MA542 Lecture

Timothy Kohl

Boston University

February 19, 2025

So what we've just demonstrated is that the kernel of any homomorphism is an ideal, but, in fact, the converse is true in a 'canonical' way.

Proposition

If $I \subseteq R$ is an ideal then the function $\pi : R \to R/I$ given by $\pi(r) = r + I$ is a homomorphism, and $Ker(\pi) = I$.

Proof.

First, $\pi(r_1 + r_2) = (r_1 + r_2) + I = (r_1 + I) + (r_2 + I) = \pi(r_1) + \pi(r_2)$ and similarly $\pi(r_1 r_2) = \pi(r_1)\pi(r_2)$.

Next, $Ker(\pi) = \{x \in R \mid x + I = 0 + I\}$ but $x + I = 0 + I$ means $x \in I$ so $Ker(\pi) = I$. □

We used the term 'First' for the isomorphism theorem mentioned above, which suggests that there are others, and indeed there are.

But first we need to make some observations about ideals.

Proposition

If I, J are ideals of R then $I \cap J$ is an ideal, as is $I + J = \{i + j \mid i \in I; j \in J\}$

Proof.

That $I \cap J$ is an ideal is not difficult and is left as an exercise. The set $I + J$ is a subring since $(i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J$ and if we multiply we get $(i_1 + j_1)(i_2 + j_2) = i_1 i_2 + i_1 j_2 + i_2 j_1 + j_1 j_2$ where now, by virtue of I, J *both* being ideals of R means that $i_1 i_2 \in I$, $i_1 j_2 \in I$ and $i_2 j_1 \in J$ and $j_1 j_2 \in J$ so this sum is in $I + J$ so the product is too. That $I + J$ is an ideal is straightforward. □

Theorem (Second Isomorphism Theorem for Rings)

Let I and J be ideals of R, then $(I + J)/J \cong I/(I \cap J)$.

PROOF:
First, let's observe the obvious fact that $J \subseteq I + J$ and the less obvious fact that J is an ideal of $I + J$. (It's clearly a subring, and if $(x + y) \in I + J$ then for $j \in J$ we have $(x + y)j = xj + yj$ which is in J because J is an ideal of R, and R contains $I + J$ of course.

This is a bit unintuitive, but we can verify it by looking at the function $\theta : I \to (I + J)/J$ given by $\theta(i) = i + J$.

This is readily seen to be a homomorphism. The subtle fact to show is that θ is onto.

If we look at $(I + J)/J$, a typical element is of the form $i + j + J$ where $i \in I$ and $j \in J$.

But $j \in J$ so $j + J = J$ which means $i + j + J = i + J$, so θ is indeed onto.

PROOF continued:
To finish, let's determine $Ker(\theta)$.

Note $i + J = J$ if and only if $i \in J$, but since $i + J \in I + J$ then this means $i \in I$ of course, so $i \in I \cap J$, so $Ker(\theta) = I \cap J$ and thus, by the first isomorphism theorem:

$$I/I \cap J \cong (I + J)/J$$

since θ is onto and $Ker(\theta) = I \cap J$. $\square$

We round out this discussion with one more 'major' theorem involving ring isomorphisms which we state, but will leave the proof as an exercise.

Theorem (Third Isomorphism Theorem for Rings)

If R is a ring and I, J are ideals with $I \subseteq J$ then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

We now return to quotient calculations, in particular one which points to a definition for certain classes of ideals in a ring.

Prime vs. Maximal Ideals

Let $R = \mathbb{Q}[x]$ and $I = \langle x^2 - 2 \rangle$, what is R/I?

First, we need to enumerate the distinct cosets, and we have that

$$f(x) + I = g(x) + I$$

if and only if $f(x) - g(x)$ is a multiple of $x^2 - 2$ since $I = \langle x^2 - 2 \rangle$.

This doesn't seem like a terribly useful fact at the moment.

What *is* more useful is that $x^2 - 2 + I = 0 + I$ which means $x^2 + I = 2 + I$.

So we have $x^2 + I = 2 + I$ which (if we multiply both sides by $x + I$) implies

$$x^3 + I = 2x + I$$

and similarly $x^4 + I = 2x^2 + I$, and since $x^2 + I = 2 + I$ then $2x^2 + I = 4 + I$, and so $x^4 + I = 4 + I$, which implies that $x^5 + I = 4x + I$ etc.

So the general pattern we observe is that

$$x^{2n} + I = 2^n + I$$
$$x^{2n+1} + I = 2^n x + I$$

so, for example, $ax^2 + bx + c + I = (2a + c) + bx + I$ and $ax^3 + bx^2 + cx + d + I = (2b + d) + (2a + c)x + I$.
(You may wonder why we write it in the form $c + dx$ instead of $dx + c$, we'll see why later.)

