Chapter 7: Rings

Matthew Macauley

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

Math 8510, Abstract 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

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

A familar example

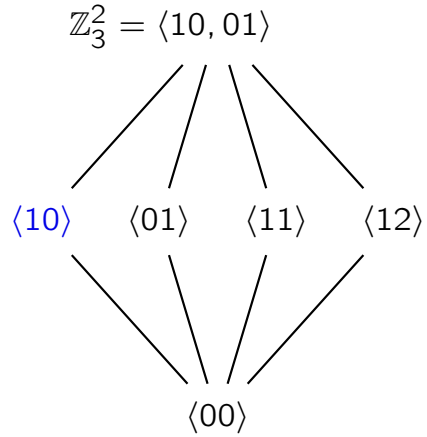
Consider the ring $R = \mathbb{Z}_3^2 = \{ab \mid a, b \in \mathbb{Z}_3\}$.

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?



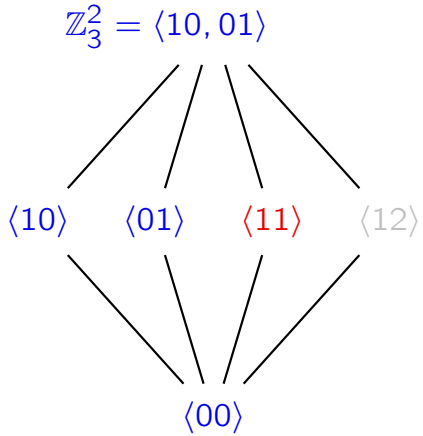
+	00	10	20	01	11	21	02	12	22
00	00	10	20	01	11	21	02	12	22
10	10	20	00	11	21	01	12	22	02
20	20	00	10	21	01	11	22	02	12
01	01	11	21	02	12	22	00	10	20
11	11	21	01	12	22	02	10	20	00
21	21	01	11	22	02	12	20	00	10
02	02	12	22	00	10	20	01	11	21
12	12	22	02	10	20	00	11	21	01
22	22	02	12	20	00	10	21	01	11

×	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

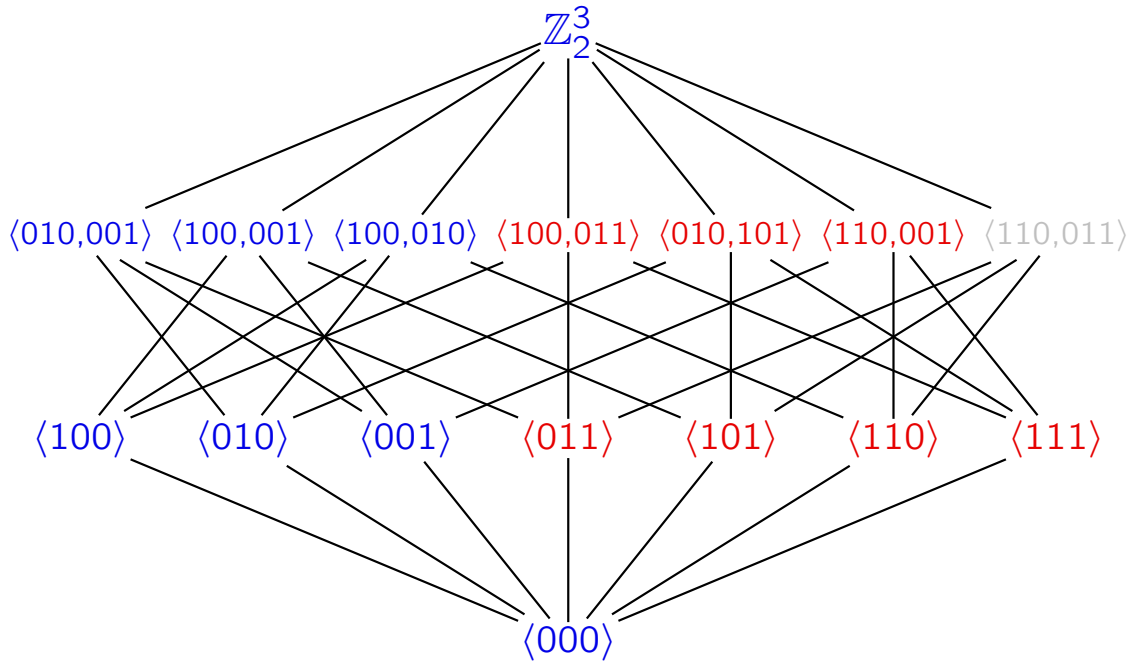
Subring lattices

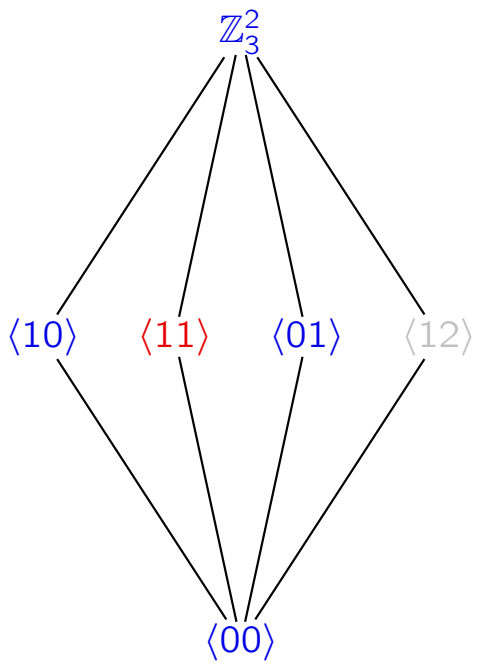
Like we did with groups, we can create the **subring lattice** of a (finite) ring.

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:

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

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:

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

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

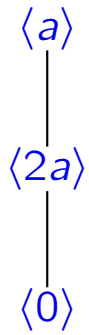
How different would these ideals be in the ring $R = \mathbb{Q}[x]$?

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	$2a$



$\{0,1,2,3\} = \mathbb{Z}_4$

$\langle a \mid 4a = 0,\ a^2 = a \rangle$

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

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

$\{0,2,4,6\} = 2\mathbb{Z}_4 \subseteq \mathbb{Z}_8$

$\langle a \mid 4a = 0,\ a^2 = 2a \rangle$

$\times$	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

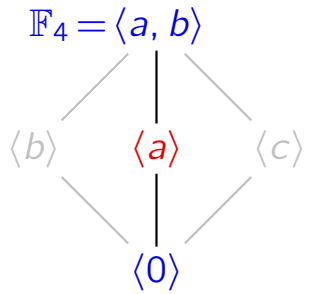
$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix} \right\} \subseteq M_2(\mathbb{Z}_4)$$

Some rings of order 4

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

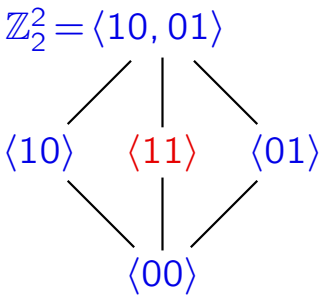
Three have unity: $\mathbb{F}_4$, $\mathbb{Z}_2^2$, and $\langle I, \mathbf{1} \rangle$.

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



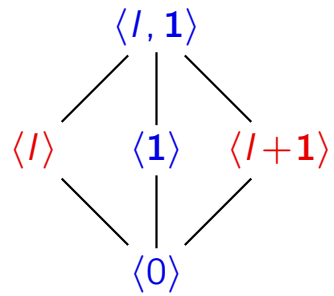
$\times$	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	b	c	a
c	0	c	a	b

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



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

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



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

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

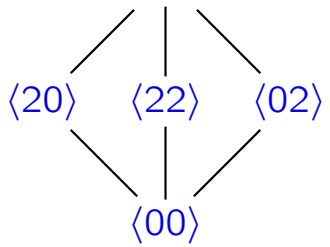
Some rings of order 4

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

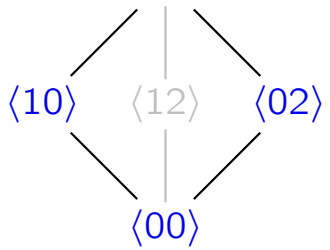
$2\mathbb{Z}_2^2 = \langle 20, 02 \rangle$



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

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

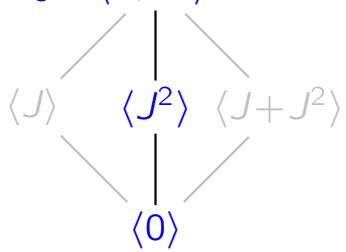
$\mathbb{Z}_2 \times 2\mathbb{Z}_2 = \langle 10, 02 \rangle$



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

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

$R_J = \langle J, J^2 \rangle$



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

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

Some rings of order 4

There are two noncommutative rings of order 4.

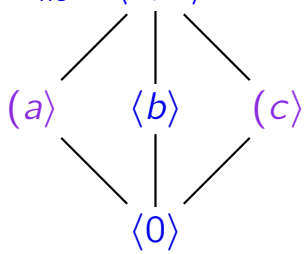
Each is the "opposite ring" of the other.

+	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.

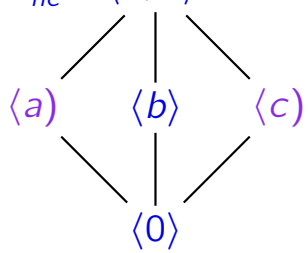
$R_{nc} = \langle a, b\rangle$



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

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

$R_{nc}^T = \langle a, b\rangle$



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

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

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, the only fintie 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 $F = \{f : R \to R\}$ 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:

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

- subrings that are not ideals:

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

- ideals:

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

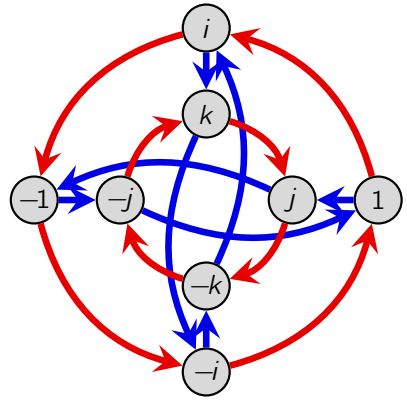
$$(x) = \{xf(x) \mid f \in \mathbb{Z}[x]\} = \{a_n x^n + \cdots + a_1 x \mid a_i \in \mathbb{Z}\},$$

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

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.

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 $I = R$. □

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

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

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 $x - y = 0$. □

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 $a, a^2, a^3, a^4, \ldots$, 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: $\mathsf{Ker}(\phi) \trianglelefteq G$.
- 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: $\mathsf{Ker}(\phi) \trianglelefteq R$.
- 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 $f : R \to S$ 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 $f : R \to S$ is the set $\mathsf{Ker}(f) := \{x \in R \mid f(x) = 0\}$.

Examples

1. The ring homomorphism $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ sending $k \mapsto k \pmod{n}$ has $\mathsf{Ker}(\phi) = n\mathbb{Z}$.
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 $\mathsf{Ker}(\phi)$ is an additive subgroup of R. We must show that it's an ideal.

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

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

Showing that $\mathsf{Ker}(\phi)$ 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)

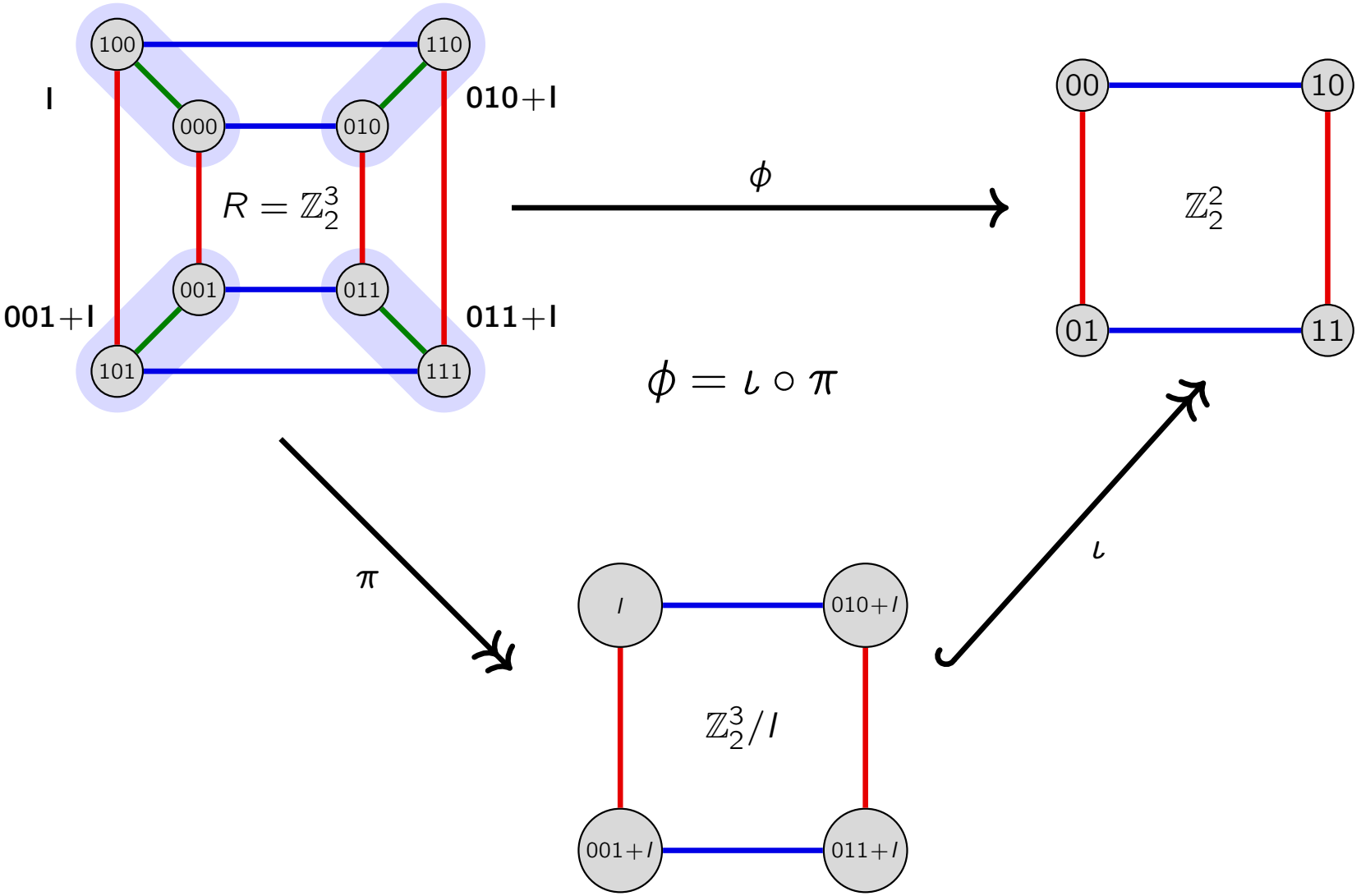
The statement holds for the underlying additive group R. Thus, it remains to show that the relabeling map (a group isomorphism)

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

is also a ring homomorphism:

The FHT for rings

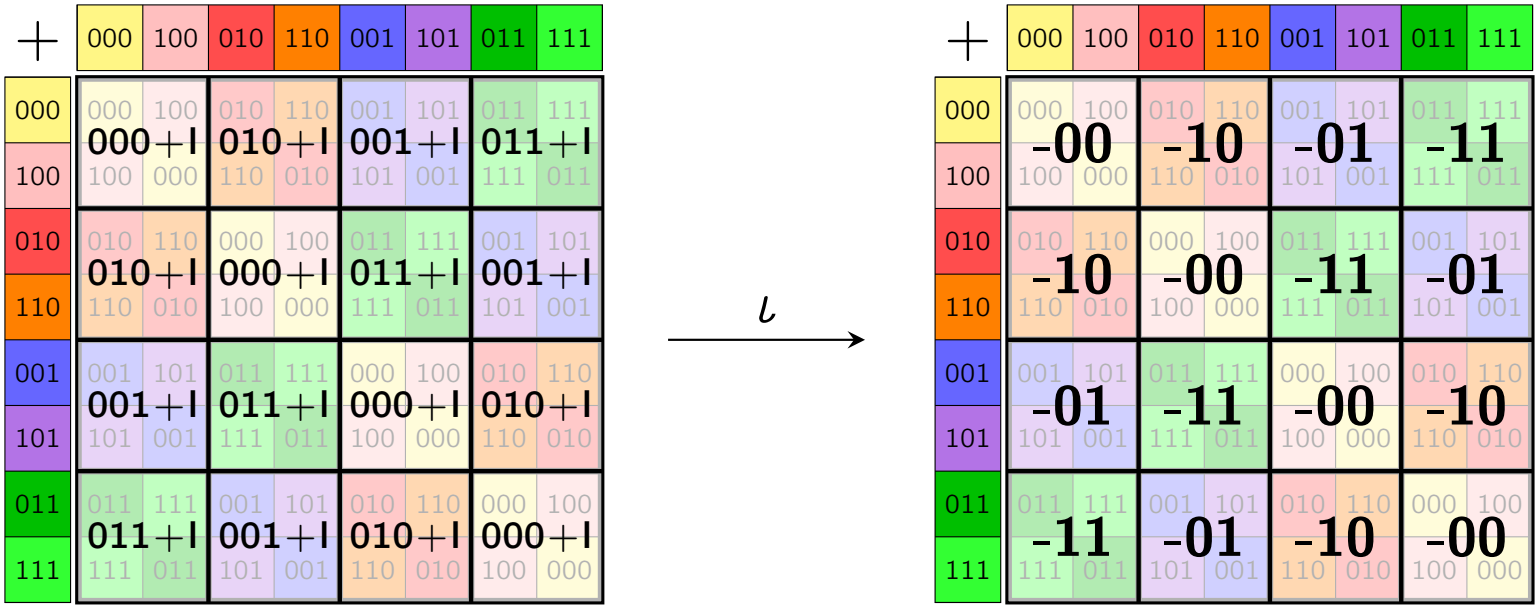
Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2$, $\phi\colon abc \longmapsto bc$.



The FHT for rings

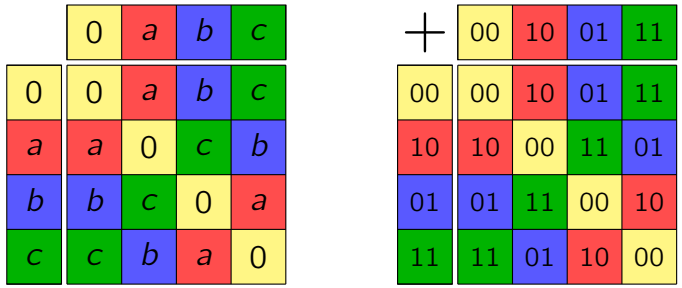
Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2$, $\qquad \phi\colon abc \longmapsto bc$.

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



The image is isomorphic to the Klein 4-group

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



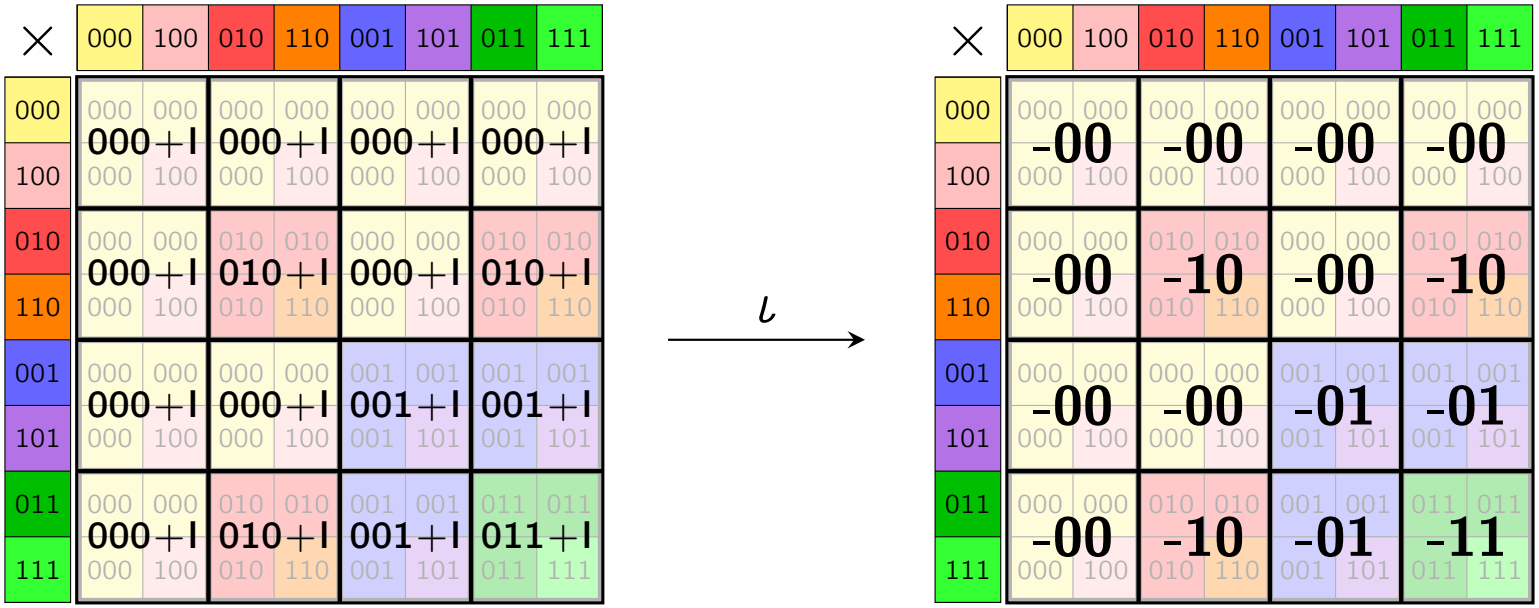
The FHT theorem for rings says that ι also preserves the multiplicative structure of R/I.

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:

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



This quotient ring is isomorphic to

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

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

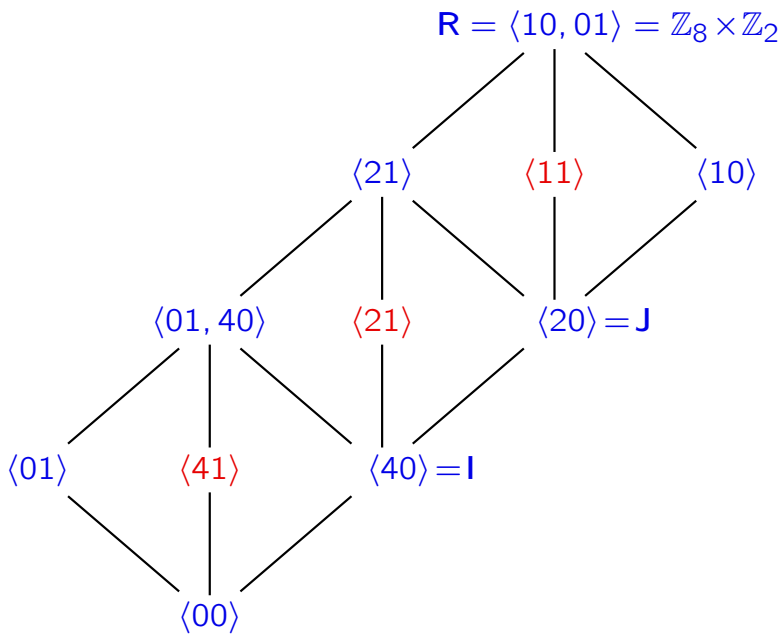
×	00	10	01	11
00	00	00	00	00
10	00	10	00	10
01	00	00	01	01
11	00	10	01	11

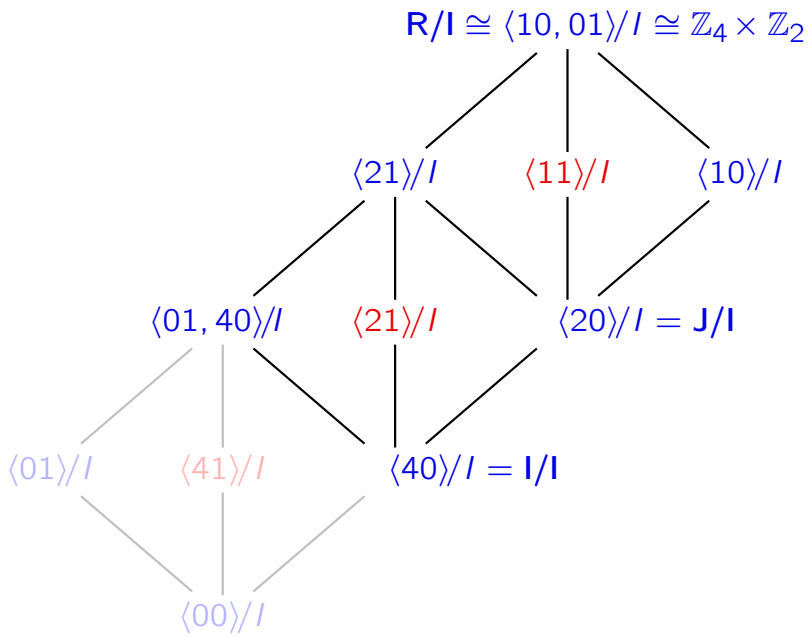
The correspondence theorem: subrings of quotients

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 $I \subseteq J \subseteq R$.



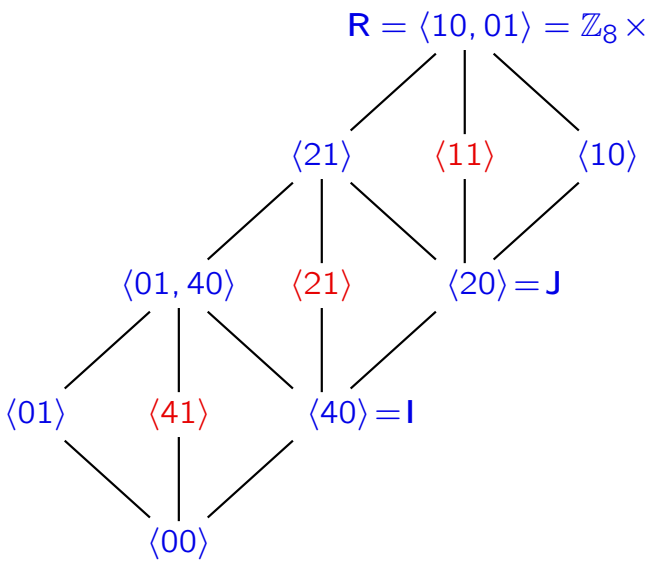


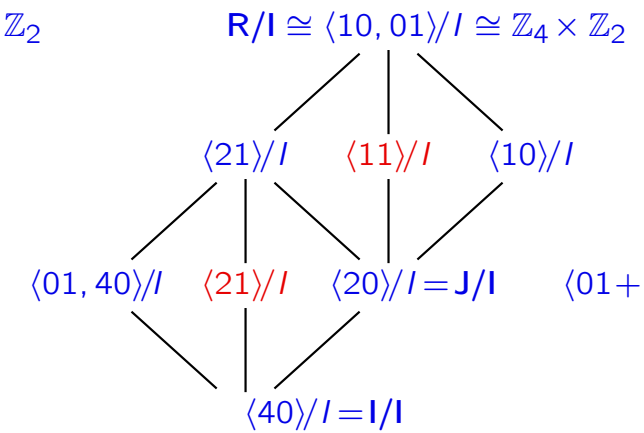
Big idea

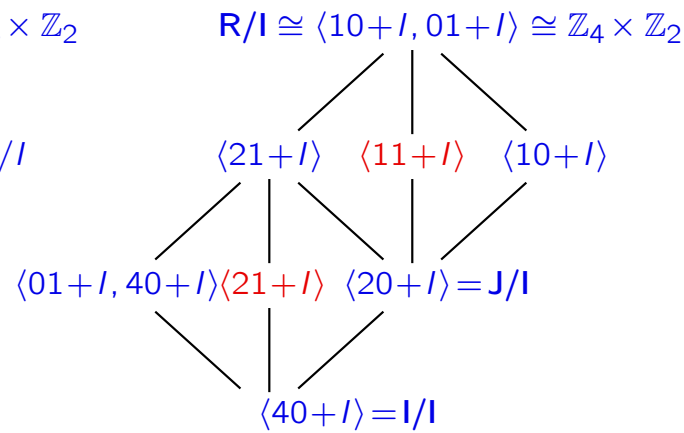
This is just like the correspondence theorem for groups, but it also "preserves colors."

