Graduate Algebra

Arthur Li

November 27, 2022

Introduction

This collection of notes serve as a guide to modern abstract algebra, covering content from group theory to more advanced concepts such as commutative algebra. The notes combine knowledge from different sources, including course notes and various textbooks.

Prerequisites

These notes will assume no familiarity with any aspects of abstract algebra, and builds upon the foundation from Group Theory to more abstract topics such as Categories and Commutative Algebra. A good starting point will be the series on *Visual Group Theory by Professor Matthew Macauley*.

Familiarity with basic styles of proof is assumed (contradiction, contrapositive, etc.).

Organization and Sources

This section will be edited as the notes progress towards completion.

Unfinished Proofs

Unfinished proof at Proposition 2.1.1.6 (v)

Contents

1 Preliminaries

1.1 Introductory Ideas and Definitions

Definition 1.1.0.1. *Class* is a collection A of objects (elements) such that given any object x it is possible to determine if x is a member of A.

Definition 1.1.0.2. *Axiom of extensionality* asserts that two classes with the same elements are equal. Formally,

$$[x \in A \iff x \in B] \Rightarrow A = B$$

Definition 1.1.0.3. A class is defined to be a *set* if and only if there exists a class B such that $A \in B$.
A class that is not a set is called a *proper set*.

Definition 1.1.0.4. *Axiom of class formation* asserts that for any statement $P(y)$ in the first predicate calculus involve a variable y, there exists a class A such that $x \in A$ if and only if x is a set and the statement $P(x)$ is true. The class is denoted $\{x|P(x)\}$.

Definition 1.1.0.5. A class A is a *subclass* of class B ($B \subset A$) provided $\forall x \in A, x \in A \iff x \in B$.
A subclass A of a class B that is itself a set is called a *subset* of B.
The *empty or null set* (denoted $\emptyset$) is the set with no elements.

Definition 1.1.0.6. *Power axiom* asserts that for every set A the class $P(A)$ of all subsets of A is itself a set. $P(A)$ is the *power set* of A, denoted 2^A.

Definition 1.1.0.7. A *family of sets* indexed by (nonempty) class I is a collection of sets A_i, one for each $i \in I$ (denoted $\{A_i|i \in I\}$).
The *union* is defined as

$$\bigcup_{i \in I} A_i = \{x|x \in A_i \ for\ some\ i \in I\}$$

The *intersection* is defined as

$$\bigcap_{i \in I} A_i = \{x|x \in A_i \ for\ every\ i \in I\}$$

If $A \cap B = \emptyset$, then A and B are disjoint.

Definition 1.1.0.8. The *relative complement* of A in B is the following subclass of B:

$$B - A = \{x|x \in B \ and\ x \notin A\}$$

If all classes under discussion are subsets of some fixed set U (the universe of discussion), then $U - A = A'$ is the *complement* of A.

Definition 1.1.0.9. Given classes A and B, a *function / map / mapping* f from A to B (written $f : A \to B$ assigns to each $a \in A$ exactly one element $b \in B$.
Then b is the value of function at a, or the *image* of a, written $f(a)$.
A is the *domain* of the function, written $dom f$, and B is the *range* or *codomain*.
Two functions are *equal* if they have the same domain and range, and have the same value for each element of their common domain.

Definition 1.1.0.10. If $f : A \to B$ is a function and $S \subset A$, the function from S to B given by $a \mapsto f(a)$, for $a \in S$, is *restriction* of f to S, denoted $f|S : S \to B$.
If $S \in A$, the function $1_A|S : S \to A$ is the *inclusion map* of S into A.

Definition 1.1.0.11. Let $f : A \to B$ and $g : B \to C$ be functions. The *composite* of f and g is the function

$$\begin{aligned} g \circ f = gf : A \to C \\ a \mapsto g(f(a)),\ a \in A \end{aligned}$$

Definition 1.1.0.12. The *diagram of functions* is said to be commutative if $gf = h$, or if $kh = gf$.

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "h"'] & & B \arrow[dl, "g"] \\ & C & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[d, "g"] \\ C \arrow[r, "k"] & D \end{tikzcd}$$

Definition 1.1.0.13. Let $f : A \to B$ be a function. If $S \in A$, *the image of S under f* is the class

$$f(S)) = \{b \in B | b = f(a) \ for \ some \ a \in S\}$$

The class $f(A)$ is the *image of f*, denoted $im \ f$.
If $T \subset B$, the *inverse image of T* under f is the class

$$f^{-1}(T) = \{a \in A | f(a) \in T\}$$

Definition 1.1.0.14. A function $f : A \to B$ is said to be *injective* (or one-to-one) provided

$$\forall a, \ a' \in A, \ a \neq a' \Rightarrow f(a) \neq f(a')$$
$$f(a) = f(a') \Rightarrow a = a'$$

A function f is *surjective* (or on-to) provided $f(A) \approx B$; in other words, $\forall b \in B$, $b = f(a)$ for some $a \in A$.
A function f is *bijective* (or one-to-one correspondence) if it is both injective and surjective.

Definition 1.1.0.15. The map $g : B \to A$ is a *left inverse* of f if $gf = 1_A$.
The map $h : B \to A$ is a *right inverse* of f if $fb = 1_B$.
If a map $f : A \to B$ has both a left inverse g and a right inverse h, then

$$g = g1_B = g(fh) = (gf)h = 1_{\mathrm{A}}h = h$$

and $g = h$ is the *two-sided inverse*.

2 Group Theory

The study of modern abstract algebra begins with the simple abstract definition of a *group*, and quickly builds up complexity with structures of such objects. It is useful to isolate specific characteristics and the structure imposed on an object sharing similar characteristics. The structure of the algebraic object, made more precise with the concept of isomorphism, is used repeatedly in the study of groups.

2.1 Introduction to Groups

The basic algebraic structure to be studied in Group Theory is introduced in this subsection.

2.1.1 Basic Axioms

Definition 2.1.1.1.

(i) A *binary operation* $*$ on a set G is a function $* : G \times G \to G$. For any $a, b \in G$, write $a * b$ for $*(a, b)$.

(ii) A binary operation $*$ on a set G is *associative* if $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$

(iii) If $*$ is a binary operation on a set G, then $a, b \in G$ *commutes* if $a * b = b * a$. Then $*$ (or G) is commutative if $\forall a, b, \in G, a * b = b * a$.

(iv) For $H \subseteq G$, the restriction of $*$ to H is a binary operation on H, i.e., $\forall a, b, \in H, a * b \in H$.
H is *closed* under $*$.

The examples of operations are as follows.

Example 2.1.1.2.

(i) $+$ (addition) is a commutative binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(ii) $\times$ (multiplication) is a commutative binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(iii) $-$ (subtraction) is a non-commutative binary operation on $\mathbb{Z}$, where $-(a, b) = a - b$. The map $a \to -a$ is not a binary opeartion.

(iv) $-$ (subtraction) is not a binary operation on $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$. If $a < b$, then $a - b \notin \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$.

