Chapter 8: Rings

Matthew Macauley

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

Math 4130, Visual Algebra

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

$\times$	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 $(\mathbb{Z}_6, +)$.

$\times$	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

$\times$	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	$2a$	$4a$

$\times$	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

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

A familar example

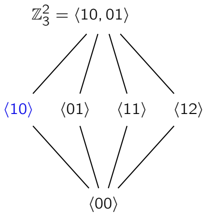
Consider the ring $R = \mathbb{Z}_3^2 = \{ab \mid a, b \in \mathbb{Z}_3\}$.

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.

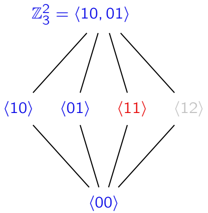
Do you see why $\langle 10 \rangle$ is an ideal?



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

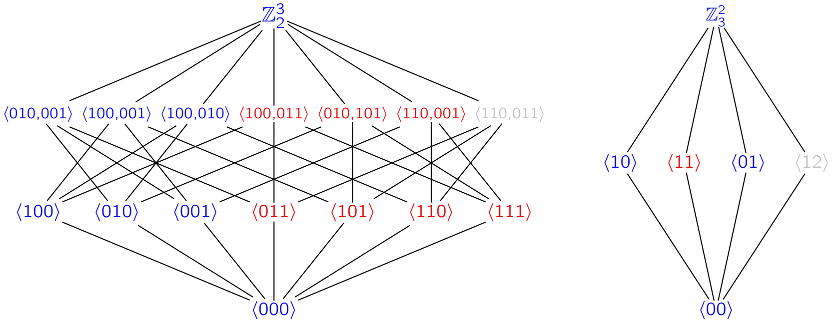
Subring lattices

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:

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

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

- Left: $\{r_1x_1 + \cdots + r_nx_n : n \in \mathbb{N}, \ r_i \in R, \ x_i \in X\}$,
- Right: $\{x_1r_1 + \cdots + x_nr_n : n \in \mathbb{N}, \ r_i \in R, \ x_i \in X\}$,
- Two-sided: $\{r_1x_1s_1 + \cdots + r_nx_ns_n : n \in \mathbb{N}, \ r_i, s_i \in R, \ x_i \in X\}$.

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:

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

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 $R = \mathbb{Z}[x]$.

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

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

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

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 $R = \mathbb{Q}[x]$?

Some rings of order 4

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

Their multiplictive 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	$2a$

$$\begin{tikzcd}[arrows=dash] \langle a \rangle \arrow[d] \\ \langle 2a \rangle \arrow[d] \\ \langle 0 \rangle \end{tikzcd}$$

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

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

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} \right\} \subseteq M_2(\mathbb{Z}_4)$$

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

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

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix} \right\} \subseteq M_2(\mathbb{Z}_4)$$

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

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

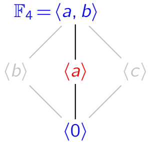
$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix} \right\} \subseteq M_2(\mathbb{Z}_4)$$

Some rings of order 4

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

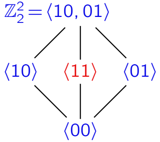
Three have unity: $\mathbb{F}_4$, $\mathbb{Z}_2^2$, and $\langle I, \mathbf{1}\rangle$.

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



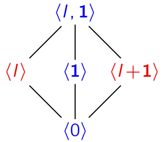
×	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	b	c	a
c	0	c	a	b

$$\mathbb{F}_4 \cong \left\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}}_{c} \right\} \subseteq M_2(\mathbb{Z}_2)$$



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

$$\mathbb{Z}_2^2 \cong \left\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}}_{c} \right\} \subseteq M_2(\mathbb{Z}_2)$$



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

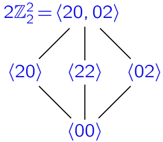
$$\langle I, \mathbf{1}\rangle \cong \left\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{c} \right\} \subseteq M_2(\mathbb{Z}_2)$$

Some rings of order 4

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

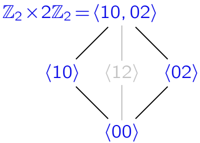
Three are commutative but without unity.

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



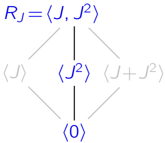
×	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	0	0	0
c	0	0	0	0

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



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

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



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

$$R_J = \Bigg\langle \underbrace{\begin{bmatrix}0&1&0\\0&0&1\\0&0&0\end{bmatrix}}_{J} \Bigg\rangle \subseteq M_3(\mathbb{Z}_2), \qquad \underbrace{\begin{bmatrix}0&0&1\\0&0&0\\0&0&0\end{bmatrix}}_{J^2}$$

Some rings of order 4

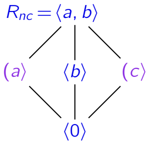
+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

There are two noncommutative rings of order 4.

Each is the "opposite ring" of the other.

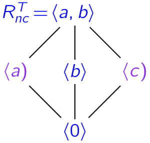
We'll write non 2-sided ideals in purple, and write

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



$\times$	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	0	0	0
c	0	a	b	c

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



$\times$	0	a	b	c
0	0	0	0	0
a	0	a	0	a
b	0	b	0	b
c	0	c	0	c

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

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
$$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R\}$$
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:

$$\langle x \rangle = \{nx \mid n \in \mathbb{Z}\}, \qquad \langle 1, x, x^2 \rangle = \{a_0 + a_1x + a_2x^2 \mid a_i \in \mathbb{Z}\}.$$

- subrings that are not ideals:

$$\langle 2 \rangle = 2\mathbb{Z}, \qquad \langle 1, x^2, x^4, \dots \rangle = \{a_0 + a_2x^2 + \cdots + a_{2k}x^{2k} \mid a_i \in \mathbb{Z}\}.$$

- ideals:

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

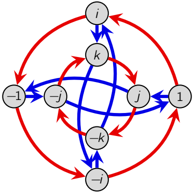
$$(x) = \{xf(x) \mid f \in \mathbb{Z}[x]\} = \{a_nx^n + \cdots + a_1x \mid a_i \in \mathbb{Z}\},$$

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

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.

Units

Informally, a ring is a set where we can add, substract, multiply, but not necessarily divide.

Definition

A unit is any $u \in R$ that has a multiplicative inverse: some $v \in R$ such that $uv = vu = 1$.

Let $U(R)$ be the set (a multiplicative group) of units of R.

Proposition

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

Proof

Consider a unit $u \in I$. Then for any $r \in R$: $r = (ru^{-1})u \in I$, hence $I = R$. $\square$

Examples

1. Let $R = \mathbb{Z}$. The units are $U(R) = \{-1, 1\}$.
2. Let $R = \mathbb{Z}_{10}$. Then 7 is a unit (and $7^{-1} = 3$) because $7 \cdot 3 = 1$. But 2 is not a unit.
3. Let $R = \mathbb{Z}_n$. A nonzero $k \in \mathbb{Z}_n$ is a unit if $\gcd(n, k) = 1$.
4. The units of $M_2(\mathbb{R})$ are the invertible matrices.

Zero divisors

Definition

An element $x \in R$ is a left zero divisor if $xy = 0$ for some $y \neq 0$. (Right zero divisors are defined analogously.)

Examples

1. There are no (nonzero) zero divisors of $R = \mathbb{Z}$.
2. The zero divisors of $R = \mathbb{Z}_{10}$ are $0, 2, 4, 5, 6, 8$.
3. A nonzero $k \in \mathbb{Z}_n$ is a zero divisor $\gcd(n, k) > 1$.
4. The ring $R = M_2(\mathbb{R})$ has zero divisors, such as:

$$\begin{bmatrix} 1 & -2 \\ -2 & 4 \end{bmatrix} \begin{bmatrix} 6 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

One particular type of zero divisor will be important later.

Definition

An element a in a ring R is nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$.

Group rings

A rich family of examples of rings can be constructed from multiplicative groups.

Let G be a finite (multiplicative) group, and R a commutative ring (usually, $\mathbb{Z}$, $\mathbb{R}$, or $\mathbb{C}$).

The group ring RG is the set of formal linear combinations of groups elements with coefficients from R. That is,

$$RG := \{a_1 g_1 + \cdots + a_n g_n \mid a_i \in R,\ g_i \in G\},$$

where multiplication is defined in the "obvious" way.

For example, let $R = \mathbb{Z}$ and $G = D_4$, and take $x = r + r^2 - 3f$ and $y = -5r^2 + rf$ in $\mathbb{Z}D_4$.

Their sum is

$$x + y = r - 4r^2 - 3f + rf,$$

and their product is

$$\begin{aligned} xy &= (r + r^2 - 3f)(-5r^2 + rf) = r(-5r^2 + rf) + r^2(-5r^2 + rf) - 3f(-5r^2 + rf) \\ &= -5r^3 + r^2 f - 5r^4 + r^3 f + 15fr^2 - 3frf = -5 - 8r^3 + 16r^2 f + r^3 f. \end{aligned}$$

Tip

Think of $\mathbb{Z}D_4$ as linear combinations of the "basis vectors"

$$\{\mathbf{e}_1,\ \mathbf{e}_r,\ \mathbf{e}_{r^2},\ \mathbf{e}_{r^3},\ \mathbf{e}_f,\ \mathbf{e}_{rf},\ \mathbf{e}_{r^2 f},\ \mathbf{e}_{r^3 f}\}.$$

Group rings

For another example, consider the group ring $\mathbb{R}Q_8$. Elements are formal sums

$$a + bi + cj + dk + e(-1) + f(-i) + g(-j) + h(-k), \qquad a, \ldots, h \in \mathbb{R}.$$

Every choice of coefficients gives a different element in $\mathbb{R}Q_8$!