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)

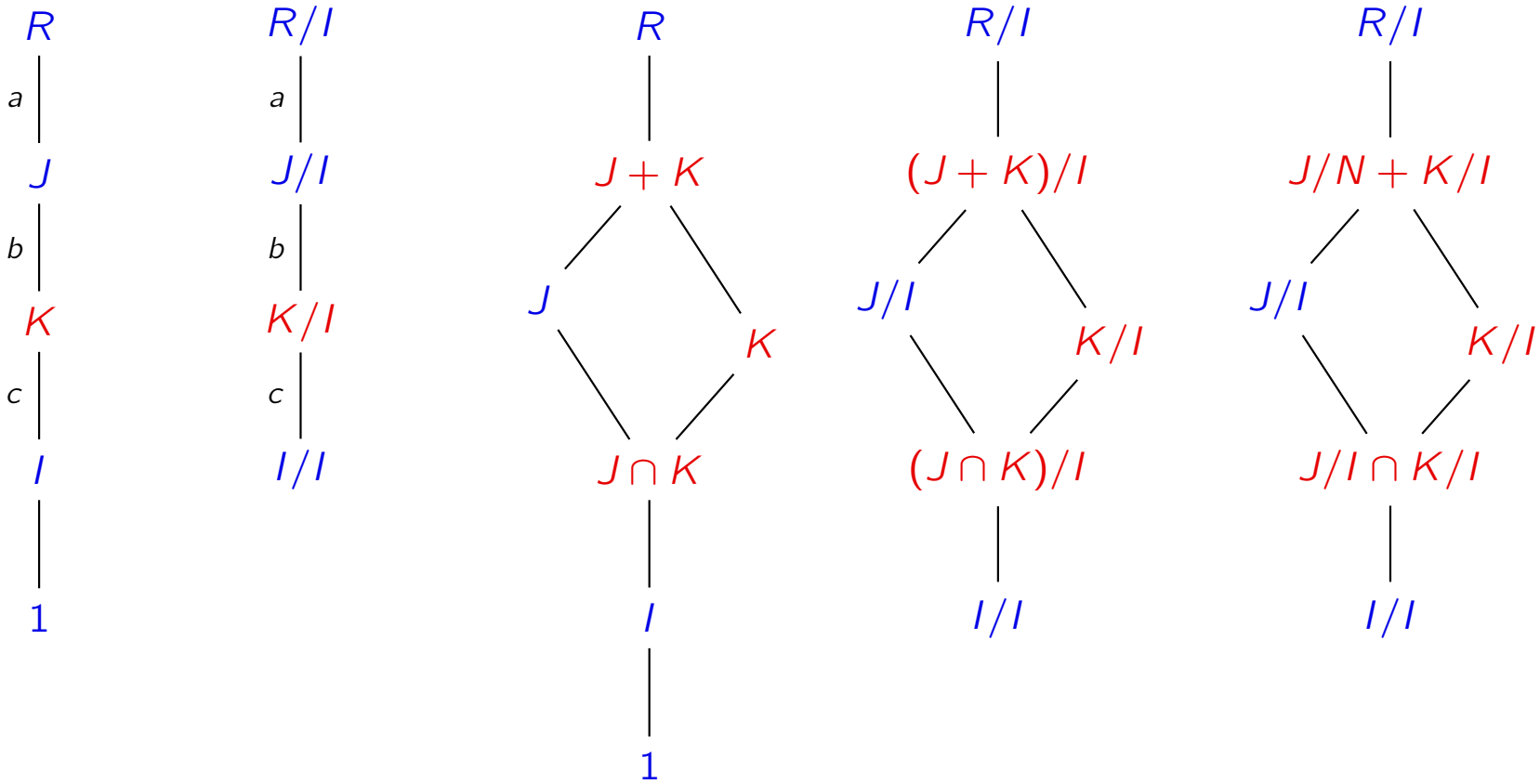
Let $I \leq J \leq R$ and $I \leq K \leq R$ be chains of subrings and $I \trianglelefteq G$. Then

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 $I \leq J \leq R$.

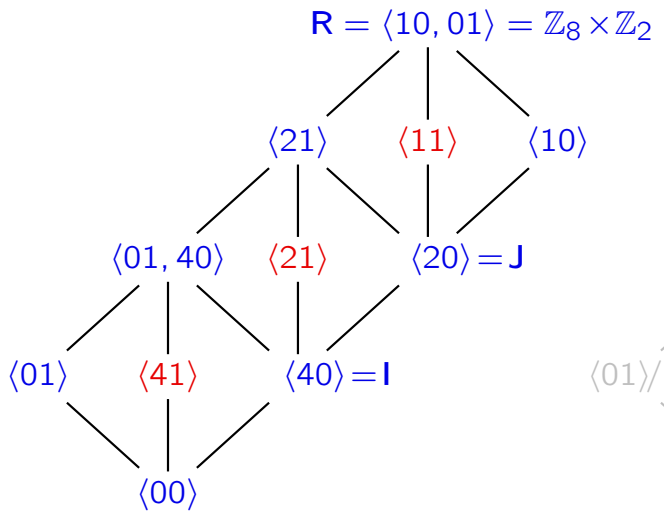
Moreover, if $J \trianglelefteq R$ is an ideal, then $J/I \trianglelefteq R/I$. In this case, we can ask:

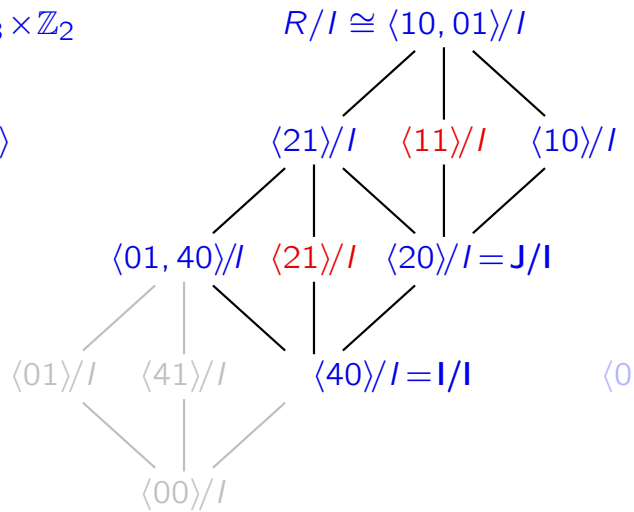
"*What is the quotient ring* $(R/I)/(J/I)$ *isomorphic to?*"

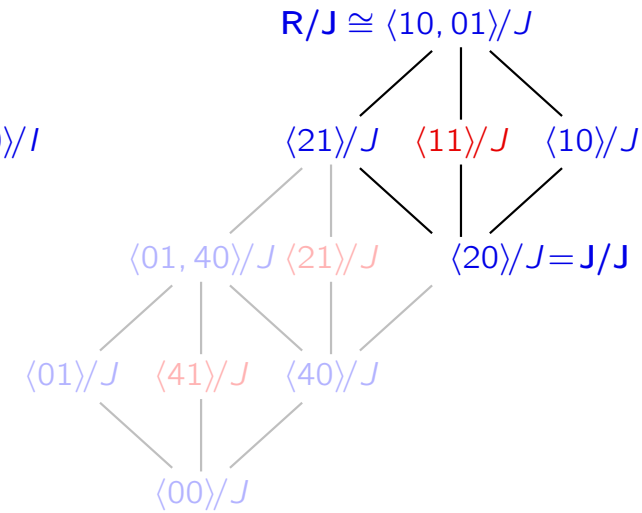
Fraction theorem

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

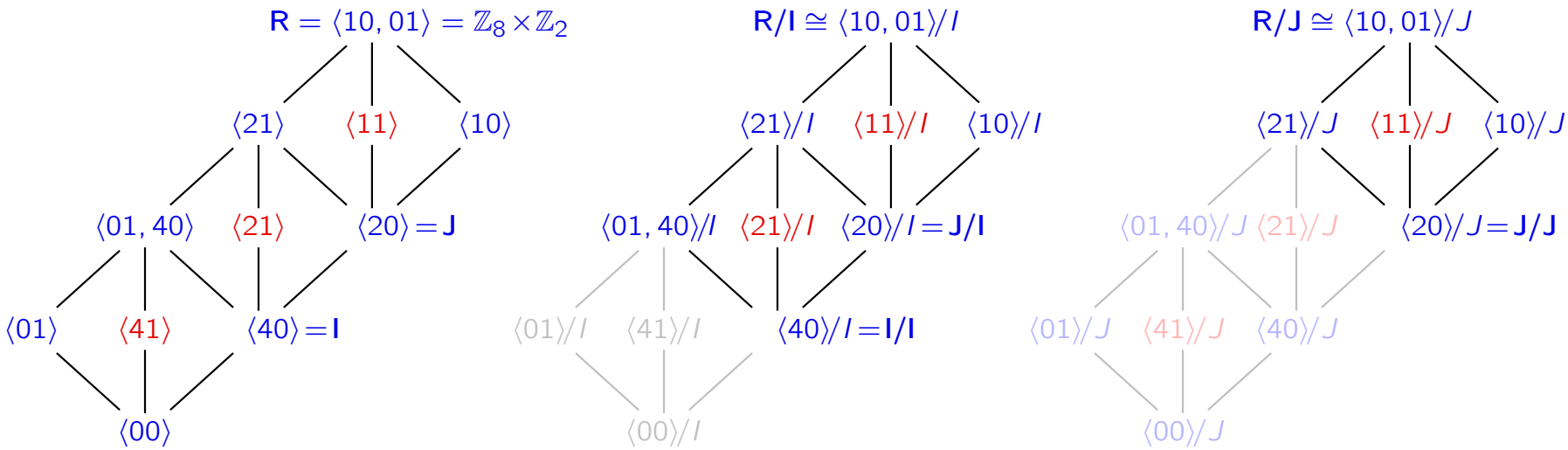
$$(R/I)/(J/I) \cong R/J.$$

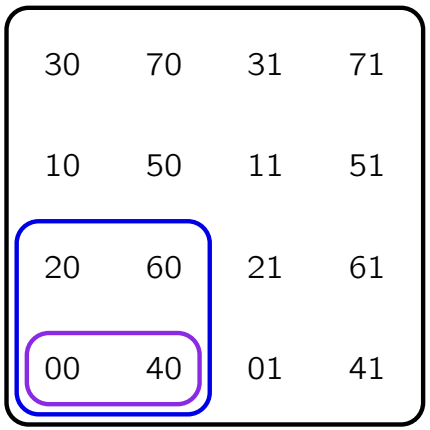




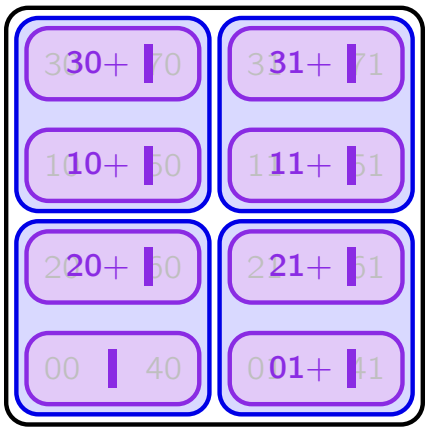


The fraction theorem: quotients of quotients

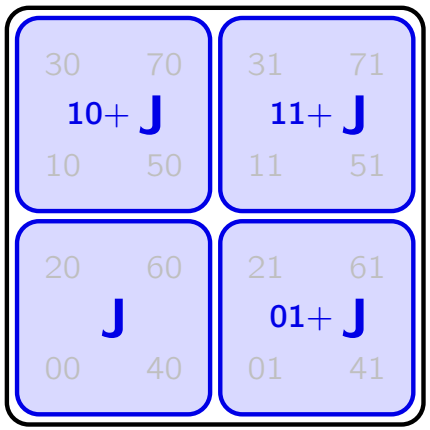




$I \leq J \leq R$



R/I consists of 8 cosets



R/J consists of 4 cosets

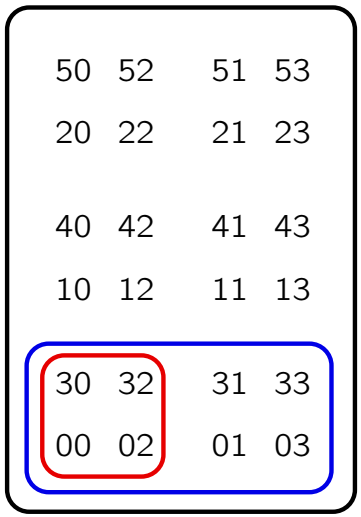
The fraction theorem: quotients of quotients

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

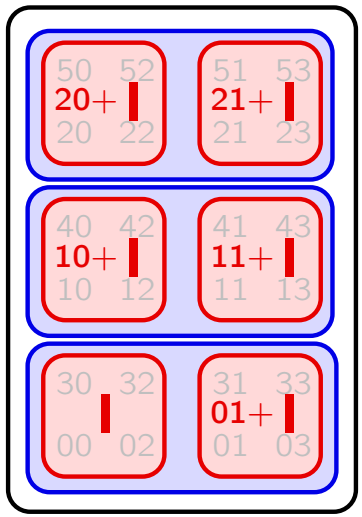
Consider the ideals $J = \langle 30, 02 \rangle \cong \mathbb{Z}_2^2$ and $I = \langle 30, 01 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

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

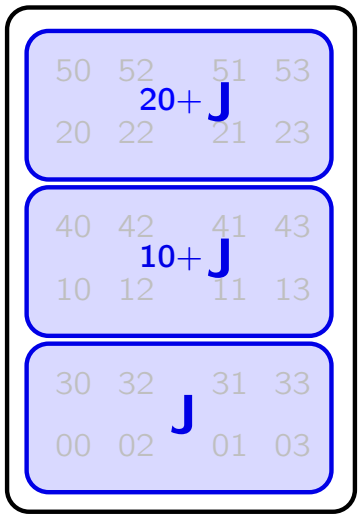
$$R/I = \{I,\ 01+I,\ 10+I,\ 11+I,\ 20+I,\ 21+I\}, \qquad J/I = \{I,\ 01+I\}$$
$$R/J = \{I \cup (01+I),\ (10+I) \cup (11+I),\ (20+I) \cup (21+I)\}$$
$$(R/I)/(J/I) = \{\{I,\ 01+I\},\ \{10+I,\ 11+I\},\ \{20+I,\ 21+I\}\}.$$



$I \leq J \leq R$



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

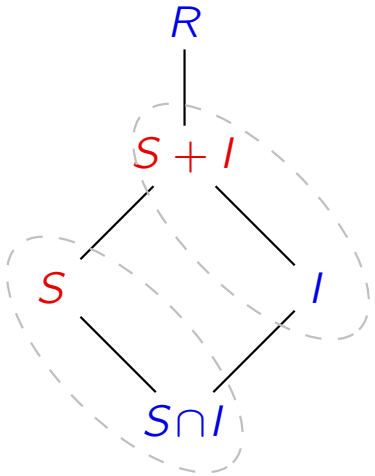
Diamond theorem

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

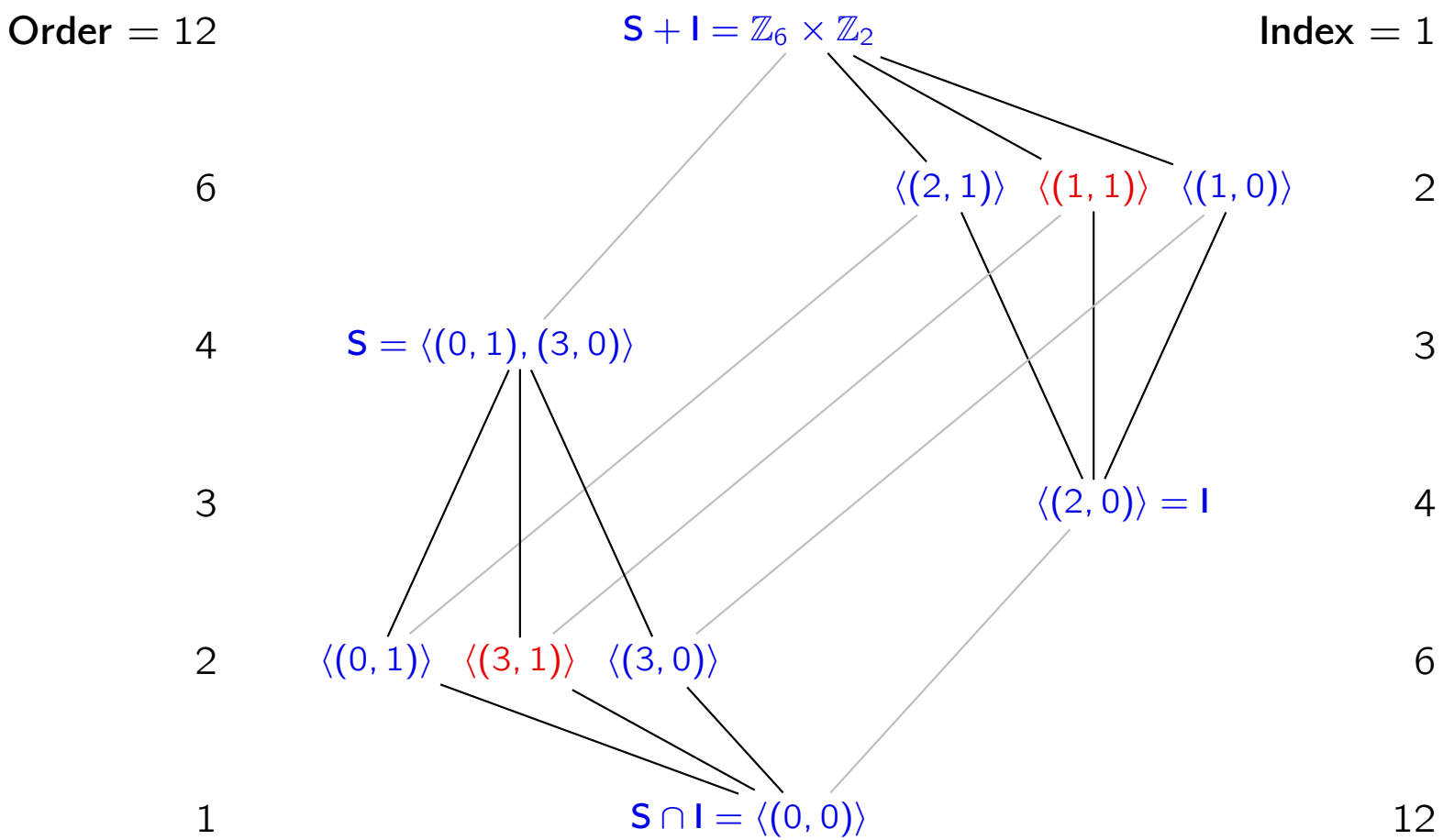
$$\phi\colon S \longrightarrow (S + I)/I, \qquad \phi\colon s \longmapsto s + I.$$

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

The diamond theorem: quotients of sums by factors

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

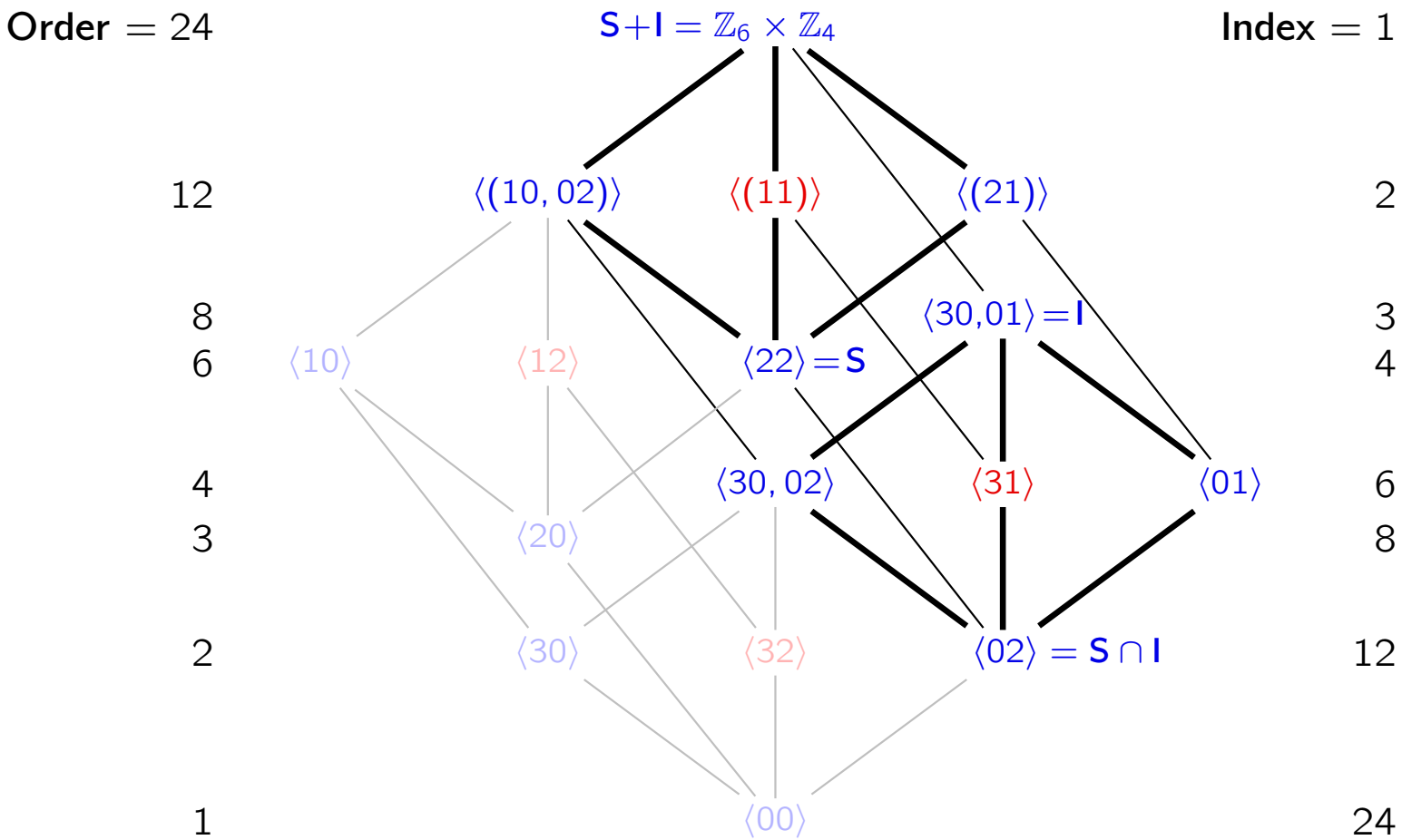
For rings, it also "preserves the colors" – subgroup, subring, and ideal structure.



The diamond theorem: quotients of sums by factors

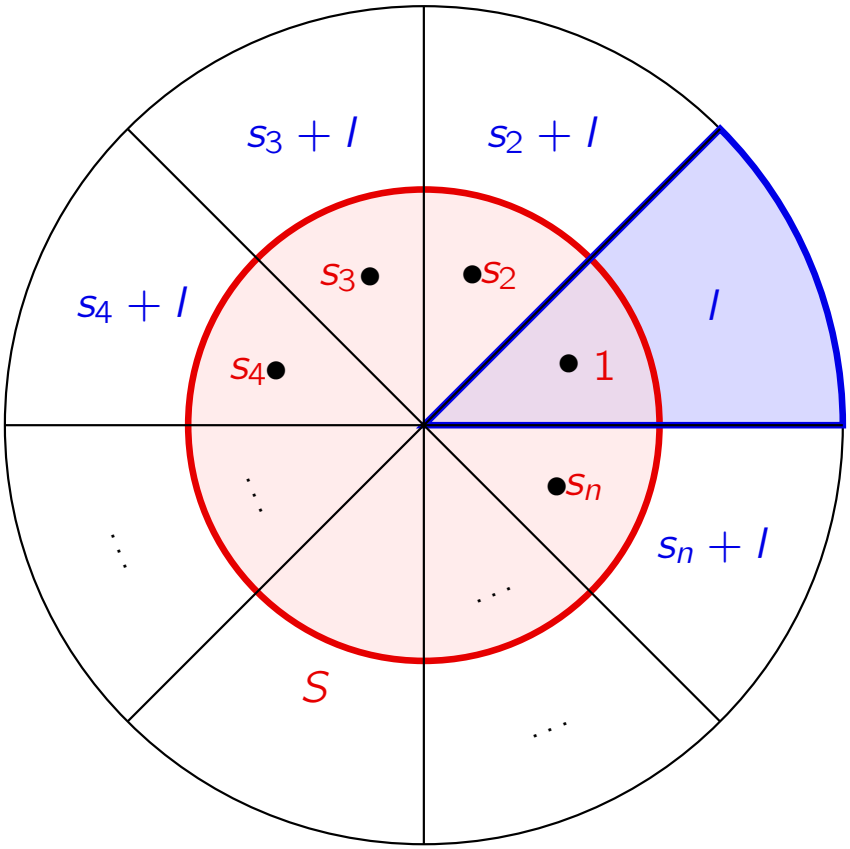
Like for groups, the diamond theorem guarantees an inherent "duality" in subring lattices.

