

# Foundations of Module Theory

Sean K. Sather-Wagstaff (they/them/theirs)

Clemson University

17–19 December 2020

Online CIMPA Pre-School El Salvador 2020

Algebraic Methods in Topology

•

## Take-Home Points

- 1 Rings and modules have many applications.
- 2 Modules give a unified way to study vector spaces, abelian groups, and other constructions.

- 1 Motivation
  - Why Study Rings?
  - Why Study Modules?
- 2 Rings
- 3 Modules
- 4 Conclusion

# 1.1. Motivation: Why Study Rings?

## Number Theory (Rings of Integers in Number Fields)

Let  $P = \sum_{i=0}^n a_i X^i$  be a polynomial with  $d \geq 2$  and all  $a_i \in \mathbb{Z}$ .

# 1.1. Motivation: Why Study Rings?

## Number Theory (Rings of Integers in Number Fields)

Let  $P = \sum_{i=0}^n a_i X^i$  be a polynomial with  $d \geq 2$  and all  $a_i \in \mathbb{Z}$ .  
Let  $\alpha \in \mathbb{C}$  be a root of  $P$  and consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) = \left\{ \sum_{i=0}^{n-1} b_i \alpha^i \mid b_i \in \mathbb{Q} \right\} \subseteq \mathbb{C}$$

# 1.1. Motivation: Why Study Rings?

## Number Theory (Rings of Integers in Number Fields)

Let  $P = \sum_{i=0}^n a_i X^i$  be a polynomial with  $d \geq 2$  and all  $a_i \in \mathbb{Z}$ .  
Let  $\alpha \in \mathbb{C}$  be a root of  $P$  and consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) = \left\{ \sum_{i=0}^{n-1} b_i \alpha^i \mid b_i \in \mathbb{Q} \right\} \subseteq \mathbb{C}$$

The **ring of integers** in  $\mathbb{Q}(\alpha)$  is the set  $R$  of all roots in  $\mathbb{Q}(\alpha)$  of monic polynomials with coefficients in  $\mathbb{Z}$ .

# 1.1. Motivation: Why Study Rings?

## Number Theory (Rings of Integers in Number Fields)

Let  $P = \sum_{i=0}^n a_i X^i$  be a polynomial with  $d \geq 2$  and all  $a_i \in \mathbb{Z}$ .  
Let  $\alpha \in \mathbb{C}$  be a root of  $P$  and consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) = \left\{ \sum_{i=0}^{n-1} b_i \alpha^i \mid b_i \in \mathbb{Q} \right\} \subseteq \mathbb{C}$$

The **ring of integers** in  $\mathbb{Q}(\alpha)$  is the set  $R$  of all roots in  $\mathbb{Q}(\alpha)$  of monic polynomials with coefficients in  $\mathbb{Z}$ .

Properties of  $R$  give information about  $P$ .

Useful for studying Fermat's Last Theorem.

# 1.1. Motivation: Why Study Rings?

## Algebraic Geometry

### 1 Coordinate Rings of Algebraic Varieties

Let  $V \subseteq \mathbb{C}^n$  be the set of roots of some polynomials over  $\mathbb{C}$ .



# 1.1. Motivation: Why Study Rings?

## Algebraic Geometry

### 1 Coordinate Rings of Algebraic Varieties

Let  $V \subseteq \mathbb{C}^n$  be the set of roots of some polynomials over  $\mathbb{C}$ . The associated **coordinate ring**  $\mathbb{C}[V]$  is the set of functions  $V \rightarrow \mathbb{C}$  that can be represented by polynomials.

# 1.1. Motivation: Why Study Rings?

## Algebraic Geometry

### 1 Coordinate Rings of Algebraic Varieties

Let  $V \subseteq \mathbb{C}^n$  be the set of roots of some polynomials over  $\mathbb{C}$ .

The associated **coordinate ring**  $\mathbb{C}[V]$  is the set of functions  $V \rightarrow \mathbb{C}$  that can be represented by polynomials.

Algebraic properties of  $\mathbb{C}[V] \leftrightarrow$  geometric properties of  $V$ .

# 1.1. Motivation: Why Study Rings?

## Algebraic Geometry

### 1 Coordinate Rings of Algebraic Varieties

Let  $V \subseteq \mathbb{C}^n$  be the set of roots of some polynomials over  $\mathbb{C}$ . The associated **coordinate ring**  $\mathbb{C}[V]$  is the set of functions  $V \rightarrow \mathbb{C}$  that can be represented by polynomials.

Algebraic properties of  $\mathbb{C}[V] \leftrightarrow$  geometric properties of  $V$ .

### 2 Schemes

Hilbert's Nullstellensatz:  $V \leftrightarrow \{\text{maximal ideals of } \mathbb{C}[V]\}$

# 1.1. Motivation: Why Study Rings?

## Algebraic Geometry

### 1 Coordinate Rings of Algebraic Varieties

Let  $V \subseteq \mathbb{C}^n$  be the set of roots of some polynomials over  $\mathbb{C}$ . The associated **coordinate ring**  $\mathbb{C}[V]$  is the set of functions  $V \rightarrow \mathbb{C}$  that can be represented by polynomials.

Algebraic properties of  $\mathbb{C}[V] \leftrightarrow$  geometric properties of  $V$ .

### 2 Schemes

Hilbert's Nullstellensatz:  $V \leftrightarrow \{\text{maximal ideals of } \mathbb{C}[V]\}$

Grothendieck:  $\{\text{prime ideals of } \mathbb{C}[V]\}$  contains more geometric information about  $V$ .

# 1.1. Motivation: Why Study Rings?

## Algebraic Topology

### Singular Cohomology Ring

Let  $X$  be a topological space, e.g., a curve, surface, or manifold.