For example, if all coefficients are zero except $a = e = 1$, we get

$$1 + (-1) \neq 0 \in \mathbb{R}Q_8 \qquad \textit{(because "}\mathbf{e}_1 + \mathbf{e}_{-1} \neq \mathbf{0}\textit{")}.$$

In contrast, in the Hamiltonians, $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$,

$$1 + (-1) = [1 + 0i + 0j + 0k] + [(-1) + 0i + 0j + 0k] = (1 - 1) + 0i + 0j + 0k = 0.$$

Therefore, $\mathbb{H}$ and $\mathbb{R}Q_8$ are different rings.

Remarks

- If $g \in G$ has finite order $|g| = k > 1$, then RG always has zero divisors:

$$(1 - g)(1 + g + \cdots + g^{k-1}) = 1 - g^k = 1 - 1 = 0.$$

- RG contains a subring isomorphic to R.
- the group of units $U(RG)$ contains a subgroup isomorphic to G.

Fields and division rings

Definition

If every nonzero element of R has a multiplicative inverse, then R is a division ring. It is a

- field if R is commutative,
- skew field ir R is not commutative.

Examples of fields we've seen include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_p$ for prime p.

The Hamiltonians $\mathbb{H}$ are a skew field.

Definition

A quadratic field is any field of the form

$$\mathbb{Q}(\sqrt{m}) = \left\{ r + s\sqrt{m} \mid r, s \in \mathbb{Q} \right\},$$

where $m \neq 0, 1$ is a square-free integer. We say "$\mathbb{Q}$ *adjoin* $\sqrt{m}$."

This is a field because:

$$(r + s\sqrt{m})(r - s\sqrt{m}) = r^2 - s^2 m, \qquad (r + s\sqrt{m})^{-1} = \frac{r - s\sqrt{m}}{r^2 - s^2 m}.$$

Integral domains

Definition

An integral domain is a commutative ring with 1 and with no (nonzero) zero divisors.

An integral domain is a "field without inverses".

A field is just a commutative division ring. Moreover:

$$\text{fields} \subsetneq \text{division rings}, \qquad \text{fields} \subsetneq \text{integral domains}.$$

Examples

- Rings that are not integral domains: $\mathbb{Z}_n$ (composite n), $2\mathbb{Z}$, $M_n(\mathbb{R})$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{H}$.
- Integral domains that are not fields $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{R}[[x]]$ (formal power series).

The ring "$\mathbb{Z}$ adjoin $\sqrt{m}$," defined as

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\},$$

is an integral domain, but not a field.

Cancellation

When doing basic algebra, we often take for granted basic properties such as cancellation:

$$ax = ay \quad \Longrightarrow \quad x = y.$$

This need not hold in all rings!

Examples where cancellation fails

- In $\mathbb{Z}_6$, note that $2 = 2 \cdot 1 = 2 \cdot 4$, but $1 \neq 4$.
- In $M_2(\mathbb{R})$, note that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$.

However, everything works fine as long as there aren't any (nonzero) zero divisors.

Proposition

Let R be an integral domain and $a \neq 0$. If $ax = ay$ for some $x, y \in R$, then $x = y$.

Proof

If $ax = ay$, then $ax - ay = a(x - y) = 0$.

Since $a \neq 0$ and R has no (nonzero) zero divisors, then $x - y = 0$. $\square$

Finite integral domains

Remark

If R is an integral domain and $0 \neq a \in R$ and $k \in \mathbb{N}$, then $a^k \neq 0$. □

Theorem

Every finite integral domain is a field.

Proof

Suppose R is a finite integral domain and $0 \neq a \in R$. It suffices to show that a has a multiplicative inverse.

Consider the infinite sequence $a, a^2, a^3, a^4, \dots,$ which must repeat.

Find $i > j$ with $a^i = a^j$, which means that

$$0 = a^i - a^j = a^j(a^{i-j} - 1).$$

Since R is an integral domain and $a^j \neq 0$, then $a^{i-j} = 1$.

Thus, $a \cdot a^{i-j-1} = 1$. □

Ideals and quotients

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

- $R/I = \{x + I \mid x \in R\}$ 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, $xy - rs \in I$:

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

Group theory

- normal subgroups are characterized by being invariant under conjugation:

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

- The quotient G/N exists iff N is a normal: $N \trianglelefteq G$
- A homomorphism is a structure-preserving map: $f(x * y) = f(x) * f(y)$.
- The kernel of a homomorphism is normal: $\mathrm{Ker}(\phi) \trianglelefteq G$.
- If $N \trianglelefteq G$, there is a natural quotient $\pi\colon G \to G/N$, $\pi(g) = gN$.
- There are four isomorphism theorems.

Ring theory

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

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

- The quotient ring R/I exists iff I is a two-sided ideal: $I \trianglelefteq R$.
- A homomorphism is structure-preserving: $f(x+y) = f(x)+f(y)$, $f(xy) = f(x)f(y)$.
- The kernel of a homomorphism is a two-sided ideal: $\mathrm{Ker}(\phi) \trianglelefteq R$.
- If $I \trianglelefteq R$, there is a natural quotient $\pi\colon R \to R/I$, $\pi(r) = r + I$.
- There are four isomorphism theorems.

Ring homomorphisms

Definition

A ring homomorphism is a function $f\colon R \to S$ satisfying

$$f(x+y) = f(x) + f(y) \qquad \text{and} \qquad f(xy) = f(x)f(y) \quad \text{for all } x, y \in R.$$

A ring isomorphism is a homomorphism that is bijective.

The kernel $f\colon R \to S$ is the set $\mathrm{Ker}(f) := \{x \in R \mid f(x) = 0\}$.

Examples

1. The ring homomorphism $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ sending $k \mapsto k \pmod{n}$ has $\mathrm{Ker}(\phi) = n\mathbb{Z}$.
2. For a fixed real number $\alpha \in \mathbb{R}$, the "evaluation function"

$$\phi\colon \mathbb{R}[x] \longrightarrow \mathbb{R}\,, \qquad \phi\colon p(x) \longmapsto p(\alpha)$$

   is a homomorphism. The kernel consists of all polynomials that have α as a root.
3. The following is a homomorphism, for the ideal $I = (x^2 + x + 1)$ in $\mathbb{F}_2[x]$:

$$\phi\colon \mathbb{F}_2[x] \longrightarrow \mathbb{F}_2[x]/I, \qquad f(x) \longmapsto f(x) + I\,.$$

Isomoprhism theorem prerequisites

Proposition

The kernel of a ring homomorphism $\phi \colon R \to S$ is a two-sided ideal.

Proof

We know that $\mathrm{Ker}(\phi)$ is an additive subgroup of R. We must show that it's an ideal.

Left ideal: Let $k \in \mathrm{Ker}(\phi)$ and $r \in R$. Then

$$\phi(rk) = \phi(r)\phi(k) = \phi(r) \cdot 0 = 0 \quad \Longrightarrow \quad rk \in \mathrm{Ker}(\phi). \qquad \checkmark$$

Showing that $\mathrm{Ker}(\phi)$ is a right ideal is analogous. $\square$

Proposition

The sum $S + I = \{s + i \mid s \in S,\ i \in I\}$ of a sum and an ideal is a subring of R.

Proof

$S + I$ is an additive subgroup, and it's closed under multiplication because

$$s_1, s_2 \in S,\ i_1, i_2 \in I \quad \Longrightarrow \quad (s_1 + i_1)(s_2 + i_2) = \underbrace{s_1 s_2}_{\in S} + \underbrace{s_1 i_2 + i_1 s_2 + i_1 i_2}_{\in I} \in S + I. \qquad \square$$

The isomorphism theorems for rings

All of the isomorphism theorems for groups have analogues for rings.

- Fundamental homomorphism theorem: "*All homomorphic images are quotients*"
- Correspondence theorem: Characterizes "*subrings and ideals of quotients*"
- Fraction theorem: Characterizes "*quotients of quotients*"
- Diamond theorem: characterizes "*quotients of a sum*"

Since a ring is an abelian group with extra structure, we don't have to prove these from scratch.

FHT for rings

If $\phi\colon R \to S$ is a ring homomorphism, then $R/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$.

Proof (sketch)

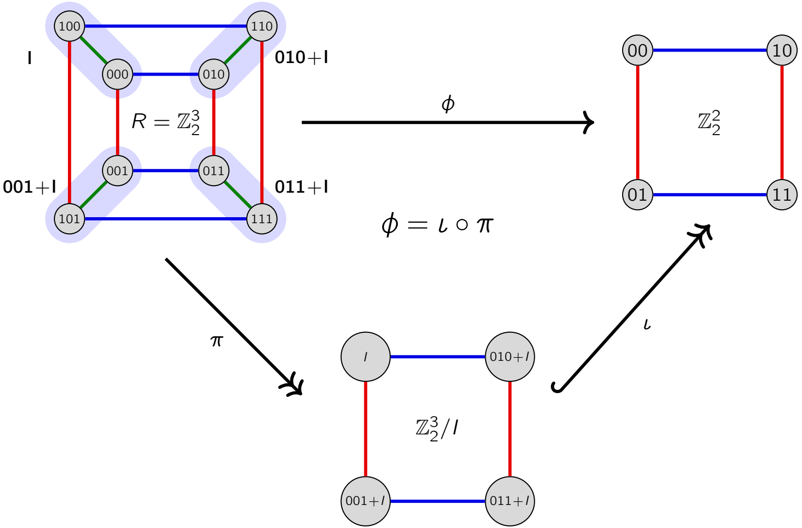
The statement holds for the underlying additive group R. Thus, it remains to show that the relabeling map (a group isomorphism)

$$\iota\colon R/I \longrightarrow \operatorname{Im}(\phi)\,, \qquad \iota(r+I) = \phi(r).$$

is also a ring homomorphism:

The FHT for rings

Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2$, $\qquad \phi\colon abc \longmapsto bc$.



