Definitions for Commutative Algebra

Robert L. Bocchino Jr.

Revised January 2023

This document defines concepts used in the area of mathematics known as **commutative algebra**. This area focuses on commutative rings, and modules and algebras over commutative rings. It is important in other areas of mathematics such as algebraic geometry and algebraic number theory.

The motivations for this document are as follows:

1. These definitions form the essential vocabulary of commutative algebra. Mastering them is essential for understanding even basic results in the field.
2. There are many definitions, drawn from a wide range of subjects, including classical algebra, homological algebra, topology, and category theory.
3. I find it hard to keep all the definitions in my head, especially if I haven't thought about commutative algebra for a while.

It therefore seems useful to extract these definitions and present them in a self-contained and systematic way that is suitable for study and reference. If you have mastered the definitions in this document, then you should be able to open any book on commutative algebra — say [Matsumura 1986] or [Eisenbud 1995] — and at least feel that you understand what most of the terms and the symbols mean. On the other hand, if you don't understand these definitions, then trying to read any part of any such book is likely to be a bewildering experience.

The definitions are of course available in the standard textbooks, but they are buried inside long expositions ([Eisenbud 1995], for example, runs to over 800 pages) containing detailed discussions and proofs. By reading this document, you can get the essential definitions, without searching through hundreds of pages of text. The definitions provide a good sense of what the subject is about, as well as a strong foundation for understanding the results stated and proved elsewhere. Also, I don't know of any other text that defines all these terms in a self-contained and self-consistent way, starting with the very basics (sets, maps, monoids, and groups).

I have tried as much as possible to describe the objects of study without proving facts about them — the proofs I leave to the textbooks. However, in some cases it is necessary to assert basic facts. For example, one cannot talk about "the" inverse of an element in a group without asserting that each element has a unique inverse. Easy proofs I include inline; other proofs I omit with a note "(proof omitted)." Some of these proofs are straightforward exercises. All of them are available in the standard textbooks, or online.

This document is self-contained, in the sense that it starts with fundamental concepts (numbers, sets, and maps) and uses only terms that it has defined. However, the document is somewhat terse. If you have never seen these ideas before, particularly the ideas in the first few sections, then it may be best to consult a basic textbook before reading this document, or while reading it. Good basic textbooks include [Lang 1987] (introductory algebra) and [Atiyah and Macdonald 1967] (introductory commutative algebra). More advanced textbooks are given in the references.

The document is readable in order. Later sections refer to earlier ones.

1. Numbers

We assume the existence and standard properties of the following basic mathematical objects:

1. The natural numbers $\mathbf{N}$. These are the numbers $0, 1, 2, \ldots$. We write $\mathbf{N}^+$ to denote the positive natural numbers $1, 2, \ldots$.
2. The integers $\mathbf{Z}$. These are the natural numbers together with the negative numbers $-1, -2, \ldots$.
3. The rational numbers $\mathbf{Q}$. These are fractions a/b, where a and b are integers.

4. The real numbers **R**. These are numbers each of which may be represented as an integer plus a finite or infinite sequence of decimal digits.
5. The complex numbers **C**. These are numbers $a + bi$, where a and b are real numbers, and $i^2 = -1$.

2. Sets and Maps

A **set** S is a collection of elements, called the **members** or **elements** of S. We write $s \in S$ to indicate that s is a member of S. (The symbol $\in$ is similar to the Greek letter epsilon or ε and probably stands for "element.") When we wish to enumerate the members of a set, we write a list of members enclosed in braces. For example $\{1, 2, 3\}$ denotes the set containing the elements 1, 2, and 3. In this notation, the order in which the elements are listed is not significant. Any duplicate elements are ignored: for example, $\{1, 2, 2, 3\}$ has the same meaning as $\{1, 2, 3\}$.

The **empty set**, written $\varnothing$, is the unique set that has no members.

Fix sets A and B.

1. A is a **subset** of B if for each $a \in A$, we have $a \in B$. We write $A \subseteq B$ or $B \supseteq A$ to indicate that A is a subset of B. We also say that B is a **superset** of A.
2. A is a **strict subset** of B if $A \subseteq B$ and $A \neq B$. We write $A \subset B$ or $B \supset A$ to indicate that A is a strict subset of B. We also say that B is a **strict superset** of A.
3. A **equals** B if A and B have the same members. We write $A = B$ to indicate that A equals B. $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$ (proof omitted).
4. The **set difference** of A and B", written $A - B$ or $A \setminus B$, is the set consisting of all elements $a \in A$ such that $a \notin B$.
5. A **relation** on (A, B) is a set of ordered pairs (a, b) such that $a \in A$ and $b \in B$.
6. A **map** $f\colon A \to B$ is a relation R on (A, B) such that for each element $a \in A$, there is a unique pair $(a, b) \in R$. We write $b = f(a)$, and we write the relation as a mapping $a \mapsto f(a)$, indicating that f maps a to $f(a)$ as ranges over the elements of A.
7. The terms **mapping** and **function** are synonyms for "map." Some authors reserve the term "function" for maps from numbers to numbers.

Fix sets A and B. Two maps $f\colon A \to B$ and $g\colon A \to B$ are **equal** if the corresponding relations on (A, B) are equal sets. Equivalently, for each $a \in A$, we have $f(a) = g(a)$. In this case we write $f = g$.

Fix a set S and a map $f\colon S \to \{\text{true}, \text{false}\}$. The notation $\{s \in S \mid f(s)\}$ or $\{s \in S : f(s)\}$ is called a **set comprehension**. It denotes all elements s in S such that $f(s) = \text{true}$. For example, $\{n \in \mathbf{N} \mid n > 0\}$ denotes the set $\mathbf{N}^+$.

Fix sets A and B and a map $f\colon A \to B$.

1. The **image** of f, denoted $f(A)$, is the set of elements $b \in B$ such that $b = f(a)$ for some $a \in A$.
2. f is **injective** if $f(a) = f(a')$ implies $a = a'$. That is, no two distinct elements in A map to the same element of B. Some texts say that an injective map is a map **into** B.
3. f is **surjective** if $f(A) = B$. Some texts say that a surjective map is a map **onto** B.
4. f is **bijective** if it is injective and surjective.
5. For any set $C \subseteq B$, the **inverse image** of C under f, written $f^{-1}(C)$, is the set of all $a \in A$ such that $f(a) \in C$.

If $f\colon A \to B$ is injective, then the induced map $f'\colon A \to f(A) = a \mapsto f(a)$ is bijective. An injective map is sometimes called an **inclusion map** or an **embedding**, because we can think of A as being included in B via the bijection f' and the inclusion $f'(A) \subseteq B$.

The **cardinality** of a set S is defined as follows:

1. If there is a bijection between S and a finite set with n elements, then the cardinality is **finite** and equal to n.
2. Otherwise if there is a bijection between S and **N**, then the cardinality is **countably infinite**.
3. Otherwise the cardinality is **uncountable**.

In cases 1 and 2, we say that the cardinality is **countable**. In cases 2 and 3, we say that the cardinality is **infinite**. **N**, **Z**, and **Q** are countably infinite (proof omitted). **R** and **C** are uncountable (proof omitted).

Fix sets A, B, and C, and maps $f\colon A \to B$ and $g\colon B \to C$. The **composition** $g \circ f$ is the map from A to C defined by $a \mapsto g(f(a))$. Note that g and f appear in the same order in the expressions $g \circ f$ and $g(f(a))$.

Fix a set A. The **identity map** on A is the map $a \mapsto a$. It is a bijection from A to A.

Fix sets A and B and a bijective map $f\colon A \to B$. The **inverse** of f, written f^{-1}, is the unique map $f^{-1}\colon B \to A$ such that $f^{-1} \circ f$ is the identity map on A and $f \circ f^{-1}$ is the identity map on B.

A **family** is a set S, a set I called the **index set**, and a bijective map $f\colon I \to S$. S and I may be finite or infinite. When I is finite, we say that the family is **finite**. For $i \in I$, we write $f(i)$ as S_i, and we write $\{S_i\}_{i \in I}$ to denote the family.

Let F be a family of sets $\{S_i\}_{i \in I}$.

1. The **union** $\bigcup_{i \in I} S_i$ represents the set of all elements s, each of which a member of at least one S_i. If any s is a member of both S_i and S_j, for $i \neq j$, then s appears only once in the union. When $I = \{1, \ldots, n\}$, we may write $S_1 \cup \cdots \cup S_n$ or $\bigcup_{i=1}^{n} S_i$.
2. The **intersection** $\bigcap_{i \in I} S_i$ represents the set of all elements s_i, each of which is a member of every S_i. When $I = \{1, \ldots, n\}$, we may write $S_1 \cap \cdots \cap S_n$ or $\bigcap_{i=1}^{n} S_i$. Two sets A and B are **disjoint** if $A \cap B = \varnothing$.
3. The **disjoint union** $\biguplus_{i \in I} S_i$ represents the set of all ordered pairs (s, i) such that $i \in I$ and $s \in S_i$. When $I = \{1, \ldots, n\}$, we may write $S_1 \uplus \cdots \uplus S_n$ or $\biguplus_{i=1}^{n} S_i$.

When constructing disjoint unions, we often (but not always) omit the labels i and refer to elements (s, i) as s. In particular, we do this when constructing families with repeated elements. For example, we write the family $\{(\mathbf{Z}, i)\}_{i \in I}$ as $\{\mathbf{Z}\}_{i \in I}$. Either notation means that there is one distinct copy of $\mathbf{Z}$ for each element of I.

Fix a family of mutually disjoint, non-empty sets $\{S_i\}_{i \in I}$. The **axiom of choice** is an axiom of standard set theory.[1] It says that there exists a set $S \subseteq \bigcup_{i \in I} S_i$ and a bijection $f\colon I \to S$ (the "choice function") such that for all $i \in I$, $f(i) \in S_i$.

Let F be a family of sets $\{S_i\}_{i \in I}$, where I is an index set.

1. $S = \bigtimes_{i \in I} S_i$ denotes the **Cartesian product** of F. It is the set consisting of all families of elements $\{s_i\}_{i \in I}$ such that $s_i \in S_i$ for all $i \in I$. In particular, if any $S_i = \varnothing$, then $S = \varnothing$. When $I = \{1, \ldots, n\}$, we can write the Cartesian product as $S_1 \times \cdots \times S_n$ or $\bigtimes_{i=1}^{n} S_i$, and we can write each element of the Cartesian product as an ordered tuple $(s_1, \ldots, s_n)$.
2. For any $i \in I$, the ith **projection map** $\pi_i\colon S \to S_i$ is defined by $\pi_i(\{s_i\}_{i \in I}) = s_i$. For example, let $s = (1, 2, 3) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$. Then $\pi_2(s) = 2$.
3. For any $i \in I$, a map $f\colon S_i \to S$ is an **injection map** if $\pi_i \circ f\colon S_i \to S_i$ is the identity map. f is **stable** if, in addition, for each $j \neq i$, $\pi_j \circ f$ is a constant map $s \mapsto s_j$, where the constant s_j depends on f and on j but not on s. For example, the map $x \mapsto (x, 1, 2)$ is a stable injection map from $\mathbf{Z}$ to $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$.

Fix a set S.

1. A **partition** of S is a family $\{S_i\}_{i \in I}$ of mutually disjoint subsets of S such that $\bigcup_{i \in I} S_i = S$.
2. An **equivalence relation on** S is a relation R on (S, S) where we write $a \sim b$ to denote that $(a, b) \in R$, and the following conditions hold:
   a. **Reflexivity:** For all $a \in S$, $a \sim a$.
   b. **Symmetry:** If $a \sim b$ then $b \sim a$.
   c. **Transitivity:** If $a \sim b$ and $b \sim c$, then $a \sim c$.

   An equivalence relation on S induces a partition $\{S_i\}_{i \in I}$ of S in which a and b belong to the same S_i if and only if $a \sim b$. The mutually disjoint subsets in the partition are called **equivalence classes**. Conversely, every partition induces an equivalence relation, with the sets in the partition as the equivalence classes.

[1] Specifically, it is an axiom of ZFC, or Zermelo-Fraenkel set theory with the axiom of choice. ZFC is the standard set theory used in mathematics.

3. A **partial order on** S is a relation R on (S, S) where we write $a \leq b$ to denote that $(a, b) \in R$, and the following conditions hold:
   a. **Reflexivity:** For all $a \in S$, $a \leq a$.
   b. **Antisymmetry:** If $a \leq b$ and $b \leq a$, then $a = b$.
   c. **Transitivity:** If $a \leq b$ and $b \leq c$, then $a \leq c$.

   The relation $\subseteq$ is a partial order on any set of sets (proof omitted).
4. A **total order on** S is a relation T on (S, S) such that
   a. T is a partial order.
   b. For any elements a and b in S, either $a \leq b$ or $b \leq a$ (or both).

A **partially ordered set** is a set S together with a partial order P on S. A **totally ordered set** is a set S together with a total order T on S.

Fix a partially ordered set A and a subset B of A.

1. An **upper bound** of B in A is an element $a \in A$ such that for all $b \in B$, $b \leq a$.
2. A **maximal element** of B is an element $b \in B$ that is an upper bound of B in A.
3. B is a **chain** in A if it is finite and it is totally ordered with respect to the partial order inherited from A.
4. If every chain in A has an upper bound in A, then A contains a maximal element of A. This statement is called **Zorn's lemma**; it is equivalent to the axiom of choice (proof omitted).

A **directed set** is a nonempty partially ordered set S in which every pair of elements of S has an upper bound. That is, for all a and b in S, there exists c in S such that $a \leq c$ and $b \leq c$.

Fix a set S of sets and a set $A \in S$.

1. A is **minimal** among the sets in S if for any set $B \in S$, $A \subseteq B$.
2. A is **maximal** among the sets in S if for any set $B \in S$, $B \subseteq A$.

Fix a set S.

1. A **net** of in S is a family of indexed pairs $\{(s_i, i)\}_{i \in I}$, where I is a directed set (not necessarily countable), and $s_i \in S$ for all i.
2. A **sequence** in S is a net $\{(s_i, i)\}_{i \in I}$, where I is totally ordered and countable.
   a. If I is finite, then we say that the sequence is **finite**. The most common index sets for finite sequences are $\{1, 2, \ldots, n\}$ and $\{0, 1, 2, \ldots, n\}$.
   b. Otherwise we say that the sequence is **infinite**. Often we use $\mathbf{N}$ or $\mathbf{N}^+$ as the index set for an infinite sequence.

When writing sequences and nets, we often omit the index labels, i.e., we write $\{s_i\}_{i \in I}$. We also write sequences by enumerating the elements, e.g., $s_1, s_2, \ldots$.

Fix a set S, and fix a sequence of elements $s = \{s_i\}_{i \in \mathbf{N}}$ in S. s is **stationary** if there exists $i \in I$ such that for all $j \geq i$, $s_j = s_i$. We may represent a stationary sequence as follows:

$$s_0, s_1, \ldots, s_i, s_i, s_i, \ldots$$

Fix a partially ordered set A and a sequence $B = \{a_i\}_{i \in I}$ of elements in A that is totally ordered with respect to $\leq$.

1. B is **increasing** if for all $i \geq j$, $a_i \geq a_j$.
2. B is **decreasing** or if for all $i \geq j$, $a_i \leq a_j$.

Let S be a set of numbers.

1. The **supremum** of S, written sup S, is the smallest number n such that $n \geq s$ for all $s \in S$ if there is such an n; otherwise sup $S = \infty$.
2. The **infimum** of S, written inf S, is the largest number n such that $n \leq s$ for all $s \in S$ if there is such an n; otherwise sup $S = -\infty$.

A **class** is a collection of elements that is not required to be a set.[2]

1. Every set is a class, but not every class is a set.
    a. A class that is not a set is called a **proper class**.
    b. A class that is a set is called a **small class**.
2. We define mappings between classes analogously to mappings between sets.
3. A **class-indexed family** is a class indexed by another class, analogously to the way that a family is a set indexed by another set.

Proper classes provide a way to specify collections of elements that are impossible to specify as sets. For example, consider the collection C of all sets S such that $S \notin S$.[3] If we require C to be a set, then we arrive at a contradiction: $C \in C$ implies $C \notin C$, and vice versa. This is the famous **Russell Paradox**. On the other hand, if C is a class, there is no contradiction, because C is not required to be a set.

3. Binary Operations

A **binary operation** on a set S is a map $o\colon S \times S \to S$. We write $o(a, b)$ as $a \cdot b$ or $a\ o\ b$.

1. o is **associative** if for all a_1, a_2, and a_3 in S, $a_1 \cdot (a_2 \cdot a_3) = (a_1 \cdot a_2) \cdot a_3$. In this case we can write $a_1 \cdot a_2 \cdot a_3$ without ambiguity, and similarly we can write $a_1 \cdot \ldots \cdot a_n$ for, $n > 3$.
2. o is **commutative** if for all a and b in S, $a \cdot b = b \cdot a$.
3. o has an **identity element** if there exists an element $e \in S$ (the identity element) such that for all $a \in S$, $a \cdot e = e \cdot a = a$. In this case, if e' is an identity element, then $e = e \cdot e' = e'$. So if o has an identity element, then that element is unique.

Fix a set S and an operation o on S. An element $s \in S$ is **idempotent** with respect to o if $s \cdot s = s$. The identity element e, if it exists, is idempotent.

Fix a set S and an associative operation o on S with an identity element e.

1. For any $a \in S$, a **has an inverse** with respect to o if there exists an element a^{-1} (the inverse) such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. In this case, if b is an inverse for a, then
$$b = b \cdot e = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = e \cdot a^{-1} = a^{-1}.$$
So if a has an inverse with respect to o, then that inverse is unique.
2. The operation o **has inverses** if for all $a \in S$, a has an inverse with respect to o.