(v) Vector cross product of two vectors is a binary operation which is neither associative nor commutative.

We then have the following definition of groups.

Definition 2.1.1.3. A *group* is an ordered pair $(G, *)$ where G is a set, and $*$ is a binary operation on G satisfying the following exaioms:

(i) Associativity: $(a * b) * c = a * (b * c)\ \forall a, b, c, \in G$

(ii) Existence of identity: $e \in G$ such that $\forall a \in G$, we have $a * e = e * a = a$

(iii) Existence of inverse: $a^{-1} \in G$ such that $\forall a \in G$, we have $a * a^{-1} = a^{-1}a = e$

The group is *abelian* if $a * b = b * a\ \forall a, b, \in G$. The group is a *finite group* if G is a finite set.
Axiom (ii) ensures a group is always nonempty.

Example 2.1.1.4.

(i) The basic groups are $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ with $e = 0$ and $a^{-1} = -a\ \forall a$

(ii) The multiplicative groups are $(\mathbb{Q} - \{0\}, \times), (\mathbb{R} - \{0\}, \times), (\mathbb{C} - \{0\}, \times), (\mathbb{Q}^+, \times), (\mathbb{R}^+, \times)$ with $e = 1$ and $a^{-1} = \frac{1}{a}$. Note that $(\mathbb{Z} - \{0\}, \times)$ is not a group as the element 2 (for instance) does not have an inverse

(iii) The additive group consisting of vector space V, i.e., $(V, +)$

(iv) For $n \in \mathbb{Z}^+$, $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group. The identity is $e = \overline{0}\ \forall \overline{a} \in \mathbb{Z}/n\mathbb{Z}$. The inverse of $\overline{a}$ is $\overline{-a}$. Hence the group operation is addition of classes $\mod n$

(v) For $n \in \mathbb{Z}^+$, $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ of equivalence classes $\overline{a}$ which have multiplicative inverses $\mod n$ is an abelian group under multiplication of residue classes. The identity is $e = \overline{1}$. By definition of $(\mathbb{Z}/n\mathbb{Z})^\times$, each element has a multiplicative inverse. Group operation is multiplication of classes $\mod n$.

Definition 2.1.1.5. If $(A, *)$ and $(B, \diamond)$ are groups, then we can from new group $A \times B$, which is the *direct product*, with elements are in Cartesian product $A \times B = \{(a, b) \mid a \in A, b \in B\}$, with operation defined component-wise: $(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2)$

We now prove two basic results that allows discussion of the identity and inverse of an element.

Proposition 2.1.1.6. *If G is a group under operation $*$, then*

(i) the identity of G is unique

(ii) for each $a \in G$, a^{-1} is uniquely determined

(iii) $(a^{-1})^{-1} = a \ \forall a \in G$

(iv) $(a * b)^{-1} = (b^{-1}) * (a^{-1})$

(v) for any $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 * a_2 * \cdots a_n$ is independent of how the expression is bracketed (the generalised associative law)

Proof.

(i) If f, g are both identities, then by Definition 2.1.1.3(ii) of a group $f * g = f$ (with $a = f, e = g$). By the same axiom, $f * g = g$ (with $a = g, e = f$). Hence, $f = g = e$, and the identity is unique.

(ii) Assume b, c are both inverses of a, and let e be the identity of G. By Definition 2.1.1.3(iii), $a * b = e$ and $c * a = e$, thus

$$
\begin{aligned}
c &= c * e && \text{(by definition of } e \text{ in Definition 2.1.1.3(iii))} \\
&= c * (a * b) && \text{(since } e = a * b) \\
&= (c * a) * b && \text{(associative law)} \\
&= e * b && \text{(since } e = c * a) \\
&= b && \text{(by Definition 2.1.1.3(iii))}
\end{aligned}
$$

(iii) By part (ii), a has a unique inverse. By definition of a^{-1}, with a and a^{-1} interchanged, this shows that a satisfies the defining property for the inverse of a^{-1}, hence a is the inverse of a^{-1}.

(iv) Let $c = (a * b)^{-1}$. By definition of c, $(a * b) * c = e$. By associative law, $a * (b * c) = e$.
Multiply both sides on left by a^{-1} to get $a^{-1} * (a * (b * c)) = a^{-1} * e$.
By associative law and definition of e, $(a^{-1}) * (b * c) = a^{-1}$, hence $e * (b * c) = a^{-1}$.
Thus $b * c = a^{-1}$. Multiply both sides on left by b^-1.

$$
\begin{aligned}
b^{-1} * (b * c) &= b^{-1} * a^{-1} \\
(b^{-1} * b) * c) &= b^{-1} * a^{-1} \\
e * c &= b^{-1} * a^{-1} \\
c &= b^{-1} * a^{-1}
\end{aligned}
$$

(v) By induction on n. *PROOF NOT COMPLETE. TBD.*

□

We use the notation ab for $a \cdot b$, and identity of an abstract group G as 1 for brevity.
For any group with $\cdot$ operation, $x \in G$ and $n \in \mathbb{Z}^+$, we denote $xx \cdots x$ (n terms) with x^n, $x^{-1}x^{-1} \cdots x^{-1}$ (n terms) by x^{-n}. The identity of G is then denoted $x^0 = 1$.

Proposition 2.1.1.7. *Let G be a group, and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation law holds in G, i.e.,*

(i) if $au = av$ then $u = v$, and

(ii) if $ub = vb$, then $u = v$

Proof. Solve $ax = b$ by multiplying both sides on left by a^{-1} and simplify to get $x = a^{-1}b$. Uniqueness of x follows as a^{-1} is unique. Similarly, if $ya = b$, then $y = ba^{-1}$. If $au = av$, multiply both sides on left by a^{-1} to get $u = v$. Similarly, the right cancellation law holds. □

A consequence of the proposition is that if a is any element of G, and for some $b \in G$, $ab = e$ or $ba = e$, then $b = a^{-1}$, i.e., we do not have to show both equations hold.
Also, if for some $b \in G$, $ab = a$ (or $ba = a$), then b must be the identity of G. We do not have to check $bx = xb = x$ for all $x \in G$

Definition 2.1.1.8. For group G and $x \in G$, the *order of x* is the smallest positive integer n such that $x^n = 1$, denoted $|x|$. If no positive power of x is the identity, then $|x| = \infty$.

Example 2.1.1.9.

(i) In multiplicative groups $\mathbb{R} - \{0\}$ or $\mathbb{Q} - \{0\}$, the element -1 has order 2, and other non-identity elements have infinite order.
(ii) In additive groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, every nonzero (non-identity) element has infinite order.
(iii) The additive group $\mathbb{Z}/9\mathbb{Z}$'s element $\overline{6}$ has order 3, $\overline{5}$ has order 9.

Definition 2.1.1.10. Let $G = g_1, g_2, \ldots, g_n$ be a finite group with $g_1 = 1$. The *multiplication table* or *group table* of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

2.1.2 Dihedral Groups

This family of groups consists of elements which are symmetries of geometric objects. First, we introduce the notion of generators and relations as they provide simple ways of describing and computing groups.

