

## Motivation and Introduction

Main purpose of this course is to study Galois theory — a field that arose in trying to study roots of polynomials.

Consider  $f(x) = ax^2 + bx + c$ . If we want to find a general, closed-form expression for the roots of the function, we complete the square.

$$\text{roots} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We found these roots by by the coefficients,  $\mathbb{Q}$ , addition, subtraction, multiplication, division, and square root (raising to the  $1/2$  power: see Math 310 notes, Page 104). Naturally, this leads us to ask whether we can do this for cubic polynomials with the same operations. Obviously, we have to change from  $1/2$  power to the  $1/3$  power, but Cardano showed that it was possible to solve a cubic and quartic equation using these traditional operations and radicals.

Évariste Galois invented his theory to prove there is no such closed formula by radicals for any polynomial of degree 5 or above.

For example,  $x^5 - x + 1$  does not have roots given by radicals.

### Example: A Solvable Polynomial

Consider the polynomial  $f(x) = x^2 - 2$ . We know that the roots of this polynomial are  $\pm\sqrt{2}$ . From this, we want to create a set  $K(f)$  that satisfies the following rules:

- $\mathbb{Q} \subseteq K(f)$ .
- $K(f)$  must contain the roots of  $f$ .
- $K(f)$  must be closed under the traditional operations:  $+, -, \times, /$
- $K(f)$  must be the smallest field that satisfies the above three requirements.

**Claim:**  $K(f) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ .

- $\mathbb{Q} \subseteq K(f)$ , because we can set  $b = 0$ .
- $\sqrt{2} = 0 + (1)(\sqrt{2})$ ,  $-\sqrt{2} = 0 + (-1)(\sqrt{2})$
- Let  $a + b\sqrt{2}$  and  $c + d\sqrt{2}$  be elements of  $K(f)$ . Then,
  - $(a + b\sqrt{2}) \pm (c + d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$
  - $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$
  - Set  $c + d\sqrt{2} \neq 0$

$$\begin{aligned} \frac{a + b\sqrt{2}}{c + d\sqrt{2}} &= \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} \\ &= \frac{1}{c^2 - 2d^2} ((ac - 2bd) + (bc - ad)\sqrt{2}) \\ &= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2} \sqrt{2} \end{aligned}$$

- $K(f)$  is indeed the smallest set.
  - Note that  $K(f)$  is a  $\mathbb{Q}$ -vector space, with basis  $\{1, \sqrt{2}\}$ . Therefore,  $\dim_{\mathbb{Q}} K(f) = 2$ .  $K(f)$  is known as the “splitting field” of  $f$ .

We want to consider a bijective function  $\varphi : K(f) \rightarrow K(f)$  with the following properties:

- $\varphi(r) = r$  for every  $r \in \mathbb{Q}$
- $\varphi(x + y) = \varphi(x) + \varphi(y)$
- $\varphi(xy) = \varphi(x)\varphi(y)$

We denote the collection of all such  $\varphi$  as  $\text{Aut}(K(f)/\mathbb{Q})$ . This is a group under the operation  $\circ$  (composition). Specifically, we have

$$\begin{aligned}\varphi(a + b\sqrt{2}) &= \varphi(a) + \varphi(b)\varphi(\sqrt{2}) \\ &= a + b\varphi(\sqrt{2}).\end{aligned}$$

Notice

$$\begin{aligned}(\varphi(\sqrt{2}))^2 - 2 &= \varphi((\sqrt{2})^2 - 2) \\ &= \varphi(0) \\ &= 0.\end{aligned}$$

Therefore,  $\varphi(\sqrt{2}) = \pm\sqrt{2}$ . Therefore, we have that the elements of  $\text{Aut}(K(f)/\mathbb{Q})$  as the following:

$$\begin{aligned}\varphi_0 : a + b\sqrt{2} &\mapsto a + b\sqrt{2} \\ \varphi_1 : a + b\sqrt{2} &\mapsto a - b\sqrt{2} \\ \varphi_1 \circ \varphi_1 &= \varphi_0\end{aligned}$$

Thus,

$$\begin{aligned}\text{Aut}(K(f)/\mathbb{Q}) &= \{\varphi_0, \varphi_1\} \\ &\cong \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

### Example: A Harder Polynomial

Let  $f(x) = (x^2 - 2)(x^2 - 3)$ . Our roots are  $\{\pm\sqrt{2}, \pm\sqrt{3}\}$ . We want to form  $K(f)$  with the same properties. Let

$$\begin{aligned}K(f) &= \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.\end{aligned}$$

Just as with our previous example,  $K(f)$  is a vector space over  $\mathbb{Q}$ , with basis  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ , so  $\dim_{\mathbb{Q}} K(f) = 4$ .

Now, we want  $\text{Aut}(K(f)/\mathbb{Q})$ . If  $\varphi \in \text{Aut}(K(f)/\mathbb{Q})$ , then

$$\begin{aligned}\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{6}) \\ &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{2})\varphi(\sqrt{3}).\end{aligned}$$

Thus, we need to know  $\varphi(\sqrt{2})$  and  $\varphi(\sqrt{3})$ . So,

$$\begin{aligned}f(\varphi(\sqrt{2})) &= ((\varphi(\sqrt{2}))^2 - 2)((\varphi(\sqrt{2}))^2 - 3) \\ &= 0\end{aligned}$$

and the same is the case with  $\varphi(\sqrt{3})$ . So,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\} \\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}.\end{aligned}$$

Suppose  $\varphi(\sqrt{2}) = \sqrt{3}$ . Then,

$$\begin{aligned}((\varphi(\sqrt{2}))^2) &= (\sqrt{3}^2 - 1) \\ &= 0 \\ &= (\varphi(2) - 3) \\ &= -1. \perp\end{aligned}$$

Thus,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}\} \\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{3}\},\end{aligned}$$

and we have the maps as:

$$\begin{aligned}\varphi_0 : \sqrt{2} &\mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \varphi_1 : \sqrt{2} &\mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \varphi_2 : \sqrt{2} &\mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \\ \varphi_3 : \sqrt{2} &\mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\end{aligned}$$

### Example: A Cubic Polynomial

Consider the function  $f(x) = x^3 - 2$ . The function has one real root,  $r_1 = \sqrt[3]{2}$ , and two complex roots. Let's examine  $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ ;  $r_2$  and  $r_3$  are not in  $\mathbb{Q}(\sqrt[3]{2})$ . We could instead consider  $\mathbb{Q}(\sqrt[3]{2}, r_1, r_2)$ .

$$\begin{aligned} x^3 - 2 &= (x - r_1)(x^2 + r_1x + r_1^2) \\ r_2 &= \frac{-r_1 + \sqrt{r_1^2 - 4r_1^2}}{2} \\ &= r_1 \frac{-1 + \sqrt{-3}}{2} \\ &= r_1 \zeta_3 \\ r_3 &= r_1 \frac{-1 - \sqrt{-3}}{2} \\ &= r_1 \zeta_3^2 \end{aligned}$$

However, including  $r_2$  and  $r_3$  is excessive — all we need is  $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ . Therefore, the basis of this vector space is  $\{1, r_1, r_1^2, \zeta_3, \zeta_3 r_1, \zeta_3 r_1^2\}$  (note that  $\zeta_3^2 = -1 - \zeta_3$ ). Therefore,  $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = 6$ , and  $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = K(f)$ . Additionally, we have  $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\varphi_0\}$ , but  $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$ . For the full field extension, we need to find  $\varphi(\sqrt[3]{2})$  and  $\varphi(\zeta_3)$ .

$$\begin{aligned} \varphi(\sqrt[3]{2}) &\in \{r_1, \zeta_3 r_1, \zeta_3^2 r_1\} \\ \varphi(\zeta) &\in \{\zeta_3, \zeta_3^2\} \\ \varphi_0 : r_1 &\mapsto r_1, \zeta_3 \mapsto \zeta_3 \\ \varphi_1 : r_1 &\mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3 \\ \varphi_2 : r_1 &\mapsto r_1, \zeta_3 \mapsto \zeta_3^2 \\ \varphi_3 : r_1 &\mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3 \\ \varphi_4 : r_1 &\mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3^2 \\ \varphi_5 : r_1 &\mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3^2 \end{aligned}$$

Therefore,

$$\begin{aligned} \text{Aut}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) &= 6 \\ &= \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) \end{aligned}$$

### Rings

Consider the integers under the normal operations,  $(\mathbb{Z}, +, \cdot)$ ; this will serve as the motivation for rings in the future.

#### Definition of a Ring

Let  $R$  be a nonempty set with operations  $(+, \cdot)$ , with the following properties:

(1)  $(R, +)$  is an abelian group:

- Closed:  $r_1 + r_2 \in R, \forall r_1, r_2 \in R$
- Identity:  $\exists 0_R, r + 0_R = 0_R + r = r$
- Associativity:  $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$
- Inverse:  $\forall r \in R, \exists -r \in R, r + (-r) = 0_R$
- Commutativity:  $r_1 + r_2 = r_2 + r_1$

(2) Closure under Multiplication:  $r_1 \cdot r_2 \in R, \forall r_1, r_2 \in R$

(3) Associativity under Multiplication:  $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$

(4) Distributivity:  $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3, (r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$

We say  $(R, +, \cdot)$  is a ring if it satisfies all these properties.

If  $\exists 1_R \in R$  such that  $r \cdot 1_R = 1_R \cdot r = r$ , then we say  $R$  is a ring with identity, and  $1_R$  is the multiplicative identity. If multiplication is commutative, then  $R$  is known as a commutative ring.

**Examples**

- (1)  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  are commutative rings with identity value of 1.
- (2)  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  is a commutative ring with identity  $1_R = [1]_n$ .
- (3)  $(\mathbb{R}[x], +, \cdot)$ , where  $\mathbb{R}[x] = \left\{ \sum_{i=0}^n a_i x^i \mid a_i \in \mathbb{R} \right\}$ , is a commutative ring with identity.
- (4)  $(2\mathbb{Z}, +, \cdot)$  is a commutative ring *without* identity.
- (5)  $(\text{Mat}_n(\mathbb{R}), +, \cdot)$ , where  $\text{Mat}_n(\mathbb{R})$  refers to  $n \times n$  matrices with real entries, is a *noncommutative* ring with identity.

**Division Rings and Fields**

Let  $R$  be a ring with identity. We say  $R$  is a *division ring* if  $\forall r \in R \setminus \{0_R\}, \exists r^{-1} \in R$  with  $r \cdot r^{-1} = 1_R = r^{-1} \cdot r$ . If  $R$  is also commutative, then  $R$  is a *field*.

**Examples**

- (1)  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ , and  $(\mathbb{C}, +, \cdot)$  are all fields.
- (2) Let  $p$  be prime, and set  $F = \mathbb{Z}/p\mathbb{Z}$ . Then,  $F$  is a field; we denote this  $\mathbb{F}_p$ .
- (3) Define

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik\}.$$

Then,  $\mathbb{H}$  is a division ring, known as the Hamiltonian quaternions. Note that  $\mathbb{C} \subset \mathbb{H}$ .

**Properties of Rings**

**Proposition 4.1:** Let  $R$  be a ring.

- (1)  $0_R a = a 0_R = 0 \forall a \in R$
- (2)  $(-a)b = a(-b) = -(ab) \forall a, b \in R$
- (3)  $(-a)(-b) = ab \forall a, b \in R$
- (4) If  $\exists 1_R \in R$ , then  $1_R$  is unique, and  $-a = (-1_R)a$ .

**Proof of (1):** Let  $a \in R$ . Then,

$$\begin{aligned} 0_R a &= (0_R + 0_R)a && \text{Additive Inverse} \\ 0_R a &= 0_R a + 0_R a && \text{Distributivity} \\ 0_R a + (-0_R a) &= 0_R a + 0_R a(-0_R a) \\ 0_R &= 0_R a. && \text{Additive Inverse} \end{aligned}$$

**Proof of (2):** Let  $a, b \in R$ . Note that  $-(ab)$  is the unique inverse such that  $ab + (-(ab)) = 0_R$  via group theory. We have

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{Distributivity} \\ &= (0_R)b && \text{Additive Inverse} \\ &= 0_R. && \text{By Property (1)} \end{aligned}$$

Thus,  $(-a)b = -(ab)$ .

**Zero Divisor and Units in Rings**

Let  $a \in R$ ,  $a \neq 0_R$ . If  $\exists b \in R$  with  $b \neq 0_R$  such that  $ab = 0_R = ba$ , then we say  $a$  is a zero divisor.

If  $1_R \in R$ , we say  $u \in R$  is a unit if  $\exists v \in R$  (can be equal to  $u$ ) with  $uv = 1_R = vu$ . The collection of units in  $R$  is denoted  $R^\times$ .