The FHT for rings

Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2, \qquad \phi\colon abc \longmapsto bc.$

By the FHT for groups, we know that $\mathbb{Z}_2^3/\,\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi) = \mathbb{Z}_2^2$, as (additive) groups.

+	000	100	010	110	001	101	011	111
000	000	100	010	110	001	101	011	111
100	100	000	110	010	101	001	111	011
010	010	110	000	100	011	111	001	101
110	110	010	100	000	111	011	101	001
001	001	101	011	111	000	100	010	110
101	101	001	111	011	100	000	110	010
011	011	111	001	101	010	110	000	100
111	111	011	101	001	110	010	100	000

000+I	010+I	001+I	011+I
010+I	000+I	011+I	001+I
001+I	011+I	000+I	010+I
011+I	001+I	010+I	000+I

$\xrightarrow{\ \iota\ }$

+	000	100	010	110	001	101	011	111
000	000	100	010	110	001	101	011	111
100	100	000	110	010	101	001	111	011
010	010	110	000	100	011	111	001	101
110	110	010	100	000	111	011	101	001
001	001	101	011	111	000	100	010	110
101	101	001	111	011	100	000	110	010
011	011	111	001	101	010	110	000	100
111	111	011	101	001	110	010	100	000

-00	-10	-01	-11
-10	-00	-11	-01
-01	-11	-00	-10
-11	-01	-10	-00

The image is isomorphic to the Klein 4-group

$$\mathbb{Z}_2^2 \cong \{\underbrace{(0,0)}_{0}, \underbrace{(1,0)}_{a}, \underbrace{(0,1)}_{b}, \underbrace{(1,1)}_{c}\}.$$

	0	*a*	*b*	*c*
0	0	*a*	*b*	*c*
a	*a*	0	*c*	*b*
b	*b*	*c*	0	*a*
c	*c*	*b*	*a*	0

+	00	10	01	11
00	00	10	01	11
10	10	00	11	01
01	01	11	00	10
11	11	01	10	00

The FHT theorem for rings says that ι also preserves the multiplicative structure of R/I.

The FHT for rings

Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2$, $\qquad \phi\colon abc \longmapsto bc$.

The following Cayley tables show how ι preserves the multiplicative structure:

$$\iota\big((r+I)(s+I)\big) = \iota(rs+I).$$

×	000 100	010 110	001 101	011 111
000 100	000 000 000+I 000 100	000 000 000+I 000 100	000 000 000+I 000 100	000 000 000+I 000 100
010 110	000 000 000+I 000 100	010 010 010+I 010 110	000 000 000+I 000 100	010 010 010+I 010 110
001 101	000 000 000+I 000 100	000 000 000+I 000 100	001 001 001+I 001 101	001 001 001+I 001 101
011 111	000 000 000+I 000 100	010 010 010+I 010 110	001 001 001+I 001 101	011 011 011+I 011 111

$\xrightarrow{\quad\iota\quad}$

×	000 100	010 110	001 101	011 111
000 100	000 000 -00 000 100	000 000 -00 000 100	000 000 -00 000 100	000 000 -00 000 100
010 110	000 000 -00 000 100	010 010 -10 010 110	000 000 -00 000 100	010 010 -10 010 110
001 101	000 000 -00 000 100	000 000 -00 000 100	001 001 -01 001 101	001 001 -01 001 101
011 111	000 000 -00 000 100	010 010 -10 010 110	001 001 -01 001 101	011 011 -11 011 111

This quotient ring is isomorphic to

$$\Bigg\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{c} \Bigg\}.$$

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

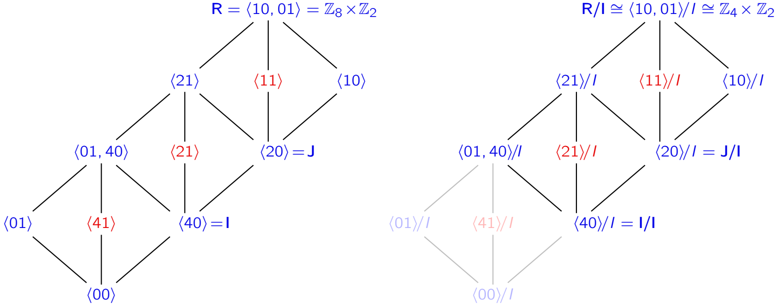
×	00	10	01	11
00	00	00	00	00
10	00	10	00	10
01	00	00	01	01
11	00	10	01	11

The correspondence theorem: subrings of quotients

Correspondence theorem

Let I be an ideal of R. There is a bijective correspondence between subrings of R/I and subrings of R that contain I.

Moreover every ideal of R/I has the form J/I, for some ideal satisfying $I \subseteq J \subseteq R$.

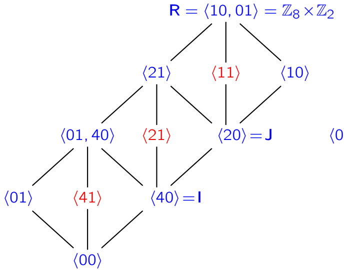


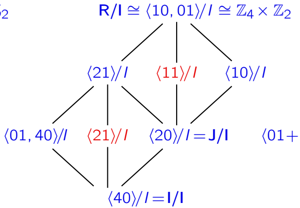
Big idea

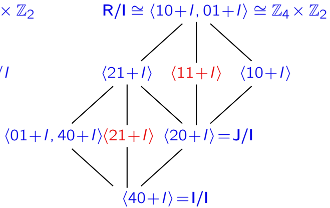
This is just like the correspondence theorem for groups, but it also "preserves colors."

The correspondence theorem: subrings of quotients

"*The ideals of a quotient R/I are just the quotients of the ideals that contain I.*"







"*shoes out of the box*"

30	70	31	71
10	50	11	51
20	60	21	61
00	40	01	41

$J = \langle 20\rangle \leq R$

"*shoeboxes; lids off*"

30	70	31	71
10	50	11	51
20	60	21	61
00	40	01	41

$\langle 20\rangle/I \leq R/I$

"*shoeboxes; lids on*"

$30+I$	$31+I$
$10+I$	$11+I$
$20+I$	$21+I$
I	$01+I$

$\langle 20+I\rangle \leq R/I$

The correspondence theorem: subrings of quotients

Correspondence theorem (informally)

There is a bijection between subrings of R/I and subrings of R that contain I.

"Everything that we want to be true" about the subring lattice of R/I is inherited from the subring lattice of R.

Most of these can be summarized as:

"The __________ of the quotient is just the quotient of the __________"

Correspondence theorem (formally)

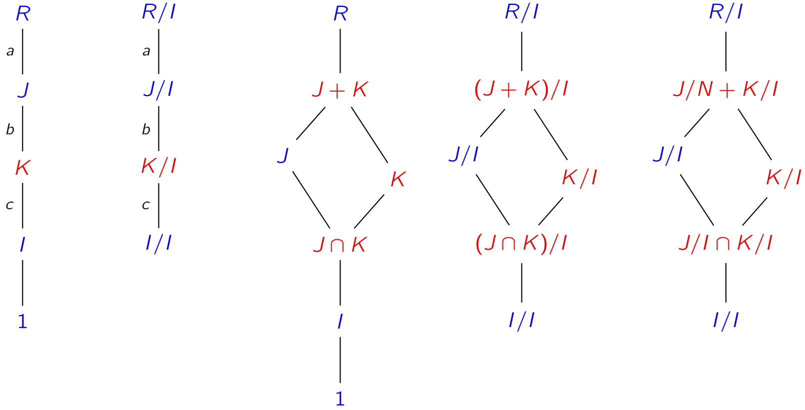
Let $I \leq J \leq R$ and $I \leq K \leq R$ be chains of subrings and $I \trianglelefteq G$. Then

1. Subrings of the quotient R/I are quotients of the subring $J \leq R$ that contain I.
2. $J/I \trianglelefteq R/I$ if and only if $J \trianglelefteq R$
3. $[R/I : J/I] = [R : J]$
4. $J/I \cap K/I = (J \cap K)/I$
5. $J/I + K/I = (J + K)/I$

The correspondence theorem: subring structure of quotients

All parts of the correspondence theorem have nice subring lattice interpretations.

We've already interpreted the the first part. Here's what the next four parts say.



The fraction theorem: quotients of quotients

The correspondence theorem characterizes the subring structure of the quotient R/J.

Every subring of R/I is of the form J/I, where $I \leq J \leq R$.

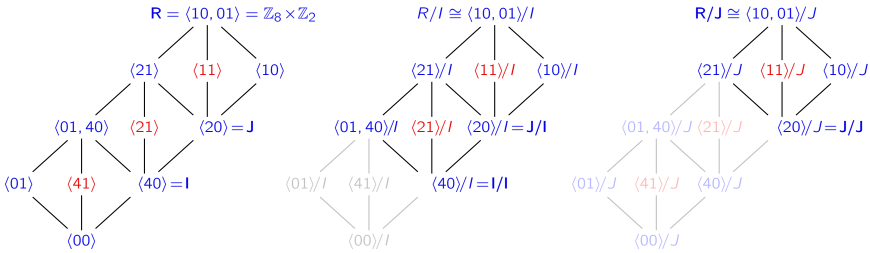
Moreover, if $J \trianglelefteq R$ is an ideal, then $J/I \trianglelefteq R/I$. In this case, we can ask:

"*What is the quotient ring* $(R/I)/(J/I)$ *isomorphic to?*"

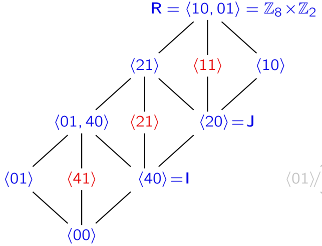
Fraction theorem

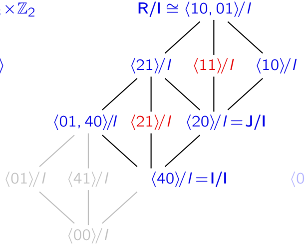
Suppose R is a ring with ideals $I \subseteq J$. Then J/I is an ideal of R/I and

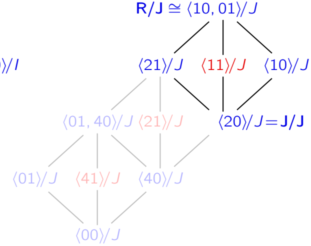
$$(R/I)/(J/I) \cong R/J.$$

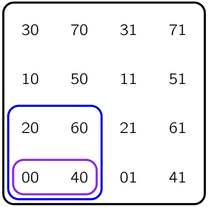


The fraction theorem: quotients of quotients

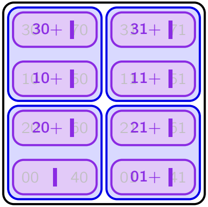




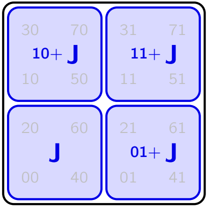




$I \leq J \leq R$



R/I consists of 8 cosets



R/J consists of 4 cosets

The fraction theorem: quotients of quotients

For another visualization, consider $R = \mathbb{Z}_6 \times \mathbb{Z}_4$ and write elements as strings.