Fix an element $s \in S$ and a subset $A \subseteq S$. We write $s \cdot A$ (respectively $A \cdot s$) to represent the set $\{s \cdot a \mid a \in A\}$ (respectively $\{a \cdot s \mid a \in A\}$).

Fix a set S and an operation o on S.

1. o **distributes over** an operation o' on S if for all a, b, and c in S
    a. $a\ o\ (b\ o'\ c) = (a\ o\ b)\ o'\ (a\ o\ c)$.
    b. $(a\ o'\ b)\ o\ c = (a\ o\ c)\ o'\ (b\ o'\ c)$.

    For example, in the integers, multiplication distributes over addition, so $1 \cdot (2 + 3) = 1 \cdot 2 + 1 \cdot 3$ and $(1 + 2) \cdot 3 = 1 \cdot 3 + 2 \cdot 3$.
2. Fix subsets A and B of S.
    a. A is **closed under** o **with respect to** B if for any $a \in A$, $a \cdot B \subseteq B$ and $B \cdot a \subseteq B$.
    b. A is **closed under** o if it is closed under o with respect to itself. In this case, o is a binary operation on A.

Fix a family of sets $\{S_i\}_{i \in I}$ such that each S_i has a binary operation o_i. The **direct product** $\prod_{i \in I} S_i$ is the set consisting of all families of elements $\{s_i \in S_i\}_{i \in I}$. It is equipped with the following binary operation o:

[2] The concept of a class comes from an alternative to ZFC called Von Neumann-Bernays-Gödel set theory (NBG).

[3] Note that we cannot specify C as a set comprehension, as defined above, because we have no set T to put into the formula $\{S \in T : S \notin S\}$. For this reason, the form of set comprehension defined above is sometimes called **restricted comprehension**. Unrestricted comprehension leads to the paradox discussed in the text.

$$\{s_i\}_{i \in I} \cdot \{s_i'\}_{i \in I} = \{s_i \cdot s_i'\}_{i \in I}$$

o has the following properties:

1. If each o_i is associative, then o is associative.
2. If each o_i is commutative, then o is commutative.
3. If each o_i has an identity element e_i, then o has an identity element $\{e_i\}_{i \in I}$.
4. If each o_i has inverses, then o has inverses, and the inverse of $\{s_i\}_{i \in I}$ is $\{s_i^{-1}\}_{i \in I}$.

The **direct sum** $\bigoplus_{i \in I} S_i$ is the set of elements $\{s_i\}_{i \in I}$ of the direct product $\prod_{i \in I} S_i$ such that all but finitely many of the s_i are the identity element e_i for S_i. This means that for the direct sum to be defined, either the index set I must be finite, or all but finitely many of the o_i must have an identity element. The direct sum has the same binary operation o as the direct product, applied to the elements of the direct product that lie in the direct sum. This operation is well defined, because if s and s' both lie in the direct sum, then all but finitely many of the elements $s_i \; o \; s_i'$ are the identity element e_i. Also:

1. When I is finite, then the definitions of the direct product and the direct sum coincide.
2. When $I = \{1, \ldots, n\}$, we can write the direct sum $S_1 \oplus \cdots \oplus S_n$ or $\bigoplus_{i=1}^{n} S_i$, and we can represent the elements of the direct sum as ordered tuples $(s_1, \ldots, s_n)$.

The name "direct sum" comes from the behavior of this construct when $\{S_i\}_{i \in I}$ is a family of additive monoids. We explain this behavior in the next section.

4. Monoids

A **monoid** $A = (S, o)$ is a set S with a binary operation o that is associative and has an identity element e.

A **submonoid** B of a monoid A is a subset of A that contains e and that is closed under the monoid operation o. B is a monoid with respect to o.

Fix a monoid A and a subset (not necessarily a submonoid) $S \subseteq A$. The set S' **generated by** S is the set of all $s_1 \cdot \ldots \cdot s_n$ where all $s_i \in S$. S' is a submonoid if and only if S contains e. In this case it is minimal among the submonoids of A that contain S.

Fix monoids A and B. A **monoid homomorphism** (or just **homomorphism**, when the context is clear) from A to B is a map $f\colon A \to B$ such that for all a and a' in A, $f(a \cdot a') = f(a) \cdot f(a')$ and $f(e) = e$.

1. A homomorphism that is injective (§ 2) is sometimes called a **monomorphism**.
2. A homomorphism that is surjective (§ 2) is sometimes called an **epimorphsim**.

In category theory, the terms "monomorphism" and "epimorphism" are more general.

An **additive monoid** is a commutative monoid together with the following conventions:

1. We call the operation o **addition**, and we write $a \; o \; a'$ as $a + a'$.
2. We write e as 0.
3. For any $n \geq 0$, let $\sum_{i=1}^{n} a_i$ denote 0 if $n = 0$, otherwise $a_1 + \cdots + a_n$. We write $\sum_{i=1}^{n} a$ as na. In particular, $1a = a$ and $0a = 0$, where the zero on the left-hand side is an integer, and the zero on the right-hand side is the identity element of the monoid.
4. Fix an element $s \in S$ and a subset $A \subseteq S$. We write $A + s$ (or $s + A$) to represent the set $\{a + s \mid s \in S\}$.

The nonnegative integers $0, 1, 2, \ldots$ with addition form an additive monoid.

Fix an additive monoid A. A set $S \subseteq A$ **generates** A if each element $a \in A$ may be expressed as $a = \sum_{i=1}^{m} n_i s_i$, with n_i a positive natural number and $s_i \in S$. In this case we say that S is a set of **generators** for A. A is **finitely generated** if it is generated by a finite set S.

A **multiplicative monoid** is a monoid together with the following conventions:

1. We call the operation o **multiplication**, and we write aa' for $a \; o \; a'$.

2. We write e as 1.
3. For any $n \geq 0$, let $\prod_{i=1}^{n} a_i$ denote 1 if $n = 0$, otherwise $a_1 \cdots a_n$. We write $\prod_{i=1}^{n} a$ as a^n. In particular, $a^1 = a$ and $a^0 = 1$.
4. Fix an element $s \in S$ and a subset $A \subseteq S$. We write As (or sA) to represent the set $\{as \mid a \in A\}$.

The natural numbers $\mathbf{N}^+ = \{1, 2, \ldots\}$ with multiplication form a multiplicative monoid.

Fix a multiplicative monoid A. A set $S \subseteq A$ **generates** A if each element $a \in A$ may be expressed as $a = \prod_{i=1}^{m} s_i^{n_i}$, with $s_i \in S$ and $s_i \in S$. In this case we say that S is a set of **generators** for A. A is **finitely generated** if it is generated by a finite set S.

A multiplicative monoid need not be commutative. For example, the set of all 3×3 matrices over the real numbers forms a non-commutative multiplicative monoid, with matrix multiplication as o and the identity matrix as e.

Fix a family $F = \{A_i\}_{i \in I}$ of monoids. The **direct product** (respectively **direct sum**) of F as a monoid is the direct product (respectively direct sum) of F with respect to the monoid operations o_i of the family. It is a monoid. When F is a family of additive monoids, the direct sum $\bigoplus_{i \in I} A_i$ is isomorphic to the additive monoid $(S, +)$ constructed in the following way:

1. S is the set of finite formal sums $\sum_{j=1}^{n} a_j$ with each $a_j \in \bigcup_{i \in I} A_i$, where two formal sums are equivalent if each may be put into a common form by carrying out monoid addition (when a_j and a_k are in the same A_i) and rearranging terms.
2. The zero element is the empty sum.
3. $(\sum_{j=1}^{m} a_j) + (\sum_{j=1}^{n} b_j) = \sum_{j=1}^{m} a_j + \sum_{j=1}^{n} b_j$.

This fact motivates the name "direct sum."

5. Groups

A **group** is a monoid whose operation o has inverses.

An **abelian group** is a group whose operation is commutative. The integers $\mathbf{Z}$ under addition form an abelian group. The set $\mathbf{Q} - \{0\}$, where $\mathbf{Q}$ represents the rational numbers with multiplication, forms an abelian group.

A **subgroup** B of a group A is a subset of A that is a group with respect to o.

Fix groups A and B. A **group homomorphism** from A to B is a map $f: A \to B$ that is a monoid homomorphism with respect to the group operation. For all a in A, $e = f(e) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$, so $f(a^{-1}) = f(a)^{-1}$.

A **group isomorphism** is a group homomorphism that is bijective. Two groups A and B are **isomorphic** if there is an isomorphism $f: A \to B$. Then there is also an isomorphism $f^{-1}: B \to A$. In this case we write $A \cong B$.

An **additive group** is an additive monoid with inverses, so it is an abelian group. We adopt the following conventions for additive groups:

1. We write a^{-1} as $-a$.
2. We write $a + -a'$ as $a - a'$.
3. We extend the notation na for $n \geq 0$ to $n \in \mathbf{Z}$ as follows: if $n < 0$, then $-n > 0$, and $na = -((-n)a)$. For example, if $n = -3$, then $na = -(3a) = -(a + a + a)$.
4. We write $S' + -s$ as $S' - s$. (Note the similarity to set difference notation. There is no ambiguity because s is an element, not a set.)

Fix an additive group A and a subset (not necessarily a subgroup) $S \subseteq A$. The subgroup B **generated by** S is the set of all finite sums $\sum_{i=1}^{n} s_i$ where $s_i \in S$ or $-s_i \in S$. It is minimal among the subgroups of A that contain S. We say that S **generates** B and that the members of S are **generators** of B. B is **finitely generated** if it is generated by a finite set S. In particular, A is finitely generated if it is generated by a finite set $S \subseteq A$.

Fix an additive group A.

1. Fix a subgroup B of A and an element $a \in A$. The set $B + a$ is called the **coset** of B with respect to a. An element $a' \in B + a$ is called a **representative** of the coset $B + a$.

   Consider two cosets $B + a$ and $B + a'$. If these cosets have an element in common, say $b + a = b' + a'$, then $a = b' - b + a'$ and $a' = b - b' + a$, i.e., $a \in B + a'$ and $a' \in B + a$. So $B + a$ and $B + a'$ are either identical or disjoint. In the first case, both $a - a'$ and $a' - a$ are elements of B, and we say that "the" difference of a and a' lies in B. (There are actually two differences, but either both lie in B or neither does.)

2. Fix a subgroup B of A. The **quotient group** or **factor group** A/B is the set of distinct cosets $B + a$, together with the following group law:

   i. The identity element of A/B is $B + 0 = B$.

   ii. For any elements a and a' in A, $(B + a) + (B + a') = B + (a + a')$.

   iii. For any element a in A, $-(B + a) = B - a$.

   Equivalently, A/B is the group obtained from A after identifying all pairs of elements whose difference lies in B. In particular, for any $b \in B$, $b - 0 = b$ lies in B, so b is identified with 0.

Fix a family $F = \{A_i\}_{i \in I}$ of groups. The **direct product** (respectively **direct sum**) of F as a group is the direct product (respectively direct sum) of F with respect to the group operations o_i of the family. It is a group.

6. Rings and Fields

A **ring** is an additive group A with a second operation o' (usually called **ring multiplication** or **multiplication**) that makes the non-zero elements of A into a multiplicative monoid and that distributes over addition. The multiplicative identity 1 and the additive identity 0 are distinct elements except in the case of the ring with the single element 0, called the **zero ring**. The definition of a ring implies the following facts:

1. For all $a \in A$, $a = 1a = (1 + 0)a = 1a + 0a = a + 0a$, so $0a = 0$.
2. For all a and a' in A, $0 = 0a = (a' + -a')a = a'a + (-a')a$, so $(-a')a = -(a'a)$.

The same facts hold with the multiplication reversed.

Fix a ring A. A set $S \subseteq A$ **generates** A if it generates A as an additive group. In this case we say that S is a set of **generators** for A. A is **finitely generated** if it is generated by a finite set S.

A **commutative ring** is a ring whose multiplication operation is commutative. The integers $\mathbf{Z}$ with addition and multiplication form a commutative ring.

The subject of commutative algebra is commutative rings. Therefore we will hereafter use the word "ring" as a shorthand for "commutative ring," unless otherwise specified.

Fix a ring A. The **characteristic** of A, written $\mathrm{char}(A)$, is a natural number defined as follows:

1. If there exists a natural number $n > 0$ such that the multiplicative identity 1 added to itself n times is zero, then $\mathrm{char}(A)$ is the smallest such n.
2. Otherwise $\mathrm{char}(A) = 0$.

A **subring** B of a ring A is a subset of A that is a ring with respect to the addition and multiplication of A.

Fix a ring A and an element $a \in A$.

1. a is a **zero divisor** if there exists $a' \in A$ such that $a' \neq 0$ and $aa' = 0$. 0 is a zero divisor. If $a \neq 0$, then a' is also a zero divisor.
2. a is **nilpotent** if there exists $n > 0$ such that $a^n = 0$.
3. a is a **unit** if it has an inverse with respect to multiplication.

An **integral domain** is a ring in which $1 \neq 0$ and there are no zero divisors other than 0. $\mathbf{Z}$ is an integral domain.

A **field** is a commutative ring in which $1 \neq 0$ and every non-zero element is a unit. Each of the rational numbers $\mathbf{Q}$, the real numbers $\mathbf{R}$, and the complex numbers $\mathbf{C}$ with addition and multiplication forms a field. Every field is an integral domain (proof omitted).

The **multiplicative group** of a field F, denoted F^*, is the abelian group whose elements are $F - \{0\}$ and whose group operation is multiplication in F.

Fix a ring A and an element a of A.

1. a **divides** an element b of A if there exists an element c of A such that $b = ac$.
2. a is **prime** if (a) it is not zero; (b) it is not a unit; and (c) for any elements b, c, and d of A, if $a = bc$ and d divides a, then d divides b or d divides c. For example, 2, 3, 5, and 7 are prime numbers in $\mathbf{Z}$.
3. a is **irreducible** if it is not a unit and it cannot be represented as the product of two non-units. For example, in $\mathbf{Z}$, the prime numbers are irreducible.

In an integral domain, every prime element is irreducible (proof omitted).

A ring A is a **unique factorization domain** or **UFD** if

1. Every element a of A that is not zero and not a unit may be written as a product $u\ b_1 \cdots b_n$ with u a unit and all b_i irreducible; and
2. The representation in item 1 is unique in the sense that if $a = u'\ b'_1 \cdots b'_m$ with u' a unit and all b'_i irreducible, then (a) $m = n$ and (b) there exists a bijection $\sigma\colon [1, n] \to [1, n]$ such that for all i in $[1, n]$, $b'_i = u_i b_{\sigma(i)}$, with u_i a unit.

$\mathbf{Z}$ is a unique factorization domain.

Every unique factorization domain is an integral domain (proof omitted). If A is a unique factorization domain, then an element a of A is irreducible if and only if it is prime (proof omitted). An integral domain A is a unique factorization domain if and only if every nonzero element a of A may be written as a product of a unit and prime elements of A (proof omitted).

An **ideal** of a ring A is an additive subgroup I of A that is closed under multiplication with respect to A. That is, for all $a \in A$, $aI \subseteq I$. In general an ideal I is not a ring (but it is a module; see § 7).

Fix a ring A and a subset $S \subseteq A$. The ideal **generated by** S is the additive subgroup generated by all elements as with $a \in A$ and $s \in S$. It is minimal among the ideals of A that contain S.

1. If $S = \{s_1, \ldots, s_n\}$ is a finite set, then we write $(s_1, \ldots, s_n)$ for the ideal generated by S.
2. In particular, we write (s) to denote the ideal generated by a single element s. This is called a **principal ideal**. The ideal (0) is the zero ring. The ideal (1) is A.

Fix a ring A and an ideal B of A. B is **irreducible** if for every intersection $B = C \cap D$, with C and D ideals of A, we have $C = B$ or $D = B$. For example, in $\mathbf{Z}$, the ideal (p), for p any prime number, is irreducible. The ideal (6) is not irreducible, since it is the intersection of the ideals (2) and (3).

A ring A is a **principal ideal domain** or **PID** if every ideal of A is principal. $\mathbf{Z}$ is a principal ideal domain.

Fix a ring A and an ideal B of A.

1. B is a **proper ideal** if $A \neq B$.
2. B is a **prime ideal** if B is a proper ideal and $A - B$ is closed under multiplication. Equivalently, B is a prime ideal if B is a proper ideal and for all a and a' in A such that $aa' \in B$, either $a \in B$ or $a' \in B$. If A is an integral domain, then a principal ideal (a) is prime if and only if $a = 0$ or a is a prime element of A (proof omitted).
3. B is a **maximal ideal** if B is a proper ideal and B is maximal among the proper ideals of A, considered as sets (§ 2). Every maximal ideal is prime (proof omitted).
4. The **quotient ring** or **residue class ring** A/B is the quotient group A/B together with the multiplication law $(B + a)(B + a') = B + aa'$. This law is well-defined, because for any $b, b' \in B$, we have

   $$(b + a)(b' + a') = bb' + ba' + ab' + aa' \in B + aa'.$$

   This law makes A/B into a ring. If B is a maximal ideal, then A/B is a field (proof omitted). In this case, A/B is called a **residue field**.

Fix a ring A.

1. The **nilradical** of A is the set of all nilpotent elements of A. It is an ideal of A (proof omitted) and is equal to the intersection of all prime ideals of A (proof omitted).
2. The **Jacobson radical** of A is the intersection of all the maximal ideals of A.

Every ring other than 0 has at least one maximal ideal (proof omitted).

Fix a ring A.

1. A is **local** if it has exactly one maximal ideal. The term "local" comes from algebraic geometry, where local rings describe the behavior near the points on an algebraic variety.
2. A is **semi-local** if it has a finite number of maximal ideals.

Fix rings A and B. A **ring homomorphism** from A to B is a map $f\colon A \to B$ that is a group homomorphism with respect to the addition operations of A and B and a monoid homomorphism with respect to the multiplication operations on the non-zero elements of A and of B.