Definition 2.1.2.1. Any equations in a general group G that generators satisfy are called *relations* in G.
If a group G is generated by a subset S, and there is some collection of relations, say $R_1, R_2, \ldots, R_m$ (where each R_i is an equation in the elements from $S \cup \{1\}$ such that any relations among the elements of S can be deduced from these, then this is a *presentation of G*, written:

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle$$

Note that in an arbitrary presentation, it may be difficult to tell when two elements of the group are equal. It may not be evident what the order of presented group is, or even whether the group is finite or infinite.
Also even in quite simple presentation, some 'collapsing' may occur as relations are intertwined in some unobvious way. There may be 'hidden' or implicit relations that are not explicitly given in the presentation, but rather are the consequences of the specified ones.

Definition 2.1.2.2. A *dihedral group* is the group of symmetries of a regular n-gon, denoted

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

where r is a rotation counterclockwise about the origin by $\frac{2\pi}{n}$,
s is a reflection about the line of symmetry through the vertex 1

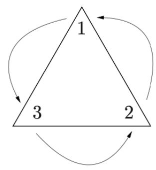

Figure 1: Example of an equilateral triangle as a Dihedral Group D_6

Remark 2.1.2.3. The properties of dihedral groups are as follows:

(i) $|r| = n$, as $1, r, \ldots, r^n$ are all distint, and $r^n = 1$
(ii) $|s| = 2$, as $s^2 = 1$
(iii) $s \neq r^i$ for any i
(iv) $sr^i \neq sr^j$ for all $0 \leq i, j \leq n-1$, with $i \neq j$
Hence $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$.
Each element can be written uniquely in the form $s^k r^i$ for $k \in 0, 1$, $0 \leq i \leq n-1$.
(v) $rs = sr^{-1}$. Hence r and s do not commute, and D_{2n} is non-abelian.
(vi) $r^i s = sr^{-i}$ for all $0 \leq i \leq n$

2.1.3 Symmetric Groups

Definition 2.1.3.1. Let Ω be any nonempty set, and S_Ω be the set of all bijections from Ω to itself (the set of all permutations of Ω. Then the set S_Ω is a group under function composition $\circ$.
The identity of S_Ω is the permutation 1 defined by $1(a) = a \ \forall a \in \Omega$.
For every permutation $\sigma : \Omega \to \Omega$ there is a 2-sided inverse function $\sigma^{-1} : \Omega \to \Omega$ satisfying
$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. Thus all group axioms hold for $(S_\Omega, \circ)$, the *symmetric group on the set Ω*.
The elements of S_Ω are the permutations of Ω, not elements of Ω itself.
If $\Omega = \{1, 2, \ldots, n\}$ is a finite set, then S_n is the *symmetric group of degree n*.

The group S_n plays an important role as a means of illustrating and motivating the general theory.

Theorem 2.1.3.2. *The order of S_n is $n!$.*

Proof. The permutations of $\{1, 2, \ldots, n\}$ are precisely the injective functions of this set to itself as it is finite. We count the number of injective functions. For $\sigma(n)$, this is precisely $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$ possible injective functions from $\{1, 2, \ldots, n\}$ to itself. $\square$

We now introduce the notation for writing elements σ of S_n with cycle decomposition.

Definition 2.1.3.3. A *cycle* is a string of integers which represents the elements of S_n which cyclically permutes these integers and fixes other integers.
The cycle $(a_1\ a_2\ \cdots\ a_m)$ is the permutation which sends a_i to a_{i+1}, $1 \leq i \leq m-1$ and sends a_m to a_1.
In general, for each $\sigma \in S_n$, the numbers from 1 to n will be rearranged and grouped into k cycles of the form

$$(a_1\ a_2\ \cdots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \cdots\ a_{m_2})\cdots(a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \cdots\ a_{m_k})$$

Remark 2.1.3.4. In Cauchy's two line notation, the natural order of elements of Ω, say $x_1, x_2, \ldots, x_n$ is listed in the first row, then the images of each element in the second row.

$$\sigma = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}$$

We may omit the first row and write the permutation in one-line notation as:

$$\begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}$$

Definition 2.1.3.5. The *length* of a cycle is the number of integers which appear in it.
A cycle of length t is called a *t-cycle*.
Two cycles are *disjoint* if they have no numbers in common.
The inverse permutation is given by reversing the order of elements in the permutation's cycles.

Algorithm 2.1.3.6. The *cycle decomposition algorithm* is as follows:

1. Write an opening bracket then select an arbitrary element x of Ω and write it down: $(x$
2. Trace the orbit of x, write down its values over successive applications of σ: $(x\ \sigma(x)\ \sigma(\sigma(x))\cdots$
3. Repeat until the value returns to x and write a closing parenthesis rather than x: $(x\ \sigma(x)\ \sigma(\sigma(x))\cdots)$
4. Now continue with an element y of Ω not yet written down, and proceed in the same way: $(x\ \sigma(x)\ \sigma(\sigma(x))\cdots)(y\cdots)$
5. Repeat until all elements of Ω are written in cycles.

2.1.4 Matrix Groups

Matrix groups have coefficients that come from fields. A field is the smallest mathematical structure which all arithmetic operations $(+, -, \times, \div)$ (division by nonzero elements) can be performed.

Definition 2.1.4.1. A *field* is a set F with two binary operations $+, \cdot$ on F such that $(F, +)$ is an abelian group (with identity 0), and $(F - \{0\}, \cdot)$ is also an abelian group. The following distributive law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \forall a, b, c \in F$$

For any field F, let $F^\times = F - \{0\}$

Definition 2.1.4.2. A *matrix group* is a group G consisting of invertible matrices over a field K, with the operation of matrix multiplication.
The *general linear group* of degree n is the set of $n \times n$ invertible matrices with matrix multiplication, denoted $GL_n(\mathbf{F})$. If $n \geq 2$, then the group $GL_n(\mathbf{F})$ is not abelian.
The *special linear group* is a subgroup of $GL_n(\mathbf{F})$, consisting of matrices with determinant 1, denoted $SL_n(\mathbf{F})$.

We dive deeper into the results in Modules and Vector Spaces in Section 4.

2.1.5 The Quaternion Group

Definition 2.1.5.1. The *quaternion group* is defined by $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, with product $\cdot$ computed as follows:

$$\begin{aligned}
1 \cdot a = a \cdot 1 &= a && \forall a \in Q_8 \\
(-1) \cdot (-1) = 1, \ \ (-1) \cdot a = a \cdot (-1) &= -a && \forall a \in Q_8 \\
i \cdot i = j \cdot j = k \cdot k &= -1 \\
i \cdot j = k, \qquad j \cdot i &= -k \\
j \cdot k = i, \qquad k \cdot j &= -i \\
k \cdot i = j, \qquad i \cdot k &= -j
\end{aligned}$$

Note that Q_8 is a non-abelian group of order 8.