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

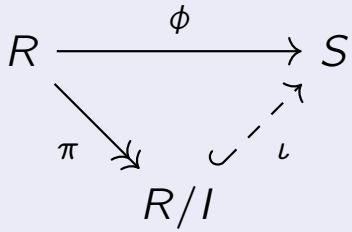
$(S + I)/I = \{\text{large pizza slices}\}$

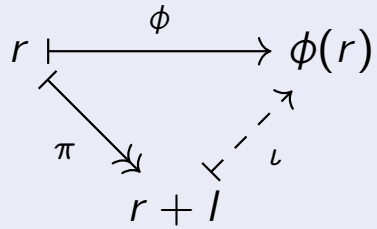
$S/(S \cap I) = \{\text{small pizza slices}\}$

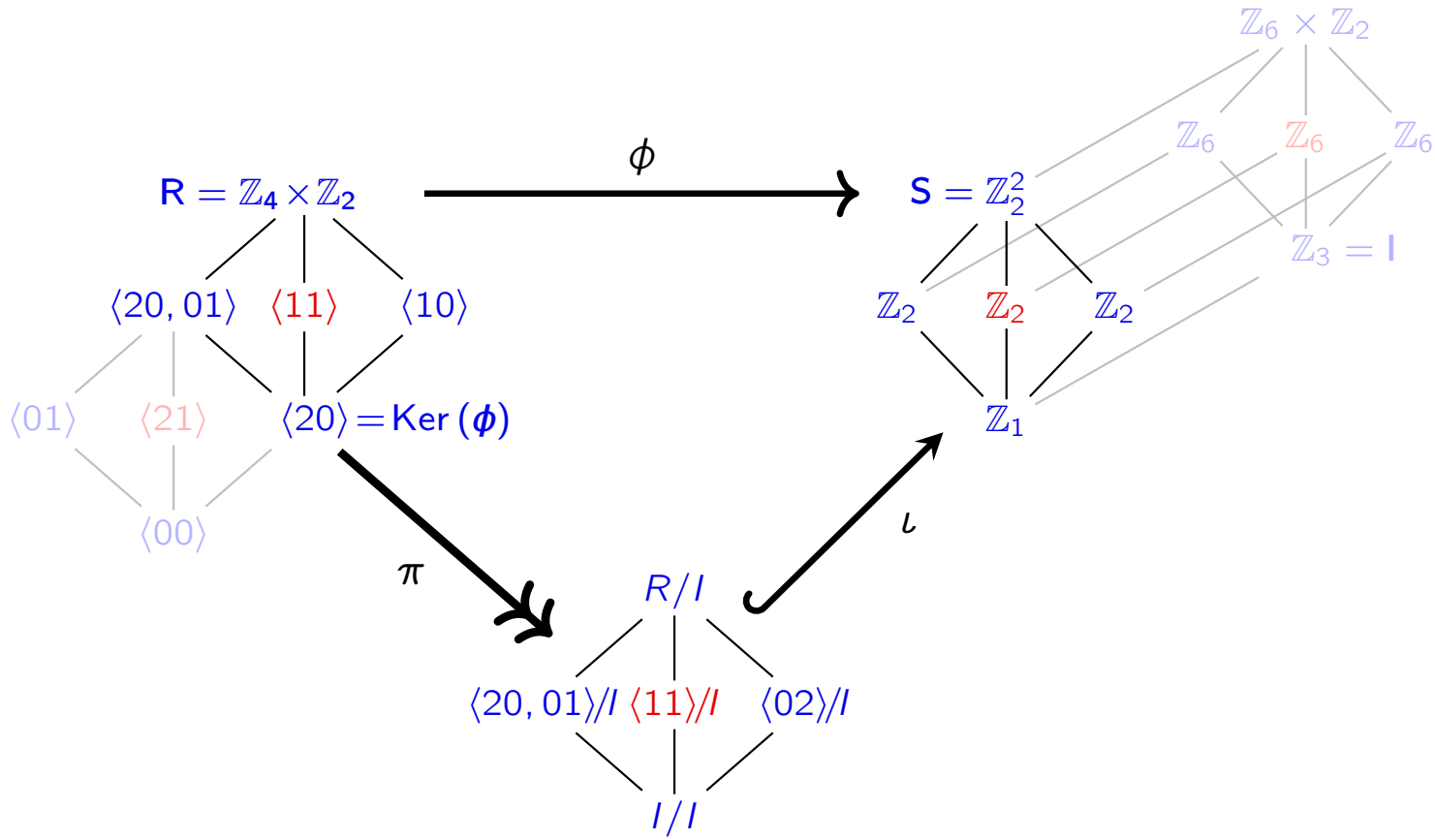
Diamond theorem: $(S + I)/I \cong S/(S \cap I)$

Theorem (exercise)

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







Maximal ideals and simple rings

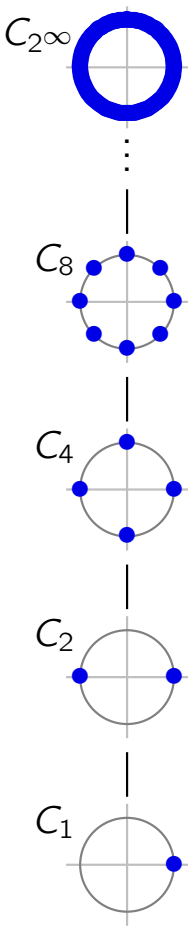
A maximal normal subgroup M of G has no normal subgroups $M \lneq N \lneq G$. Formally:

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

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 $I \lneq R$ 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. The maximal ideals of $R = \mathbb{Z}[x]$ are of the form

$$(x, p) = \{xf(x) + p \cdot g(x) \mid f, g \in \mathbb{Z}[x]\} = \{a_n x^n + \cdots + a_1 x + pa_0 \mid a_i \in \mathbb{Z}\}.$$

   In the quotient field, "$x := 0$" and "$p := 0$", and so

$$\mathbb{Z}[x]/(x, p) = \{a_0 + M \mid a_0 = 0, \ldots, p-1\} \cong \mathbb{Z}_p.$$

3. Let $R = \mathbb{Q}[x]$. The ideal

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

   is maximal. In the quotient field, "$x := 0$", and so

$$\mathbb{Q}[x]/(x) = \{a_0 + M \mid a_0 \in \mathbb{Q}\} \cong \mathbb{Q}.$$

4. In the multivariate ring $R = \mathbb{F}[x, y]$ over a field, the ideal

$$I = (x, y) = \{x \cdot f(x, y) + y \cdot g(x, y) \mid f, g \in R\}$$

   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

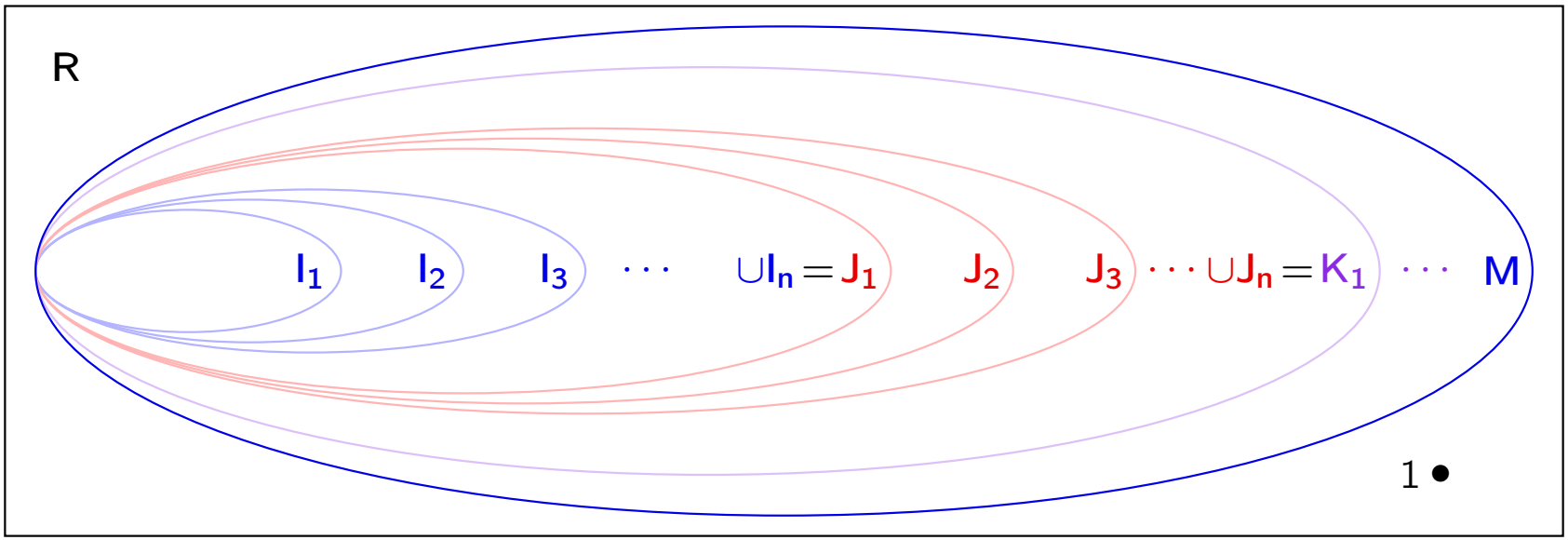
Given an ideal $I_1 \subsetneq R$. Let's try to find a maximal ideal that contains it.

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

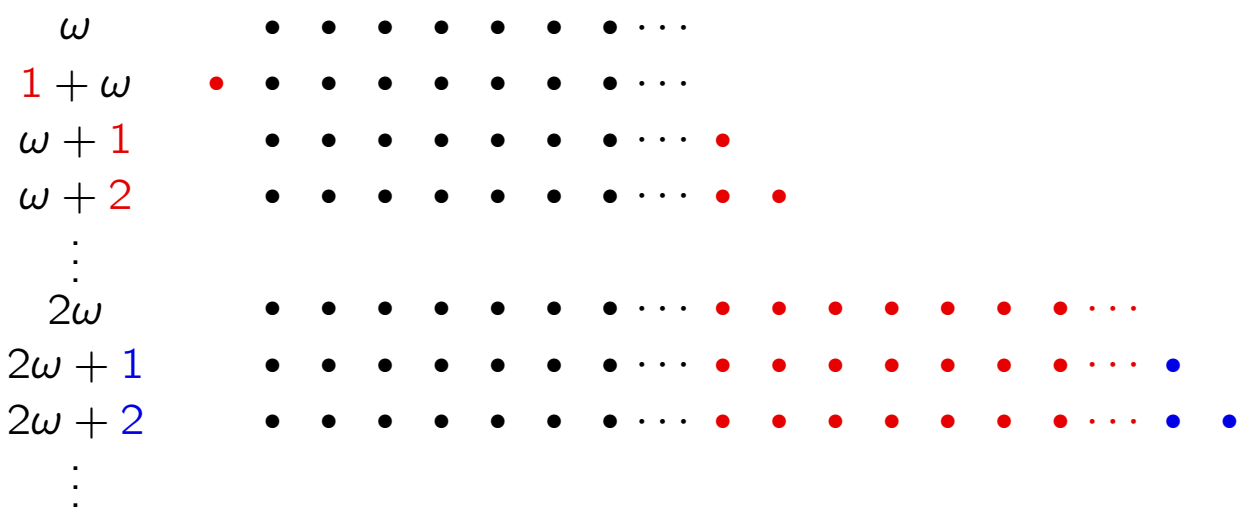
A set is well-ordered if every subset has a minimal element.

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 $\omega = 1 + \omega \neq \omega + 1$.

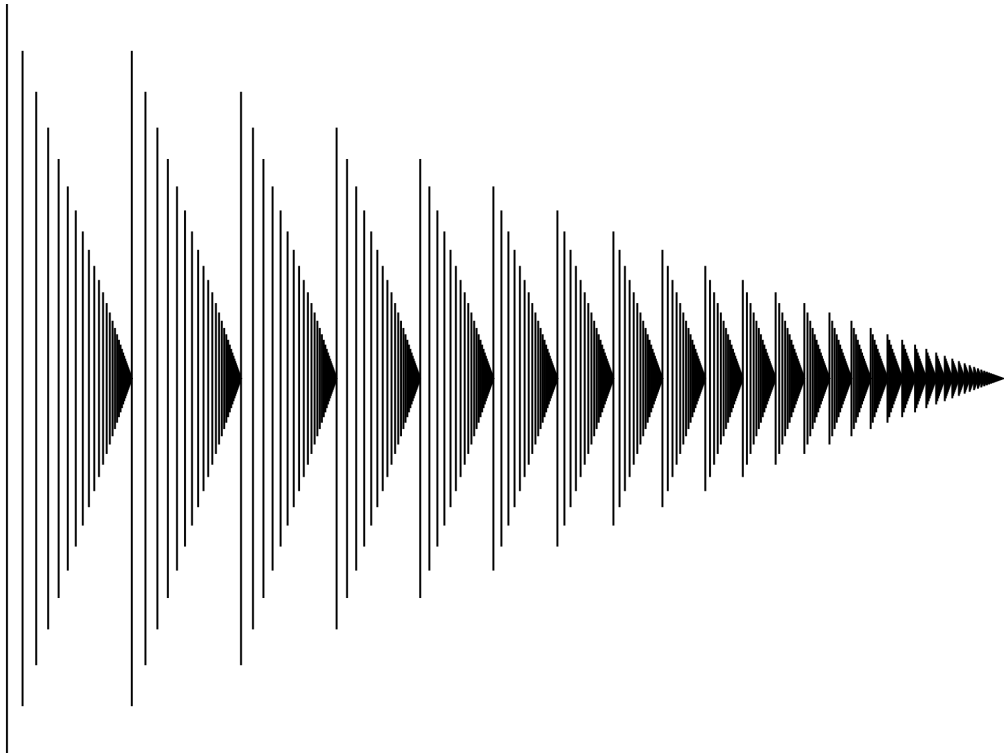


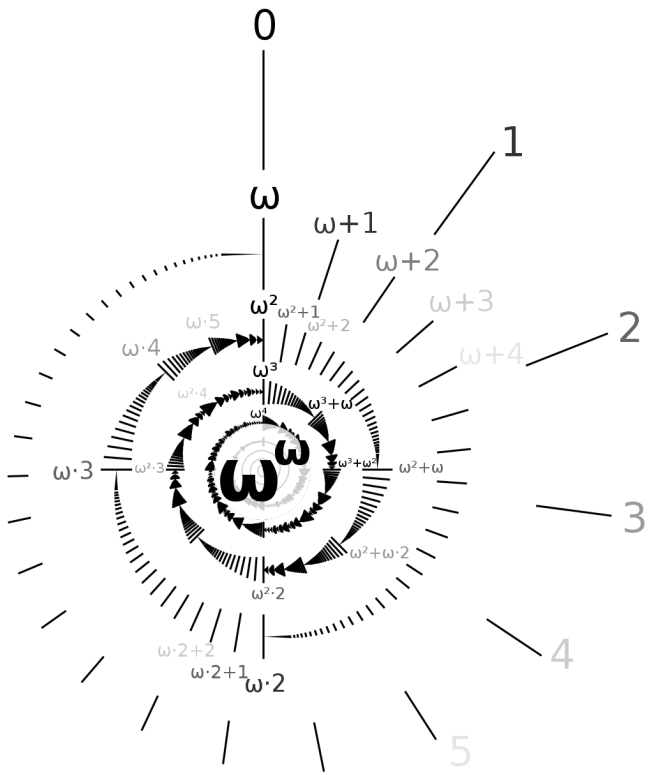
There are three types:

- 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 $I \subsetneq R$ 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:

- $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ 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:

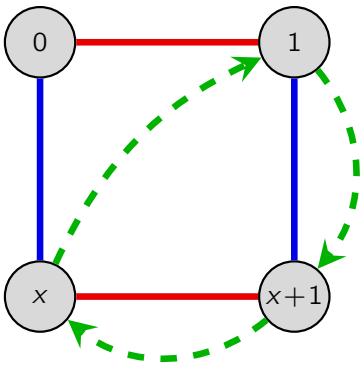
$$0 + I\,, \qquad 1 + I\,, \qquad x + I\,, \qquad (x+1) + I.$$

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

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

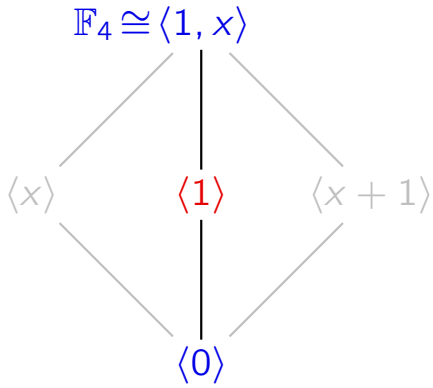
Finite fields

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

×	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

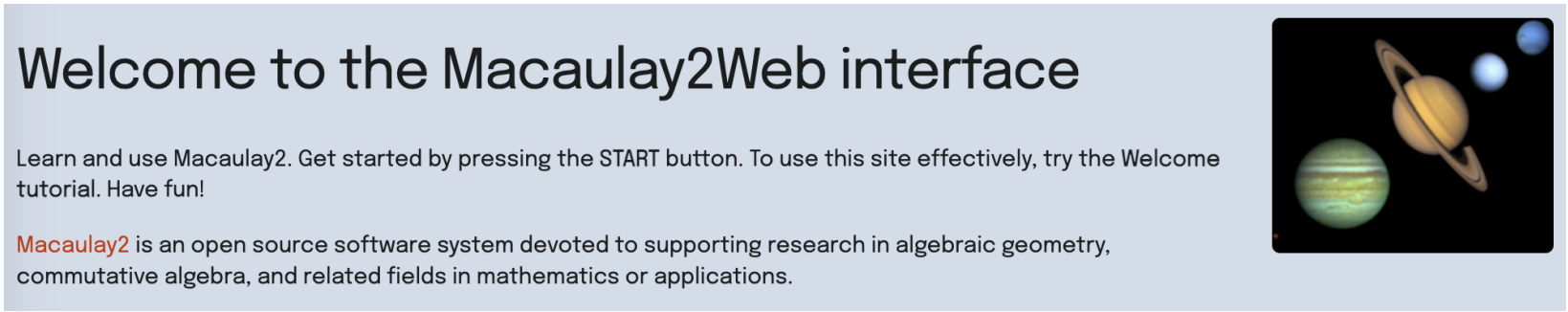
$$\mathbb{F}_p[x]/(f),$$

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

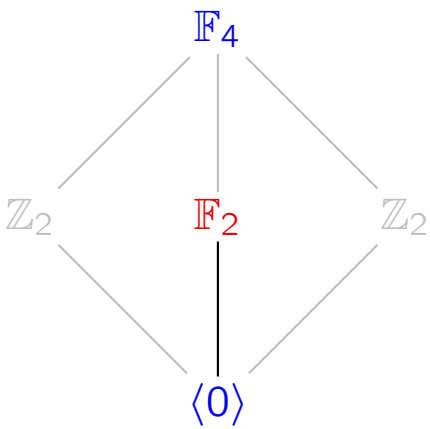
$\times$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	x^2+x+1	x^2+1	x	1	x^2+x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

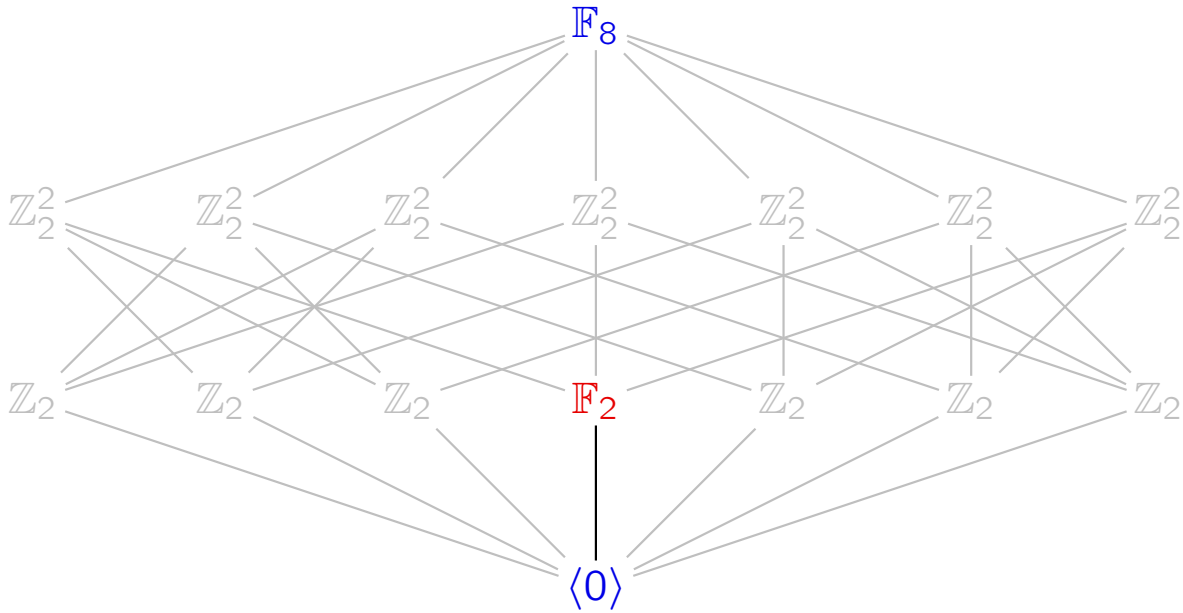
Notice how $\mathbb{F}_2 = \{0, 1\}$ arises is a subfield, but not $\mathbb{F}_4$. (*Why?*)

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.

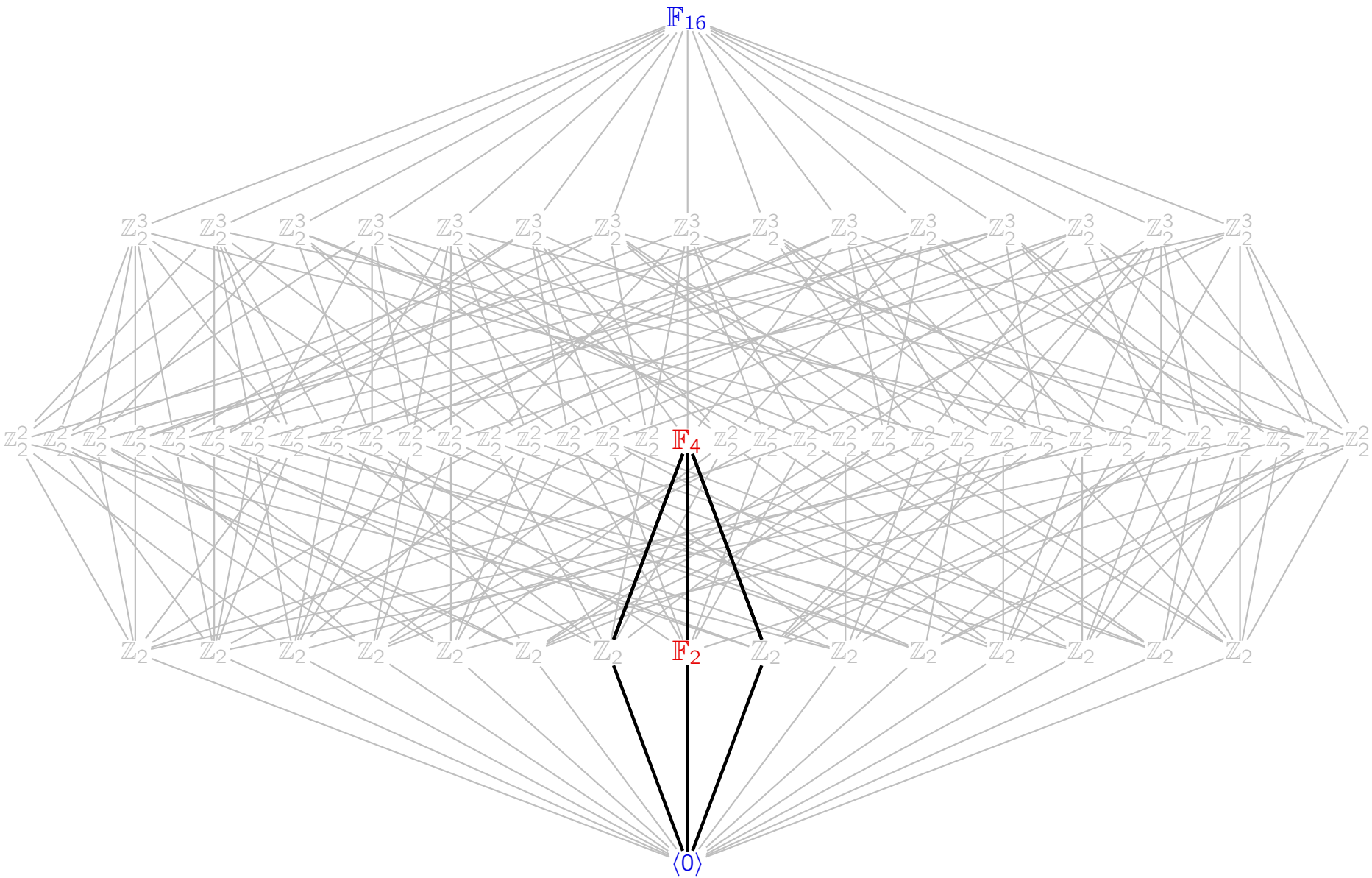




Similarly, $\mathbb{F}_{16}$ has 35 $\mathbb{Z}_2^2$-subgroups, but $\mathbb{F}_{16}^\times \cong C_{15}$ has only two elements of order 3.

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

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

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 $x_1, \ldots, x_k$, 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. □

Prime ideals

Proposition

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

Proof

Consider the canonical quotient

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

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",

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

□

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.

The nilradical of R

Recall that $a \in R$ is nilpotent if $a^n = 0$ for some $n \geq 1$.

Definition

The nilradical of R is the set of nilpotent elements

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

Proposition

$\mathfrak{N}(R)$ is an ideal of R.

Proof

Subgroup: Suppose $x, y \in \mathfrak{N}(R)$, 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 $rx \in \mathfrak{N}(R)$. ✓

The radical of an ideal

Definition

The radical of an ideal I is the set

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

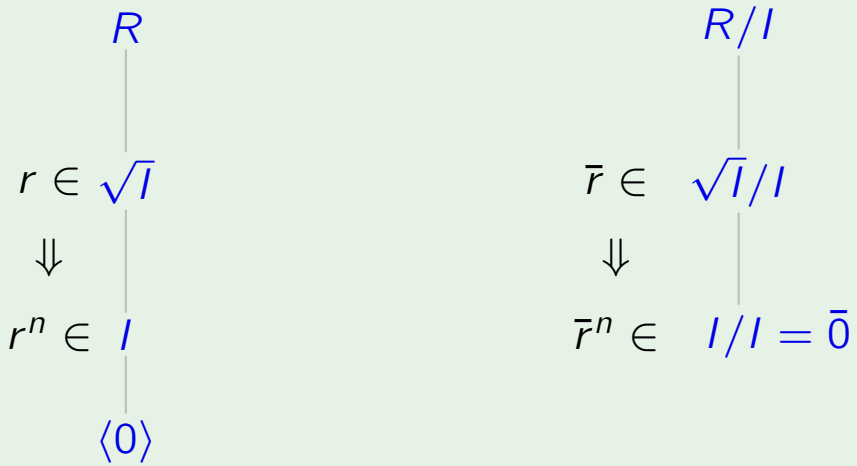
If $\sqrt{I} = I$, then I is a radical ideal.

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

Proposition

$\mathfrak{N}(R/I) = \sqrt{I}/I$.

Proof (sketch; details for HW)



The nilradical

Proposition

The nilradical is the intersection of all nonzero prime ideals: $\mathfrak{N}_R = \bigcap_{P \subsetneq R \text{ prime}} P$.

Proof

"$\subseteq$" Let $a \in \mathfrak{N}_R$ 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 $a \notin \mathfrak{N}_R$; we'll show $a \notin \cap P$.

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

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 $a^n \in (x) + P$ and $a^m \in (y) + P$ for some n, m.

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

Radicals of ideals and rings

Loosely speaking, a radical of a ring is an ideal of "bad elements."

Definition / corollary

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: $\mathfrak{N}(R) := \sqrt{0}$.

Definition

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

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

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

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

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

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)

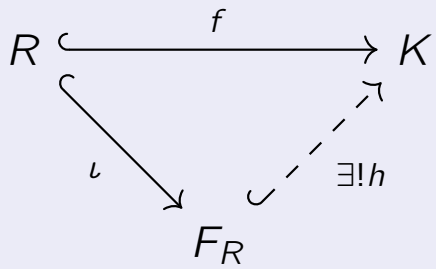
Every integral domain canonically embeds into its field of fractions, via $r \mapsto r/1$.

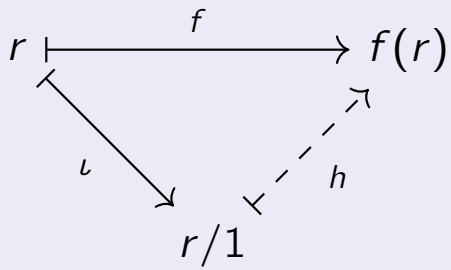
Moreover, this is the *minimal* field containing R.

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 $f : R \hookrightarrow K$ into a field, there is a unique $h\colon F_R \hookrightarrow K$ such that $h \circ \iota = f$.





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,

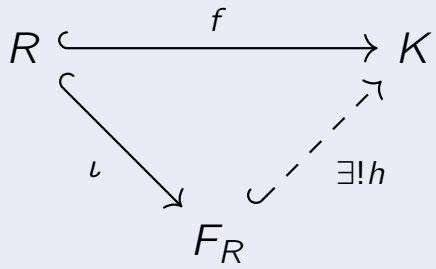
(iii) unique

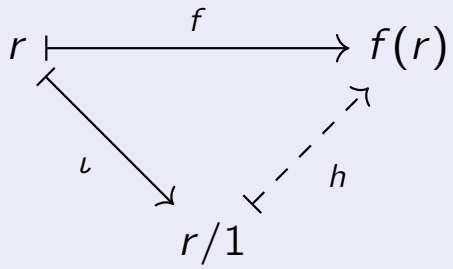
(iv) injective.

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 $f : R \hookrightarrow K$ into a field, there is a unique $h\colon F_R \hookrightarrow K$ such that $h \circ \iota = f$.





Proof

Define the map

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

(i) Well-defined. Suppose $a/b = c/d$. Then

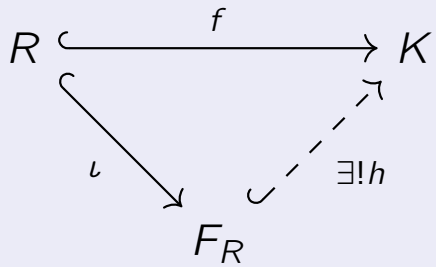
$$\begin{aligned} h(a/b) = h(a/1)h(b/1)^{-1} &= h(bc/d)h(b/1)^{-1} = f(bc)f(d)^{-1}f(b)^{-1} \\ &= f(b)f(c)f(d)^{-1}f(b)^{-1} = f(c)f(d)^{-1} \\ &= h(c/1)h(d/1)^{-1} = h(c/d). \end{aligned}$$

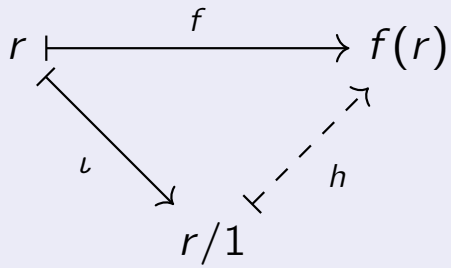
✓

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 $h \circ \iota = f$.





Proof

Define the map

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

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

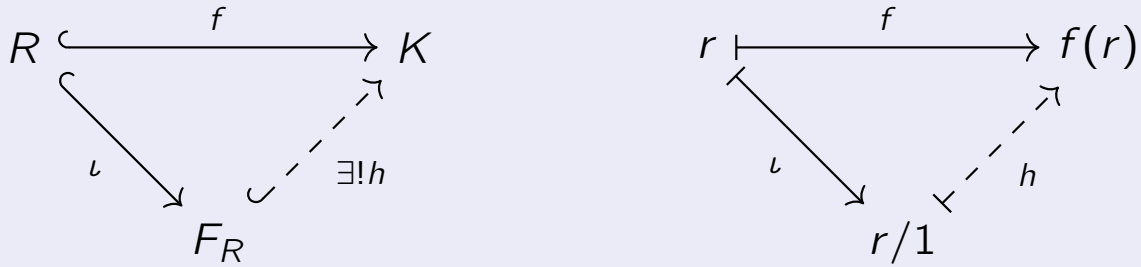
$$\begin{aligned} h(a/b \cdot c/d) = h(ac/bd) &= h(ac/1)h(bd/1)^{-1} = f(ac)f(bd)^{-1} = f(a)f(c)f(b)^{-1}f(d)^{-1} \\ &= h(a/1)h(b/1)^{-1}h(c/1)h(d/1)^{-1} = h(a/b)h(c/d). \end{aligned}$$ ✓

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 $h \circ \iota = f$.