A **ring isomorphism** is a ring homomorphism that is bijective. Two rings A and B are **isomorphic** if there is an isomorphism $f\colon A \to B$, and therefore there is an isomorphism $f^{-1}\colon B \to A$.

Fix rings A and B and a ring homomorphism $f\colon A \to B$.

1. The **image** of f, denoted im f, is the image $f(A)$ of f as a map. It is a subring of B.
2. The **kernel** of f, denoted ker f, is $f^{-1}(0)$, i.e., the inverse image of 0 under f as a map. It is an ideal of A.
3. The **coimage** of f, denoted coim f, is A/ker f. It is isomorphic to im f.
4. The **cokernel** of f, denoted coker f, is B/im f.

f is injective if and only if ker $f = 0$. f is surjective if and only if coker $f = 0$.

Fix a ring A, and let $X = \{x_i\}_{i \in I}$ be a family of elements. We define a ring A **adjoin** X, written $A[X]$. When X is a finite family of formal variables $\{x_1, \ldots, x_n\}$, $A[X]$ is called the **polynomial ring** over A in the variables x_i and is written $A[x_1, \ldots, x_n]$. $A[X]$ is defined as follows:

1. The elements of $A[X]$ are finite sums $\sum_{i=1}^{n} t_i$, for $n \geq 0$, where each term t_i is an element ap, where a is a member of A, and p is a finite product of zero or more elements in X with duplicates allowed. For example, in $\mathbf{Z}[x, y]$, valid terms include 3, xy, and $3xy$. By convention we use exponents to represent repeated instances of the same variable. For example, we can write $3x^2$ instead of $3xx$.
2. The element $0 \in A[X]$ is the empty sum. The element $1 \in A[X]$ is the sum consisting of the single element $1 \in A$. The ring operations are the familiar rules of polynomial arithmetic.
   a. Addition operates by removing parentheses:
   $$(\sum_{i=1}^{m} s_i) + (\sum_{j=1}^{n} t_j) = \sum_{i=1}^{m} s_i + \sum_{j=1}^{n} t_j.$$
   b. Multiplication operates by distributing over addition:
   $$(\sum_{i=1}^{m} s_i)(\sum_{j=1}^{n} t_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} s_i t_j.$$
3. Two elements of $A[X]$ are equal if one can be transformed into the other using operations that must hold in order for $A[X]$ to be a commutative ring. For example, $x_1 + x_2 x_3 = x_3 x_2 + x_1$, $0x_1 = 0$, $x_1 + x_1 = (1 + 1)x_1$, etc.
4. If A and the elements X are members of a ring B, then two elements of $A[X]$ are equal if the finite sums $\sum_{i=1}^{n} t_i$ are equal in B. For example, if a is a member of A, then $A[a] = A$, because any finite sum $\sum_{i=1}^{n} t_i$ can be simplified to a member of A.

Formally, the elements of $A[X]$ are the equivalence classes of the formal sums (1) under the equivalence relation (3) and (4) on the formal sums.

Fix a ring A and ideals B and C of A.

1. The **sum** of B and C, written $B + C$, is the set of all elements $b + c$ such that $b \in B$ and $c \in C$. The sum of two ideals is an ideal, so the sum provides a binary operation on the ideals of A. The operation is commutative and associative with identity (0), so it makes the set of ideals of A into an additive monoid.

2. The **product** of B and C, written BC, is the ideal generated by the elements bc with $b \in B$ and $c \in C$.[4] The product provides a binary operation on the ideals of A. The operation is commutative and associative with identity (1), so it makes the set of ideals of A into a multiplicative monoid. It distributes over the sum.
3. B and C are **coprime** or **relatively prime** if $B + C = (1)$. In $\mathbf{Z}$, (n) and (m) are coprime if and only if they have no common factors, other than the units 1 and -1. For example, (2) and (3) are coprime.
4. The **ideal quotient** $(B : C)$ is the set $\{a \in A \mid aC \subseteq B\}$. It is an ideal. If B or C is a principal ideal, then we may omit the extra parentheses. For example, we may write $(b : c)$ instead of $((b) : (c))$.

   The motivation for the name is as follows. If B and C are principal ideals, and c divides b, and $b/c = d$ (i.e., $b = dc$), then $(b : c) = (d)$.

Fix a ring A and an ideal C of A. The **annihilator** of C is the ideal $(0 : C)$. It is the set of elements $a \in A$ such that $aC = 0$.

Fix a ring A and a set $B \subseteq A$. The **radical** of B, written $\mathrm{rad}(B)$, is the set of all elements $a \in A$ such that $a^n \in B$ for some $n > 0$.

Fix a family $F = \{A_i\}_{i \in I}$ of rings. The **direct product** (respectively **direct sum**) of F as a ring is the direct product (respectively direct sum) of F as a family of additive groups, together with the multiplication operation that comes from the direct product of the multiplicative monoids of F as a family of multiplicative monoids. It is a ring. Note that in any element $\{a_i\}$ of a direct sum of rings, all but finitely of the elements a_i are zero.

Fix rings A and B and a ring homomorphism $f\colon A \to B$.

1. Let C be an ideal of A. The **extension** of C by f is the ideal in B generated by $f(C)$.
2. Let C be an ideal of B. The **contraction** of C by f is $f^{-1}(C)$, which is an ideal of A.

7. Modules

In this section, unless otherwise specified, A denotes a commutative ring.

Let B be an additive group.

1. An **endomorphism** of B is a homomorphism $f\colon B \to B$.
2. The **endomorphism ring** of B, written $\mathrm{end}(B)$, is the ring defined as follows:
   a. The set S is the set of endomorphisms of B.
   b. Addition is defined by $f + g = b \mapsto f(b) + g(b)$.
   c. The additive identity 0 is the map $b \mapsto 0$.
   d. Multiplication is defined by $fg = f \circ g$.
   e. The multiplicative identity 1 is the identity map.

   In general, $\mathrm{end}(B)$ is a non-commutative ring.

An A-**module** is an additive group B together with a ring homomorphism $f\colon A \to \mathrm{end}(B)$. f associates to each element $a \in A$ a map $f(a)\colon B \to B$. We write ab to mean $f(a)(b)$ and call this operation **multiplication by** A.

1. Because f is a homomorphism, we have $(a + a')b = ab + a'b$ and $(aa')b = a(a'b)$.
2. Because $f(a)$ is an endomorphism, we have $1b = b$ and $a(b + b') = ab + ab'$.
3. We adopt the same notation as for ring multiplication. For example, aC means the set of all ac such that $c \in C$.

The concept of an A-module generalizes the concept of an ideal (every ideal of A is an A-module). In particular, every ring A is an A-module, and every field F is an F-module.

Every additive group B is a $\mathbf{Z}$-module, where the rule for multiplying $n \in \mathbf{Z}$ by $b \in B$ is given by the rule for expanding nb in an additive group, i.e., $0b = 0$, $nb = \sum_{i=1}^{n} b$, and $(-n)b = -(nb)$, where $n > 0$ is a natural number. For the same reason, every ring and every A-module is a $\mathbf{Z}$-module.

[4] Some authors write BC to represent the set of *elements* bc, instead of the ideal generated by this set. In general the two definitions are not the same. For example, in the ring $\mathbf{Z}[x, y]$, the product $(x)(y)$ contains $x + y$ under the first definition but not under the second.

Unless otherwise specified, in the rest of this section, "module" means "A-module."

Fix a module B. A **submodule** C of B is a subset of C that is an A-module with respect to the addition and multiplication by A inherited from B. An ideal of A is a submodule of A, considered as an A-module.

A module B is **simple** if it has no submodules except itself and 0.

Fix a module B, and a subset $S \subseteq B$.

1. The submodule C **generated by** S is the module generated as an additive subgroup by all elements as with $a \in A$ and $s \in S$. It is minimal among the submodules of B that contain S. In this case we say that S generates C, and the members of S are **generators** for C.
2. B is **finitely generated** if it is generated by a finite set S.

Notice that an additive group (respectively ring) is finitely generated if and only if it is finitely generated as a $\mathbf{Z}$-module.

Fix a ring A and a subset $S \subseteq A$, The submodule of A (as an A-module) generated by S is equivalent to the ideal of A (as a ring) generated by S.

Fix a module B and a submodule C of B. The **quotient module** B/C is the quotient group B/C together with the multiplication law $a(C + b) = C + ab$. This law makes B/C into an A-module.

Fix A and modules B and C.

1. An A-**module homomorphism** from B to C is a map $f\colon B \to C$ that (a) is a group homomorphism with respect to the group structure of B and C and (b) satisfies the equation $f(ab) = a(f(b))$ for all $a \in A$ and $B \in B$. When the context is clear, we will write "homomorphism" instead of "A-module homomorphism."
   a. A map $f\colon B \to C$ is A-**linear** (or just linear) if it is an A-module homomorphism.
   b. A **module isomorphism** is a module homomorphism that is bijective. Two modules B and C are **isomporphic** if there is an isomorphism $f\colon B \to C$, and therefore there is an isomorphism $f^{-1}\colon C \to B$.
   c. The image, kernel, coimage, and cokernel of a module homomorphism are defined as for ring homomorphisms, replacing "ring" with "module."
2. The A-module $\mathrm{Hom}(B, C)$ is defined as follows:
   a. The set S is the set of A-module homomorphisms $f\colon B \to C$.
   b. Addition is defined by $f + g = b \mapsto f(b) + g(b)$.
   c. Multiplication by A is defined by $af = b \mapsto a(f(b))$.

   When we want to specify that $\mathrm{Hom}(B, C)$ is an A-module, we write $\mathrm{Hom}_A(B, C)$.

Fix modules B, B', C, and C'. Fix homomorphisms $f\colon B' \to B$ and $g\colon C \to C'$.

1. $\mathrm{Hom}(f, g)$ or $\mathrm{Hom}_A(f, g)$ is the homomorphism from $\mathrm{Hom}(B, C)$ to $\mathrm{Hom}(B', C')$ given by
$$h \mapsto g \circ h \circ f.$$
   Notice that Hom is **contravariant** in its first argument, because it reverses the positions of B and B'. We take up this idea further below, in the section on functors.
2. We write $\mathrm{Hom}(f, C)$ or $\mathrm{Hom}_A(f, C)$ in the case where $C' = C$ and $g\colon C \to C$ is the identity map. $\mathrm{Hom}(f, C)$ is the mapping $h \mapsto h \circ f$ that says, "Given a homomorphism h, construct a new homomorphism $\mathrm{Hom}(f, C)(h)$ by composing h with f on the right."
3. We write $\mathrm{Hom}(B, g)$ or $\mathrm{Hom}_A(B, g)$ in the case where $B' = B$ and $f\colon B \to B$ is the identity map. $\mathrm{Hom}(B, g)$ is the mapping $h \mapsto g \circ h$ that says, "Given a homomorphism h, construct a new homomorphism $\mathrm{Hom}(B, g)(h)$ by composing h with g on the left."

Many authors write f^* for $\mathrm{Hom}(f, C)$ and f_* for $\mathrm{Hom}(B, f)$.

Fix a module B, and fix submodules C and D of B.

1. Let $F = \{C_i\}_{i \in I}$ be a family of submodules of B. The sum $\sum_{i \in I} C_i$ is the submodule of B generated by $\bigcup_{i \in I} C_i$.
   It is the set of all finite sums $\sum_{j=1}^{n} c_j$ such that each c_j is a member of some C_i.

2. Let C be an ideal of A and D be a submodule of B. The product CD is the submodule of B generated by elements cd with $c \in C$ and $d \in D$.
3. Fix submodules C and D of B. The **quotient** $(C : D)$ is the set $\{\ a \in A \mid aD \subseteq C\ \}$. It is an ideal of A.
4. The **annihilator** of B, written $\operatorname{ann}(B)$, is the ideal $(0 : B)$ of A. It is the set of all $a \in A$ such that $aB = 0$.

A module B is **faithful** if $\operatorname{ann}(B) = 0$.

Fix a family $F = \{B_i\}_{i \in I}$ of modules. The **direct product** (respectively **direct sum**) of F as an A-module is the direct product (respectively direct sum) of F as a family of additive groups, together with the multiplication rule

$$a\{b_i\}_{i \in I} = \{ab_i\}_{i \in I}.$$

It is an A-module. As for rings, for any element $\{b_i\}$ of a direct sum of modules, all but finitely many of the elements b_i are 0.

A **free A-module** is an A-module that is isomorphic to the direct sum $\bigoplus_{i \in I} A$, for some index set I. I may be finite or infinite. Each element of the direct sum is a family of elements $\{a_i\}_{i \in I}$. If I is infinite, then all but finitely many of the elements a_i are 0.

Fix a family $F = \{B_i\}_{i \in I}$ of modules, and let $B = \bigtimes_{i \in I} B_i$.

1. Fix a module C and a map $f\colon B \to C$. f is map of sets, not of modules, because B is not a module.
   a. Fix an index $i \in I$. We say that f is A-**linear in index** i if for every stable injection map $g_i\colon B_i \to B$, $f \circ g_i\colon B_i \to C$ is an A-module homomorphism. In particular, when $I = \{1, 2\}$ and f is a map from $B_1 \times B_2$ to C, each stable injection map g_1 is of the form $b \mapsto (b, b_2)$, where $b_2 \in B_2$ is a constant that depends on g_1 but not b; and similarly for each stable injection map g_2.
   b. If f is A-linear in i for all $i \in I$, then we say that f is A-**multilinear**. In particular, when $I = \{1, 2\}$, we say that f is A-**bilinear**.
2. The **tensor product** of F, written $\bigotimes_{A\ i \in I} B_i$, is an A-module D with the following properties:
   a. There exists an A-multilinear map $h\colon B \to D$.
   b. For any module C and any A-multilinear map $f\colon B \to C$, there exists a unique module homomorphism $f'\colon D \to C$ such that $f = f' \circ h$. We say that f **factors through** h.

   Informally, the tensor product transforms (a) a Cartesian product of modules B into a module D and (b) an A-multilinear map $f\colon B \to C$ into an A-module homomorphism $f'\colon D \to C$. The tensor product exists and is unique up to unique isomorphism (proof omitted).
3. We may represent each element of the tensor product of F as a finite sum $\sum_{j=1}^{n} a_j t_j$, where $a_j \in A$, and t_j is a term of the form $\bigotimes_{A\ i \in I} b_{ij}$ with $b_{ij} \in B_i$. In the bilinear case, each element of the tensor product has the form $\sum_{j=1}^{n} a_j (b_j \otimes_A b'_j)$. Because of the multilinearity of h, many of these sums are equivalent. In particular:
   a. In the bilinear case,
   $$a(b_1 \otimes b_2) = ab_1 \otimes b_2 = b_1 \otimes ab_2.$$
   In general, $a \bigotimes_{A\ i \in I} b_i = \bigotimes_{A\ i \in I} b'_i$ if $b_i = b'_i$ for all $i \neq j$ and $ab_j = b'_j$.
   b. In the bilinear case,
   $$b_1 \otimes b_2 + b'_1 \otimes b_2 = (b_1 + b'_1) \otimes b_2$$
   $$b_1 \otimes b_2 + b_1 \otimes b'_2 = b_1 \otimes (b_2 + b'_2).$$
   In general, $\bigotimes_{A\ i \in I} b_i + \bigotimes_{A\ i \in I} b'_i = \bigotimes_{A\ i \in I} b''_i$ if $b_i = b'_i = b''_i$ for all $i \neq j$ and $b_j + b'_j = b''_j$.

   Because of observation (a), we may represent each element of the tensor product of F as $\sum_{j=1}^{n} t_j$, i.e., we may assume that $a_j = 1$ for all j. Remember: An element of $B_1 \otimes_A B_2$ is in general a *sum* of elements of the form

$b_1 \otimes_A b_2$, not (in general) a single element of the form $b_1 \otimes_A b_2$.

4. Where the ring A is clear from the context, we may omit the qualifiers A- and subscripts A in the notation.
5. Fix a family $\{C_i\}_{i \in I}$ of A-modules and a family of A-module homomorphisms $\{f_i \colon B_i \to C_i\}_{i \in I}$.
   a. $\bigotimes_{i \in I} f_i \colon \bigotimes_{i \in I} B_i \to \bigotimes_{i \in I} C_i$ is the homomorphism that takes $\sum_{j=1}^{n} t_j$ to $\sum_{j=1}^{n} f(t_j)$, where
   $$f(\bigotimes_{i \in I} b_{ij}) = \bigotimes_{i \in I} f(b_{ij}).$$
   For example, $(f_1 \otimes f_2)(b_1 \otimes b_2) = f_1(b_1) \otimes f_2(b_2)$.
   b. When $B_i = C_i$ and f_i is the identity map, we write B_i for f_i. For example,
   $$(f_1 \otimes B_2)(b_1 \otimes b_2) = f_1(b_1) \otimes b_2.$$

Fix rings A and B and a ring homomorphism $f \colon A \to B$.

1. Fix a B-module C. Make C into an A-module as follows: for all $a \in A$ and $c \in C$, $ac = f(a)c$. This operation is called **restriction of scalars**.
2. Fix an A-module C. B is a B-module because it is a ring. Make it into an A-module by restriction of scalars and construct the A-module $D = B \otimes_A C$. Now make D into a B-module according to the following multiplication rule:
   $$b \cdot \sum_{i=1}^{n} (b_i \otimes_A c_i) = \sum_{i=1}^{n} (bb_i \otimes_A c_i).$$
   This operation is called **extension of scalars**.

8. Vector Spaces

Where A is a field, an A-module is called a **vector space over** A or just a vector space, when the field A is understood.

Every vector space B is a free module. That is, $B = \bigoplus_{i \in I} A$, for some field A and some index set I (proof omitted). When I is a finite set of cardinality n, we denote this vector space A^n. The **dimension** of B is the cardinality of I. It is finite and equal to n for some natural number n, or it is infinite. If the dimension of B is infinite, then for each element $\{b_i\}$ of B, all but finitely many of the elements b_i are zero.

