Visual Algebra

Lecture 8.2: Examples of rings

Dr. Matthew Macauley

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

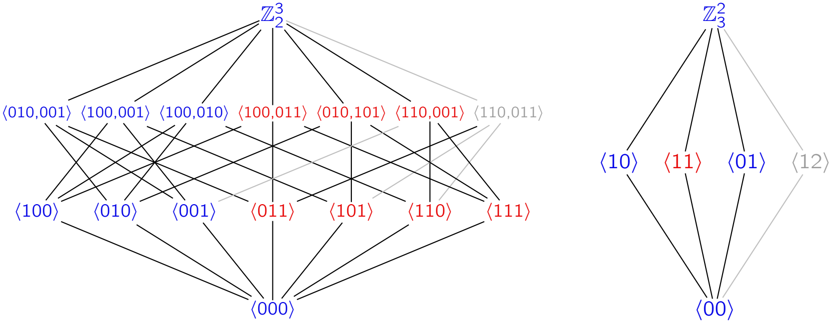
Subring lattices

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. gray: a subgroup that is not subring.

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

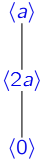


Some rings of order 4

There are 3 rings whose additive group is $\mathbb{Z}_4$.

Their multiplicative structures are shown below.

$+$	0	a	$2a$	$3a$
0	0	a	$2a$	$3a$
a	a	$2a$	$3a$	0
$2a$	$2a$	$3a$	0	a
$3a$	$3a$	0	a	$2a$



$$\{0,1,2,3\} = \mathbb{Z}_4$$
$$\langle a \mid 4a=0,\ a^2=a \rangle$$

$\times$	0	a	$2a$	$3a$
0	0	0	0	0
a	0	a	$2a$	$3a$
$2a$	0	$2a$	0	$2a$
$3a$	0	$3a$	$2a$	a

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} \right\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_4)$$

$$\{0,2,4,6\} = 2\mathbb{Z}_4 \subseteq \mathbb{Z}_8$$
$$\langle a \mid 4a=0,\ a^2=2a \rangle$$

$\times$	0	a	$2a$	$3a$
0	0	0	0	0
a	0	$2a$	0	$2a$
$2a$	0	0	0	0
$3a$	0	$2a$	0	$2a$

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix} \right\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_4)$$

$$\{0,4,8,12\} = 4\mathbb{Z}_4 \subseteq \mathbb{Z}_{16}$$
$$\langle a \mid 4a=0,\ a^2=0 \rangle$$

$\times$	0	a	$2a$	$3a$
0	0	0	0	0
a	0	0	0	0
$2a$	0	0	0	0
$3a$	0	0	0	0

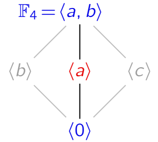
$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix} \right\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_4)$$

Some rings of order 4

There are 8 rings whose additive group is $\mathbb{Z}_2^2$.

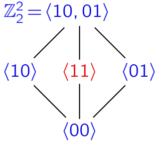
Three have unity: $\mathbb{F}_4$, $\mathbb{Z}_2^2$, and $\langle I, \mathbf{1} \rangle$.

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0



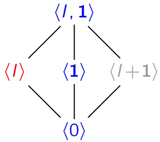
×	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	b	c	a
c	0	c	a	b

$$\mathbb{F}_4 \cong \Big\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}}_{c} \Big\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_2)$$



×	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	b	b	0
c	0	c	0	c

$$\mathbb{Z}_2^2 \cong \Big\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}}_{c} \Big\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_2)$$



×	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	b	0	b
c	0	c	b	a

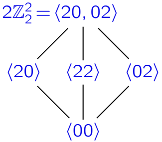
$$\langle I, \mathbf{1} \rangle \cong \Big\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{c} \Big\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_2)$$

Some rings of order 4

There are 8 rings whose additive group is $\mathbb{Z}_2^2$.

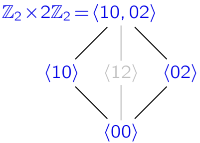
Three are commutative but without unity.

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0



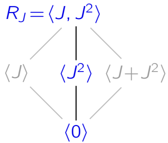
×	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	0	0	0
c	0	0	0	0

$$\left\langle \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \right\rangle \cong 2\mathbb{Z}_2^2 := \big\{(0,0),(2,0),(0,2),(2,2)\big\} \subseteq \mathbb{Z}_4^2$$



×	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	0	b	b
c	0	0	b	b

$$\mathbb{Z}_2 \times 2\mathbb{Z}_2 := \big\{(0,0),(0,2),(1,0),(1,2)\big\} \subseteq \mathbb{Z}_2 \times \mathbb{Z}_4$$



×	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	0	a	a
c	0	0	a	a

$$R_J = \Big\langle \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}}_{J} \Big\rangle \subseteq \mathrm{Mat}_3(\mathbb{Z}_2), \qquad \underbrace{\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{J^2}$$

Some rings of order 4

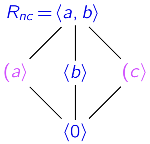
There are two noncommutative rings of order 4.

Each is the "opposite ring" of the other.

