Algebra III: A Complete Guide

Math 511

September 17, 2022

E Thompson,
Physics and Math Honors

Solo Pursuit of Learning

Contents

Part I

Ring Theory

Chapter 1

Definition of Ring

In this chapter we define the category of rings, **Ring**, and basic properties of rings.

1.1.0 Definition and First Examples

We define rings (and later modules) by 'decorating' abelian groups with additional data. In number systems we wish to multiply elements, and for this multiplication to 'preserve' addition in some precise sense; examples are $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p, ...$. We begin by studying the structure of homomorphisms of abelian groups. Recall if G, H are abelian groups, then $\mathbf{Hom}_{\mathbf{Ab}}(G, H)$ is also an abelian group. In particular, $\mathbf{End}_{\mathbf{Ab}}(G)$ is an abelian group, and more. Under composition $\mathbf{End}_{\mathbf{Ab}}(G)$ has the form of a monoid, such that the monoidal structure preserves the abelian structure - this is precisely the notion of a ring.

Definition 1.1.1 (Ring). *A **ring** $(R, +, \cdot)$ is an abelian group $(R, +)$ endowed with a binary operation $\cdot$ and an element $1_R \in R$ such that*

- $\forall r, s, t \in R; (r \cdot s) \cdot t = r \cdot (s \cdot t)$
- $\forall r \in R; r \cdot 1_R = r = 1_R \cdot r$
- $\forall r, s, t \in R : (r + s) \cdot t = r \cdot t + s \cdot t \text{ and } t \cdot (r + s) = t \cdot r + t \cdot s$

Hence we are implicitly considering rings with identity. We can define a ring structure on a trivial group $\{*\}$, through which $0 = 1$. If the monoid structure on our ring is commutative, we say the ring is commutative. Not all rings are commutative, an important example of which is of 2×2 matrices over a field.

Definition 1.1.2. *An element $a \in R$ is a **(left-)zero-divisor** if there exists $b \neq 0$ in R for which $ab = 0$.*

Right-zero-divisors are defined similarly. 0 is always a zero divisor in nonzero rings, so the zero ring is the only ring without zero-divisors.

Proposition 1.1.1. *In a ring R, $a \in R$ is not a left- (resp., right-) zero-divisor if and only if left (resp., right) multiplication by a is an injective function $R \to R$.*

In the case where all non-zero elements are such, we have the following definition:

Definition 1.1.3. *An **integral domain** is a nonzero commutative ring R (with 1) such that*

$$\forall a, b \in R : ab = 0 \implies a = 0 \text{ or } b = 0$$

Further non-zero elements in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ satisfy an even nicer property:

Definition 1.1.4. *An element $u \in R$ is a **left-(resp.,right-)unit** if $\exists v \in R$ such that $uv = 1$ (resp. $vu = 1$). **Units** are two-sided units.*

Proposition 1.1.2. *In a ring R:*

- *u is a left-(resp., right-) unit if and only if left- (resp., right-) multiplication by u is a surjective function $R \to R$.*
- *the inverse of a two-sided unit is unique*
- *two-sided units form a group under multiplication.*

Definition 1.1.5. *A **division ring** is a ring in which every nonzero element is a two-sided unit.*

If the ring is also commutative with 1 we say it is a **field**. Fields are always integral domain, but the converse is not in general true. The following is a special case where it is:

Proposition 1.1.3. *Assume R is a finite commutative ring; then R is an integral domain if and only if it is a field.*

1.2.0 Polynomial Rings

Definition 1.2.1. *Let R be a ring. A **polynomial** $f(x)$ in the **indeterminate** x and with coefficients in R is a finite linear combination of nonnegative powers of x with coefficients in R:*

$$f(x) = \sum_{i \geqslant 0} a_i x^i$$

where all $a_i \in R$ and we require $a_i = 0$ for $i \gg 0$. Two polynomials $f(x) = \sum_{i \geqslant 0} a_i x^i$ and $g(x) = \sum_{i \geqslant 0} b_i x^i$ are equal if and only if $a_i = b_i$ for all i. It is equipped with operations

$$f(x) + g(x) := \sum_{i \geqslant 0} (a_i + b_i) x^i$$

and

$$f(x) \cdot g(x) := \sum_{k \geqslant 0} \sum_{i+j=k} a_i b_j x^k$$

The **degree** of a non-zero polynomial $f(x) = \sum_{i \geqslant 0} a_i x^i$ is $\max_n\{n : a_n \neq 0\}$ if $f(x) \neq 0$, and we define $\deg 0$ to either be $-\infty$, or simply don't define it. We can define polynomial rings in finitely many indeterminates iteratively. We can also define a ring of polynomials in countably many indeterminates, $R[x_1, x_2, ...]$, as well as the ring of formal power series, $R[[x]]$.