Proof

Define the map

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

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

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

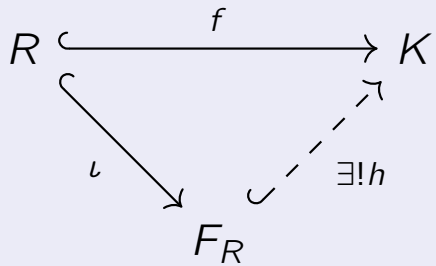
However, $f(b)^{-1} \neq 0$ because since f is an embedding and $b \neq 0$.

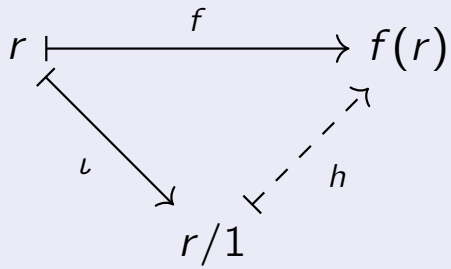
Thus $f(a) = 0$, so $a = 0$ in R. Thus $a/1 = 0/1$, the zero element in F_R. ✓

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 $h \circ \iota = f$.





Proof

Define the map

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

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

$$\begin{aligned} g(a/b) &= g((a/1)\cdot(b/1)^{-1}) = g(a/1)g(b/1)^{-1} = g(\iota(a))g(\iota(b))^{-1} \ = f(a)f(b)^{-1} \\ &= h(\iota(a))h(\iota(b))^{-1} = h(a/1)h(b/1)^{-1} = h((a/1)\cdot(b/1)^{-1}) = h(a/b). \end{aligned}$$

✓

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.

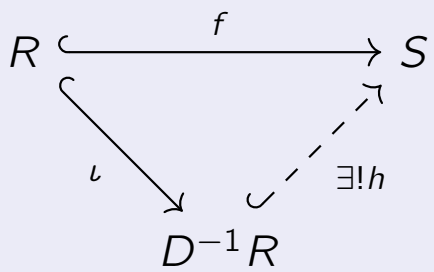
We can carry out the same construction of the set

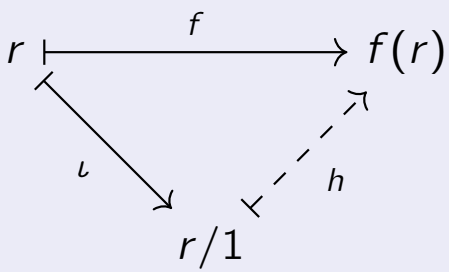
$$R \times D = \{(r, d) \mid r \in R,\ d \in D\}, \qquad (r_1, d_1) \sim (r_2, d_2) \text{ iff } r_1 d_2 = r_2 d_1.$$

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 $h \circ \iota = f$.





Localization with zero divisors

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

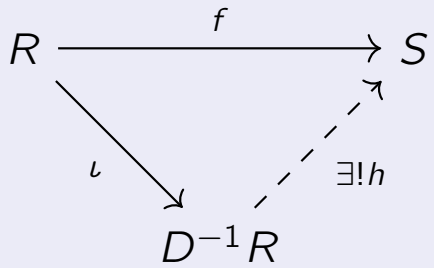
The mapping $R \longrightarrow D^{-1}R$ sending r to its equivalence class is no longer injective:

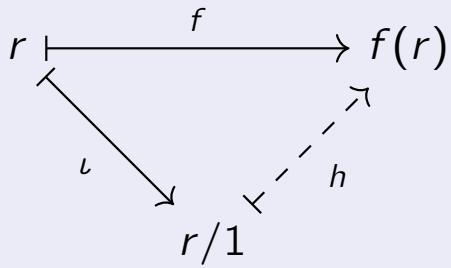
$$\iota\colon R \longrightarrow D^{-1}R, \qquad \iota(z) = 0, \quad \text{for all zero divisors } z \in D.$$

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 $h \circ \iota = f$.





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

Rings of fractions

Examples

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 nonzero divisors, then $D^{-1}R$ is the ring of fractions of R.
3. If $R = F[x]$ and $D = \{x^n \mid n \in \mathbb{Z}\}$, then $D^{-1}R = F[x, x^{-1}]$, the Laurent polynomials.
4. If $R = \mathbb{Z}$ and $D = \{5^n \mid n \in \mathbb{N}\}$, then $R_D = \mathbb{Z}[\frac{1}{5}]$, which are "*polynomials in* $\frac{1}{5}$" over $\mathbb{Z}$.
5. 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.

Divisibility and factorization

We just saw how to extend a familiar construction (fractions) from $\mathbb{Z}$ to other commutative rings.

Now, we'll do the same for other basic features of the integers.

Blanket assumption

Unless otherwise stated, R is an integral domain, and $R^* := R \setminus \{0\}$.

The integers have several basic properties that we usually take for granted:

- every nonzero number can be factored uniquely into primes;
- any two numbers have a unique greatest common divisor and least common multiple;
- for a and $b \neq 0$ the division algorithm gives us

$$a = qb + r, \qquad \text{where } |r| < |b|.$$

- the Euclidean algorithm uses the divison algorithm to find GCDs.

These need not hold in integrals domains! We would like to understand this better.

Divisibility

Definition

If $a, b \in R$, then a divides b, or b is a multiple of a if $b = ac$ for some $c \in R$. Write $a \mid b$.

If $a \mid b$ and $b \mid a$, then a and b are associates, written $a \sim b$.

Examples

- In $\mathbb{Z}$: n and $-n$ are associates.
- In $\mathbb{R}[x]$: $f(x)$ and $c \cdot f(x)$ are associates for any $c \neq 0$.

This defines an equivalence relation on R^*, and partitions it into equivalence classes.

- The unique maximal class is $\{0\}$ (because $r \mid 0$, $\forall r \in R$).
- The unique minimal class is $U(R)$ (because $u \mid r$, $\forall u \in U(R)$, $r \in R$).
- Elements in the minimal classes of $R - U(R)$ are called irreducible.

Exercise

The following are equivalent for $a, b \in R$:

(i) $a \sim b$, (ii) $a = bu$ for some $u \in U(R)$, (iii) $(a) = (b)$.

Divisibility via ideals

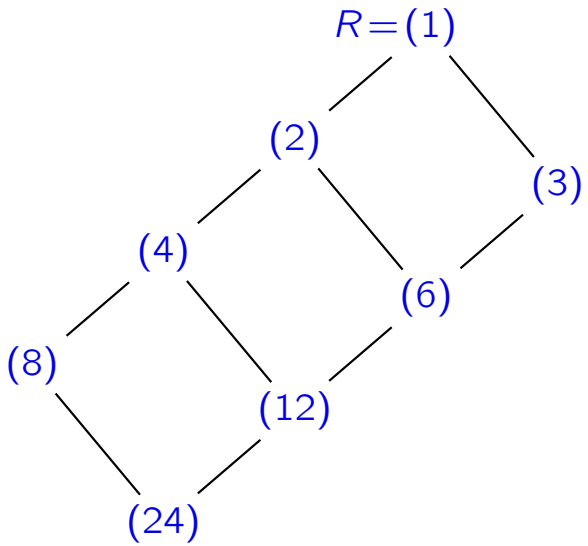
Remark

For nonzero $a, b \in R$,

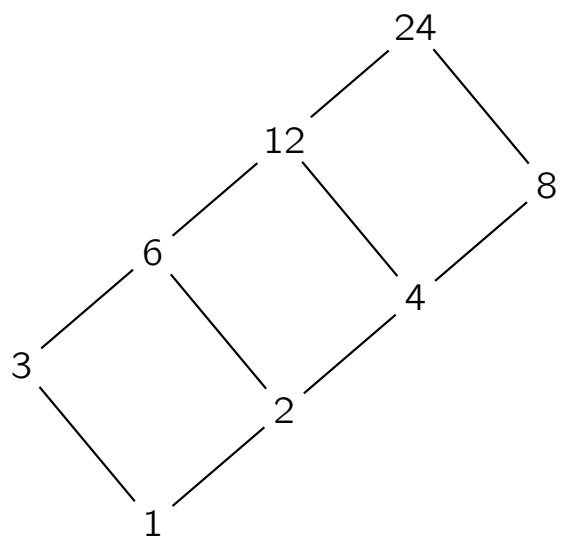
$$a \mid b \quad \Leftrightarrow \quad (b) \subseteq (a).$$

Key idea

Questions about divisibility are cleaner when translated into the language of ideals.



subring lattice; $\langle d \rangle = (d)$



divisor lattice

Divisibility is well-behaved in rings where *every* ideal is generated by a single element.

Divisibility, factorization, and principal ideals

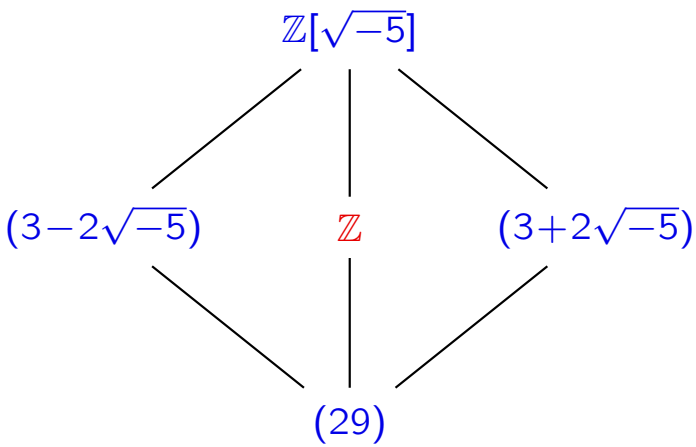
Definition

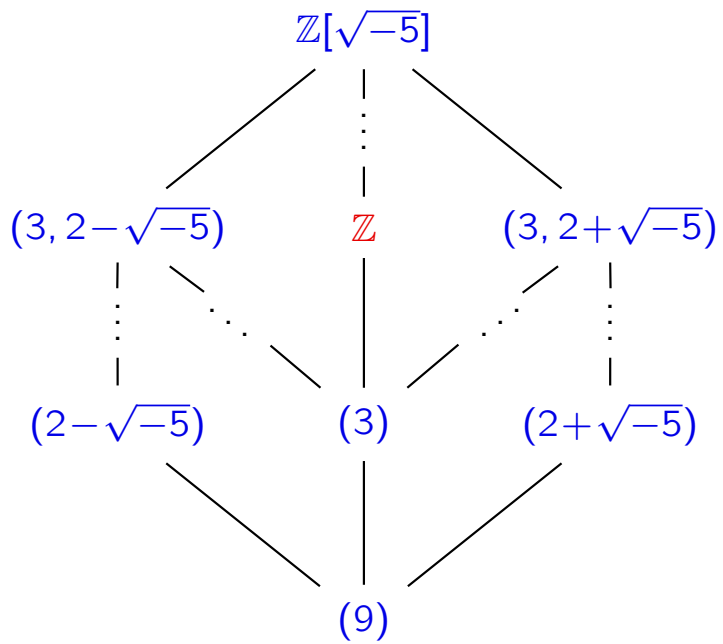
An ideal generated by a single element $a \in R$, denoted $I = (a)$, is called a principal ideal.

When unique factorization fails, non-principal ideals lurk.

Consider the following examples in $\mathbb{Z}[\sqrt{-5}]$:

$$29 = (3 - 2\sqrt{-5})(3 + 2\sqrt{-5}), \qquad 3 \cdot 3 = 9 = (2 - \sqrt{-5})(2 + \sqrt{-5}).$$





- The element 29 is reducible, whereas 3 is irreducible.
- Neither of the ideals (3) and (29) are prime in $\subseteq \mathbb{Z}[\sqrt{-5}]$.

Principal ideal domains

I

f every ideal of R is principal, then R is a principal ideal domain (PID).

Divisibility via ideals: a summary

Let R be an integral domain.

1. u is a unit iff $(u) = R$,
2. $a \mid b$ iff $(b) \subseteq (a)$,
3. a and b are associates iff $(a) = (b)$.
4. a is irreducible iff there is no $(b) \supsetneq (a)$.

The following are all PIDs (stated without proof):

- the integers $\mathbb{Z}$,
- any field F,
- the ring $F[x]$.

Key idea

Divisibility and factorization are well-behaved in PIDs.

Prime ideals, prime elements, and irreducibles

Euclid's lemma (300 B.C.)

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

In the language of ideals:

If (a non-unit) p is prime, then $(ab) \subseteq (p)$ implies either $(a) \subseteq (p)$ or $(b) \subseteq (p)$.

Definition

An element $p \in R$ is prime if it is not a unit, and one of the equivalent conditions holds:

- $p \mid ab$ implies $p \mid a$ or $p \mid b$
- $(ab) \subseteq (p)$ implies $(a) \subseteq (p)$ or $(b) \subseteq (p)$.

Compare this to what it means for p to be irreducible: $a \mid p \Rightarrow a \sim p$ $(a \notin U(R))$.

These concepts coincide in PIDs (like $\mathbb{Z}$), but not in all integral domains.

Irreducibles and primes

Recall that a nonzero $p \notin U(R)$ is:

- irreducible if $\underbrace{p = ab}_{(ab)=(p)} \Rightarrow \underbrace{b \in U(R)}_{(a)=(p)}$ or $\underbrace{a \in U(R)}_{(b)=(p)}$.
- prime if $\underbrace{p \mid ab}_{(ab)\subseteq(p)} \Rightarrow \underbrace{p \mid a}_{(a)\subseteq(p)}$ or $\underbrace{p \mid b}_{(b)\subseteq(p)}$.

Proposition

If $0 \neq p \in R$ is prime, then p is irreducible.

Proof

Suppose p is not irreducible. Then $p = ab$ with $a, b \notin U(R)$.

Then (wlog) $p \mid a$, so $a = pc$ for some $c \in R$. Now,

$$p = ab = (pc)b = p(cb).$$

This means that $cb = 1$, and thus $b \in U(R)$. Therefore, p is prime. □

Prime ideals in a PID

Proposition

In a PID, a nonzero ideal P is prime if and only if it is maximal.

Proof

"$\Leftarrow$": Maximal ideals are always prime in a commutative ring. ✓

"$\Rightarrow$": Let (p) be a prime ideal in a PID. We need to show:

$$\underbrace{(p) \subseteq (m)}_{m \mid p} \subseteq R \qquad \Longrightarrow \qquad \underbrace{(m) = (p)}_{m \mid p} \quad \text{or} \quad \underbrace{(m) = R}_{m \in U(R)}.$$

If $m \mid p$, then $p = ma$ for some $a \in R$.

Since primes are irreducible, either $m \in U(R)$ or $a \in U(R)$.

- If $m \in U(R)$, then $(m) = R$.
- If $a \in U(R)$, then $p \sim a$, and hence $(m) = (p)$. □

Corollary

In a PID, every irreducible is prime.

When irreducibles fail to be prime, and non-unique factorization

Caveat: Irreducible $\not\Rightarrow$ prime

In the ring $\mathbb{Z}[\sqrt{-5}] := \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$,

$$2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3, \quad \text{but} \quad 2 \nmid (1 \pm \sqrt{-5}).$$

Thus, 2 (and 3) are irreducible but not prime.

When irreducibles fail to be prime, we can lose nice properties like unique factorization.

Things can get really bad: not even the factorization *lengths* need be the same!

For example:

- $30 = 2 \cdot 3 \cdot 5 = -\sqrt{-30} \cdot \sqrt{-30} \in \mathbb{Z}[\sqrt{-30}]$,
- $81 = 3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}) \in \mathbb{Z}[\sqrt{-14}]$.

For another example, in the ring $R = \mathbb{Z}[x^2, x^3] = \left\{a_0 + a_2x^2 + a_3x^3 + \cdots + a_nx_n \mid a_i \in \mathbb{Z}\right\}$,

$$x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3.$$

The element $x^2 \in R$ is not prime because $x^2 \mid x^3 \cdot x^3$ yet $x^2 \nmid x^3$ in R.

Noetherian rings (weaker than being a PID)

A ring is Noetherian if it satisfies any of the three equivalent conditions.

Proposition

Let R be a ring. The following are equivalent:

(i) Every ideal of R is finitely generated.

(ii) Every ascending chain of ideals stabilizes. ("*ascending chain condition*")

(iii) Every nonempty family of ideals has a maximal element. ("*maximal condition*")

Proof (sketch)

$(1 \Rightarrow 2)$: Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain with $I = \bigcup_{j=1}^{\infty} I_j = (a_1, \ldots, a_n)$.

$(2 \Rightarrow 3)$: Let S be a nonempty family of ideals.

Take $I_1 \in S$. If it isn't maximal, take some $I_2 \supseteq I_1$ in S. Repeat; this process must stop.

$(3 \Rightarrow 1)$: Given I, let $S = \{\text{f.g. } J \trianglelefteq I\}$, with max'l element $M \subseteq I$. Suppose $a \in I - M$.

Then $M \subsetneq (M, a) \subseteq I \;\Rightarrow\; (M, a) = I$. □

We can define left-Noetherian and right-Noetherian rings analogously.

Greatest common divisors & least common multiples

Proposition

If $I \subseteq \mathbb{Z}$ is an ideal, and $a \in I$ is its smallest positive element, then $I = (a)$.

Proof

Pick any positive $b \in I$. Write $b = aq + r$, for $q, r \in \mathbb{Z}$ and $0 \leq r < a$.

Then $r = b - aq \in I$, so $r = 0$. Therefore, $b = qa \in (a)$. $\square$

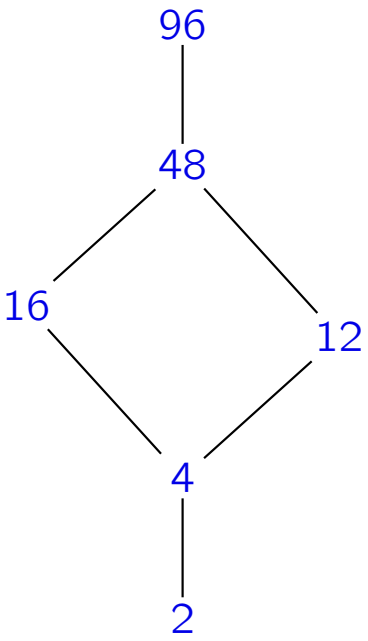
Definition

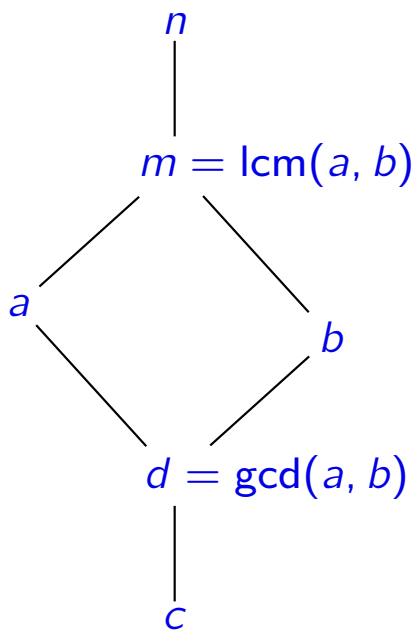
Given $a, b \in R$,

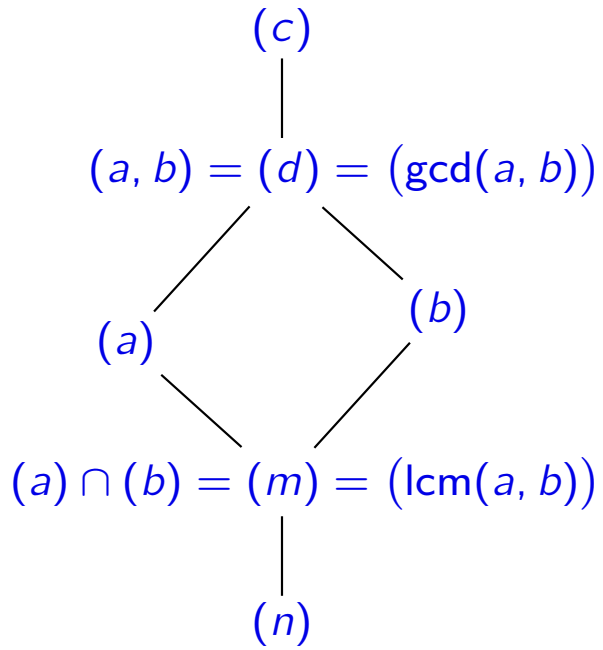
- $d \in R$ is a common divisor if $d \mid a$ and $d \mid b$.
- d is a greatest common divisor (GCD) if $c \mid d$ for every common divisor c.
- $m \in R$ is a common multiple if $a \mid m$ and $b \mid m$.
- $m \in R$ is a least common multiple (LCM) if $m \mid n$ for every common multiple n.

Greatest common divisors & least common multiples

The GCD and LCM have nice interpretations in the divisor and ideal lattices.







This is how we'll prove their existence and uniqueness in a PID.

Note that ab is a common multiple of a and b, so $(ab) \subseteq (a) \cap (b)$.

Nice properties of PIDs

Proposition

If R is a PID, then any $a, b \in R^*$ have a GCD, $d = \gcd(a, b)$.

It is *unique up to associates*, and can be written as $d = xa + yb$ for some $x, y \in R$.

Proof

Existence. The ideal generated by a and b is

$$I = (a, b) = \{ua + vb \mid u, v \in R\}.$$

Since R is a PID, we can write $I = (d)$ for some $d \in I$, and so $d = xa + yb$.

Since $a, b \in (d)$, both $d \mid a$ and $d \mid b$ hold.

If c is a divisor of a & b, then $c \mid xa + yb = d$, so d is a GCD for a and b. ✓

Uniqueness. If d' is another GCD, then $d \mid d'$ and $d' \mid d$, so $d \sim d'$. ✓ □

The second statement above is called Bézout's identity.

Unique factorization domains

Definition

An integral domain is a unique factorization domain (UFD) if:

(i) Every nonzero element is a product of irreducibles;

(ii) Every irreducible is prime.

Examples

1. $\mathbb{Z}$ is a UFD: Every $n \in \mathbb{Z}$ can be uniquely factored as a product of irreducibles (primes):

$$n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$

   This is the *fundamental theorem of arithmetic*.

2. The ring $\mathbb{Z}[x]$ is a UFD, because every polynomial can be factored into irreducibles. It is not a PID because the following ideal is not principal:

$$(2, x) = \{f(x) \mid \text{ the constant term is even}\}.$$

3. The ring $\mathbb{Q}[x, x^{1/2}, x^{1/4}, \ldots]$ has no irreducibles.

4. The ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

5. We've shown that (ii) holds for PIDs. Next, we will see that (i) holds as well.

Unique factorization domains

Theorem

If R is a PID, then R is a UFD.

Proof

We need to show Condition (i) holds: every element is a product of irreducibles.

We'll show that if this fails, we can construct

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots,$$

which is impossible in a PID. (They are Noetherian.)

Define

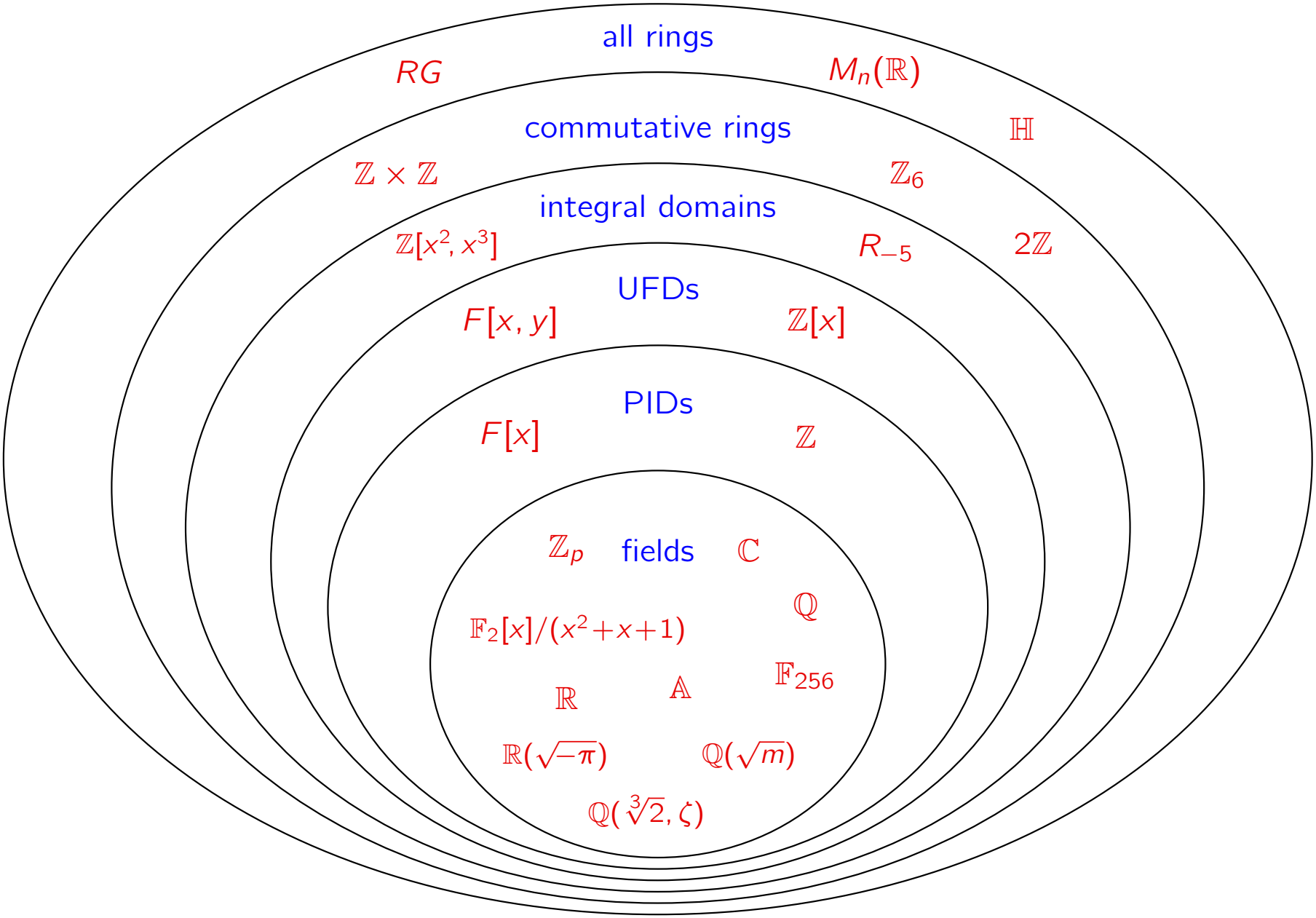
$$X = \{a \in R^* \setminus U(R) \mid a \text{ can't be written as a product of irreducibles}\}.$$

If $X \neq \emptyset$, then pick $a_1 \in X$. Factor this as $a_1 = a_2 b$, where $a_2 \in X$ and $b \notin U(R)$. Then $(a_1) \subsetneq (a_2) \subsetneq R$, and repeat this process. We get an ascending chain

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

that does not stabilize. Since this is impossible in a PID, $X = \emptyset$. □

Summary of ring types



The Euclidean algorithm

Around 300 B.C., Euclid wrote his famous book, the *Elements*, in which he described what is now known as the Euclidean algorithm:

Proposition VII.2 (Euclid's *Elements*)

Given two numbers not prime to one another, to find their greatest common measure.

The algorithm works due to two key observations:

- If $a \mid b$, then $\gcd(a, b) = a$;
- If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

This is best seen by an example: Let $a = 654$ and $b = 360$.

$654 = 360 \cdot 1 + 294$	$\gcd(654, 360) = \gcd(360, 294)$
$360 = 294 \cdot 1 + 66$	$\gcd(360, 294) = \gcd(294, 66)$
$294 = 66 \cdot 4 + 30$	$\gcd(294, 66) = \gcd(66, 30)$
$66 = 30 \cdot 2 + 6$	$\gcd(66, 30) = \gcd(30, 6)$
$30 = 6 \cdot 5$	$\gcd(30, 6) = 6$.

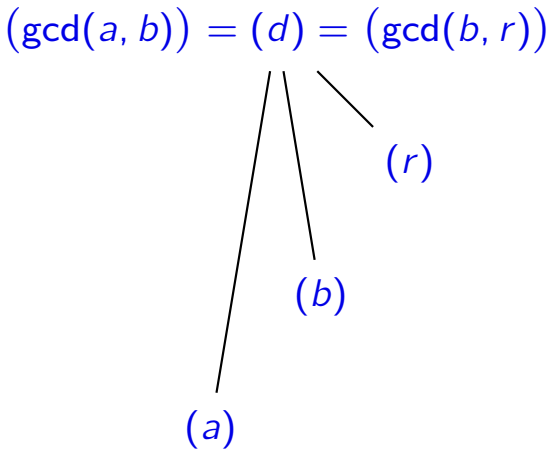
We conclude that $\gcd(654, 360) = 6$.