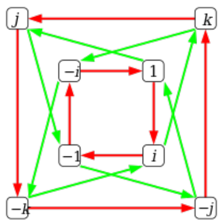

Figure 2: The Cayley diagram of the Quaternion Group Q_8.

2.1.6 Homomorphism and Ismomorphism

We define what makes two group 'look the same', i.e., having exactly the same group-theoretic structure (an isomorphism) in this section.

Definition 2.1.6.1. Let $(G, *), (H, \diamond)$ be groups. A map $\varphi : G \to H$ such that

$$\varphi(x * y) = \varphi(x) \diamond \varphi(y), \quad \forall x, y \in G$$

is a *homomorphism*.

If the group operations for G, H are not explicitly written, then this is simply $\varphi(xy) = \varphi(x)\varphi(y)$, but the product xy on the left is computed in G, while the product $\varphi(x)\varphi(y)$ is computed in H.
Intuitively, a map φ is a homomorphism if it respects the group structures of its domains and codomains.

Definition 2.1.6.2. The map $\varphi : G \to H$ is a *isomorphism* and G and H are *isomorphic*, denoted $G \cong H$, if:

(i) φ is a homomorphism (i.e., $\varphi(xy) = \varphi(x)\varphi(y)$), and

(ii) φ is a bijection.

Intuitively, G and H are the same group, except the elements and operations may be written different in G and H. Thus, any property which G has which only depends on group structure of G also holds for H.

Definition 2.1.6.3. Let $\mathscr{G}$ be any nonempty collection of groups. Then the relation $\cong$ is an equivalent relation on $\mathscr{G}$, and the equivalence classes are called *isomorphism classes*.

Example 2.1.6.4.

(i) For any group G, $G \cong G$, the identity map.

(ii) The exponential map $\exp : \mathbb{R} \to \mathbb{R}^+$, defined by $\exp(x) = e^x$, is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$

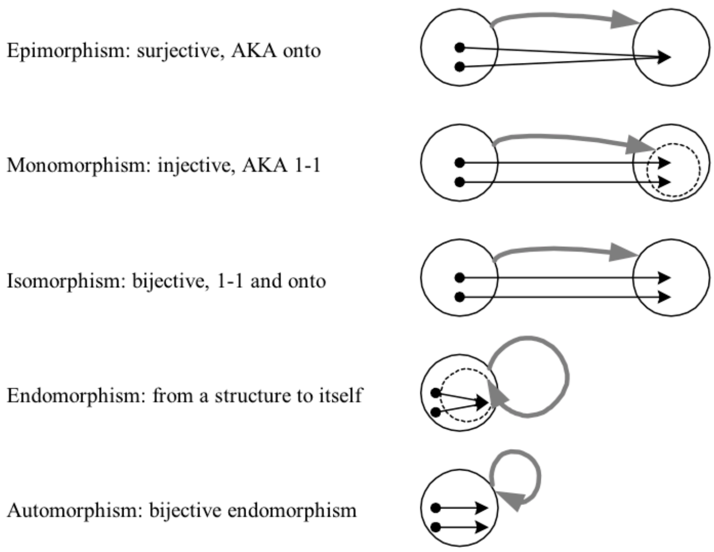

Figure 3: Comparison of all types of morphism.

2.1.7 Group Actions

Group action is a powerful tool for proving theorems for abstract groups, and for unravelling the structure of the groups. This is a method for studying an algebraic object by seeing how it can act on other structures.

Definition 2.1.7.1. A *(left) group action* of a group G on a set A is a map from $G \times A$ to A, written as $g \cdot a \; \forall g \in G$ and $a \in A$, satisfying the following properties:

(i) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a \; \forall g_1, g_, 2 \in G$ and $a \in A$, and

(ii) $1 \cdot a = a \; \forall a \in A$

A *right group action* is similarly defined, with group elements on the right of set elements.
Hence, for each fixed $g \in G$, we get a map σ_g defined by:

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a$$

Proposition 2.1.7.2.

(i) For each $g \in G$, σ_g is a permutation of A, and

(ii) the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism

Proof.

(i) To show that σ_g is a permutation of A, we show that as a set map from A to A, it has a 2-sided inverse $\sigma_{g^{-1}}$. For all $a \in A$:

$$\begin{aligned}
(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) && \text{(by definition of function composition)} \\
&= g^{-1} \cdot (g \cdot a) && \text{(by definition of } \sigma_{g^{-1}} \text{ and } \sigma_g) \\
&= (g^{-1} g) \cdot a && \text{(by property (1) of an action)} \\
&= 1 \cdot a = a && \text{(by property (2) of an action)}
\end{aligned}$$

Hence, $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map from A to A, with a 2-sided inverse. Since g is arbitrary, we may interchange the roles of g and g^{-1} to obtain $\sigma_g \circ \sigma_{g^{-1}}$, which is also the identity map on A. Hence σ_g has a 2-sided inverse, hence is a permutation of A.

(ii) let $\varphi : G \to S_A$ be defined by $\varphi(g) = \sigma_g$. Note that (i) has shown that σ_g is indeed an element of S_A. To see that φ is a homomorphism, we must prove $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$. For all $a \in A$:

$$\begin{aligned}
\varphi(g_1 g_2)(a) &= \sigma_{g_1 g_2}(a) && \text{(by definition of } \varphi) \\
&= (g_1 g_2) \cdot a && \text{(by definition of } \sigma_{g_1 g_2}) \\
&= g_1 \cdot (g_2 \cdot a) && \text{(by property (1) of an action)} \\
&= \sigma_{g_1}(\sigma_{g_2}(a)) && \text{(by definition of } \sigma_{g_1} \text{ and } \sigma_{g_2}) \\
&= (\varphi(g_1) \circ \varphi(g_2))(a) && \text{(by definition of } \varphi)
\end{aligned}$$

□

Definition 2.1.7.3. The *permutation representation* associated to the group action is the homomorphism from G to S_A. Let $\varphi : G \to S_A$ be any homomorphism from a group G to the symmetric group on a set A, then the map $G \times A \mapsto A$ is defined by

$$g \cdot a = \varphi(g)(a) \ \ \forall g \in G, \mathbf{a} \in A$$

Definition 2.1.7.4. Let $ga = a$ for all $g \in G, a \in A$. Then this is the *trivial action*, and G is said to *act trivially* on A. The distinct elements of G induce the same permutation on A. The associated permutation representation $G \to S_A$ is the trivial homomorphism which maps every element of G to the identity.

Definition 2.1.7.5. If G acts on a set B and distinct elements of G induce distinct permutations of B, then the action is *faithful*. The associated permutation representation is injective.
The *kernel* of the action G on B is $\ker = \{g \in G \mid gb = b \ \forall b \in B\}$.

2.2 Subgroups

To study the structure of a group, a basic method is to study quotients of an object (to collapse a group into a smaller group).

2.2.1 Centralisers, Normalisers, Stabilisers, Kernels

Definition 2.2.1.1. Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses. If H is a subgroup of G, this is denoted $H \leq G$.