A **basis** for a vector space B is a minimal set of generators for B as an A-module.

1. If S is a basis for B, then (a) each element of B may be written as a finite sum $\sum_{i=1}^{n} a_i s_i$, where each $a_i \in A$ and each $s_i \in S$; and (b) S is minimal among sets with property (1) (i.e., property (a) is not true for any proper subset of S). An equivalent statement of property (a) is that B is equal to the the direct sum of vector spaces $\bigoplus_{s \in S} As$. An expression $\sum_{i=1}^{n} a_i s_i$ is called a **linear combination** of elements of S.
2. Every vector space B has a basis, and either all bases are infinite, or all bases are finite with the same size d (proof omitted). In the first case the dimension of B is infinite. In the second case the dimension is finite and equal to d.

Consider the operation of the direct sum and the tensor product on a pair of vector spaces A^m and A^n:

1. $A^m \oplus A^n = A^{m+n}$. This is clear from the definitions. For example, an element of $\mathbf{R}^2 \oplus \mathbf{R}^2$ is $((a, b), (c, d))$, which corresponds to the element (a, b, c, d) in $\mathbf{R}^4$.
2. $A^m \otimes A^n = A^{mn}$. Given bases B_1 for A^m and B_2 for A^n, a basis for $A^m \otimes A^n$ is the set of all $b_1 \otimes b_2$ such that $b_1 \in B_1$ and $b_2 \in B_2$.

These observations motivate the notation $\oplus$ and $\otimes$.

9. Algebras

Let A be a ring. An A-**algebra** is a ring B together with a ring homomorphism $f\colon A \to B$. By restriction of scalars (§ 7), f makes B into an A-module. Thus every A-algebra is a ring B that is also an a A-module, with multiplication by A given by $ab = f(a)b$. Every ring A is an A-algebra, with f equal to the identity map on A. Every ring A is also a $\mathbf{Z}$-algebra, with $f = n \mapsto n1$. (Recall that $n1$ denotes 0 if $n = 0$, $\sum_{i=1}^{n} 1$ if $n > 0$, and $-((-n)1) = -\sum_{i=1}^{n} 1$ if $n < 0$.) The polynomial ring $P = A[x_1, \ldots, x_n]$ is an A-algebra, with f equal to the identity map on A as a subset of P.

Fix a ring A, and let (B, f) and (C, g) be A-algebras. An A-**algebra homomorphism** $h\colon B \to C$ is a ring homomorphism that is also an A-module homomorphism. h is an A-algebra homomorphism if and only if $h \circ f = g$ (proof omitted).

Fix an A-algebra (B, f).

1. B is **finitely generated** if there exists a set $X = \{x_1, \ldots, x_n\}$ with $X \cap A = \varnothing$ and a surjective A-algebra homomorphism $g\colon A[X] \to B$. We may represent any element of B by any of the polynomials in $g^{-1}(b) \subseteq A[X]$. Equivalently, there exists a set $\{b_i\} \subseteq B$ such that we may represent any element $b \in B$ as a sum of terms, each of which is an element of A times a nonnegative power of one of the b_i. In this case we say that the ring homomorphism f is of **finite type**.
2. B is **finite** if it is finitely generated as an A-module. Equivalently, there exists a set $\{b_i\} \subseteq B$ such that we may represent any element of B as a sum of terms, each of which is an element of A times one of the b_i. (Unfortunately, this terminology is misleading, since it suggests that the set of elements of B is finite, which is not in general true. Remember: a finite algebra is not in general a finite set.) In this case we say that the ring homomorphism f is **finite**.

Some authors say that B is **ring finite** in case 1 and **module finite** in case 2.

Fix a ring A, and let (B, f) and (C, g) be A-algebras. Use the A-module structure of B and of C to form the tensor product $D = B \otimes_A C$. D is an A-module. Now define a multiplication on D as follows:

$$\sum_{i=1}^{n}(b_i \otimes c_i) \cdot \sum_{j=1}^{m}(b'_i \otimes c'_i) = \sum_{i=1}^{n}\sum_{j=1}^{m}(b_i b'_j \otimes c_i c'_j).$$

This operation makes D into a commutative ring with identity $1 \otimes 1$ (proof omitted). The map $a \mapsto f(a) \otimes g(a)$ is a ring homomorphism $A \to D$, so D is an A-algebra. Thus the tensor product $\otimes_A$ is a binary operation on A-algebras.

10. Direct and Inverse Limits of Modules

Recall that a **directed set** is a nonempty partially ordered set S in which every pair of elements of S has an upper bound (§ 2).

Fix a directed set I, a ring A, and a family $F = \{B_i\}_{i \in I}$ of A-modules.

1. F is a **direct system of modules** over I (direct system for short) if there exist homomorphisms $f_{ij}\colon B_i \to B_j$ for all $i \le j$ such that
   a. For all $i \in I$, f_{ii} is the identity map on B_i.
   b. For all $i \le j \le k$, $f_{ik} = f_{jk} \circ f_{ij}$.
2. F is an **inverse system of modules** over I (inverse system for short) if there exist homomorphisms $f_{ij}\colon B_j \to B_i$ for all $i \le j$ such that
   a. For all $i \in I$, f_{ii} is the identity map on B_i.
   b. For all $i \le j \le k$, $f_{ik} = f_{ij} \circ f_{jk}$.

Fix a direct system S. The **direct limit** of S, written $\varinjlim B_i$, is the disjoint union of the modules B_i, subject to the equivalence relation $(b, i) \sim (f_{ij}(b), j)$ for all $i \le j$ and all $b \in B_i$. In particular, if $b \in B_i$ and $b' \in B_j$, then $(b, i) \sim (b', j)$ if and only if there exists k with $i \le k$ and $j \le k$ such that $f_{ik}(b) = f_{jk}(b')$. The direct limit is an A-module with the following operations:

a. Fix $a \in A$, $i \in I$, and $b \in B_i$. Then $a(b, i) = (ab, i)$.

b. Fix i and j, $b \in B_i$, and $b' \in B_j$. Pick k such that $i \le k$ and $j \le k$. Then $(b, i) \cdot (b', j) = (f_{ik}(b) \cdot f_{jk}(b), k)$ and $(b, i) + (b', j) = (f_{ik}(b) + f_{jk}(b), k)$.

Fix an inverse system S. The **inverse limit** of S, written $\varprojlim B_i$, consists of all elements $\{b_i\}_{i \in I}$ of the direct product $\prod_{i \in I} B_i$ such that for all $i \le j$, $b_i = f_{ij}(b_j)$. The inverse limit is a submodule of the direct product.

In § 24, we will give a concrete example of an inverse limit.

11. Module Sequences

An A-**module sequence** consists of a ring A, a sequence $\{B_i\}_{i \in I}$ of A-modules, where I is a consecutive subset of $\mathbf{Z}$, and one of the following:

1. A sequence of A-module homomorphisms $\{f_i \colon B_i \to B_{i+1}\}_{i \in J}$, where $J = \{i \in I \mid i + 1 \in I\}$. In this case, we say the module sequence is **ascending**.
2. A sequence of A-module homomorphisms $\{f_i \colon B_i \to B_{i-1}\}_{i \in J}$, where $J = \{i \in I \mid i - 1 \in I\}$. In this case, we say the module sequence is **descending**.

Note that an A-module sequence may be a $\mathbf{Z}$-module sequence, i.e., a sequence of abelian groups. When there is no ambiguity, we write "module sequence" or "sequence" instead of "A-module sequence."

Common choices for I are $\mathbf{Z}$ and $\{0, \dots, n\}$. When $I = \mathbf{Z}$, we write an ascending sequence as follows:

$$\cdots \xrightarrow{f^{-2}} B^{-1} \xrightarrow{f^{-1}} B^0 \xrightarrow{f^0} B^1 \xrightarrow{f^1} \cdots$$

We write a descending sequence as follows:

$$\cdots \xleftarrow{f_{-1}} B_{-1} \xleftarrow{f_0} B_0 \xleftarrow{f_1} B_1 \xleftarrow{f_2} \cdots$$

When $I = \{0, \dots, n\}$, we write an ascending sequence as follows:

$$B^0 \xrightarrow{f^0} \cdots \xrightarrow{f^{n-1}} B^n$$

We write a descending sequence as follows:

$$B_0 \xleftarrow{f_1} \cdots \xleftarrow{f_n} B_n$$

Sometimes we write a descending sequence with the arrows going left to right, e.g.,

$$\cdots \xrightarrow{f^2} B^1 \xrightarrow{f^1} B^0 \xrightarrow{f^0} B^{-1} \xrightarrow{f^{-1}} \cdots$$

We also write sequences S with no explicit indices, e.g.,

$$A \xrightarrow{f} B \xrightarrow{g} C$$

In this case, it doesn't matter whether S is ascending or descending; we can make S into either one by appropriately numbering the modules and homomorphisms.

We adopt the following conventions, for any module B:

1. The map $0 \to B$ is the identity map on 0 as a subset of B.
2. The map $B \to 0$ is the map $b \mapsto 0$.

Fix an A-module sequence S.

1. S is **exact at** i if (a) S is ascending and $\operatorname{im} f^{i-1} = \ker f^i$; or (b) S is descending and $\operatorname{im} f_{i+1} = \ker f_i$.
2. S is **exact** if it is exact at all $i \in J$.

When an A-module sequence is exact, we say it is an **exact sequence**.

A **left exact sequence** is an exact sequence of the form

$$0 \to B \xrightarrow{f} C \to D$$

Because of the exactness, f is injective (its kernel is the image of the left-hand arrow, which is 0).

A **right exact sequence** is an exact sequence of the form

$$B \to C \xrightarrow{f} D \to 0$$

Because of the exactness, f is surjective (its image is the kernel of the right-hand arrow, which is all of D).

For any modules B and C and homomorphism $f\colon B \to C$, we can write the the following exact sequence S:

$$0 \to \ker f \xrightarrow{g} B \xrightarrow{f} C \xrightarrow{h} \operatorname{coker} f \to 0$$

where g is the identity map on $\ker f$ as a subset of B, and h is the map taking each element c to its coset in $C/\operatorname{im} f$. Let S' be the exact sequence formed by deleting $0 \to$ and $\to 0$ from S. Then f is injective if and only if S' is left exact (i.e., $\ker f = 0$), and it is surjective if and only if S' is right exact (i.e., $\operatorname{coker} f = 0$).

Let S_1 and S_2 be module sequences. S_2 is the **dual sequence** of S_1 (and vice versa) if the modules and homomorphisms of S_1 and S_2 may be put in one-to-one correspondence, with each arrow reversed. Each left exact sequence has a dual right exact sequence. Each ascending sequence has a dual descending sequence (but notice that the numbering of the homomorphisms must be shifted by one).

A **short exact sequence** is an exact sequence of the form

$$0 \to B \xrightarrow{f} C \xrightarrow{g} D \to 0$$

Because of the exactness, f is injective and g is surjective.

A **split exact sequence** is a short exact sequence of the form

$$0 \to B \xrightarrow{f} B \oplus D \xrightarrow{g} D \to 0$$

where f is the injection map $b \mapsto (b, 0)$, and g is the projection map $(b, d) \mapsto d$.

1. Every split exact sequence has a dual sequence

   $$0 \to D \xrightarrow{g'} B \oplus D \xrightarrow{f'} B \to 0$$

   where $g' = d \mapsto (0, d)$ and $f' = (b, d) \mapsto b$.

2. Fix a short exact sequence S given by $0 \to B \xrightarrow{f} C \xrightarrow{g} D \to 0$. The following conditions are equivalent (proof omitted):
   a. S is a split exact sequence (that is, $C \cong B \oplus D$). In this case, we say that the sequence **splits**.
   b. There exists a homomorphism $f'\colon C \to B$ such that $f' \circ f\colon B \to B$ is the identity map.
   c. There exists a homomorphism $g'\colon D \to C$ such that $g \circ g'\colon D \to D$ is the identity map.

Fix a ring A and an A-module B.

1. B is **projective** if any of the following conditions holds:
   a. For every exact sequence $C \xrightarrow{f} D \to 0$ and every A-module sequence $B \xrightarrow{g} D$, there exists an A-module sequence $B \xrightarrow{h} C$ such that $g = f \circ h$.
   b. There exists an A-module C such that $D = B \oplus C$ is free. In this case, B, C, and D are all projective (proof omitted).
   c. Every short exact sequence of A-modules $0 \to C \to D \to B \to 0$ is a split exact sequence.

   Conditions a through c are equivalent (each one implies the other two) (proof omitted).
2. B is **injective** if any of the following conditions holds:
   a. For every exact sequence $0 \to C \xrightarrow{f} D$ and every A-module sequence $C \xrightarrow{g} B$, there exists an A-module sequence $D \xrightarrow{h} B$ such that $g = f \circ h$.

b. If B is a submodule of an A-module D, then there exists an A-submodule C of D such that $D \cong B \oplus C$.

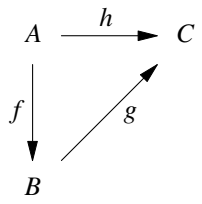
c. Every short exact sequence of A-modules $0 \to B \to C \to D \to 0$ is a split exact sequence.

Conditions a through c are equivalent (proof omitted).

12. Diagrams

A **diagram of modules** is a collection of modules and homomorphisms between the modules, in which the homomorphisms are represented as arrows between the modules, possibly with labels. For example:

1. Every module sequence (§ 11) is a diagram of modules.
2. The following diagram shows modules A, B, and C and homomorphisms $f: A \to B$, $g: B \to C$, and $h: A \to C$.



In this document, we will refer to a diagram of modules as a **diagram**. In category theory, the concept of a diagram is more general.

Let D be a diagram. We say that D is **commutative** (or **commutes**) if every composition of arrows with the same endpoints represents the same map. For example, the diagram above commutes if $h = g \circ f$.

13. Functors of Modules

For any ring A, let M_A denote the class (§ 2) of all A-modules, and let H_A denote the class of all homomorphisms between modules in M_A.[5]

Fix rings A and A'. A **functor of modules** between M_A and $M_{A'}$ is a pair of maps $F: M_A \to M_{A'}$ and $F: H_A \to H_{A'}$ such that

1. For all modules B in M_A, if f is the identity map on B, then $F(f)$ is the identity map on $F(B)$.
2. One of the following conditions holds:
   a. The functor is **covariant**:
      i. For all sequences $B \xrightarrow{f} C$ in M_A, there is a corresponding sequence $F(B) \xrightarrow{F(f)} F(C)$ in $M_{A'}$.
      ii. For all sequences $B \xrightarrow{f} C \xrightarrow{g} D$ in M_A, $F(g \circ f) = F(g) \circ F(f)$.
   b. The functor is **contravariant**:
      i. For all sequences $B \xrightarrow{f} C$ in M_A, there is a corresponding sequence $F(C) \xrightarrow{F(f)} F(B)$ in $M_{A'}$.
      ii. For all sequences $B \xrightarrow{f} C \xrightarrow{g} D$ in M_A, $F(g \circ f) = F(f) \circ F(g)$.

   Covariant functors preserve the directions of the arrows, and contravariant functors reverse the directions.

We will write a functor of modules as $F: M_A \to M_{A'}$, with the map $F: H_A \to H_{A'}$ implied. In this document, we will refer to a functor of modules as a **functor**. In category theory, the concept of a functor is more general.

We associate functors with Hom and $\otimes$ as follows:

1. Fix a module C. The functor $\mathrm{Hom}(-, C)$ defined by the maps $B \mapsto \mathrm{Hom}(B, C)$ and $f \mapsto \mathrm{Hom}(f, C)$ is contravariant because it maps $f: B' \to B$ to $g \mapsto g \circ f: \mathrm{Hom}(B, C) \to \mathrm{Hom}(B', C)$.

[5] An alternative approach used in category theory is to restrict all A-modules to be "small" sets, i.e., sets that are members of some universe set U. In this approach M_A and H_A are sets instead of classes. See [Mac Lane 1998], pp. 21–24.

2. Fix a module B. The functor $\mathrm{Hom}(B,-)$ defined by the maps $C \mapsto \mathrm{Hom}(B,C)$ and $f \mapsto \mathrm{Hom}(B,f)$ is covariant because it maps $f\colon C \to C'$ to $g \mapsto f \circ g\colon \mathrm{Hom}(B,C) \to \mathrm{Hom}(B,C')$.
3. Fix a module C. The functor $- \otimes C$ defined by the maps $B \mapsto B \otimes C$ and $f \mapsto f \otimes C$ is covariant because it maps $f\colon B \to B'$ to $f \otimes C\colon B \otimes C \to B' \otimes C$.
4. The definition of the tensor product is symmetric in its indices. Therefore we can fix a module B and write the covariant functor $B \otimes -$.

Let S be the sequence $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$.

1. A covariant functor F takes S to the sequence $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \xrightarrow{F(h)} F(D)$. A covariant functor is **left exact** if it takes a left exact sequence to a left exact sequence, **right exact** if it takes a right exact sequence to a right exact sequence, and **exact** if it takes an exact sequence to an exact sequence.
2. A contravariant functor F takes S to the sequence $F(D) \xrightarrow{F(h)} F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A)$. A contravariant functor is **left exact** if it takes a left exact sequence to a right exact sequence, **right exact** if it takes a right exact sequence to a left exact sequence, and **exact** if it takes an exact sequence to an exact sequence.

The functors associated with Hom and the tensor product have the following exactness properties (proofs omitted):

1. For any module B, $\mathrm{Hom}(B,-)$ is left exact. B is projective if and only if $\mathrm{Hom}(B,-)$ is exact (proof omitted).
2. For any module C, $\mathrm{Hom}(-,C)$ is right exact. C is injective if and only if $\mathrm{Hom}(-,C)$ is exact (proof omitted).
3. For any module B, $B \otimes -$ is right exact.