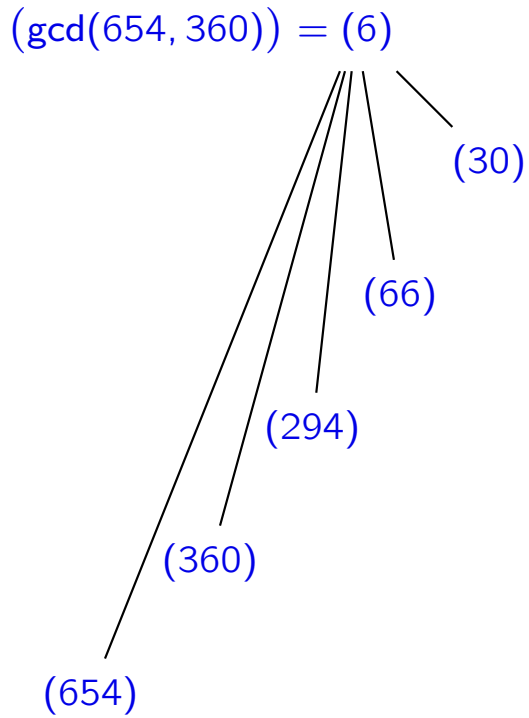
The Euclidean algorithm in terms of ideals

Let's see that example again: Let $a = 654$ and $b = 360$.

$$
\begin{aligned}
654 &= 360 \cdot 1 + 294 & \gcd(654, 360) &= \gcd(360, 294) \\
360 &= 294 \cdot 1 + 66 & \gcd(360, 294) &= \gcd(294, 66) \\
294 &= 66 \cdot 4 + 30 & \gcd(294, 66) &= \gcd(66, 30) \\
66 &= 30 \cdot 2 + 6 & \gcd(66, 30) &= \gcd(30, 6) \\
30 &= 6 \cdot 5 & \gcd(30, 6) &= 6.
\end{aligned}
$$

We conclude that $\gcd(654, 360) = 6$.





Euclidean domains

Loosely speaking, a Euclidean domain is a ring for which the Euclidean algorithm works.

Definition

An integral domain R is Euclidean if it has a degree function $d\colon R^* \to \mathbb{Z}$ satisfying:

(i) non-negativity: $d(r) \geq 0 \quad \forall r \in R^*$.

(ii) monotonicity: if $a \mid b$, then $d(a) \leq d(b)$,

(iii) division-with-remainder property: For all $a, b \in R$, $b \neq 0$, there are $q, r \in R$ such that

$$a = bq + r \qquad \text{with} \qquad r = 0 \quad \text{or} \quad d(r) < d(b)\,.$$

Note that Property (ii) could be restated to say: $d(a) \leq d(ab)$ *for all* $a, b \in R^*$.

Since 1 divides every $x \in R$,

$$d(1) \leq d(x), \qquad \text{for all } x \in R.$$

Similarly, if x divides 1, then $d(x) \leq d(1)$. Elements that divide 1 are the units of R.

Proposition

If u is a unit, then $d(u) = d(1)$. □

The division algorithm in $R = \mathbb{Z}$

The integers are a Euclidean domain with degree function

$$d : \mathbb{Z}^* \longrightarrow \mathbb{Z}, \qquad d(n) = |n|.$$

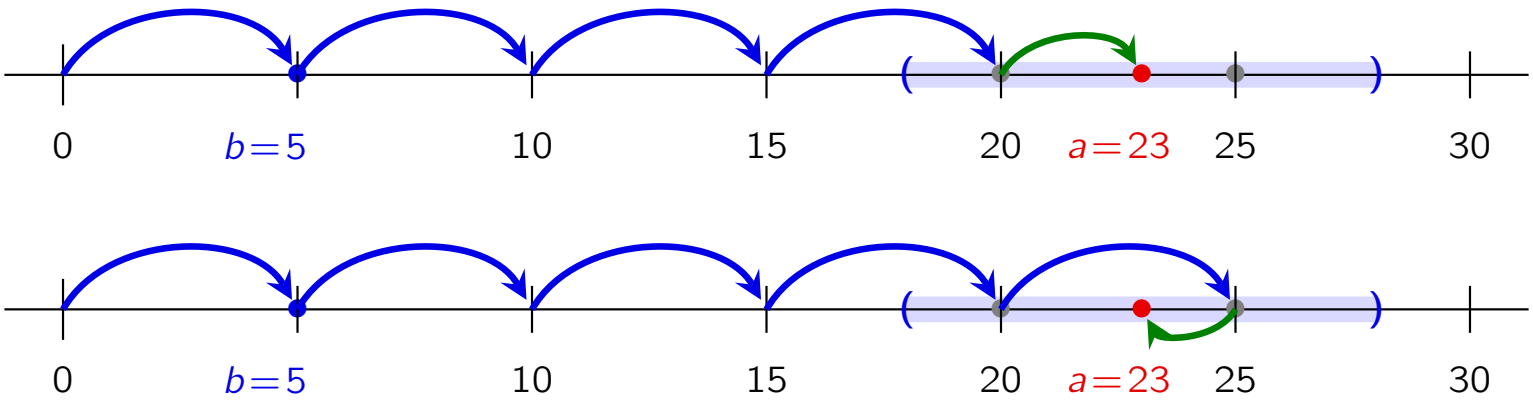
The division algorithm takes $a, b \in R$, $b \neq 0$, and finds $q, r \in R$ such that

$$a = bq + r \qquad \text{with} \qquad r = 0 \quad \text{or} \quad d(r) < d(b)\,.$$

Note that q and r are not unique!

There are two possibilities for q and r when dividing $b = 5$ into $a = 23$:

$$23 = 4 \cdot 5 + 3, \qquad 23 = 5 \cdot 5 + (-2).$$



Euclidean domains

Examples

- $R = \mathbb{Z}$ is Euclidean, with $d(r) = |r|$.
- $R = F[x]$ is Euclidean if F is a field. Define $d(f(x)) = \deg f(x)$.
- The Gaussian integers
$$\mathbb{Z}[\sqrt{-1}] = \{a + bi \mid a, b \in \mathbb{Z}\}$$
is Euclidean with degree function $d(a + bi) = a^2 + b^2$.

Proposition

If R is Euclidean, then $U(R) = \{x \in R^* \mid d(x) = d(1)\}$.

Proof

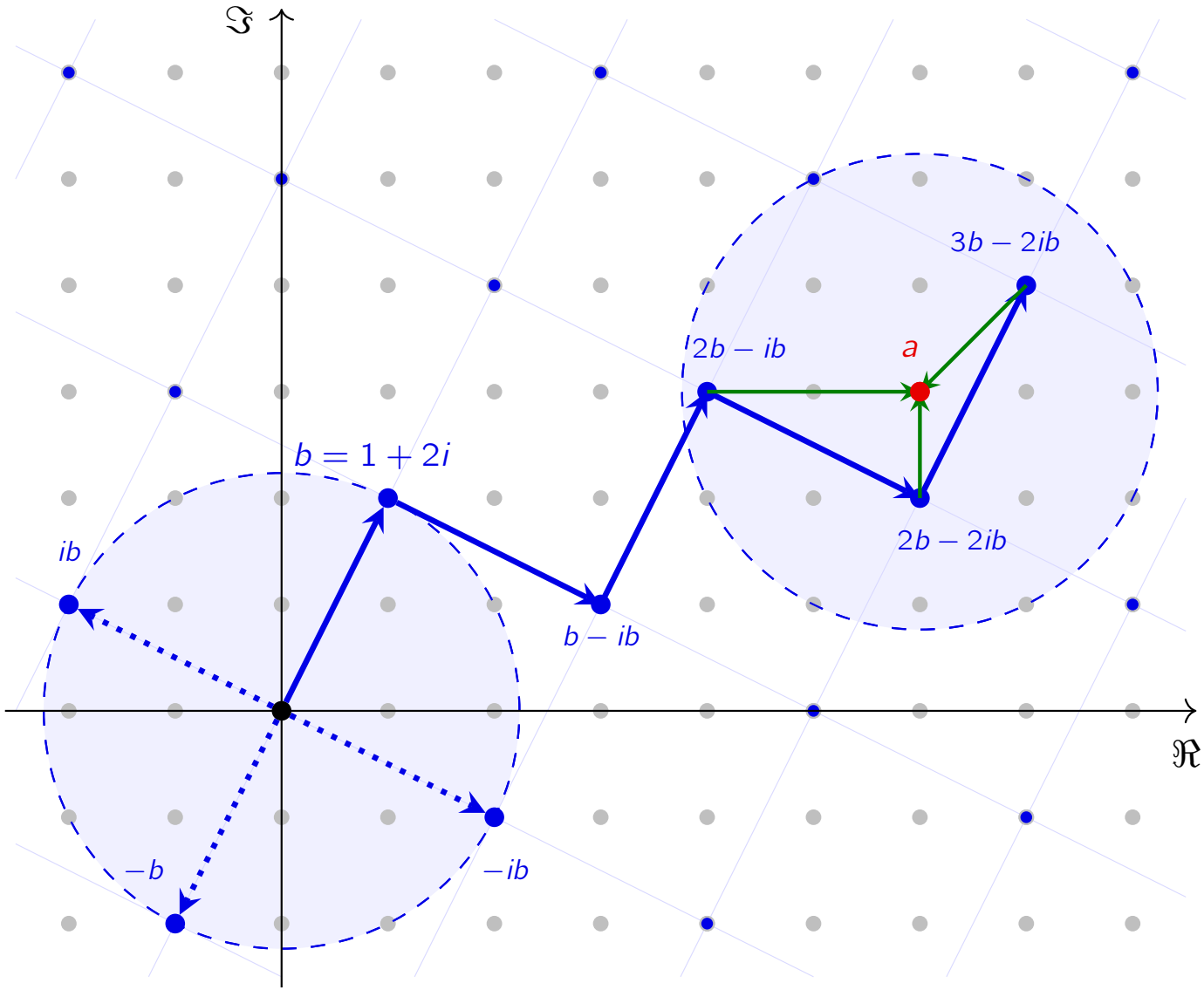
We've already established "$\subseteq$". For "$\supseteq$", Suppose $x \in R^*$ and $d(x) = d(1)$.

Write $1 = qx + r$ for some $q \in R$, and $r = 0$ or $d(r) < d(x) = d(1)$.

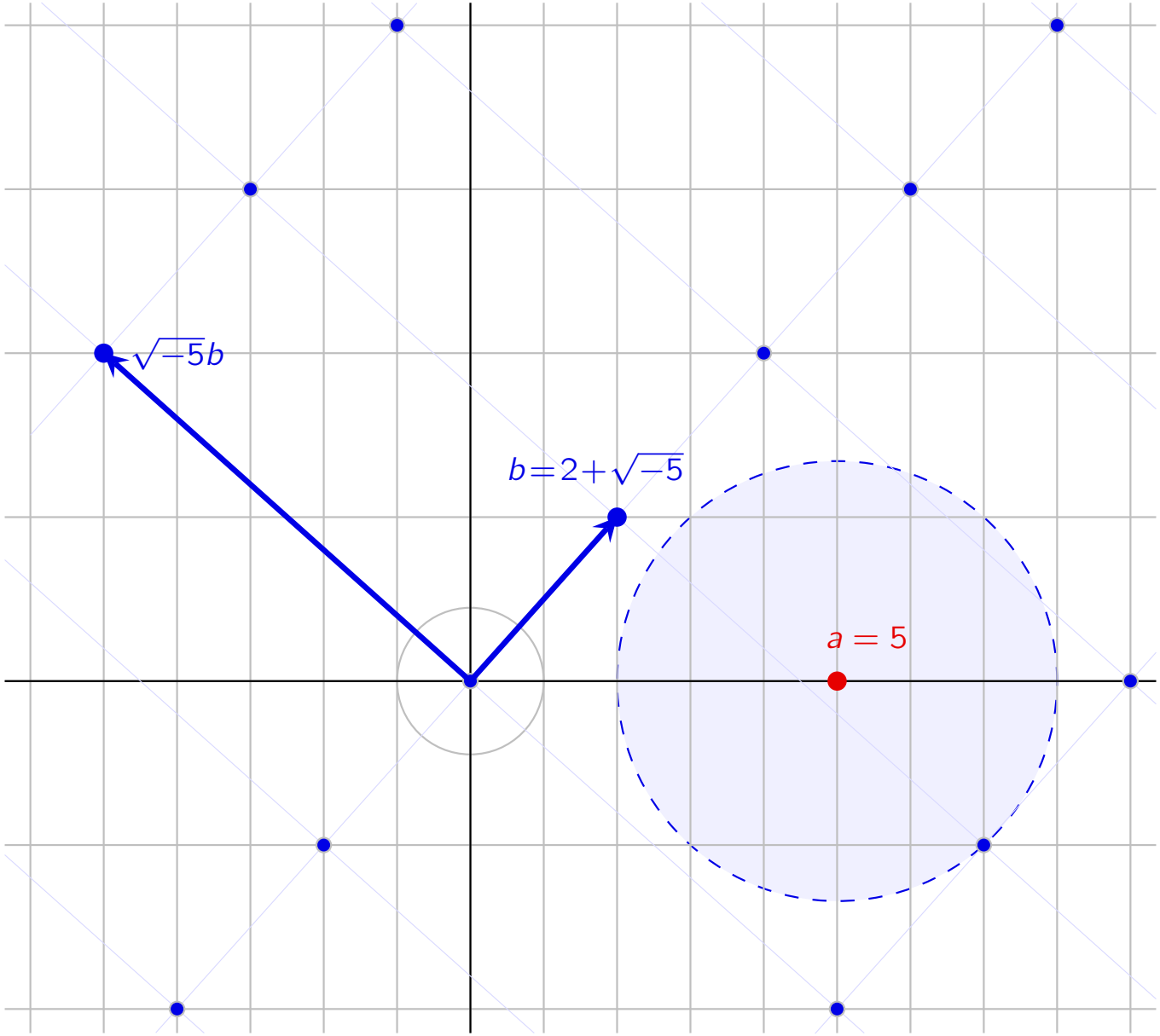
But $d(r) < d(1)$ is impossible, and so $r = 0$, which means $qx = 1$ and hence $x \in U(R)$. $\square$

The division algorithm in the Gaussian integers

$$6+3i = a = (2-i)b+2 = (2-2i)b+i = (3-2i)b+(-1-i)$$

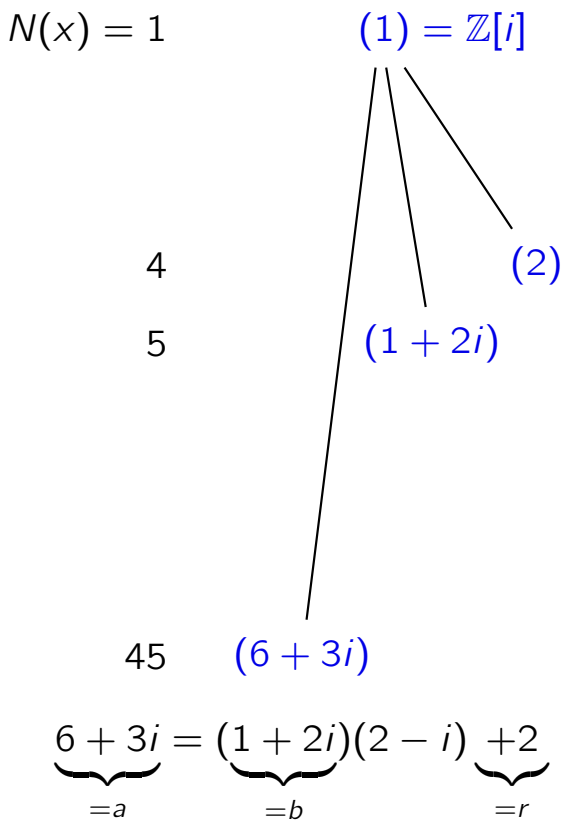


Failure of the division algorithm in $R_{-5} = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$

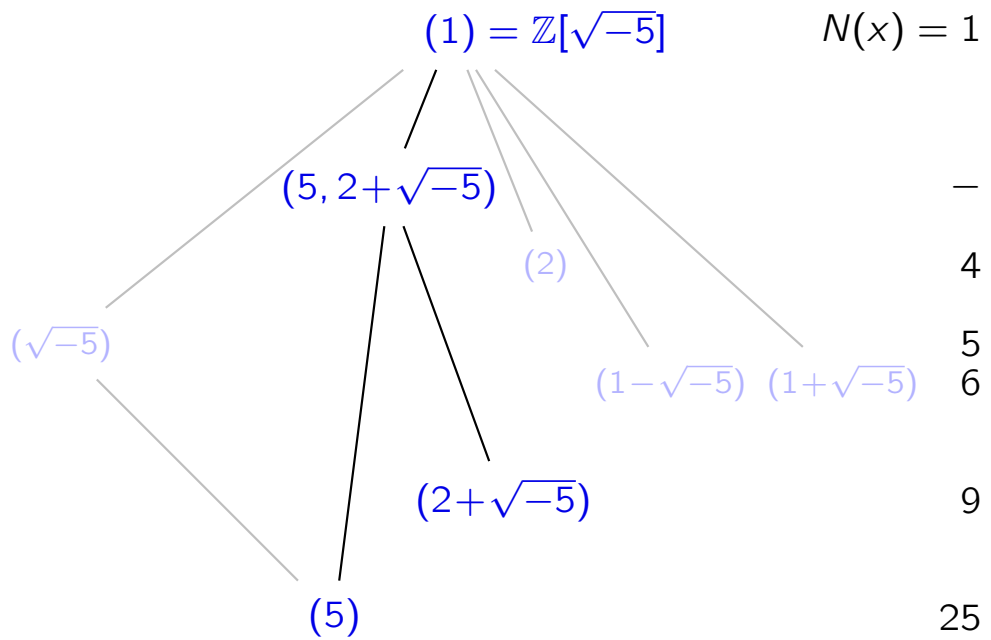


The Euclidean algorithm in terms of principal ideals and lattices

- $\gcd(6+3i, 1+2i) = 1$ in $\mathbb{Z}[i]$: (1) is the min'l princ. ideal containing $(6+3i)$ & $(1+2i)$.
- $\gcd(5, 2+\sqrt{-5}) = 1$ in $\mathbb{Z}[\sqrt{-5}]$: (1) is the min'l princ. ideal containing (5) & $(2+\sqrt{-5})$.



$$\underbrace{6+3i}_{=a} = \underbrace{(1+2i)}_{=b}(2-i)\underbrace{+2}_{=r}$$



$$5 \neq (2+\sqrt{-5})q + r, \quad N(r) < N(b) = 9$$

Note that there are only four principal ideals of $\mathbb{Z}[\sqrt{-5}]$ of norm less than $N(2+\sqrt{-5}) = 9$!

Euclidean domains and PIDs

Proposition

Every Euclidean domain is a PID.

Proof

Let $I \neq 0$ be an ideal of R and pick some $b \in I$ with $d(b)$ minimal.

Pick $a \in I$, and write

$$a = bq + r, \qquad \text{where } r = 0 \text{ or } \underbrace{0 < d(r) < d(b)}_{\text{impossible by minimality}}.$$

Therefore, $r = 0$, which means $a = bq \in (b)$.

Since a was arbitrary, $I = (b)$. □

Therefore, non-PIDs like the following cannot be Euclidean:

(i) $\mathbb{Z}[\sqrt{-5}]$, (ii) $\mathbb{Z}[x]$, (iii) $F[x, y]$.

Quadradic fields

The quadratic field for a square-free $m \in \mathbb{Z}$ is

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}.$$

Proposition (exercise)

In $\mathbb{Q}[x]$, since $x^2 - m$ is irreducible, it generates a maximal ideal, and there's an isomorphism

$$\mathbb{Q}[x]/(x^2 - m) \longrightarrow \mathbb{Q}(\sqrt{m}), \qquad f(x) + I \longmapsto f(\sqrt{m}).$$

Definition

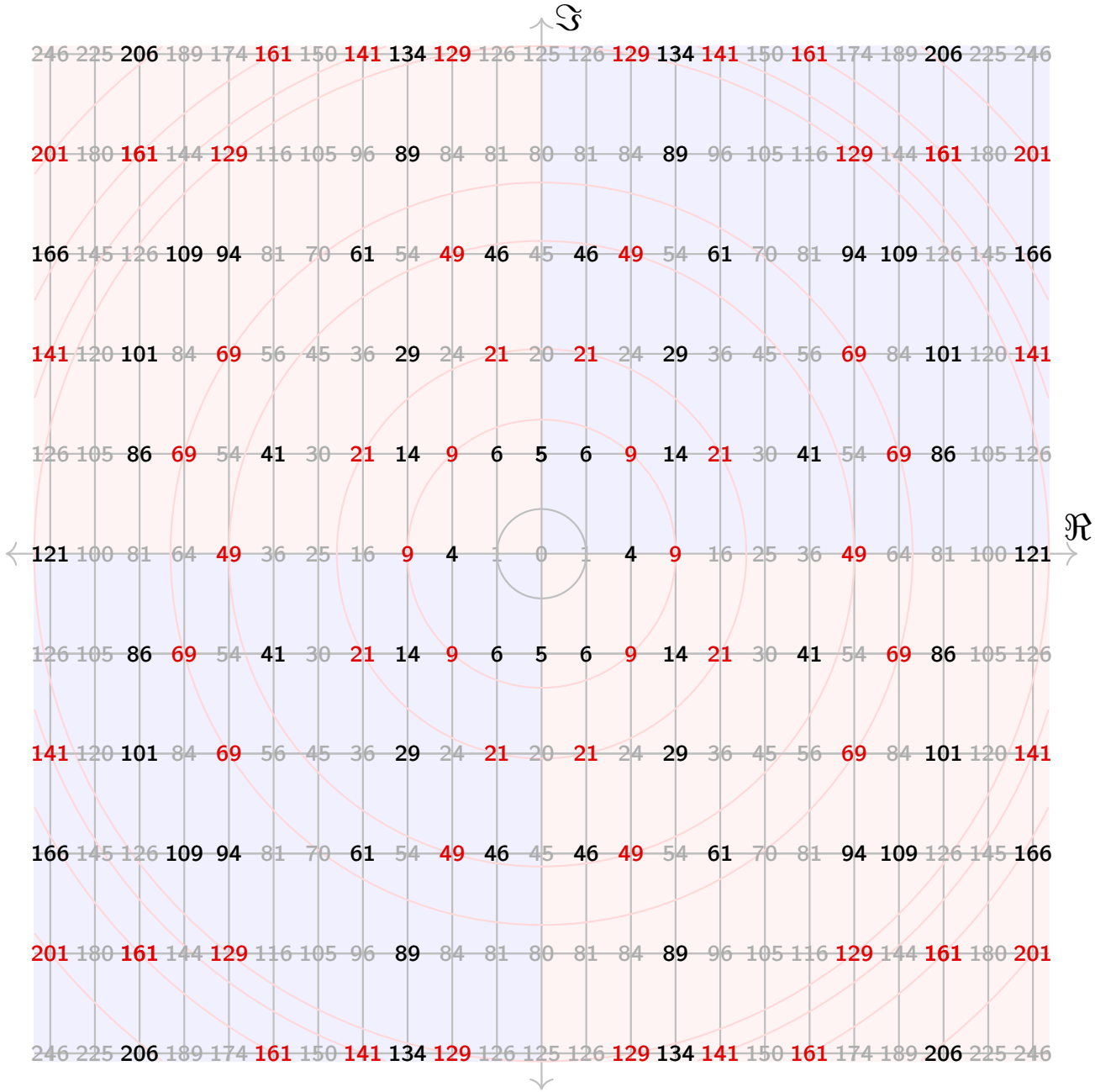
The field norm of $\mathbb{Q}(\sqrt{m})$ is

$$N \colon \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}, \qquad N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

Remarks (exercises)

- The field norm is multiplicative: $N(xy) = N(x)N(y)$.
- If $m < 0$ and $z = a + b\sqrt{m} \in \mathbb{C}$, then $N(a + b\sqrt{m}) = z\bar{z} = |z|^2$.
- If $m > 0$, then $N(x)$ isn't a classic "norm" – it can take negative values.

Norms of elements in $\mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\} \subseteq \mathbb{Q}(\sqrt{-5})$



Quadradic integers

Every number in $\mathbb{Z}[\sqrt{m}]$ is a root of a monic degree-2 polynomial:

$$a + b\sqrt{m} \qquad \text{is a root of} \qquad f(x) = x^2 - 2ax + (a^2 - b^2 m) \in \mathbb{Z}[x].$$

If $m \equiv 1 \bmod 4$, then

$$\mathbb{Z}\left[\tfrac{1+\sqrt{m}}{2}\right] = \left\{a + b\tfrac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z}\right\} = \left\{\tfrac{c}{2} + \tfrac{d\sqrt{m}}{2} \mid c \equiv d \pmod 2\right\}$$

also contains roots of monic polynomials:

$$\tfrac{a+b\sqrt{m}}{2} \qquad \text{is a root of} \qquad f(x) = x^2 - ax + \tfrac{a^2 - b^2 m}{4} \in \mathbb{Z}[x].$$

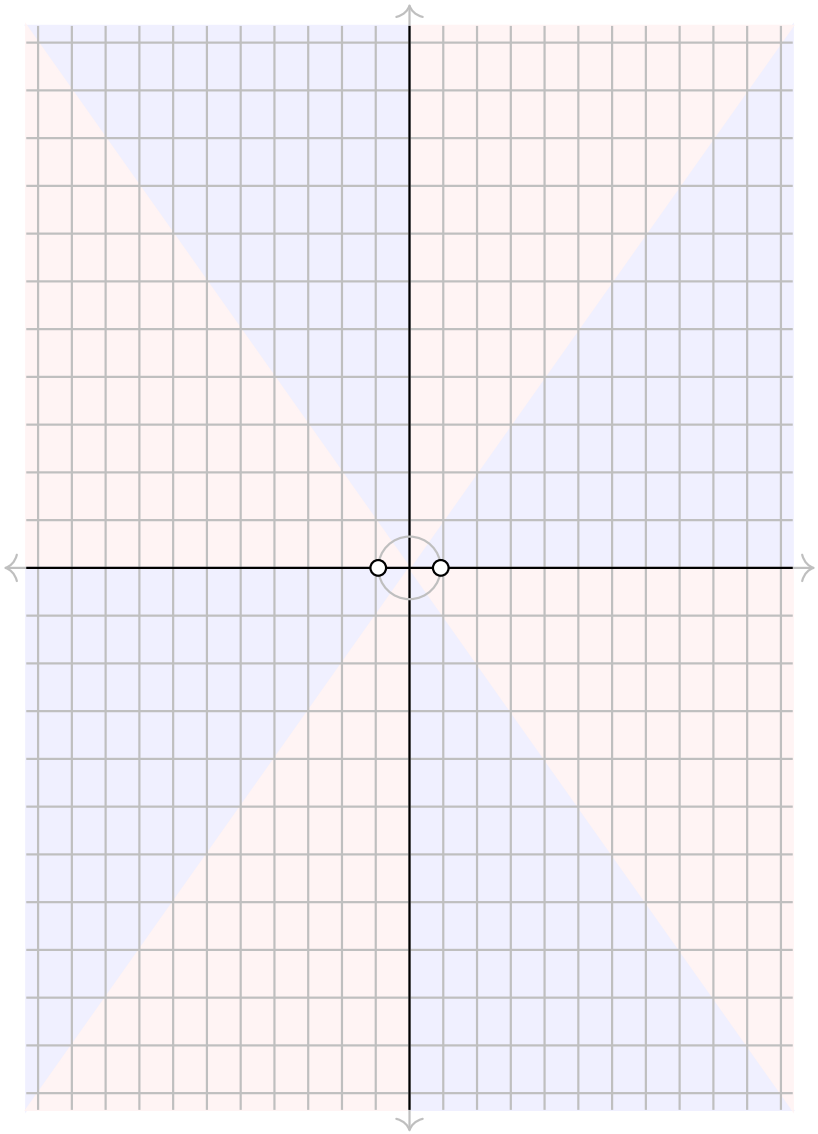
Definition

For a square-free $m \in \mathbb{Z}$, the ring R_m of quadratic integers is the subring of $\mathbb{Q}(\sqrt{m})$ consisting of roots of monic quadratic polynomials in $\mathbb{Z}[x]$:

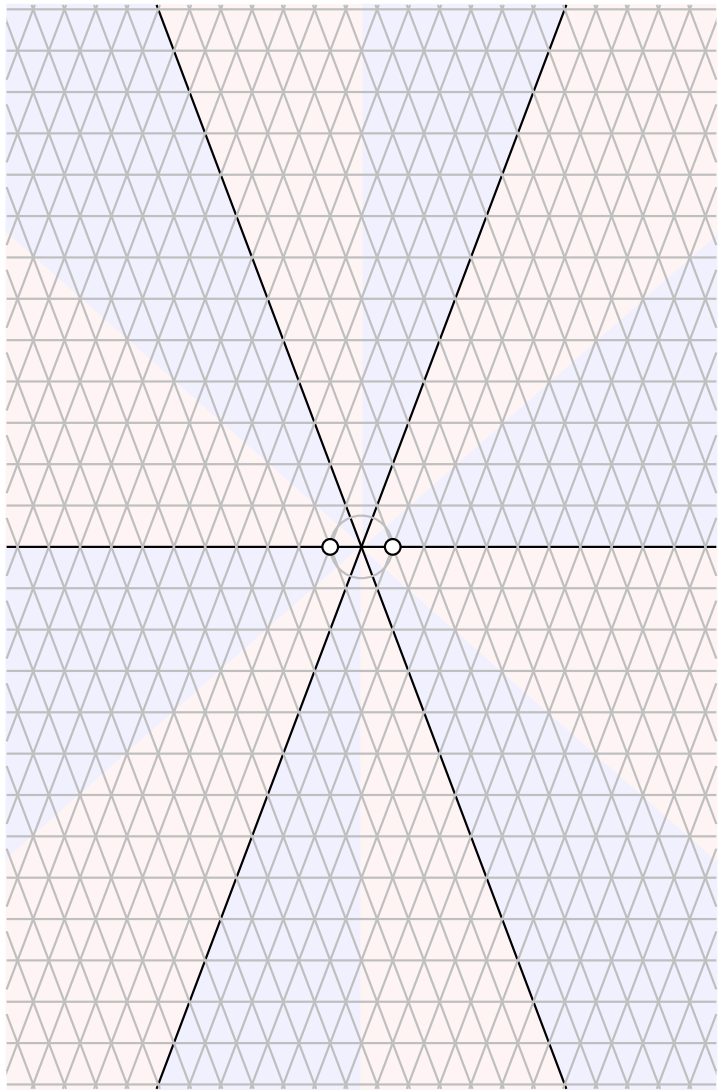
$$R_m = \begin{cases} \mathbb{Z}[\sqrt{m}] & m \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbb{Z}\left[\tfrac{1+\sqrt{m}}{2}\right] & m \equiv 1 \pmod 4 \end{cases}$$

These are subrings of the algebraic integers, the roots of polynomials, and the algebraic numbers, the roots of all polynomials in $\mathbb{Z}[x]$.