# 1.1. Motivation: Why Study Rings?

## Algebraic Topology

### Singular Cohomology Ring

Let  $X$  be a topological space, e.g., a curve, surface, or manifold. The singular cohomology  $H^*(X, \mathbb{C})$  has the structure of a graded commutative ring with identity.

# 1.1. Motivation: Why Study Rings?

## Algebraic Topology

### Singular Cohomology Ring

Let  $X$  be a topological space, e.g., a curve, surface, or manifold. The singular cohomology  $H^*(X, \mathbb{C})$  has the structure of a graded commutative ring with identity.

## Graph Theory and Combinatorics

- 1 Graph  $\mapsto$  edge ring
- 2 Simplicial complex  $\mapsto$  Stanley-Reisner ring
- 3 Poset  $\mapsto$  poset ring

# 1.1. Motivation: Why Study Rings?

## Algebraic Topology

### Singular Cohomology Ring

Let  $X$  be a topological space, e.g., a curve, surface, or manifold. The singular cohomology  $H^*(X, \mathbb{C})$  has the structure of a graded commutative ring with identity.

## Graph Theory and Combinatorics

- 1 Graph  $\mapsto$  edge ring
- 2 Simplicial complex  $\mapsto$  Stanley-Reisner ring
- 3 Poset  $\mapsto$  poset ring

Combinatorial information  $\leftrightarrow$  algebraic information



# 1.1. Motivation: Why Study Rings?

## Algebraic Topology

### Singular Cohomology Ring

Let  $X$  be a topological space, e.g., a curve, surface, or manifold. The singular cohomology  $H^*(X, \mathbb{C})$  has the structure of a graded commutative ring with identity.

## Graph Theory and Combinatorics

- 1 Graph  $\mapsto$  edge ring
- 2 Simplicial complex  $\mapsto$  Stanley-Reisner ring
- 3 Poset  $\mapsto$  poset ring

Combinatorial information  $\leftrightarrow$  algebraic information

Rings are the algebraic objects that connect all these areas.

# 1.1. Motivation: Why Study Modules?

- 1 Study vector spaces and abelian groups simultaneously.
- 2 Understand a ring by understanding which sets the ring acts on

# 1.1. Motivation: Why Study Modules?

- 1 Study vector spaces and abelian groups simultaneously.
- 2 Understand a ring by understanding which sets the ring acts on - Sylow Theorems, representation theory for rings

# 1.1. Motivation: Why Study Modules?

- 1 Study vector spaces and abelian groups simultaneously.
- 2 Understand a ring by understanding which sets the ring acts on - Sylow Theorems, representation theory for rings

## Number Theory

Divisor class groups of rings of integers in number fields

# 1.1. Motivation: Why Study Modules?

- 1 Study vector spaces and abelian groups simultaneously.
- 2 Understand a ring by understanding which sets the ring acts on - Sylow Theorems, representation theory for rings

## Number Theory

Divisor class groups of rings of integers in number fields

## Algebraic Geometry

Sheaves, Picard groups, sheaf cohomology

# 1.1. Motivation: Why Study Modules?

- 1 Study vector spaces and abelian groups simultaneously.
- 2 Understand a ring by understanding which sets the ring acts on - Sylow Theorems, representation theory for rings

## Number Theory

Divisor class groups of rings of integers in number fields

## Algebraic Geometry

Sheaves, Picard groups, sheaf cohomology

## Algebraic Topology

Graded modules over singular cohomology rings

# 1.1. Motivation: Why Study Modules?

- 1 Study vector spaces and abelian groups simultaneously.
- 2 Understand a ring by understanding which sets the ring acts on - Sylow Theorems, representation theory for rings

## Number Theory

Divisor class groups of rings of integers in number fields

## Algebraic Geometry

Sheaves, Picard groups, sheaf cohomology

## Algebraic Topology

Graded modules over singular cohomology rings

## Analysis

Operators on a Hilbert space  $X$  make  $X$  into a module

## Take-Home Points

- 1 Rings and modules have many applications.



- 1 Motivation
- 2 Rings
  - Definitions and Examples
  - Quotient Rings
- 3 Modules
- 4 Conclusion

# 1.2. Rings - Definitions and Examples

## Definition

A **ring** or **commutative ring with identity** is a set  $R$  equipped with two binary operations  $+$  and  $\cdot$  such that

- 1  $(R, +)$  is an additive abelian group with additive identity  $0_R = 0$  and additive inverses denoted  $-r$ .
- 2  $(R, \cdot)$  is associative and commutative with multiplicative identity  $1_R = 1$
- 3 distributive law:  $r(s + t) = rs + rt$  for all  $r, s, t \in R$

## 1.2. Rings - Definitions and Examples

### Definition

A **ring** or **commutative ring with identity** is a set  $R$  equipped with two binary operations  $+$  and  $\cdot$  such that

- 1  $(R, +)$  is an additive abelian group with additive identity  $0_R = 0$  and additive inverses denoted  $-r$ .
- 2  $(R, \cdot)$  is associative and commutative with multiplicative identity  $1_R = 1$
- 3 distributive law:  $r(s + t) = rs + rt$  for all  $r, s, t \in R$

### Examples ( $A$ is a ring)

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$$\mathbb{Z}[i] \subseteq \mathbb{C}$$

$$\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{R}$$

## 1.2. Rings - Definitions and Examples

### Definition

A **ring** or **commutative ring with identity** is a set  $R$  equipped with two binary operations  $+$  and  $\cdot$  such that