A module B is **flat** if the functor $B \otimes -$ is exact.

Fix rings A and A'. Let $F\colon M_A \to M_{A'}$ and $F'\colon M_A \to M_{A'}$ be covariant functors. A **natural transformation** $\eta\colon F \to F'$ is a class-indexed family (§ 2) of homomorphisms $\{\eta_B\colon F(B) \to F'(B)\}_{B \in M_A}$ such that for each sequence $B \xrightarrow{f} C$ of modules in M_A, the following diagram commutes:

$$\begin{array}{ccc} F(B) & \xrightarrow{\eta_B} & F'(B) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle F'(f)} \\ F(C) & \xrightarrow[\eta_C]{} & F'(C) \end{array}$$

A natural transformation of contravariant functors has the same definition with the vertical arrows reversed. For each $B \in M_A$, the homomorphism η_B is called the **component** of η associated with B. If each η_B is an isomorphism of modules, then we say that η is a **natural isomorphism** of functors.

Fix rings A_L and A_R. Let $L\colon M_{A_L} \to M_{A_R}$ and $R\colon M_{A_R} \to M_{A_L}$ be functors. L and R are **adjoint functors**, and L is the **left adjoint**, and R is the **right adjoint**, if for each $(B_L, B_R) \in M_{A_L} \times M_{A_R}$ there is a bijection of sets

$$\phi(B_L, B_R)\colon \mathrm{Hom}(L(B_L), B_R) \to \mathrm{Hom}(B_L, R(B_R))$$

such that for all $(B'_L, B'_R) \in M_{A_L} \times M_{A_R}$ and for all $(f_L, f_R) \in \mathrm{Hom}(B'_L, B_L) \times \mathrm{Hom}(B_R, B'_R)$, the following diagrams commute:

$$\begin{array}{ccc} \mathrm{Hom}(L(B_L), B_R) & \xrightarrow{\phi(B_L, B_R)} & \mathrm{Hom}(B_L, R(B_R)) \\ {\scriptstyle \mathrm{Hom}(L(B_L), f_R)}\downarrow & & \downarrow{\scriptstyle \mathrm{Hom}(B_L, R(f_R))} \\ \mathrm{Hom}(L(B_L), B'_R) & \xrightarrow[\phi(B_L, B'_R)]{} & \mathrm{Hom}(B_L, R(B'_R)) \end{array}$$

$$\begin{array}{ccc} \mathrm{Hom}(L(B_L), B_R) & \xrightarrow{\phi(B_L, B_R)} & \mathrm{Hom}(B_L, R(B_R)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(L(B'_L), B_R) & \xrightarrow[\phi(B'_L, B_R)]{} & \mathrm{Hom}(B'_L, R(B_R)) \end{array}$$

Equivalently, for all $f \in \mathrm{Hom}(L(B_L), B_R)$,

$$\phi(B_L, B'_R)(f_R \circ f) = R(f_R) \circ \phi(B_L, B_R)(f)$$

$$\phi(B'_L, B_R)(f \circ L(f_L)) = \phi(B_L, B_R)(f) \circ f_L$$

For any A-module C, let $L = - \otimes_A C$ and $R = \mathrm{Hom}_A(C, -)$. Then L and R are adjoint functors (proof omitted). For example, let B, C, and D be A-modules, and let f be an element of $\mathrm{Hom}(B \otimes C, D)$. Then

$$R(f) = \mathrm{Hom}(C, f)\colon \mathrm{Hom}(C, B \otimes C) \to \mathrm{Hom}(C, D) = g \mapsto f \circ g.$$

Let

$$\eta\colon B \to \mathrm{Hom}(C, B \otimes C) = b \mapsto (c \mapsto b \otimes c).$$

Then $\mathrm{Hom}(C, f) \circ \eta$ is an element of $\mathrm{Hom}(B, \mathrm{Hom}(C, D))$, and

$$\phi(B, D)(f) = R(f) \circ \eta = b \mapsto (c \mapsto f(b \otimes c))),$$

where $\phi(B, D)\colon \mathrm{Hom}(B \otimes C, D) \to \mathrm{Hom}(B, \mathrm{Hom}(C, D))$ is the bijection associated with the adjoint functors. η is called the **unit** associated with the adjoint functors. It is the map that, when composed with $R(f)$, yields $\phi(f)$. A similar calculation in the other direction, applying $- \otimes C$ to an element of $\mathrm{Hom}(B, \mathrm{Hom}(C, D))$, yields the **counit**.

14. Fractions and Localization

Fix an integral domain A. The **field of fractions** of A is a field F with the following properties:

1. There is an injective ring homomorphism $f\colon A \to F$
2. F is minimal among fields with property (1).

The field of fractions F of A exists and is unique up to isomorphism (proof omitted). We may represent F in the following way:

1. The elements of F are fractions a/b, where $a \in A$, $b \in A - \{0\}$, and a/b is equivalent to c/d if and only if $ad - bc = 0$. This is the usual rule for canceling common factors from the numerator and denominator of a fraction. For example, if $A = \mathbf{Z}$, then 1/2 is equivalent to 2/4 because $1 \cdot 4 - 2 \cdot 2 = 0$.
2. Addition is given by $a/b + c/d = (ad + cb)/bd$. This is the usual rule for adding fractions. For example, $1/2 + 1/3 = (3 + 2)/6 = 5/6$.
3. Multiplication is given by $a/b \cdot c/d = ac/bd$. This is the usual rule for multiplying fractions. For example, $1/2 \cdot 2/3 = 2/6 = 1/3$.

The field of fractions of the integers $\mathbf{Z}$ is the field of rational numbers $\mathbf{Q}$.

We generalize the field of fractions of A as follows. Let A be a general ring (not necessarily an integral domain). Let $S \subseteq A$ be a multiplicative monoid (i.e., S contains 1 and is closed under the multiplication of A). Informally, the **ring of fractions** of A with respect to S, written $S^{-1}A$, extends A so that the elements in S are units (i.e., have inverses). Formally, $S^{-1}A$ is a ring with the following properties:

1. There is a ring homomorphism $f\colon A \to S^{-1}A$. f is not necessarily an injection.
2. For all $s \in S$, $f(s)$ is a unit in $S^{-1}A$.
3. If $g\colon A \to B$ is a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$, then there exists a unique ring homomorphism $h\colon S^{-1}A \to B$ such that $g = h \circ f$.

$S^{-1}A$ exists and is unique up to unique isomorphism, given A and S (proof omitted). We may represent $S^{-1}A$ as follows:

1. The elements of $S^{-1}A$ are fractions a/s, where $a \in A$, $s \in S$, and a/s is equivalent to a'/s' if and only if there exists $s'' \in S$ such that $(as' - a's)s'' = 0$. This rule ensures that equivalence is transitive. It is similar to the rule for canceling common factors in the field of fractions of an integral domain, but it accounts for the fact that we may have $(as' - a's)s'' = 0$ with both $as' - a's \neq 0$ and $s'' \neq 0$.
2. Addition and multiplication are as for the field of fractions.
3. The ring homomorphism f is $a \mapsto a/1$.

Fix a ring A and a prime ideal P of A. By definition, $A - P$ is multiplicatvely closed. Write A_P to denote the ring $S^{-1}A$, with $S = A - P$. The elements a/s with $a \in P$ form a maximal ideal M of A_P, and M is the only maximal ideal of A_P (proof omitted). Therefore A_P is a local ring. The process of passing from A to A_P is called **localization** at the prime ideal P. Localization at a prime ideal is a fundamental operation in algebraic geometry.

Fix a ring A. A **local property** of A is a property that holds for A if and only if it holds for each ring A_P, where P is a prime ideal of A.

We generalize the ring of fractions $S^{-1}A$ as follows. Let B be an A-module. As before, let $S \subseteq A$ be a multiplicative monoid. Construct the $S^{-1}A$-module $S^{-1}B$ as follows:

1. The elements of $S^{-1}B$ are fractions b/s, where $b \in B$, $s \in S$, and b/s is equivalent to b'/s' if and only if there exists $s'' \in S$ such that $(bs' - b's)s'' = 0$. This rule is similar to the equivalence rule for $S^{-1}A$, but it uses module multiplication instead of ring multiplication.
2. Addition and module multiplication are as for the field of fractions, using module multiplication instead of ring multiplication. That is, $b/s + b'/s' = (bs' + b's)/ss'$, and $a/s \cdot b/s' = ab/ss'$.

Fix a ring A and an A-module B. A **local property** of B is a property that holds for B if and only if it holds for each module B_P, where P is a prime ideal of A.

Fix a ring A, an A-module B, and a prime ideal P of A. We write B_P to denote $S^{-1}B$, with $S = A - P$. In particular, if I is an ideal of A, we can write I_P, because I is an A-module.

Fix an A-module homomorphism $f: B \to C$. Define the $S^{-1}A$-module homomorphism $S^{-1}f: S^{-1}B \to S^{-1}C$ by $b/s \mapsto f(b)/s$. The operation $S^{-1} -$ that takes B to $S^{-1}B$ and f to $S^{-1}f$ is an exact functor (proof omitted).

15. Polynomials

In this section, A denotes a ring.

A **polynomial** in variables $x_1, \ldots, x_n$ over A is a member of the polynomial ring $A[x_1, \ldots, x_n]$ defined in § 6. Every polynomial $p(x_1, \ldots, x_n)$ defines a map $p: A^n \to A$ given by $(a_1, \ldots, a_n) \mapsto p(a_1, \ldots, a_n)$, where $p(a_1, \ldots, a_n) \in A$ denotes $p(x_1, \ldots, x_n)$ after substituting a_i for x_i at each index i and simplifying.

Every polynomial in one variable x over A may be written uniquely in the form $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, for some $n \geq 0$ and all $a_i \in A$.

1. The **coefficients** of a polynomial p are the values a_i. The value a_n is the **leading coefficient** of the polynomial. If the leading coefficient is 1, then we say that the polynomial is **monic**.
2. The natural number n is called the **degree** of the polynomial.
3. A nonzero polynomial p is **reducible** if it can be expressed as the product of two polynomials p_1 and p_2, each of degree greater than zero. A nonzero polynomial that is not reducible is **irreducible**.
4. A **root** of a polynomial $p(x)$ is an element $a \in A$ such that $p(a) = 0$.

If A is an integral domain, then $A[x_1, \ldots, x_n]$ is an integral domain (proof omitted). In particular, if A is a field, then $A[x_1, \ldots, x_n]$ is an integral domain, and we may construct its field of fractions (§ 14). This field of fractions is denoted $A(x_1, \ldots, x_n)$.

Fix a ring B and a subring A of B. Let $b_1, \ldots, b_n$ be elements of B. The ring $A[b_1, \ldots, b_n]$ is a subring of B. It consists of all elements $b \in B$ such that $b = p(b_1, \ldots b_n)$ for some polynomial $p \in A[x_1, \ldots, x_n]$, taken as a member of $B[x_1, \ldots, x_n]$. As an example, let $\rho \in \mathbf{R}$ be the cube root of 2, i.e., the unique real number such that $\rho^3 = 2$. Then $\mathbf{Q}[\rho]$ is a subring of $\mathbf{R}$. It consists of elements of the form $a + b\rho + c\rho^2$, where a, b, and c are rational numbers.

Let $p = \sum_{i=1}^{m} t_i$ be a polynomial in n variables, where the terms t_i are as defined in § 6.

1. The **degree** of the term t_i is the number of variables appearing in t_i, counting duplicates with multiplicity. For example, the term $2x^2y$ has degree 3, the term $5x$ has degree one, and the term 5 has degree zero.
2. p is **homogeneous** of degree d if all terms t_i have the same degree d. For example, $3x^2 + 2xy$ is homogeneous of degree 2.

For any $d \geq 0$, the homogeneous polynomials of degree d form a submodule of $A[X]$, considered as an A-module.

16. Formal Power Series

In this section, A denotes a ring.

A **formal power series** over A is an expression of the form $\sum_{i \in \mathbf{N}} a_i x^i$ or $\sum_{i=0}^{\infty} a_i x^i$, where x is an element not in A, the coefficients a_i are in A, and the sum represents the "formal summation" (not actual addition) of the infinitely many terms $a_i x^i$ as i ranges over $\mathbf{N}$. A formal power series is therefore just an alternate notation for a sequence $\{a_i\}_{i \in \mathbf{N}}$ — the terms x^i are placeholders for the coefficients. However, the analogy to ordinary summation is useful. For example, as discussed below, we can place a ring structure on formal power series that is similar to the structure of the polynomial ring in one variable. In analysis, formal power series may be interpreted as **power series**, which are limits of sequences of polynomial functions.

Let $A[[x]]$ denote the set of all formal power series over A. We make $A[[x]]$ into a ring as follows:

1. The zero element of $A[[x]]$ is the formal power series in which $a_i = 0$ for all i.
2. Addition in $A[[x]]$ is given by the rule $\sum_{i \in \mathbf{N}} a_i x^i + \sum_{i \in \mathbf{N}} b_i x^i = \sum_{i \in \mathbf{N}} (a_i + b_i) x^i$.
3. The element 1 in $A[[x]]$ is the formal power series in which $a_0 = 1$ and $a_i = 0$ for $i > 0$.
4. Multiplication in $A[[x]]$ is given by the rule $(\sum_{i \in \mathbf{N}} a_i x^i)(\sum_{i \in \mathbf{N}} b_i x^i) = \sum_{i \in \mathbf{N}} c_i x^i$, where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$. That is, term i of the product is the (finite) sum of all terms of degree i obtained by multiplying a term of the first formal power series by a term of the second formal power series. This product is called the **Cauchy product**.

The units (invertible elements) of $A[[x]]$ are the formal power series for which a_0 is a unit in A. Let $P(x) = \sum_{i \in \mathbf{N}} a_i x^i$ be such a series. Then $P(x)^{-1} = \sum_{i \in \mathbf{N}} b_i x^i$, where

- $b_0 = a_0^{-1}$.
- $b_i = -a_0^{-1} \sum_{j=1}^{i} a_j b_{i-j}$, for $i \geq 1$.

It is straightforward to check that $P(x) \cdot P(x)^{-1} = 1$.

For example, let $P(x) = 1 - x$ be the formal power series with $a_0 = 1$, $a_1 = -1$, and $a_i = 0$ for $i > 1$. Let

$$Q(x) = \sum_{i \in \mathbf{N}} x^i = 1 + x + x^2 + \cdots.$$

Then $Q(x) = P(x)^{-1}$ (and vice versa). Indeed, taking the Cauchy product $P(x)Q(x)$, we see that $a_0 = 1$ and $a_i = x^i - x^i = 0$ for all $i > 0$.

The formal power series ring $A[[x]]$ is an A-algebra.

There is an injective homomorphism $f\colon A[x] \to A[[x]]$. Given an element $p(x) \in A[x]$ with coefficients $a_0, \ldots, a_n$, $f(p(x))$ is the formal power series whose first $n+1$ coefficients are the a_i and whose other coefficients are all zero. Thus $f(A[x])$ is an isomorphic copy of $A[x]$ contained in $A[[x]]$. By abuse of language, we say that an element of $f(A[x])$ (i.e., a formal power series with finitely many nonzero coefficients) is a polynomial. f makes $A[[x]]$ into an $A[x]$-algebra.

Let $P(x)$ be a formal power series in $A[[x]]$. If $P(x) = p(x)q(x)^{-1}$, where $p(x)$ and $q(x)$ are polynomials in $A[[x]]$ and $q(x)$ is invertible in $A[[x]]$, then we say that $P(x)$ is a **rational function**, and we write

$$P(x) = \frac{p(x)}{q(x)}.$$

Note that p and q have finitely many terms, while in general q^{-1} and P have infinitely many terms. For example,

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots.$$

The rational functions form a subring of $A[[x]]$, with

$$\frac{p_1(x)}{q_1(x)} + \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)q_2(x) + p_2(x)q_1(x)}{q_1(x)q_2(x)}.$$

and

$$\frac{p_1(x)}{q_1(x)} \cdot \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)p_2(x)}{q_1(x)q_2(x)}$$

This subring is a $A[x]$-algebra.

Let S denote the set of sequences $\{a_i\}_{i \in \mathbf{N}}$ of elements in A. Fix an element $s \in S$. A **generating function** for s in the variable x is the image $f(s)$ of a map $f\colon S \to A[[x]]$.

1. The **ordinary generating function** $G(a_i; x)$ is the image of the map $\{a_i\} \mapsto \sum_{i \in \mathbf{N}} a_i x^i$.
2. When A includes the rational numbers $\mathbf{Q}$, the **exponential generating function** $EG(a_i; x)$ is the image of the map $\{a_i\} \mapsto \sum_{i \in \mathbf{N}} a_i \frac{x^i}{i!}$.
3. There are several other standard generating functions $f(s)$.

Note that generating functions are not actually functions — they are formal power series. In some contexts they can be interpreted as functions (e.g., if they are convergent power series).

17. Primary Decomposition

In this section, A denotes a commutative ring.

Let B be a proper ideal of A. B is a **primary ideal** if for all a and a' in A such that $aa' \in B$, either (1) $a \in B$ or (2) $a' \in B$ or (3) $a \in \mathrm{rad}(B)$ and $a' \in \mathrm{rad}(B)$, where $\mathrm{rad}(B)$ denotes the radical of B.[6] Recall that B is prime if for all such a and a', (1) or (2) holds. Therefore every prime ideal is primary. In $\mathbf{Z}$, the primary ideals are the ideals (p^n), where p is a prime number and $n > 0$ is a natural number.

Let B be a primary ideal of A. Then $\mathrm{rad}(B)$ is prime (proof omitted). If $P = \mathrm{rad}(B)$, then we say that B is **P-primary**. Every primary ideal B is P-primary for exactly one prime ideal P. In $\mathbf{Z}$, the primary ideal (p^n) is (p)-primary.

