\overline{1} = 1$, $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$. To check the last one, let $z_1 = a + bi,\ z_2 = c + di$:

$$z_1 z_2 = (a + bi)(c + di) = ac - bd + (ad + bc)i$$

but

$$\overline{z_1}\ \overline{z_2} = (a - bi)(c - di) = ac - bd - (ad + bc)i = \overline{z_1 z_2}.$$

(2) Evaluation: For any ring R, choose $r \in R$. Then evaluation at $x = r$ gives a ring homomorphism $\phi_r : R[x] \to R$ defined by $\phi_r(f(x)) = f(r)$. In other words, if $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ is a polynomial in $R[x]$, then

$$\phi_r(f(x)) = f(r) = a_0 + a_1 r + \ldots + a_n r^n.$$

It is the case that $f(a)$ is in R, since the coefficients of f were in R, $a \in R$, and all the operations on polynomials are the addition and multiplication operations used in the ring.

Think about how evaluation at $x = r$ is defined on a sum $f(x) + g(x)$ and product $f(x)g(x)$ of polynomials, and why this means that ϕ_r preserves addition and multiplication. So ϕ_r is a homomorphism, even when R is not a commutative ring.

As an example of the evaluation homomorphism, think of when $R = \mathbb{Z}$ and we choose some integer $n \in \mathbb{Z}$. Then $\phi_n(1 + x + 2x^2) = 1 + n + 2n^2$. For which $f(x)$ does $\phi_n(f(x)) = 0$? Can you describe this set of $f(x)$ as "all multiples of some particular polynomial"?

P.S. As another nice example of the evaluation homomorphism, one could think of evaluation at a matrix of a polynomial in $R[x]$ where $R = M_n(\mathbb{R})$. The fact that this is a homomorphism provides the essential details for why the Cayley-Hamilton theorem (from linear algebra) is true.

Proposition 1. *Composition of two ring homomorphisms is a ring homomorphism.*

Date: Oct. 12 – Oct. 19.

Proof. Let $\phi : R \to S$ and $\psi : S \to T$ be two ring homomorphisms. We need to show that $\psi \circ \phi$ (defined by $\psi(\phi(r))$) is a ring homomorphism.

First, we check that 1 is sent to 1: $\psi(\phi(1)) = \psi(1) = 1$, the first equality because ϕ is a ring homomorphism, the second equality because ψ is a ring homomorphism.

Second, choose $r_1, r_2 \in R$. We check that the composition preserves addition: $\psi(\phi(r_1+r_2)) = \psi(\phi(r_1)+\phi(r_2)) = \psi(\phi(r_1))+\psi(\phi(r_2))$. Again, the first equality holds because ϕ is a ring homomorphism, the second equality because ψ is a ring homomorphism.

The reason that multiplication is preserved is similar:
$\psi(\phi(r_1 \cdot r_2)) = \psi(\phi(r_1) \cdot \phi(r_2)) = \psi(\phi(r_1)) \cdot \psi(\phi(r_2))$. □

So we can compose two homomorphisms and still have a homomorphism.

Exercise. Think about the rings $\mathbb{Z}_9$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ and a ring homomorphism $\mathbb{Z}_9 \to \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Since it is a ring homomorphism, we know to where $[1] \in \mathbb{Z}_9$ must be sent. But this tells us where $[2] = [1] + [1]$ must be sent (since it is a ring homomorphism), and [3], etc. How many ring homomorphisms $\mathbb{Z}_9 \to \mathbb{Z}_3 \oplus \mathbb{Z}_3$ exist? Are any of them onto (remember, there are nine elements in $Z_3 \oplus \mathbb{Z}_3$?

Exercise. Do the same as above, but with $\mathbb{Z}_6$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

Kernels. The **kernel** of a ring homomorphism $\phi : R \to S$ is the set

$$\{r \in R \mid \phi(r) = 0\} =^{defn} \ker \phi.$$

Examples:

for evaluation $\phi_n : \mathbb{Z}[x] \to \mathbb{Z}$:

$$\ker(\phi_n) = \{(x - n)g(x) \mid g(x) \in \mathbb{Z}[x]\}$$

for 'reduction mod n,' $\psi : \mathbb{Z} \to \mathbb{Z}_n$:

$$\ker \psi = \{nd \mid d \in \mathbb{Z}\}$$

for 'projection to a coordinate' $p_1 : R^2 \to R$:

$$\ker p_1 = \{(r_1, r_2) \mid r_1 = 0\}$$

Proposition 2. *A ring homomorphism* $\phi : R \to S$ *is 1-1* $\iff$ $\ker \phi = \{0\}$.