- 1  $(R, +)$  is an additive abelian group with additive identity  $0_R = 0$  and additive inverses denoted  $-r$ .
- 2  $(R, \cdot)$  is associative and commutative with multiplicative identity  $1_R = 1$
- 3 distributive law:  $r(s + t) = rs + rt$  for all  $r, s, t \in R$

### Examples ( $A$ is a ring)

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$                        $\mathbb{Z}[i] \subseteq \mathbb{C}$                        $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{R}$
- polynomial ring:  $A[X] = \{\sum_{i=0}^{\text{finite}} a_i X^i \mid a_i \in A\}$

## 1.2. Rings - Definitions and Examples

### Definition

A **ring** or **commutative ring with identity** is a set  $R$  equipped with two binary operations  $+$  and  $\cdot$  such that

- 1  $(R, +)$  is an additive abelian group with additive identity  $0_R = 0$  and additive inverses denoted  $-r$ .
- 2  $(R, \cdot)$  is associative and commutative with multiplicative identity  $1_R = 1$
- 3 distributive law:  $r(s + t) = rs + rt$  for all  $r, s, t \in R$

### Examples ( $A$ is a ring)

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$                        $\mathbb{Z}[i] \subseteq \mathbb{C}$                        $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{R}$
- polynomial ring:  $A[X] = \{\sum_{i=0}^{\text{finite}} a_i X^i \mid a_i \in A\}$
- $A[X, Y] = A[X][Y]$  and  $A[X_1, \dots, X_d] = A[X_1, \dots, X_{d-1}][X_d]$

## 1.2. Rings - Definitions and Examples

### Definition

A **ring** or **commutative ring with identity** is a set  $R$  equipped with two binary operations  $+$  and  $\cdot$  such that

- 1  $(R, +)$  is an additive abelian group with additive identity  $0_R = 0$  and additive inverses denoted  $-r$ .
- 2  $(R, \cdot)$  is associative and commutative with multiplicative identity  $1_R = 1$
- 3 distributive law:  $r(s + t) = rs + rt$  for all  $r, s, t \in R$

### Examples ( $A$ is a ring)

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$                        $\mathbb{Z}[i] \subseteq \mathbb{C}$                        $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{R}$
- polynomial ring:  $A[X] = \{\sum_{i=0}^{\text{finite}} a_i X^i \mid a_i \in A\}$
- $A[X, Y] = A[X][Y]$  and  $A[X_1, \dots, X_d] = A[X_1, \dots, X_{d-1}][X_d]$
- Matrix rings are generally non-commutative.

## 1.2. Rings - Definitions and Examples, cont.

### Facts (Let $R$ be a ring)

- 1 0 and 1 are unique, and  $0r = 0$  for all  $r \in R$
- 2 additive inverses are unique and  $-(-r) = r$

## 1.2. Rings - Definitions and Examples, cont.

### Facts (Let $R$ be a ring)

- 1 0 and 1 are unique, and  $0r = 0$  for all  $r \in R$
- 2 additive inverses are unique and  $-(-r) = r$

### Definition

- A **field** is a non-zero ring  $\mathbb{K}$  such that every non-zero element is a **unit**, i.e., has a **multiplicative inverse**:



## 1.2. Rings - Definitions and Examples, cont.

### Facts (Let $R$ be a ring)

- 1 0 and 1 are unique, and  $0r = 0$  for all  $r \in R$
- 2 additive inverses are unique and  $-(-r) = r$

### Definition

- A **field** is a non-zero ring  $\mathbb{K}$  such that every non-zero element is a **unit**, i.e., has a **multiplicative inverse**:  
for every  $r \in \mathbb{K}$  there is an element  $s \in R$  such that  $rs = 1$ .

## 1.2. Rings - Definitions and Examples, cont.

### Facts (Let $R$ be a ring)

- 1 0 and 1 are unique, and  $0r = 0$  for all  $r \in R$
- 2 additive inverses are unique and  $-(-r) = r$

### Definition

- A **field** is a non-zero ring  $\mathbb{K}$  such that every non-zero element is a **unit**, i.e., has a **multiplicative inverse**:  
for every  $r \in \mathbb{K}$  there is an element  $s \in R$  such that  $rs = 1$ .

### Examples ( $A$ is a ring)

- fields:  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

## 1.2. Rings - Definitions and Examples, cont.

### Facts (Let $R$ be a ring)

- 1 0 and 1 are unique, and  $0r = 0$  for all  $r \in R$
- 2 additive inverses are unique and  $-(-r) = r$

### Definition

- A **field** is a non-zero ring  $\mathbb{K}$  such that every non-zero element is a **unit**, i.e., has a **multiplicative inverse**:  
for every  $r \in \mathbb{K}$  there is an element  $s \in R$  such that  $rs = 1$ .

### Examples ( $A$ is a ring)

- fields:  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- not fields:  $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{5}], A[X],$  and  $A[X_1, \dots, X_d]$  for  $d \geq 1$

## 1.2. Rings - Quotient Rings

Constructing  $\mathbb{Z}_n = \{0, \dots, n-1\}$

Let  $n \in \mathbb{Z}_{\geq 2}$ . Build a ring using the equivalence relation

## 1.2. Rings - Quotient Rings

Constructing  $\mathbb{Z}_n = \{0, \dots, n-1\}$

Let  $n \in \mathbb{Z}_{\geq 2}$ . Build a ring using the equivalence relation

$$a \equiv b \pmod{n} \iff n \mid (b - a)$$

$$\mathbb{Z}/\langle n \rangle = \{\text{equivalence classes in } \mathbb{Z} \text{ mod } n\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$0 = \overline{0}$$

$$\overline{a} \overline{b} = \overline{ab}$$

$$1 = \overline{1}$$

## 1.2. Rings - Quotient Rings

Constructing  $\mathbb{Z}_n = \{0, \dots, n-1\}$

Let  $n \in \mathbb{Z}_{\geq 2}$ . Build a ring using the equivalence relation

$$a \equiv b \pmod{n} \iff n \mid (b - a)$$

$$\mathbb{Z}/\langle n \rangle = \{\text{equivalence classes in } \mathbb{Z} \text{ mod } n\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

$$\overline{a} + \overline{b} = \overline{a+b} \qquad 0 = \overline{0} \qquad \overline{a}\overline{b} = \overline{ab} \qquad 1 = \overline{1}$$

Adjoining a Root

Let  $\mathbb{K}$  be a field, and let  $P = \sum_{i=0}^d a_i X^i \in \mathbb{K}[X]$ .