Let B be an ideal of A. A **primary decomposition** of B is a finite set of ideals B_i such that each B_i is P_i-primary and $B = \bigcap_{i=1}^{n} B_i$. B is **decomposable** if it has a primary decomposition. A primary decomposition is **reduced** if (1) P_i is distinct for all i and (2) there is no i such that $B_i \supseteq \bigcap_{j \neq i} B_j$. Any primary decomposition can be transformed into a reduced one by (1) replacing all sets of B_i sharing the same P_i with their intersection and then (2) deleting redundant elements (proof omitted).

Let B be a decomposable ideal of A, and let $\{B_i\}_{1 \leq i \leq n}$ and $\{B'_i\}_{1 \leq i \leq n'}$ be reduced primary decompositions of B, where each B_i is P_i-primary, and each B'_i is P'_i-primary. Then $n = n'$, and $\{P_i\}_{1 \leq i \leq n}$ and $\{P'_i\}_{1 \leq i \leq n}$ are equal as sets (proof omitted). The prime ideals $\{P_i\}_{1 \leq i \leq n}$, which are independent of the reduced primary decomposition, are called the prime ideals **associated with** or **belonging to** the decomposable ideal B.

Let B be a decomposable ideal of A, and let $\{P_i\}_{1 \leq i \leq n}$ be the associated prime ideals. For each i, by the definition of primary decomposition, we have $P_i = \mathrm{rad}(B_i) \supseteq B_i \supseteq B$. If P_i is minimal among prime ideals that contain B, then we say that P_i is a **minimal** or **isolated** prime ideal associated with B. Otherwise we say that P_i is an **embedded**

[6] An equivalent definition found in many textbooks says that if $aa' \in B$, then either (1) $a \in B$ or (2) $a' \in \mathrm{rad}(B)$. This definition may be confusing: on its face it depends on the fact that a appears before a' in the product, and in a commutative ring, the order of operands should not matter. However, if $aa' \in B$ then $a'a \in B$ as well because $a'a = aa'$. Therefore we must also have either (3) $a' \in B$ or (4) $a \in \mathrm{rad}(B)$. By writing out the condition $((1) \vee (2)) \wedge ((3) \vee (4))$, distributing and over or, and simplifying, we arrive at the definition stated in the text.

prime ideal associated with B.[7] The minimal prime ideals associated with B are all and only the minimal elements in the set of all prime ideals that contain B (proof omitted).

18. Ring Extensions

In this section, A and B denote rings.

Recall that a subring of B is a set $A \subseteq B$ that is a ring under the operations inherited from B. In particular, A contains the elements 0 and 1 of B. If A is a subring of B, then we also say that B is an **extension ring** of A.

Fix an extension ring B of A.

1. An element $b \in B$ is **integral over** A if there exists a monic polynomial $p(x) \in A[x]$ such that b is a root of p as a member of $B[x]$. For example:
   - 5 is integral over $\mathbf{Z}$ as a member of $\mathbf{Q}$, because it is a root of the monic polynomial $x - 5$.
   - 1/2 is not integral over $\mathbf{Z}$ as a member of $\mathbf{Q}$ (proof omitted).
   - x is not integral over A as a member of $A[x]$.
2. The set of elements $b \in B$ that are integral over A is called the **integral closure** of A in B. It is a subring of B that contains A (proof omitted).
3. Let C be the integral closure of A in B.
   a. If $C = A$, then we say that A is **integrally closed** in B. $\mathbf{Z}$ is integrally closed in $\mathbf{R}$. The integral domain $\mathbf{Z}[\sqrt{5}]$ is not integrally closed in its field of fractions: it does not contain the element $(\sqrt{5}+1)/2$, which is a root of the monic polynomial $x^2 - x - 1$.
   b. If $C = B$, then we say that B is **integral over** A.

   C is integrally closed in B (proof omitted).

19. Field Extensions

In this section, A and B denote fields.

A **subfield** of B is a set $A \subseteq B$ that is a field under the operations inherited from B. In particular, A contains the elements 0 and 1 of B. If A is a subfield of B, then we also say that B is an **extension field** of B, and we write B/A to denote that B extends A.

Let B be an extension field of A. Since B is a field, it is an additive group. Further, the multiplication of elements of A by elements of B satisfies the rules for an A-module. Therefore B is a vector space over A. We denote the dimension of this vector space $[B : A]$. If $[B : A]$ is infinite, then we say that the extension is **infinite**. Otherwise we say that the extension is **finite**. As examples:

- $\mathbf{C}$ is a finite extension of $\mathbf{R}$. A basis for $\mathbf{C}$ as a vector space over $\mathbf{R}$ is $\{1, i\}$.
- $\mathbf{R}(x)$, the field of fractions of the integral domain $\mathbf{R}[x]$, is an infinite extension of $\mathbf{R}$. A basis for $\mathbf{R}(x)$ over $\mathbf{R}$ is $\{\ x^n \mid n \in \mathbf{Z}\ \}$.

Fix an extension field B of A and an element b of B.

1. The element b is **algebraic over** A if there exists a nonzero polynomial $p(x) \in A[x]$ such that b is a root of p as a member of $B[x]$. We may require that p be irreducible and monic; in this case, p is unique, and $A[x]/p(x)$ is isomorphic to $A[b]$ (proof omitted). Note that in general $A[b]$ is a ring, not a field. We call p the **minimal polynomial** associated with b. As an example, i is algebraic over $\mathbf{R}$ as a subfield of $\mathbf{C}$, because i is a root of $1 + x^2$ as a member of $\mathbf{C}[x]$. Also, $\mathbf{C}$ is isomorphic to $\mathbf{R}[x]/(1 + x^2)$.
2. Otherwise b is **transcendental** over A. For example, x is transcendental over $\mathbf{R}$ as a subfield of $\mathbf{R}(x)$, the field of fractions of $\mathbf{R}[x]$, because there is no nonzero polynomial $p(y) \in \mathbf{R}[y]$ such that x is a root of p as a member of $\mathbf{R}(x)[y]$.

[7] The names come from algebraic geometry. If A is the polynomial ring $C[x_1, \ldots, x_n]$, where C is a field, an ideal B of A defines an **affine variety** $V(B)$ consisting all points $p = (c_1, \ldots, c_n) \in C^n$ such that each polynomial in B evaluates to zero at p. Each of the isolated prime ideals P_i associated with B corresponds to an **irreducible component** of $V(B)$, i.e., an affine variety $V(P_i) \subseteq V(B)$ that cannot be expressed as the union of two proper affine subvarieties. Each embedded prime ideal P_j defines an affine variety $V(P_j)$ embedded in one of the irreducible components.

Fix an extension field B of A.

1. B is **algebraic over** A if every element of B is algebraic over A. For example, $\mathbf{C}$ is algebraic over $\mathbf{R}$. In general, any finite extension B of A is algebraic (proof omitted).
2. Otherwise B is **transcendental over** A. For example, $\mathbf{R}(x)$ is transcendental over $\mathbf{R}$. In general, any transcendental extension is infinite.

Fix an extension field B of A and a subset S of B.

1. Let $A(S) \subseteq B$ denote the field of fractions of the integral domain $A[S]$, where $A[S]$ is defined as in § 6. $A(S)$ is the minimal subfield of B containing A and S.
   a. If B is algebraic over $A(S)$, and if there exists no proper subset T of S such that B is algebraic over $A(T)$, then we say that S is a **transcendence basis** for the extension B/A. Every field extension has a transcendence basis, and all transcendence bases have the same cardinality (proof omitted).
   b. The cardinality of a transcendence basis for B/A is called the **transcendence degree** of the extension B/A. For example, let $F = \mathbf{Z}(\sqrt{2}, x)$ be the minimal subfield of $\mathbf{R}(x)$ containing the polynomial combinations of $\sqrt{2}$ and x over $\mathbf{Z}$. The transcendence degree of F over $\mathbf{Z}$ is one, because F is algebraic over $\mathbf{Z}(x)$. In general the transcendence degree is zero (i.e., $S = \varnothing$) if and only if B/A is algebraic.
2. Assume that S is a transcendence basis for B/A. Then by definition B is algebraic over $A(S)$. If in fact we have $B = A(S)$, then we say that the extension B/A is **purely transcendental**. For example, the extension $\mathbf{R}(x)/\mathbf{R}$ is purely transcendental.

A is **algebraically closed** if every polynomial in $A[x]$ has a root in A. In this case, every polynomial $p \in A[x]$ of degree d may be written as $\prod_{i=1}^{d}(x - a_i)$ with all $a_i \in A$ (proof omitted).

An algebraic extension of A that is algebraically closed is called an **algebraic closure** of A. Every field has an algebraic closure. The algebraic closure of a field A is unique up to isomorphism (proof omitted).

Fix a field A, and let B be an algebraic closure of A. Let p be a polynomial in $A[x]$ of degree d. As a member of $B[x]$, p factors as $\prod_{i=1}^{d}(x - b_i)$. If the elements $b_1, \ldots, b_d$ are all distinct, then we say that the polynomial p is **separable**.

Fix a field A and an extension field B of A.

1. Fix an element $b \in B$ that is algebraic over A. Let p be the minimal polynomial associated with b. If p is separable, then we say that b is **separable over** A.
2. If every element $b \in B$ is separable over A, then we say that the extension B is **separable over** A.

20. Chains of Modules and Ideals

In this section, A denotes a ring, and B denotes an A-module.

Fix a module B, and let S be the set of submodules of B, partially ordered by inclusion (i.e., $C \leq D$ if $C \subseteq D$).

1. If every increasing sequence $\{B_i\}_{i \in \mathbf{N}}$ in S is stationary (§ 2), i.e., of the form
   $$B_1 \subseteq B_2 \subseteq \cdots \subseteq B_i = B_{i+1} = B_{i+2} = \cdots$$
   then we say that B satisfies the **ascending chain condition**. Equivalently, every non-empty subset of S has a maximal element (proof omitted). In this case, we say that the module B is **Noetherian**. B is Noetherian if and only if every submodule of B (including B itself) is finitely generated (proof omitted).
2. If every decreasing sequence $\{B_i\}_{i \in \mathbf{N}}$ in S is stationary, i.e., of the form
   $$B_1 \supseteq B_2 \supseteq \cdots \supseteq B_i = B_{i+1} = B_{i+2} = \cdots$$
   then we say that B satisfies the **descending chain condition**. Equivalently, every non-empty subset of S has a minimal element (proof omitted). In this case, we say that the module B is **Artinian**.

A ring A is an A-module. Further, a subset B of A is an A-submodule of the module A if and only if B is an ideal of the ring A. Therefore we have the following definitions for rings:

1. A ring A is Noetherian if it satisfies the ascending chain condition for its submodules, i.e., its ideals.
2. A ring A is Artinian if it satisfies the descending chain condition for its submodules, i.e., its ideals.

Note the following:

1. Any ring A is finitely generated as an A-module by the element 1. However, a Noetherian ring A is not necessarily finitely generated as a ring (i.e., as an additive group).
2. A field F has only two ideals, 0 and F. Therefore every field is a Noetherian ring.

Fix a Noetherian ring A. Then the polynomial ring $A[x_1, \ldots, x_n]$ is Noetherian. This statement follows from **Hilbert's basis theorem** (proof omitted).

Fix a module B. A **chain of submodules** of B is a finite sequence of submodules $\{B_i\}_{0 \le i \le n}$ such that $B_0 = B$, $B_n = 0$, and $B_{i-1} \supset B_i$ for all $1 \le i \le n$ (strict inclusion). We may represent a chain of submodules as follows:

$$B = B_0 \supset B_1 \supset \cdots \supset B_n = 0$$

The nonnegative integer n is called the **length** of the chain. It is the number of $\supset$ symbols appearing in the chain.

A **composition series** is a chain of modules of maximal length, i.e., one in which no new submodules can be inserted. Equivalently, for each $1 \le i \le n$, M_{i-1}/M_i is simple.

Fix a module B. Either B has no composition series, or it has a composition series of length n. In the second case, every composition series of B has length n (proof omitted). We define the **length** of B as follows:

1. If B has no composition series, then the length is ∞.
2. Otherwise B has at least one composition series of length n for some n, and the length of B is n.

We write $l(B)$ to denote the length of B.

Fix a ring A.

1. A **chain of prime ideals** of A is a finite sequence of prime ideals $\{P_i\}_{0 \le i \le n}$ such that $B_{i-1} \subset B_i$ for all $1 \le i \le n$. We may represent a chain of prime ideals as follows:

   $$P_0 \subset P_1 \subset \cdots \subset P_n$$

   The nonnegative integer n is called the **length** of the chain. It is the number of $\subset$ symbols appearing in the chain.
2. If $A \neq 0$, then the **Krull dimension** of A is the supremum of the lengths of all chains of prime ideals in A. The Krull dimension of the zero ring is either -1 or $-\infty$, depending on the context. Where there is no ambiguity, we write "dimension" instead of "Krull dimension." We also write dim A for the dimension of A.
3. Fix an A-module B. The **Krull dimension** of B, written $\dim_A B$, is $\dim (A/\mathrm{ann}_A(B))$, where $\mathrm{ann}_A(B)$ is the annihilator of B in A (§ 7). Note that if $B = A$, then $\mathrm{ann}_A(B) = 0$, and $\dim_A B = \dim A$.

A field has dimension zero. The ring $\mathbf{Z}$ has dimension one. A ring A is Artinian if and only if A is Noetherian and $\dim A = 0$ (proof omitted). A Noetherian ring of dimension one is called a **Dedekind domain**.

Fix a ring A and a prime ideal $P \subset A$.

1. The **height** of P, written $\mathrm{ht}(P)$, is the supremum of the lengths of all chains of prime ideals in A with $P_n = P$.
2. The **depth** of P is the supremum of the lengths of all chains of prime ideals in A with $P_0 = P$.

21. Fractional and Invertible Ideals

In this section, let A be an integral domain, and let F be its field of fractions.

A **fractional ideal** I of A is an A-submodule of F such that for some $a \neq 0$ in A we have $aI \subseteq A$.

1. For example, let $A = \mathbf{Z}$ and $F = \mathbf{Q}$. Let I be all integer multiples of 1/2. Then I is a fractional ideal of $\mathbf{Z}$ with $a = 2$.
2. More generally, fix an element $f \in F$. Let I be the set of all multiples af with $a \in A$. If $f \in A$, then $I \subseteq A$. Otherwise $f^{-1} \in A$, and $f^{-1}I \subseteq A$. Therefore I is a fractional ideal of F. A fractional ideal in this form is called a **principal fractional ideal**. It is denoted (f) or Af.

3. Any ideal of A is a fractional ideal of F with $a = 1$.

Consider F and A as F-modules. Recall from § 6 that if M is a submodule of F, the ideal quotient $(A : M)$ denotes the set of all $f \in F$ such that $fM \subseteq A$.

An A-submodule I of F is an **invertible ideal** of A if there exists an F-submodule J of F such that $IJ = A$. In this case

1. J is unique and equal to $(A : I)$ (proof omitted).
2. I is finitely generated (proof omitted).
3. I is a fractional ideal of A (proof omitted).

Let A be a Dedekind domain.

1. The non-zero fractional ideals of A form a group G with respect to multiplication (proof omitted). We call G the **group of ideals** of A.
2. Recall that F^* denotes the multiplicative group of F (§ 6). each $f \in F$ defines a principal fractional ideal (f), and the map $f \mapsto (f)$ is a homomorphism $\phi\colon F^* \to G$.
    a. The image $P = \phi(F^*)$ is the group of principal fractional ideals.
    b. The cokernel $H = G/P$ of ϕ is called the **ideal class group** of A.
    c. The kernel U of ϕ is j called the **group of units** of A. It is the set of all $f \in F^*$ such that $(f) = (1)$.

22. Valuation Rings

Fix a field F.

1. Let G be an additive group whose elements are totally ordered as a set. Let S be the set $G \cup \{\infty\}$ with a total order given by the ordering on G plus $g \le \infty$ for all g in G. A **valuation** (v, G) on F is a map $v\colon F \to S$ such that the following conditions hold for all f and g in F:
    a. $v(f) = \infty$ if and only if $f = 0$.
    b. $v(fg) = v(f) + v(g)$.
    c. $v(f + g) \ge \min(v(f), v(g))$.
2. A **discrete valuation** v on F is a valuation $(v, \mathbf{Z})$ on F.

Note that every discrete valuation is a valuation.

For example, let $A = \mathbf{C}(x)$, the field of fractions of the integral domain $\mathbf{C}[x]$. Every nonzero element $f(x)$ of $\mathbf{C}(x)$ may be written uniquely up to constant factors as $x^n(p_1(x)/p_2(x))$, where p_1 and p_2 are polynomials in $\mathbf{C}[x]$ with nonzero constant terms. Let $\mathrm{ord}\colon \mathbf{C}(x) \to \mathbf{Z}$ be the function that takes 0 to ∞ and takes each nonzero $f(x) = x^n(p_1(x)/p_2(x))$ to n.

Because p_2 has a nonzero constant term, p_2 is invertible in $\mathbf{C}[[x]]$ (§ 16). Let $P(x)$ be the formal power series $p_1(x)p_2^{-1}(x)$, and write $f(x) = x^n P(x)$. Then $p_1(x) = P(x)p_2(x)$, so $P(x)$ has a nonzero constant term. Thus we see that $\mathrm{ord}(f)$ is the order of the Laurent series expansion of the rational complex function f at zero. See § 5.1 of my paper *Calculus over the Complex Numbers*.

We now show that ord is a discrete valuation on $\mathbf{C}(x)$. Property 1 holds by construction. Property 2 holds because

$$\mathrm{ord}(fg) = \mathrm{ord}(x^n P \cdot x^m Q) = \mathrm{ord}(x^{n+m} PQ) = n + m.$$

Property 3 holds because, assuming $n \le m$, we have

$$\mathrm{ord}(f + g) = \mathrm{ord}(x^n P + x^m Q) = \mathrm{ord}(x^n (P + x^{m-n} Q)).$$

If $m \ne n$, or if the constant term of $P + Q$ is not zero, then $\mathrm{ord}(f + g) = n$. Otherwise if $P + Q$ has any nonzero term, then the lowest-order term has an exponent greater than zero, so $\mathrm{ord}(f + g) > n$. Otherwise $\mathrm{ord}(f + g) = \infty$.