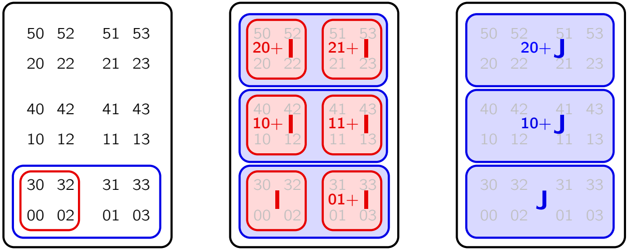
Consider the ideals $J = \langle 30, 02 \rangle \cong \mathbb{Z}_2^2$ and $I = \langle 30, 01 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

Notice that $I \leq J \leq R$, and $I = J \cup (01{+}J)$, and

$$R/I = \big\{I,\ 01{+}I,\ 10{+}I,\ 11{+}I,\ 20{+}I,\ 21{+}I\big\}, \qquad J/I = \{I,\ 01{+}I\}$$

$$R/J = \Big\{I \cup (01{+}I),\ (10{+}I) \cup (11{+}I),\ (20{+}I) \cup (21{+}I)\Big\}$$

$$(R/I)/(J/I) = \Big\{\{I,\ 01{+}I\},\ \{10{+}I,\ 11{+}I\},\ \{20{+}I,\ 21{+}I\}\Big\}.$$



$I \leq J \leq R$

R/I consists of 6 cosets
$J/I = \{I,\ 01{+}I\}$

R/J consists of 3 cosets
$(R/I)/(J/I) \cong R/J$

The diamond theorem: quotients of sums

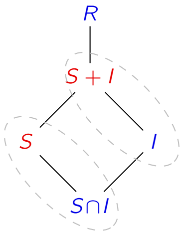
Diamond theorem

Suppose S is a subring and I an ideal of R. Then

(i) The intersection $S \cap I$ is an ideal of S.

(ii) The following quotient rings are isomorphic:

$$(S+I)/I \cong S/(S \cap I)\,.$$



Proof (sketch)

(i) Showing $S \cap I$ is an ideal of S is straightforward (exercise).

(ii) We already know that $(S+I)/I \cong S/(S \cap I)$ as additive groups.

Recall that we proved this by applying the FHT to the (group) homomorphism

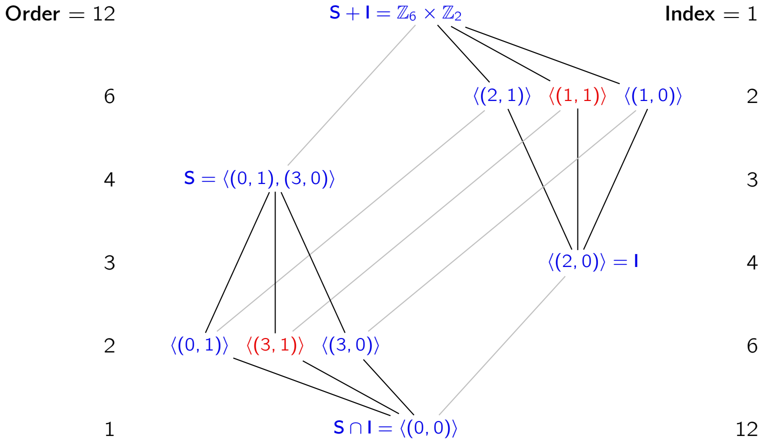
$$\phi\colon S \longrightarrow (S+I)/I, \qquad \phi\colon s \longmapsto s+I.$$

It remains to show that ϕ is a ring homomorphism, i.e., $\phi(s_1 s_2) = \phi(s_1)\phi(s_2)$. $\square$

The diamond theorem: quotients of sums by factors

Like for groups, the diamond theorem guarantees an inherent “duality” in subring lattices.

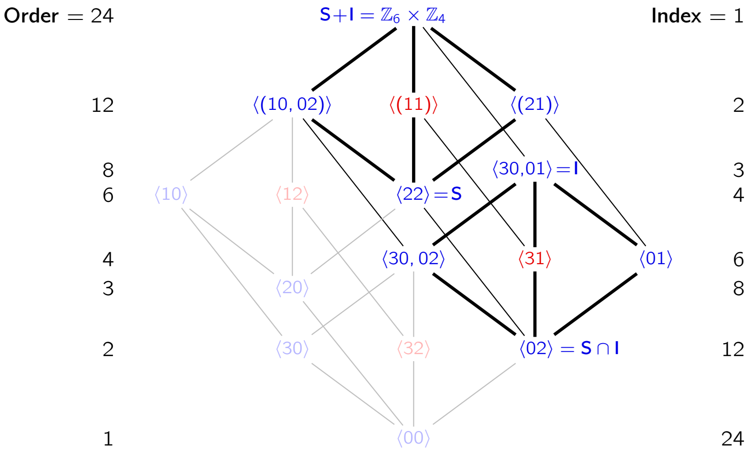
For rings, it also “preserves the colors” – subgroup, subring, and ideal structure.



The diamond theorem: quotients of sums by factors

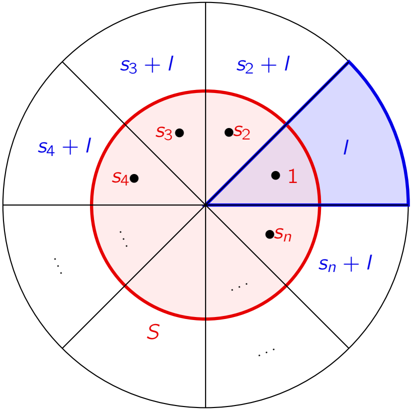
Like for groups, the diamond theorem guarantees an inherent "duality" in subring lattices.

For rings, it also "preserves the colors" – subgroup, subring, and ideal structure.



The diamond theorem illustrated by a "pizza diagram"

The following analogy is due to Douglas Hofstadter:



$S + I =$ large pizza

$S =$ small pizza

$I =$ large pizza slice

$S \cap I =$ small pizza slice

$(S + I)/I = \{\text{large pizza slices}\}$

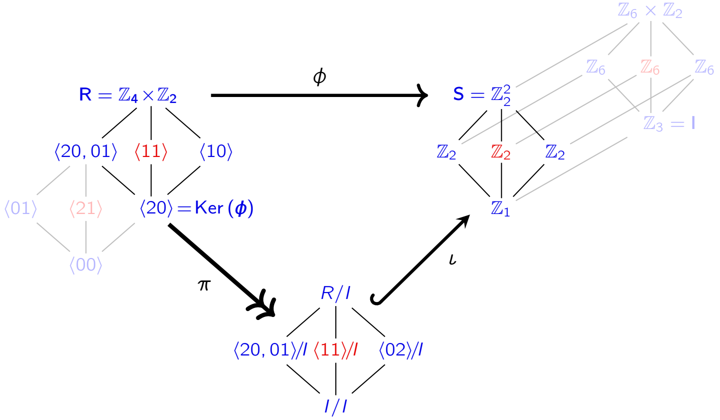
$S/(S \cap I) = \{\text{small pizza slices}\}$

Diamond theorem: $(S + I)/I \cong S/(S \cap I)$

Theorem (exercise)

Every homomorphism $\phi\colon R \to S$ can be factored as a quotient and embedding:

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, two heads, "\pi"'] & & S \\ & R/I \arrow[ur, hook, dashed, "\iota"'] & \end{tikzcd} \qquad \begin{tikzcd} r \arrow[rr, mapsto, "\phi"] \arrow[dr, mapsto, two heads, "\pi"'] & & \phi(r) \\ & r+I \arrow[ur, mapsto, dashed, "\iota"'] & \end{tikzcd}$$



Maximal ideals and simple rings

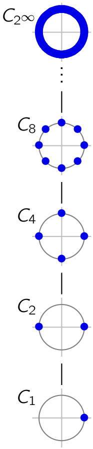
A maximal normal subgroup M of G has no normal subgroups $M \lneq N \lneq G$. Formally:

$$M \leq N \leq G, \quad \text{and} \quad M, N \trianglelefteq G \qquad \Longrightarrow \qquad N = M, \text{ or } N = G.$$

By the correspondence theorem, a normal subgroup $M \trianglelefteq G$ is maximal iff G/M is simple.

The Prüfer group C_{p^∞} of all p^n-th roots of unity ($n \in \mathbb{N}$) has no maximal normal subgroups:

$$\langle 1 \rangle \leq C_p \leq C_{p^2} \leq C_{p^3} \leq \cdots \leq C_{p^\infty}, \qquad C_n = \left\{ e^{2\pi i k/n} \mid k \in \mathbb{N} \right\} \subseteq \mathbb{C}.$$



Definition

An ideal $I \subsetneq R$ is maximal if $I \subseteq J \trianglelefteq R$ implies $J = I$ or $J = R$.