Build a new ring using the equivalence relation

## 1.2. Rings - Quotient Rings

### Constructing $\mathbb{Z}_n = \{0, \dots, n-1\}$

Let  $n \in \mathbb{Z}_{\geq 2}$ . Build a ring using the equivalence relation

$$a \equiv b \pmod{n} \iff n \mid (b - a)$$

$$\mathbb{Z}/\langle n \rangle = \{\text{equivalence classes in } \mathbb{Z} \text{ mod } n\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

$$\bar{a} + \bar{b} = \overline{a+b} \qquad 0 = \bar{0} \qquad \bar{a}\bar{b} = \overline{ab} \qquad 1 = \bar{1}$$

### Adjoining a Root

Let  $\mathbb{K}$  be a field, and let  $P = \sum_{i=0}^d a_i X^i \in \mathbb{K}[X]$ .

Build a new ring using the equivalence relation

$$F \equiv G \pmod{P} \iff P \mid (G - F)$$

$$\mathbb{K}[X]/\langle P \rangle = \{\text{eq. classes in } \mathbb{K}[X] \text{ mod } P\} = \text{span}(\bar{1}, \bar{X}, \dots, \bar{X}^{d-1})$$

$$\bar{F} + \bar{G} = \overline{F+G} \qquad 0 = \bar{0} \qquad \bar{F}\bar{G} = \overline{FG} \qquad 1 = \bar{1}$$

## 1.2. Rings - Quotient Rings

### Constructing $\mathbb{Z}_n = \{0, \dots, n-1\}$

Let  $n \in \mathbb{Z}_{\geq 2}$ . Build a ring using the equivalence relation

$$a \equiv b \pmod{n} \iff n \mid (b - a)$$

$$\mathbb{Z}/\langle n \rangle = \{\text{equivalence classes in } \mathbb{Z} \text{ mod } n\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

$$\overline{a} + \overline{b} = \overline{a+b} \qquad 0 = \overline{0} \qquad \overline{a}\overline{b} = \overline{ab} \qquad 1 = \overline{1}$$

### Adjoining a Root

Let  $\mathbb{K}$  be a field, and let  $P = \sum_{i=0}^d a_i X^i \in \mathbb{K}[X]$ .

Build a new ring using the equivalence relation

$$F \equiv G \pmod{P} \iff P \mid (G - F)$$

$$\mathbb{K}[X]/\langle P \rangle = \{\text{eq. classes in } \mathbb{K}[X] \text{ mod } P\} = \text{span}(\overline{1}, \overline{X}, \dots, \overline{X}^{d-1})$$

$$\overline{F} + \overline{G} = \overline{F+G} \qquad 0 = \overline{0} \qquad \overline{F}\overline{G} = \overline{FG} \qquad 1 = \overline{1}$$

$\overline{X}$  is a root of  $P$ . E.g.,  $\mathbb{C} = \mathbb{R}[X]/\langle X^2 + 1 \rangle \ni \overline{X} = i$ .



## 1.2. Rings - Quotient Rings, cont.

Definition (Let  $R$  be a ring.)

An **ideal** of  $R$  is an additive subgroup  $I \subseteq R$  that absorbs multiplication:  $r \in R$  and  $a \in I \implies ra \in I$ .

## 1.2. Rings - Quotient Rings, cont.

Definition (Let  $R$  be a ring.)

An **ideal** of  $R$  is an additive subgroup  $I \subseteq R$  that absorbs multiplication:  $r \in R$  and  $a \in I \implies ra \in I$ .

Examples

①  $\langle n \rangle = \{cn \mid c \in \mathbb{Z}\} \subseteq \mathbb{Z}$  and  $\langle P \rangle = \{HP \mid H \in \mathbb{K}[X]\} \subseteq \mathbb{K}[X]$

## 1.2. Rings - Quotient Rings, cont.

Definition (Let  $R$  be a ring.)

An **ideal** of  $R$  is an additive subgroup  $I \subseteq R$  that absorbs multiplication:  $r \in R$  and  $a \in I \implies ra \in I$ .

Examples

- 1  $\langle n \rangle = \{cn \mid c \in \mathbb{Z}\} \subseteq \mathbb{Z}$  and  $\langle P \rangle = \{HP \mid H \in \mathbb{K}[X]\} \subseteq \mathbb{K}[X]$
- 2  $x_1, \dots, x_n \in R \implies \langle x_1, \dots, x_n \rangle = \{\sum_{i=1}^n r_i x_i \mid r_i \in R\} \subseteq R$

## 1.2. Rings - Quotient Rings, cont.

Definition (Let  $R$  be a ring.)

An **ideal** of  $R$  is an additive subgroup  $I \subseteq R$  that absorbs multiplication:  $r \in R$  and  $a \in I \implies ra \in I$ .

