Lecture 7.2: Ideals, quotient rings, and finite fields

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Ideals

In the theory of groups, we can quotient out by a subgroup if and only if it is a normal subgroup. The analogue of this for rings are (two-sided) ideals.

Definition

A subring $I \subseteq R$ is a left ideal if

$$rx \in I \qquad \text{for all } r \in R \text{ and } x \in I.$$

Right ideals, and two-sided ideals are defined similarly.

If R is commutative, then all left (or right) ideals are two-sided.

We use the term ideal and two-sided ideal synonymously, and write $I \trianglelefteq R$.

Examples

- $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.
- If $R = M_2(\mathbb{R})$, then $I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : a, c \in \mathbb{R} \right\}$ is a left, but *not* a right ideal of R.
- The set $\text{Sym}_n(\mathbb{R})$ of symmetric $n \times n$ matrices is a subring of $M_n(\mathbb{R})$, but *not* an ideal.

Ideals

Remark

If an ideal I of R contains 1, then $I = R$.

Proof

Suppose $1 \in I$, and take an arbitrary $r \in R$.

Then $r1 \in I$, and so $r1 = r \in I$. Therefore, $I = R$. $\square$

It is not hard to modify the above result to show that if I contains *any* unit, then $I = R$. (HW)

Let's compare the concept of a normal subgroup to that of an ideal:

- normal subgroups are characterized by being invariant under conjugation:

$$H \leq G \text{ is normal iff } ghg^{-1} \in H \text{ for all } g \in G,\ h \in H.$$

- (left) ideals of rings are characterized by being invariant under (left) multiplication:

$$I \subseteq R \text{ is a (left) ideal iff } ri \in I \text{ for all } r \in R,\ i \in I.$$

Ideals generated by sets

Definition

The left ideal generated by a set $X \subset R$ is defined as:

$$(X) := \bigcap \{ I : \ I \text{ is a left ideal s.t. } X \subseteq I \subseteq R \} .$$

This is the smallest left ideal containing X.

There are analogous definitions by replacing "left" with "right" or "two-sided".

Recall the two ways to define the subgroup $\langle X \rangle$ generated by a subset $X \subseteq G$:

- "*Bottom up*": As the set of all finite products of elements in X;
- "*Top down*": As the intersection of all subgroups containing X.

Proposition (HW)

Let R be a ring *with unity*. The (left, right, two-sided) ideal generated by $X \subseteq R$ is:

- Left: $\{r_1 x_1 + \cdots + r_n x_n : n \in \mathbb{N},\ r_i \in R,\ x_i \in X\}$,
- Right: $\{x_1 r_1 + \cdots + x_n r_n : n \in \mathbb{N},\ r_i \in R,\ x_i \in X\}$,
- Two-sided: $\{r_1 x_1 s_1 + \cdots + r_n x_n s_n : n \in \mathbb{N},\ r_i, s_i \in R,\ x_i \in X\}$.

Ideals and quotients

Since an ideal I of R is an additive subgroup (and hence normal), then:

- $R/I = \{x + I \mid x \in R\}$ is the set of cosets of I in R;
- R/I is a quotient group; with the binary operation (addition) defined as

$$(x + I) + (y + I) := x + y + I.$$

It turns out that if I is also a two-sided ideal, then we can make R/I into a ring.

Proposition

If $I \subseteq R$ is a (two-sided) ideal, then R/I is a ring (called a quotient ring), where multiplication is defined by

$$(x + I)(y + I) := xy + I\,.$$

Proof

We need to show this is well-defined. Suppose $x + I = r + I$ and $y + I = s + I$. This means that $x - r \in I$ and $y - s \in I$.

It suffices to show that $xy + I = rs + I$, or equivalently, $xy - rs \in I$:

$$xy - rs = xy - ry + ry - rs = (x - r)y + r(y - s) \in I\,.$$

Finite fields

We've already seen that $\mathbb{Z}_p$ is a field if p is prime, and that finite integral domains are fields. But *what do these "other" finite fields look like?*

Let $R = \mathbb{Z}_2[x]$ be the polynomial ring over the field $\mathbb{Z}_2$. (Note: we can ignore all negative signs.)

The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$ because it does not have a root. (Note that $f(0) = f(1) = 1 \neq 0$.)

Consider the ideal $I = (x^2 + x + 1)$, the set of multiples of $x^2 + x + 1$.

In the quotient ring R/I, we have the relation $x^2 + x + 1 = 0$, or equivalently, $x^2 = -x - 1 = x + 1$.

The quotient has only 4 elements:

$$0 + I\,, \qquad 1 + I\,, \qquad x + I\,, \qquad (x+1) + I\,.$$

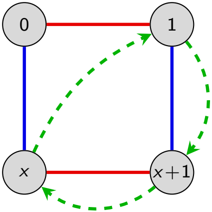
As with the quotient group (or ring) $\mathbb{Z}/n\mathbb{Z}$, we usually drop the "I", and just write

$$R/I = \mathbb{Z}_2[x]/(x^2 + x + 1) \cong \{0,\ 1,\ x,\ x+1\}\,.$$

It is easy to check that this is a field!

Finite fields

Here is a Cayley diagram, and the operation tables for $R/I = \mathbb{Z}_2[x]/(x^2+x+1)$:



$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Theorem

There exists a finite field $\mathbb{F}_q$ of order q, which is unique up to isomorphism, iff $q = p^n$ for some prime p. If $n > 1$, then this field is isomorphic to the quotient ring

$$\mathbb{Z}_p[x]/(f)\,,$$

where f is *any* irreducible polynomial of degree n.

Much of the error correcting techniques in coding theory are built using mathematics over $\mathbb{F}_{2^8} = \mathbb{F}_{256}$. This is what allows your CD to play despite scratches.