A ring R is simple if its only (two-sided) ideals are 0 and R.

The following is immediate by the correspondence theorem.

Remark

An ideal $M \trianglelefteq R$ is maximal iff R/M is simple.

Maximal ideals and simple rings

Simple rings have no nontrivial proper ideals. Proper ideals cannot contain units.

In a field, *every* nonzero element is a unit. Therefore, fields have no nontrivial proper ideals.

Proposition

A commutative ring R with unity is simple iff it is a field.

Proof

"$\Rightarrow$": Assume R is simple. Then $(a) = R$ for any nonzero $a \in R$.

Thus, $1 \in (a)$, so $1 = ba$ for some $b \in R$, so $a \in U(R)$ and R is a field. ✓

"$\Leftarrow$": Let $I \subseteq R$ be a nonzero ideal of a field R. Take any nonzero $a \in I$.

Then $a^{-1}a \in I$, and so $1 \in I$, which means $I = R$. ✓ □

Theorem

Let R be a commutative ring with 1. The following are equivalent for an ideal $I \subseteq R$.

(i) I is maximal; (ii) R/I is simple; (iii) R/I is a field.

Examples of maximal ideals & simple rings

1. The maximal ideals of $R = \mathbb{Z}$ are $M = (p)$. The quotient field is $\mathbb{Z}/(p) \cong \mathbb{Z}_p$
2. Maximal ideals of $R = \mathbb{Z}[x]$ includes those of the form
$$(x, p) = \big\{xf(x) + p \cdot g(x) \mid f, g \in \mathbb{Z}[x]\big\} = \big\{a_n x^n + \cdots + a_1 x + pa_0 \mid a_i \in \mathbb{Z}\big\}.$$
In the quotient field, "$x := 0$" and "$p := 0$", and so
$$\mathbb{Z}[x]/(x, p) = \big\{a_0 + M \mid a_0 = 0, \ldots, p-1\big\} \cong \mathbb{Z}_p.$$
3. Let $R = \mathbb{Q}[x]$. The ideal
$$(x) = \big\{xf(x) \mid f \in \mathbb{Q}[x]\big\} = \big\{a_n x^n + \cdots + a_1 x \mid a_i \in \mathbb{Z}\big\}$$
is maximal. In the quotient field, "$x := 0$", and so
$$\mathbb{Q}[x]/(x) = \big\{a_0 + M \mid a_0 \in \mathbb{Q}\big\} \cong \mathbb{Q}.$$
4. In the multivariate ring $R = \mathbb{F}[x, y]$ over a field, the ideal
$$I = (x, y) = \big\{x \cdot f(x, y) + y \cdot g(x, y) \mid f, g \in R\big\}$$
of polynomials with no constant term is maximal. The quotient field is $R/I \cong \mathbb{F}$.
5. Examples of simple noncommutative rings: $\mathbb{H}$, and $\mathrm{M}_n(\mathbb{F})$.

Existence of maximal ideals

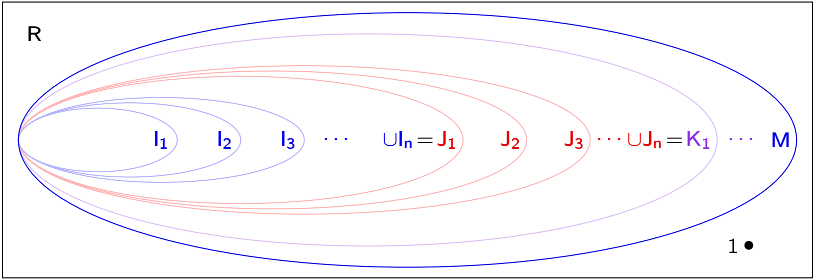
Given an ideal $I_1 \subsetneq R$. Let's try to find a maximal ideal that contains it.

If we have a sequence $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ of ideals, then $J_1 := \bigcup I_k \subsetneq R$ is an ideal.

If this isn't maximal, find $r_2 \notin J_1$, and let $J_2 = (J_1, r_2)$, and repeat this process.

Suppose we have $J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$. Then $K_1 := \bigcup J_k \subsetneq R$ is an ideal.

Is this process going to "stop"?



Assuming the axiom of choice: **YES!**

Ordinals and transfiniteness

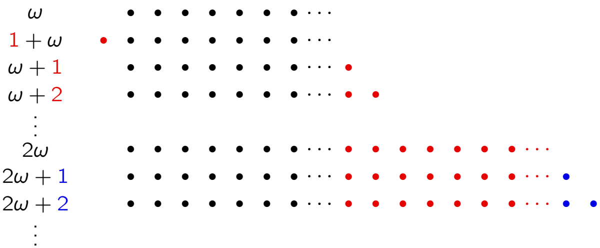
A set is well-ordered if every subset has a minimal element.

The natural numbers $\mathbb{N}$ are well-ordered, the integers $\mathbb{Z}$ are not.

Loosely speaking, an ordinal is an equivalence class of well-ordered sets.

Ordinal arithemetic involves addition, multiplication, and exponentiation.

The ordinal for $\mathbb{N}$ is denoted ω. Some things may be surprising, like $\omega = 1 + \omega \neq \omega + 1$.

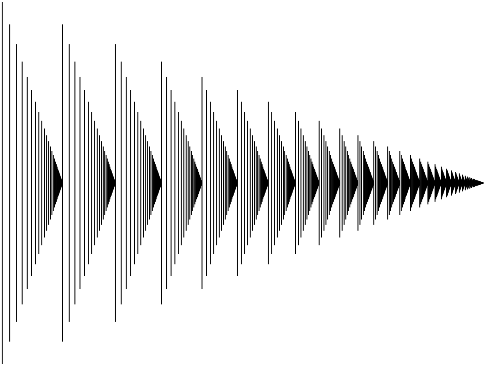


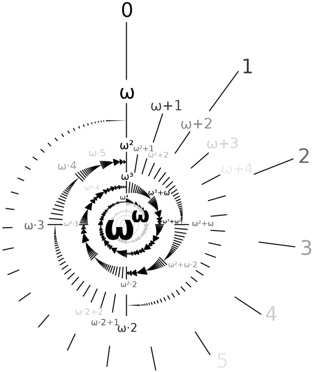
There are three types:

- finite ordinals
- successor ordinals
- limit ordinals

Ordinals and transfiniteness

Here are some depictions of the ordinals ω^2 and ω^ω.





Mathematical induction and recursion is traditionally done over the ordinal ω.

Over general ordinals, these are callled transfinite induction and recursion.

The axiom of choice is needed.

The maximal ideal of $I \subseteq R$ is basically the result of a *transfinite union*.

Existence of maximal ideals

Zorn's lemma (equivalent to the axiom of choice)

If $\mathcal{P} \neq \emptyset$ is a poset in which every chain has an upper bound, then $\mathcal{P}$ has a maximal element.

Proposition

If R is a ring with 1, then every ideal $I \neq R$ is contained in a maximal ideal M.

Proof

Fix I, and let $\mathcal{P}$ be the poset of *proper ideals* containing it.

Every chain $I \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ has an upper bound, $\bigcup I_k \subsetneq R$.

Zorn's lemma guarantees a maximal element M in $\mathcal{P}$, which is a maximal ideal containing I.

Corollary

If R is a ring with 1, then every non-unit is contained in a maximal ideal M.

Do you see why this doesn't work for maximal subgroups?

The characteristic of a field

Definition

The characteristic of $\mathbb{F}$, denoted $\mathbf{char}\,\mathbb{F}$, is the smallest $n \geq 1$ for which

$$n1 := \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If there is no such n, then $\mathbf{char}\,\mathbb{F} := 0$.

Proposition

If the characteristic of a field is positive, then it must be prime.

Proof

If $\mathbf{char}\,\mathbb{F} = n = ab$, we can write

$$\underbrace{1 + \cdots + 1}_{n} = (\underbrace{1 + \cdots + 1}_{a})(\underbrace{1 + \cdots + 1}_{b}) = 0.$$

Since $\mathbb{F}$ contains no zero divisors, either $a = n$ or $b = n$, hence n is prime. $\square$

Finite fields

We've already seen:

- $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ is a field if p is prime
- every finite integral domain is a field.

But *what do these "other" finite fields look like?*

Let $R = \mathbb{F}_2[x]$. (We can ignore negative signs.)

The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$ because it doesn't factor as $f(x) = g(x)h(x)$ of lower-degree terms. (Note that $f(0) = f(1) = 1 \neq 0$.)

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

In 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:

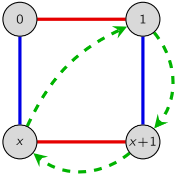
$$0 + I\,, \qquad 1 + I\,, \qquad x + I\,, \qquad (x+1) + I.$$

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

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

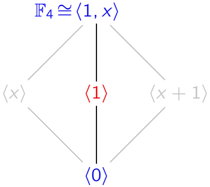
Finite fields

Here is the finite field of order 4: $F_4 \cong R/I = \mathbb{F}_2[x]/(x^2+x+1)$:



$+$	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 (wait until Galois theory)

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

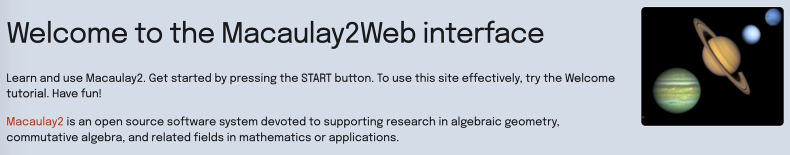
$$\mathbb{F}_p[x]/(f),$$

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 DVDs to play despite scratches.