Examples: $R_{-2} = \mathbb{Z}[\sqrt{-2}]$ and $R_{-7} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \subseteq \mathbb{C}$

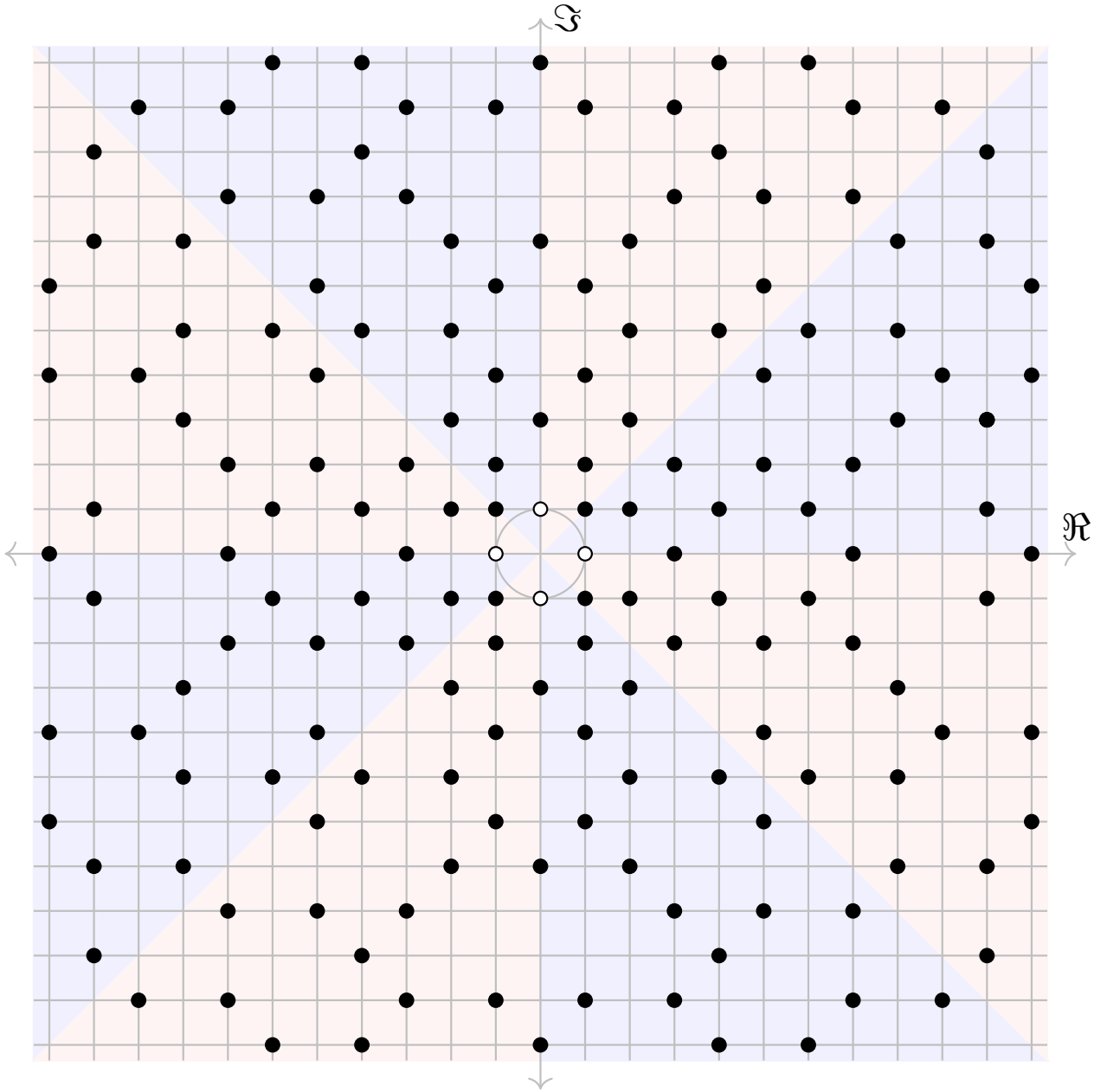


"*rectangular*"

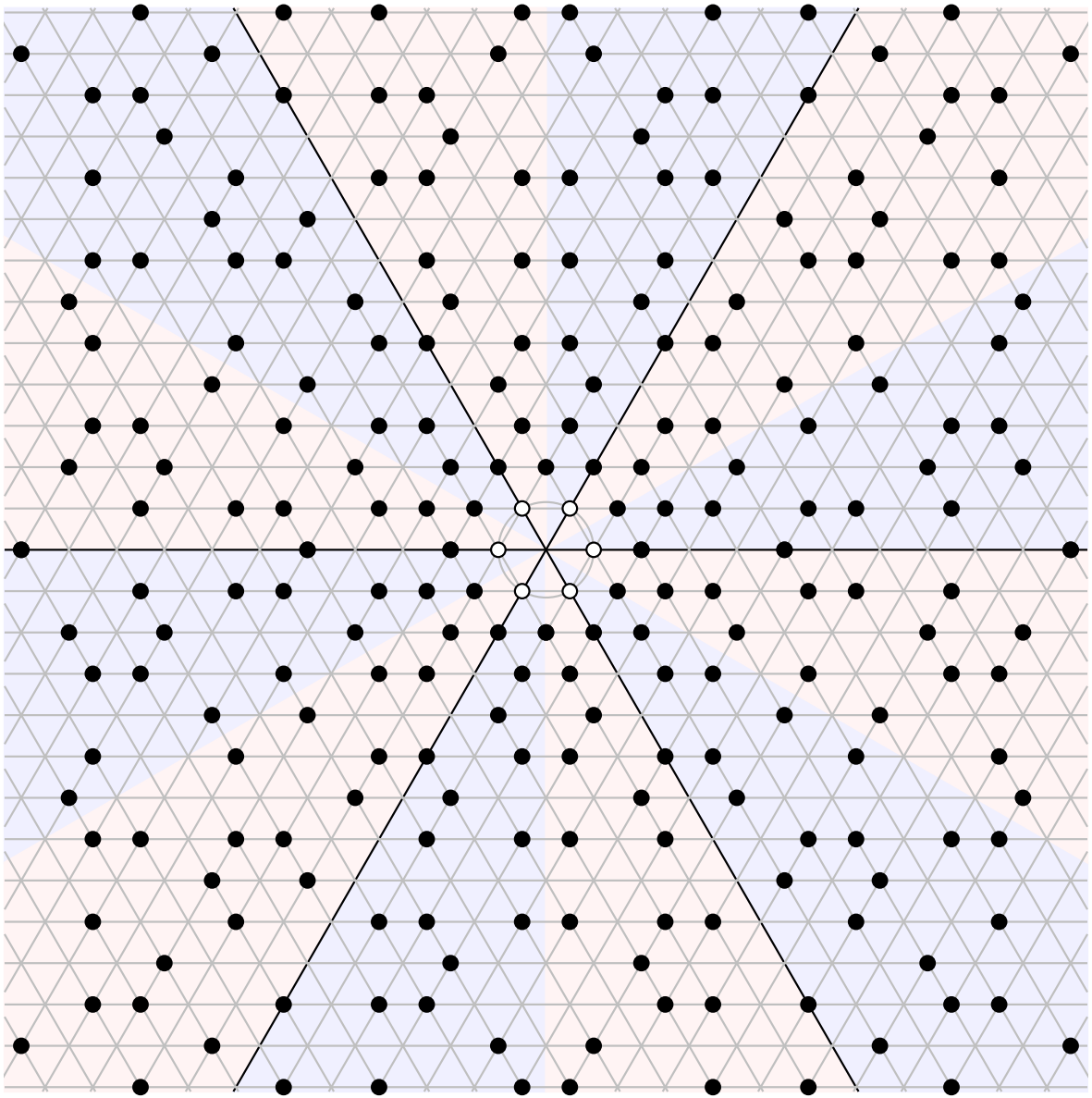


"*triangular*"

Primes in the Gaussian integers: $R_{-1} = \left\{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\right\}$

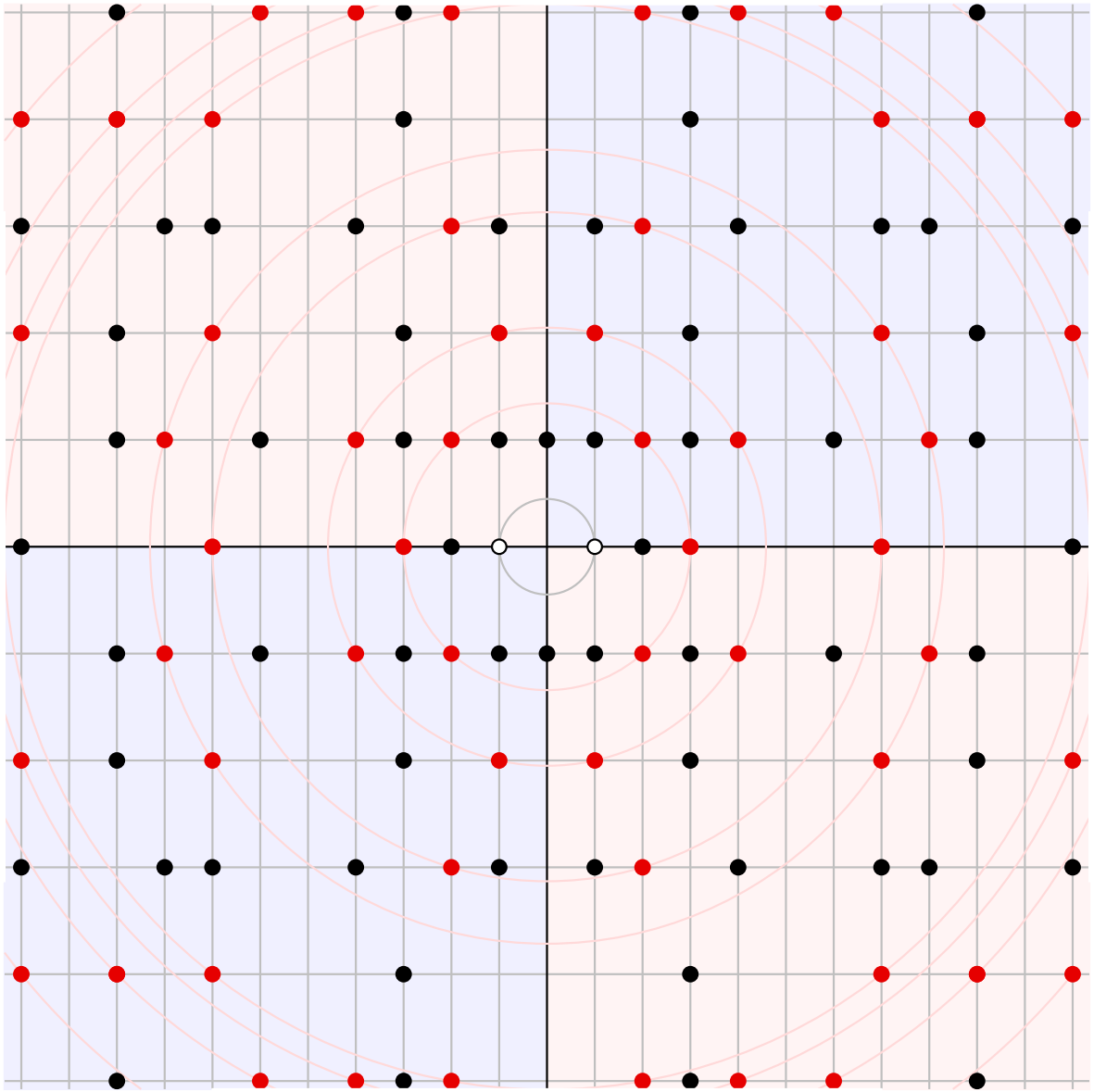


Primes in the Eisenstein integers: $R_{-3} = \{a + \omega b \mid a, b \in \mathbb{Z}\}$, $\omega = \frac{1+\sqrt{-3}}{2}$



Primes in $R_{-5} = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$

Units are white, primes are **black**, non-prime irreducibles are **red**.



Units, primes, and irreducibles in algebraic integer rings

The field norm of $z \in R_m$ is an integer, even in $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$:

$$N\left(a + b\tfrac{1+\sqrt{m}}{2}\right) = a^2 + ab + \tfrac{1-m}{4}b^2 \in \mathbb{Z}, \qquad \text{if } m \equiv 1 \bmod 4.$$

This, with $N(xy) = N(x)N(y)$, means that $u \in U(R_m)$ iff $N(u) = \pm 1$.

Units in R_m

- R_{-1} has 4 units: ± 1 and $\pm i$ (solutions to $N(a+bi) = a^2 + b^2 = 1$).
- R_{-3} has 6 units: ± 1, and $\pm\frac{1\pm\sqrt{-3}}{2}$ (solutions to $N(a+b\sqrt{-3}) = a^2 + 3b^2 = 1$).
- $U(R_m) = \{\pm 1\}$ for all other $m < 0$.
- If $m \geq 0$, then R_m has infinitely many units – solutions to Pell's equation:

$$N(a + b\sqrt{m}) = a^2 - b^2 m = \pm 1.$$

The norm is useful for determining the primes and irreducibles in R_m.

Non-prime irreducibles lead to multiple elements with the same norm. In R_{-5}:

$$3 \cdot 3 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5}) \quad \Rightarrow \quad N(3) = N(2 + \sqrt{-5}) = 9.$$

If $N(x)$ is prime, then x is prime in R_m, but not conversely.

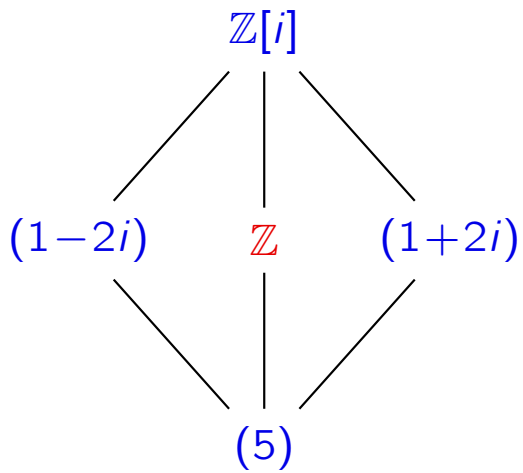
Primes in R_m

Consider a prime $p \in \mathbb{Z}$ but in the larger ring R_m. There are three possible behaviors:

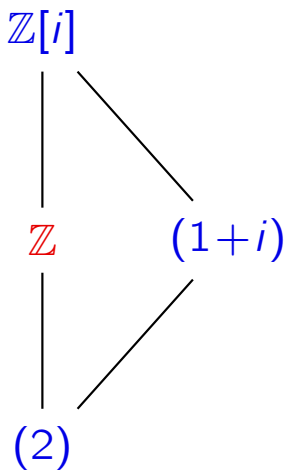
- p **splits** if $(p) = P_1 P_2$ for P_i prime (distinct). *E.g.*, $5 = (1+2i)(1-2i) \in \mathbb{Z}[i]$.
- p is **inert** if (p) remains prime in R_m. *E.g.*, $3 \in \mathbb{Z}[i]$.
- p is **ramified** if $(p) = P^2$, for P prime. *E.g.*, $2 = -i(1+i)^2 \in \mathbb{Z}[i]$.

Here's what this looks like in the subring lattice, for the Gaussian integers.

"3 *is inert*"



"5 *splits*"



"2 *is ramified*"

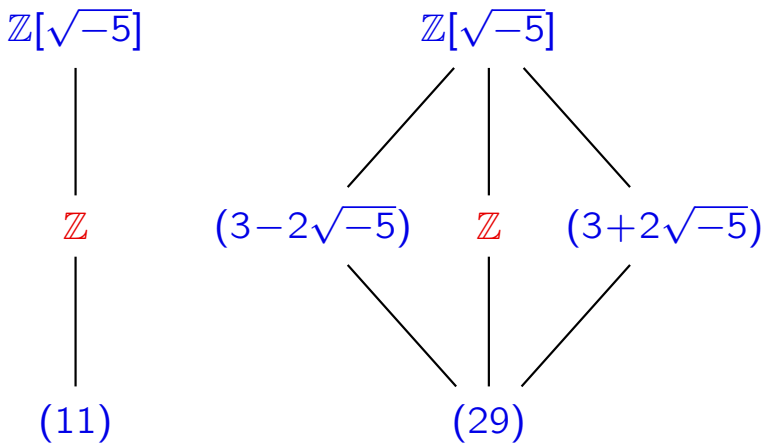
Notice that if a prime splits in $\mathbb{Z}[i]$, then it is reducible, and must factor.

Primes in R_m that aren't PIDs

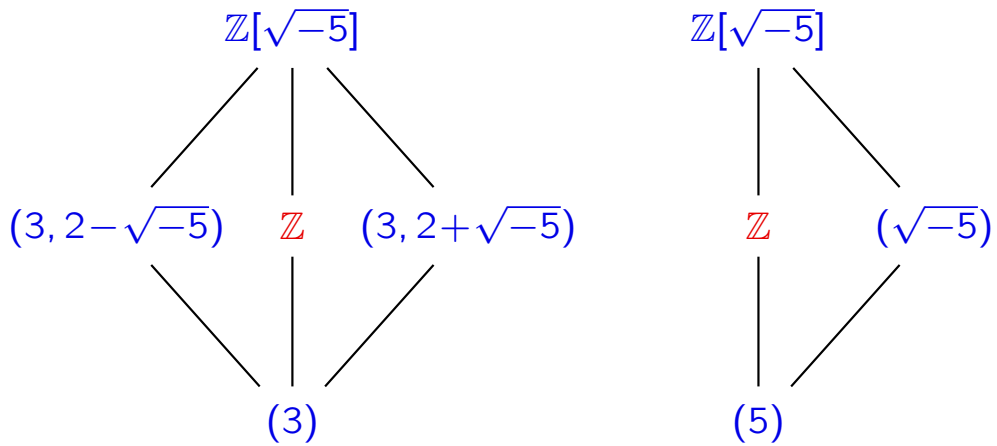
Consider a prime $p \in \mathbb{Z}$ but in the larger ring R_m. There are three possible behaviors:

- p **splits** if $(p) = P_1 P_2$ for P_i.
- p is **inert** if (p) remains prime in R_m.
- p is **ramified** if $(p) = P^2$, for P prime.

Here's what this looks like in the subring lattice of $R_{-5} = \mathbb{Z}[\sqrt{-5}]$.



"11 *is inert*" "29 *splits; is reducible*"



"3 *splits; is irreducible*" "5 *is ramified*"

Remark

In a non-PID, a split prime p may or may not factor, but its ideal (p) will.

Primes in R_m

If p is split or ramified, then (p) isn't a prime ideal because it factors.

The following characterizes *when* and *how* it factors.

Proposition (HW)

Consider the ring R_m of quadratic integers and a odd prime $p \in \mathbb{Z}$.

- If $p \nmid m$ and m is a *quadratic residue* mod p (i.e., $m \equiv n^2 \pmod{p}$), then p splits:

$$(p) = \left(p, n + \sqrt{m}\right)\left(p, n - \sqrt{m}\right),$$

- If $p \nmid m$ and m is not a quadratic residue mod p, then p is inert.
- If $p \mid m$, then p is ramified, and

$$(p) = \left(p, \sqrt{m}\right)^2.$$

Remark

This extends to all primes by replacing $p \mid m$ with $p \mid \Delta$, the **discriminant** of $\mathbb{Q}(\sqrt{-m})$:

$$\Delta = \begin{cases} m & m \equiv 1 \pmod{4} \\ 4m & m \equiv 2, 3 \pmod{4} \end{cases}$$

Primes in R_m

The behavior of a prime $p \in \mathbb{Z}$ in R_m is completely characterized by quadratic residues.

The discriminant Δ of R_m is $\Delta = m$ (triangular) or $\Delta = 4m$ (rectangular).

A prime $p \neq 2$ in $\mathbb{Z}$, when passed to R_m, becomes:

- ramified iff $\Delta \equiv 0 \pmod{p}$.
- split iff $\Delta \equiv a^2 \pmod{p}$, for some $a \not\equiv 0$,
- inert iff $\Delta \not\equiv a^2 \pmod{p}$, for all a.

The prime $p = 2$ in $\mathbb{Z}$, when passed to R_m, becomes:

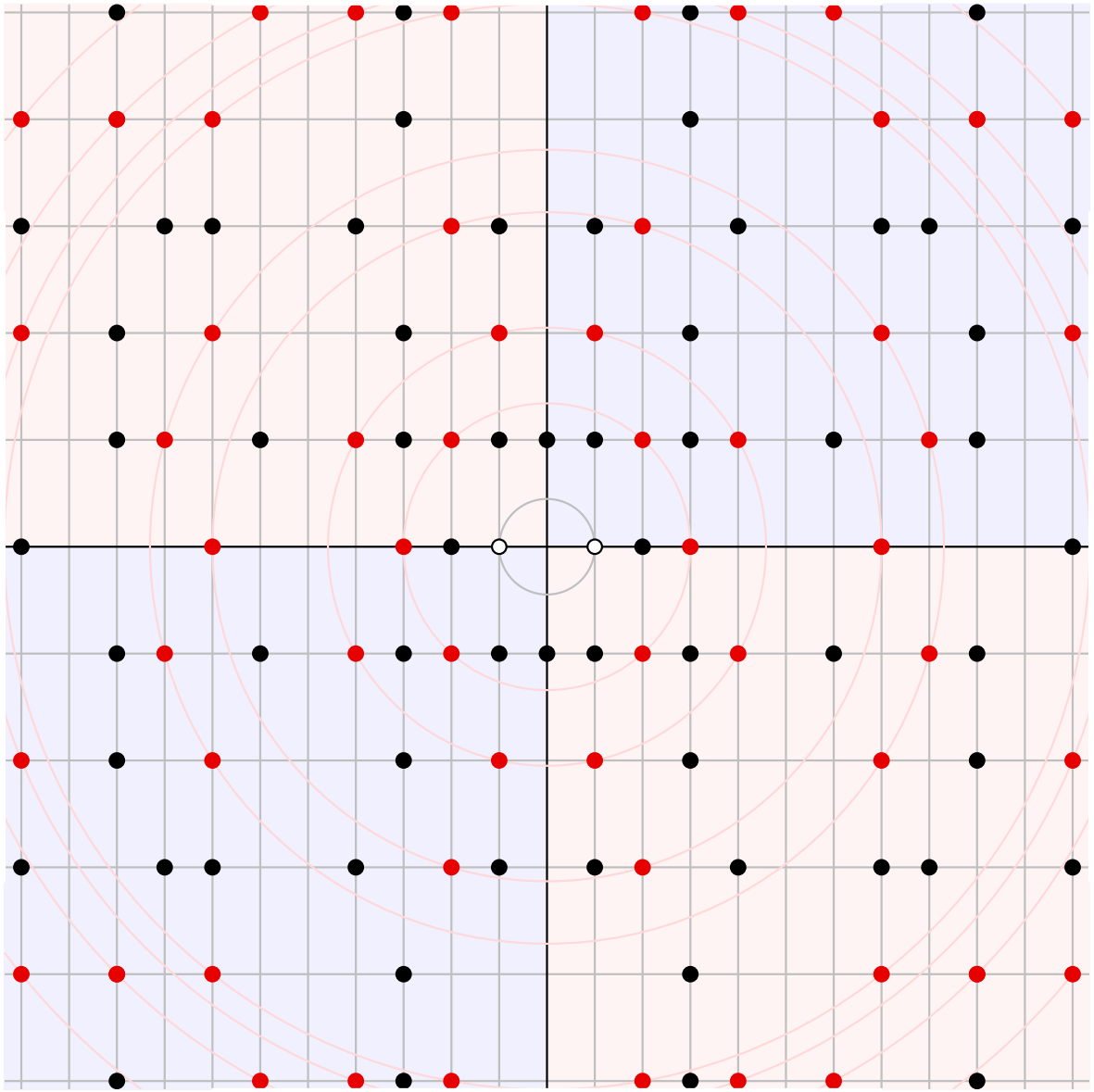
- ramified iff $\Delta \equiv 0, 4 \pmod{8}$.
- split iff $\Delta \equiv 1 \pmod{8}$.
- inert iff $\Delta \not\equiv 5 \pmod{8}$.

Remark

- If R_m is a PID and p splits, then it is reducible.
- If R_m is not a PID and p splits, then
  - p might be reducible, or
  - p could be a non-prime irreducible.

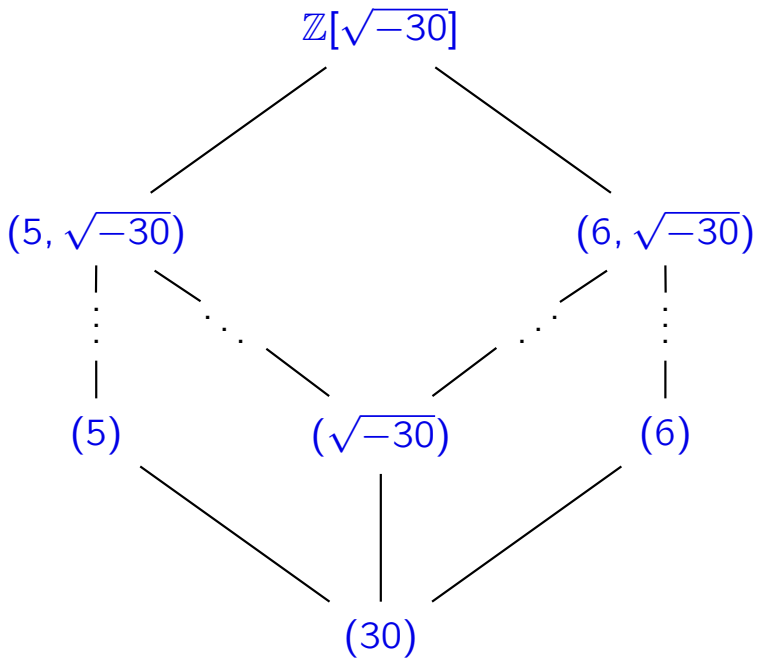
Primes in $R_{-5} = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$

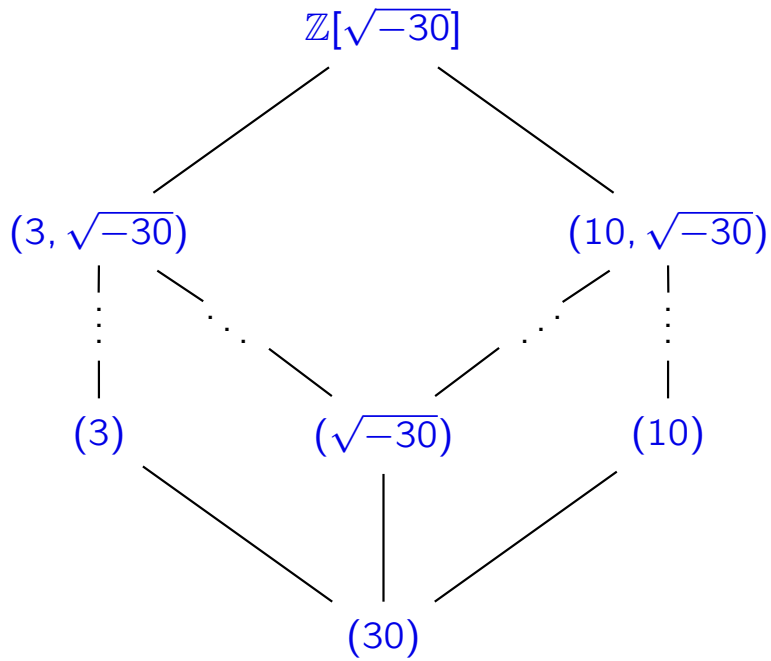
Units are white, primes are **black**, non-prime irreducibles are **red**.