1.3.0 Monoid Rings

Given a monoid $(M, \cdot)$ and a ring R, we can obtain a new ring $R[M]$ as follows. Elements of $R[M]$ are formal linear combinations

$$\sum_{m \in M} a_m \cdot m$$

where $a_m \in R$ and $a_m \neq 0$ for at most finitely many summands. Addition is as before, and multiplication is given by

$$\left(\sum_{m \in M} a_m \cdot m\right) \cdot \left(\sum_{m \in M} b_m \cdot m\right) = \sum_{m \in M} \sum_{m_1 m_2 = m} (a_{m_1} b_{m_2}) \cdot m$$

Chapter 2

The Category Ring

2.1.0 Ring Homomorphisms

If R, S are rings, a function $\varphi : R \to S$ is a ring homomorphism if it preserves both operations and the identity element. It then follows that rings form a category, with ring homomorphisms as morphisms. We denote this category by **Ring**. The zero-ring is final in **Ring**, but it has no maps out of it to non-zero rings.

Ring does have initial objects, namely the ring of integers $\mathbb{Z}$.

2.2.0 Universal Property of Polynomial Rings

Let $A = \{a_1, ..., a_n\}$ be a set of order n. Consider the category whose objects are pairs (j, R), where R is a commutative ring and $j : A \to R$. Morphisms are commutative diagram (explicitly we are looking at a comma category). For example $(i, \mathbb{Z}[x_1, ..., x_n])$ is an object in this category where $i : A \to \mathbb{Z}[x_1, ..., x_n]$ sends a_k to x_k. The pair $(i, \mathbb{Z}[x_1, ..., x_n])$ is in fact initial in this category.

Example 2.2.1. More generally, let $\alpha : R \to S$ be a fixed ring homomorphism, and let $s \in S$ be an element commuting with $\alpha(R)$. Then there is a unique ring homomorphism $\overline{\alpha} : R[x] \to S$ extending α and sending x to s.

In particular this gives an evaluation map for polynomials over commutative rings, $R[x] \to R$.

2.3.0 Monomorphisms and Epimorphisms

The kernel of a homomorphism of rings is not in general a subring, and in fact is only a subring if it is the whole ring and we are mapping to the zero ring. However we do have the nice property that a ring homomorphism is a monomorphism if and only if its kernel is trivial.

However, unlike in group epimorphisms need not be surjective in **Ring**. For example the monomorphism $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is also an epimorphism. This also provides an example of a map which is both a monomorphism and an epimorphism but not an isomorphism.

Further, on a categorical note, **Ring** has finite products.

2.4.0 Endomorphism Rings

For an abelian group G we return to the endomorphism group $\mathbf{End}_{\mathbf{Ab}}(G)$. Under composition we can endow this group with a ring structure. For example, $\mathbf{End}_{\mathbf{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$ as rings. The group of units in these rings is simply $\mathbf{Aut}_{\mathbf{Ab}}(G)$.

Every ring R interacts with the ring of endomorphisms of the underlying abelian group through left and right multiplication.

Proposition 2.4.1. *Let R be a ring. Then the function $r \mapsto L_r$ is an injective ring homomorphism*

$$\lambda : R \to \mathbf{End}_{\mathbf{Ab}}(R)$$

The right multiplication map is almost a ring homomorphism, in the sense that composition reverses the order of multiplication, which means it is a ring homomorphism in the case of a commutative R.

Chapter 3

Ideals and Quotient Rings

3.1.0 Ideals

Definition 3.1.1. *Let R be a ring. A subgroup I of $(R,+)$ is a **left-ideal** of R if $rI \subseteq I$ for all $r \in R$; that is*

$$\forall r \in R, \forall a \in I : ra \in I$$

*it is a **right-ideal** if $Ir \subseteq I$ for all $r \in R$; that is*

$$\forall r \in R, \forall a \in I : ar \in I$$

*A **two-sided ideal** is a subgroup I which is both a left- and a right-ideal.*

Kernels and two-sided ideals in **Ring** are equivalent.