Computations within finite fields

The Macaulay2 software system was written for researchers in algebraic geometry and commutative algebra.



It is freely available online:

`https://www.unimelb-macaulay2.cloud.edu.au/`

If we want to work in the quotient field $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3+x+1)$, we can type in:

```
R = ZZ/2[x] / ideal(x^3+x+1)
```

In $\mathbb{F}_2[x]$, the product $(x^2+x+1)(x+1) = x^3+2x^2+2x+1$ is just x^3+1.

Since $x^3 \equiv x+1$ modulo (x^3+x+1), this reduces down to x.

Macaulay2 can compute this immediately, just by typing:

```
(x^2+x+1)*(x+1)
```

Finite fields

Here is finite field of order 8: $\mathbb{F}_8 \cong R/I = \mathbb{F}_2[x]/(x^3+x+1)$:

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

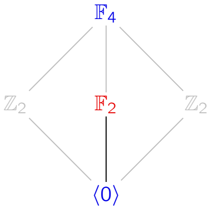
$\times$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

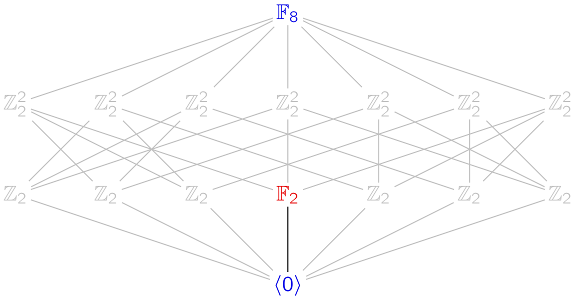
Notice how $\mathbb{F}_2 = \{0, 1\}$ arises is a subfield, but not $\mathbb{F}_4$. (*Why?*)

Finite fields

The multiplictive groups of these finite fields are $\mathbb{F}_4^\times \cong C_3$ and $\mathbb{F}_8^\times \cong C_7$.

If $\mathbb{F}_8$ had $\mathbb{F}_4$ as a subfield, then it would have three elements of order 3.

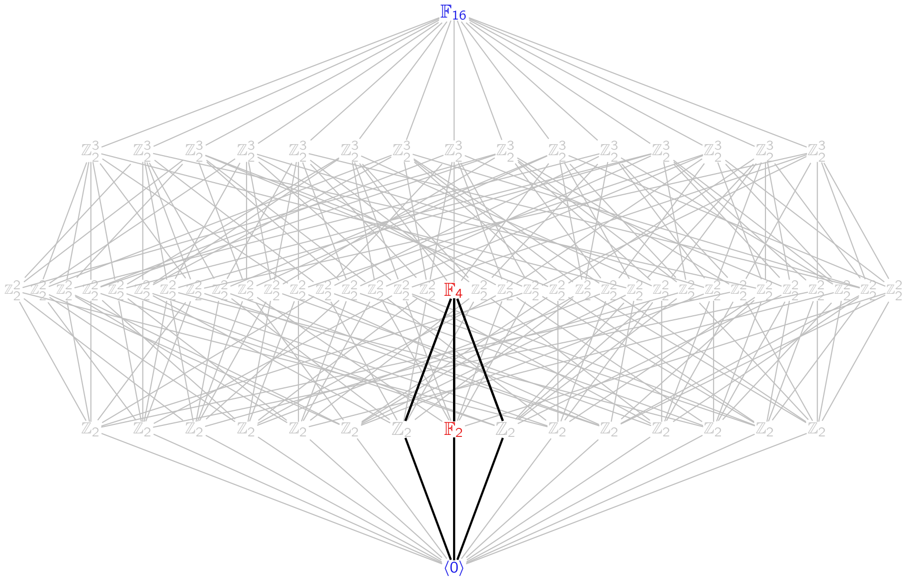




Similarly, $\mathbb{F}_{16}$ has 35 $\mathbb{Z}_2^2$-subgroups, but $\mathbb{F}_{16}^\times \cong C_{15}$ has only two elements of order 3.

These, with 0 and 1, comprise its unique $\mathbb{F}_4$-subfield.

The subring lattice of the finite field $\mathbb{F}_{16} \cong \mathbb{Z}_2[x]/(x^4+x+1)$



Subfields of finite fields

Proposition

If $\mathbb{F}$ is a finite field, then $|\mathbb{F}| = p^n$ for some prime p and $n \geq 1$.

Proof

If **char** $\mathbb{F} = p$, then $\mathbb{F}$ contains $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ as a subfield.

Note that $\mathbb{F}$ is an $\mathbb{F}_p$-vector space, so pick a basis, $x_1, \dots, x_n$.

Every $x \in \mathbb{F}$ can be written uniquely as

$$x = a_1 x_1 + \cdots + a_n x_n, \qquad a_i \in \mathbb{F}_p.$$

Counting elements immediately gives $|\mathbb{F}| = p^n$.

Proposition

If $\mathbb{F}_{p^n}$ contains a subfield isomorphic to $\mathbb{F}_{p^m}$, then $m \mid n$.

Proof

Same as above, but $\mathbb{F}_{p^n}$ is an $\mathbb{F}_{p^m}$-vector space. Take a basis $x_1, \dots, x_k$, count elements. $\square$

Finite multiplictive subgroups of a field

Proposition (upcoming)

In a field, a degree-n polynomial can have at most n roots.

Proof (sketch)

The polynomial ring $\mathbb{F}[x]$ has unique factorization. (We'll show this soon.)

If $f(r) = 0$, then factor $f(x) = (x - r)g(x)$, where $\deg g = n - 1$. Apply induction.

Proposition

Every finite subgroup of the multiplictive group $\mathbb{F}^\times$ is cyclic.

Proof

Let $H \leq \mathbb{F}^\times$ have finite order. If it were not cyclic, then $C_{p^n} \times C_{p^m} \leq H$ for $n, m \geq 1$.

Since each factor has a C_p-subgroup, $\mathbb{F}^\times$ has a C_p^2-subgroup.

All p^2 elements in H satisfy $f(x) = x^p - 1$, which is impossible. $\square$

Prime ideals

Euclid's lemma (300 B.C.)

If a prime p divides ab, then it must divide a or b.

Definition

Let R be a commutative ring. An ideal $P \subsetneq R$ is prime if $ab \in P$ implies $a \in P$ or $b \in P$.

Examples

1. The ideal (n) of $\mathbb{Z}$ is a prime ideal iff n is a prime number (possibly $n = 0$).
2. In $\mathbb{Z}[x]$, the ideals $(2, x)$ and (x) are prime.
3. The ideal $(2, x^2 + 5)$ is not prime in $\mathbb{Z}[x]$ because

$$x^2 - 1 = (x+1)(x-1) \in (2, x^2+5), \qquad \text{but } x \pm 1 \notin (2, x^2+5).$$

Proposition (exercise)

R is an integral domain if and only if $0 := \{0\}$ is a prime ideal. $\square$

Prime ideals

Proposition

An ideal $P \subsetneq R$ is prime iff R/P is an integral domain.

Proof

Consider the canonical quotient

$$\pi\colon R \longrightarrow R/P, \qquad \pi(r) = \overline{r} := r + P.$$

Note that the zero element is $\overline{0} = P = p + P$, for any $p \in P$, and

$$\overline{a}\,\overline{b} = \overline{ab}, \qquad \text{because } (a+P)(b+P) = ab + P.$$

Using the definitions, and our "boring but useful coset lemma",

$$\begin{aligned} P \text{ is prime} \quad &\Longleftrightarrow \quad ab \in P \;\Rightarrow\; a \in P \text{ or } b \in P \\ &\Longleftrightarrow \quad \overline{ab} = 0 \;\Rightarrow\; \overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0} \\ &\Longleftrightarrow \quad R/P \text{ is an integral domain.} \end{aligned}$$

□

Corollary

In a commutative ring, every maximal ideal is prime. □

Primary ideals

Definition

Let R be a commutative ring. An ideal $P \subsetneq R$ is primary if $ab \in P$ implies $a \in P$ or $b^n \in P$ for some $n \in \mathbb{N}$.

In the integers:

- The prime ideals are of the form $(p) = p\mathbb{Z}$, for some prime p.
- The primary ideals are of the form $(p^n) = p^n\mathbb{Z}$, for some prime p.
- Every ideal can be written uniquely as an intersection of primary ideals. For example,

$$200\mathbb{Z} = 8\mathbb{Z} \cap 25\mathbb{Z}.$$

  This is its primary decomposition.

Remark

An ideal P of R is:

- prime iff the only zero divisor of R/P is zero,
- primary iff every zero divisor of R/P is nilpotent.

Radical ideals

Loosely speaking, a radical I of R is an ideal of "bad elements;" the quotient R/I is "nice."

Preview example 1

The nilradical of R has two equivalent characterizations:

- The set of nilpotent elements.
- The intesection of nonzero prime ideals.

$$\operatorname{Nil}(R) := \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N}\} = \bigcap_{0 \neq P \subsetneq R \text{ prime}} P.$$

The quotient $R/\operatorname{Nil}(R)$ is a "subdirect product" of integral domains.

Preview example 2

The Jacobson radical of R has two equivalent characterizations:

- The set of elements $x \in R$ that annihilate simple R-modules, i.e., $xM = 0$ for all M.
- The intesection of maximal ideals.

$$\operatorname{Jac}(R) := \{x \in R \mid 1 - rx \text{ is a unit for all } r \in R\} = \bigcap_{M \subsetneq R \text{ max'l}} M.$$

The quotient $R/\operatorname{Jac}(R)$ is a "subdirect product" of fields.

Subdirect products

Think of a subdirect product as being "*almost a direct product*."

The "diagonal subring" $S = \{(n, n) \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$ is a subdirect product because:

(i) It is a subring of $\mathbb{Z} \times \mathbb{Z}$.

