

## Section 7: Ring theory

Matthew Macauley

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

Math 4120, Modern Algebra

# What is a ring?

## Definition

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

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

## Remarks

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

## A few more terms

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."

A **subring** of  $R$  is a subset  $S \subseteq R$  that is also a ring.

# What is a ring?

## Examples

1.  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$  are all commutative rings with 1.
2.  $\mathbb{Z}_n$  is a commutative ring with 1.
3. 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.
4. For any ring  $R$ , the set of functions  $F = \{f: R \rightarrow R\}$  is a ring by defining

$$(f + g)(r) = f(r) + g(r), \quad (fg)(r) = f(r)g(r).$$

5. The set  $S = 2\mathbb{Z}$  is a subring of  $\mathbb{Z}$  but it does *not* have 1.
6.  $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}$  is a subring of  $R = M_2(\mathbb{R})$ . However, note that

$$1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{but} \quad 1_S = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

7. If  $R$  is a ring and  $x$  a variable, then the set

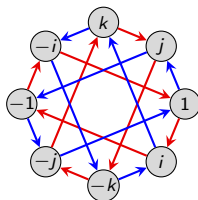
$$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R\}$$

is called the **polynomial ring over  $R$** .

## Another example: the quaternions

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  $4 \times 4$  matrices:

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

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

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

We say that  $\mathbb{H}$  is **represented** by a set of matrices.

## Units and zero divisors

### Definition

Let  $R$  be a ring with 1. A **unit** is any  $x \in R$  that has a multiplicative inverse. Let  $U(R)$  be the set (a **multiplicative group**) of units of  $R$ .

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. Let  $R = \mathbb{Z}$ . The units are  $U(R) = \{-1, 1\}$ . There are no (nonzero) zero divisors.
2. Let  $R = \mathbb{Z}_{10}$ . Then 7 is a unit (and  $7^{-1} = 3$ ) because  $7 \cdot 3 = 1$ . However, 2 is not a unit.
3. Let  $R = \mathbb{Z}_n$ . A nonzero  $k \in \mathbb{Z}_n$  is a unit if  $\gcd(n, k) = 1$ , and a zero divisor if  $\gcd(n, k) \geq 2$ .
4. The ring  $R = M_2(\mathbb{R})$  has zero divisors, such as:

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

The groups of units of  $M_2(\mathbb{R})$  are the **invertible matrices**.

## Group rings

Let  $R$  be a commutative ring (usually,  $\mathbb{Z}$ ,  $\mathbb{R}$ , or  $\mathbb{C}$ ) and  $G$  a finite (multiplicative) group. We can define the **group ring**  $RG$  as

$$RG := \{a_1g_1 + \cdots + a_ng_n \mid a_i \in R, g_i \in G\},$$

where multiplication is defined in the “obvious” way.

For example, let  $R = \mathbb{Z}$  and  $G = D_4 = \langle r, f \mid r^4 = f^2 = rfrf = 1 \rangle$ , and consider the elements  $x = r + r^2 - 3f$  and  $y = -5r^2 + rf$  in  $\mathbb{Z}D_4$ . Their sum is

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

and their product is

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

### Remarks

- The (real) Hamiltonians  $\mathbb{H}$  is *not* the same ring as  $\mathbb{R}Q_8$ .
- 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  $R$ , and the group of units  $U(RG)$  contains a subgroup isomorphic to  $G$ .

## Types of rings

### Definition

If all nonzero elements of  $R$  have a multiplicative inverse, then  $R$  is a **division ring**. (Think: “field without commutativity”.)

An **integral domain** is a commutative ring with 1 and with no (nonzero) zero divisors. (Think: “field without inverses”.)

A field is just a commutative division ring. Moreover:

fields  $\subsetneq$  division rings

fields  $\subsetneq$  integral domains  $\subsetneq$  all rings

### 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 (or even division rings):  $\mathbb{Z}$ ,  $\mathbb{Z}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{R}[[x]]$  (formal power series).
- Division ring but not a field:  $\mathbb{H}$ .

## Cancellation

When doing basic algebra, we often take for granted basic properties such as cancellation:  $ax = ay \implies x = y$ . However, *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

### Lemma (HW)

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

### Theorem

Every finite integral domain is a field.