Proof. Suppose ϕ is 1-1 and let $x \in \ker \phi$ (x could be anything in $\ker \phi$). Then $\phi(0) = 0 = \phi(x)$. Since ϕ is 1-1 this forces $0 = x$. So anything that is in $\ker \phi$ must be 0, so $\ker \phi = \{0\}$.

Suppose that $\ker \phi = \{0\}$ and let $x, y \in R$ be such that $\phi(x) = \phi(y)$. We need to show that x must equal y. But $\phi(x) = \phi(y)$ implies $\phi(x - y) = \phi(x) - \phi(y) = 0$, so $x - y \in \ker \phi$, and so $x - y = 0$. □

Each of the kernels in examples above is a set of all multiples of some element. But not all ideals can be described as the set of multiples of one element:

Define $\zeta : \mathbb{Z}[x] \to \mathbb{Z}_2$ by composing ϕ_0 (evaluation at $x = 0$) with reduction mod 2. Then $\zeta(f(x)) = 0$ if and only if $f(x)$ has an even constant coefficient. This is true for $2 \in \mathbb{Z}[x]$ and for $x \in \mathbb{Z}[x]$.

But it cannot be that $\ker \zeta$ is the set of multiples (in $\mathbb{Z}[x]$) of some $f_0(x) \in \mathbb{Z}[x]$. Looking at 2, this f_0 would need to be constant. It cannot be ± 1, because then $\ker \zeta$ would be all of $\mathbb{Z}[x]$ since every polynomial is something times ± 1. So this would force $f_0(x)$ to be ± 2, but then x cannot be a multiple of it (using only polynomials in $\mathbb{Z}[x]$).

A nice proposition.

Proposition 3. *If $\mathbb{F}$ is a field and $\phi : \mathbb{F} \to R$ is a ring homomorphism (where $0 \neq 1$ in R), then ϕ must be 1-1.*

Proof. We know that $\phi(1) = 1_R$, the '1' in R. Choose $x \in \ker \phi$.

Now if $x \neq 0$ then x^{-1} exists in $\mathbb{F}$. But then

$$1 = \phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = 0 \cdot \phi(x^{-1}) = 0,$$

which is untrue. So it must be that $x = 0$. Thus $\ker \phi = \{0\}$ and so ϕ is 1-1 by Proposition 2. $\square$

Ideals. It will be convenient to introduce the notion of a 'ring without 1,' which is a set with addition and multiplication that would be a ring, except it does not have a multiplicative identity (a '1').

A simple example to think of is the set $n\mathbb{Z}$ of all integer multiples of some n. So for example, $2\mathbb{Z}$: this is closed under adding, multiplying, has zero in it, has additive inverses, etc.

Let R be a commutative ring. An **ideal** $I \subset R$ is a subset that is either a ring or a 'ring without 1' and has the *super-closed* under multiplication property:

$$\text{for any } r \in R, \text{ and any } x \in I, \ rx \in I.$$

So an ideal always has a commutative ring R in which it sits. And if you multiply anything in R by something in I, you get something in I.

Think again of $2\mathbb{Z}$. You can take any integer, multiply it by an even integer, and you get an even integer.

Note: If an ideal $I \subset R$ contains 1, then $I = R$: if $1 \in I$, then $\forall r \in R$, $r = r \cdot 1 \in I$. Also, any ideal contains 0. We call an ideal **proper** if I contains more than 0 and does not contain 1.

Proposition 4. $\ker \phi \subset R$ *is an ideal for any ring h'sm $\phi : R \to S$.*

Try checking this. You need to check $\ker \phi$ satisfies all the ring axioms (except existence of 1) and the super-closed condition. The reason it will work is that multiplying by 0 gives 0 (and adding 0 to 0 gives 0), so you remain in the set of things sent by ϕ to 0.