Example 2.2.1.2.

(i) $\mathbb{Z} \leq \mathbb{Q}$, and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.

(ii) Any group G has two subgroups: $H = G$, and $H = \{1\}$ (the *trivial subgroup*).

(iii) If $H \leq G$ and $K \leq H$, then $H \leq G$ by transitivity property.

Proposition 2.2.1.3. *(The Subgroup Criterion)*

2.3 Quotient Groups, Homomorphisms

2.4 Group Actions

2.5 Direct and Semidirect Products, Abelian Groups

This section introduces methods to construct larger groups from smaller ones with direct and semidirect product. This then allow us to completely classify all finite abelian groups with the Fundamental Theorem on Finitely Generated Abelian Groups.

2.5.1 Direct Products

Definition 2.5.1.1. The *direct product* $G_1 \times G_2 \times \cdots$ of groups $G_1, G_2, \ldots$ with operations $*_1, *_2, \ldots$ is the set of sequences $(g_1, g_2, \ldots)$ where $g_i \in G_i$, with operation defined component-wise:

$$(g_1, g_2, \ldots) * (h_1, h_2, \ldots) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots)$$

Example 2.5.1.2.

(i) Let $G_i = \mathbb{R}$ for $i = 1, 2, \ldots, n$. Then $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ (n-factors) is the Euclidean n-space $\mathbb{R}^n$ with vector addition $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$

(ii) For groups forming direct product, let $G_1 = \mathbb{Z}, G_2 = S_3, G_3 = GL_2(\mathbb{R})$, where the group operations are addition, composition, and matrix multiplication. Then the operation $G_1 \times G_2 \times G_3$ is defined to be

$$(n, \sigma, \begin{pmatrix} a & b \\ c & d \end{pmatrix})(m, \tau, \begin{pmatrix} p & q \\ r & s \end{pmatrix}) = (n + m, \tau \circ \sigma, \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix})$$

Proposition 2.5.1.3. *If $G_1, \ldots, G_n$ are groups, then their direct product is a group of oder $|G_1|\,|G_2| \cdots |G_n|$. If any G_i is infinite, so is the direct product.*

Proof. Let $G = G_1 \times G_2 \times \cdots \times G_n$.
The group axioms hold for G since each axiom is a consequence of the fact that the same axiom in Proposition 2.1.1.6 holds in each factor G_i, and the operation on G is defined component-wise.
The identity of G is the n-tuple $(1_1, 1_2, \ldots, 1_n)$, where each 1_i is the identity of G_i.
The inverse of $(g_1, g_2, \ldots, g_n)$ is $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$, where each g_i^{-1} is the inverse of g_i in G.
Hence the formula for the order of G is clear. $\square$

Rearranging factors of the direct product results in a direct product isomorphic to the original one.

Proposition 2.5.1.4. *Let $G_1, G_2, \ldots, G_n$ be groups, and let $G = G_1 \times \cdots \times G_n$ be their direct product.*

(i) For each fixed i, the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and the arbitrary elements of G_i in position i is the subgroup of G isomorphic to G_i:

$$G_i \cong \{(1, 1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\} \text{ (where } g_i \text{ is at the } i^{\text{th}} \text{ position)}$$

If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

(ii) For each fixed i, define $\pi_i : G \to G_i$ by

$$\pi_i((g_1, g_2, \ldots, g_n)) = g_i$$

Then π_i is a surjective homomorphism with

$$\begin{aligned} \ker \pi_i &= \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) \ \mid g_j \in G_j \ \forall j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$

where 1 appears at position i.

(iii) Under the identifications in part (i), if $x \in G$ and $y \in G_j$ for some $i \neq j$, then $xy = yx$

2.6 Further Topics in Group Theory

2.6.1 p-groups, Nilpotent Groups, Solvable Groups

3 Ring Theory

3.1 Basic Axioms

Definition 3.1.0.1. A *ring* is a nonempty set R with two binary operations $+$ (addition) and $\times$ (multiplication), $(R, +, \times)$, such that:

(i) $(R, +)$ is an additive abelian group with 0 as the additive identity

(ii) the binary operation $\times$ is associative:

$$(a \times b) \times c = a \times (b \times c),\ \forall a, b, c \in R$$

(iii) left and right distributive laws:

$$(a + b) \times c = (a \times c) + (b \times c)\ \forall a, b, c \in R$$
$$a \times (b + c) = (a \times c) + (b \times c),\ \forall a, b, c \in R$$

If in addition, $a \times b = b \times a\ \forall a, b \in R$, then R is a *commutative ring*.

Definition 3.1.0.2. The ring R has a *multiplicative identity* if there is an element $1_R \in R$ such that

$$1_R \times a = a \times 1_R = a,\ \forall a \in R$$

The ring R has a *additive identity* if there is an element $0_R \in R$ such that

$$a - b = a + (-b) = 0_R$$

where $-b$ is the *additive inverse*.

Definition 3.1.0.3. A *division ring* R is a ring such that:

(i) R has a multiplicative identity 1_R;

(ii) $1_R \neq 0_R$; and

(iii) $\forall$ nonzero element $a \in R \backslash \{0\}$ has a unique multiplicative inverse a^{-1} such that

$$aa^{-1} = 1 = a^{-1}a$$

Definition 3.1.0.4. A *field* is a division ring which is commutative.
If R is a division ring (field), then $(R, \times)$ is a (commutative) *multiplicative group*, $R^{\times} = R\backslash\{0\}$.

Definition 3.1.0.5. Let $F = (F, +, \times)$ be a field. A nonempty subset $E \subseteq F$ is a *subfield* if:

(i) $(E, +)$ is an additive subgroup of $(F, +)$;

(ii) E is closed under multiplication $\times$: $a, b \in E \Rightarrow a \times b \in E$;

(iii) $1_F \in E$; and

(iv) $a \in E\backslash\{0\} \Rightarrow a^{-1} \in E$

Remark 3.1.0.6. The *trivial ring* is $\{0\}$.
The *integer ring* is $(\mathbb{Z}, +, \times)$ with 1, but is neither a division ring or field.
$n\mathbb{Z} = \{ns | s \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$.
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a commutative ring with 1 for $n \geq 2$.