### Proof

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

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

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

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

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

Thus,  $a \cdot a^{i-j-1} = 1$ . □

## Ideals

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

### Definition

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

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

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

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

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

### Examples

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

## Ideals

### Remark

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

### Proof

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

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

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

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

- **normal subgroups** are characterized by being **invariant under conjugation**:

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

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

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

## Ideals generated by sets

### Definition

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

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

This is the **smallest left ideal containing  $X$** .

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

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

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

### Proposition (HW)

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

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

## Ideals and quotients

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

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

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

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

### Proposition

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

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

### Proof

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

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

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

## Finite fields

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

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

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

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

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

The quotient has only 4 elements:

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

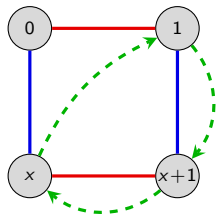
As with the quotient group (or ring)  $\mathbb{Z}/n\mathbb{Z}$ , we usually drop the " $I$ ", and just write

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

It is easy to check that this is a field!

## Finite fields

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



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

×	1	x	x+1
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

### Theorem

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

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

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

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

## Motivation (spoilers!)

Many of the big ideas from group homomorphisms carry over to ring homomorphisms.

### Group theory

- The **quotient group**  $G/N$  exists iff  $N$  is a **normal subgroup**.
- A **homomorphism** is a structure-preserving map:  $f(x * y) = f(x) * f(y)$ .
- The **kernel** of a homomorphism is a **normal subgroup**:  $\text{Ker } \phi \trianglelefteq G$ .
- For every **normal subgroup**  $N \trianglelefteq G$ , there is a natural **quotient homomorphism**  $\phi: G \rightarrow G/N$ ,  $\phi(g) = gN$ .
- There are four standard **isomorphism theorems** for groups.

### Ring theory

- The **quotient ring**  $R/I$  exists iff  $I$  is a **two-sided ideal**.
- A **homomorphism** is a structure-preserving map:  $f(x + y) = f(x) + f(y)$  and  $f(xy) = f(x)f(y)$ .
- The **kernel** of a homomorphism is a **two-sided ideal**:  $\text{Ker } \phi \trianglelefteq R$ .
- For every **two-sided ideal**  $I \trianglelefteq R$ , there is a natural **quotient homomorphism**  $\phi: R \rightarrow R/I$ ,  $\phi(r) = r + I$ .
- There are four standard **isomorphism theorems** for rings.



# Ring homomorphisms

## Definition

A **ring homomorphism** is a function  $f: R \rightarrow S$  satisfying

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

A **ring isomorphism** is a homomorphism that is bijective.

The **kernel**  $f: R \rightarrow S$  is the set  $\text{Ker } f := \{x \in R : f(x) = 0\}$ .

## Examples

1. The function  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$  that sends  $k \mapsto k \pmod{n}$  is a ring homomorphism with  $\text{Ker}(\phi) = n\mathbb{Z}$ .
2. For a fixed real number  $\alpha \in \mathbb{R}$ , the “evaluation function”

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

is a homomorphism. The kernel consists of all polynomials that have  $\alpha$  as a root.

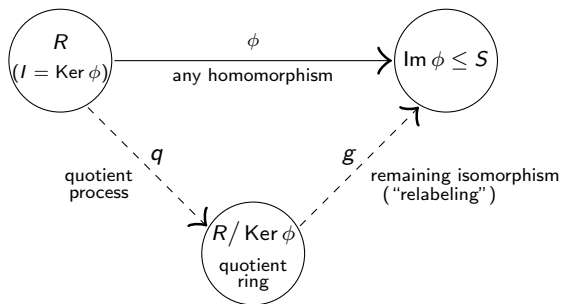
3. The following is a homomorphism, for the ideal  $I = (x^2 + x + 1)$  in  $\mathbb{Z}_2[x]$ :

$$\phi: \mathbb{Z}_2[x] \longrightarrow \mathbb{Z}_2[x]/I, \quad f(x) \longmapsto f(x) + I.$$

# The isomorphism theorems for rings

## Fundamental homomorphism theorem

If  $\phi: R \rightarrow S$  is a ring homomorphism, then  $\text{Ker } \phi$  is an ideal and  $\text{Im}(\phi) \cong R/\text{Ker}(\phi)$ .