(ii) It projects onto each component of the product.

Let $\{R_i \mid i \in I\}$ be a family of rings with direct product and projection maps

$$R = \prod_{i \in I} R_i, \qquad \begin{aligned} \pi_j \colon R &\longrightarrow R_j \\ (r_i)_{i \in I} &\longmapsto r_j. \end{aligned}$$

Definition

A ring S is a subdirect product of R if there is $\iota \colon S \hookrightarrow R$ such that each composition

$$S \xrightarrow{\iota} R \xrightarrow{\pi_j} R_j, \qquad s \xmapsto{\iota} (r_i)_{i \in I} \xmapsto{\pi_j} r_j$$

is surjective.

Subdirect products can be defined analogously for sets, groups, vector spaces, etc.

Subdirect products

Proposition

Let $\{J_i \mid i \in I\}$ be a family of ideals of R with $J = \bigcap_{i \in I} J_i$. Then R/J is a subdirect product of $\{R/J_i \mid i \in I\}$.

Proof

The map

$$\phi \colon R \longrightarrow \prod_{i \in I} R/J_i, \qquad x \longmapsto (x + J_i)_{i \in I}$$

is a homomorphism with $\mathrm{Ker}(\phi) = J$. By the FHT for rings, there is an isomorphism

$$\iota \colon R/J \longrightarrow \mathrm{Im}(\phi) \leq \prod_{i \in I} R/J_i.$$

The composition of maps is surjective, for each $j \in I$:

$$R/J \overset{\iota}{\hookrightarrow} \prod_{i \in I} R/J_i \xrightarrow{\pi_j} R/J_j, \qquad r + J \overset{\iota}{\longmapsto} \prod_{i \in I} (r + J_i)_{i \in I} \overset{\pi_j}{\longmapsto} r + J_j.$$

The nilradical of a ring

Definition (membership test)

The nilradical of R is the set of nilpotent elements:

$$\mathrm{Nil}(R) = \{a \in R \mid a^n = 0, \text{ for some } n \in \mathbb{N}\}.$$

Proposition

$\mathrm{Nil}(R)$ is an ideal of R.

Proof

Subgroup: Suppose $x, y \in \mathrm{Nil}(R)$, and $x^n = y^m = 0$. Using the binomial theorem,

$$(x-y)^{n+m} = \sum_{i=1}^{n+m} a_i x^i y^{n+m-i}.$$

Either $i \geq n$ (so $x^i = 0$) or $n+m-i \geq m$ (so $y^{n+m-i} = 0$) must hold. ✓

Ideal: If $x^n = 0$ and $r \in R$, then $(rx)^n = r^n x^n = 0$, so $rx \in \mathrm{Nil}(R)$. ✓

The nilradical of a ring

Proposition (ideal characterization)

The nilradical is the intersection of all nonzero prime ideals: $\text{Nil}(R) = \bigcap_{P \subsetneq R \text{ prime}} P$.

Proof

"$\subseteq$" Let $a \in \text{Nil}(R)$ and $P \subseteq R$ prime. Let $n \geq 1$ be minimal such that $a^n \in P$.

Since $a^{n-1}a \in P$ (prime), either $a^{n-1} \in P$ (contradiction) or $a \in P$. Thus $a \in \cap P$. ✓

"$\supseteq$" Suppose $a \notin \text{Nil}(R)$; we'll show $a \notin \cap P$.

$$\mathcal{S} = \{ J \trianglelefteq R \;\text{ s.t. }\; a^n \notin J \text{ for all } n \in \mathbb{N} \}.$$

$\mathcal{S}$ is nonempty since it contains (0).

We can apply Zorn's lemma (why?) to get a maximal element $P \in \mathcal{S}$.

P **is prime**: Say $xy \in P$ but $x, y \notin P$. Then $a^n \in \underbrace{(x)+P}_{\notin \mathcal{S}}$ and $a^m \in \underbrace{(y)+P}_{\notin \mathcal{S}}$ for some n, m.

But then $a^{nm} \in \underbrace{(xy)+P}_{=P}$, contradicting the fact that $P \in \mathcal{S}$. $\square$

The Jacobson radical of a ring

Definition (membership test)

The Jacobson radical of R is the set

$$\mathrm{Jac}(R) = \big\{x \in R \mid 1 - rx \text{ is a unit for all } r \in R\big\}.$$

Proposition (ideal characterization)

The Jacobson radical is the intersection of all maximal ideals: $\mathrm{Jac}(R) = \bigcap_{M \subsetneq R \text{ prime}} M.$

Proof

"$\subseteq$": Suppose $1 - rx \notin U(R)$ for some $x \in R$, and let M be a maximal ideal containing it.

If $r \in \mathrm{Jac}(R)$, then $r \in M$, which is impossible because

$$1 = \underbrace{(1 - rx)}_{\in M} + \underbrace{rx}_{\in M} \in M.$$

The Jacobson radical of a ring

Definition (membership test)

The Jacobson radical of R is the set

$$\operatorname{Jac}(R) = \big\{x \in R \mid 1 - rx \text{ is a unit for all } r \in R\big\}.$$

Proposition (ideal characterization)

The Jacobson radical is the intersection of all maximal ideals: $\operatorname{Jac}(R) = \bigcap_{M \subsetneq R \text{ max'l}} M.$

Proof

"$\supseteq$": Suppose $x \not\in M$ for some maximal ideal M. Then

$$R = M + (x) = \big\{m + rx \mid m \in M,\, r \in R\big\},$$

so we can write

$$1 = m + rx \qquad \Longrightarrow \qquad \underbrace{1 - xy}_{\not\in U(R)} = m \in M.$$

Quotients by radicals are subdirect products

Corollary

The quotient $R/\,\mathrm{Nil}(R)$ is a subdirect product of integral domains.

Proof

Let $\{P_i \mid i \in I\}$ be the set of prime ideals of R; recall $\mathrm{Nil}(R) = \bigcap_{i \in I} P_i$.

Then $R/\,\mathrm{Nil}(R)$ is a subdirect product of $\{R/P_i \mid i \in I\}$, which are all integral domains. $\square$

Corollary

The quotient $R/\,\mathrm{Jac}(R)$ is a subdirect product of fields.

Proof

Let $\{M_i \mid i \in I\}$ be the set of maximal ideals of R; recall $\mathrm{Jac}(R) = \bigcap_{i \in I} M_i$.

Then $R/\,\mathrm{Jac}(R)$ is a subdirect product of $\{R/M_i \mid i \in I\}$, which are all fields. $\square$

The radical of an ideal

Definition

The radical of an ideal I is the set

$$\sqrt{I} := \big\{ r \in R \mid r^n \in I, \text{ for some } n \in \mathbb{N} \big\}.$$

If $\sqrt{I} = I$, then I is a radical ideal.

The nilradical is just the radical of the zero ideal: $\mathrm{Nil}(R) = \sqrt{0}$.

Proposition

$\mathrm{Nil}(R/I) = \sqrt{I}/I$.

Proof (sketch; details for HW)

$$\begin{array}{cc} & R \\ & | \\ r \in & \sqrt{I} \\ \Downarrow & | \\ r^n \in & I \\ & | \\ & \langle 0 \rangle \end{array} \qquad\qquad \begin{array}{cc} & R/I \\ & | \\ \bar{r} \in & \sqrt{I}/I \\ \Downarrow & | \\ \bar{r}^n \in & I/I = \bar{0} \end{array}$$

The radicals of an ideal

Definition

The Jacobson radical of I is the intersection of all maximal ideals that contain it:

$$\mathrm{jac}(I) := \bigcap_{I \subseteq M \trianglelefteq R} M.$$

The Jacobson radical of R is the Jacobson radical of the zero ideal: $\mathrm{Jac}(R) := \mathrm{jac}(0)$.

Definition / proposition

The radical of I is the intersection of all prime ideals that contain it:

$$\sqrt{I} = \bigcap_{I \subseteq P \trianglelefteq R} P.$$

The nilradical of R is the radical of the zero ideal: $\mathrm{Nil}(R) := \sqrt{0}$.

Proposition (HW)

In a commutative ring with 1, an ideal P is prime iff it is primary and radical.

Motivation: constructing $\mathbb{Q}$ from $\mathbb{Z}$

Rational numbers are ordered pairs under an equivalence, e.g., $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$

Equivalence of fractions

Given $a, b, c, d \in \mathbb{Z}$, with $b, d \neq 0$,

$$\frac{a}{b} = \frac{c}{d} \qquad \text{if and only if} \qquad ad = bc.$$

We can mimic this construction in any integral domain.

Definition

Given an integral domain R, its field of fractions is the set

$$R \times R^* = \big\{(a, b) \mid a, b \in R,\ b \neq 0\big\},$$

under the equivalence $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1 b_2 = b_2 a_1$.

Denote the class containing (a, b) as a/b. Addition and multiplication are defined as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

It's not hard to show that $+$ and $\times$ are well-defined.

Embedding integral domains in fields

Lemma

In the construction of the field of fractions from R, we must verify:

- $\sim$ is a equivalence relation
- the $+$ and $\times$ operations are well-defined on $(R \times R^*)/\sim$
- the additive identity is $0/r$ for any $r \in R^*$
- the multiplictive identity is r/r for any $r \in R^*$
- $(a, b)^{-1} = b/a$.

Integral domain	**Field of fractions**
$\mathbb{Z}$ (integers)	$\mathbb{Q}$ (rationals)
$\mathbb{Z}[i]$ (Gaussian integers)	$\mathbb{Q}(i)$ (Gaussian rationals)
$F[x]$ (polynomials)	$F(x)$ (rational functions)

Every integral domain canonically embeds into its field of fractions, via $r \mapsto r/1$.

Moreover, this is the *minimal* field containing R.

