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

Day 1 Preface

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.

Day 1 Outline

Number Theory (Rings of Integers in Number Fields)

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

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

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 $\mathbb{C}$.
   The associated coordinate ring $\mathbb{C}[V]$ is the set of functions $V \to \mathbb{C}$ 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. 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 - 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

Day 1 First Take-Home Point

Take-Home Points

1. Rings and modules have many applications.

Day 1 Outline

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 $r, s, t \in R$

Examples (A is a ring)

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ $\qquad$ $\mathbb{Z}[i] \subseteq \mathbb{C}$ $\qquad$ $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{R}$
- 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 $A[X_1, \ldots, X_d] = A[X_1, \ldots, X_{d-1}][X_d]$
- 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 $-(-r) = r$

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 $A[X_1, \ldots, X_d]$ for $d \geq 1$

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

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

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

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

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

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

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

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

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

$\overline{X}$ 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 $a \in I \implies ra \in I$.

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

Definition (Let I be an ideal of R)

Build a new ring using the equivalence relation

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

$$R/I = \{\text{equivalence classes } \overline{r} \text{ in } R \bmod I\}$$

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

$$\overline{r} + \overline{s} = \overline{r+s} \qquad 0 = \overline{0} \qquad -\overline{r} = \overline{-r} \qquad \overline{r}\,\overline{s} = \overline{rs} \qquad 1 = \overline{1}$$

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 $R \times M \to M$ 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 $V \to V$
4. Ideals of R are R-modules

1.3. Modules - Homomorphisms

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

An R-module homomorphism $\phi\colon M \to N$ 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 $\phi\colon M \to N$ 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 $x \in K \implies rx \in K$.

Fact

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

Examples (Let $\phi\colon M \to N$ 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. $\mathrm{Im}(\phi) = \phi(M) = \{\phi(m) \in N \mid m \in M\} \subseteq N$
5. $\mathrm{Ker}(\phi) = \phi^{-1}(0) = \{m \in M \mid \phi(m) = 0\} \subseteq M$

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

Build a new R-module using the equivalence relation

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

$$M/K = \{\text{eq. classes } \overline{x} \text{ in } M \bmod K\}$$

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

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

Proposition (Canonical Surjection)

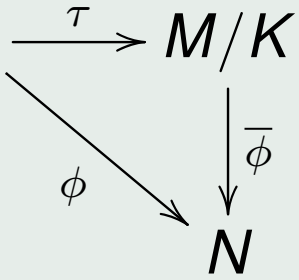
Let $K \subseteq M$ be a submodule. Then the function $\tau : M \to M/K$ given by $\tau(x) = \overline{x}$ is a well-defined R-module epimorphism (surjective homomorphism).

1.3. Modules - First Isomorphism Theorem

Theorem (Fundamental Homomorphism Theorem)

Let $\phi\colon M \to N$ be an R-module homomorphism, and let $K \subseteq M$ be a submodule such that $\operatorname{Ker}(\phi) \supseteq K$.

1. *There is a unique homomorphism $\overline{\phi}\colon M/K \to N$ such that $\overline{\phi}(\overline{x}) = \phi(x)$, i.e., such that $\overline{\phi} \circ \tau = \phi$, i.e.,*



2. $\operatorname{Im}(\overline{\phi}) = \operatorname{Im}(\phi) \subseteq N$
3. $\operatorname{Ker}(\overline{\phi}) = \operatorname{Ker}(\phi)/K \subseteq M/K$
4. *$\overline{\phi}$ is onto iff ϕ is onto.*
5. *$\overline{\phi}$ is 1-1 iff $\operatorname{Ker}(\phi) = K$.*

Theorem (First Isomorphism Theorem)

Let $\phi\colon M \to N$ be an R-module homomorphism.

1. $\operatorname{Im}(\phi) \cong M/\operatorname{Ker}(\phi)$.
2. *If ϕ is onto, then $N \cong M/\operatorname{Ker}(\phi)$.*

Day 1 Outline

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 $S = \mathbb{K}[X_1, \ldots, X_n]$ 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 $\overline{P} \in S/I(V)$ gives a well-defined function $\overline{P}\colon V \to \mathbb{K}$ given by $\overline{P}(v) = P(v)$.

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.

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

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