Fix an integral domain A, and let F be its field of fractions.

1. A is a **valuation ring** with valuation (v, G) if (v, G) is a valuation on F and A consists of all elements f of F such that $v(f) \ge 0$. Note that $v(0) = \infty \ge 0$, so zero is included.

2. A is a **discrete valuation ring** with valuation v if A is a valuation ring with valuation $(v, \mathbf{Z})$.

Note that every discrete valuation ring is a valuation ring.

For example, let S be the set of polynomials in $\mathbf{C}[x]$ with nonzero constant terms. Then S is a multiplicative monoid, so we may form $D = S^{-1}\mathbf{C}[x]$, the ring of fractions with respect to S (§ 14). Notice that D is the localization of $\mathbf{C}[x]$ at the prime ideal (x). D is an integral domain, and the field of fractions of D is $\mathbf{C}(x)$. Let ord be the valuation on $\mathbf{C}(x)$ given above. Then $p \in D \Leftrightarrow \text{ord}(p) \geq 0$, so D is a discrete valuation ring with value ord.

Fix an integral domain A, and let F be its field of fractions.

1. A is a valuation ring if and only if any one of the following conditions holds (proof omitted):
    a. For each $f \in F$, either $f \in A$ or $f^{-1} \in A$ (or both). For example, let $F = \mathbf{C}(x)$, and let $A = D$ as constructed above. Let $f = x^n(p_1/p_2)$ be an element of $\mathbf{C}(x)$. If $x \geq 0$, then $f \in A$. Otherwise $f^{-1} = x^{-n}(p_2/p_1) \in A$.
    b. The ideals of A are totally ordered by inclusion.
    c. The principal ideals of A are totally ordered by inclusion.
2. A is a discrete valuation ring if and only if any one of the following conditions holds (proof omitted):
    a. A has a unique irreducible element t. The element t generates the unique maximal ideal of A and is called a **uniformizing parameter** of A. For example, in the case of $\mathbf{C}(x)$ and D, the uniformizing parameter is x, and the unique maximal ideal of A is (x). Apart from a power of x, any two elements f and g of D differ by a factor $u = p_1/p_2$ where p_1 and p_2 have nonzero constant terms, so u is a unit in D.
    b. A is Noetherian, A is not a field, and no nonzero fractional ideal can be written as a finite intersection of fractional ideals that properly contain it.
    c. A is a local ring, and one of the following conditions holds:
        i. A is a principal ideal domain, and A is not a field.
        ii. A is a Dedekind domain, and A is not a field.
        iii. A is Noetherian, the maximal ideal of A is principal, and A is not a field.
        iv. A is Noetherian, A is integrally closed, and A has Krull dimension one.
    d. A is a principal ideal domain, and one of the following conditions holds:
        i. A has a unique nonzero maximal ideal.
        ii. A has a unique nonzero prime ideal.

23. Topological Spaces

A **topological space** is a pair (S, O), where S is a set and O is a set of subsets of S satisfying the following axioms:

1. The empty set and S are elements of O.
2. Any union of elements of O is an element of O.
3. Any intersection of finitely many elements of O is an element of O.

The set O is called a **topology** on S. The elements of O are called the **open sets** of the topology. We often write a topological space (S, O) as S. In this case the topology on S is implied.

Fix a topological space (S, O).

1. Let T be a subset of S. The **complement** of T, written T^C, is the set difference $S - T$.
2. T is **closed** if and only if its complement T^C is open.

Fix topological space (S, O) and a set of subsets B of S.

1. B is a **base** or **basis** for the topology O if every element of O may be represented as the union of elements of B.
2. B is a **subbase** or **subbasis** for O if there exists a basis B' for O such that every element of B' except S may be represented as the intersection of finitely many elements of B.

If B is a subbasis for O, then we say that B **generates** O. In this case O is minimal among the topologies on S that contain B.

Fix a set S.

1. A **metric** or **distance function** on S is a function $d\colon S \times S \to \mathbf{R}$ that satisfies the following axioms for all a, b, and c in $\mathbf{R}$:
   a. $d(a, b) = 0$ if and only if $a = b$.
   b. $d(a, b) = d(b, a)$.
   c. $d(a, c) \leq d(a, b) + d(b, c)$.

   From these axioms we can deduce

   $$0 = d(a, a) \leq d(a, b) + d(b, a) = d(a, b) + d(a, b) = 2d(a, b)$$

   Therefore $d(a, b) \geq 0$.
2. Fix a metric d on S.
   a. Fix a point $s \in S$ and real number $r > 0$. The **open ball** $B(s, r)$ is the set of all points x in S such that $d(s, x) < r$.
   b. The metric d induces a topology T on S. Its basis is the set of all open balls $B(s, r)$ with $s \in S$ and $r \geq 0$. T is called the topology **induced** by the metric d.

Let $S = \mathbf{R}^n$.

1. The **Euclidean metric** on $\mathbf{R}^n$ is the function

   $$d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}.$$

   When $n = 1$, d is the absolute difference function $|x - y|$.
2. The **Euclidean topology** on $\mathbf{R}^n$ is the topology induced by the Euclidean metric.

Let $F = \{(S_i, O_i)\}_{i \in I}$ be a family of topological spaces. Let $S = \underset{i \in I}{\times} S_i$ be the Cartesian product of F. The **product topology** on F is the topology O generated by all sets $\underset{i \in I}{\times} U_i$, where

1. For some $j \in I$, U_j is an element of O_j.
2. For all $i \neq j$, $U_i = S_i$.

For example, let $S = \mathbf{R} \times \mathbf{R}$, with the Euclidean topology on each copy of $\mathbf{R}$. Then the product topology on S is generated by all sets of the form $T \times \mathbf{R}$ and $\mathbf{R} \times T$ where T is open in $\mathbf{R}$. This topology is equivalent to the Euclidean topology on $\mathbf{R}^2$.

Let (S, O) and (S', O') be topological spaces. Fix a map $f\colon S \to S'$.

1. f is **continuous** if for every open set U in O', $f^{-1}(U)$ is in O.
2. f is a **homeomorphism** if it is a continuous bijection, and its inverse is continuous.

Fix a topological space (S, O).

1. Fix a point $p \in S$.
   a. A **neighborhood** of p is a subset U of S (not necessarily open) that contains an open set V that contains p. If U itself is open, then we say it is an **open neighborhood**.
   b. A **fundamental system of neighborhoods** of p is a family of neighborhoods $\{U_i\}_{i \in I}$ of p such that any neighborhood V of p contains at least one of the U_i. For example, let (S, O) be $\mathbf{R}$ with the Euclidean topology. Then the open balls $B(p, 1/n)$, where n is a positive integer, form a fundamental system of neighborhoods of p.
2. (S, O) is **Hausdorff** if, given any two distinct points p and p' in S, there exists a neighborhood U of p and a neighborhood U' of p' such that $U \cap U' = \varnothing$.

Fix a topological space (S, O), a point $p \in S$, and a net $N = \{s_i \in S\}_{i \in I}$. We say that N **converges to** p and write $N \to p$ or $s_i \to p$ if for all $i \in I$ if for any neighborhood U of p, there exists $i \in I$ such that for all $j \geq i$, $s_j \in U$. Note that the same definition applies to sequences, because every sequence is a net.

24. Topological Groups

Let A be an additive group, and let O be a topology on A, considered as a set. The topological space (A, O) is a **topological group** if the following conditions hold:

1. $(a, b) \mapsto a + b$ is a continuous map from $A \times A$ to A, where we put the product topology on $A \times A$.
2. $a \mapsto -a$ is a continuous map from A to A.

Fix a topological group (A, O).

1. For any $a \in A$, the translation map $t_a: A \to A$ given by $t_a(x) = x + a$ is bijective and continuous with inverse t_{-a}, so it is a homeomorphism.
2. Therefore for any set $U \subseteq A$ and element $a \in A$, U is open if and only if $U + a$ is open. In particular, to specify a topology O, it suffices to specify the open neighborhoods of zero in O.

We extend the concept of a topological group to rings and modules in the obvious way.

1. A **topological ring** is a topological space (A, O) in which A is a ring and the ring operations of A are continuous with respect to the topology O.
2. A **topological module** has the analogous definition, after substituting "module" for "ring" everywhere.

Fix a topological group A.

1. A sequence $S = \{a_i \in A\}_{i \in I}$ is **Cauchy** if for any neighborhood U of 0, there exists $i \in I$ such that for all $j \geq i$ and $k \geq i$, $a_j - a_k$ lies in U.
2. Two Cauchy sequences $S = \{a_i \in A\}_{i \in I}$ and $S' = \{a'_i \in A\}_{i \in I}$ are **equivalent** if the sequence $\{a_i - a'_i\}_{i \in I}$ converges to zero.

Fix a topological group A with a countable fundamental system of neighborhoods of $0 \in A$. Let N be such a fundamental system.

1. Let $\hat{A}$ denote the set of equivalence classes of Cauchy sequences in A. Then $\hat{A}$ is an additive group, according to the addition rule $\{a_i\} + \{b_i\} = \{a_i + b_i\}$. $\hat{A}$ is called the **completion** of A. It has the following properties:
   a. The map $a \mapsto \{a\}_{i \in I}$ is a group homomorphism $\phi: A \to \hat{A}$. ϕ is injective if and only if (A, O) is Hausdorff (proof omitted).
   b. $\hat{A}$ is **complete**: that is, every Cauchy sequence in $\hat{A}$ converges to an element of $\hat{A}$.

   As an example, let $A = \mathbf{Q}$, considered as an additive group, with the Euclidean topology. Then $\hat{A} = \mathbf{R}$.
2. Assume that N is a sequence of subgroups $A = A_0 \supseteq A_1 \supseteq \cdots$.
   a. For all $i \leq j$, let $f_{ij}: A/A_j \to A/A_i$ be the map that takes each coset $A_j + a$ in A/A_j to the coset $A_i + a$ in A/A_i. This map is well-defined, because
   $$A_j + a = A_j + a' \Rightarrow a - a' \in A_j \Rightarrow a - a' \in A_i \Rightarrow A_i + a = A_i + a'.$$
   Further, f_{ij} is a homomorphism of additive groups, and the maps f_{ij} make the family $\{A/A_i\}_{i \in I}$ into an inverse system of additive groups, i.e., $\mathbf{Z}$-modules (§ 10).
   b. As an additive group, each A_j contains the element zero, so it is a neighborhood of zero.
   c. Let $S = \{a_i\}$ be a Cauchy sequence in A. Fix $j \in I$, and let $\phi_j: A \to A/A_j$ be the map that takes each $a \in A$ to its coset in A/A_j. For large enough i, the differences between the elements a_i lie in A_j (because S is Cauchy and A_j is a neighborhood of zero), and therefore map to zero under ϕ_j. So for large enough i, each element of the sequence $\{\phi_j(a_i)\}$ is a constant $b_j \in A/A_j$.
   d. By carrying out step (c) for each $j \in I$, we can associate the Cauchy sequence S with the element $b = \{b_j\}$ of the direct product $\prod_{j \in I} A/A_j$. The element b satisfies the mapping criteria for membership in the inverse limit $\varprojlim A/A_i$ (§ 10). Further, each member of the inverse limit corresponds to a Cauchy sequence. Therefore the completion $\hat{A}$ is isomorphic to $\varprojlim A/A_i$.

   An example is the **p-adic topology** on $\mathbf{Z}$. This is the topology on $\mathbf{Z}$ whose open neighborhoods of zero are the sets $A_j = p^j\mathbf{Z}$ for $j \geq 0$. It is induced by the distance function $d(a, b) = p^{-n}$ for $a \neq b$, where n is the largest power of p that divides $a - b$. The completion of $\mathbf{Z}$ with respect to the p-adic topology yields the **p-**

adic integers $\lim_{\leftarrow} \mathbf{Z}/p^i\mathbf{Z}$.

We generalize the p-adic topology as follows. Fix a ring A and an ideal $I \subseteq A$.

1. Let $\{A_i\}$ be the sequence of ideals given by $A_i = I^i$ for $i \geq 0$, where $I^0 = (1) = A$, $I^1 = I$, $I^2 = II$, etc. The **I-adic topology** on A is the unique topology whose open neighborhoods of zero are the sets A_i. The I-adic topology makes A into a topological ring. The completion $\hat{A} = \lim_{\leftarrow} A/A_i$ is also a topological ring (proof omitted).
2. Fix an A-module B.
   a. Fix a sequence S of submodules $B = B_0 \supseteq B_1 \supseteq \cdots$.
      i. S is called a **filtration** and written (B_i).
      ii. (B_i) is an **I-filtration** if $IB_i \subseteq B_{i+1}$ for all i.
      iii. (B_i) is a **stable I-filtration** if $IB_i = B_{i+1}$ for all sufficiently large i.
   b. Let (B_i) be the stable I-filtration (I^iB). The **I-adic topology** on B is the unique topology whose open neighborhoods of zero are the sets B_i. The I-adic topology makes B into a topological module. The completion $\hat{B} = \lim_{\leftarrow} B/B_i$ is also a topological module (proof omitted).

For example, fix a ring B and let A be $B[x]$, the ring of polynomials in one variable over B. Let $I = (x) \subseteq A$, and put the I-adic topology on A. Then $\hat{A}$ is $B[[x]]$, the ring of formal power series over B.

Fix a ring A an ideal $I \subseteq A$, an A-module B, and I-filtrations (B_i) and (B'_i) of B.

1. We say that (B_i) and (B'_i) have **bounded difference** if there exists a natural number $n \geq 0$ such that for all $i \geq 0$, $B_{i+n} \subseteq B'_{i+n}$ and $B'_{i+n} \subseteq B_{i+n}$.
2. If (B_i) and (B'_i) are stable I-filtrations, then they have bounded difference (proof omitted). Therefore all stable I-filtrations determine the same topology, i.e., the I-adic topology.

25. Graded Rings and Modules

In this section, A denotes a ring.

Let $P = A[x_1, \ldots, x_n]$ be the polynomial ring in n variables over A. For each $i \geq 0$, let P_i be the set of homogeneous polynomials of P of degree i. Observe that P has the following structure:

1. $P_0 = A$. Each P_i is a submodule of P, considered as an A-module.
2. P is the direct sum $\bigoplus_{i \in \mathbf{N}} P_i$. Indeed, for any polynomial $p \in P$, for each $i \in \mathbf{N}$, let p_i be the sum of all terms of p of degree i (or 0 if there are no such terms). Then $\{p_i\}_{i \in \mathbf{N}}$ is an element of $\bigtimes_{i \in \mathbf{N}} P_i$, and all but finitely many of the p_i are zero.
3. For all $i, j \geq 0$, let P_iP_j denote the set of all products ab with $a \in P_i$ and $b \in P_j$. Then $P_iP_j \subseteq P_{i+j}$.

We generalize this structure as follows:

1. A ring A is a **graded ring** if there exists a family $\{A_i\}_{i \in \mathbf{N}}$ of additive subgroups of A such that $A = \bigoplus_{i \in \mathbf{N}} A_i$ and for all $i, j \geq 0$, $A_iA_j \subseteq A_{i+j}$. In particular, $A_0A_0 = A_0$, so A_0 is a subring of A, and each A_i is a submodule of A, considered as an A_0-module. The polynomial ring in n variables is a graded ring.
2. Fix a graded ring A. An A-module B is a **graded A-module** if there exists a family $\{B_i\}_{i \in \mathbf{N}}$ of additive subgroups of B such that $B = \bigoplus_{i \in \mathbf{N}} B_i$ and for all $i, j \geq 0$, $A_iB_j \subseteq B_{i+j}$. In particular, $A_0B_i \subseteq B_i$, so each B_i is an A_0-module. A ring A is an A-module, so every graded ring A is a graded A-module.

Fix a graded ring A and a graded A-module B.

1. An element $b \in B$ is **homogeneous** if $b \in B_d$ for some $d \geq 0$. d is the **degree** of the homogeneous element b.
2. Any element $b \in B$ has a unique representation $\sum_{i \in \mathbf{N}} b_i$, where each $b_i \in B_i$, and all but finitely many of the b_i are zero. The nonzero elements b_i are called the **homogeneous components** of b.

Fix a graded ring A and graded A-modules B and C. A map $f\colon B \to C$ is a **homomorphism of graded A-modules** if (1) it is a homomorphism of A-modules and (2) $f(B_i) \subseteq C_i$ for all $i \geq 0$.

Fix a graded ring A. Define $A_+ = \bigoplus_{i>0} A_i$. A_+ is an ideal of A.

Fix a ring A (not necessarily graded) and an ideal $I \subseteq A$.

1. Define $A^* = \bigoplus_{i \in \mathbf{N}} I^i$. A^* is a graded ring.
2. Define $G_I(A) = \oplus_{i \in \mathbf{N}} I^i/I^{i+1}$. For each pair of cosets $I^{i+1} + b_i \in I^i/I^{i+1}$ and $I^{j+1} + b_j \in I^j/I^{j+1}$, define $(I^{i+1} + b_i)(I^{j+1} + b_j)$ to be the coset $I^{i+j+1} + b_i b_j \in I^{i+j}/I^{i+j+1}$. This multiplication is well-defined, because for any $b'_{i+1} \in I^{i+1}$ and $b'_{j+1} \in I^{j+1}$, we have

   $$(b'_{i+1} + b_i)(b'_{j+1} + b_j) = b'_{i+1}b'_{j+1} + b'_{i+1}b_j + b_i b'_{j+1} + b_i b_j \in I^{i+j+1} + b_i b_j.$$

   This multiplication makes $G_I(A)$ into a graded ring, called the **associated graded ring** of A and I.
3. Fix an A-module B and an I-filtration $F = (B_i)$.
   a. Define $B^* = \bigoplus_{i \in \mathbf{N}} B_i$. B^* is a graded A-module, since for all $i, j \geq 0$ we have $I^i B_j \subseteq B_{i+j}$.
   b. Define $G_F(B) = \bigoplus_{i \in \mathbf{N}} B_i/B_{i+1}$. Define multiplication on $G_F(B)$ analogously to the definition for the associated graded ring. This multiplication makes $G_F(B)$ into a graded module, called the **associated graded module** of B and F.