**Exercise:** Show that  $R^\times$  is a group under multiplication.

**Examples**

- (1) Let  $R = \mathbb{Z}/6\mathbb{Z}$ . Note that  $[2]_6[3]_6 = [6]_6 = [0]_6$ , so both  $[2]_6$  and  $[3]_6$  are both zero divisors. Additionally,  $[4]_6[3]_6 = [6]_6 = [0]_6$ . Meanwhile, since  $(\mathbb{Z}/6\mathbb{Z})^\times = \{[1]_6, [5]_6\}$ , those are the two units of  $\mathbb{Z}/6\mathbb{Z}$ .
- (2)  $\mathbb{Z}$  has no zero divisors.  $\mathbb{Z}^\times = \{\pm 1\}$ .
- (3)  $\mathbb{Q}$  has no zero divisors.  $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ .
- (4)  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$  has no zero divisors (as  $\mathbb{C}$  is a field).  $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ .

**Subrings**

Let  $(R, +, \times)$ . If  $S \subseteq R$  is a nonempty subset, and  $(S, +, \cdot)$  is a ring, then  $S$  is a subring of  $R$ . To see  $S$  is a subring, it is enough to show:

- $S \neq \emptyset$ .
- $S$  is closed under subtraction.
- $S$  is closed under multiplication of elements in  $S$ .

**Examples**

(1)

$$\underbrace{\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}}_{\text{subrings}}$$

- (2)  $\mathbb{R} \subseteq \mathbb{R}[x]$  is a subring.
- (3)  $S = \{[0]_4, [2]_4\} \subseteq \mathbb{Z}/4\mathbb{Z}$  is a subring.

**Integral Domains**

Let  $R$  be a commutative ring with identity. We say  $R$  is an integral domain if  $R$  has no zero divisors.

**Examples**

- (1)  $\mathbb{Z}$ , the integers, is an integral domain, that is not a field.
- (2) All fields are integral domains.
- (3)  $\mathbb{Z}/6\mathbb{Z}$  is *not* an integral domain, as it has zero divisors.
- (4)  $\mathbb{Z}/n\mathbb{Z}$  is not an integral domain if  $n$  is composite.

Integral domains are nice due to allowance of cancellations. For example, if  $2m = 2n$  in  $\mathbb{Z}$ , then we find  $2(m - n) = 0$ , and since  $\mathbb{Z}$  has no zero divisors, it must be the case that  $m = n$ .

However, in a ring that is not an integral domain, such as  $\mathbb{Z}/6\mathbb{Z}$ , we cannot use the same technique to find the solution to a similar equation. For example,  $3 \cdot 2 = 0 = 3 \cdot 4$ , but  $2 \neq 4$ .

**Proposition: Equations in Integral Domains**

Let  $R$  be an integral domain. If  $a, b, c \in R$  with  $a \neq 0_R$ , and  $ab = ac$ , then  $b = c$ .

**Proof:**

$$\begin{aligned} ab &= ac \\ a(b - c) &= 0_R \end{aligned}$$

Since  $a \neq 0$ ,

$$\begin{aligned} b - c &= 0_R \\ b &= c. \end{aligned}$$

**Theorem: Finite Integral Domains and Fields**

If  $R$  is an integral domain, and  $\text{card}(R) < \infty$ , then  $R$  is a field.

**Proof:** Let  $a \in R$ ,  $a \neq 0_R$ . Note  $ab \neq 0_R$  for all  $b \in R$ ,  $b \neq 0_R$ .

Define  $\varphi_a : R \setminus \{0_R\} \rightarrow R \setminus \{0_R\}$ ,  $b \mapsto ab$ . If  $\varphi_a(b) = \varphi_a(c)$ , then  $ab = ac$ , and by our previous result,  $b = c$  — therefore,  $\varphi_a$  is injective.

Since  $R \setminus \{0_R\}$  is finite, and  $\varphi_a$  is injective, then  $\varphi_a$  is surjective. In particular, this means  $\exists b \in R \setminus \{0_R\}$  with  $\varphi_a(b) = 1_R$ ; therefore,  $ab = 1_R$ . Since  $R$  is commutative,  $ba = 1_R$ , so  $b = a^{-1}$ .

**Examples of Abstract Rings****Ring of Integers in a Field**

Let  $d \in \mathbb{Z}$ ,  $d$  is square-free (there is no square that divides  $d$ ). Set  $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ . This is a field (can be verified as a subfield of  $\mathbb{C}$ ).

We can define

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \{a + b\left(\frac{1+\sqrt{d}}{2}\right) \mid a, b \in \mathbb{Z}\} & d \equiv 1 \pmod{4} \end{cases}.$$

Then,  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$  is a subring of  $\mathbb{Q}(\sqrt{d})$ . This is known as the ring of integers of  $\mathbb{Q}(\sqrt{d})$ . This set behaves in  $\mathbb{Q}(\sqrt{d})$  the same way that  $\mathbb{Z}$  does inside  $\mathbb{Q}$ . The set  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$  is the collection of all roots in  $\mathbb{Q}(\sqrt{d})$  of monic (coefficient of highest degree is 1) polynomials with coefficients in  $\mathbb{Z}$ .

For example, if  $d = -1$ , defining  $\mathbb{Q}(i)$ , then we can verify that  $\mathbb{Z}[i]$  is a root of a monic polynomial with coefficients in  $\mathbb{Z}$ .

**Ring of Matrices**

Let  $R$  be a ring. Then,

$$\text{Mat}_n(R) = \{n \times n \text{ matrices with entries in } R\}$$

is a ring under matrix addition and multiplication.

**Ring of Functions**

Let  $L^1(\mathbb{R})$  be all functions  $f : \mathbb{R} \rightarrow \mathbb{R}$  such that

$$\int_{\mathbb{R}} |f(x)| dx$$

exists. The set  $L^1(\mathbb{R})$  is a ring under pointwise addition and convolution, where convolution is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(x-y)g(y)dy.$$

This is a commutative ring without identity.

**Group Ring**

Let  $K$  be a field and  $G$  a group. Set  $K[G]$  to be all formal linear combinations of the form

$$\alpha = \sum_{x \in G} a_x x,$$

with  $a_x \in K$ ,  $x \in G$ , with  $a_x = 0$  for all but finitely many  $x$ .

Given

$$\begin{aligned} \alpha &= \sum_{x \in G} a_x x \\ \alpha &= \sum_{y \in G} b_y y, \end{aligned}$$

define

$$\begin{aligned}\alpha + \beta &= \sum_{x \in G} (a_x + b_x)x \\ \alpha\beta &= \sum_{x \in G} \sum_{y \in G} a_x b_y xy \\ &= \sum_{z \in G} \left( \sum_{xy=z} a_x b_y \right) z.\end{aligned}$$

This is a ring under these operations, known as the group ring. It is commutative if and only if  $G$  is abelian.

### Polynomials under a Ring

Let  $R$  be a ring. Set

$$R[x] = \left\{ \sum_{i=1}^n a_i x^i \mid a_i \in R, n \in \mathbb{Z}_{\geq 0} \right\}$$

to be the all polynomials with coefficients in  $R$ . This is a ring under polynomial addition and multiplication. If  $R$  is commutative, then  $R[x]$  is commutative.

### Proposition: Polynomial Properties

Let  $R$  be an integral domain, with  $p(x), q(x) \in R[x] \setminus \{0\}$ . Then:

- (1)  $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$
- (2)  $R[x]^\times = R^\times$
- (3)  $R[x]$  is an integral domain.

**Proof of (1):** Let

$$\begin{aligned}p(x) &= a_m x^m + \cdots + a_1 x + a_0 \\ q(x) &= b_n x^n + \cdots + b_1 x + b_0\end{aligned}$$

with  $a_m, b_n \neq 0$  —  $\deg(p) = m$  and  $\deg(q) = n$ . Then,

$$p(x)q(x) = a_m b_n x^{m+n} + \text{lower degree terms},$$

and since  $a_m b_n \neq 0$  as  $R$  is an integral domain with  $a_m, b_n \neq 0$ ,  $\deg(pq) = m + n$ .

### Ring Homomorphism

Let  $R$  and  $S$  be rings. A ring homomorphism between  $R$  and  $S$  is a map  $\varphi : R \rightarrow S$  that satisfies the following properties for all  $r_1, r_2 \in R$ :

- (1)  $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$
- (2)  $\varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2)$

The kernel of a ring homomorphism  $\varphi$  is given by

$$\ker(\varphi) : \{r \in R \mid \varphi(r) = 0_S\}$$

A bijective ring homomorphism is called an isomorphism. If there exists such a bijection between  $R$  and  $S$ , we say  $R$  and  $S$  are isomorphic.

If  $\varphi$  is an isomorphism, we write

$$\varphi : R \xrightarrow{\cong} S$$

## Examples: Ring Homomorphisms

### Not a Ring Homomorphism

Let  $R = \mathbb{Z}$  and  $S = 2\mathbb{Z}$ . Define

$$\begin{aligned}\varphi : \mathbb{Z} &\rightarrow 2\mathbb{Z} \\ n &\mapsto 2n.\end{aligned}$$

Let  $m, n \in \mathbb{Z}$ . We have

$$\begin{aligned}\varphi(m+n) &= 2(m+n) \\ &= 2m + 2n \\ &= \varphi(m) + \varphi(n).\end{aligned}$$

However,

$$\begin{aligned}\varphi(mn) &= 2(mn) \\ \varphi(m)\varphi(n) &= 4(mn).\end{aligned}$$

### Homomorphism between Integers and Integers Modulo $n$

Consider  $R = \mathbb{Z}$  and  $S = \mathbb{Z}/n\mathbb{Z}$ . Define

$$\begin{aligned}\varphi : \mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto [a]_n.\end{aligned}$$

Let  $a, b \in \mathbb{Z}$ . We have

$$\begin{aligned}\varphi(a+b) &= [a+b]_n \\ &= [a]_n + [b]_n \\ &= \varphi(a) + \varphi(b).\end{aligned}$$

Additionally, we have

$$\begin{aligned}\varphi(ab) &= [ab]_n \\ &= [a]_n[b]_n \\ &= \varphi(a)\varphi(b).\end{aligned}$$

So,  $\varphi$  is a ring homomorphism. Note that

$$\begin{aligned}\ker(\varphi) &= \{a \in \mathbb{Z} \mid \varphi(a) = [0]_n\} \\ &= \{a \in \mathbb{Z} \mid [a]_n = [0]_n\} \\ &= \{a \in \mathbb{Z} \mid n \mid a\} \\ &= n\mathbb{Z}.\end{aligned}$$

### Homomorphism Between the Polynomials and Reals

Let  $S = \mathbb{R}[x]$  and  $T = \mathbb{R}$ . Define

$$\begin{aligned}\varphi_a : \mathbb{R}[x] &\rightarrow \mathbb{R} \\ f &\mapsto f(a)\end{aligned}$$

Let  $f(x), g(x) \in \mathbb{R}[x]$ . Then,

$$\begin{aligned}\varphi_a(f(x) + g(x)) &= \varphi_a((a_0 + b_0) + \cdots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + \cdots + b_n x^n) \\ &= (a_0 + b_0) + \cdots + (a_m + b_m)a^m + b_{m+1}a^{m+1} + \cdots + b_n a^n \\ &= \varphi_a(f(x)) + \varphi_a(g(x)).\end{aligned}$$

Similarly, we can verify that  $\varphi_a(f(x)g(x)) = \varphi_a(f(x))\varphi_a(g(x))$ . So,  $\varphi_a$  is a ring homomorphism. Note that

$$\begin{aligned}\ker(\varphi_a) &= \{f(x) \in \mathbb{R}[x] \mid f(a) = 0\} \\ &= \{f(x) \in \mathbb{R}[x] \mid (x-a) \mid f(x)\} \\ &= (x-a)\mathbb{R}[x]\end{aligned}$$



**Homomorphism between Matrices**

Define

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in \text{Mat}_2(\mathbb{R}) \right\}$$

$$S = \mathbb{R},$$

and

$$\varphi : R \rightarrow S$$

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mapsto a.$$

Then,

$$\begin{aligned} \varphi \left( \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \right) &= \varphi \left( \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & d_1 + d_2 \end{bmatrix} \right) \\ &= a_1 + a_2 \\ &= \varphi \left( \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \right) + \varphi \left( \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \right), \end{aligned}$$

and

$$\begin{aligned} \varphi \left( \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \right) &= \varphi \left( \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{bmatrix} \right) \\ &= a_1 a_2 \\ &= \varphi \left( \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \right) \varphi \left( \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \right). \end{aligned}$$

So  $\varphi$  is a ring homomorphism that is surjective but not injective. Note

$$\ker(\varphi) = \left\{ \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} \mid b, d \in \mathbb{R} \right\}.$$

**Proposition: Fundamental Theorem of Ring Homomorphisms**

Let  $\varphi : R \rightarrow S$  be a ring homomorphism.