3.2.0 Quotients

For I a two-sided ideal of R we can form the quotient ring R/I, with natural multiplication and addition. This satisfies the suitable universal property as in the group homomorphisms case. The structure on R/I is completely forced by the requirement that the natural projection $\pi : R \to R/I$ is a ring homomorphism.

The fact that $\mathbb{Z}$ is initial in **Ring** prompts a natural definition: for a ring R, let $f : \mathbb{Z} \to R$ be the unique ring homomorphism. Then $\ker f = n\mathbb{Z}$ for a well-defined nonnegative integer n determined by R.

Definition 3.2.1. *The **characteristic** of R is this nonnegative integer n.*

Thus, the characteristic of R is $n > 0$ if the order of 1_R as an element of $(R,+)$ is finite, while the characteristic is 0 if the order of 1_R is ∞.

Our universal property for quotients is as follows:

Theorem 3.2.1. *Let I be a two-sided ideal of a ring R. Then for every ring homomorphism $\varphi : R \to S$ such that $I \subseteq \ker\varphi$, there exists a unique ring homomorphism $\widetilde{\varphi} : R/I \to S$ so that the diagram*

$$\begin{tikzcd}
R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & S \\
& R/I \arrow[ur, dashed, "\widetilde{\varphi}"'] &
\end{tikzcd}$$

commutes.

From this result we can further derive a decomposition of ring homomorphisms:

Theorem 3.2.2. *Every ring homomorphism $\varphi : R \to S$ may be decomposed as follows:*

$$\begin{tikzcd}
R \arrow[r, two heads, "\pi"'] \arrow[rrr, bend left, "\varphi"] & R/\ker\varphi \arrow[r, dashed, "\sim", "\widetilde{\varphi}"'] & \operatorname{Im}\varphi \arrow[r, hook, "\iota"'] & S
\end{tikzcd}$$

where the isomorphism $\widetilde{\varphi}$ is induced by φ.

We immediately obtain the first isomorphism theorem as a corollary:

Corollary 3.2.3. *Suppose $\varphi : R \to S$ is a surjective ring homomorphism. Then $S \cong R/\ker\varphi$.*

We also have the correspondence of ideals of R/I with ideals of R containing I, given by the natural projection map. We also have the following consequence:

Proposition 3.2.4. *Let I be a two-sided ideal of a ring R and let J be a two-sided ideal of R containing I. Then J/I is a two-sided ideal of R/I, and*

$$\frac{R/I}{J/I} \cong R/J$$

3.3.0 Operations on Ideals

Let $a \in R$. Then Ra (resp. aR) is a left- (resp. right-) ideal of R. In the commutative case these coincide and are denoted (a), the **principal ideal generated by** a.

If $\{I_\alpha\}_{\alpha\in A}$ is a family of ideals of a ring R, then the sum $\sum_\alpha I_\alpha$ is an ideal of R. In the case of a family of principle ideals we have

$$(a_\alpha)_{\alpha\in A} := \sum_{\alpha\in A}(a_\alpha)$$

Definition 3.3.1. *A commutative ring R is* ***Noetherian*** *if every ideal of R is finitely generated.*

Definition 3.3.2. *An integral domain R is a* ***Principal Ideal Domain (PID)*** *if every ideal of R is principal.*

$\mathbb{Z}$ is a well-known example of a PID. If k is a field, the ring of polynomials $k[x]$ is a PID, but $\mathbb{Z}[x]$ is not.

The intersection of an arbitrary family of ideals is again an ideal, and for two ideals $I, J \subseteq R$, their product IJ is the ideal generated by all products ij for $i \in I$ and $j \in J$.

3.4.0 Quotients of Polynomial Rings

Let R be a nonzero ring and let $f \in R[x]$ be a monic polynomial. Supposing that f is monic allows us to **divide** by $f(x)$, with remainder. That is for any $g(x) \in R[x]$, there exist $q(x), r(x) \in R[x]$ such that $g(x) = f(x)q(x) + r(x)$ where $\deg r(x) < \deg f(x)$. Further the quotient and remainder polynomials are unique.