26. Differential Sequences of Modules

In this section, A denotes a ring.

A **differential sequence of A-modules** S consists of an A-module sequence $\{B_i\}$ (§ 11) with the following additional structure:

1. The index i is called the **degree** or **dimension** of the A-module B_i.
2. The A-module homomorphisms $f_i\colon B_i \to B_{i+1}$ (if S is ascending) or $f_i\colon B_i \to B_{i-1}$ (if S is descending) are called **boundary operators** or **differentials** and written d_i.
3. The composition of any successive differentials is zero: that is, for all $i \in J$, $d_i \circ d_{i-1} = 0$ (if S is ascending) or $d_i \circ d_{i+1} = 0$ (if S is descending). Equivalently, $\operatorname{im} f_{i+1} \subseteq \ker f_i$ or $\operatorname{im} f_{i-1} \subseteq \ker f_i$.

A differential sequence of modules may be a sequence of $\mathbf{Z}$-modules, i.e., abelian groups. When there is no ambiguity, we write "differential sequence" instead of "differential sequence of A-modules."

Fix a differential sequence S whose index set is $\mathbf{Z}$. S is **bounded above** if all $B_i = 0$ for i greater than some fixed degree. S is **bounded below** if all $B_i = 0$ for i less than some fixed degree. S is **bounded** if it is bounded above and bounded below. If S is bounded, then all but finitely many of its modules B_i are zero.

27. Chain Complexes of Modules

In this section, A denotes a ring.

An **A-module chain complex** is a descending A-module differential sequence (§ 26) whose index set is $\mathbf{Z}$. When there is no ambiguity, we write "chain complex" instead of "A-module chain complex."

Fix an A-module chain complex C.

1. For each i,
   a. The elements of B_i are called **chains** of B_i.
   b. The elements of $\ker d_i$ are called **cycles** or **closed elements** of B_i.
   c. The elements of $\operatorname{im} d_{i+1}$ are called **boundaries** or **exact elements** of B_i. By definition, all boundaries of B_i are cycles of B_i.
   d. The ith **homology module** H_i is equal to the cycles of B_i modulo the boundaries of B_i: $H_i = \ker d_i/\operatorname{im} d_{i+1}$. By definition, C is exact at i if and only if $H_i = 0$.
2. The sequence $\{H_i\}$ is called the **homology** of C. It expresses whether and how C deviates from being an exact sequence.

An A-**module cochain complex** is an ascending A-module differential sequence whose index set is $\mathbf{Z}$. When there is no ambiguity, we write "cochain complex" instead of "A-module cochain complex."

Note that chain complexes are descending and cochain complexes are ascending. This may seem backwards.

Fix an A-module cochain complex C.

1. For each i,
    a. The elements of B^i are called **cochains** of B_i.
    b. The elements of $\ker d^i$ are called **cocycles** or **closed elements** of B^i.
    c. The elements of $\operatorname{im} d^{i-1}$ are called **coboundaries** or **exact elements** of B^i. By definition, all coboundaries of B^i are cocycles of B^i.
    d. The ith **cohomology module** H^i is equal to the cycles of B^i modulo the boundaries of B^i: $H^i = \ker d^i / \operatorname{im} d^{i+1}$. By definition, C is exact at i if and only if $H^i = 0$.
2. The sequence $\{H^i\}$ is called the **cohomology** of C. It expresses whether and how C deviates from being an exact sequence.

Note that in the abstract, chain complexes and cochain complexes (and therefore homology and cohomology) are identical, up to the numbering of the modules and homomorphisms. This may seem confusing. Why have two essentially identical definitions, that differ only in the assignment of labels? There are at least two reasons:

1. Once we pick a numbering, then the homology and cohomology are fixed, and it is useful to have both.
2. Often there is a natural notion of degree or dimension that determines which direction is homology and which is cohomology.

28. Resolutions of Modules

In this section, A denotes a ring.

Fix an A-module C. A **left resolution** of C is an exact sequence consisting of the following:

1. A descending differential sequence $\{B_i\}$ (§ 26) whose index set is $\mathbf{N}$.
2. A sequence $B_0 \xrightarrow{\varepsilon} C \to 0$.

We typically write a left resolution as follows:

$$\cdots \xrightarrow{d_2} B_1 \xrightarrow{d_1} B_0 \xrightarrow{\varepsilon} C \to 0$$

We may also write it as follows:

$$B_\cdot \xrightarrow{\varepsilon} C \to 0$$

Fix an A-module C and a left resolution R of C.

1. The **length** of R is the minimum value of n such that $B_i = 0$ for all $i > n$ if such an n exists; otherwise ∞.
2. R is **free** if each of the modules B_i is free.
3. R is **projective** if each of the modules B_i is projective (§ 11).
4. R is **flat** if each of the modules B_i is flat (§ 13).

Every A-module C has a free resolution, a projective resolution, and a flat resolution (proof omitted).

Fix an A-module C. A **right resolution** of C is an exact sequence consisting of the following:

1. An ascending differential sequence $\{B^i\}$ (§ 26) whose index set is $\mathbf{N}$.
2. A sequence $0 \to C \xrightarrow{\varepsilon} B^0$.

We typically write a right resolution as follows:

$$0 \to C \xrightarrow{\varepsilon} B^0 \xrightarrow{d^0} B^1 \xrightarrow{d^1} \cdots$$

We may also write it as follows:

$$0 \to C \overset{\varepsilon}{\to} B^{\cdot}$$

Fix an A-module C and a right resolution R of C.

1. The **length** of R is the minimum value of n such that $B^i = 0$ for all $i > n$ if such an n exists; otherwise ∞.
2. R is **injective** if each of the modules B^i is injective.

Every A-module C has an injective resolution (proof omitted).

Fix an A-module C other than the trivial module 0.

1. The **projective dimension** of C is the infimum of the lengths of all projective resolutions of C. In particular:
   a. C has projective dimension zero if and only if it is a projective module. In this case, we may set $B_0 = C$ and let ε be the identity map, yielding the exact sequence
   $$0 \to B_0 \overset{\varepsilon}{\to} C \to 0$$
   This sequence is a projective resolution of C of minimal length.
   b. C has projective dimension ∞ if and only if there is no projective resolution of C with finite length.
2. The **flat dimension** of C is the infimum of the lengths of all flat resolutions of C.
3. The **injective dimension** of C is the infimum of the lengths of all injective resolutions of C.

29. Derived Functors

In this section, A and A' are rings.

Let $F\colon M_A \to M_{A'}$ be a covariant right exact functor or a contravariant left exact functor (§ 13). We construct a family of functors $\{L_iF\colon M_A \to M_{A'}\}_{i \in \mathbf{N}}$ called the **left derived functors** of F as follows:

1. If F is covariant, then do the following:
   a. Fix a family $N = \{N_C\}_{C \in M_A}$, where each N_C is a projective resolution of C (§ 28), and write
   $$N_C = \cdots \overset{d(N,C,2)}{\to} B(N,C,1) \overset{d(N,C,1)}{\to} B(N,C,0) \overset{\varepsilon(N,C)}{\to} C \to 0$$
   b. For each $C \in M_A$, apply F to the modules $B(N,C,i)$ and homomorphisms $d(N,C,i)$ of N_C to construct the sequence
   $$X(N,C) = \cdots \overset{F(d(N,C,2))}{\to} F(B(N,C,1)) \overset{F(d(N,C,1))}{\to} F(B(N,C,0) \to 0 \to \cdots$$
2. Otherwise do the following:
   a. Fix a family $\{N_C\}_{C \in M_A}$, where each N_C is an injective resolution of C (§ 28), and write
   $$N_C = 0 \to C \overset{\varepsilon(N,C)}{\to} B(N,C,0) \overset{d(N,C,0)}{\to} B(N,C,1) \overset{d(N,C,1)}{\to} \cdots$$
   b. For each $C \in M_A$, apply F to the modules $B(N,C,i)$ and homomorphisms $d(N,C,i)$ of N_C to construct the sequence
   $$X(N,C) = \cdots \overset{F(d(N,C,1))}{\to} F(B(N,C,1)) \overset{F(d(N,C,0))}{\to} F(B(N,C,0)) \to 0 \to \cdots$$
3. In either case, each $X(N,C)$ is a descending sequence of A'-modules indexed by $\mathbf{Z}$, where $X(N,C)_i = F(B(N,C,i))$ for $i \geq 0$ and $X(N,C)_i = 0$ for $i < 0$. Each $X(N,C)$ is a chain complex (§ 27), not necessarily exact (proof omitted).
   a. For each $C \in M_A$ and $i \in \mathbf{N}$, let $H(N,C)_i \in M_{A'}$ be the ith homology module (§ 27) of $X(N,C)$.
   b. For each $i \in \mathbf{N}$ there exists a unique functor $L_iF(N)\colon M_A \to M_{A'}$ such that $L_iF(N)(C) = H(N,C)_i$ (proof omitted).
   c. For any two families N and N', the functors $L_iF(N)$ and $L_iF(N')$ are naturally isomorphic (§ 13) (proof omitted). Therefore $L_iF(N) \sim L_iF(N')$, and we write the equivalence class as L_iF.

Let $F\colon M_A \to M_{A'}$ be a covariant left exact functor or a contravariant right exact functor (§ 13). We construct a family of functors $\{R^iF\colon M_A \to M_{A'}\}_{\,i\,\in\,\mathbf{N}}$ called the **right derived functors** of F as follows:

1. If F is covariant, then do the following:
   a. Fix a family $\{N_C\}_{C\,\in\,M_A}$, where each N_C is an injective resolution of C (§ 28), and write
   $$N_C = 0 \to C \overset{\varepsilon(N,C)}{\to} B(N,C,0) \overset{d(N,C,0)}{\to} B(N,C,1) \overset{d(N,C,1)}{\to} \cdots$$
   b. For each $C \in M_A$, apply F to the modules $B(N,C,i)$ and homomorphisms $d(N,C,i)$ of N_C to construct the sequence
   $$X(N,C) = \cdots \to 0 \to F(B(N,C,0)) \overset{F(d(N,C,0))}{\to} F(B(N,C,1)) \overset{F(d(N,C,1))}{\to} \cdots$$
2. Otherwise do the following:
   a. Fix a family $N = \{N_C\}_{C\,\in\,M_A}$, where each N_C is a projective resolution of C (§ 28), and write
   $$N_C = \cdots \overset{d(N,C,2)}{\to} B(N,C,1) \overset{d(N,C,1)}{\to} B(N,C,0) \overset{\varepsilon(N,C)}{\to} C \to 0$$
   b. For each $C \in M_A$, apply F to the modules $B(N,C,i)$ and homomorphisms $d(N,C,i)$ of N_C to construct the sequence
   $$X(N,C) = \cdots \to 0 \to F(B(N,C,0)) \overset{F(d(N,C,1))}{\to} F(B(N,C,1)) \overset{F(d(N,C,2))}{\to} \cdots$$
3. In either case, each $X(N,C)$ is an ascending sequence of A'-modules indexed by $\mathbf{Z}$, where $X(N,C)^i = F(B(N,C,i))$ for $i \geq 0$ and $X(N,C)_i = 0$ for $i < 0$. Each $X(N,C)$ is a cochain complex (§ 27), not necessarily exact (proof omitted).
   a. For each $C \in M_A$ and $i \in \mathbf{N}$, let $H(N,C)^i \in M_{A'}$ be the ith cohomology module (§ 27) of $X(N,C)$.
   b. For each $i \in \mathbf{N}$ there exists a unique functor $R^iF(N)\colon M_A \to M_{A'}$ such that $R^iF(N)(C) = H(N,C)^i$ (proof omitted).
   c. For any two families N and N', the functors $R^iF(N)$ and $R^iF(N')$ are naturally isomorphic (§ 13) (proof omitted). Therefore $R^iF(N) \sim R^iF(N')$, and we write the equivalence class as R^iF.

Fix a ring A and an A-module B.

1. The functor $- \otimes_A B\colon M_A \to M_A$ is covariant and right exact (§ 13), so it has left derived functors. The functors $\{L_i(- \otimes_A B)\}_{\,i\,\in\,\mathbf{N}}$ are called the **Tor functors** associated with B and written $\operatorname{Tor}_i^A(-,B)$.
2. The functor $\operatorname{Hom}_A(B,-)$ is covariant and left exact (§ 13), so it has right derived functors. The functors $\{R^i(\operatorname{Hom}_A(B,-))\}_{\,i\,\in\,\mathbf{N}}$ are called the **Ext functors** associated with B and written $\operatorname{Ext}^i_A(B,-)$.

30. Hilbert and Characteristic Polynomials

Let M be a class of A-modules, and let G be an abelian group. A map $f\colon M \to G$ is **additive** if for every short exact sequence (§ 11)

$$0 \to B \to C \to D \to 0$$

with members in M, we have $f(B) - f(C) + f(D) = 0$. For example, let A be a field, and let V_A be the class of finite-dimensional vector spaces over A. Then the map $\dim\colon V_A \to \mathbf{Z}$ additive, because for every linear map $f\colon C \to D$ with C and D in V_A, $\dim \ker f + \dim \operatorname{im} f = \dim C$ (proof omitted).

Let $A = \oplus_{i\,\in\,\mathbf{N}} A_i$ be a Noetherian (§ 20) graded ring (§ 25), and let $B = \oplus_{i\,\in\,\mathbf{N}} B_i$ be a finitely-generated graded A-module (§ 25).[8] Then each B_i is a finitely-generated A_0-module (proof omitted).

1. Let M_{A_0} be the class of all finitely-generated A_0-modules, and fix an additive map $\lambda\colon M_{A_0} \to \mathbf{Z}$. The **Poincaré series** $P(B,x)$ of B with respect to λ is the ordinary generating function (§ 16) of $\{\lambda(B_i)\}$, i.e.,

[8] For example, let C be a field, and let A and B both be the polynomial ring $C[x_1,\ldots,x_n]$. In this case, $A_0 = C$. This example is important in algebraic geometry.

$$P(B, x) = \sum_{i \in \mathbf{N}} \lambda(B_i) x^i \in \mathbf{Z}[[x]].$$

2. $P(B, x)$ is a rational function $\dfrac{p(x)}{q(x)}$ (§ 16), where $p(x) = \sum_{i=0}^{m} a_i x^i$ is a polynomial of degree m in $\mathbf{Z}[x]$, $q(x)$ is a product of n terms $\prod_{i=1}^{n}(1 - x^{e_i})$, and $p(x)$ and $q(x)$ have no common factors (proof omitted).
3. If $q(x) = (1 - x)^n$ in item 2 (i.e., $e_i = 1$ for all i), then for all $i \geq m$, we have

$$\lambda(B_i) = H(i) = \sum_{j=0}^{m} a_j \binom{d + i - j}{d},$$

where $d = n - 1$ and $\binom{a}{b} = \dfrac{a!}{b!(a-b)!}$. Expanding the sum and and rearranging terms makes $H(i)$ into a polynomial in i of degree d. It is called the **Hilbert polynomial** of B with respect to λ.

Fix a Noetherian local ring A. Let M be its maximal ideal, I be an M-primary ideal (§ 17), B be a finitely-generated A-module, and $F = (B_i)$ be a stable I-filtration of B (§ 24). Then

1. For all $i \geq 0$, B/B_i is of finite length (§ 20) (proof omitted).
2. For all sufficiently large i, $l(B/B_i)$ is a polynomial in i (proof omitted).

In the case $F = (I^i B)$, the polynomial in item 2 is denoted ${\chi^B}_I(i)$ when $B \neq A$. In the case $B = A$, it is denoted $\chi_I(i)$ and called the **characteristic polynomial** of I.

31. Regular Local Rings

Fix a Noetherian local ring A of dimension d. Let M be its maximal ideal, and let $F = A/M$. Then M/M^2 has the structure of an F-vector space because it is an A module that is annihilated by M. A is a **regular local ring** if it satisfies any of the following conditions:

1. $G_M(A) \cong F[x_1, \ldots, x_n]$, where G_M denotes the localization of G at M (§ 14), and $G_M(A)$ denotes the associated graded ring of G_M (§ 25).
2. M/M^2 has dimension d as an F-vector space.
3. M can be generated by d elements.

Conditions 1 through 3 are equivalent (each one implies the other two) (proof omitted).

A regular local ring is an integral domain (proof omitted).

The regular local rings of Krull dimension one (§ 20) are precisely the discrete valuation rings (§ 22) (proof omitted).

References

Atiyah, M.F. and Macdonald, I.G. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

Bocchino, R. *Calculus over the Complex Numbers.* https://rob-bocchino.net/Professional/Diversions.html.

Cartan, H. and Eilenberg, S. *Homological Algebra.* Princeton University Press, 1956.

Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry.* Third Edition. Springer Verlag, 1995.

Lang, S. *Undergraduate Algebra.* Springer Verlag, 1987.

Lang, S. *Algebra.* Third Edition. Springer Verlag, 2002.

Mac Lane, S. *Categories for the Working Mathematician.* Second Edition. Springer Verlag, 1998.

Matsumura, H. *Commutative Ring Theory.* Trans. M. Reid. Cambridge University Press, 1986.

Weibel, C. *An Introduction to Homological Algebra.* Cambridge University Press, 1994.

Index