- (1) The image of  $\varphi$ ,  $\varphi(R) = \{s \in S \mid s = \varphi(r) \text{ for some } r \in R\}$ , is a subring of  $S$ .
- (2) The kernel,  $\ker(\varphi)$ , is a subring of  $R$ .

Additionally, for any  $r \in R$ , and  $a \in \ker(\varphi)$ ,  $ar \in \ker(\varphi)$  and  $ra \in \ker(\varphi)$ .

**Proof of (2):** To show  $\ker(\varphi)$  is a subring, we must show that  $\ker(\varphi)$  is non-empty, closed under subtraction, and closed under multiplication.

First, since  $\varphi(0_R) = 0_S$  (verify this),  $\ker(\varphi)$  is non-empty.

Let  $a, b \in \ker(\varphi)$ . We have

$$\begin{aligned} \varphi(a - b) &= \varphi(a + (-b)) \\ &= \varphi(a) + \varphi(-b) \\ &= \varphi(a) - \varphi(b) && \text{check } \varphi(-b) = -\varphi(b) \\ &= 0_S - 0_S \\ &= 0_S. \end{aligned}$$

Thus,  $a - b \in \ker(\varphi)$ , and  $\ker(\varphi)$  is closed under subtraction.

To show  $\ker(\varphi)$  is closed under multiplication, we will prove the general case. Let  $a \in \ker(\varphi)$  and  $r \in R$ . We have

$$\begin{aligned} \varphi(ra) &= \varphi(r)\varphi(a) \\ &= \varphi(r)0_S \\ &= 0_S. \end{aligned}$$

Similarly,  $\varphi(ar) = 0_S$ . So,  $ar, ra \in \ker(\varphi)$ .

The stronger condition that we found for  $\ker(\varphi)$  (closed under multiplication of all elements of the ring, not merely those from the subring) forms what we call an ideal.

## Quotient Rings

### Defining an Equivalence Relation on a Ring

Set  $K = \ker(\varphi)$ . We will define a relation on  $R$ ,  $\sim$ , where  $r_1 \sim r_2$  if  $r_1 - r_2 \in K$ . We want to see if  $\sim$  is an equivalence relation:

- Reflexive:  $r \sim r$  since  $r - r = 0_R \in K$ .
- Symmetric:  $r_1 \sim r_2$  implies  $r_1 - r_2 = k$  for some  $k \in K$ . Since  $k$  is a subring,  $-k \in K$ , so  $r_2 - r_1 \in K$ .
- Transitive: suppose  $r_1 \sim r_2$  and  $r_2 \sim r_3$ . This means there are elements  $k_1, k_2 \in K$  with  $r_1 - r_2 = k_1$  and  $r_2 - r_3 = k_2$ . Since  $K$  is a subring,  $(r_1 - r_2) + (r_2 - r_3) = r_1 - r_3 = k_1 + k_2 \in K$ . Thus,  $r_1 \sim r_3$ .

Since  $\sim$  is reflexive, symmetric, and transitive,  $\sim$  is an equivalence relation on  $R$ .

Since  $\sim$  is an equivalence relation on  $R$ , we will want to examine equivalence classes of  $R$  under  $\sim$ . Specifically, for  $r \in R$ , we have

$$\begin{aligned} [r]_K &= \{\tilde{r} \in R \mid r - \tilde{r} \in K\} \\ &= \{\tilde{r} \in R \mid r - \tilde{r} = k \text{ for some } k \in K\} \\ &= \{r + k \mid k \in K\} \\ &= r + K. \end{aligned}$$

We will define the set

$$R/K = \{r + K \mid r \in R\}$$

to be the set of all equivalence classes.

**Example:** Let  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ ,  $a \mapsto [a]_n$ . Then,  $\ker(\varphi) = n\mathbb{Z}$ . Then,  $R/K = \mathbb{Z}/n\mathbb{Z}$ .

Let  $r_1 + K, r_2 + K \in R/K$ . The new question is whether or not we can define addition and multiplication on  $R/K$ . Suppose that the following are the definition of multiplication and addition on  $R/K$ .

$$\begin{aligned} (r_1 + K) + (r_2 + K) &= (r_1 + r_2) + K \\ (r_1 + K)(r_2 + K) &= (r_1 r_2) + K. \end{aligned}$$

Suppose  $r_1 + K = \tilde{r}_1 + K$  and  $r_2 + K = \tilde{r}_2 + K$ . This means there are  $k_1, k_2 \in K$  with  $r_1 - \tilde{r}_1 = k_1$ ,  $r_2 - \tilde{r}_2 = k_2$ , or that  $r_1 = \tilde{r}_1 + k_1$ ,  $r_2 = \tilde{r}_2 + k_2$ .

To see if the map is well-defined, we have

$$\begin{aligned} (r_1 + K) + (r_2 + K) &= (r_1 + r_2) + K \\ &= (\tilde{r}_1 + k_1 + \tilde{r}_2 + k_2) + K \\ &= (\tilde{r}_1 + k_1) + K + (\tilde{r}_2 + k_2) + K \\ &= (\tilde{r}_1 + K) + (\tilde{r}_2 + K) \end{aligned}$$

since  $\tilde{r}_1 + k_1 - \tilde{r}_1 = k_1 \in K$ .

Thus, our addition is well-defined.

Examining multiplication, we see that

$$\begin{aligned} (r_1 + K)(r_2 + K) &= r_1 r_2 + K \\ &= (\tilde{r}_1 + k_1)(\tilde{r}_2 + k_2) + K \\ &= \tilde{r}_1 \tilde{r}_2 + \underbrace{k_1 \tilde{r}_2 + \tilde{r}_1 k_2 + k_1 k_2}_{\in K \text{ since } K = \ker(\varphi)} + K \\ &= \tilde{r}_1 \tilde{r}_2 + K. \end{aligned}$$

Therefore, our multiplication is well-defined.

We can show that  $R/K$  is a ring (verify for yourself).

**Note:** This construction would not have worked if  $K$  was merely a subring, as multiplication would not be well-defined.

### Ideals

Let  $I \subseteq R$  be a subring.

- (1) If  $ra \in I$  for every  $r \in R$ , we say  $I$  is a left-ideal of  $R$ .
- (2) If  $ar \in I$  for every  $r \in R$ , then we say  $I$  is a right-ideal of  $R$ .
- (3) If  $I$  is a left-ideal and a right-ideal of  $R$ , then we say  $I$  is an ideal of  $R$ .

If  $I \subseteq R$  is an ideal, we define  $r_1 \sim_I r_2$  if  $r_1 - r_2 \in I$ , and  $R/I = \{r + I \mid r \in R\}$ . Addition and multiplication in  $R/I$  are defined as

$$\begin{aligned}(r_1 + I) + (r_2 + I) &= (r_1 + r_2) + I \\ (r_1 + I)(r_2 + I) &= r_1 r_2 + I.\end{aligned}$$

### Examples of Ideals

- (1)  $n\mathbb{Z} \subseteq \mathbb{Z}$  is an ideal; if  $nk \in n\mathbb{Z}$ , and  $m \in \mathbb{Z}$ , then  $m(nk) = n(mk) \in n\mathbb{Z}$ .
- (2) Let  $R = \mathbb{Z}[x]$ . Set  $\langle x^2 \rangle = \{f(x)x^2 \mid f(x) \in \mathbb{Z}[x]\}$ . This is an ideal.
- (3) Let  $R$  be a ring. If  $r \in R$ , we define  $\langle r \rangle = \{ar \mid a \in R\}$ .
- (4) Set  $I = \{(2n, 0) \mid n \in \mathbb{Z}\}$  in  $\mathbb{Z} \times \mathbb{Z}$ . Let  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ . Then,  $(a, b)(2n, 0) = (2an, 0) \in I$ , meaning  $I$  is an ideal.

- (5) Define  $R = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in \text{Mat}_2(\mathbb{R}) \right\}$ . Consider  $I = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$ . Then,

$$\begin{aligned}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} s & 0 \\ 0 & t \end{bmatrix} &= \begin{bmatrix} as & bt \\ 0 & dt \end{bmatrix} \\ \begin{bmatrix} s & 0 \\ 0 & t \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} &= \begin{bmatrix} sa & sb \\ 0 & td \end{bmatrix}.\end{aligned}$$

Therefore,  $I$  is a subring but not an ideal.

- (6) Let  $R = \mathbb{Z}[x]$ . Consider  $I = \langle 2f(x) + g(x) \mid f(x), g(x) \in \mathbb{Z}[x] \rangle$ . Then,

$$\begin{aligned}(2f_1(x) + xg_1(x))(2f_2(x) + xg_2(x)) &= 2(f_1(x)(2f_2(x) + xg_2(x))) + x(g_1(x)(2f_2(x) + xg_2(x))) \\ h(x)(2f(x) + xg(x)) &= 2(f(x)h(x)) + x(g(x)h(x)),\end{aligned}$$

meaning  $I$  is an ideal.

### Examples of Quotient Rings

- (1) Let  $R = \mathbb{Z}$ ,  $I = n\mathbb{Z}$ . Then,  $R/I = \mathbb{Z}/n\mathbb{Z}$ .
- (2) Let  $R = \mathbb{R}[x]$ ,  $I = \langle x^2 \rangle$  as defined earlier. Then,

$$\begin{aligned}R/I &= \mathbb{R}[x]/\langle x^2 \rangle \\ &= f(x) + \langle x^2 \rangle.\end{aligned}$$

Other examples include

$$\begin{aligned}f(x) &= a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x] \\ f(x) + \langle x^2 \rangle &= a_1 x + a_0 + \langle x^2 \rangle \in \mathbb{R}[x]/\langle x^2 \rangle \\ \mathbb{R}[x]/\langle x^2 \rangle &= \{a + bx + \langle x^2 \rangle \mid a, b \in \mathbb{R}\}. \\ (a + bx + \langle x^2 \rangle)(c + dx + \langle x^2 \rangle) &= ac + adx + bcx + bdx^2 + \langle x^2 \rangle \\ &= (ac) + (ad + bc)x + \langle x^2 \rangle \\ (x + \langle x^2 \rangle)^2 &= x^2 + \langle x^2 \rangle \\ &= \langle x^2 \rangle.\end{aligned}$$

- (3) Let  $R = \mathbb{Z} \times \mathbb{Z}$ ,  $I = \{(2n, 0) \mid n \in \mathbb{Z}\}$ . Then,

$$\begin{aligned}R/I &= \{(a, b) + I \mid a, b \in \mathbb{Z}\}. \\ (a, b) + I &= ([a]_2, b) + I\end{aligned}$$

where  $[a]_2$  is  $a$  modulo 2.

We would expect that  $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \rightarrow R/I$ ,  $([a]_2, b) \mapsto (a, b) + I$  is an isomorphism (verify for yourself).

**Isomorphisms to Quotient Rings**

Let  $R = \mathbb{Z}[x]$ ,  $I = \langle 2, x \rangle$ ,  $J = \langle 2 \rangle = \{2f(x) \mid f(x) \in \mathbb{Z}[x]\}$ .

$$R/J = \{f(x) + \langle 2 \rangle \mid f(x) \in \mathbb{Z}[x]\}$$

$$f(x) + \langle 2 \rangle = g(x) + \langle 2 \rangle$$

if  $2 \mid (f(x) - g(x))$ , meaning all coefficients of  $f(x) - g(x)$  are divisible by 2. Therefore,

$$\begin{aligned} f(x) + \langle 2 \rangle &= 5 + 4x + 7x^2 - 5x^3 + \langle 2 \rangle \\ &= (1 + (2)(2)) + 2(2x) + x^2 + 2(3x^2) - x^3 - 2(2x^3) + \langle 2 \rangle \\ &= 1 + x^2 - x^3 + \langle 2 \rangle \\ &= 1 + x^2 - 2(x^3) + x^3 + \langle 2 \rangle \\ &= 1 + x^2 + x^3 + \langle 2 \rangle. \end{aligned}$$

$$\begin{aligned} (1 + x + x^2 + \langle 2 \rangle) + (x + \langle 2 \rangle) &= 1 + 2x + x^2 + \langle 2 \rangle \\ &= 1 + x^2 + \langle 2 \rangle. \end{aligned}$$

Therefore, we can consider

$$\begin{aligned} \mathbb{Z}[x]/\langle 2 \rangle &= \mathbb{Z}[x]/2\mathbb{Z}[x] \\ &\cong \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

$$R/I = \mathbb{Z}[x]/\langle 2, x \rangle$$

$$\begin{aligned} f(x) + \langle 2, x \rangle &= a_n x^n + \cdots + a_1 x + a_0 + \langle 2, x \rangle \\ &= a_0 + \langle 2, x \rangle \\ &= \begin{cases} 0 & 2 \mid a_0 \\ 1 & 2 \nmid a_0 \end{cases}. \end{aligned}$$

So, we can consider

$$\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

**Isomorphism Example: Complex Numbers to Matrices**

Consider the set

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \text{Mat}_2(\mathbb{R}) \right\}.$$

We can verify that  $R$  is a ring.