Looking at this in another way we have that all cosets in $R[x]/(f(x))$ are represented by polynomials of degree less than $\deg f(x)$. We can then view the quotient as $R^{\oplus \deg f(x)}$ with a naturally endowed ring structure. In particular as abelian groups $R[x]/(f(x)) \cong R^{\oplus \deg f(x)}$. If $\deg f(x) = 1$ then these ring structures are isomorphic, but for degrees 2 or greater we already can find interesting distinct structures.

3.5.0 Prime and Maximal Ideals

Definition 3.5.1. *Let $I \neq R$ be an ideal of commutative ring R.*

- *I is a* ***prime ideal*** *if R/I is an integral domain*
- *I is a* ***maximal ideal*** *if R/I is a field.*

Proposition 3.5.1. *Let $I \neq R$ be a proper ideal of a commutative ring R. Then*

- *I is prime if and only if for all $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$. Equivalently,*

$$(ab) \subseteq I \implies ((a) \subseteq I) \vee (b) \subseteq I)$$

- *I is maximal if and only if for all ideals J of R,*

$$I \subseteq J \implies (I = J \vee J = R)$$

Note that maximal implies prime, but in general the converse is false.

Proposition 3.5.2. *Let I be an ideal of a commutative ring R. If R/I is finite then I is prime if and only if it is maximal.*

For PIDs we have equivalence:

Proposition 3.5.3. *Let R be a PID, and let I be a nonzero ideal in R. Then I is prime if and only if it is maximal.*

Definition 3.5.2. *The* ***Krull dimension*** *of a commutative ring R is the length of the longest chain of prime ideals in R.*

Hence all PIDs have dimension 1, so they correspond to curves in algebraic geometry.

Chapter 4

Chain Conditions and Factorization

4.1.0 Prime and irreducible elements

Let R be a commutative ring. We say that $a, b \in R$ are **associates** if $(a) = (b)$.

Lemma 4.1.1. *Let a, b be nonzero elements of an integral domain R. Then a and b are associated if and only if $a = ub$ for u a unit in R.*

Definition 4.1.1. *Let R be an integral domain.*

- *An element $a \in R$ is **prime** if the ideal (a) is prime.*
- *An element $a \in R$ is **irreducible** if a is not a unit and*

$$a = bc \implies (b \in R^\times \vee c \in R^\times)$$

The definition of irreducible is equivalent to the statement that (a) is maximal among proper principal ideals. These notions are not in general equivalent, though in an integral domain primality implies irreducibility.

Lemma 4.1.2. *Let R be an integral domain, and let $a \in R$ be a nonzero prime element. Then a is irreducible.*

4.2.0 Factorization into Irreducibles

Definition 4.2.1. *Let R be an integral domain. An element $r \in R$ has a **factorization** into irreducibles if there exist irreducible elements $q_1, ..., q_n$ such that $r = q_1 \cdots q_n$.*

This factorization is said to be unique if the elements q_i are determined by r up to order and associates.

Definition 4.2.2. *An integral domain R is a domain with factorizations if every nonzer nonunit element $r \in R$ has a factorization into irreducibles.*

Definition 4.2.3. *An integral domain R is a* **unique factorization domain (UFD)***, if every nonzero, nonunit element $r \in R$ has a unique factorization into irreducibles.*

Existence of factorizations is implies by an ascending chain condition:

Proposition 4.2.1. *Let R be an integral domain, and let r be a nonzero, nonunit element of R. Assume that every ascending chain of principal ideals*

$$(r) \subseteq (r_1) \subseteq (r_2) \subseteq \cdots$$

stabilizes. Then r has a factorization into irreducibles.

Corollary 4.2.2. *Let R be a Noetherian domain. Then factorizations exist in R.*

However Noetherian domains are not necessary for factorizations. For example $\mathbb{Z}[x_1, x_2, x_3, ...]$ does have factorizations but is not a Noetherian ring.

Chapter 5

UFDs, PIDs, Euclidean Domains

5.1.0 Irreducible Factors and GCDs

In a UFD all elements determine a multiset of irreducible factors, determined up to the associate relation.

Lemma 5.1.1. *Let R be a UFD, and let a, b, c be nonzero elements of R. Then*

- $(a) \subseteq (b) \iff$ *the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a.*
- *a and b are associates if and only if the two multisets coincide.*
- *the irreducible factors of a product bc are the collection of all irreducible factors of b and of c.*

Definition 5.1.1. *Let R be an integral domain, and let $a, b \in R$. An element $d \in R$ is a* ***greatest common divisor*** *of a and b if $(a, b) \subseteq (d)$ and (d) is the smallest principal ideal in R with this property.*

GCDs need not exist in general, but they do in UFDs.