The ideal class group

The degree to which unique factorization fails in R is measured by the class group, $\mathrm{Cl}(R)$.





Formally, two ideals I and J are equivalent if $\alpha I = \beta J$ for some $\alpha, \beta \in R$.

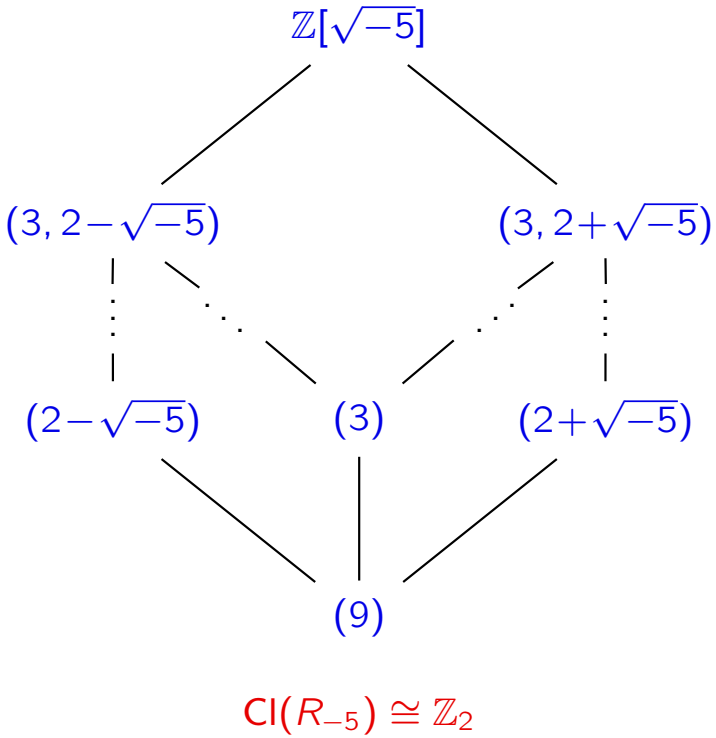
The equivalence classes form a group, under $[I] \cdot [J] := [IJ]$.

The identity element is the class of principal ideals, $[(1)]$.

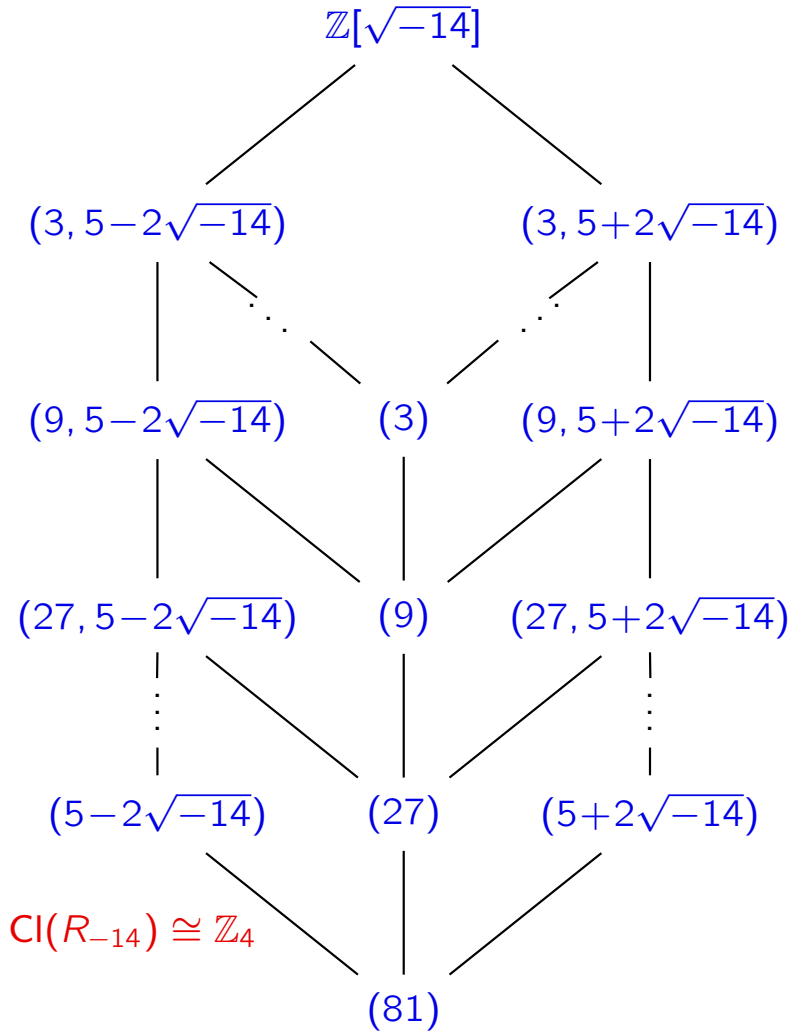
In the example above, $\mathrm{Cl}(R_{-30}) = \left\{(1),\ (2, \sqrt{-30}),\ (3, \sqrt{-30}),\ (5, \sqrt{-30})\right\} \cong \mathbb{Z}_2^2$.

The ideal class group

The degree to which unique factorization fails in R is measured by the class group, $\mathrm{Cl}(R)$.



$\mathrm{Cl}(R_{-5}) \cong \mathbb{Z}_2$



$\mathrm{Cl}(R_{-14}) \cong \mathbb{Z}_4$

Quadratic integers and norm-Euclidean domains

Proposition

If $m = -2, -1, 2, 3$, then R_m is Euclidean with $d(x) = |N(x)|$; ("norm-Euclidean").

Proof

Take $a, b \in R_m = \mathbb{Z}[\sqrt{m}]$, with $b \neq 0$. Let $a/b = s + t\sqrt{m} \in \mathbb{Q}(\sqrt{m})$.

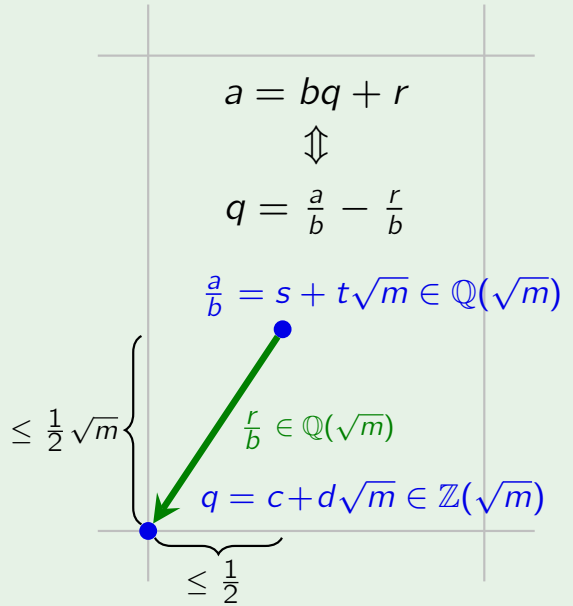
Pick $q = c + d\sqrt{m} \in R_m$, the nearest element to a/b.

Since $N(b) = N(r)N(b/r)$, we have

$$|N(r)| < |N(b)| \quad \Leftrightarrow \quad |N(r/b)| < |N(1)|$$

For each $m = -2, -1, 2, 3$:

$$-1 < N\left(\tfrac{r}{b}\right) = \underbrace{(c-s)^2}_{\leq \frac{1}{4}} - m\underbrace{(d-t)^2}_{\leq \frac{1}{4}} < 1.$$



Proposition (HW)

If $m = -3, -7, -11$, then $R_m = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ is norm-Euclidean.

PIDs that are not Euclidean

Theorem

The ring R_m is norm-Euclidean iff

$$m \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Theorem (D.A. Clark, 1994)

The rings R_{69} and R_{14} are Euclidean domains that are *not* norm-Euclidean.

The following degree function works for R_{69}, defined on the primes

$$d(p) = \begin{cases} |N(p)| & \text{if } p \neq 10 + 3\alpha \\ c & \text{if } p = 10 + 3\alpha \end{cases} \qquad \alpha = \frac{1 + \sqrt{69}}{2}, \quad c > 25 \text{ an integer.}$$

Theorem

If $m < 0$, then R_m is Euclidean iff $m \in \{-11, -7, -3, -2, -1\}$.

Theorem

If $m < 0$, then R_m is a PID iff $m \in \{\underbrace{-163, -67, -43, -19}_{\text{non-Euclidean}}, \underbrace{-11, -7, -3, -2, -1}_{\text{Euclidean}}\}$.

Algebraic integers (roots of monic polynomials)

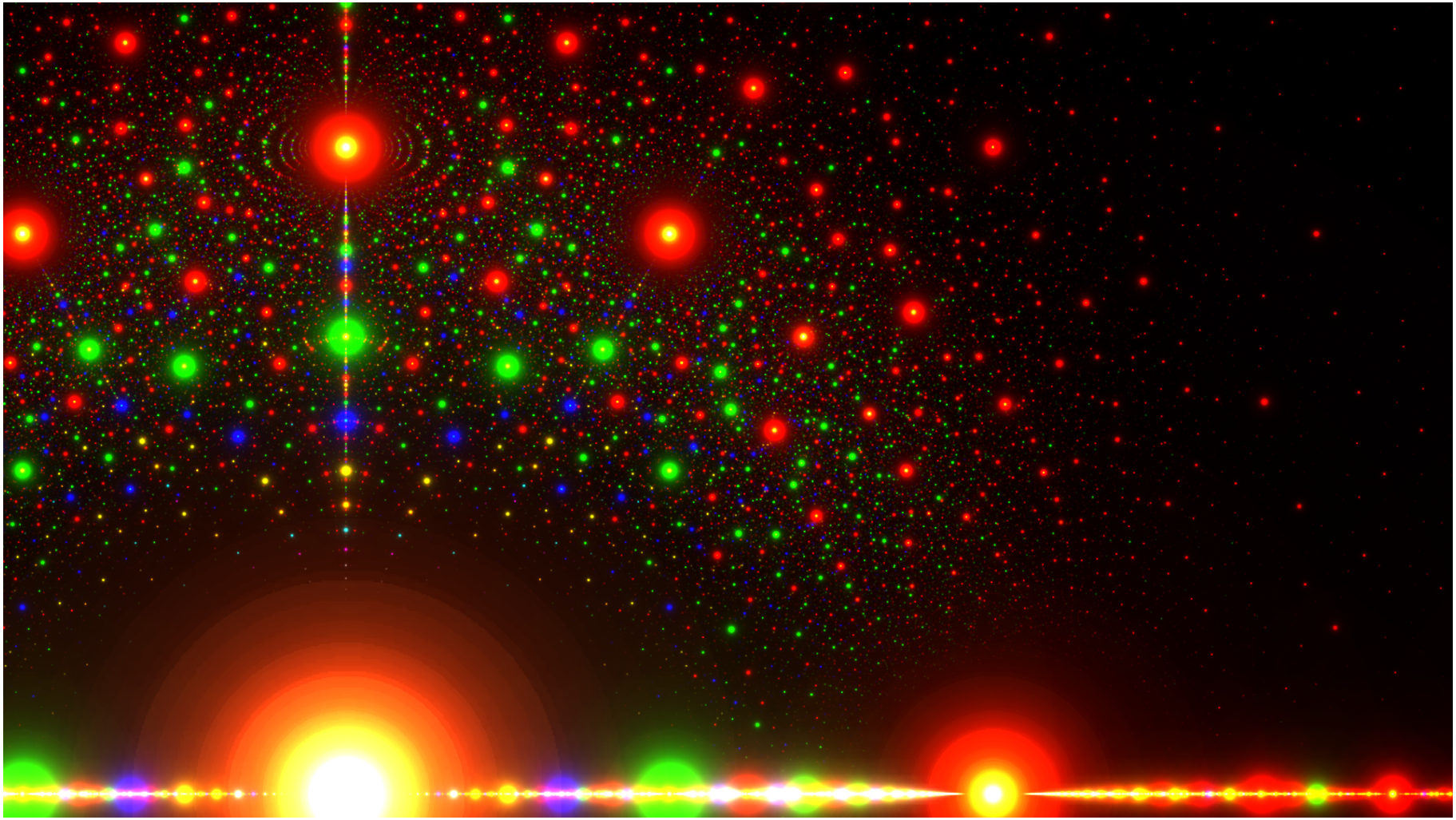


Figure: Algebraic numbers in $\mathbb{C}$. Colors indicate the coefficient of the leading term: red $= 1$ (algebraic integer), green $= 2$, blue $= 3$, yellow $= 4$. Large dots mean fewer terms and smaller coefficients. Image from Wikipedia (made by Stephen J. Brooks).

Algebraic integers (roots of monic polynomials)

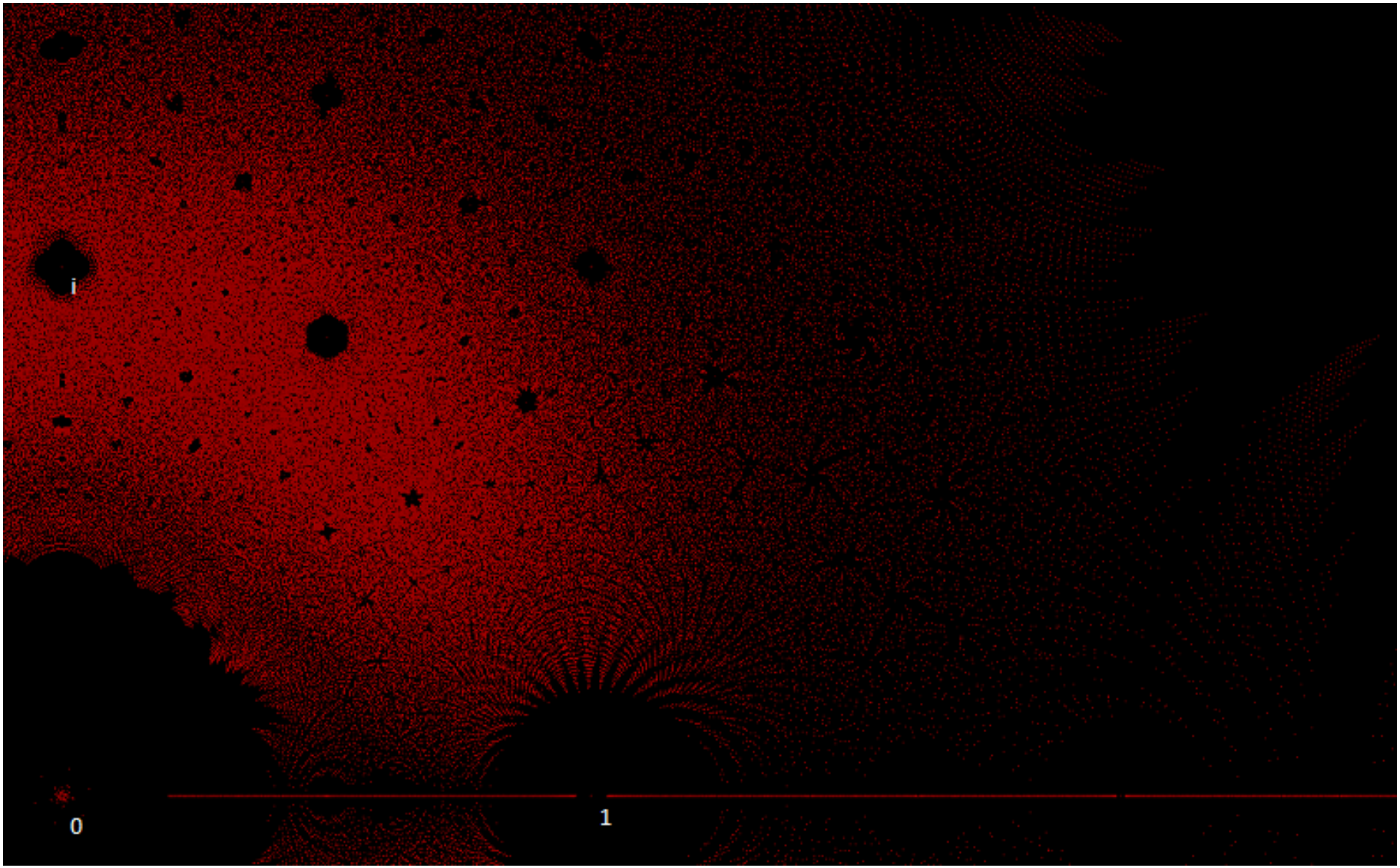
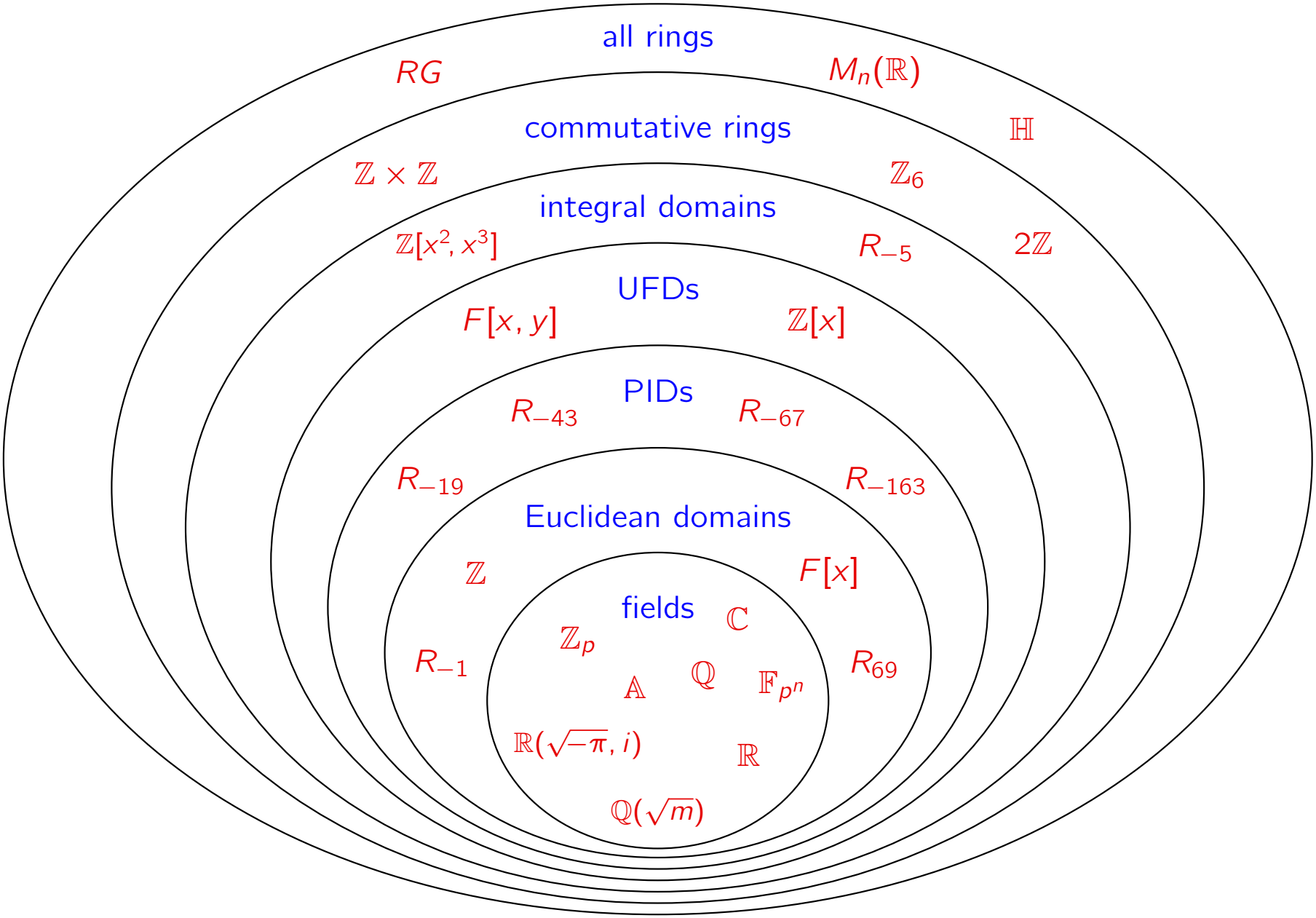


Figure: Algebraic integers in $\mathbb{C}$. Each red dot is the root of a monic polynomial of degree ≤ 7 with coefficients from $\{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$. From Wikipedia.

Summary of ring types



Sunzi's remainder theorem: motivating examples

Exercise 1

Find all solutions to the system $\begin{cases} 2x \equiv 5 \pmod 7 \\ 3x \equiv 4 \pmod 8 \end{cases}$

Since $2^{-1} = 4$ in $\mathbb{Z}_7$,

$$4(2x \equiv 5) \mod 7 \implies x \equiv 6 \mod 7 \implies x = 6 + 7t, \text{ for } t \in \mathbb{Z}.$$

Plug this into $3x \equiv 4 \pmod 8$:

$$3(6 + 7t) \equiv 4 \mod 8 \implies 5t \equiv 2 \mod 8 \implies 5(5t \equiv 2) \mod 8$$

and we get $t \equiv 2 \mod 8$, and hence $t = 2 + 8s$, for $s \in \mathbb{Z}$.

Backsubstituting $t = 2 + 8s$ yields

$$x = 6 + 7t = 6 + 7(2 + 8s) = 20 + 56s,$$

and thus $x \equiv 20 \pmod{56}$.

Exercise 2

Show that the following system has no solutions: $\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 6 \end{cases}$

Number theory version

Sunzi's remainder theorem

Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ be pairwise co-prime (that is, $\gcd(n_i, n_j) = 1$ for $i \neq j$). For any $a_1, \ldots, a_k \in \mathbb{Z}$, the system

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has a solution $x \in \mathbb{Z}$. Moreover, all solutions are congruent modulo $N = n_1 n_2 \cdots n_k$.

This can be generalized. To see how, first recall the following operations on ideals:

1. *Intersection*: $I \cap J = \{r \in R \mid r \in I \text{ and } r \in J\}$.
2. *Product*: $IJ = (ab \mid a \in I,\ b \in J) = \{a_1 b_1 + \cdots + a_k b_k \mid a_i \in I,\ b_j \in J\} \subseteq I \cap J$.
3. *Sum*: $I + J = \{a + b \mid a \in I,\ b \in J\}$.

Example: $R = \mathbb{Z}$, $I = (9) = 9\mathbb{Z}$, $J = (6) = 6\mathbb{Z}$.

1. *Intersection*: $(9) \cap (6) = (18)$ (lcm)
2. *Product*: $(9)(6) = (54)$ (product)
3. *Sum*: $(9) + (6) = (3)$ (gcd).

Sunzi's remainder theorem in a PID

In a PID, $\gcd(m, n) = 1$ iff $am + bn = 1$ for some $a, b \in \mathbb{Z}$.

Or equivalently, $(m) + (n) = \mathbb{Z}$.

Definition

Two ideals I, J of R are co-prime if $I + J = R$.

Sunzi's remainder theorem (2 ideals in a PID)

Let R be a PID, and $I + J = R$. Then for any $r_1, r_2 \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I} \\ x \equiv r_2 \pmod{J} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I \cap J$.

This just means that there is an element in both cosets, $r_1 + I$ and $r_2 + J$.

Sunzi's remainder theorem in a PID

Sunzi's remainder theorem (2 ideals in a PID)

Let R have 1 and $I + J = R$. Then for any $r_1, r_2 \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I} \\ x \equiv r_2 \pmod{J} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I \cap J$.

Proof

Write $1 = a + b$, with $a \in I$ and $b \in J$, and set $r = r_2 a + r_1 b$.

This works because

$$r - r_1 = (r - r_1 b) + (r_1 b - r_1) = r_2 a + r_1(b - 1) = r_2 a - r_1 a = (r_2 - r_1)a \in I$$

implies that $r \equiv r_1 \pmod{I}$, and

$$r - r_2 = (r - r_2 a) + (r_2 a - 1) = r_1 b + r_2(a - 1) = r_1 b - r_2 b = (r_1 - r_2)b \in J$$

means that $r \equiv r_2 \pmod{J}$. □

Sunzi's remainder theorem in a PID

Sunzi's remainder theorem (n ideals in a PID)

Let $I_1, \ldots, I_n$ be pairwise co-prime ideals of R. For any $r_1, \ldots, r_n \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad \vdots \\ x \equiv r_n \pmod{I_n} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I_1 \cap \cdots \cap I_n$.

Proof

Take $k = 1$. For $j = 2, \ldots, n$, write $1 = a_j + b_j$, where $a_j \in I_1$, $b_j \in I_j$. Then

$$\begin{aligned} 1 &= (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) \\ &= a_2\left[(a_3 + b_3) \cdots (a_n + b_n)\right] + b_2\left[(a_3 + b_3) \cdots (a_n + b_n)\right] \in I_1 + \prod_{j=2}^{n} I_j = R. \end{aligned}$$

Now apply the SRT for 2 ideals to the system $\begin{cases} x \equiv 1 \pmod{I_1} \\ x \equiv 0 \pmod{\prod_{j \neq 1} I_j}. \end{cases}$

Let $\mathbf{s_1} \in \mathbf{R}$ be a solution. Next, we'll find solutions $s_2, \ldots, s_n$ to related systems.

Sunzi's remainder theorem in a PID

Sunzi's remainder theorem (n ideals in a PID)

Let R have 1 and $I_1, \ldots, J_n$ be pairwise co-prime ideals. Then for any $r_1, \ldots, r_n \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad \vdots \\ x \equiv r_n \pmod{I_n} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I_1 \cap \cdots \cap I_n$.

Proof (cont.)

Fix $k \in \{2, \ldots, n\}$. For $j = 1, \ldots, \cancel{k}, \ldots, n$, write $1 = a_j + b_j$, where $a_j \in I_k$, $b_j \in I_j$. Then

$$1 = (a_2 + b_2) \cdots \cancel{(a_k + b_k)} \cdots (a_n + b_n) \in I_k + \prod_{j \neq k} I_j = R.$$

Now apply the SRT for 2 ideals to the system $\begin{cases} x \equiv 1 \pmod{I_k} \\ x \equiv 0 \pmod{\prod_{j \neq 1} I_j} \end{cases}$

Let $s_k \in R$ be a solution, and consider our solutions $s_1, \ldots, s_n$.

Sunzi's remainder theorem in a PID

Sunzi's remainder theorem (n ideals in a PID)

Let R have 1 and $I_1, \ldots, J_n$ be pairwise co-prime ideals. Then for any $r_1, \ldots, r_n \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad \vdots \\ x \equiv r_n \pmod{I_n} \end{cases}$$

has a solution $r \in R$. Moreover, any two solutions are congruent modulo $I_1 \cap \cdots \cap I_n$.

Proof (cont.)

By construction, $s_k \in \pmod{\prod_{j \neq k} I_j}$, and so $s_k \in I_j$ for all $j \neq k$.

We have $s_k \equiv 1 \pmod{I_k}$ and $s_k \equiv 1 \pmod{I}_j$ for $j \neq k$.

Set $\mathbf{r = r_1 s_1 + \cdots + r_n s_n}$. It is easy to see that this works.

If $s \in R$ is another solution, then $s \equiv r_j \equiv r \pmod{I_j}$, for $j = 1, \ldots, n$, and so

$$s \equiv r \mod \bigcap_{j=1}^{n} I_j.$$

Applications

When is $\mathbb{Z}_n$ isomorphic to a product?

Let $R = \mathbb{Z}$ and $I_j = (m_j)$, for $j = 1, \ldots, n$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$. Then

$$I_1 \cap \cdots \cap I_n = (m_1 m_2 \cdots m_n), \qquad \text{and} \qquad \mathbb{Z}_{m_1 m_2 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}.$$

Corollary

Factor $n = p_1^{d_1} \cdots p_n^{d_n}$ into a product of distinct primes. Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{{p_1}^{d_1}} \times \cdots \times \mathbb{Z}_{{p_n}^{d_n}}.$$

Remark

If R is a Euclidean domain, then the proof of the SRT is *constructive*.