Define

$$\begin{aligned} \varphi : \mathbb{C} &\rightarrow R \\ a + bi &\mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}. \end{aligned}$$

We can verify that  $\varphi$  is a bijective map.

Let  $a + bi, c + di \in \mathbb{C}$ . Then,

$$\begin{aligned} \varphi((a + bi) + (c + di)) &= \varphi((a + c) + (b + d)i) \\ &= \begin{bmatrix} a + c & b + d \\ -(b + d) & a + c \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \varphi(a + bi) + \varphi(c + di), \end{aligned}$$

and

$$\begin{aligned} \varphi((a + bi)(c + di)) &= \varphi((ac - bd) + (ad + bc)i) \\ &= \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix} \\ \varphi(a + bi)\varphi(c + di) &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix}. \end{aligned}$$

Therefore,  $\mathbb{C} \cong R$ .

## First Isomorphism Theorem

Let  $\varphi : R \rightarrow S$  be a homomorphism. We have  $R/\ker \varphi \cong \varphi(R)$ .

### Proof of the First Isomorphism Theorem

We want to show that  $R/\ker(\varphi) \cong \varphi(R)$ . Without loss of generality, assume  $\varphi$  is surjective. Let  $K = \ker(\varphi)$ .

We define  $\Phi : R/K \rightarrow S$ ,  $r + K \mapsto \varphi(r)$ . We must show that  $\Phi$  is a well-defined map. Let  $r_1 + K = r_2 + K$  (meaning  $r_1 - r_2 \in K$ ). This means  $r_1 = r_2 + k$  for some  $k \in K$ . Applying  $\Phi$ , we have

$$\begin{aligned}\Phi(r_1 + K) &= \varphi(r_1) \\ &= \varphi(r_2 + k) \\ &= \varphi(r_2) + \varphi(k) \\ &= \varphi(r_2) \\ &= \Phi(r_2 + K).\end{aligned}$$

Let  $r_1 + K, r_2 + K \in R/K$ . Observe

$$\begin{aligned}\Phi((r_1 + K) + (r_2 + K)) &= \Phi((r_1 + r_2) + K) \\ &= \varphi(r_1 + r_2) \\ &= \varphi(r_1) + \varphi(r_2) \\ &= \Phi(r_1 + K) + \Phi(r_2 + K),\end{aligned}$$

and

$$\begin{aligned}\Phi((r_1 + K)(r_2 + K)) &= \Phi(r_1 r_2 + K) \\ &= \varphi(r_1 r_2) \\ &= \varphi(r_1)\varphi(r_2) \\ &= \Phi(r_1 + K)\Phi(r_2 + K),\end{aligned}$$

meaning  $\Phi$  is a homomorphism.

Let  $s \in S$ . Since  $\varphi$  is surjective, there exists  $r \in R$  with  $\varphi(r) = s$ . So,  $\Phi(r + K) = \varphi(r) = s$ . Thus,  $\Phi$  is surjective.

Let  $r + K \in \ker(\Phi)$ . Then,

$$\begin{aligned}\Phi(r + K) &= 0_S \\ &= \varphi(r),\end{aligned}$$

meaning  $r \in \ker(\varphi) = K$ . So,  $r + K = 0_R + K = 0_{R/K}$ . Thus,  $\Phi$  is injective.

### Using the First Isomorphism Theorem: Example 1

Let  $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}/2\mathbb{Z}$ ,  $a_0 + a_1x + \cdots + a_nx^n \mapsto [a_0]_2$ .

To apply the first isomorphism theorem, we must check that this is a ring homomorphism. Let

$$\begin{aligned}f &= a_0 + a_1x + \cdots + a_mx^m \\ g &= b_0 + b_1x + \cdots + b_mx^m\end{aligned}$$

be elements in  $\mathbb{Z}[x]$ . Note that

$$\begin{aligned}\varphi(f + g) &= \varphi((a_0 + b_0) + \cdots) \\ &= [a_0 + b_0]_2 \\ &= [a_0]_2 + [b_0]_2 \\ &= \varphi(f) + \varphi(g)\end{aligned}$$

and

$$\begin{aligned}\varphi(fg) &= \varphi((a_0b_0) + \cdots) \\ &= [a_0b_0]_2 \\ &= [a_0]_2 + [b_0]_2 \\ &= \varphi(f)\varphi(g).\end{aligned}$$

So  $\varphi$  is a homomorphism. Note that  $\varphi(0) = [0]_2$  and  $\varphi(1) = [1]_2$ . The first isomorphism theorem gives that  $\mathbb{Z}[x]/\ker \varphi \cong \mathbb{Z}/2\mathbb{Z}$ .

We claim that  $\ker \varphi = \langle 2, x \rangle$ .

If  $2f(x) + xg(x) \in \langle 2, x \rangle$ , and we write  $f(x) = a_0 + a_1x + \cdots + a_nx^n$ , then

$$\begin{aligned}\varphi(2f(x) + g(x)) &= \varphi(2)\varphi(f(x)) + \varphi(x)\varphi(g(x)) \\ &= [0]_2[a_0]_2 + [0]_2\varphi(g(x)) \\ &= [0]_2,\end{aligned}$$

so  $\langle 2, x \rangle \subseteq \ker \varphi$ .

Let  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \ker(\varphi)$ , meaning

$$\begin{aligned}[0]_2 &= \varphi(f(x)) \\ &= [a_0]_2.\end{aligned}$$

Therefore,  $a_0 = 2k$ . So,

$$\begin{aligned}f(x) &= 2kx(a_1 + a_2x + \cdots + a_nx^{n-1}) \\ &\in \langle 2, x \rangle.\end{aligned}$$

Thus,  $\ker(\varphi) \subseteq \langle 2, x \rangle$ , meaning  $\ker(\varphi) = \langle 2, x \rangle$ .

By the first isomorphism theorem,  $\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{Z}/2\mathbb{Z}$ .

## Using the First Isomorphism Theorem: Example 2

We want to find the ring that is isomorphic to  $(\mathbb{Z} \times \mathbb{Z})/(2\mathbb{Z} \times 5\mathbb{Z})$ . We define

$$\begin{aligned}\varphi : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ (m, n) &\mapsto ([m]_2, [n]_5).\end{aligned}$$

We will start by showing homomorphism as follows:

$$\begin{aligned}\varphi((m_1, n_1) + (m_2, n_2)) &= \varphi((m_1 + m_2, n_1 + n_2)) \\ &= ([m_1 + m_2]_2, [n_1 + n_2]_5) \\ &= ([m_1]_2 + [m_2]_2, [n_1]_5 + [n_2]_5) \\ &= ([m_1]_2, [n_1]_5) + ([m_2]_2, [n_2]_5) \\ &= \varphi((m_1, n_1)) + \varphi((m_2, n_2)),\end{aligned}$$

and similarly for multiplication

$$\begin{aligned}\varphi((m_1, n_1)(m_2, n_2)) &= \varphi((m_1m_2, n_1n_2)) \\ &= ([m_1m_2]_2, [n_1n_2]_5) \\ &\vdots \\ &= \varphi((m_1, n_1))\varphi((m_2, n_2))\end{aligned}$$

Let  $([a]_2, [b]_5) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ . Then,  $\varphi((a, b)) = ([a]_2, [b]_5)$ . Thus,  $\varphi$  is surjective.

Finally, we have  $(m, n) \in \ker(\varphi)$  if and only if  $[m]_2 = [0]_2$  and  $[n]_5 = [0]_5$ , meaning  $m \in 2\mathbb{Z}$  and  $n \in 5\mathbb{Z}$ . Therefore,  $\ker(\varphi) = 2\mathbb{Z} \times 5\mathbb{Z}$ .

### Using the First Isomorphism Theorem: Example 3

Consider the map  $\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ,  $n \mapsto ([n]_2, [n]_5)$ . Note

$$\begin{aligned}\varphi(m+n) &= ([m+n]_2, [m+n]_5) \\ &= ([m]_2 + [n]_2, [m]_5 + [n]_5) \\ &= ([m]_2, [m]_5) + ([n]_2, [n]_5) \\ &= \varphi(m) + \varphi(n),\end{aligned}$$

and

$$\varphi(mn) = \varphi(m)\varphi(n).$$

We want to find if this map is surjective. Let  $([a]_2, [b]_5) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ . We are trying to find  $n \in \mathbb{Z}$  such that  $[n]_2 = [a]_2$  and  $[n]_5 = [b]_5$ , or  $n \equiv a$  modulo 2 and  $n \equiv b$  modulo 5.

$$\begin{aligned}n - a &\equiv 2k \text{ for some } k \in \mathbb{Z} \\ n &\equiv a + 2k \\ a + 2k &\equiv b \text{ modulo } 5 \\ 2k &\equiv b - a \text{ modulo } 5 \\ k &\equiv 3(b - a) \text{ modulo } 5 \\ n &\equiv a + 2(3(b - a)) \\ &\equiv a + 6(b - a).\end{aligned}$$

So  $\varphi(a + 6(b - a)) = ([a]_2, [b]_5)$ . Thus,  $\varphi$  is surjective.

Finally, we desire  $\ker(\varphi)$ . Observe that

$$\begin{aligned}\ker(\varphi) &= \{n \in \mathbb{Z} \mid [n]_2 = [0]_2, [n]_5 = [0]_5\} \\ &= \{n \in \mathbb{Z} \mid 2 \mid n, 5 \mid n\} \\ &= \{n \in \mathbb{Z} \mid 10 \mid n\} \\ &= 10\mathbb{Z}.\end{aligned}$$

Thus, the first isomorphism theorem gives  $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ .

### Proposition: Ring Homomorphisms and Ideals

Let  $R$  be a ring and  $I \subseteq R$  be an ideal. The map

$$\begin{aligned}\varphi : R &\rightarrow R/I \\ r &\mapsto r + I\end{aligned}$$

is a surjective ring homomorphism with  $\ker(\varphi) = I$ . The proof is left as an exercise to the reader.

### Using the First Isomorphism Theorem: Example 3

Let  $A$  be a ring and  $X$  be any non-empty set. Let  $R$  be the set of functions from  $X$  to  $A$ .

We have  $R$  is a ring.

$$\begin{aligned}(f+g)(x) &= f(x) +_A g(x) \\ (fg)(x) &= f(x) \cdot_A g(x).\end{aligned}$$

Fix  $x_0 \in X$ . We define  $E_{x_0} : R \rightarrow A$  by

$$E_{x_0}(f) = f(x_0).$$

We have

$$\begin{aligned}E_{x_0}(f+g) &= (f+g)(x_0) \\ &= f(x_0) +_A g(x_0) \\ &= E_{x_0}(f) +_A E_{x_0}(g)\end{aligned}$$

and

$$\begin{aligned} E(x_0)(fg) &= (fg)(x_0) \\ &= f(x_0)g(x_0) \\ &= E_{x_0}(f)E_{x_0}(g). \end{aligned}$$

Therefore,  $E_{x_0}$  is a homomorphism. Additionally,  $E_{x_0}$  is surjective, since we can find  $f_a : X \rightarrow A$ ,  $x \mapsto a$ , meaning  $E_{x_0}(f_a) = f_a(x_0) = a$ .

If  $f \in \ker(E_{x_0})$ , then  $E_{x_0}(f) = 0_A$ . However,  $E_{x_0}(f) = f(x_0)$ . Then,

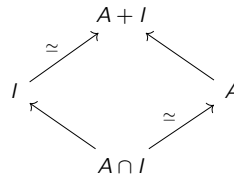
$$\begin{aligned} \ker(\varphi) &= \{f : X \rightarrow A \mid f(x_0) = 0_A\} \\ &= \mathcal{M}_{x_0}. \end{aligned}$$

By the first isomorphism theorem, we can see that  $R/\mathcal{M}_{x_0} \cong A$ .

## Other Isomorphism Theorems

Let  $R$  be a ring.

**Diamond Isomorphism Theorem:** Let  $A$  be a subring of  $R$  and  $I$  an ideal of  $R$ . Define  $A + I = \{a + i \mid a \in A, i \in I\}$ . This is an ideal of  $R$ . We also have that  $A \cap I$  is an ideal in  $A$ , and  $(A + I)/I \cong A/A \cap I$ .



**Third Isomorphism Theorem:** Let  $I, J$  be ideals of  $R$  with  $I \subseteq J$ . Then,  $J/I$  is an ideal of  $R/I$  with  $(R/I)/(J/I) \cong R/J$ .

**Lattice Isomorphism Theorem:** Let  $I \subseteq R$  be an ideal. The correspondence  $A \leftrightarrow A/I$  is an inclusion-preserving bijection between the subrings  $A$  of  $R$  that contain  $I$  and the subrings of  $R/I$ . Moreover,  $A$  is an ideal if and only if  $A/I$  is an ideal.