Alternatively, you could use this shorter way to check something is an ideal.

Proposition 5. *Let $I \subset R$ be any <u>subset</u>, which is not empty. If the following conditions are satisfied, then I is an ideal:*

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

So we have two ways to check if something is an ideal:

- identify the set is the kernel of some homomorphism;
- use Proposition 5.

Proposition 6. *Any ideal in $\mathbb{Z}$ and any ideal in $\mathbb{F}[x]$ is equal to the set of multiples of one element.*

Proof. For $\mathbb{Z}$ this statement is the content of Theorem 1.1.4. For $\mathbb{F}[x]$ this is implied by Theorem 4.2.2.

For a little more detail: Start with all multiples of some given polynomial in the ideal. If this doesn't give the whole ideal, some poly. in the ideal is not a multiple of that one. These two have a gcd, and every combination of them is a multiple of that gcd (by Theorem 4.2.2). Eventually you stop getting a new gcd; for each new choice of polynomial either the degree of the gcd drops and you use induction, or the new polynomial has same gcd and has already been accounted for. $\square$

Factor rings. *A very generalized form of congruence classes.*

Fix an ideal $I \subset R$, where R a commutative ring.

For $r \in R$, write $r + I$ to mean the set

$$r + I = \{r + x \mid x \in I\}.$$

This set $r + I$ is called a **coset**.

You can choose different r's and get the same coset. For example, take the ideal $3\mathbb{Z} \subset \mathbb{Z}$. So here $I = 3\mathbb{Z}$. Since this is multiples of 3, $2 + I$ is the set of all integers which are 2 plus a multiple of 3. But $5 + I$ is the same set, since $5 = 2 + 3$ so 5 plus a multiple of 3 is just 2 plus a different multiple of 3. So as cosets, $5 + 3\mathbb{Z} = 2 + 3\mathbb{Z}$.

(This is exactly the same as saying $[2] = [5]$ in $\mathbb{Z}_3$.)

But in the completely general setting:

Proposition 7. *For an ideal $I \subset R$ and $a, b \in R$,*
$a + I = b + I \iff a - b \in I$.

Proof. If $a - b \in I$ then for any $x \in I$, we have

$$a + x = b + a - b + x = b + (a - b + x),$$

and $a - b + x \in I$. This shows any element in $a + I$ is in $b + I$, so $a + I \subset b + I$.

Since $a - b \in I$ implies $b - a = -(a - b) \in I$, there is a symmetry, and so we also have $b + I \subset a + I$, and so they are equal cosets.

If $a + I = b + I$, then for any $x \in I$ we have that $a + x = b + x'$ for some $x' \in I$. That equality on elements in the cosets means that $a - b = x' - x$ which is in I, so $a - b \in I$. □

Constructing the factor ring R/I. We make the set of cosets of $I \subset R$ into a ring by declaring the following operations.

$$\text{Addition:} \qquad (r + I) + (s + I) = (r + s) + I$$

$$\text{Multiplication:} \qquad (r + I) \cdot (s + I) = rs + I$$

We need to know this is well-defined, in other words the answer we get when adding or multiplying should not depend on the 'r' representing the coset.

Say that $a + I = r + I$ and $b + I = s + I$. (Note, by Prop'n 7, this means $a - r \in I$ and $b - s \in I$.)

Then $a + I + b + I = (a + b) + I$ and $r + I + s + I = (r + s) + I$. Are the answers the same? Well,

$$(a + b) - (r + s) = (a - r) + (b - s) \in I$$

since each of $a - r$ and $b - s$ are in I. So $(a + b) + I = (r + s) + I$.

For multiplication: is $ab + I = rs + I$?

$$ab - rs = ab - rb + rb - rs = (a - r)b + r(b - s).$$

Each of these summands is an element of I because of the super-closed condition! So this shows $ab - rs \in I$ and so $ab + I = rs + I$.

The additive identity is $0 + I$ and the multiplicative identity is $1 + I$. Additive inverse of $r + I$ is $-r + I$.

Some examples of the factor ring R/I.