Lemma 5.1.2. *Let R be a UFD, and let a, b be nonzero elements of R. Then a, b have a greatest common divisor.*

5.2.0 Characterization of UFDs

Lemma 5.2.1. *Let R be a UFD, and let a be an irreducible element of R. Then a is prime.*

Theorem 5.2.2. *An integral domain R is a UFD if and only if*

- *the a.c.c. for principal ideals holds in R and*
- *every irreducible element of R is prime*

The PID condition is explicitly stronger than the UFD condition in that all PIDs are UFDs.

Proposition 5.2.3. *If R is a PID, then it is a UFD.*

Of course there are many UFDs which are not PIDs, evidenced by the fact that there are even UFDs which are not Noetherian rings,and all PIDs are Noetherian.

An even stronger requirement than PID is that of being a **Euclidean domain**. For the purpose of this discussion, a **valuation** on an integral domain R is a function $v : R\backslash\{0\} \to \mathbb{Z}^{\geqslant 0}$.

Definition 5.2.1. *A **Euclidean valuation** on an integral domain R is a valuation satisfying the following property: for all $a \in R$ and all nonzero $b \in R$, there exists $q, r \in R$ such that*

$$a = qb + r$$

*with either $r = 0$ or $v(r) < v(b)$. An integral domain R is a **Euclidean domain** if it admits a Euclidean valuation.*

Proposition 5.2.4. *Let R be a Euclidean domain. Then R is a PID.*

One excellent feature of Euclidean domains is a Euclidean algorithms. The key lemma on which the algorithm is based in the following fact:

Lemma 5.2.5. *Let $a = bq + r$ in a ring R. Then $(a, b) = (b, r)$.*

That is the set of common divisors of a, b and the set of common divisors of b, r coincide.

Corollary 5.2.6. *Assume $a = bq + r$. Then a, b have a gcd if and only if b, r have a gcd, and in this case $gcd(a, b) = gcd(b, r)$.*

Chapter 6

Unique Factorization in Polynomial Rings

After necessary work we aim to show that $R[x]$ is a UFD if R is.

6.1.0 Primitivity and Content; Gauss's Lemma

Observe that every ideal I of R generates an ideal of $R[X]$,

$$IR[X] := \{a_0 + a_1X + \cdots + a_dX^d \in R[X] : \forall i, a_i \in I\}$$

Lemma 6.1.1. *Let R be a ring, and let I be an ideal of R. Then*

$$R[X]/IR[X] \cong (R/I)[X]$$

Corollary 6.1.2. *If I is a prime ideal of R, then $IR[X]$ is a prime in $R[X]$.*

Definition 6.1.1. *Let R be a commutative ring, and let $f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$ be a polynomial.*

- *f is **very primitive** if for all prime ideals $\mathfrak{p}$ of R, $f \notin \mathfrak{p}R[x]$*
- *f is **primitive** if for all principal prime ideals $\mathfrak{p}$ of R, $f \notin \mathfrak{p}R[x]$*

Very primitive polynomials are primitive, but the converse does not hold in general, even in UFDs.

Lemma 6.1.3. *Let R be a commutative ring. Then for $f, g \in R[x]$,*

$$fg \text{ is primitive} \iff \text{both } f \text{ and } g \text{ are primitive}$$

Lemma 6.1.4. *Let R be a commutative ring and $f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$ as above.*

- *f is very primitive if and only if $(a_0, ..., a_d) = (1)$*

- *If R is a UFD, then f is primitive if and only if gcd$(a_0, ..., a_d) = 1$*

Definition 6.1.2. *Let R be a UFD. The **content** of a nonzero polynomial $f \in R[x]$, denoted cont$_f$, is the gcd of its coefficients.*

Thus f is primitive precisely when $(\text{cont}_f) = (1)$.