## Using the Third Isomorphism Theorem

Let  $R = \mathbb{Z}$ ,  $I = 12\mathbb{Z}$ , and  $J = 4\mathbb{Z}$ . By the third isomorphism theorem,  $J/I = 4\mathbb{Z}/12\mathbb{Z}$  is an ideal of  $R/I = \mathbb{Z}/12\mathbb{Z}$ , and

$$\begin{aligned} (R/I)/(J/I) &= (\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z}) \\ &\cong \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

## Applying the Isomorphism Theorems

Consider the rings  $3\mathbb{Z}$  and  $12\mathbb{Z}$ . We have that  $12\mathbb{Z} \subseteq 3\mathbb{Z}$  as an ideal. Therefore, we can form the quotient ring  $3\mathbb{Z}/12\mathbb{Z}$ . We might ask how it's related to other  $\mathbb{Z}/n\mathbb{Z}$ , or to  $\mathbb{Z}/12\mathbb{Z}$ .

Note that  $3\mathbb{Z}/12\mathbb{Z}$  starts with elements in  $3\mathbb{Z}$  and examines elements in  $12\mathbb{Z}$ . We might ask whether or not  $3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$ . However,

$$\begin{aligned} 3\mathbb{Z}/12\mathbb{Z} &= \{a + 12\mathbb{Z} \mid a \in 3\mathbb{Z}\} \\ &= \{3b + 12\mathbb{Z} \mid b \in \mathbb{Z}\}. \end{aligned}$$

We can define

$$\begin{aligned} \varphi : 3\mathbb{Z} &\rightarrow \mathbb{Z}/4\mathbb{Z} \\ 0 + 12\mathbb{Z} &\mapsto [0]_4, \\ 3 + 12\mathbb{Z} &\mapsto [3]_4, \\ 6 + 12\mathbb{Z} &\mapsto [2]_4, \\ 9 + 12\mathbb{Z} &\mapsto [1]_4. \end{aligned}$$

which we look at by aiming for  $12\mathbb{Z}$  to be the kernel of  $\varphi$ . Then, by the first isomorphism theorem,  $3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$ .

If we want to examine  $3\mathbb{Z}/12\mathbb{Z}$  in relation to  $\mathbb{Z}/12\mathbb{Z}$ , we see that  $3\mathbb{Z}/12\mathbb{Z} \cong \langle [3]_{12} \rangle \subseteq \mathbb{Z}/12\mathbb{Z}$ .



## Further Examination of Ideals

Let  $I, J \subseteq R$  be ideals. We define

- (1) the sum,  $I + J = \{i + j \mid i \in I, j \in J\}$ ,
- (2) the product,  $IJ$ , the collection of finite sums of elements of the form  $xy$ , where  $x \in I$  and  $y \in J$ , and
- (3) The  $n$ th power of  $I$ , denoted  $I^n$ , which is the collection of finite sums of elements of the form  $x_1, \dots, x_n \in I$ .

**Exercises:**

- (1)  $I + J$  is the smallest ideal containing  $I$  and  $J$ .
- (2)  $IJ \subseteq I \cap J$ .

Let  $R$  be a ring with  $1_R \neq 0_R$ . Let  $A \subseteq R$ .

- (1) Let  $\langle A \rangle$  be the smallest ideal that contains  $A$ . It is called the ideal *generated* by  $A$ .
- (2) We set  $RA = \{r_1 a_1 + \dots + r_n a_n \mid r_i \in R, a_i \in A\}$  for any  $n \in \mathbb{Z}_{\geq 0}$ . Additionally,  $AR$  is analogous to  $RA$ . We set  $RAR = \{r_1 a_1 \tilde{r}_1 + \dots + r_n a_n \tilde{r}_n \mid r_i, \tilde{r}_i \in R, a_i \in A\}$ .
- (3) If  $A$  is a single element  $a$ , we write  $\langle a \rangle$  to denote the ideal generated by  $A$  and refer to this as a principal ideal. If  $A$  is finite, then we say  $\langle A \rangle$  is a finitely generated ideal.

For example, if  $R = \mathbb{Z}[x_1, x_2, \dots]$ , then  $I = \langle x_1, x_2, \dots \rangle$  is not finitely generated.

**Note:** If  $R$  is commutative, then  $\langle a \rangle = Ra$  and if  $R$  is not commutative,  $\langle a \rangle = RaR$ . For  $R$  commutative, we say that for  $b \in \langle a \rangle$ ,  $b = ra$  for some  $r \in R$ . We say  $a$  divides  $b$  — if  $a$  divides  $b$ , then  $\langle b \rangle \subseteq \langle a \rangle$ .

### Principal Ideal: Example 1

Every ideal in  $\mathbb{Z}$  is a principal ideal.

Let  $I \subseteq \mathbb{Z}$  be a nonzero ideal (the zero ideal is generated by 0). Let  $m \in I, m \neq 0$ . Since  $I$  is an ideal, if  $m \in I$ , so too is  $-m \in I$ . Therefore, we know there is a positive integer in  $I$ .

By the well-ordering principle, let  $n \in I$  be the smallest positive integer in  $I$ . Let  $a \in I, a \neq 0$ . Write  $a = nq + r$  for  $q, r \in \mathbb{Z}$ , and  $0 \leq r < n$ . Then, we have  $r = a - nq$ . Since  $a \in I$  and  $n \in I, r \in I$ . Therefore,  $r = 0$ , and  $n \mid a$ . Thus,  $I = n\mathbb{Z}$ .

### Principal Ideal: Example 2

Let  $R = \mathbb{Z}[x]$ . Consider  $I = \langle 2, x \rangle$ . We claim that  $I$  is not a principal ideal.

Suppose toward contradiction that  $\langle 2, x \rangle = \langle f(x) \rangle$  for some  $f(x) \in \mathbb{Z}[x]$ . Therefore,  $2 = f(x)g(x)$  for some  $g(x) \in \mathbb{Z}[x]$ . Since degrees add,  $\deg(2) = \deg(f) + \deg(g)$ , or  $0 = \deg(f) + \deg(g)$ . Therefore,  $f(x), g(x) \in \mathbb{Z}$ . Therefore, we must have that  $f(x) \in \{\pm 1, \pm 2\}$ .

So, we have elements of  $\langle 2, x \rangle$  of the form  $2s(x) + xt(x)$ . So we have constant term divisible by 2, meaning  $f(x) \neq \pm 1$ , so  $f(x) = \pm 2$ .

Then,  $x = 2h(x)$  for some  $h(x) \in \mathbb{Z}[x]$ . However, we have that  $h(x)$  has integer coefficients. Therefore,  $\langle 2, x \rangle \neq \langle f(x) \rangle$  for any  $f(x) \in \mathbb{Z}[x]$ .

### Proposition: Ideals in Unital Rings

Let  $I$  be an ideal of  $R$ .

- (1)  $I = R$  if and only if  $I$  contains a unit.
- (2) If  $R$  is commutative, then  $R$  is a field if and only if the only ideals in  $R$  are  $\langle 0_R \rangle$  and  $R$ .

**Proof of (1):** Suppose  $I = R$ . Then,  $1_R \in I$ , and  $1_R$  is a unit.

Suppose  $I$  contains a unit,  $u$ . Then, we have  $u^{-1} \in R$ . Since  $I$  is an ideal, we have  $uu^{-1} \in I$ , and  $uu^{-1} = 1_R$ . Letting  $r \in R$ , using the fact that  $I$  is an ideal,  $(r)(1_R) = r \in I$ . Thus,  $I = R$ .

**Proof of (2):** Suppose  $R$  is a field. Let  $I$  be any nonzero ideal. Every nonzero element in  $I$  is a unit, meaning  $I = R$ .

Suppose  $\langle 0_R \rangle$  and  $R$  are the only ideals in  $R$ . Let  $r \in R, r \neq 0_R$ . Since  $r \neq 0$ ,  $\langle r \rangle = R$ . Thus,  $1_R \in \langle r \rangle$ . Thus,  $1_R = sr$  for some  $s \in R$ , implying every nonzero element of  $R$  has an inverse.

### Corollary: Field Homomorphisms

Let  $F$  be a field, and  $\varphi : F \rightarrow R$  be a homomorphism. Then,  $\varphi$  is either the zero map ( $\varphi(f) = 0_R$ ) or  $\varphi$  is injective.

Proof: Since  $\ker(\varphi)$  is an ideal in  $F$  by the first isomorphism theorem, then  $\ker(\varphi) = \langle 0_F \rangle$  or  $\ker(\varphi) = R$ . If  $\ker(\varphi) = \langle 0_F \rangle$ , then  $\varphi$  is injective, and if  $\ker(\varphi) = F$ , then  $\varphi$  is the zero map.

### Maximal Ideals

- (1) An ideal  $\mathcal{M} \subseteq R$  is a maximal ideal if  $\mathcal{M} \neq R$  and the only ideals containing  $\mathcal{M}$  are  $\mathcal{M}$  and  $R$ . The collection of maximal ideals is denoted  $\text{m-spec}(R)$  or  $\text{maxspec}(R)$ .
- (2) An ideal  $\mathfrak{p} \subseteq R$  with  $\mathfrak{p} \neq R$  is a prime ideal if whenever  $ab \in \mathfrak{p}$ , then  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ . We denote the collection of prime ideals  $\text{Spec}(R)$ .

For example,  $\text{Spec}(\mathbb{Z}) = \{0\mathbb{Z}, p\mathbb{Z}\}$  for  $p$  prime, and  $\text{maxspec}(\mathbb{Z}) = \{p\mathbb{Z}\}$ .

**Aside:** Let  $R$  be commutative. The set  $\text{Spec}(R)$  is a topological space. Let  $A \subseteq R$  be any subset. Closed sets look like

$$\begin{aligned} V(A) &= \{\mathcal{P} \in \text{Spec}(R) \mid A \subseteq \mathcal{P}\} \\ &= V(I) \\ &= \langle A \rangle \end{aligned}$$

For example, if  $R = \mathbb{R}[x, y]$ , if  $f(x, y) = y - x^2$ , then  $V(f) = \{(a, b) \in \mathbb{R}^2 \mid f(a, b) = 0\}$ . The topology on  $\text{Spec}(R)$  is called the Zariski topology.

Let  $\varphi : R \rightarrow S$  be a ring homomorphism. If  $\mathcal{P} \in \text{Spec}(S)$ , then  $\varphi^{-1}(\mathcal{P})$  is a prime ideal in  $R$ . We get a map  $\varphi^*(\text{Spec}(S)) \rightarrow \text{Spec}(R)$  given by  $\mathcal{P} \mapsto \varphi^{-1}(\mathcal{P})$ .

We get a contravariant functor that takes  $R \mapsto \text{Spec}(R)$ , mapping from the category of rings to the category of topological spaces.

### Proposition: Existence of Maximal Ideals

Let  $R$  be a ring. Every proper ideal is contained in a maximal ideal.

Let  $I$  be a proper ideal. Let  $\mathcal{S}$  be the collection of all proper ideals that contain  $I$ . We know that  $\mathcal{S}$  is non-empty as  $I \in \mathcal{S}$ . Then,  $\mathcal{S}$  has a partial ordering under inclusion.

Let  $\mathcal{C}$  be a chain of ideals (that is, totally ordered subset) in  $\mathcal{S}$ , and

$$J = \bigcup_{A \in \mathcal{C}} A.$$

Since  $\mathcal{C} \neq \emptyset$ , there is at least one  $A$  in the union with  $0_R \in A$ . So,  $J \neq \emptyset$ . Let  $a, b \in J$ . There exists  $A$  with  $a \in A$  and  $b \in A$ . Since  $\mathcal{C}$  is a chain, either  $A \subseteq B$  or  $B \subseteq A$ . So,  $a$  and  $b$  are both in either  $A$  or  $B$ . Thus,  $a - b$  and  $ab$  are in either  $A$  or  $B$ . Thus,  $a - b$  and  $ab$  are elements in  $J$ , meaning  $J$  is an ideal.

If  $J = R$ , then  $1_R \in J$ , meaning  $1_R$  is an element of some  $A \in \mathcal{C}$ . Since  $A \in \mathcal{S}$  is a proper ideal, this would be a contradiction.

Therefore,  $J$  is an upper bound for  $\mathcal{C}$ . Since every chain in  $\mathcal{S}$  has an upper bound in  $\mathcal{S}$ , then, by Zorn's Lemma, there is a maximal element in  $\mathcal{S}$ .

### Proposition: Maximal Ideals, Quotient Rings, and Fields

An ideal  $\mathcal{M} \subseteq R$  of a commutative ring with identity is maximal if and only if  $R/\mathcal{M}$  is a field.

Suppose  $\mathcal{M}$  is maximal. Let  $x + \mathcal{M} \neq 0 + \mathcal{M}$ . We want to show that  $x + \mathcal{M}$  has an inverse.

