Visual Algebra

Lecture 8.1: Rings and their substructures

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

What is a ring?

A group is a set with a binary operation, satisfying a few basic properties.

Many algebraic structures (numbers, matrices, functions) have two binary operations.

Definition

A ring is an additive (abelian) group R with an additional associative binary operation (multiplication), satisfying the distributive law:

$$x(y+z) = xy + xz \qquad \text{and} \qquad (y+z)x = yx + zx \quad \forall x, y, z \in R\,.$$

Remarks

- There need not be multiplicative inverses.
- Multiplication need not be commutative (it may happen that $xy \neq yx$).

A few more definitions

If $xy = yx$ for all $x, y \in R$, then R is commutative.

If R has a multiplicative identity $1 = 1_R \neq 0$, we say that "R has identity" or "unity", or "R is a ring with 1."

The four rings of order 6

The additive group $\mathbb{Z}_6$ is a ring, where multiplication is defined modulo 6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

However, this is not the only way to add a ring structure to $(\mathbb{Z}_6, +)$.

×	0	a	$2a$	$3a$	$4a$	$5a$
0	0	0	0	0	0	0
a	0	0	0	0	0	0
$2a$	0	0	0	0	0	0
$3a$	0	0	0	0	0	0
$4a$	0	0	0	0	0	0
$5a$	0	0	0	0	0	0

×	0	a	$2a$	$3a$	$4a$	$5a$
0	0	0	0	0	0	0
a	0	$4a$	$2a$	0	$4a$	$2a$
$2a$	0	$2a$	$4a$	0	$2a$	$4a$
$3a$	0	0	0	0	0	0
$4a$	0	$4a$	$2a$	0	$4a$	$2a$
$5a$	0	$2a$	$4a$	0	$2a$	$4a$

×	0	a	$2a$	$3a$	$4a$	$5a$
0	0	0	0	0	0	0
a	0	$3a$	0	$3a$	0	$3a$
$2a$	0	0	0	0	0	0
$3a$	0	$3a$	0	$3a$	0	$3a$
$4a$	0	0	0	0	0	0
$5a$	0	$3a$	0	$3a$	0	$4a$

These last three rings do *not* have unity. We can view them as subrings:

$$\langle 6 \rangle \cong 6\mathbb{Z}_6 \subseteq \mathbb{Z}_{36}, \qquad \langle 2 \rangle \cong 2\mathbb{Z}_6 \subseteq \mathbb{Z}_{12}, \qquad \langle 3 \rangle \cong 3\mathbb{Z}_6 \subseteq \mathbb{Z}_{18}.$$

Subgroups, subrings, and ideals

If an (additive) **subgroup** of $S \subseteq R$ is closed under multiplication, it is a **subring**.

The analogue of normal subgroups 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

In the ring $R = \mathbb{Z}[x]$ of polynomials over $\mathbb{Z}$:

- the subgroup generated by 2 is $\langle 2 \rangle = 2\mathbb{Z}$.
- the ideal generated by 2 is

$$(2) := \{2f(x) \mid f \in \mathbb{Z}[x]\} = \{2a_nx^n + \cdots + 2a_1x + 2a_0 \mid f \in \mathbb{Z}[x]\}.$$

A familiar example

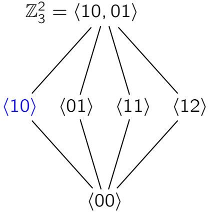
Consider the ring $R = \mathbb{Z}_3^2 = \{ab \mid a, b \in \mathbb{Z}_3\}$.

We know that the following map is a group homomorphism:

$$\phi \colon \mathbb{Z}_3^2 \to \mathbb{Z}_3, \qquad \phi(ab) = b.$$

The table below (right) shows it's also a ring homomorphism.

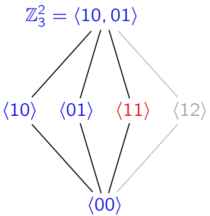
Do you see why $\langle 10 \rangle$ is an ideal?



+	00	10	20	01	11	21	02	12	22
00	00	10	20	01	11	21	02	12	22
10	10	-0	00	11	-1	01	12	-2	02
20	20	00	10	21	01	11	22	02	12
01	01	11	21	02	12	22	00	10	20
11	11	-1	01	12	-2	02	10	-0	00
21	21	01	11	22	02	12	20	00	10
02	02	12	22	00	10	20	01	11	21
12	12	-2	02	10	-0	00	11	-1	01
22	22	02	12	20	00	10	21	01	11

×	00	10	20	01	11	21	02	12	22
00	00	00	00	00	00	00	00	00	00
10	00	-0	20	00	-0	20	00	-0	20
20	00	20	10	00	20	10	00	20	10
01	00	00	00	01	01	01	02	02	02
11	00	-0	20	01	-1	21	02	-2	22
21	00	20	10	01	21	11	02	22	12
02	00	00	00	02	02	02	01	01	01
12	00	-0	20	02	-2	22	01	-1	21
22	00	20	10	02	22	12	01	21	11

Different types of substructures



Let's consider two other subgroups of $R = \mathbb{Z}_3^2$.