Remark 3.1.0.7. The 2-dimensional vector space

$$\mathbb{Q}[\sqrt{D}] = \mathbb{Q} + \mathbb{Q}\sqrt{D} = \{a + b\sqrt{D} | a, b \in \mathbb{Q}\}$$

with $\mathbb{Q}$-basis $\{1, \sqrt{D}\}$ is a *Quadratic Field*.
Define $\mathbb{Q}(\sqrt{D}) = \{\frac{a+b\sqrt{D}}{c+d\sqrt{D}} | a, b, c, d \in \mathbb{Q}, c + d\sqrt{D} \neq 0\}$.
Then $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}[\sqrt{D}]$.
More generally, for a field F,

$$\mathbb{Q}(F) = \{\frac{\alpha}{\beta} = \alpha\beta^{-1} |\ \alpha\beta, \in F, \beta \neq 0\} = F$$

Remark 3.1.0.8. Let $H = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$ be the 4-dimensional vector space over $\mathbb{R}$ with $\mathbb{R}$-basis $(1, i, j, k)$.
The multiplication is extended linearly by distributive law:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = k &= -ji \\ jk = i &= -kj \\ ki = j &= -ik \end{aligned}$$

Then H is a *Real Quaternion Ring*.
The *Rational Hamilton Quaternion Ring* is:

$$H_{\mathbb{Q}} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k = \{a + bi + cj + dk|\ a, b, c, d \in \mathbb{Q}\}$$

Remark 3.1.0.9. Let $\mathbb{R}V[x] = \{f : \mathbb{R} \to \mathbb{R}\}$ be the set of all real-valued functions.
Let $x \mapsto c(x) = c$ be a constant function.
For $f, g \in \mathbb{R}V[x]$, the natural addition is

$$x \mapsto (f + g)(x) = f(x) + g(x)$$

The multiplication (not composition) is

$$x \mapsto (fg)(x) = f(x)g(x)$$

$(\mathbb{R}V[x], +, \times)$ is a commutative *(real valued-function) ring* with multiplicative identity 1 being the constant function 1.

Definition 3.1.0.10. Let R be a ring with $1 \neq 0$. An element $u \in R$ is a *unit* if it has a multiplicative identity inverse u' such that $uu' = 1 = u'u$.
The *set of all units* of R are

$$U(R) = \{u \in R | u \text{ is a unit}\}$$

The *multiplicative group of units of the ring* R is $(U(R), \times)$.

Remark 3.1.0.11. More generally, let X be a set and R be a ring. Let $X_{\text{to}}R := \{f : X \to R\}$ be the set of all maps between X and R. Then for $f, g \in X_{\text{to}}R$, there are natural addition $f + g$ and multiplication fg $(x \mapsto f(x)g(x))$.
Then $(X_{\text{to}}R, +, \times)$ is a ring, called the *R-Valued Function Ring*.
If R has 1 then so does $X_{\text{to}}R$. If R is commutative then so does $X_{\text{to}}R$.
Every $c \in R$ defines a constant function (an element in $X_{\text{to}}R$)

$$\begin{aligned} c : X &\to R \\ x &\mapsto c(x) = c \end{aligned}$$

Identify R with the subset of $X_{\text{to}}R$ of constant function. Then R is a subring of $X_{\text{to}}R$.

Remark 3.1.0.12. Let $n \geq 2$. Then $U(\mathbb{Z}/n\mathbb{Z})$ is a commutative multiplicative group of order

$$|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$$

Hence $\varphi(n)$ is the *Euler's φ-function*,

$$\varphi(n) = |\{1 \leq s \leq n | gcd(s, n) = 1\}|$$

Definition 3.1.0.13. An *Integral Domain* is a commutative ring with $1 \neq 0$ such that
$\forall a, b, \in R,\ ab = 0 \Rightarrow a = 0 \text{ or } b = 0$, or equivalently, $\forall a, b \in R,\ a \neq 0,\ b \neq 0 \Rightarrow ab \neq 0$.
$\mathbb{Z}$ is an integral domain.
Every field is an integral domain.

Definition 3.1.0.14. Let R be a ring. A nonzero element $a \in R$ is a *zero divisor* if there is a nonzero $b \in R$ such that either $ab = 0$ or $ba = 0$.
A commutative ring R with 1 is an integral domain if and only if R as no zero divisors.

Proposition 3.1.0.15. *Let R be a ring with $1 \neq 0$. R is an integral domain if and only if cancellation law holds:*

$$\forall a, b, c \in R,\ c \neq 0,\ ca = cb \Rightarrow a = b$$

Corollary 3.1.0.16. *Let R be a finite integral domain, i.e., R is an integral domain with the cardinality $|R| < \infty$. Then R is a field.*

Proposition 3.1.0.17. *Let $n \geq 2$. Then the following are equivalent:*

(i) $\mathbb{Z}/n\mathbb{Z}$ is a field

(ii) $\mathbb{Z}/n\mathbb{Z}$ is an integral domain

(iii) n is a prime

Definition 3.1.0.18. Let R be a ring. A nonempty subset $S \subseteq R$ is a *subring* of R if:

(i) $(S, +)$ is an additive subgroup of $(R, +)$ and

(ii) S is closed under multiplication

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Proposition 3.1.0.19. *(Subring Criterion) Let R be a ring and $S \subseteq R$ a nonempty subset. Then the following are equivalent:*

(i) S is a subring of R

(ii) S is closed under subtracting and multiplication:

$$a, b \in S \Rightarrow ab \in S$$
$$a - b = a + (-b) \in S$$

Remark 3.1.0.20. Being a subring is a transitive condition. If R is a subring of S and S is a subring of T, then R is a subring of T.
If both S_i are subring of R and $S_1 \subseteq S_2$, then S_1 is a subring of S_2.

Remark 3.1.0.21. *(Subring without 1)* If R is a ring with $1 = 1_R$ then a subring $S \subseteq R$ may not contain 1, i.e., $m\mathbb{Z} = ms|s \in \mathbb{Z}, |m| \geq 2$ is a subring of $\mathbb{Z}$ which does not contain 1.

Remark 3.1.0.22. *(Intersection of subrings)* Let R_α $(\alpha \in \Sigma)$ be a (not necessarily finite or countable) collection of subrings of a ring R. Then the intersection $\bigcap\limits_{\alpha \in \Sigma} R_\alpha$ is a subring of R.
Generally, the union of subrings may not be a subring.

Remark 3.1.0.23. *(Union of ascending subrings)* Let $R_1 \subseteq R_2 \subseteq \cdots$ be an ascending chain of subrings R_i of a ring R. Then the union $\bigcup\limits_{i=1}^{\infty} R_\alpha$ is a subring of R.

Remark 3.1.0.24. *(Addition of subrings)* Let R be a ring and let R_i be subrings of R.
Then the addition $R_1 + \cdots + R_n$ is closed under subtraction, but may not be closed under multiplication, hence may not be a subring of R.

Remark 3.1.0.25. *(Integral domain is a subring of a field)*
Let F be a field. Let $R \subseteq F$ be a subring such that $1 \in R$. Then R is an integral domain.
Every integral domain R is a subring of some field $\mathbb{Q}(R)$ (the fractional field of R).

Remark 3.1.0.26. *(Product of Rings)* let $n \geq 1$ and let $R_i = (R_i, +, \times)$ $(i = 1, \ldots, n)$ be rings.
Then the direct product is a ring,

$$R = R_1 \times \cdots \times R_n$$
$$(a_1, \ldots, a_n) \times (a'_1, \ldots, a'_n) = (a_1 a'_1, \ldots, a_n a'_n)$$

The unit subgroups has the relation

$$U(R) = U(R_1) \times \cdots \times U(R_n)$$

3.2 Examples of Rings

Definition 3.2.0.1. The *polynomial ring $R[x]$ over a ring R* is $(R[x], +, \times)$, where

$$R[x] = \{\sum_{j=0}^{d} b_j x_j | d \geq 0,\ b_j \in \mathbb{R}\}$$

There are natural addition and multiplication operations for polynomials.