Consider  $\langle x, \mathcal{M} \rangle$ , the ideal generated by  $x$  and  $\mathcal{M}$ . We have  $\mathcal{M} \subset \langle x, \mathcal{M} \rangle$ , as  $x \notin \mathcal{M}$ . Therefore,  $\langle x, \mathcal{M} \rangle = R$  by the definition of a maximal ideal. Therefore,  $1_R \in \langle x, \mathcal{M} \rangle$ , meaning  $1_R = xu + mv$  for some  $u, v \in R$ ,  $m \in \mathcal{M}$ . Note

$$\begin{aligned} (x + \mathcal{M})(u + \mathcal{M}) &= xu + \mathcal{M} \\ &= (1_R - mv) + \mathcal{M} \\ &= 1_R + \mathcal{M}, \end{aligned}$$

meaning  $x + \mathcal{M}$  has an inverse, meaning  $R/\mathcal{M}$  is a field.

Suppose  $R/\mathcal{M}$  is a field. Assume we have  $\mathcal{M} \subset I \subset R$  for some ideal  $I$ . From the third isomorphism theorem, we have  $I/\mathcal{M}$  is an ideal of  $R/\mathcal{M}$ . Specifically, by our construction,  $I/\mathcal{M}$  is a proper nonzero ideal of  $R/\mathcal{M}$ , but since  $R/\mathcal{M}$  is a field, no such proper nonzero ideal exists, meaning no such  $I$  exists.

### Examples: Maximal Ideals

- (1) Let  $R = \mathbb{Z}$ . Given  $m \in \mathbb{Z}$ , we know  $m\mathbb{Z}$  is a maximal ideal if and only if  $m$  is prime. If  $p|m$  and  $p \neq m$ , then  $m\mathbb{Z} \subseteq p\mathbb{Z}$ . Additionally, if  $p$  is prime, then  $\mathbb{Z}/p\mathbb{Z}$  is a field. Additionally,  $\mathbb{Z}/m\mathbb{Z}$  is not an integral domain if  $m$  is composite.
- (2) Let  $R = F[x]$  for  $F$  a field. Let  $\alpha \in F$  and consider  $\mathcal{M}_\alpha = \langle x - \alpha \rangle$ . We claim that  $F[x]/\mathcal{M}_\alpha \cong \mathcal{F}$ , meaning  $\mathcal{M}$  is a maximal ideal.

Let  $\varphi : F[x] \rightarrow F$ ,  $x \mapsto \alpha$ ,  $f(x) \mapsto f(\alpha)$ . Let  $f(x), g(x) \in F[x]$ . Then,

$$\begin{aligned}\varphi(f + g) &= (f + g)(\alpha) \\ &= f(\alpha) + g(\alpha) \\ &= \varphi(f) + \varphi(g)\end{aligned}$$

and

$$\begin{aligned}\varphi(fg) &= (fg)(\alpha) \\ &= f(\alpha)g(\alpha) \\ &= \varphi(f)\varphi(g).\end{aligned}$$

Let  $\beta \in F$ . Then,

$$\begin{aligned}\varphi(\beta + (x - \alpha)) &= \beta + (\alpha - \alpha) \\ &= \beta.\end{aligned}$$

Thus,  $\varphi$  is surjective. Finally, we have  $f(x) \in \ker(\varphi)$  if and only if  $f(\alpha) = 0$ . However,  $f(\alpha) = 0$  if and only if  $(x - \alpha)|f(x)$ . Therefore,  $\ker(\varphi) = \langle x - \alpha \rangle$ .

- (3) Let  $R = \mathbb{Z}[x]$ . Let  $\mathcal{M} = \langle 2, x \rangle$ . We saw that  $\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ . Therefore, we know that  $\mathcal{M}$  is a maximal ideal by the above categorization.
- (4) Let  $R = \mathbb{F}_2[x]$ . Consider the ideal  $\mathcal{M} = \langle x^2 + x + 1 \rangle$ .

$$\begin{aligned}R/\mathcal{M} &= \{f(x) + \langle x^2 + x + 1 \rangle \mid f(x) \in \mathbb{F}_2[x]\} \\ f(x) &= \{(x^2 + x + 1)q(x) + r(x) \mid q(x), r(x) \in \mathbb{F}_2[x], r(x) = 0 \text{ or } \deg r(x) < 2\}.\end{aligned}$$

So,

$$f(x) + \mathcal{M} = r(x) + \mathcal{M},$$

meaning

$$R\mathcal{M} = \{0 + \mathcal{M}, 1 + \mathcal{M}, x + \mathcal{M}, 1 + x + \mathcal{M}\}.$$

This is a field.

+	$0 + \mathcal{M}$	$1 + \mathcal{M}$	$x + \mathcal{M}$	$x + 1 + \mathcal{M}$
$0 + \mathcal{M}$	0	1	x	x + 1
$1 + \mathcal{M}$	1	0	1 + x	x
$x + \mathcal{M}$	x	1 + x	0	1
$x + 1 + \mathcal{M}$	1 + x	x	1	0
×	$0 + \mathcal{M}$	$1 + \mathcal{M}$	$x + \mathcal{M}$	$x + 1 + \mathcal{M}$
$0 + \mathcal{M}$	0	0	0	0
$1 + \mathcal{M}$	0	1	x	x + 1
$x + \mathcal{M}$	0	x	1 + x	1
$x + 1 + \mathcal{M}$	0	1 + x	x	1

Specifically, this is a field of order 4. Note that  $\mathbb{F}_2 \hookrightarrow R/\mathcal{M}$ . We say  $R/\mathcal{M} \cong \mathbb{F}_4$ .

**Note:** For every  $p$  prime and every  $n \in \mathbb{Z}$  positive, there is exactly one field of order  $p^n$  up to isomorphism.

- (5) Let  $R = \mathbb{Z}[i]$ . Set  $\mathcal{M} = \langle 3 \rangle$ . This is a maximal ideal, and  $|\mathbb{Z}[i]/\langle 3 \rangle| = 9$ .

### Proposition: Prime Ideals, Quotient Rings, and Integral Domains

Let  $R$  be a commutative ring with identity. An ideal  $\mathfrak{p} \subseteq R$  is a prime ideal if and only if  $R/\mathfrak{p}$  is an integral domain.

Let  $\mathfrak{p} \subseteq R$  be a prime ideal. Let  $x, y \in R$  with  $(x + \mathfrak{p})(y + \mathfrak{p}) = 0 + \mathfrak{p}$ . We have

$$xy + \mathfrak{p} = 0 + \mathfrak{p}$$

meaning

$$xy \in \mathfrak{p},$$

so, since  $\mathfrak{p}$  is prime,

$$x \in \mathfrak{p}$$

or

$$y \in \mathfrak{p}$$

so  $x + \mathfrak{p} = 0 + \mathfrak{p}$  or  $y + \mathfrak{p} = 0 + \mathfrak{p}$ .

In the reverse direction, assume  $R/\mathfrak{p}$  is an integral domain. Let  $xy \in \mathfrak{p}$ . Then,

$$\begin{aligned} (x + \mathfrak{p})(y + \mathfrak{p}) &= xy + \mathfrak{p} \\ &= 0 + \mathfrak{p}, \end{aligned}$$

implying that  $x + \mathfrak{p}$  or  $y + \mathfrak{p}$  is equal to  $0 + \mathfrak{p}$ , or  $x \in \mathfrak{p}$  or  $y \in \mathfrak{p}$ .

### Examples: Prime Ideals

(1) If  $R = \mathbb{Z}[x]$ , then  $\mathfrak{p} = \langle x \rangle$  is a prime ideal that is not a maximal ideal, as  $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ .

### Corollary: Maximal Ideals and Prime Ideals

Let  $R$  be a commutative ring with identity. Then,  $\text{maxspec}(R) \subseteq \text{Spec}(R)$ .

### Direct Products

Let  $R$  and  $S$  be rings. The set

$$R \times S = \{(r, s) \mid r \in R, s \in S\}$$

is a ring under component-wise multiplication and addition.

**Exercise:** Let  $R_1, \dots, R_n$  be rings. Let

$$\varphi : R \rightarrow R_1 \times \dots \times R_n$$

be a map. Define

$$\begin{aligned} \pi_j : R_1 \times \dots \times R_n &\rightarrow R_j \\ (r_1, \dots, r_n) &\mapsto r_j. \end{aligned}$$

Show  $\varphi$  is a homomorphism if and only if  $\pi_j \circ \varphi$  is a homomorphism for each  $j$ .

### Comaximal Ideals

Recall that  $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$ . If  $\gcd(a, b) = 1$ , then  $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ . Conversely, if  $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ , then  $am + bn = 1$  for some  $m, n \in \mathbb{Z}$ . Thus,  $\gcd(a, b) = 1$ .

Let  $I, J$  be ideals in a commutative ring  $R$ . We say  $I$  and  $J$  are comaximal if  $I + J = R$ .

## Chinese Remainder Theorem

Let  $I_1, \dots, I_n$  be ideals in a commutative ring  $R$ . The map

$$\begin{aligned}\varphi : R &\rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_n \\ r &\mapsto (r + I_1, r + I_2, \dots, r + I_n)\end{aligned}$$

is a ring homomorphism with kernel  $I_1 \cap \dots \cap I_n$ . If  $I_i, I_j$  are comaximal for all  $1 \leq i, j \leq n$  with  $i \neq j$ , then  $\varphi$  is surjective, and  $I_1 \cap \dots \cap I_n = (I_1)(I_2) \dots (I_n)$ , so

$$R / ((I_1)(I_2) \dots (I_n)) \cong R / (I_1 \cap \dots \cap I_n) \cong R / I_1 \times \dots \times R / I_n.$$

### Corollary to the Chinese Remainder Theorem (1)

Let  $n = p_1^{e_1} \dots p_r^{e_r} \in \mathbb{Z}$ . Then,

$$\mathbb{Z} / n\mathbb{Z} \cong \mathbb{Z} / p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z} / p_r^{e_r}\mathbb{Z}.$$

Moreover,

$$(\mathbb{Z} / n\mathbb{Z})^\times \cong (\mathbb{Z} / p_1^{e_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z} / p_r^{e_r}\mathbb{Z})^\times.$$

### Corollary to the Chinese Remainder Theorem (2)

Let  $n_1, \dots, n_k$  be positive integers that are pairwise relatively prime. Then, for any  $a_1, \dots, a_k \in \mathbb{Z}$ , there is a  $x \in \mathbb{Z}$  satisfying

$$\begin{aligned}x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k}\end{aligned}$$

This solution is unique modulo  $n_1, \dots, n_k$ . If we set

$$m_i = n_1 \dots \hat{n}_i \dots n_k,$$

and  $y_i$  as the inverse of  $m_i \pmod{n_i}$ . The solution  $x$  is given by

$$x = a_1 y_1 m_1 + \dots + a_k y_k m_k.$$

We will prove the Chinese Remainder Theorem by induction, with the base case of  $n = 2$ :

$$\begin{aligned}\varphi : R &\rightarrow R/I_1 \times R/I_2 \\ r &\mapsto (r + I_1, r + I_2).\end{aligned}$$

We can verify that this is a homomorphism, with  $\ker(\varphi) = I_1 \cap I_2$ . Assume  $I_1$  and  $I_2$  are comaximal:  $I_1 + I_2 = R$ . In particular, there exist  $x \in I_1$  and  $y \in I_2$  such that  $x + y = 1_R$ . Note that

$$\begin{aligned}\varphi(x) &= (x + I_1, x + I_2) \\ &= (0 + I_1, 1_R - y + I_2) \\ &= (0 + I_1, 1_R + I_2)\end{aligned}$$

and

$$\varphi(y) = (1_R + I_1, 0 + I_2).$$

Let  $(r_1 + I_1, r_2 + I_2) \in R/I_1 \times R/I_2$ . Set  $z = r_2 x + r_1 y$ . Then,

$$\begin{aligned}\varphi(z) &= (r_2 x + r_1 y + I_1, r_2 x + r_1 y + I_2) \\ &= (r_1 + I_1, r_2 + I_2).\end{aligned}$$

So,  $\varphi$  is surjective, and we get  $R/I_1 \cap I_2 \cong R/I_1 \times R/I_2$ .

We also have that  $(I_1)(I_2) \subseteq I_1 \cap I_2$ . Let  $z \in I_1 \cap I_2$ . We have

$$\begin{aligned}z &= z(1_R) \\ &= z(x + y) \\ &= zx + zy \\ &\in (I_1)(I_2).\end{aligned}$$

Therefore,  $R/(I_1)(I_2) \cong R/I_1 \cap I_2$ .

Suppose the result holds for all values up to  $2 \leq n \leq k-1$ . Write  $J_1 = I_1$  and  $J_2 = (I_2)(I_3) \cdots (I_k)$ . We only need to show that  $J_1$  and  $J_2$  are comaximal, then apply  $n=2$  to  $J_1, J_2$  and  $n=k-1$  to split up  $J_2$ .