## Proof (HW)

The statement holds for the underlying additive group  $R$ . Thus, it remains to show that  $\text{Ker } \phi$  is a (two-sided) ideal, and the following map is a ring homomorphism:

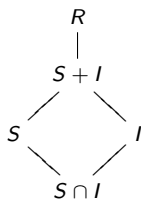
$$g: R/I \longrightarrow \text{Im } \phi, \quad g(x + I) = \phi(x).$$

## The second isomorphism theorem for rings

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

- (i) The **sum**  $S + I = \{s + i \mid s \in S, i \in I\}$  is a **subring** of  $R$  and 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)

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

$$s_1, s_2 \in S, i_1, i_2 \in I \implies (s_1 + i_1)(s_2 + i_2) = \underbrace{s_1 s_2}_{\in S} + \underbrace{s_1 i_2 + i_1 s_2 + i_1 i_2}_{\in I} \in S + I.$$

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

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

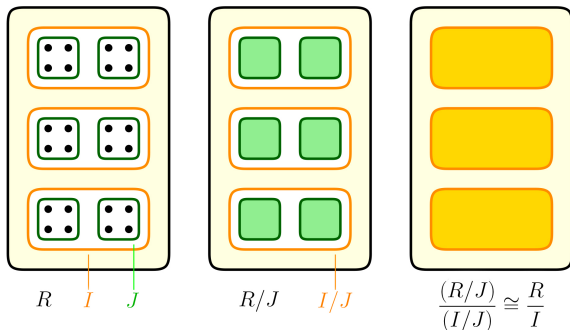
One explicit isomorphism is  $\phi: s + (S \cap I) \mapsto s + I$ . It is easy to check that  $\phi: 1 \mapsto 1$  and  $\phi$  preserves products.  $\square$

## The third isomorphism theorem for rings

### Freshman theorem

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

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

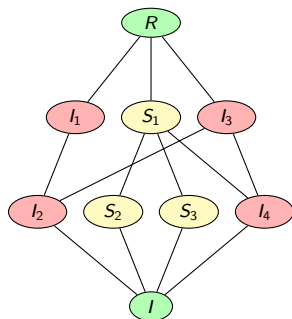


(Thanks to Zach Teitler of Boise State for the concept and graphic!)

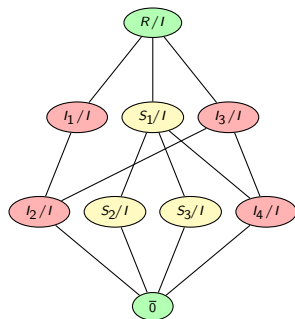
# The fourth isomorphism theorem for rings

## Correspondence theorem

Let  $I$  be an ideal of  $R$ . There is a bijective correspondence between **subrings (& ideals) of  $R/I$**  and **subrings (& ideals) of  $R$  that contain  $I$** . In particular, every ideal of  $R/I$  has the form  $J/I$ , for some ideal  $J$  satisfying  $I \subseteq J \subseteq R$ .



subrings & ideals that contain  $I$



subrings & ideals of  $R/I$

## Maximal ideals

### Definition

An ideal  $I$  of  $R$  is **maximal** if  $I \neq R$  and if  $I \subseteq J \subseteq R$  holds for some ideal  $J$ , then  $J = I$  or  $J = R$ .

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

### Examples

1. If  $n \neq 0$ , then the ideal  $M = (n)$  of  $R = \mathbb{Z}$  is **maximal** if and only if  $n$  is **prime**.
2. Let  $R = \mathbb{Q}[x]$  be the set of all polynomials over  $\mathbb{Q}$ . The ideal  $M = (x)$  consisting of all polynomials with constant term zero is a maximal ideal.

Elements in the quotient ring  $\mathbb{Q}[x]/(x)$  have the form  $f(x) + M = a_0 + M$ .

3. Let  $R = \mathbb{Z}_2[x]$ , the polynomials over  $\mathbb{Z}_2$ . The ideal  $M = (x^2 + x + 1)$  is maximal, and  $R/M \cong \mathbb{F}_4$ , the (unique) finite field of order 4.

In all three examples above, the quotient  $R/M$  is a field.

## Maximal ideals

### Theorem

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

- (i)  $I$  is a **maximal ideal**;
- (ii)  $R/I$  is **simple**;
- (iii)  $R/I$  is a **field**.

### Proof

The equivalence (i) $\Leftrightarrow$ (ii) is immediate from the Correspondence Theorem.

For (ii) $\Leftrightarrow$ (iii), we'll show that an *arbitrary* ring  $R$  is **simple** iff  $R$  is a **field**.