Examples

- 1  $\langle n \rangle = \{cn \mid c \in \mathbb{Z}\} \subseteq \mathbb{Z}$  and  $\langle P \rangle = \{HP \mid H \in \mathbb{K}[X]\} \subseteq \mathbb{K}[X]$
- 2  $x_1, \dots, x_n \in R \implies \langle x_1, \dots, x_n \rangle = \{\sum_{i=1}^n r_i x_i \mid r_i \in R\} \subseteq R$

Definition (Let  $I$  be an ideal of  $R$ )

Build a new ring using the equivalence relation

## 1.2. Rings - Quotient Rings, cont.

Definition (Let  $R$  be a ring.)

An **ideal** of  $R$  is an additive subgroup  $I \subseteq R$  that absorbs multiplication:  $r \in R$  and  $a \in I \implies ra \in I$ .

Examples

①  $\langle n \rangle = \{cn \mid c \in \mathbb{Z}\} \subseteq \mathbb{Z}$  and  $\langle P \rangle = \{HP \mid H \in \mathbb{K}[X]\} \subseteq \mathbb{K}[X]$

②  $x_1, \dots, x_n \in R \implies \langle x_1, \dots, x_n \rangle = \{\sum_{i=1}^n r_i x_i \mid r_i \in R\} \subseteq R$

Definition (Let  $I$  be an ideal of  $R$ )

Build a new ring using the equivalence relation

$$r \equiv s \pmod{I} \iff r - s \in I$$

$$R/I = \{\text{eq. classes } \bar{r} \text{ in } R \text{ mod } I\}$$

## 1.2. Rings - Quotient Rings, cont.

Definition (Let  $R$  be a ring.)

An **ideal** of  $R$  is an additive subgroup  $I \subseteq R$  that absorbs multiplication:  $r \in R$  and  $a \in I \implies ra \in I$ .

Examples

- 1  $\langle n \rangle = \{cn \mid c \in \mathbb{Z}\} \subseteq \mathbb{Z}$  and  $\langle P \rangle = \{HP \mid H \in \mathbb{K}[X]\} \subseteq \mathbb{K}[X]$
- 2  $x_1, \dots, x_n \in R \implies \langle x_1, \dots, x_n \rangle = \{\sum_{i=1}^n r_i x_i \mid r_i \in R\} \subseteq R$

Definition (Let  $I$  be an ideal of  $R$ )

Build a new ring using the equivalence relation

$$r \equiv s \pmod{I} \iff r - s \in I$$

$$R/I = \{\text{eq. classes } \bar{r} \text{ in } R \text{ mod } I\}$$

$$\bar{r} = \bar{s} \iff r - s \in I$$

$$\bar{r} + \bar{s} = \overline{r+s}$$

$$0 = \bar{0}$$

$$\overline{rs} = \bar{r}\bar{s}$$

$$1 = \bar{1}$$

# Day 1 Outline

- 1 Motivation
- 2 Rings
- 3 **Modules**
  - Definitions and Examples
  - Homomorphisms
  - Submodules
  - Quotient Modules
  - First Isomorphism Theorem
- 4 Conclusion

## 1.3. Modules - Definitions and Examples

Definition (Let  $R$  be a ring.)

An  $R$ -module is an additive abelian group  $M$  equipped with a scalar multiplication  $R \times M \rightarrow M$  denoted  $(r, m) \mapsto r \cdot m = rm$  that is unital, associative, and distributive.



# 1.3. Modules - Definitions and Examples

Definition (Let  $R$  be a ring.)

An  $R$ -module is an additive abelian group  $M$  equipped with a scalar multiplication  $R \times M \rightarrow M$  denoted  $(r, m) \mapsto r \cdot m = rm$  that is unital, associative, and distributive.

## Examples

- 1 Additive abelian group iff  $\mathbb{Z}$ -module
- 2  $\mathbb{K}$ -vector space iff  $\mathbb{K}$ -module

# 1.3. Modules - Definitions and Examples

Definition (Let  $R$  be a ring.)

An  $R$ -module is an additive abelian group  $M$  equipped with a scalar multiplication  $R \times M \rightarrow M$  denoted  $(r, m) \mapsto r \cdot m = rm$  that is unital, associative, and distributive.

## Examples

- 1 Additive abelian group iff  $\mathbb{Z}$ -module
- 2  $\mathbb{K}$ -vector space iff  $\mathbb{K}$ -module
- 3  $\mathbb{K}[X]$ -module iff  $\mathbb{K}$ -vector space  $V$  equipped with a linear transformation  $V \xrightarrow{\phi} V$   
 $x \cdot v = \phi(v)$
- 4 Ideals of  $R$  are  $R$ -modules  
 $x^2 \cdot v = \phi^2(v) = \phi(\phi(v))$

$$(\sum_i a_i X^i) \cdot v = \sum_i a_i \phi^i(v)$$

# 1.3. Modules - Homomorphisms

Definition (Let  $M$  and  $N$  be modules over a ring  $R$ .)

An  **$R$ -module homomorphism**  $\phi: M \rightarrow N$  is a homomorphism of abelian groups respecting scalar multiplication:  $\phi(rm) = r\phi(m)$ .

# 1.3. Modules - Homomorphisms

Definition (Let  $M$  and  $N$  be modules over a ring  $R$ .)

An  **$R$ -module homomorphism**  $\phi: M \rightarrow N$  is a homomorphism of abelian groups respecting scalar multiplication:  $\phi(rm) = r\phi(m)$ .

## Examples

- 1 Abelian group homomorphism iff  $\mathbb{Z}$ -module homomorphism
- 2  $\mathbb{K}$ -linear transformation iff  $\mathbb{K}$ -module homomorphism

# 1.3. Modules - Homomorphisms

Definition (Let  $M$  and  $N$  be modules over a ring  $R$ .)