For each  $i \in \{2, \dots, k\}$ , there are elements  $x_i \in I_1$  and  $y_i \in I_i$  such that  $x_i + y_i = 1_R$ . We have  $x_i + y_i \equiv y_i \pmod{I_1}$ , so

$$1_R = (x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k)$$

is an element of  $J_1 + J_2$ .

## Localization

Where does  $\mathbb{Q}$  come from?

Consider the sets  $\mathbb{Z}$  and  $\Sigma = \mathbb{Z} \setminus \{0\}$ . Set

$$\Sigma^{-1}\mathbb{Z} = \{(a, b) \mid a \in \mathbb{Z}, b \in \Sigma\}.$$

Define  $\sim$  on  $\Sigma^{-1}\mathbb{Z}$  by

$$(a, b) \sim (c, d) \text{ if } ad = bc.$$

This is an equivalence relation:

**Reflexivity:**

$$\begin{aligned} (a, b) &\sim (a, b) \\ ab &= ab. \end{aligned}$$

**Symmetry:**

$$\begin{aligned} (a, b) &\sim (c, d) \\ ad &= bc \\ bc &= ad \\ (c, d) &= (a, b) \end{aligned}$$

**Transitivity:** Suppose  $(a, b) \sim (c, d)$  and  $(c, d) \sim (e, f)$ , meaning  $ad = bc$  and  $cf = de$ . We need to show  $af = be$ .

$$\begin{aligned} ad - bc &= 0 \\ cf - de &= 0 \\ adf - bcf &= 0 \\ bcf - bde &= 0 \\ (adf - bcf) + (bcf - bde) &= 0 \\ (af - be)(d) &= 0 \end{aligned}$$

and since  $d \neq 0$  and we are in  $\mathbb{Z}$ ,

$$af = be,$$

meaning  $(a, b) \sim (e, f)$ .

Let  $\frac{a}{b}$  denote the equivalence class containing  $(a, b)$ . We define

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

**Exercise:** Show that addition and multiplication are well-defined, and make the collection of equivalence classes into a field.

The field of equivalence classes  $\Sigma^{-1}\mathbb{Z}$  under the defined addition and multiplication forms the field  $\mathbb{Q}$ .

Let  $R$  be a ring. We say  $\Sigma \subseteq R$  is multiplicatively closed if, given  $a, b \in \Sigma$ ,  $ab \in \Sigma$ .

- (1)  $\Sigma = \mathbb{Z} \setminus \{0\}$  is multiplicatively closed.
- (2) Let  $r \in R$ . Then,  $\Sigma = \{r^n \mid n \in \mathbb{Z}\}$ .
- (3) Let  $\mathfrak{p} \in R$ . Then,  $R \setminus \mathfrak{p}$  is multiplicatively closed (verify this).

## Universal Property

Let  $R$  be a commutative ring with identity and  $\Sigma \subseteq R$  a multiplicatively closed subset with  $1_R \in \Sigma$ . There is a unique commutative ring  $\Sigma^{-1}R$  and ring homomorphism

$$\pi : R \rightarrow \Sigma^{-1}R$$

satisfying for any homomorphism  $\psi : R \rightarrow S$  that sends  $1_R$  to  $1_S$  and  $\psi(\Sigma) \subseteq S^\times$ , there is a unique homomorphism

$$\Psi : \Sigma^{-1}R \rightarrow S$$

such that  $\Psi \circ \pi = \psi$ .

$$\begin{array}{ccc} R & \xrightarrow{\pi} & \Sigma^{-1}R \\ & \searrow \psi & \downarrow \Psi \\ & & S \end{array}$$

Let  $\mathcal{F} = \{(r, d) \mid r \in R, d \in \Sigma\}$ . Define a relation  $(r_1, d_1) \sim (r_2, d_2)$  if  $x(r_1 d_2 - r_2 d_1) = 0$  for some  $x \in \Sigma$ .

We claim that  $\sim$  is an equivalence relation.

- (i) It is clear that  $(r, d) \sim (r, d)$ .
- (ii) If  $(r_1, d_1) \sim (r_2, d_2)$ , it is clear that  $(r_2, d_2) \sim (r_1, d_1)$ .
- (iii) Suppose  $(r_1, d_1) \sim (r_2, d_2)$ , and  $(r_2, d_2) \sim (r_3, d_3)$ . We have  $x, y \in \Sigma$  such that

$$\begin{aligned} x(r_1 d_2 - r_2 d_1) &= 0 \\ y(r_2 d_3 - r_3 d_2) &= 0. \end{aligned}$$

Therefore, we have

$$\begin{aligned} d_3 y x (r_1 d_2 - r_2 d_1) &= 0 \\ d_1 x y (r_2 d_3 - r_3 d_2) &= 0. \end{aligned}$$

Adding together, we have

$$\begin{aligned} d_3 y x (r_1 d_2 - r_2 d_1) + d_1 x y (r_2 d_3 - r_3 d_2) &= d_3 x y r_1 d_2 - d_1 x y r_3 d_2 \\ d_2 x y (r_1 d_3 - r_3 d_1) &= 0 \end{aligned}$$

Since  $d_2, x, y \in \Sigma$ ,  $d_2 x y \in \Sigma$ , and we have  $(r_1, d_1) \sim (r_3, d_3)$ .

Since  $\sim$  is an equivalence relation on  $\mathcal{F}$ , we set  $\Sigma^{-1}R$  to be the equivalence classes of  $\sim$  on  $\mathcal{F}$ . We denote the equivalence class containing  $(r, d)$  as  $\frac{r}{d}$ . We define addition and multiplication as

$$\begin{aligned} \frac{r_1}{d_1} + \frac{r_2}{d_2} &= \frac{r_1 d_2 + r_2 d_1}{d_1 d_2} \\ \frac{r_1}{d_1} \frac{r_2}{d_2} &= \frac{r_1 r_2}{d_1 d_2}. \end{aligned}$$

These operations are well defined, and make  $\Sigma^{-1}R$  into a commutative ring with  $1_{\Sigma^{-1}R} = \frac{1}{1}$ .

Defining  $\pi : R \rightarrow \Sigma^{-1}R$  with  $r \mapsto \frac{r}{1}$ , we can verify that  $\pi$  is a homomorphism. Let  $\psi : R \rightarrow S$  with  $\psi(\Sigma) \subseteq S^\times$ , and  $\psi(1_R) = 1_S$ . Then, we define  $\Psi : \Sigma^{-1}R \rightarrow S$  as  $\frac{r}{d} \mapsto \psi(r)\psi(d)^{-1}$ .

To show this map is well-defined, let  $\frac{a}{b} = \frac{c}{d}$ . So,  $x(ad - bc) = 0$  for some  $x \in \Sigma$ . Since  $\psi$  is a homomorphism,

$$\psi(x)(\psi(a)\psi(d) - \psi(b)\psi(c)) = 0.$$

Since  $x \in \Sigma$ ,  $\psi(x) \in S^\times$ , meaning

$$\psi(a)\psi(d) - \psi(b)\psi(c) = 0.$$

Since  $b, d \in \Sigma$ ,  $\psi(b), \psi(d) \in S^\times$ . Therefore,

$$\begin{aligned} \psi(a)\psi(d) &= \psi(c)\psi(b) \\ \psi(a)\psi(b)^{-1} &= \psi(c)\psi(d)^{-1}. \end{aligned}$$

We can easily verify that  $\Psi$  is a ring homomorphism, and  $\Psi \circ \pi = \psi$ .

For example, if  $R = \mathbb{Z}$  and  $\Sigma = \mathbb{Z} \setminus \{0\}$ , then  $\Sigma^{-1}\mathbb{Z} = \mathbb{Q}$ , then for  $\pi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ , and a homomorphism from  $\mathbb{Z}$  into a set  $S$ , there must exist a map from  $\mathbb{Q}$  to  $S$ .

Consider  $\mathbb{Z}$  with  $\Sigma = \mathbb{Z} \setminus p\mathbb{Z}$ . Then,  $\Sigma^{-1}\mathbb{Z} = \{(a, b) \mid a \in \mathbb{Z}, p \nmid b\} = \mathbb{Z}_{(p)}$ . We saw on an earlier homework assignment that  $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$ , meaning it is a maximal ideal (as if  $a \nmid p$ , then  $a/b$  is a unit in  $\mathbb{Z}_{(p)}$ ). The only other ideals are  $p^m\mathbb{Z}_{(p)}$ , so we have a chain

$$p\mathbb{Z}_{(p)} \supseteq p^2\mathbb{Z}_{(p)} \supseteq \cdots.$$

### Corollary to the Universal Property

Given  $\pi$ ,  $\psi$ , and  $\Psi$  as defined above, we have the following.

- (1)  $\ker \pi = \{r \in R \mid xr = 0 \text{ for some } x \in \Sigma\}$ . In particular,  $\pi$  is an injection if  $\Sigma$  does not contain zero or any zero divisors.
- (2)  $\Sigma^{-1}R = 0$  if and only if  $0 \in \Sigma$ .

Recall that  $\pi(r) = \frac{r}{1}$ . Recall that  $r \in \ker \pi$  if and only if  $\frac{r}{1} = \frac{0}{1}$ , which is true if and only if  $x(r \cdot 1 - 0 \cdot 1) = 0$  for some  $x \in \Sigma$ , meaning  $xr = 0$ .

$\Sigma^{-1}R = 0$  if and only if  $(1, 1) \sim (0, 1)$ , which is true if and only if  $x \cdot 1 = 0$  for some  $x \in \Sigma$ , which is only true if  $x = 0 \in \Sigma$ .

The ring  $\Sigma^{-1}R$  is called the localization of  $R$  at  $\Sigma$ . If  $R$  is an integral domain and  $\Sigma = R \setminus \{0\}$ , then  $\Sigma^{-1}R$  is known as the field of fractions of  $R$ , or  $\text{Frac}(R)$ .

### Corollary: Field of Fractions

Let  $R$  be an integral domain,  $\Sigma = R \setminus \{0\}$ . Let  $F = \text{Frac}(R)$ . Let  $K$  be any field that contains a subring  $S \cong R$ . Then, any field of  $K$  generated by  $S$  (i.e., the intersection of all subfields that contain  $S$ ) is isomorphic to  $F$ .

The proof is left as an exercise for the reader.

For an outline, consider  $\varphi : R \xrightarrow{\sim} S \subseteq K$ . Recall that  $\Sigma = R \setminus \{0\}$ . Consider  $\varphi(\Sigma)$  from  $R$  to  $K$ , and use the universal property.

### Localization Examples

- (1) Let  $R$  be an integral domain,  $R[x]$  be the set of polynomials. Then, for  $\Sigma = R[x] \setminus \{0\}$ ,

$$\text{Frac}(R[x]) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in R[x], g(x) \neq 0 \right\}$$

is the field of rational functions.

- (2) Let  $R$  be a commutative ring with identity, and let  $f \in R$ . Set  $\Sigma = \{f^n \mid n \geq 0\}$ . We form  $\Sigma^{-1}R$ , denoted  $R_f$ . Then,  $R_f = 0$  if and only if  $f^n = 0$  for some  $n \geq 0$ .

If  $f$  is not nilpotent, then  $R_f \neq 0$ , meaning  $f$  is invertible in  $R_f$ . We have

$$R_f \cong R[x]/\langle xf - 1 \rangle.$$

- (3) Consider  $R = K[x, y]/\langle xy \rangle$  for  $K$  any field. We set  $f = x$ . Note that  $f$  is not nilpotent, but  $f$  is a zero divisor. Note that  $f$  is invertible in  $R_f$ .

Consider  $\pi : R \rightarrow R_f$ ,  $g \mapsto \frac{g}{1}$ . We have  $y \mapsto \frac{y}{1}$ . However, in  $R_f$ ,  $x$  is invertible, so  $1 = \frac{x}{x} \in R_f$ . So,  $\frac{y}{1} = \frac{y}{1} \cdot \frac{x}{x} = \frac{xy}{x} = \frac{0}{x} = \frac{0}{1}$ . In this case, we do not have that  $R$  injects into  $R_f$ .

**Exercise:** For  $\pi : R \rightarrow R_f$ , we have  $\pi(R) = K[x] \subseteq R_f = K[x, x^{-1}]$ .



**Proposition: Localization by Prime Ideal**

The ring  $R$  is the zero ring if and only if  $R_{\mathfrak{p}} = 0$  for all  $\mathfrak{p} \in \text{Spec}(R)$ .

If  $R = 0$ , then clearly  $R_{\mathfrak{p}} = 0$  for all  $\mathfrak{p} \in \text{Spec}(R)$ .