" $\Rightarrow$ ": 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.  $\checkmark$

" $\Leftarrow$ ": 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  $I = R$ .  $\checkmark$

□

## Prime ideals

### Definition

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

Note that  $p \in \mathbb{N}$  is a **prime number** iff  $p = ab$  implies either  $a = p$  or  $b = p$ .

### Examples

1. The ideal  $(n)$  of  $\mathbb{Z}$  is a **prime ideal** iff  $n$  is a **prime number** (possibly  $n = 0$ ).
2. In the polynomial ring  $\mathbb{Z}[x]$ , the ideal  $I = (2, x)$  is a prime ideal. It consists of all polynomials whose constant coefficient is even.

### Theorem

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

The proof is straightforward (HW). Since fields are integral domains, the following is immediate:

### Corollary

In a commutative ring, every maximal ideal is prime.



## Divisibility and factorization

A ring is in some sense, a generalization of the familiar number systems like  $\mathbb{Z}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$ , where we are allowed to add, subtract, and multiply.

Two key properties about these structures are:

- multiplication is commutative,
- there are no (nonzero) zero divisors.

### Blanket assumption

Throughout this lecture, unless explicitly mentioned otherwise,  $R$  is assumed to be an **integral domain**, and we will define  $R^* := R \setminus \{0\}$ .

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**;
- there is a **Euclidean algorithm**, which can find the gcd of two numbers.

Surprisingly, these need not always hold in integrals domains! We would like to understand this better.

# Divisibility

## Definition

If  $a, b \in R$ , say that  $a$  divides  $b$ , or  $b$  is a multiple of  $a$  if  $b = ac$  for some  $c \in R$ . We 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  $c \neq 0$ .
- The only associate of 0 is itself.
- The associates of 1 are the units of  $R$ .

## Proposition (HW)

Two elements  $a, b \in R$  are associates if and only if  $a = bu$  for some unit  $u \in U(R)$ .

This defines an equivalence relation on  $R$ , and partitions  $R$  into equivalence classes.

## Irreducibles and primes

Note that **units divide everything**: if  $b \in R$  and  $u \in U(R)$ , then  $u \mid b$ .

### Definition

If  $b \in R$  is not a unit, and the only divisors of  $b$  are units and associates of  $b$ , then  $b$  is **irreducible**.

An element  $p \in R$  is **prime** if  $p$  is not a unit, and  $p \mid ab$  implies  $p \mid a$  or  $p \mid b$ .

### Proposition

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

### Proof

Suppose  $p$  is prime but 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  $b \in U(R)$ , a contradiction.  $\square$

## Irreducibles and primes

**Caveat: Irreducible  $\not\Rightarrow$  prime**

Consider the ring  $R_{-5} := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ .

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

but  $3 \nmid 2 + \sqrt{-5}$  and  $3 \nmid 2 - \sqrt{-5}$ .

Thus, 3 is irreducible in  $R_{-5}$  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 *lengths* of factorizations into irreducibles need be the same!

For example, consider the ring  $R = \mathbb{Z}[x^2, x^3]$ . Then

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

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  $R$  (note:  $x \notin R$ ).

## Principal ideal domains

Fortunately, there is a type of ring where such “bad things” don’t happen.

### Definition

An ideal  $I$  generated by a single element  $a \in R$  is called a **principal ideal**. We denote this by  $I = (a)$ .

If every ideal of  $R$  is principal, then  $R$  is a **principal ideal domain** (PID).

### Examples

The following are all PIDs (stated without proof):

- The ring of integers,  $\mathbb{Z}$ .
- Any field  $F$ .
- The polynomial ring  $F[x]$  over a field.

As we will see shortly, PIDs are “nice” rings. Here are some properties they enjoy:

- pairs of elements have a “**greatest common divisor**” & “**least common multiple**”;
- irreducible  $\Rightarrow$  prime;
- Every element factors uniquely into primes.

## 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,  $b = qa \in (a)$ . □

### Definition

A **common divisor** of  $a, b \in R$  is an element  $d \in R$  such that  $d \mid a$  and  $d \mid b$ .

Moreover,  $d$  is a **greatest common divisor** (GCD) if  $c \mid d$  for all other common divisors  $c$  of  $a$  and  $b$ .

A **common multiple** of  $a, b \in R$  is an element  $m \in R$  such that  $a \mid m$  and  $b \mid m$ .