An  **$R$ -module homomorphism**  $\phi: M \rightarrow N$  is a homomorphism of abelian groups respecting scalar multiplication:  $\phi(rm) = r\phi(m)$ .

Examples

- 1 Abelian group homomorphism iff  $\mathbb{Z}$ -module homomorphism
- 2  $\mathbb{K}$ -linear transformation iff  $\mathbb{K}$ -module homomorphism

Definition (Let  $M$  and  $N$  be modules over a ring  $R$ .)

An  **$R$ -module isomorphism**  $\phi: M \rightarrow N$  is an  $R$ -module homomorphism with a 2-sided inverse. Notation:  $M \cong N$ .

# 1.3. Modules - Homomorphisms

Definition (Let  $M$  and  $N$  be modules over a ring  $R$ .)

An  **$R$ -module homomorphism**  $\phi: M \rightarrow N$  is a homomorphism of abelian groups respecting scalar multiplication:  $\phi(rm) = r\phi(m)$ .

Examples

- 1 Abelian group homomorphism iff  $\mathbb{Z}$ -module homomorphism
- 2  $\mathbb{K}$ -linear transformation iff  $\mathbb{K}$ -module homomorphism

Definition (Let  $M$  and  $N$  be modules over a ring  $R$ .)

An  **$R$ -module isomorphism**  $\phi: M \rightarrow N$  is an  $R$ -module homomorphism with a 2-sided inverse. Notation:  $M \cong N$ .

Fact

Isomorphism iff homomorphism that is 1-1 and onto

## 1.3. Modules - Submodules

Definition (Let  $M$  a module over a ring  $R$ .)

An  **$R$ -submodule** of  $M$  is a subgroup  $K \subseteq M$  that absorbs scalar multiplication:  $r \in R$  and  $x \in K \implies rx \in K$ .

# 1.3. Modules - Submodules

Definition (Let  $M$  a module over a ring  $R$ .)

An  **$R$ -submodule** of  $M$  is a subgroup  $K \subseteq M$  that absorbs scalar multiplication:  $r \in R$  and  $x \in K \implies rx \in K$ .

Fact

Submodule of  $M$  iff subset that is itself a module under the operations from  $M$



# 1.3. Modules - Submodules

Definition (Let  $M$  a module over a ring  $R$ .)

An  **$R$ -submodule** of  $M$  is a subgroup  $K \subseteq M$  that absorbs scalar multiplication:  $r \in R$  and  $x \in K \implies rx \in K$ .

Fact

Submodule of  $M$  iff subset that is itself a module under the operations from  $M$

Examples (Let  $\phi: M \rightarrow N$  be an  $R$ -module homomorphism)

- 1 Abelian subgroup iff  $\mathbb{Z}$ -submodule
- 2  $\mathbb{K}$ -subspace iff  $\mathbb{K}$ -submodule

# 1.3. Modules - Submodules

Definition (Let  $M$  a module over a ring  $R$ .)

An  **$R$ -submodule** of  $M$  is a subgroup  $K \subseteq M$  that absorbs scalar multiplication:  $r \in R$  and  $x \in K \implies rx \in K$ .

Fact

Submodule of  $M$  iff subset that is itself a module under the operations from  $M$

Examples (Let  $\phi: M \rightarrow N$  be an  $R$ -module homomorphism)

- 1 Abelian subgroup iff  $\mathbb{Z}$ -submodule
- 2  $\mathbb{K}$ -subspace iff  $\mathbb{K}$ -submodule
- 3 Ideal of  $R$  iff  $R$ -submodule of  $R$

# 1.3. Modules - Submodules

Definition (Let  $M$  a module over a ring  $R$ .)

An  **$R$ -submodule** of  $M$  is a subgroup  $K \subseteq M$  that absorbs scalar multiplication:  $r \in R$  and  $x \in K \implies rx \in K$ .

Fact

Submodule of  $M$  iff subset that is itself a module under the operations from  $M$

Examples (Let  $\phi: M \rightarrow N$  be an  $R$ -module homomorphism)

- 1 Abelian subgroup iff  $\mathbb{Z}$ -submodule
- 2  $\mathbb{K}$ -subspace iff  $\mathbb{K}$ -submodule
- 3 Ideal of  $R$  iff  $R$ -submodule of  $R$
- 4  $\text{Im}(\phi) = \phi(M) = \{\phi(m) \in N \mid m \in M\} \subseteq N$
- 5  $\text{Ker}(\phi) = \phi^{-1}(0) = \{m \in M \mid \phi(m) = 0\} \subseteq M$

## 1.3. Modules - Quotient Modules

Definition (Let  $K \subset M$  be a submodule over a ring  $R$ )

Build a new  $R$ -module using the equivalence relation

## 1.3. Modules - Quotient Modules

Definition (Let  $K \subset M$  be a submodule over a ring  $R$ )

Build a new  $R$ -module using the equivalence relation

$$x \equiv y \pmod{K} \iff x - y \in K$$

$$M/K = \{\text{eq. classes } \bar{x} \text{ in } M \text{ mod } K\}$$

# 1.3. Modules - Quotient Modules

Definition (Let  $K \subset M$  be a submodule over a ring  $R$ )