In the reverse direction, suppose  $R_{\mathfrak{p}} = 0$  for all  $\mathfrak{p} \in \text{Spec}(R)$ . Pick  $r \in R$ ,  $r \neq 0$ . Set

$$I = \text{Ann}_R(r) = \{x \in R \mid xr = 0\}$$

to be the annihilator of  $r$ . We can verify that  $I$  is an ideal. Since  $r \neq 0$ ,  $1_R \notin I$ , meaning  $I$  is a proper ideal. Since  $I$  is a proper ideal,  $I \subset \mathcal{M}$  for some maximal ideal  $\mathcal{M}$ .

Consider  $R_{\mathcal{M}}$ . We have  $\frac{r}{1} \in R_{\mathcal{M}}$ . However, as  $\mathcal{M}$  is maximal,  $\mathcal{M}$  is prime, so  $R_{\mathcal{M}} = 0$ . There exists  $s \in \Sigma = R \setminus \mathcal{M}$  such that  $sr = 0$ . So,  $s \in I$ . However,  $I \subset \mathcal{M}$ , and  $s \notin \mathcal{M}$ . Thus,  $r = 0$ .

**Vector Spaces**

Let  $\mathbb{F}$  be a field. We say  $V$  is a  $\mathbb{F}$ -vector space if  $V$  is an Abelian group under addition with the scalar product  $\mathbb{F} \times V \rightarrow V, (\alpha, v) \rightarrow \alpha v$  satisfying

$$(a) \ (a + b)v = av + bv \text{ for all } a, b \in \mathbb{F}, v \in V$$

$$(b) \ (ab)v = a(bv)$$

$$(c) \ a(v + w) = av + aw \text{ for all } a \in \mathbb{F}, v, w \in V$$

$$(d) \ 1v = v \text{ for all } v \in V.$$

A set  $B \subseteq V$  is said to be linearly independent if whenever

$$\sum_{i=1}^m a_i v_i = 0 \Rightarrow a_1 = a_2 = \dots = a_m = 0$$

For  $B \subseteq V$ , the  $\mathbb{F}$ -span of  $B$  is

$$\text{span}_{\mathbb{F}}(B) = \{a_1 v_1 + \dots + a_m v_m \mid a_i \in \mathbb{F}\}.$$

If  $\text{span}_{\mathbb{F}}(B) = V$ , then we say  $B$  spans  $V$ . If  $B$  is linearly independent and spans  $V$ , then we say  $B$  is a  $\mathbb{F}$ -basis for  $V$ .

**Examples: Vector Spaces and Bases**

(1) The set  $\mathbb{F}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{F}\}$  is an  $\mathbb{F}$ -vector space with basis

$$B = \{e_i\}_{i=1}^n.$$

(2)  $V = \mathbb{F}[x]$  is an  $\mathbb{F}$ -vector space with basis  $\{1, x, x^2, \dots\}$ .

**Proposition: Basis Maximality**

Let  $B = \{v_1, \dots, v_n\}$  be a spanning set for  $V$ . Assume no proper subset of  $B$  spans  $V$ . Then,  $B$  is a basis for  $V$ .

Assume  $a_1 \neq 0$ . We have

$$v_1 = \frac{-1}{a_1} (a_2 v_2 + \dots + a_n v_n),$$

so  $v_1 \in \text{span}_{\mathbb{F}}(v_2, \dots, v_n)$ . Thus,

$$V = \text{span}_{\mathbb{F}}(v_1, v_2, \dots, v_n) \subseteq \text{span}_{\mathbb{F}}(v_2, \dots, v_n),$$

which is a contradiction as we assumed no proper subset of  $B$  spanned  $V$ .

**Proposition: Finite Spanning Sets and Basis**

Let  $B$  be a finite spanning set of  $V$ . Then,  $B$  contains a basis for  $V$ .

The proof is clear from the definition of basis.

### Example: Basis of a Vector Space

Let  $f \in \mathbb{F}[x]$ . Consider  $V = \mathbb{F}[x]/\langle f(x) \rangle$  (the quotient space of  $\mathbb{F}[x]$  formed by  $f(x)$ ). Then, for  $g(x) \in \mathbb{F}[x]$ , we can write  $g(x) = f(x)q(x) + r(x)$ , where  $r(x) = 0$  or  $\deg(r(x)) < \deg(f(x))$ . Then,

$$\begin{aligned} g(x) + \langle f(x) \rangle &= (f(x)q(x) + r(x)) + \langle f(x) \rangle \\ &= r(x) + \langle f(x) \rangle. \end{aligned}$$

Therefore,

$$\{1 + \langle f(x) \rangle, x + \langle f(x) \rangle, \dots, x^{n-1} + \langle f(x) \rangle\}$$

where  $n = \deg(f(x))$  is a spanning set for  $\mathbb{F}[x]/\langle f(x) \rangle$ .

Suppose

$$\begin{aligned} (a_0 + \langle f(x) \rangle) + (a_1x + \langle f(x) \rangle) + \dots + (a_{n-1}x^{n-1} + \langle f(x) \rangle) &= 0 + \langle f(x) \rangle \\ \sum_{i=0}^{n-1} a_i x^i + \langle f(x) \rangle &= 0 + \langle f(x) \rangle. \end{aligned}$$

Then,  $f(x) \mid \sum_{i=0}^{n-1} a_i x^i$ . However,  $\deg(f(x)) = n$ , so we must have  $a_0 = a_1 = \dots = a_{n-1} = 0$ .

### Theorem: Reordering a Basis

Let  $B = \{v_1, \dots, v_n\}$  be a basis for  $V$ . Let  $A = \{w_1, \dots, w_m\}$  be linearly independent vectors. Then, there is a reordering of  $B$  such that  $\{w_1, \dots, w_i, v_{i+1}, \dots, v_n\}$  is a basis for  $V$ .

We will prove this by induction. For the base case, we have  $i = 0$ , which means there is no replacement, and the hypothesis of the theorem is satisfied.

The induction hypothesis is that  $S = \{w_1, \dots, w_i, v_{i+1}, \dots, v_n\}$  is a basis for  $V$ . Since  $S$  is spanning,

$$w_{i+1} = a_1 w_1 + \dots + a_i w_i + a_{i+1} v_{i+1} + \dots + a_n v_n.$$

If  $a_{i+1} = a_{i+2} = \dots = a_n = 0$ , then  $w_{i+1} \in \text{span}_{\mathbb{F}}(w_1, \dots, w_i)$ , which contradicts  $A$  being linearly independent.

After reordering, we can assume  $a_{i+1} \neq 0$ . Thus,

$$v_{i+1} = \frac{1}{a_{i+1}} (w_{i+1} - a_1 w_1 - \dots - a_i w_i - a_{i+2} v_{i+2} - \dots - a_n v_n) \quad (*)$$

Hence,

$$\text{span}_{\mathbb{F}}(w_1, \dots, w_i, v_{i+1}, \dots, v_n) = \text{span}_{\mathbb{F}}(w_1, \dots, w_{i+1}, v_{i+1}, \dots, v_n).$$

Suppose  $b_1 w_1 + \dots + b_{i+1} w_{i+1} + b_{i+1} v_{i+1} + \dots + b_n v_n = 0$ . We replace  $w_{i+1}$ , and find

$$\begin{aligned} 0 &= b_1 w_1 + \dots + b_{i+1} (a_1 w_1 + \dots + a_i w_i + a_{i+1} v_{i+1} + \dots + a_n v_n) + b_{i+2} v_{i+2} + \dots + b_n v_n \\ &= (b_1 + b_{i+1} a_1) w_1 + \dots + b_{i+1} a_i w_i + (b_{i+1} a_{i+1} + b_{i+2}) v_{i+1} + \dots + (b_n + b_{i+1} a_n) v_n \end{aligned}$$

Since  $\{w_1, \dots, w_i, v_{i+1}, \dots, v_n\}$  is a coefficient, we know all coefficients are zero. Specifically,  $b_{i+1} a_{i+1} = 0$ . Since  $a_{i+1} \neq 0$  by assumption, we know that  $b_{i+1} = 0$ . Then,

$$b_1 w_1 + \dots + b_i w_i + b_{i+2} v_{i+2} + \dots + b_n v_n = 0.$$

So,  $b_{i+1} = b_1 = \dots = b_i = \dots = b_n$ .

### Corollary: Linearly Independent Sets in Vector Spaces

- (1) Let  $V$  have a finite basis with  $n$  elements. Any linearly independent set must have  $n$  or fewer elements. Any spanning set must have  $n$  or greater elements.
- (2) If  $V$  has a finite basis with  $n$  elements, any other basis must also have  $n$  elements.

### Finite-Dimensional Vector Spaces

Let  $V$  have a basis of  $n$  elements over a field  $\mathbb{F}$ . We say the dimension of  $V$  over  $\mathbb{F}$  is  $n$ , and write  $\dim_{\mathbb{F}} V = n$ . We say  $V$  is finite-dimensional if such  $n$  is finite; otherwise, we say  $V$  is infinite-dimensional.

## Examples: Dimensions of Vector Spaces

- (1)  $\dim_{\mathbb{R}} \mathbb{R}^n = n$
- (2)  $\dim_{\mathbb{C}} \mathbb{C}^n = n$ ,  $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$  (verify this for yourself)
- (3)  $\dim_{\mathbb{Q}} \mathbb{R} = \infty$
- (4) For  $\deg(f(x)) = n$ ,  $\dim_{\mathbb{F}}(\mathbb{F}[x]/\langle f(x) \rangle) = n$

## Subspaces

Let  $W \subseteq V$  be a subgroup. If  $W$  is closed under scalar multiplication, then  $W$  is known as a subspace of  $V$ .

- (1)  $\mathbb{Q}^n$  is a  $\mathbb{Q}$ -subspace of  $\mathbb{R}^n$ , but it is *not* an  $\mathbb{R}$ -subspace of  $\mathbb{R}^n$  (it is not closed under scalar multiplication by  $\mathbb{R}$ ).
- (2)  $W = \{a + bx \mid a, b \in \mathbb{F}\}$  is an  $\mathbb{F}$ -subspace of  $\mathbb{F}[x]$ .

## Corollary: Basis and Subspace

Let  $A$  be a set of linearly independent vectors in a finite-dimensional vector space  $V$ . There is a basis of  $V$  that contains  $A$ . In particular, if  $W \subseteq V$  is a subspace and  $A$  is a basis of  $W$ , then there is a basis of  $V$  that contains  $A$ .

Taking  $B = \{v_1, \dots, v_n\}$  as a basis for  $V$ , we replace vectors in  $B$  with vectors from  $A$ .

## Linear Transformations

Let  $V, W$  be  $\mathbb{F}$ -vector spaces. A map  $T : V \rightarrow W$  is said to be a linear transformation if, for all  $v_1, v_2 \in V$  and  $\alpha, \beta \in \mathbb{F}$ ,

$$T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2).$$

The collection of all linear transformations between  $V$  and  $W$  is denoted  $\text{Hom}_{\mathbb{F}}(V, W)$ .

## Lemma: Isomorphism of Finite-Dimensional Vector Spaces

If  $V$  is an  $\mathbb{F}$ -vector space of dimension  $n$ , then  $V \cong \mathbb{F}^n$  as  $\mathbb{F}$ -vector spaces.

Let  $B = \{v_1, \dots, v_n\}$  be a basis of  $V$ . Define

$$\begin{aligned} T : \mathbb{F}^n &\rightarrow V \\ (a_1, \dots, a_n) &\mapsto a_1 v_1 + \dots + a_n v_n. \end{aligned}$$

Let  $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{F}^n$ ,  $\alpha \in \mathbb{F}$ . We have

$$\begin{aligned} T(\alpha(a_1, \dots, a_n) + (b_1, \dots, b_n)) &= T((\alpha a_1 + b_1, \dots, \alpha a_n + b_n)) \\ &= (\alpha a_1 + b_1)v_1 + \dots + (\alpha a_n + b_n)v_n \\ &= \alpha(a_1 v_1 + \dots + a_n v_n) + (b_1 v_1 + \dots + b_n v_n) \\ &= \alpha T((a_1, \dots, a_n)) + T((b_1, \dots, b_n)). \end{aligned}$$

Let  $v \in V$ . Then,  $v = a_1 v_1 + \dots + a_n v_n$  for some  $a_1, \dots, a_n \in \mathbb{F}$ . So,

$$\begin{aligned} T((a_1, \dots, a_n)) &= a_1 v_1 + \dots + a_n v_n \\ &= v. \end{aligned}$$

Suppose  $T((a_1, \dots, a_n)) = T((b_1, \dots, b_n))$ . Then,

$$\begin{aligned} a_1 v_1 + \dots + a_n v_n &= b_1 v_1 + \dots + b_n v_n \\ 0 &= (a_1 - b_1)v_1 + \dots + (a_n - b_n)v_n. \end{aligned}$$

Since  $\{v_1, \dots, v_n\}$  is linearly independent,  $a_i - b_i = 0$  for all  $i \in \{1, \dots, n\}$ , meaning  $a_i = b_i$  for all  $i$ . Thus,  $T$  is bijective.