Remark 3.2.0.2. Let R be a commutative ring with 1. Let $S := R[x]$ be the polynomial ring over R.

(i) R is a subring of S which consists of constant polynomial functions.

(ii) $0_S = 0_R$

(iii) S contains $1 = 1_S$, and $1_S = 1_R$.

Proposition 3.2.0.3. *(Polynomial ring over integral domain) Let R be an integral domain. Let $f(x), g(x) \in R[x]$. Then*

(i) $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

(ii) $U(R[x]) = U(R)$. Namely, $g(x)$ is a unit of $R[x]$ if and only if $g = a_0 \in R$ (constant polynomial) with a_0 a unit in R.

(iii) $R[x]$ is an integral domain

Remark 3.2.0.4. The matrix ring of $n \times n$ square matrices with entries in the ring R is defined as $(M_n(R), +, \times)$, where

$$M_n(R) = \left\{ A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} | a_{ij} \in R \right\}$$

If $A = (a_{ij}), B = (b_{ij}) \in M_n(F)$, then $A + B = (a_{ij} + b_{ij}), AB = (c_{ij})$ where $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.
$A = (a_{ij}) = Diag[a_{11}, \ldots, a_{nn}]$ is a diagonal matrix if $a_{ij} = 0\ (i \neq j)$.
$A = (a_{ij}) = Diag(a_1, \ldots, a_n)$ is a scalar matrix if $a_{ii} = a \in R\ \forall i$, and $a_{ij} = 0\ (i \neq j)$.
$A = (a_{ij})$ is an upper triangular matrix if $a_{ij} = 0\ (i < j)$. The lower triangular matrix is defined similarly.

Remark 3.2.0.5. Let R be a ring and $S = M_n(R)$ the matrix ring with entries in R. Then

(i) $0_S = (a_{ij})$ where $a_{ij} = 0$ (the zero matrix)

(ii) If R has $1 = 1_R$, then S also has $1 = 1_S$ with $1_S = Diag[1_R, \ldots, 1_R]$

(iii) The set $S_{c_n}(R) = \{Diag[a, \ldots, a] | a_i \in R\}$ of all scalar matrices in $M_n(R)$ is a subring of $M_n(R)$. There is a natural ring isomorphism $R \cong S_{c_n}(R)$.

(iv) The set $D_n(R) = \{Diag[a_1, \ldots, a_n] | a_i \in R\}$ of all diagonal matrices in $M_n(R)$ is a subring of $M_n(R)$. There is a natural ring isomorphism $D_n(R) \cong R^n := R \times \cdots \times R$ (n times).

(v) The set $UT_n(R) := \{(a_{ij} | (a_{ij} \in R, (a_{ij} = 0 (\forall\ i > j))\}$ of all upper triangular matrices in $M_n(R)$ is a subring of $M_n(R)$. Similarly, the set $LT_n(R)$ of all lower triangular matrices in $M_n(R)$ is a subring of $M_n(R)$.

(vi) If R is a subring of R, then $M_n(T)$ is a subring of $M_n(R)$

(vii) Even if R is commutative, $M_n(R)$ may not be commutative when $n \geq 2$.

(viii) If $n \geq 2$, then $M_n(R)$ is not an integral domain (even when R is a field).

Definition 3.2.0.6. Let R be a ring with 1. Set $GL_n(R) := U(M_n(R))$ the set of all units in $M_n(R)$. Then $GL_n(R)$ is a multiplicative group called the *general linear group of degree n over R*.

Definition 3.2.0.7. Let R be a commutative ring with 1. Define determinant $det(A) = |A|$, Let $SL_n(R) := \{A \in M_n(R) | det(A) = 1\}$ be the set of all matrices in $M_n(R)$ with determinants equal to 1. Then $SL_n(R)$ is a multiplicative subgroup of $GL_n(R)$ called the *special linear group of degree n over R*.

Definition 3.2.0.8. *(Group Rings $R[G]$)*
Let R be a commutative ring with $1 \neq 0$. Let $G = \{g_1, \ldots, g_n\}$ be a finite multiplicative group of order n. Then $R[G]$ is a *group ring*, where

$$R[G] = Rg_1 + \cdots + Rg_n = \{a_1 g_1 + \cdots + a_n g_n | a_i \in R\}$$

Natural addition is defined as

$$(\sum_{i=1}^{n} a_i g_i) + (\sum_{i=1}^{n} b_i g_i) := (\sum_{i=1}^{n} (a_i + b_i) g_i)$$

Multiplication is defined as

$$(\sum_{i=1}^{n} a_i g_i) \times (\sum_{j=1}^{n} b_j g_j) := (\sum_{k=1}^{n} c_k g_k)$$

where $c_k = \sum_{g_i g_j = g_k} a_i b_j$ with the sum running $\forall (i,j)$ with $g_i g_j = g_k$.

Remark 3.2.0.9. Let R be a commutative ring with $1 \neq 0$, G a multiplicative group, and $R[G]$ the group ring. Then

(i) $R[G]$ is a commutative ring if and only if G is commutative (=abelian) group

(ii) $R[G]$ has the multiplicative identity $1 = 1_R e_G$

Remark 3.2.0.10. Let $R[G]$ be a group ring.

(i) There is a natural injective ring homomorphism

$$R \to R[G]$$
$$r \mapsto r e_G$$

Identify R with the image Re_G of this injective homomorphism.

(ii) For every $g \in G$, the element $1_R g$ is a unit in $R[G]$

(iii) There is a natural injective group homomorphism

$$G \to U(G[R])$$
$$g \mapsto 1_R g$$

Identify G with the image $1_R G$ of this injective homomorphism.

(iv) If S is a subring of R, then $S[G]$ is a subring of $R[G]$. If H is a subgroup of G, then $R[H]$ is a subring of $R[G]$.

(v) $T = \{\sum_{i=1}^{n} a_i g_i \in R[G] | \sum_{i=1}^{n} a_i = 0\}$ is a subring of $R[G]$ (an ideal of $R[G]$)

Remark 3.2.0.11. When R is a division ring or field, then $R[G]$ (as an additive group) is a vector space over R of dimension equal to $|G|$ with basis $\{g_1, \ldots, g_n\} = G$. Hence $R[G] = Rg_1 + \cdots + Rg_n = Rg_1 \oplus \cdots \oplus Rg_n$, the direct sum of 1-dimensional vector subspaces Rg_i over R.

3.3 Ring Homomorphisms

Definition 3.3.0.1. Let R, S be rings. A map $\varphi : R \to S$ is a *ring homomorphism* if it respects the additive and multiplicative structures.

$$\varphi(a + b) = \varphi(a) + \varphi(b) \ \forall a, b \in R$$
$$\varphi(ab) = \varphi(a)\varphi(b) \ \forall a, b \in R$$

Definition 3.3.0.2. Let R, S be rings. A map $\varphi : R \to S$ is a *ring isomorphism* if it is a ring homomorphism and bijective. This is denoted $\varphi : R \xrightarrow{\sim} S$. Rings R and S is *isomorphic*, denoted $R \cong S$ or $R \simeq S$.