Moreover,  $m$  is a **least common multiple** (LCM) if  $m \mid n$  for all other common multiples  $n$  of  $a$  and  $b$ .

## 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

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

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  $d \sim d'$ . ✓

□

## Nice properties of PIDs

### Corollary

If  $R$  is a PID, then every **irreducible** element is **prime**.

### Proof

Let  $p \in R$  be irreducible and suppose  $p \mid ab$  for some  $a, b \in R$ .

If  $p \nmid a$ , then  $\gcd(p, a) = 1$ , so we may write  $1 = xa + yp$  for some  $x, y \in R$ . Thus

$$b = (xa + yp)b = x(ab) + (yb)p.$$

Since  $p \mid x(ab)$  and  $p \mid (yb)p$ , then  $p \mid x(ab) + (yb)p = b$ . □

Not surprisingly, **least common multiples** also have a nice characterization in PIDs.

### Proposition (HW)

If  $R$  is a PID, then any  $a, b \in R^*$  have an LCM,  $m = \text{lcm}(a, b)$ .

It is *unique up to associates*, and can be characterized as a generator of the ideal  $I := (a) \cap (b)$ .



# Unique factorization domains

## Definition

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

- (i) Every nonzero element is a product of irreducible elements;
- (ii) Every irreducible element is prime.

## Examples

1.  $\mathbb{Z}$  is a UFD: Every integer  $n \in \mathbb{Z}$  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. But it is not a PID because the following ideal is not principal:

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

3. The ring  $R_{-5}$  is not a UFD because  $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ .
4. 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. A ring is **Noetherian** if every **ascending chain of ideals**

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilizes, meaning that  $I_k = I_{k+1} = I_{k+2} = \cdots$  holds for some  $k$ .

Suppose  $R$  is a PID. It is not hard to show that  $R$  is Noetherian (HW). Define

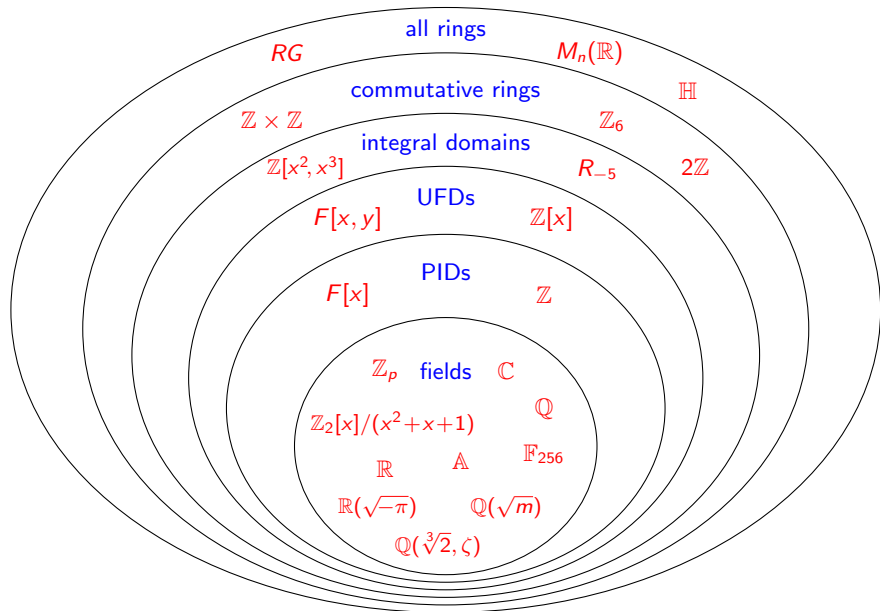
$$X = \{a \in R^* \setminus U(R) : a \text{ can't be written as a product of irreducibles}\}.$$

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. This is impossible in a PID, so  $X = \emptyset$ . □

# 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.

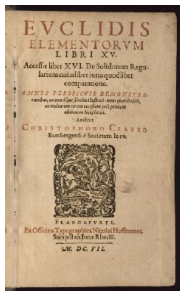
The algorithm works due to two key observations:

- 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  $b = 360$ .

