MA542 Lecture

Timothy Kohl

Boston University

February 12, 2025

Ideals and Factor Rings

Observe that in $\mathbb{Z}$, n·(any even integer) = (some other even integer).

This is an example of the following fundamental concept.

Definition

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

Another way to think of this is, given a subring I and $r \in R$

$$rI = \{ra \,|a \in I\} \subseteq I$$
$$Ir = \{ar \,|a \in I\} \subseteq I$$

if I is an ideal.

Theorem

A non-empty subset $I \subseteq R$ is an ideal of R if
(a) $a - b \in I$ for all $a, b \in I$
(b) $ra \in I$ and $ar \in I$ for all $a \in I$ and $r \in R$.

Examples: For any ring R, $I = \{0\}$ and $I = R$ are always ideals.

For $R = \mathbb{Z}$,

$$\begin{aligned} I = n\mathbb{Z} &= \{nk \mid k \in \mathbb{Z}\} \\ &= \{0, \pm n, \pm 2n, \dots\} \end{aligned}$$

for a given $n \geq 0$.

This is one example of a broad class of ideals.

Definition

For any commutative ring R, for any $a \in R$ the set

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

is an ideal called the principal ideal generated by a.

There is actually a bit of proof needed to verify these are ideals.

If $ra, sa \in \langle a \rangle$ then clearly $ra - sa = (r - s)a \in \langle a \rangle$.

And if $ra \in \langle a \rangle$ and $s \in R$ then clearly $s(ra) = (sr)a \in \langle a \rangle$ but also, $(ra)s = s(ra) = (sr)a \in \langle a \rangle$ since, by commutativity, $(ra)s = s(ra)$.

This example shows up in ring theory and geometry.

$R = \mathbb{R}[x]$ (polynomials with real coefficients)

$$\begin{aligned} I &= \text{polynomials } f(x) \text{ with constant term } 0 \\ &= \langle x \rangle \end{aligned}$$

Why? Well if $f(x) = a_n x^n + \ldots a_1 x + a_0$ has zero constant term (i.e. $a_0 = 0$) so in fact

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x \\ &= x(a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_1) \end{aligned}$$

and clearly any polynomial $f(x) = xg(x)$ has the property that $f(0) = 0g(0) = 0$ meaning it has zero as its constant term.

Beyond simply the principal ideals which have one generator, i.e. $\langle a \rangle$, we can consider ideals with multiple generators.

The idea behind this is that if $a, b \in R$ for R a ring, then obviously $a + b \in R$ and $ab \in R$ and all powers of a and b lie in R, all because of closure, and indeed all polynomial combinations of a and b lie in R.

That is, what do we get when we consider the different ways of combining together one or more elemens of R?

Definition

If R is a commutative ring and $a_1, \ldots, a_n \in R$ then

$$I = \langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R\}$$

namely all 'R-linear combinations' of $\{a_1, \ldots, a_n\}$ is an ideal.

and this too requires a (fairly easy) verification.

Example: Let $R = \mathbb{R}[x, y] = \{\textit{polynomials in} x, y \textit{ with real coefficients}\}$ (which is a ring as you can check!).

For example R contains expressions like $x^2 + y^2 - 1$, $x + 2xy + y$, x^2y^3 etc.

Let $I = \langle x, y \rangle$ which is the set of all polynomials of the form

$$xf(x, y) + yg(x, y)$$

for polynomials $f(x, y), g(x, y)$ in R.

Observe that we can characterize I as the set of those polynomials $F(x, y) \in R$ such that $F(0, 0) = 0$.

What's nice about this example (and even the $\langle x \rangle$ one) is that one encompasses the set of polynomials with prescribed roots into a collection, and this collection has the structure of an ideal.

Broadly considered, this is (in some sense) the basis of what one thinks about in the subject known as algebraic geometry.

Ideals versus Subrings

Consider the following example:

$R = C^0(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continuous}\}$

$I = C^1(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ differentiable}\}$

I is a proper subring of R (i.e. differentiable implies continuous, but not the converse) but not an ideal.

For example, $f(x) = 2 \in I$ and $g(x) = |x| \in R$ but $f(x)g(x) = 2|x| \notin I$.

Factor/Quotient Rings

For a ring R with ideal $I \subseteq R$, consider for $r \in R$ the *coset*

$$r + I = \{r + a \mid a \in I\}$$

For example, in $R = \mathbb{Z}$ with

$$\begin{aligned} I &= 3\mathbb{Z} \\ &= \{3k \mid k \in \mathbb{Z}\} \\ &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \end{aligned}$$

we have that

$$\begin{aligned} 0 + I &= \{0 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\ 1 + I &= \{1 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\ 2 + I &= \{2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \end{aligned}$$

We observe the obvious fact (seen but not stated on the previous page)

$$0 + I = \{0 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = I$$

and also

$$3 + I = \{3 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} = I$$

where the equality $0 + I = 3 + I$ is something you've seen in the discussion of cosets from group theory.

Moreover note that (also familiar from group theory) one has

$$\begin{aligned} 4 + I &= \{4 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -9 + 4, -6 + 4, -3 + 4, 0 + 4, 3 + 4, \dots\} \\ &= \{\dots, -5, -2, 1, 4, 7, \dots\} \\ &= 1 + I \end{aligned}$$

Of course one can show some of these set equalities by means of an explicit bijection

$$I \ni 3k \mapsto 3 + 3(k-1) \in 3 + I$$

since $3k = 3 + 3(k-1)$, and similarly

$$1 + I \ni 1 + 3k \mapsto 4 + 3(k-1) \in 4 + I$$

since $1 + 3k = 4 + 3(k-1)$.

Although it's not so much a bijection as a way of representing an element in one coset as being representable as a member of the other coset which shows that they are in fact equal.

Of course, there is no need for any ad-hoc demonstration to see if two cosets are identical.

We have the following basic fact from group theory which still holds true here.

Proposition

If $I \subseteq R$ is an ideal, then $a + I = b + I$ if and only if $a - b \in I$.

We can apply this to an example we examined earlier.

Recall the example $R = \mathbb{R}[x]$ and $I = \langle x \rangle$.

In this case $f(x) + I = g(x) + I$ if and only if $f(x) - g(x) \in I$, namely that $f(x) - g(x)$ is divisible by x.

But this means that, if $h(x) = f(x) - g(x)$ then $h(x) = xq(x)$, but this, in turn, implies that $h(0) = 0q(0) = 0$.

The upshot of this is that $f(0) = g(0)$, where now $f(0)$ is the constant term of $f(x)$ and $g(0)$ is the constant term of $g(x)$.

The conclusion we draw then is that $f(x) + I = g(x) + I$ if and only if $f(x)$ and $g(x)$ have the same constant terms.

What's kind of further surprising is that this distinction between cosets has nothing to do with the other terms in the polynomial.

We shall revisit this example a bit later.