And so for *every* $f(x) \in \mathbb{Q}[x]$ we have $f(x) + I = (a + bx) + I$ for some $a, b \in \mathbb{Q}$.

Moreover, if $(a_1 + b_1 x) + I = (a_2 + b_2 x) + I$ then $(a_1 - a_2) + (b_1 - b_2)x \in I$ which means

$$x^2 - 2 \mid (a_1 - a_2) + (b_1 - b_2)x$$

which, (unless $a_1 - a_2 = 0$ and $b_1 - b_2 = 0$) is impossible because $deg(x^2 - 2) = 2$.

Thus the distinct cosets in $\mathbb{Q}[x]/I$ are

$$\{(a + bx) + I \mid a, b \in \mathbb{Q}\}$$

where

$$[(a + bx) + I] + [(c + dx) + I] = (a + c) + (b + d)x + I$$

and $x^2 = 2$ implies that

$$[(a + bx) + I][(c + dx) + I] = (ac + 2bd) + (ad + bc)x + I$$

If you look at the rule $(x + I)(x + I) = x^2 + I = 2 + I$ it's almost as if $x + I$ plays the role of $\sqrt{2}$.

This is not an accident, and indeed, what we have is that

$$\mathbb{Q}[x]/\langle x^2 - 2\rangle \cong \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b, \in \mathbb{Q}\}$$

under the mapping $(a + bx) + I \mapsto a + b\sqrt{2}$.

And we have already observed that $\mathbb{Q}(\sqrt{2})$ is a field, and so we have another example of a quotient ring which is field, but in this case, an infinite field.

What we also see about this example is the relationship between the ideal $\langle x^2 - 2 \rangle$ and the field $\mathbb{Q}(\sqrt{2})$ which the quotient ring $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ is isomorphic to.

If you look at the equation $x^2 - 2 = 0$ then this has no solutions in $\mathbb{Q}$ since $\sqrt{2} \notin \mathbb{Q}$ but $\sqrt{2}$ is in $\mathbb{Q}(\sqrt{2})$.

So it's almost as if we can 'make' a field which contains the root of an equation where that root is not already in $\mathbb{Q}$.

As an example to contemplate, what is the structure of $\mathbb{Q}[x]/\langle x^2 + 1 \rangle$?

We just saw that $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is isomorphic to the field $\mathbb{Q}(\sqrt{2})$.

In contrast, if we construct the quotient ring $\mathbb{Z}[x]/\langle x^2 - 2\rangle$ we have that this is isomorphic to the integral domain $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

And we note that $\mathbb{Z}[\sqrt{2}]$ is *not* a field, since, for example

$$\frac{1}{2+\sqrt{2}} = \frac{1}{2} - \frac{1}{2}\sqrt{2} \notin \mathbb{Z}[\sqrt{2}]$$

but it is a domain. (Exercise!).

So the question is, why is one of these a field, but the other just a domain?

Definition

A prime ideal I of a commutative ring R is a proper ideal such that

$$ab \in I \text{ implies that either } a \in I \text{ or } b \in I$$

A maximal ideal I of a commutative ring R is a proper ideal such that if there is another ideal J such that $I \subseteq J \subseteq R$ then either $I = J$ or $J = R$.

So how do we determine if a given ideal is prime or maximal?

For example, in $R = \mathbb{Z}$ the ideal $I = n\mathbb{Z}$ is prime if and only if n is a prime number.

Why? Well if $ab \in n\mathbb{Z}$ then $n \mid ab$ but this need not imply that $n \mid a$ or $n \mid b$, for example $8 \cdot 3 \in 12\mathbb{Z}$ but $12 \nmid 8$ and $12 \nmid 3$.

However, for $n = p$ a prime, $p \mid ab$ implies that either $p \mid a$ and/or $p \mid b$.

Note: All ideals of $\mathbb{Z}$ are of the form $I = n\mathbb{Z}$ for some n.

Why? Well if I is an ideal, then let n be the smallest non-zero positive number in I. (This exists due to the well ordering principle.)

If $x \in I$ then by the division algorithm $x = qn + r$ for some $r \in \{0, 1, \ldots, n-1\}$.

If $r = 0$ then $x = qn$ and is a multiple of n.

If $r \neq 0$ then, since $x \in I$ (by assumption) and $qn \in I$ (since I is an ideal) then $x - qn \in I$, but $x - qn = r$ where $r < n$ which contradicts the choice of n as being the smallest positive number in I.

So every element $x \in I$ is of the form $x = qn$ so $I = \langle n \rangle$. □