Lemma 6.1.5. *Let R be a UFD, and let $f \in R[x]$. Then*

- *$(f) = (\text{cont}_f)(\underline{f})$, where $\underline{f}$ is primitive*
- *if $(f) = (c)(g)$, with $c \in R$ and g primitive, then $(c) = (\text{cont}_f)$.*

Proposition 6.1.6 (Gauss's Lemma)**.** *Let R be a UFD, and let $f, g \in R[x]$. Then*

$$(\text{cont}_{fg}) = (\text{cont}_f)(\text{cont}_g)$$

Corollary 6.1.7. *Let R be a UFD, and let $f, g \in R[x]$. Assume $(f) \subseteq (g)$. Then $(\text{cong}_f) \subseteq (\text{cont}_g)$.*

6.2.0 The Field of Fractions

The Field of Fractions is a special case of a universal construction known as localization. For an integral domain R, its field of fractions is the pair $(i, K(R))$ where $i : R \to K(R)$ is an injective ring homomorphism and $K(R)$ is a field, and this pair is initial with this property. Thus $K(R)$ is in a way the 'smallest field containing R'.

An explicit construction of $K(R)$ is given by $R \times (R\backslash\{0\})/\sim$, where $(a, b) \sim (d, c)$ if and only if $ac = bd$. Multiplication and addition are done as in $\mathbb{Q}$ (in particular, $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$).

Definition 6.2.1. *The field of **rational functions** with coefficients in R is the field of fractions of the ring $R[x]$. This field is denoted $R(x)$.*

We are now in a position to prove the following:

Theorem 6.2.1. *Let R be a UFD, then $R[x]$ is a UFD.*

By an immediate induction we have that $\mathbb{Z}[x_1, ..., x_n]$ and $k[x_1, ..., x_n]$ are UFDs. However, $R[[x]]$ is not necessarily a UFD even if R is.

We aim to verify that $R[x]$ satisfies the a.c.c. on principal ideals, and that every irreducible element in $R[x]$ is prime, provided R is a UFD. We aim to reduce these questions to $K(R)[x]$.

Lemma 6.2.2. *Let R be a UFD and let K be its field of fractions. For nonzero $f, g \in R[x]$, denote by $(f), (g)$ the principal ideals $fR[x], gR[x]$ in $R[x]$, and denote by $(f)_K, (g)_K$ the principal ideals $fK[x], gK[x]$ in $K[x]$. Assume*

- $(\mathrm{cont}_g) \subseteq (\mathrm{cont}_f)$ *and*
- $(g)_K \subseteq (f)_K$

Then $(g) \subseteq (f)$.

Proposition 6.2.3. *Let R be a UFD, and let $f \in R[x]$ be a nonconstant, irreducible polynomial. Then f is irreducible as an element of $K(R)[x]$.*

Corollary 6.2.4. *Let R be a UFD and let $f \in R[x]$ be a nonconstant polynomial. Then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$ and primitive.*

Part II

Module Theory

Chapter 7

Intro to Modules over a Ring

The category **Ring** fails to satisfy many nice properties, such as how kernels and cokernels behave. Modules will fix a majority of these issues. If R is a ring and $I \subseteq R$ is a two-sided ideal, then all three structures R, I, and R/I will be modules over R.

7.1.0 Definition of (left-)R-modules

A left-R-module M is simply an abelian group $(M, +)$ along with a ring action given by a homomorphism of rings

$$\sigma : R \to \mathbf{End}_{\mathbf{Ab}}(M)$$

Proposition 7.1.1. *The datum of a homomorphism σ as above is precisely the same as the datum of a function*

$$\rho : R \times M \to M$$

satisfying the following requirements: $\forall r, s \in R, \forall m, n \in M$

- $\rho(r, m + n) = \rho(r, m) + \rho(r, n)$
- $\rho(r + s, m) = \rho(r, m) + \rho(s, m)$
- $\rho(rs, m) = \rho(r, \rho(s, m))$
- $\rho(1, m) = m$

We can define right-R-modules analogously, viewing a right-R-module as a left-R^{op}-module structure. These issues become immaterial if R is commutative. Then the identity $R \to R^{op}$ is an isomorphism, and left-modules/right-modules are identical concepts.

7.2.0 The Category R-mod

As a first example we note that $\mathbb{Z} - \mathbf{mod} \cong \mathbf{Ab}$ are equivalent categories in a natural way.

A homomorphism of R-modules is a homomorphism of abelian groups which is compatible with the module structure. The set $\mathbf{Hom}_R(M, N)$ has the structure of an abelian group for any R-modules M and N.

Given a ring homomorphism $\alpha : R \to S$, we can induce an R-module structure on S. Further if $\alpha(R)$ also lands in the center of S we define the following notion.