- The subgroup $\langle 11 \rangle$ is a subring but not an ideal.
- The subgroup $\langle 12 \rangle$ is a not even a subring.

×	00	11	22	12	21	10	20	01	02
00	00	00	00	00	00	00	00	00	00
11	00	11	22	12	21	10	20	01	02
22	00	22	11	21	12	20	10	02	01
12	00	12	21	11	22	10	20	01	02
21	00	21	12	22	11	20	10	02	01
10	00	10	20	10	20	10	20	00	00
20	00	20	10	20	10	20	10	00	00
01	00	01	02	02	01	00	00	01	02
02	00	02	01	01	02	00	00	02	01

×	00	12	21	10	22	01	11	20	02
00	00	00	00	00	00	00	00	00	00
12	00	11	22	10	21	02	12	20	01
21	00	22	11	20	12	01	21	10	02
10	00	10	20	10	20	00	10	20	00
22	00	21	12	20	11	02	22	10	01
01	00	02	01	00	02	01	01	00	02
11	00	12	21	10	22	01	11	20	02
20	00	20	10	20	10	00	20	10	00
02	00	01	02	00	01	02	02	00	01

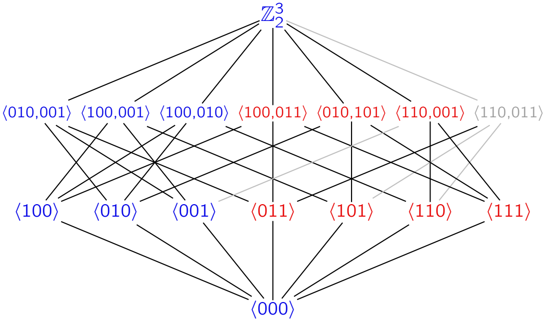
Subring lattices

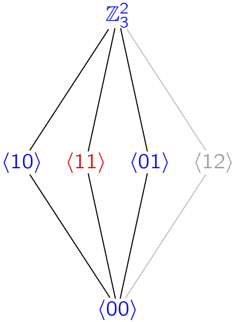
Like we did with groups, we can create the **subring lattice** of a (finite) ring.

Start with the **subgroup lattice**, and color-code the subgroups of R as follows:

1. Blue: an ideal,
2. Red: a subring that is not an ideal,
3. faded: a subgroup that is not subring.

Technically, we shouldn't have non-subrings, but it's nice to include them.





Ideals generated by sets

Definition

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

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

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 1. The (left, right, two-sided) ideal generated by $X \subseteq R$ is:

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

Ideals in rings without unity

Proposition

Let R be a commutative rng (=need not have unity). Then

$$\{r_1x_1 + \cdots + r_nx_n \mid n \in \mathbb{N},\ r_i \in R,\ x_i \in X\} \subseteq \bigcap_{X \subseteq I_\alpha \trianglelefteq R} I_\alpha .$$

Perhaps surprisingly, equality above need not hold!

Consider the following polynomial ring:

$$R = 2\mathbb{Z}[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in 2\mathbb{Z},\ n \in \mathbb{N}\}$$
$$= \{2c_0 + 2c_1x + \cdots + 2c_nx^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N}\}.$$

Since the ideal (2) contains 2 by definition,

$$\{2f(x) \mid f(x) \in 2\mathbb{Z}[x]\} = \{4c_0 + 4c_1x + \cdots + 4c_nx^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N}\} \subsetneq (2).$$

Similarly, the ideal $(2, 2x)$ contains 2 and $2x$, and so

$$\{2f(x) + 2xg(x) \mid f(x) \in 2\mathbb{Z}[x]\} = \{4c_0 + 4c_1x + \cdots + 4c_nx^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N}\} \subsetneq (2, 2x).$$

Ideals generated by sets

As we did with groups, if $S = \{x\}$, we can write (x) rather than $(\{x\})$, etc.

Let's see some examples of ideals in $R = \mathbb{Z}[x]$.

$$(x) = \big\{xf(x) \mid f \in \mathbb{Z}[x]\big\} = \big\{a_n x^n + \cdots + a_1 x \mid a_i \in \mathbb{Z}\big\}.$$

$$(2) = \big\{2f(x) \mid f \in \mathbb{Z}[x]\big\} = \big\{2a_n x^n + \cdots + 2a_1 x + 2a_0 \mid a_i \in \mathbb{Z}\big\}.$$

$$(x, 2) = \big\{xf(x) + 2g(x) \mid f, g \in \mathbb{Z}[x]\big\} = \big\{a_n x^n + \cdots + a_1 x + 2a_0 \mid a_i \in \mathbb{Z}\big\}.$$

Notice that we have

$$(x) \subsetneq (x, 2) \subsetneq R, \qquad \text{and} \qquad (2) \subsetneq (x, 2) \subsetneq R.$$

The ideal $(x, 2)$ is said to be maximal, because there is nothing "between" it and R.

Question

How different would these ideals be in the ring $R = \mathbb{Q}[x]$?