Build a new  $R$ -module using the equivalence relation

$$x \equiv y \pmod{K} \iff x - y \in K$$

$$M/K = \{\text{eq. classes } \bar{x} \text{ in } M \text{ mod } K\}$$

$$\bar{x} = \bar{y} \iff x - y \in K$$

$$\bar{x} + \bar{y} = \overline{x + y}$$

$$0 = \bar{0}$$

$$r\bar{x} = \overline{rx}$$

## 1.3. Modules - Quotient Modules

**Definition** (Let  $K \subset M$  be a submodule over a ring  $R$ )

Build a new  $R$ -module using the equivalence relation

$$x \equiv y \pmod{K} \iff x - y \in K$$

$$M/K = \{\text{eq. classes } \bar{x} \text{ in } M \text{ mod } K\}$$

$$\bar{x} = \bar{y} \iff x - y \in K$$

$$\bar{x} + \bar{y} = \overline{x + y}$$

$$0 = \bar{0}$$

$$r\bar{x} = \overline{rx}$$

**Proposition** (Canonical Surjection)

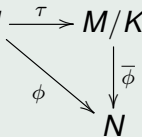
*Let  $K \subseteq M$  be a submodule. Then the function  $\tau: M \rightarrow M/K$  given by  $\tau(x) = \bar{x}$  is a well-defined  $R$ -module epimorphism (surjective homomorphism).*

# 1.3. Modules - First Isomorphism Theorem

## Theorem (Fundamental Homomorphism Theorem)

Let  $\phi: M \rightarrow N$  be an  $R$ -module homomorphism, and let  $K \subseteq M$  be a submodule such that  $\text{Ker}(\phi) \subseteq K$ .

- 1 There is a unique homomorphism  $\bar{\phi}: M/K \rightarrow N$  such that  $\bar{\phi}(\bar{x}) = \phi(x)$ , i.e., such that  $\bar{\phi} \circ \tau = \phi$ , i.e.,
- 2  $\text{Im}(\bar{\phi}) = \text{Im}(\phi) \subseteq N$
- 3  $\text{Ker}(\bar{\phi}) = \text{Ker}(\phi)/K \subseteq M/K$
- 4  $\bar{\phi}$  is onto iff  $\phi$  is onto.
- 5  $\bar{\phi}$  is 1-1 iff  $\text{Ker}(\phi) = K$ .



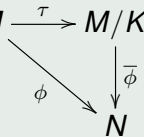


# 1.3. Modules - First Isomorphism Theorem

## Theorem (Fundamental Homomorphism Theorem)

Let  $\phi: M \rightarrow N$  be an  $R$ -module homomorphism, and let  $K \subseteq M$  be a submodule such that  $\text{Ker}(\phi) \subseteq K$ .

1 There is a unique homomorphism  $\bar{\phi}: M/K \rightarrow N$  such that  $\bar{\phi}(\bar{x}) = \phi(x)$ , i.e., such that  $\bar{\phi} \circ \tau = \phi$ , i.e.,



2  $\text{Im}(\bar{\phi}) = \text{Im}(\phi) \subseteq N$

3  $\text{Ker}(\bar{\phi}) = \text{Ker}(\phi)/K \subseteq M/K$

4  $\bar{\phi}$  is onto iff  $\phi$  is onto.

5  $\bar{\phi}$  is 1-1 iff  $\text{Ker}(\phi) = K$ .

## Theorem (First Isomorphism Theorem)

Let  $\phi: M \rightarrow N$  be an  $R$ -module homomorphism.

1  $\text{Im}(\phi) \cong M/\text{Ker}(\phi)$ .

2 If  $\phi$  is onto, then  $N \cong M/\text{Ker}(\phi)$ .

# Day 1 Outline

- 1 Motivation
- 2 Rings
- 3 Modules
- 4 **Conclusion**

# 1.4. Conclusion

## Take-Home Points

- 1 Rings and modules have many applications.
- 2 Modules give a unified way to study vector spaces, abelian groups, and other constructions.

# 1.4. Conclusion

## Take-Home Points

- 1 Rings and modules have many applications.
- 2 Modules give a unified way to study vector spaces, abelian groups, and other constructions.

## Next Lecture

- 1 Understand a ring by understanding its modules.
- 2 This is like the Sylow Theorems, but for rings.
- 3 This is representation theory for rings.
- 4 Simple rings have only simple modules and conversely.
- 5 Modules are not generally nice like they are over a principal ideal domain.

## 1.4. Exercises

### Exercise (1)

Let  $\mathbb{K}$  be a field, and let  $V$  be a non-empty subset of  $\mathbb{K}^n$ . Set  $S = \mathbb{K}[X_1, \dots, X_n]$  and  $I(V) = \{P \in S \mid P(v) = 0 \text{ for all } v \in V\}$ .

- 1 Prove that  $I(V)$  is an ideal of  $S$ .
- 2 Prove that every element  $\bar{P} \in S/I(V)$  gives a well-defined function  $\bar{P}: V \rightarrow \mathbb{K}$  given by  $\bar{P}(v) = P(v)$ .

### Exercise (2)

Let  $K \subseteq M$  be a submodule over a ring  $R$ .

- 1 Prove that the following operations make  $M/K$  into a well-defined  $R$ -module.

$$\bar{x} + \bar{y} = \overline{x + y} \qquad 0 = \bar{0} \qquad r\bar{x} = \overline{rx}$$

- 2 Prove the Fundamental Homomorphism Theorem.
- 3 Prove the First Isomorphism Theorem.

## Exercise (1)

Let  $\mathbb{K}$  be a field, and let  $V$  be a non-empty subset of  $\mathbb{K}^n$ . Set  $S = \mathbb{K}[X_1, \dots, X_n]$  and  $I(V) = \{P \in S \mid P(v) = 0 \text{ for all } v \in V\}$ .