Specifically, we can use the Euclidean algorithm to write

$$c_k m_k + d_k \prod_{j \neq k} m_j = \gcd\left(m_k, \prod_{j \neq k} m_j\right) = 1, \quad \text{where} \quad I_j = (m_j).$$

Then, set $s_k = d_k \prod_{j \neq k} m_j$, and $r = r_1 s_1 + \cdots + r_n s_n$ is the solution.

Sunzi's remainder theorem in an arbitrary ring

Theorem

Let $I_1, \ldots, I_n$ be pairwise co-prime (two-sided) ideals of a ring R. Then the following map is an isomorphism:

$$R/(I_1 \cap \cdots \cap I_n) \longrightarrow (R/I_1) \times \cdots \times (R/I_n), \qquad x \longmapsto (x \mod I_1, \ldots, x \mod I_n).$$

If R is commutative, then $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$.

Rings of polynomials and formal power series

For a fixed $n \in \mathbb{Z}$, consider the polynomials of degree $\leq n$:

$$R = \left\{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Z} \right\}.$$

This is a ring, and a vector space, and there is a natural isomorphism

$$R \longrightarrow \mathbb{Z} \times \cdots \times \mathbb{Z} \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}, \qquad a_0 + a_1 x + \cdots a_n x^n \longmapsto (a_0, a_1, \ldots, a_n)$$

Now, consider two "infinite-dimensional" verions of this:

$$\mathbb{Z}[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Z},\ n \in \mathbb{Z} \right\}, \qquad \mathbb{Z}[[x]] = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots \mid a_i \in \mathbb{Z} \right\}.$$

These are naturally isomorphic to the direct sum

$$\bigoplus_{i=1}^{\infty} \mathbb{Z} \cong \left\{ \sum_{i=1}^{n} a_i \mathbf{e}_i \mid a_i \in \mathbb{Z},\ n \geq 1 \right\}$$
$$\cong \left\{ (a_1, a_2, a_3, \ldots) \mid a_i \in \mathbb{Z},\ \text{all but finitely many } a_j \text{ are zero} \right\}$$

and direct product,

$$\prod_{i=1}^{\infty} \mathbb{Z} := \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots = \left\{ (a_1, a_2, a_3, \ldots) \mid a_i \in \mathbb{Z} \right\},$$

respectively.

Polynomial rings, formalized

Let $P(R) \cong \bigoplus_{i=1}^{\infty} R$ be the set of sequences over R, with all but finitely many entries 0.

Write $a = (a_i) = (a_0, a_1, a_2, \dots)$, and define the binary operations as

$$a + b = (a_i + b_i)$$

$$ab = \left(\sum_{j=0}^{i} a_j b_{i-j} \right) = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_0 b_2 + a_1 b_1 + a_2 b_0,\ \dots)$$

Proposition (exercise)

If R is a ring, then $P(R)$ is a ring. It is commutative iff R is, and it has 1 iff R does, in which case $1_{P(R)} = (1_R, 0, 0, \dots)$.

Henceforth, assume R is commutative with 1.

Defining $x = (0, 1, 0, 0, \dots) \in P(R)$, note that

$$x^2 = (0, 0, 1, 0, 0, \dots), \qquad x^3 = (0, 0, 0, 1, 0, \dots) \in P(R),$$

and thus we define $x^0 := 1_{P(R)}$.

Polynomial rings, formalized

The embedding

$$R \hookrightarrow P(R), \qquad a \longmapsto (a, 0, 0, \dots)$$

identifies R with a subring of $P(R)$, with $1_R = 1_{P(R)}$. Now, we may write

$$a = (a_0, a_1, a_2, \dots) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

for each $a \in P(R)$.

We call x an indeterminate, and write $R[x] = P(R)$.

Most definitions are predictable:

- write $f(x)$ for $a \in R[x]$, called a polynomial with coefficients in R.
- if $a_n \neq 0$ but $a_m = 0$ for all $m > n$, then $f(x)$ has degree n, and leading coefficient a_n.
- if $f(x)$ has leading coefficient 1, it is monic.
- The zero polynomial $0 := (0, 0, \dots)$ has degree $-\infty$.
- Polynomials of non-positive degree are constants.

We can construct the ring $R[[x]]$ of formal power series similarly, using $\prod_{i=1}^{\infty} R$ instead of $\bigoplus_{i=1}^{\infty} R$.

Single variable polynomials

The following are immediate from the definition of $R[x]$.

Proposition

Let R be a ring with 1, and $f, g \in R[x]$. Then

1. $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$, and
2. $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.

Moreover, equality holds in (b) if R has no zero divisors.

Corollary 1

If R has no zero divisors, then $f(x) \in R[x]$ is a unit iff $f(x) = r$ with $r \in U(R)$.

Corollary 2

$R[x]$ is an integral domain iff R is an integral domain.

The division algorithm

Proposition

Suppose $f, g \in R[x]$ with $g(x)$ having leading coefficient $b \in R$. Then there exists $k \geq 0$ and $q(x), r(x) \in R[x]$ such that

$$b^k f(x) = q(x)g(x) + r(x), \qquad \deg r(x) < \deg g(x).$$

If b is not a zero divisor, then $q(x)$ and $r(x)$ are unique. If $b \in U(R)$, we may take $k = 0$.

The polynomials $q(x)$ and $r(x)$ are called the quotient and remainder.

Proof (details done on board)

Non-trival case: $\deg f(x) = m \geq \deg g(x) = n$.

Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $g(x) = b_0 + \cdots + b_n x^n$, (let $a = a_m$, $b = b_n$).

Induct on m, with the degree $< m$ polynomial $f_1(x) := bf(x) - ax^{m-n}g(x)$.

Write $b^{k-1} f_1(x) = p(x)g(x) + r(x)$, and plug into $b^k f(x) = b^{k-1} \cdot bf(x)$. □

The division algorithm also holds when R is not commutative, as long as b is a unit.

Substitution

Henceforth, R and S are assumed to be commutative with 1.

Theorem

Suppose $\theta\colon R \to S$ is a homomorphism with $\theta(1_R) = 1_S$ and $a \in S$. Then there exists a unique evaluation map $E_a\colon R[x] \to S$ such that

(i) $E_a(r) = \theta(r)$, for all $r \in R$,

(ii) $E_a(x) = a$.

Though θ need not be 1–1, it is usually the canonical inclusion. In this case,

$$E_a(f(x)) = r_0 + r_1 a + \cdots + r_n a^n,$$

which we call $f(a)$. The image of E_a is $R[a] = \{f(a) \mid f(x) \in R[x]\}$.

Remainder theorem

Suppose R is commutative with unity, $f(x) \in R[x]$, and $a \in R$. Then the remainder of $f(x)$ divided by $g(x) = x - a$ is $r = f(a)$.

Proof

Write $f(x) = q(x)(x - a) + r$, and substitute a for x. □

Algebraic and transcendental elements

Corollary: Factor theorem

Suppose R is commutative with unity, $f(x) \in R[x]$, $a \in R$, and $f(a) = 0$. Then $x - a$ is a factor of $f(x)$, i.e., $f(x) = q(x)(x - a)$ for some $q(x) \in R[x]$.

Note that this *fails* if:

- R is not commutative: recall $f(x) = x^2 + 1$ in $\mathbb{H}[x]$.
- R does not have 1: consider $2x^2 + 4x + 2$ in $2\mathbb{Z}[x]$.

Definition

If $R \subseteq S$ with $1_R = 1_S$, then $a \in S$ is algebraic over R if $f(a) = 0$ for some nonzero $f(x) \in R[x]$, and transcendental otherwise.

Remark

$a \in S$ is algebraic over R iff E_a is not 1–1.

Primitive elements and Gauss' lemma

Let I be an ideal of a commutative ring R with 1. The canonical quotient map

$$\pi\colon R \longrightarrow \bar{R} := R/I, \qquad \pi\colon r \longmapsto \bar{r} := r + I$$

defines a homomorphism

$$R[x] \longrightarrow \bar{R}[x], \qquad f(x) : a_0 + a_1 x + \cdots + a_n x^n \;\longmapsto\; \bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$$

called the reduction of coefficients modulo I.

Definition

If R is a UFD, then the content of a polynomial $f(x)$ in $R[x]$ is the GCD of its coefficients (defined up to associates).

If the content is 1, then $f(x)$ is primitive.

Lemma (Exercise)

If $\deg f(x) = n$ and $\deg g(x) = m$ in $\mathbb{F}[x]$, then

$$f(x)g(x) = x^{n+m} \qquad \Longrightarrow \qquad f(x) = x^n \quad \text{and} \quad g(x) = x^m.$$

Primitive elements and Gauss' lemma

Gauss' lemma

Let R be a UFD. If $f(x), g(x) \in R[x]$ are primitive, then so is $f(x)g(x)$.

Proof (contrapositive)

Suppose a prime $p \in R$ divides all coeficients of $f(x)g(x)$.

Reducing coefficients modulo $I = (p)$ sends $f(x)g(x) \mapsto \bar{0}$ in $\bar{R}[x]$.

But since $I = (p)$ is a prime ideal, $\bar{R} = R/I$ is an integral domain, hence $\bar{R}[x]$ is too.

Thus,

$$\overline{f(x)} \cdot \overline{g(x)} = \bar{0} \quad \Longrightarrow \quad \overline{f(x)} = \bar{0} \text{ or } \overline{g(x)} = \bar{0}.$$

Primitive elements

Proposition

Suppose R is a UFD with field of fractions $F = F_R$. Suppose $f(x)$ and $g(x)$ are primitive in $R[x]$, but associates in $F[x]$. Then they are associates in $R[x]$.

Proof

Since $f(x)$ and $g(x)$ are associates, then $f(x) = ag(x)$ for some $a \in U(F[x]) = F^\times$.

Write $a = b/c$, for some $b, c \in R$, so $cf(x) = bg(x) \in R[x]$.

Since $f(x)$ and $g(x)$ are primitive, the content of $cf(x)$ and $bg(x)$ are c and b.

Thus $b \sim c$ in R, and so $a = b/c$ is a unit in R.

This means that $f(x) \sim g(x)$ in $R[x]$. $\square$

Primitive elements

Proposition

Let R be a UFD and $F = F_R$ its field of fractions. If $f(x)$ is irreducible in $R[x]$, then it is irreducible in $F[x]$.

Proof

Since $f(x)$ is irreducible in $R[x]$, it is primitive.

Suppose $f(x) = f_1(x)f_2(x) \in R[x]$ with $\deg(f_i(x)) > 0$.

Write $f_i(x) = a_i g_i(x)$, with $a_i \in F$ and $g_i(x)$ primitive, and so

$$f(x) = a_1 a_2 g_1(x)_2 g(x),$$

so $f(x) \sim g_1(x)g_2(x)$ in $F[x]$.

By Gauss' lemma, $g_1(x)g_2(x)$ is primitive.

Since $f(x) \sim g_1(x)g_2(x)$ in $F[x]$, they are associates in $R[x]$ as well.

This means that $f(x) = ug_1(x)g_2(x)$ for some $u \in U(R)$, contradicting irredicibility of $f(x)$.

An irreducibility test

Eisenstein criterion

Consider a polynomial $$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x].$$

over a PID. If there is a prime $p \in P$ such that:

1. $p \mid a_i$ for all $i < n$
2. $p \nmid a_n$,
3. $p^2 \nmid a_0$,

then $f(x)$ is irreducible.

Proof

Suppose $f(x)$ factors as a product of non-units, $f(x) = g(x)h(x)$, where

$$g(x) = b_0 + b_1 x + \cdots + b_k x^k, \quad \text{and} \quad h(x) = c_0 + c_1 x + \cdots + c_\ell x^\ell$$

Assume that $f(x)$ is primitive, so $\deg g(x) = k > 0$ and $\deg h(x) = \ell > 0$.

Reducing coefficients modulo $I = (p)$ leaves the monomial

$$\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x) = \bar{b}_k \bar{c}_\ell x^{k+\ell} = \bar{a}_n x^n \in \bar{R}[x].$$

By the lemma, $\bar{g}(x) = \bar{b}_k x^k$ and $\bar{h}(x) = \bar{c}_\ell x^\ell$. Note that

$$\bar{b}_0 = \bar{c}_0 = 0 \quad \Longrightarrow \quad p \mid b_0 \text{ and } p \mid c_0 \quad \Longrightarrow \quad p^2 \mid b_0 c_0 = a_0.$$

Polynomials in several indeterminates

Let $I = \{0, 1, 2, 3, \ldots, \}$ and $I^n = I \times \cdots \times I$ (n copies).

Informally, think of element of I^n as "exponent vectors" of monomials, e.g.,

$$(0, 3, 4) \text{ corresponds to } x_1^0 x_2^3 x_3^4.$$

Write 0 for $(0, \ldots, 0) \in I^n$. Addition on I^n is defined component-wise.

Over a fixed ring R, polynomials can be encoded as functions

$$P_n(R) = \{a \colon I^n \to R \mid a(x) = 0 \text{ all but finitely many } x \in I^n\}$$

Note that elements in $P_n(R)$ specify the coefficients of monomials, e.g.,

$$a(0, 3, 4) = -6 \quad \text{corresponds to} \quad -6x_1^0 x_2^3 x_3^4.$$

For example, in $\mathbb{Z}[x_1, x_2, x_3]$, the polynomial $f(x_1, x_2, x_3) = -6x_1^0 x_2^3 x_3^4 + 12x_1^5 - 9$ is

$$a(i_1, i_2, i_3) = \begin{cases} -6 & (i_1, i_2, i_3) = (0, 3, 4) \\ 12 & (i_1, i_2, i_3) = (5, 0, 0) \\ -9 & (i_1, i_2, i_3) = (0, 0, 0) \\ 0 & \text{otherwise.} \end{cases}$$

Polynomials in several indeterminates

Functions in $P_n(R)$ are added componentwise, and multiplied as

$$(ab)(i) := \sum \{a(j)b(k) \mid j,k \in I^n,\ j+k=i\}, \qquad a,b \in P_n(R), \quad i \in I^n.$$

The following is straightforward but tedious.

Proposition

$P_n(R)$ is a ring. It is commutative iff R is, and has 1 iff R does.

Each $r \in R$ defines a constant polynomial via a function $a_r \in P_n(R)$, where

$$a_1 : I^n \longrightarrow R, \qquad a_r(i) = \begin{cases} r & i = (0,\ldots,0) \\ 0 & \text{otherwise.} \end{cases}$$

Note that the identity function is $1 := a_1 \in P_n(R)$.
It is easy to check that $a_r + a_s = a_{r+s}$ and $a_r a_s = a_{rs}$, and so the map

$$R \longrightarrow P_n(R), \qquad r \longmapsto a_r$$

is 1–1. As such, we may identify r with $a_r \in P_n(R)$ and view R as a subring of $P_n(R)$.

Polynomials in several indeterminates

If R has 1, then let

$$e_k := (0, 0, \ldots, 0, \underbrace{1}_{\text{pos. } i}, 0, \ldots, 0) \in I^n.$$

Define the indeterminates $x_k \in P_n(R)$ as

$$x_k(i) = \begin{cases} 1 & i = e_k \\ 0 & \text{otherwise.} \end{cases}$$

Often, if $n = 2$ or 3, we use $x = x_1$, $y = x_2$, $z = x_3$, etc.

Note that

$$x_k^2(i) = \begin{cases} 1 & i = 2e_k \\ 0 & \text{otherwise,} \end{cases} \qquad x_k^m(i) = \begin{cases} 1 & i = me_k \\ 0 & \text{otherwise.} \end{cases}$$

(Secretly: $(1, 0, \ldots, 0) \mapsto x_1^1 x_2^0 \cdots x_n^0 = x_1$ and $(m, 0, \ldots, 0) \mapsto x_1^m x_2^0 \cdots x_n^0 = x_1^m$.)

It is easy to check that $x_i x_j = x_j x_i$ (i.e., these commute as functions $I^n \to R$).

Every $a \in P_n(R)$ can be written uniquely using functions with one-point support, which are called monomials.

Polynomials in several indeterminates

The degree of $a = rx_1^{i_1} \cdots x_n^{i_n}$ is $\deg a = i_1 + \cdots + i_n$.

If a is a sum of monomials, then say $\deg = \max\{\deg a_i \mid 1 \leq i \leq m\}$.

Also, say that $\deg 0 = -\infty$, and if all a_i's have the same degree, then $a \in P_n(R)$ is homogeneous.

The elements of $P_n(R)$ are called polynomials in the n commuting indeterminates $x_1, \ldots, x_n$.

We write $R[x_1, \ldots, x_n]$ for $P_n(R)$ and denotes elements by $f(x_1, \ldots, x_n)$, etc.

Often we write $x := (x_1, \ldots, x_n)$ and $f(x) := f(x_1, \ldots x_n)$.

Proposition

Let R be a ring with 1 and $f(x), g(x) \in R[x_1, \ldots, x_n]$. Then

(a) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$,

(b) $\deg(f(x)g(x)) \leq \deg f(x) \cdot \deg g(x)$.

Moreover, equality holds in (b) if R has no zero divisors.

Substitution for multivariable polynomials

Theorem

Suppose $\theta\colon R \to S$ is a homomorphism with $\theta(1_R) = 1_S$ and $a = (a_1, \ldots, a_n) \in S^n$. Then there exists a unique evaluation map $E_a\colon R[x] \to S$ such that

(i) $E_a(r) = \theta(r)$, for all $r \in R$,

(ii) $E_a(x_i) = a_i$, for all $i = 1, \ldots, n$.

Proof (sketch)

Define $E(rx_1^{j_1} \cdots x_n^{j_n}) = \theta(r)a_1^{j_1} \cdots a_n^{j_n}$ for monomials; extend naturally to polynomials.

Remarks

1. If θ is 1–1, then E_a "substitutes" elements from S in place of the x_i's, by

$$f(x_1, \ldots, x_n) \overset{E_a}{\longmapsto} f(a_1, \ldots, a_n).$$

2. This is easily extended to an arbitrary number of variables.
3. We could have defined $R[x_1, \ldots, x_n]$ abstractly via a universal mapping property.
4. Another construction: Define $R[x_1, x_2] = (R[x_1])[x_2]$, etc.

Substitution for multivariable polynomials

Definition

Elements $a_1, \ldots, a_n \in S$ are algebraically dependent over R if $f(a_1, \ldots, a_n) = 0$ for some nonzero $f(x) \in R[x_1, \ldots, x_n]$.

Otherwise, they are algebraically independent over R.

Examples

1. $a_1 = \sqrt{3}$, $a_2 = \sqrt{5}$ are algebraically dependent over $\mathbb{Z}$. Consider $f(x, y) = (x^2 - 3)(y^2 - 5)$.
2. $a_1 = \sqrt{\pi}$, $a_2 = 2\pi + 1$ are algebraically dependent over $\mathbb{Z}$. Consider $f(x, y) = 2x^2 - y + 1$.
3. It is "unknown" whether $a_1 = \pi$, $a_2 = e$ are algebraically dependent over $\mathbb{Z}$.

Remarks

1. $a \in S$ algebraically independent over $R \iff a$ transcendental over R.
2. $a_1, \ldots, a_n \in S$ algebraically indep. over $R \implies a_1, \ldots, a_n$ transcendental over R.

Multivariate polynomials rings over a UFD

Theorem

If R is a UFD, then $R[x_1, \ldots, x_n]$ is as well.

Proof

Since $R[x_1, \ldots, x_n] \cong (R[x_1, \ldots, x_{n-1}])[x_n]$, it suffices to take $n = 1$. We need to show:

(i) Each nonzero nonunit $f(x) \in R[x]$ is a product of irreducibles. (simple induction)

(ii) Every irreduible is prime.

(ii): Suppose $f(x)$ is irreducible and $f(x) \mid g(x)h(x)$ in $R[x]$.

Then $f(x)$ is irreducible in $F[x]$, a UFD, so it is prime there as well.

WLOG, suppose $f(x) \mid g(x)$ in $F[x]$, with $g(x) = f(x)k(x)$ for some $k(x) \in F[x]$. Write

$$g(x) = ag_1(x) = (b/c)f(x)k_1(x),$$

with $g_1(x)$ and $k_1(x)$ primitive in $R[x]$, hence

$$g_1(x) \sim f(x)k_1(x) \text{ in } F[x] \overset{\text{Gauss}}{\Longrightarrow} f(x)k_1(x) \text{ primitive} \overset{\text{Prop}}{\Longrightarrow} g_1(x) \sim f(x)k_1(x) \text{ in } R[x]$$

Writing $g_1(x) = uf(x)k_1(x)$ for some $u \in U(R)$ shows $f(x) \mid g_1(x) \mid g(x) \in R[x]$. $\square$

Hilbert's basis theorem

If a 0 exponent occurs in a monomial, we suppress writing the indeterminate.

For example, $5x_1^0x_2^1x_3^0x_4^8 = 5x_2x_4^8$. By doing this, we can consider

$$R[x_1] \subseteq R[x_1, x_2] \subseteq R[x_1, x_2, x_3] \subseteq \cdots$$

We write

$$R[x_1, x_2, x_3, \ldots] = \bigcup_{i=1}^{\infty} R[x_1, \ldots, x_k].$$

Not surprisingly, this ring has non-finitely generated ideals, e.g., $I = (x_1, x_2, \ldots)$.

Perhaps surprisingly, this is *not* the case in $R[x_1, \ldots, x_n]$.

Hilbert's basis theorem

If R is a Noetherian ring, then $R[x_1, \ldots, x_n]$ is Noetherian as well.

It suffices to prove this for $n = 1$, because

$$R[x_1, \ldots, x_{n-1}, x_n] \cong (R[x_1, \ldots, x_{n-1}])[x_n].$$

Proof of Hilbert's basis theorem

Given an ideal $I \subseteq R[x]$, and $m \geq 0$, define

$$I(m) = \{\text{coeffs. of degree-}m\text{ polynomials in } I\} \cup \{0\}.$$

$$\begin{array}{ccccccccccc}
 & & & & & & \vdots & & \vdots & & \\
 & & & & & & \| & & \| & & \\
 & & & & & \cdots & \mathbf{I_r(s)} & = & \mathbf{I_r(s{+}1)} & = & \cdots \\
\vdots & & \vdots & & & & \vdots & & & & \\
\cup & & \cup & & & & \cup & & & & \\
\mathbf{I_2(0)} & \subseteq & \mathbf{I_2(1)} & \subseteq & \cdots & \subseteq & \mathbf{I_2(s{-}1)} & \subseteq & \mathbf{I_2(s)} & \subseteq & \cdots \\
\cup & & \cup & & & & \cup & & & & \\
\mathbf{I_1(0)} & \subseteq & \mathbf{I_1(1)} & \subseteq & \cdots & \subseteq & \mathbf{I_1(s{-}1)} & \subseteq & \mathbf{I_1(s)} & \subseteq & \cdots \\
\cup & & \cup & & & & \cup & & & & \\
\mathbf{I_0(0)} & \subseteq & \mathbf{I_0(1)} & \subseteq & \cdots & \subseteq & \mathbf{I_0(s{-}1)} & \subseteq & \mathbf{I_0(s)} & \subseteq & \cdots
\end{array}$$

Proof of Hilbert's basis theorem

Lemma

Let $I \subseteq J$ be ideals of $R[x]$. If $I(m) = J(m)$ for all m, then $I = J$.

Proof

If not, then pick $f(x) \in J - I$ of minimal degree $m > 0$.

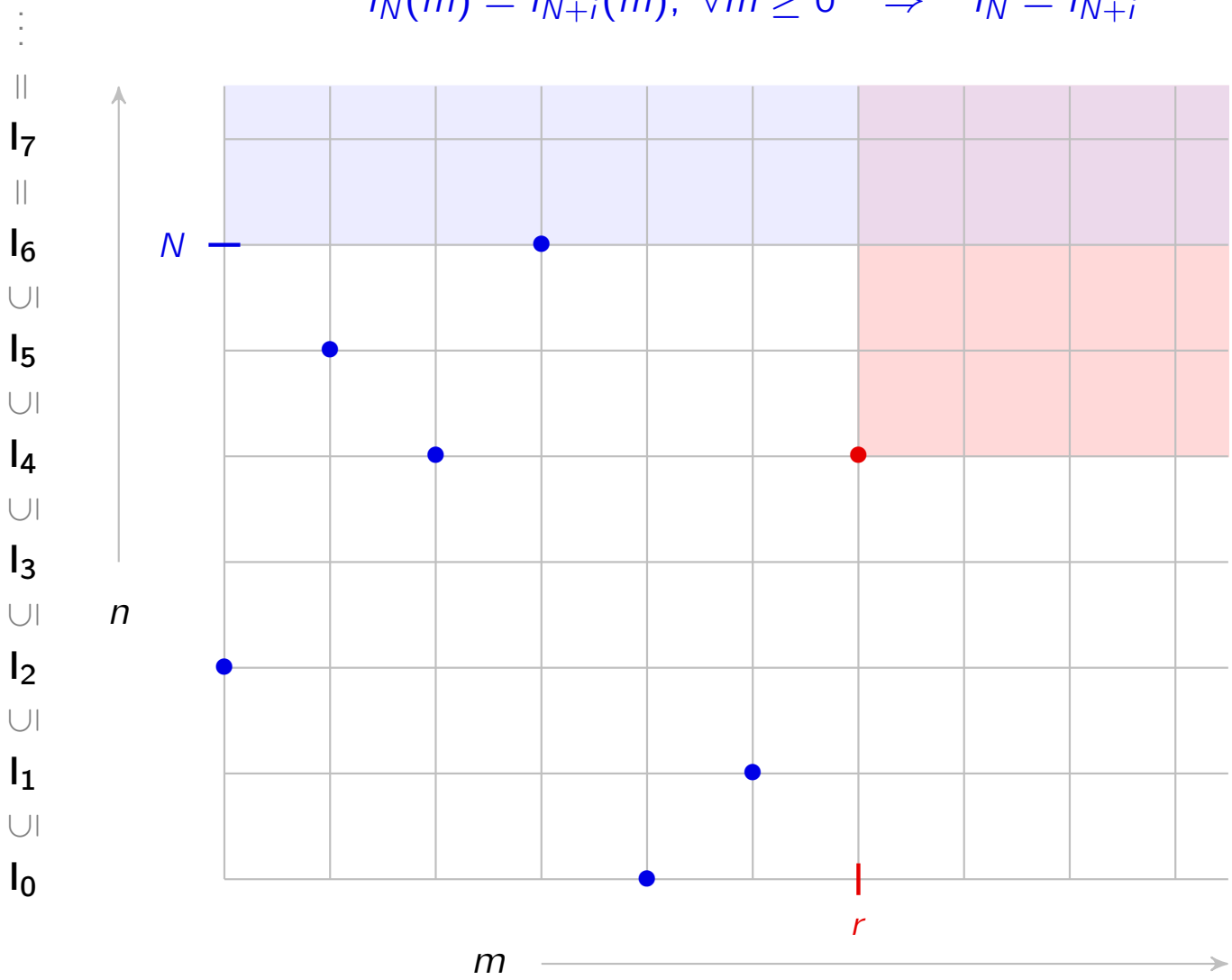
Since $I(m) = J(m)$, there is some $g(x) \in I$ of degree m with the same coefficient.

Then $f(x) - g(x)$ is in $J - I$ with smaller degree. $\square$

Proof of Hilbert's basis theorem

Let $n_m =$ where the sequence $I_n(m) \subseteq I_{n+1}(m) \subseteq \cdots$ stabilizes, and $N = \max_{m=1,\ldots,s} \{n_m\}$.

$$I_N(m) = I_{N+i}(m),\ \forall m \geq 0 \quad \Rightarrow \quad I_N = I_{N+i}$$



A counterexample to Hilbert's basis theorem?

Let $R = 2\mathbb{Z}$, and recall the polynomial ring

$$\begin{aligned} R = 2\mathbb{Z}[x] &= \left\{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in 2\mathbb{Z},\ n \in \mathbb{N} \right\} \\ &= \left\{ 2c_0 + 2c_1 x + \cdots + 2c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \right\}, \end{aligned}$$

with the following ideals:

$$(2) = \left\{ 2c_0 + 4c_1 x + \cdots + 4c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \right\},$$

$$(2, 2x) = \left\{ 2c_0 + 2c_1 x + 4c_2 x^2 + \cdots + 4c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \right\},$$

$$(2, 2x, 2x^2) = \left\{ 2c_0 + 2c_1 x + 2c_2 x^2 + 4c_3 x^3 + \cdots + 4c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \right\}.$$

We now have an ascending sequence of ideals that does not terminate:

$$(2) \subsetneq (2, 2x) \subsetneq (2, 2x, 2x^2) \subsetneq (2, 2x, 2x^2, 2x^3) \subsetneq \cdots .$$