Co-universal property of the field of fractions

Proposition

Let R be an integral domain with embedding $\iota\colon R \hookrightarrow F_R$ into its field of fractions. Then for every other embedding $f\colon R \hookrightarrow K$ into a field, there is a unique $h\colon F_R \hookrightarrow K$ such that $h \circ \iota = f$.

$$\begin{tikzcd} R \arrow[rr, hook, "f"] \arrow[dr, hook, "\iota"'] & & K \\ & F_R \arrow[ur, hook, dashed, "\exists! h"'] & \end{tikzcd} \qquad \begin{tikzcd} r \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & f(r) \\ & r/1 \arrow[ur, mapsto, dashed, "h"'] & \end{tikzcd}$$

Proof

Define the map

$$h\colon F_R \longrightarrow K, \qquad h(a/b) \longmapsto h(a/1)h(b/1)^{-1} = f(a)f(b)^{-1}.$$

We need to show that h is

(i) well-defined

(ii) a ring homomorphism,

(iii) injective

(iv) unique.

Co-universal property of the field of fractions

Proposition

Let R be an integral domain with embedding $\iota\colon R \hookrightarrow F_R$ into its field of fractions. Then for every other embedding $f\colon R \hookrightarrow K$ into a field, there is a unique $h\colon F_R \hookrightarrow K$ such that $h \circ \iota = f$.

$$\begin{tikzcd} R \arrow[rr, hook, "f"] \arrow[dr, hook, "\iota"'] & & K \\ & F_R \arrow[ur, hook, dashed, "\exists! h"'] & \end{tikzcd} \qquad \begin{tikzcd} r \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & f(r) \\ & r/1 \arrow[ur, mapsto, dashed, "h"'] & \end{tikzcd}$$

Proof

Define the map

$$h\colon F_R \longrightarrow K, \qquad h(a/b) \longmapsto h(a/1)h(b/1)^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}).$$

(i) Well-defined. Suppose $a/b = c/d \quad \Leftrightarrow \quad ad = bc \quad \Leftrightarrow \quad ab^{-1} = cd^{-1}$.

$$h(a/b) = f(a)f(b^{-1}) = f(ab^{-1}) = f(cd^{-1}) = f(c)f(d^{-1}) = h(c/d). \qquad \checkmark$$

Co-universal property of the field of fractions

Proposition

Let R be an integral domain with embedding $\iota\colon R \hookrightarrow F_R$ into its field of fractions. Then for every other embedding $f\colon R \hookrightarrow K$ into a field, there is a unique $h\colon F_R \hookrightarrow K$ such that $h \circ \iota = f$.

$$\begin{tikzcd}
R \arrow[rr, hook, "f"] \arrow[dr, hook, "\iota"'] & & K \\
& F_R \arrow[ur, hook, dashed, "\exists ! h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
r \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & f(r) \\
& r/1 \arrow[ur, mapsto, dashed, "h"'] &
\end{tikzcd}$$

Proof

Define the map

$$h\colon F_R \longrightarrow K, \qquad h(a/b) \longmapsto h(a/1)h(b/1)^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}).$$

(ii) Ring homomorphism. Suppose $a/b = c/d$. Then

$$\begin{aligned} h(a/b \cdot c/d) = h(ac/bd) &= f(ac)f(d^{-1}b^{-1}) = f(a)f(c)f(d^{-1})f(b^{-1}) \\ &= f(a)f(b^{-1}) \cdot f(c)f(d^{-1}) = h(a/b)h(c/d). \end{aligned} \qquad \checkmark$$

Verification of $h(a/b + c/d) = h(a/b) + h(c/d)$ is similar. (Exercise)

Co-universal property of the field of fractions

Proposition

Let R be an integral domain with embedding $\iota\colon R \hookrightarrow F_R$ into its field of fractions. Then for every other embedding $f\colon R \hookrightarrow K$ into a field, there is a unique $h\colon F_R \hookrightarrow K$ such that $h \circ \iota = f$.

$$\begin{tikzcd} R \arrow[rr, hook, "f"] \arrow[dr, hook, "\iota"'] & & K \\ & F_R \arrow[ur, hook, dashed, "\exists ! h"'] & \end{tikzcd} \qquad \begin{tikzcd} r \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & f(r) \\ & r/1 \arrow[ur, mapsto, dashed, "h"'] & \end{tikzcd}$$

Proof

Define the map

$$h\colon F_R \longrightarrow K, \qquad h(a/b) \longmapsto h(a/1)h(b/1)^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}).$$

(iii) Injective. It suffices to show that $\mathrm{Ker}(h) = \{0\}$. Suppose

$$0 = h(a/b) = f(a)f(b)^{-1} \in K.$$

However, $f(b)^{-1} \neq 0$ since f is an embedding and $b \neq 0$.

Thus $f(a) = 0$, so $a = 0$ in R. Thus $a/1 = 0/1$, the zero element in F_R. ✓

Co-universal property of the field of fractions

Proposition

Let R be an integral domain with embedding $\iota\colon R \hookrightarrow F_R$ into its field of fractions. Then for every other embedding $f\colon R \hookrightarrow K$ into a field, there is a unique $h\colon F_R \hookrightarrow K$ such that $h \circ \iota = f$.

$$\begin{tikzcd} R \arrow[rr, hook, "f"] \arrow[dr, hook, "\iota"'] & & K \\ & F_R \arrow[ur, hook, dashed, "\exists! h"'] & \end{tikzcd} \qquad \begin{tikzcd} r \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & f(r) \\ & r/1 \arrow[ur, mapsto, dashed, "h"'] & \end{tikzcd}$$

Proof

Define the map

$$h\colon F_R \longrightarrow K, \qquad h(a/b) \longmapsto h(a/1)h(b/1)^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}).$$

(iv) Uniqueness. Suppose there is another $g\colon F_R \to K$ such that $f = g \circ \iota$. Then

$$g(a/b) = g((a/1)\cdot(b/1)^{-1}) = g(a/1)g(b/1)^{-1} = g(\iota(a))g(\iota(b))^{-1} = f(a)f(b)^{-1} = h(a/b),$$

which completes the proof. □

Rings of fractions and localization

The co-universal property can be used as the *definition* of the field of fractions, allowing:

- the generalization to rings without 1, e.g., $R = 2\mathbb{Z}$. (Exercise: show that $F_{2\mathbb{Z}} = \mathbb{Q}$.)
- the generalization to constructing fractions of certain subsets.

Let R be commutative, $D \subseteq R$ nonempty and multiplicatively closed with no zero divisors.

We can carry out the same construction of the set

$$R \times D = \big\{(r,d) \mid r \in R,\ d \in D\big\}, \qquad (r_1,d_1) \sim (r_2,d_2) \ \text{ iff } \ r_1 d_2 = r_2 d_1.$$

The resulting ring is the localization of R at D, denoted $D^{-1}R$.

Proposition (HW)

Let R be a commutative ring with embedding $\iota\colon R \hookrightarrow D^{-1}R$. Then for every other embedding $f\colon R \hookrightarrow S$ to a ring where $f(D)$ are units, there is a unique $h\colon D^{-1}R \hookrightarrow S$ such that $h \circ \iota = f$.

$$\begin{tikzcd}
R \arrow[rr, hook, "f"] \arrow[dr, hook, "\iota"'] & & S \\
& D^{-1}R \arrow[ur, hook, dashed, "\exists! h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
r \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & f(r) \\
& r/1 \arrow[ur, mapsto, dashed, "h"'] &
\end{tikzcd}$$

Localization with zero divisors

We can generalize this further! Allow D to contain zero divisors.

The mapping $R \to D^{-1}R$ sending r to its equivalence class is no longer injective:

$$\iota\colon R \longrightarrow D^{-1}R, \qquad \iota(z) = 0, \quad \text{for all zero divisors } z \in D.$$

We still have a co-universal property, that could have been the definition.

Proposition (exercise)

Let R be a commutative ring with $\iota\colon R \to D^{-1}R$. For every other $f\colon R \to S$ to a ring where the non zero-divisors in $f(D)$ are units, there is a unique $h\colon D^{-1}R \to S$ such that $h \circ \iota = f$.

$$\begin{tikzcd}
R \arrow[rr, "f"] \arrow[dr, "\iota"'] & & S \\
& D^{-1}R \arrow[ur, dashed, "\exists! h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
r \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & f(r) \\
& r/1 \arrow[ur, mapsto, dashed, "h"'] &
\end{tikzcd}$$

Thus, $D^{-1}R$ is the "smallest ring" where all non zero-divisors in D are invertible.

Examples of rings of fractions

1. If R is an integral domain and $D = R^*$, then $D^{-1}R$ is its field of fractions.
2. If D is the set of non zero divisors, then $D^{-1}R$ is the total ring of fractions of R.
3. If non-unit of R is a zero divisor, then R is equal to its total ring of fractions.

   Examples include $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

   In these rings, every prime ideal is maximal (exercise).
4. The localization of $R = F[x]$ at $D = \{x^n \mid n \in \mathbb{Z}\}$ are the Laurent polynomials:
$$D^{-1}R = F[x, x^{-1}] = \left\{a_{-m}x^{-m} + \cdots + a_{-1}x^{-1} + a_0 + a_1x + \cdots + a_nx^n \mid a_i \in F\right\}.$$
5. If $R = \mathbb{Z}$ and $D = \left\{5^n \mid n \in \mathbb{N}\right\}$, then
$$D^{-1}R = \mathbb{Z}[\tfrac{1}{5}] = \left\{a_0 + \frac{a_1}{5} + \frac{a_2}{5^2} + \cdots + \frac{a_n}{5^n} \mid a_i \in \mathbb{Z}\right\}.$$
   which are "*polynomials in* $\frac{1}{5}$" over $\mathbb{Z}$.
6. If $D = R - P$ for a prime ideal, then $R_P := D^{-1}R$ is the localization of R at P. It is a local ring – it has a unique maximal ideal, PR_P.