Definition 7.2.1. *Let R be a commutative ring. An R-**algebra** is a ring homomorphism $\alpha : R \to S$ such that $\alpha(R)$ is contained in the center of S.*

An R-algebra S is a **division algebra** if S is a division ring. This gives us another category **R-Alg**. Further, $\mathbb{Z} - \mathbf{Alg}$ is equivalent to **Ring**.

Canonical examples are the polynomial rings $R[x_1, ..., x_n]$ and their R-algebras.

The category of R-modules has a zero object given by inducing a module structure on the trivial group, 0.

Now, if R is commutative, $\mathbf{Hom}_R(M, N) \in R - \mathbf{mod}$.

7.3.0 Submodules and Quotients

A **submodule** N of an R-module M is a subgroup preserved by the action of R. Equivalently N is an R-module with the natural inclusion $N \subseteq M$ being an R-module homomorphism. Both the kernel and image of a homomorphism of R-modules are submodules.

If N is a submodule of M we can define the quotient M/N of abelian groups, and it can then be shown that their is a unique module structure on M/N for which $\pi : M \to M/N$ is an R-module homomorphism.

Remark 7.3.1. If R is not commutative and I is a left-ideal, then the quotient R/I need not be defined as a ring, but it is defined as a left-module.

Theorem 7.3.1. *Let N be a submodule of an R-module M. Then for every homomorphism of R-modules $\varphi : M \to P$ such that $N \subseteq \ker \varphi$ there exists a unique homomorphism of R-modules $\widetilde{\varphi} : M/N \to P$ so that the diagram*

$$\begin{tikzcd}
M \arrow[rr, "\varphi"] \arrow[dr, two heads, "\pi"'] & & N \\
& M/N \arrow[ur, dashed, "\widetilde{\varphi}"'] &
\end{tikzcd}$$

commutes.

As in previous cases we have a one-to-one correspondence between kernels of R-module homomorphisms out of M and submodules of M. Further, every monomorphism in R-mod is a kernel.

Theorem 7.3.2. *Every R-module homomorphism $\varphi : M \to M'$ may be decomposed as follows:*

$$\begin{tikzcd} M \arrow[r, two heads, "\pi"'] \arrow[rrr, bend left, "\varphi"] & M/\ker\varphi \arrow[r, dashed, "\sim", "\widetilde{\varphi}"'] & \operatorname{Im}\varphi \arrow[r, hook, "\iota"'] & M' \end{tikzcd}$$

where the isomorphism $\widetilde{\varphi}$ is induced by φ.

Corollary 7.3.3. *Suppose $\varphi : M \to M'$ is a surjective R-module homomorphism. Then $M' \cong M/\ker\varphi$.*

If N is a submodule of M then there is a bijection between submodules of M containing N and submodules of M/N, induced by π.

Proposition 7.3.4. *Let N be a submodule of an R-module M, and let P be a submodule of R containing N. Then P/N is a submodule of M/N and*

$$\frac{M/N}{P/N} \cong M/P$$

Proposition 7.3.5. *Let N and P be submodules of an R-module M. Then*

- *$N + P$ is a submodule of M*
- *$N \cap P$ is a submodule of P, and*

$$\frac{N+P}{N} \cong \frac{P}{N \cap P}$$

7.4.0 Noetherian Modules

Definition 7.4.1. *An R-module M is Noetherian if every submodule of M is finitely generated.*

This condition is preserved through exact sequences: if M, N, P are R-modules and

$$0 \to N \hookrightarrow M \twoheadrightarrow P \to 0$$

is an exact sequence, then M is Noetherian if and only if both N and P are Noetherian.

Corollary 7.4.1. *Every finitely sum of Noetherian modules is Noetherian.*

Proposition 7.4.2. *Let R be a commutative ring, and let M be an R-module. Then the following are equivalent:*

1. *M is Noetherian*
2. *M satisfies the a.c.c. on submodules*
3. *Every nonempty family of submodules of M has a maximal element with respect to incluson.*

Theorem 7.4.3. *Let R be a Noetherian ring, and let J be an ideal of the polynomial ring $R[x_1, ..., x_n]$. Then the ring $R[x_1, ..., x_n]/J$ is Noetherian.*

Lemma 7.4.4 (Hilbert's Basis Theorem)**.** *If R is Noetherian then $R[x]$ is Noetherian.*

Appendices