(1) $R = \mathbb{Z}$ and $I = n\mathbb{Z}$: $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.
(2) All multiples of one element is an ideal:

$$\langle p(x) \rangle = \{p(x)g(x) \mid g(x) \in \mathbb{F}[x]\}$$

Then $\mathbb{F}[x]/\langle p(x) \rangle$ is a factor ring.

Theorem 1 (Fundamental Theorem for Homomorphisms)**.** *Let $\phi : R \to S$ be a ring h'sm, where R is a commutative ring. Use $\phi(R)$ to denote the image of ϕ (everything that is $\phi(r)$ for some r). Then $\phi(R) \cong R/\ker\phi$.*

Proof. One should note that $\phi(R)$ is itself a ring. Check this.

Let $I = \ker\phi$ which is an ideal by Prop'n 4. Define $\psi : R/\ker\phi \to \phi(R)$ by setting $\psi(r + I) = \phi(r)$.

Check that ψ is a well-defined homomorphism.

Also, it is clear that ψ is onto. Lastly, consider the $\ker\psi$:

$$\begin{aligned}\ker\psi &= \{r+I \mid \phi(r)=0\}\\ &= \{r+I \mid r\in\ker\phi\}\\ &= \{r+I \mid r\in I\} = \{I\}.\end{aligned}$$

Since I is the zero of R/I, this means that ψ is 1-1 by Prop'n 2. $\square$

Using the Fundamental Theorem: Let $p_1 : \mathbb{Z}\oplus\mathbb{Z}_n \to \mathbb{Z}$ be projection to first coordinate. Since for any $r\in\mathbb{Z}$, we know that $p_1((r,0)) = r$, we have that $p_1(\mathbb{Z}\oplus\mathbb{Z}_n) = \mathbb{Z}$ (that is, p_1 is onto).

The kernel is $\ker p_1 = \{(0,s) \mid s\in\mathbb{Z}_n\}$. If we call $\ker p_1 = K$ then the Fundamental Theorem says that

$$\mathbb{Z} \cong (\mathbb{Z}\oplus\mathbb{Z}_n)/K.$$

In other words, the cosets, under the addition,multiplication we've given, make a ring structure just like that of $\mathbb{Z}$.

To see that this is natural, notice that $(r_1,s_1)+K = (r_2,s_2)+K$ if and only if $r_1 = r_2$.

So an equation of the form $(r_0,s_0)+K+(r_1,s_1)+K = (r_2,s_2)+K$ occurs if and only if $r_0+r_1-r_2 = 0$, that is $r_0+r_1 = r_2$.

Hence, since the first coordinate is $\mathbb{Z}$ every coset $(r,s)+K$ is equal to either $(1,s)+K$ added to itself r times or (if $r<0$) $(-1,s)+K$ added to itself $|r|$ times.

That is exactly how $\mathbb{Z}$ is structured (multiplication in $\mathbb{Z}$ is just a consequence of distribution, the fact that 1 is mult. identity, and that $r = 1+1+\ldots+1$ (r times)).

Note that $K = \{(0,s) \mid s\in\mathbb{Z}_n\}$ which can be treated very much like $\mathbb{Z}_n$: $(0,1)+(0,1)+\ldots+(0,1)$ (n times) is equal to $(0,0)$. In this sense, we can say that $(\mathbb{Z}\oplus\mathbb{Z}_n)/\mathbb{Z}_n \cong \mathbb{Z}$, which is pleasing.

Tie in to Theorem 4.3.6. Finally, say that α is a root of an irreducible $p(x)\in\mathbb{F}[x]$ and let $\phi_\alpha : \mathbb{F}[x]\to\mathbb{F}(\alpha)$ be the evaluation homomorphism, where $\mathbb{F}(\alpha)$ is the smallest field containing $\mathbb{F}$ and α.

It turns out that $\langle p(x)\rangle$ is equal to $\ker\phi_\alpha$ (takes some care to see). By the fundamental theorem, $\mathbb{F}[x]/\langle p(x)\rangle \cong \phi_\alpha(\mathbb{F}[x])$, which is a subfield of $\mathbb{F}(\alpha)$ (since we know the left side is a field!). Since $\mathbb{F}(\alpha)$ is the smallest field containing α and $\mathbb{F}$, it must be that ϕ_α is onto.