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

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



## Euclidean domains

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

### Definition

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

- (i) **non-negativity**:  $d(r) \geq 0 \quad \forall r \in R^*$ .
- (ii) **monotonicity**:  $d(a) \leq d(ab)$  for all  $a, b \in R^*$ .
- (iii) **division-with-remainder property**: For all  $a, b \in R$ ,  $b \neq 0$ , there are  $q, r \in R$  such that

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

Note that Property (ii) could be restated to say: *If  $a \mid b$ , then  $d(a) \leq d(b)$ ;*

### Examples

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

## Euclidean domains

### Proposition

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

### Proof

“ $\subseteq$ ”: First, we'll show that **associates have the same degree**. Take  $a \sim b$  in  $R^*$ :

$$\begin{aligned} a \mid b &\implies d(a) \leq d(b) \\ b \mid a &\implies d(b) \leq d(a) \end{aligned} \implies d(a) = d(b).$$

If  $u \in U(R)$ , then  $u \sim 1$ , and so  $d(u) = d(1)$ .  $\checkmark$

“ $\supseteq$ ”: Suppose  $x \in R^*$  and  $d(x) = d(1)$ .

Then  $1 = qx + r$  for some  $q \in R$  with either  $r = 0$  or  $d(r) < d(x) = d(1)$ .

If  $r \neq 0$ , then  $d(1) \leq d(r)$  since  $1 \mid r$ .

Thus,  $r = 0$ , and so  $qx = 1$ , hence  $x \in U(R)$ .  $\checkmark$

□

## Euclidean domains

### Proposition

If  $R$  is Euclidean, then  $R$  is a PID.

### Proof

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

Pick  $a \in I$ , and write  $a = bq + r$  with either  $r = 0$ , or  $d(r) < d(b)$ .

This latter case is impossible:  $r = a - bq \in I$ , and by minimality,  $d(b) \leq d(r)$ .

Therefore,  $r = 0$ , which means  $a = bq \in (b)$ . Since  $a$  was arbitrary,  $I = (b)$ .  $\square$

### Exercises.

- (i) The ideal  $I = (3, 2 + \sqrt{-5})$  is not principal in  $R_{-5}$ .
- (ii) If  $R$  is an integral domain, then  $I = (x, y)$  is not principal in  $R[x, y]$ .

### Corollary

The rings  $R_{-5}$  (not a PID or UFD) and  $R[x, y]$  (not a PID) are not Euclidean.

## Algebraic integers

The **algebraic integers** are the roots of *monic* polynomials in  $\mathbb{Z}[x]$ . This is a subring of the **algebraic numbers** (roots of all polynomials in  $\mathbb{Z}[x]$ ).

Assume  $m \in \mathbb{Z}$  is square-free with  $m \neq 0, 1$ . Recall the **quadratic field**

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

### Definition

The ring  $R_m$  is the set of **algebraic integers** in  $\mathbb{Q}(\sqrt{m})$ , i.e., the subring consisting of those numbers that are roots of monic quadratic polynomials  $x^2 + cx + d \in \mathbb{Z}[x]$ .

### Facts

- $R_m$  is an integral domain with 1.
- Since  $m$  is square-free,  $m \not\equiv 0 \pmod{4}$ . For the other three cases:

$$R_m = \begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} & m \equiv 2 \text{ or } 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \{a + b\left(\frac{1+\sqrt{m}}{2}\right) : a, b \in \mathbb{Z}\} & m \equiv 1 \pmod{4} \end{cases}$$

- $R_{-1}$  is the **Gaussian integers**, which is a PID. (easy)
- $R_{-19}$  is a PID. (hard)



# Algebraic integers

## Definition

For  $x = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ , define the **norm** of  $x$  to be

$$N(x) = (r + s\sqrt{m})(r - s\sqrt{m}) = r^2 - ms^2.$$

$R_m$  is **norm-Euclidean** if it is a Euclidean domain with  $d(x) = |N(x)|$ .

Note that the norm is multiplicative:  $N(xy) = N(x)N(y)$ .

## Exercises

Assume  $m \in \mathbb{Z}$  is square-free, with  $m \neq 0, 1$ .

- $u \in U(R_m)$  iff  $|N(u)| = 1$ .
- If  $m \geq 2$ , then  $U(R_m)$  is infinite.
- $U(R_{-1}) = \{\pm 1, \pm i\}$  and  $U(R_{-3}) = \{\pm 1, \pm \frac{1 \pm \sqrt{-3}}{2}\}$ .
- If  $m = -2$  or  $m < -3$ , then  $U(R_m) = \{\pm 1\}$ .