- ① Prove that  $I(V)$  is an ideal of  $S$ .  $\mathbb{C}[V] \cong \mathbb{C}[X_1, \dots, X_n]/I(V)$
- ② Prove that every element  $\bar{P} \in S/I(V)$  gives a well-defined function  $\bar{P}: V \rightarrow \mathbb{K}$  given by  $\bar{P}(v) = P(v)$ .

$$I(V) \neq \emptyset$$

closed under subtraction  
absorbs multiplication

Bibliography: Dummit & Foote. Abstract Algebra.

$$0 \in I(V) \text{ b/c } 0 \in S \text{ \& } 0(\sigma) = 0 \forall \sigma.$$

$$f, g \in I(V) \Rightarrow f(\sigma) = 0 = g(\sigma) \forall \sigma \in V \Rightarrow$$

$$(f - g)(\sigma) = f(\sigma) - g(\sigma) = 0 - 0 = 0 \Rightarrow f - g \in I(V).$$

$$t \in S \text{ \& } f \in I(V) \Rightarrow (t \cdot f)(\sigma) = t(\sigma) \cdot \underbrace{f(\sigma)}_{=0} = t(\sigma) \cdot 0 = 0 \Rightarrow t \cdot f \in I(V)$$

$$f - g \in S \text{ \& } t \cdot f \in S$$

$$\bar{P}: V \rightarrow \mathbb{K}$$

$$\textcircled{2} \bar{P} \in S/I(V) \Rightarrow \bar{P}(\sigma) = P(\sigma) \text{ well-defined.}$$

Need to show: If  $\bar{P} = \bar{Q}$  then  $\bar{P}(\sigma) = \bar{Q}(\sigma) \forall \sigma \in V$

$$\bar{P} = \bar{Q} \Leftrightarrow P - Q \in I(V)$$

$$\Leftrightarrow (P - Q)(\sigma) = 0 \quad \forall \sigma \in V$$

$$\Leftrightarrow P(\sigma) - Q(\sigma) = 0 \quad \forall \sigma \in V$$

$$\Leftrightarrow P(\sigma) = Q(\sigma) \quad \forall \sigma \in V$$

$$\Leftrightarrow \bar{P}(\sigma) = \bar{Q}(\sigma) \quad \forall \sigma \in V$$

Q.  $M$  is  $R$ -mod  $\nRightarrow$  every submod.  $K \subseteq M$  is the kernel of a homomorphism  $\phi: M \rightarrow N$ ?

A. Yes. Use  $\tau: M \rightarrow M/K$  by  $\tau(x) = \bar{x}$ . This is well-defined homomorphism s.t.  $\text{Ker}(\tau) = K$ .

## Exercise (2)

Let  $K \subseteq M$  be a submodule over a ring  $R$ .

- ① Prove that the following operations make  $M/K$  into a well-defined  $R$ -module.  $-\bar{x} = \overline{-x}$      $\overline{x-y} = \overline{x-y}$

$$\overline{x+y} = \overline{x+y} \qquad 0 = \bar{0} \qquad r\bar{x} = \overline{rx}$$

- ② Prove the Fundamental Homomorphism Theorem.  
 ③ Prove the First Isomorphism Theorem.

operations well-defined? axioms satisfied?  
 Assume  $\bar{x} = \bar{a}$  &  $\bar{y} = \bar{b}$  & show  $\overline{x+y} = \overline{a+b}$  &  $\overline{rx} = \overline{ra}$   
 $\bar{x} = \bar{a} \Leftrightarrow x - a \in K$  .  $\bar{y} = \bar{b} \Leftrightarrow y - b \in K$   
 Show:  $\overline{(x+y)} - \overline{(a+b)} \in K$ !

$$\overline{(x+y)} - \overline{(a+b)} = \underbrace{(x-a)}_{\in K} + \underbrace{(y-b)}_{\in K} \in K \quad \checkmark$$

$$-\bar{x} = 0 - \bar{x} = \overline{0-x} = \overline{-x} = \overline{-x}$$

$$0 - x = -x$$

$$\overline{rx} = \overline{ra} \Leftrightarrow rx - ra \in K \Leftrightarrow r \underbrace{(x-a)}_{\in K} \in K$$

$$r(s\bar{x}) \stackrel{?}{=} (rs)\bar{x}$$

$$\parallel$$

$$r(\overline{sx})$$

$$\parallel$$

$$\overline{(rs)x}$$

$$\parallel$$

$$\frac{r \cdot (sx)}{r \cdot (sx)}$$

$$r(sx) = (rs)x$$

by module axioms for  $M$

$$0 \neq \bar{0}$$

show:  $\bar{0} + \bar{x} \stackrel{?}{=} \bar{x} \quad \forall \bar{x} \in M/K$

$$\parallel$$

$$\frac{0+x}{0+x}$$

$$0+x = x$$

etc.

Edge ring:  $a - b - c \quad P_2$

$$K[a,b,c] / \langle ab, bc \rangle \ni \bar{f}, \bar{g}$$

$$\overline{f+g} = \overline{f+g} \quad \& \quad \overline{f \cdot g} = \overline{f \cdot g}$$

$$\begin{aligned} \overline{(a^2+ac)(b^2+a)} &= \overline{(a^2+ac)(b^2+a)} \\ &= \overline{a^2b^2 + a^3 + ab^2c + a^2c} \\ &= \overline{a^2b^2} + \overline{a^3} + \overline{ab^2c} + \overline{a^2c} \end{aligned}$$

$$a^2b^2 \in \langle ab, ac \rangle$$

$$" ab \cdot ab + 0 \cdot ac$$

$$ab^2c \in \langle ab, ac \rangle$$

$$ab \in \langle ab, ac \rangle$$

$$= \overline{a^3} + \overline{a^2c} = \overline{a^2(a+c)}$$

unique factorization fails

$$\overline{a} \cdot \overline{b} = \overline{ab} = 0$$

$$\overline{a} \neq 0 \quad \& \quad \overline{b} \neq 0$$

$$a^3 \rightarrow b^2 \leftarrow c^5$$

$$I = \langle ab^2, b^2c \rangle$$