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

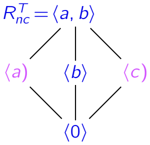
We'll write non 2-sided ideals in purple, and write

- $(x\rangle$ for a left ideal that is not a right ideal
- $\langle x)$ for a right ideal that is not a left ideal.



×	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	0	0	0
c	0	a	b	c

$$R_{nc} = \Big\{ \underbrace{\begin{bmatrix}0&0\\0&0\end{bmatrix}}_{0}, \underbrace{\begin{bmatrix}1&0\\0&0\end{bmatrix}}_{a}, \underbrace{\begin{bmatrix}0&1\\0&0\end{bmatrix}}_{b}, \underbrace{\begin{bmatrix}1&1\\0&0\end{bmatrix}}_{c} \Big\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_2)$$



×	0	a	b	c
0	0	0	0	0
a	0	a	0	a
b	0	b	0	b
c	0	c	0	c

$$R_{nc}^T = \Big\{ \underbrace{\begin{bmatrix}0&0\\0&0\end{bmatrix}}_{0}, \underbrace{\begin{bmatrix}1&0\\0&0\end{bmatrix}}_{a}, \underbrace{\begin{bmatrix}0&0\\1&0\end{bmatrix}}_{b}, \underbrace{\begin{bmatrix}1&0\\1&0\end{bmatrix}}_{c} \Big\} \subseteq \mathrm{Mat}_2(\mathbb{Z}_2)$$

Finite rings

In general, we'll be more interested in infinite rings.

However, let's say a few words about finite rings, mostly for fun.

n	1	2	3	4	5	6	7	8	9	10	11	12	16	32
# groups	1	1	1	2	1	2	1	5	2	2	1	5	14	51
# rings w/ 1	1	1	1	4	1	1	1	11	4	1	1	4	50	208
# rings	1	2	2	11	2	4	2	52	11	4	2	22	390	> 18590
# non-comm	0	0	0	2	0	0	0	18	2	0	0	18	228	?

Small noncommutative rings with 1 are "rare". There are

- 13 of size 16
- one each of sizes 8, 24, and 27
- and no others of order less than 32.

For distinct primes p and q, ($p \geq 3$), there are the following number of algebraic structures:

n	p	p^2	p^3	pq	p^2q
# groups	1	2	5	2	≤ 5
# rings	2	11	$3p + 50$	4	22

Going forward, most finite rings we'll typically encounter are $\mathbb{Z}_n$ and finite fields.

Some infinite rings

Examples

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are all commutative rings with 1.
2. For any ring R with 1, the set $M_n(R)$ of $n \times n$ matrices over R is a ring. It has identity $1_{M_n(R)} = I_n$ iff R has 1.
3. For any ring R, the set of functions $F = \{f \colon R \to R\}$ is a ring by defining
$$(f+g)(r) = f(r) + g(r), \qquad (fg)(r) = f(r)g(r)\,.$$
4. The set $S = 2\mathbb{Z}$ is a subring of $\mathbb{Z}$ but without unity.
5. $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}$ is a subring of $R = M_2(\mathbb{R})$. However, note that
$$1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \text{but} \qquad 1_S = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$
6. If R is a ring and x a variable, then the set
$$R[x] = \left\{ a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R \right\}$$
is called the polynomial ring over R.

More examples of ideals

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

- subgroups that are not subrings:

$$\langle x \rangle = \{nx \mid n \in \mathbb{Z}\}, \qquad \langle 1, x, x^2 \rangle = \{a_0 + a_1 x + a_2 x^2 \mid a_i \in \mathbb{Z}\}.$$

- subrings that are not ideals:

$$\langle 2 \rangle = 2\mathbb{Z}, \qquad \langle 1, x^2, x^4, \dots \rangle = \{a_0 + a_2 x^2 + \cdots + a_{2k} x^{2k} \mid a_i \in \mathbb{Z}\}.$$

- ideals:

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

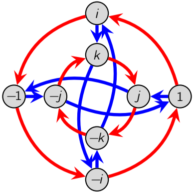
$$(x) = \{xf(x) \mid f \in \mathbb{Z}[x]\} = \{a_n x^n + \cdots + a_1 x \mid a_i \in \mathbb{Z}\},$$

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

In $R = M_2(\mathbb{R})$:

- $I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : a, c \in \mathbb{R} \right\}$ is a left, but not right ideal of R.
- The set $\mathrm{Sym}_2(\mathbb{R})$ of symmetric matrices is a subgroup, but not a subring.

Another example: the Hamiltonians



Recall the (unit) quaternion group:

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = -1,\ ij = k \rangle.$$

Allowing addition makes them into a ring $\mathbb{H}$, called the quaternions, or Hamiltonians:

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

The set $\mathbb{H}$ is isomorphic to a subring of $M_4(\mathbb{R})$, the real-valued 4×4 matrices:

$$\mathbb{H} \cong \left\{ \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\} \subseteq M_4(\mathbb{R}).$$

Formally, we have an embedding $\phi \colon \mathbb{H} \hookrightarrow M_4(\mathbb{R})$ where

$$\phi(i) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \phi(j) = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad \phi(k) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Just like with groups, we say that $\mathbb{H}$ is represented by a set of matrices.