## Euclidean domains and algebraic integers

### Theorem

$R_m$  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 ring  $R_{69}$  is a Euclidean domain that is *not* norm-Euclidean.

Let  $\alpha = (1 + \sqrt{69})/2$  and  $c > 25$  be an integer. Then the following degree function works for  $R_{69}$ , defined on the prime elements:

$$d(p) = \begin{cases} |N(p)| & \text{if } p \neq 10 + 3\alpha \\ c & \text{if } p = 10 + 3\alpha \end{cases}$$

### Theorem

If  $m < 0$  and  $m \notin \{-11, -7, -3, -2, -1\}$ , then  $R_m$  is not Euclidean.

### Open problem

Classify which  $R_m$ 's are PIDs, and which are Euclidean.

## PIDs that are not Euclidean

### Theorem

If  $m < 0$ , then  $R_m$  is a PID iff

$$m \in \underbrace{\{-1, -2, -3, -7, -11\}}_{\text{Euclidean}}, -19, -43, -67, -163.$$

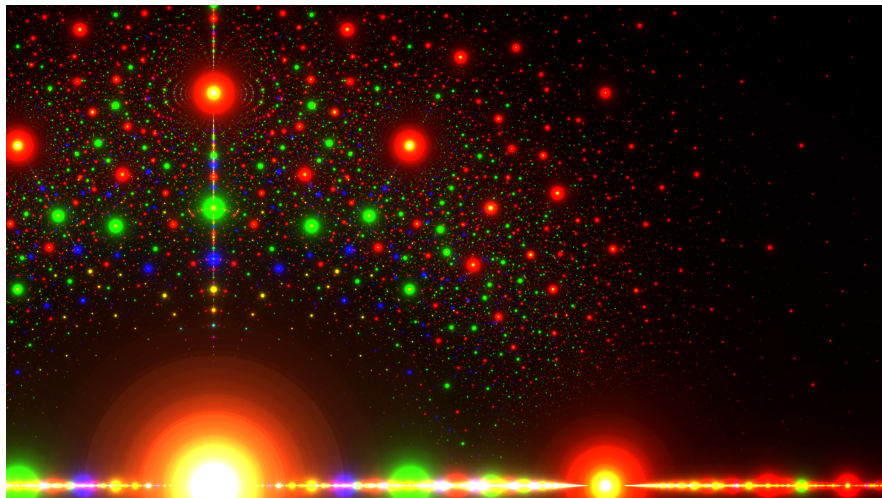
Recall that  $R_m$  is norm-Euclidean iff

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

### Corollary

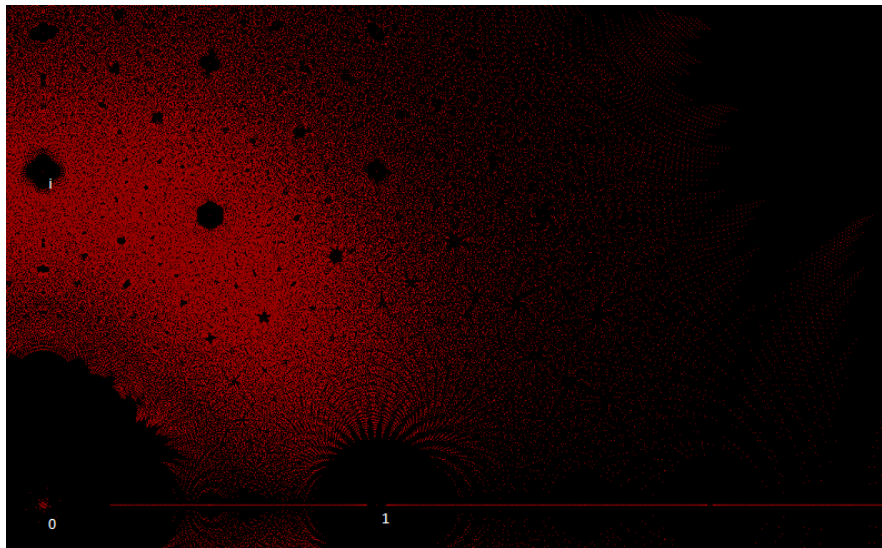
If  $m < 0$ , then  $R_m$  is a PID that is not Euclidean iff  $m \in \{-19, -43, -67, -163\}$ .

## Algebraic integers



**Figure:** Algebraic numbers in the complex plane. 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



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

# Summary of ring types