Definition 3.3.0.3. The *kernel* of a ring homomorphism φ is defined as
$ker\ \varphi = \varphi^{-1}(0_S) = \{a \in R | \varphi(a) = 0_S\}$.

Remark 3.3.0.4. *(Examples of homomorphism)*

(i) Let R, S be rings. The map $R \to S$, $a \mapsto 0$ is a *zero or trivial map / homomorphism*.

(ii) Suppose R_1 is a subring of a ring R. The map $\iota : R_1 \to R$, $a \mapsto a$ is a *inclusion homomorphism*.

(iii) Let $n \in \mathbb{Z}$. The quotient map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ s &\mapsto \overline{s} = [s]_n \end{aligned}$$

is a *quotient homomorphism* between additive groups $(\mathbb{Z}, +)$ and $((Z)/n(Z), +)$.

(iv) Let X be a set, R a ring, and $X_{to}R = \{f : X \to R\}$ the ring of all maps from X to R. Fix an element $c \in R$. Then

$$\begin{aligned} E_c : X_{to}R \to R \\ f \mapsto E_c(f) := f(c) \end{aligned}$$

is a *function evaluation map*, called the *Evaluation at c*.

Proposition 3.3.0.5. *Let R, S be rings and $\varphi : R \to S$ be a ring homomorphism. Let $R_1 \subseteq R$ be a subring. Then*

(i) The φ-image $\varphi(R_1) = \{b \in S | b = \varphi(a)\ for\ some\ a \in R_1\}$ is a subring of S.

(ii) ker φ is a subring of R such that $\forall a \in R$, $\forall k \in ker\ \varphi \Rightarrow ak \in ker\ \varphi$. In other words, ker φ is a subring of R, $R(ker\ \varphi) \subseteq ker\ \varphi$ and $(ker\ \varphi)R \subseteq ker\ \varphi$.

Definition 3.3.0.6. Let R be a ring, $I \subseteq R$ a subset and $r \in R$. The subset $I \subseteq R$ is a *left-ideal* of R if:

(i) I is a subring of R; and

(ii) I is closed under left multiplication by elements from R: $rI \subseteq I$ $(\forall r \in R)$, i.e., $RI \subseteq I$.

Definition 3.3.0.7. Let R be a ring, $I \subseteq R$ a subset and $r \in R$. The subset $I \subseteq R$ is a *right-ideal* of R if:

(i) I is a subring of R; and

(ii) I is closed under right multiplication by elements from R: $Ir \subseteq I$ $(\forall r \in R)$, i.e., $IR \subseteq I$.

Definition 3.3.0.8. Let R be a ring, $I \subseteq R$ a subset and $r \in R$. The subset $I \subseteq R$ is a *(two-sided) ideal* of R if is both a left-ideal and right-ideal. In other words, $RI \subseteq I$ and $IR \subseteq I$.

Proposition 3.3.0.9. *(Ideal Criterion) Let R be a ring and I a nonempty subset of R. The following are equivalent:*

(i) I is a two-sided ideal of R;

(ii) $\forall r \in R$, $\forall a, b \in R \Rightarrow ra, ar, a - b \in I$

(iii) (If R is commutative) $\forall r \in R$, $\forall a, b \in R \Rightarrow ra, a - b \in I$

(iv) (If R is commutative with 1) $\forall r \in R$, $\forall a, b \in R \Rightarrow a + rb \in I$

Proposition 3.3.0.10. *Let R_α $(\alpha \in \sum)$ be a family of subrings of a ring R. Let J_α be a left (resp. 2-sided) ideal of R_α. Then the intersection $\bigcap\limits_{\alpha \in \sum} J_\alpha$ is a left (resp. 2-sided) ideal of the subring $\bigcap\limits_{\alpha \in \sum} R_\alpha$.*

Corollary 3.3.0.11. *Let J_α $(\alpha \in \sum)$ be a family of left (resp. 2-sided) ideals of a ring R. Then the intersection $\bigcap\limits_{\alpha \in \sum} J_\alpha$ is also a left (resp. 2-sided) ideal of R.*

Proposition 3.3.0.12. *Let J_α $(\alpha \in \sum)$ be a finite family of left (resp. 2-sided) ideals of a ring R. Then the addition $\sum_{\alpha \in \sum} J_\alpha$ is also a left (resp. 2-sided ideal) of R. More generally, if J_α $(\alpha \in \sum)$ is an infinite (countable or uncountable) family of left (resp. 2-sided) ideals of a ring R, then the subset*

$$\{\sum x_\alpha | x_\alpha \in J_\alpha, x_\alpha \neq 0\ for\ only\ finitely\ many\ \alpha\}$$

is also a left (resp. 2-sided) ideal of R.

Definition 3.3.0.13. Let X be a subset of a ring R. Let J_α $(\alpha \in \sum)$ be all the ideals of R with $J_\alpha \supseteq X$. Then the intersection $\bigcap\limits_{\alpha\in\sum} J_\alpha$ is the *ideal generated by X*, denoted (X).
This (X) is the smallest among all ideals of R containing X.
If $X = \{r_1, \ldots, r_n\}$, then write $(X) = (r_1, \ldots, r_n)$.

Definition 3.3.0.14. For $r \in R$, the ideal (r) generated by a single element r is the *principal ideal of ring R*.

Definition 3.3.0.15. Let R be a ring. An ideal I is *finitely generated* if $I = (r_1, \ldots, r_n)$ for some $r_i \in R$.

Proposition 3.3.0.16. *Let R be a ring; X, Y, X_i the subsets of R; and $r_j \in R$.*

(i) Let J be an ideal of R. Then $(X) \subseteq J$ if and only if $X \subseteq J$.

(ii) The equality of ideals holds: $(X_1 \cup \cdots \cup X_n) = (X_1) + \cdots + (X_n)$.

(iii) In particular, $(r_1, \ldots, r_n) = (r_1) + \cdots + (r_n)$.

Proposition 3.3.0.17. *Let R be a ring. Let $B \subseteq R$ and $a, a_1, \ldots, a_n \in R$.*

(i) $RB = \{\sum_{i=1}^{s} r_i b_i | r_i \in R, b_i \in B, s \geq 1\}$ is a left-ideal of R, but may not be a 2-sided ideal.

(ii) More generally,

$$R\{a_1, \ldots, a_n\} = Ra_1 + \cdots + Ra_n = \left\{\sum_{i=1}^{n} r_i a_i | r_i \in R\right\}$$

are left-ideals of R, but they may not be 2-sided ideals.

(iii) The ideal (a) generated by a is given by

$$(a) = \mathbb{Z}a + aR + Ra + RaR$$

An arbitrary element of (a) is of the form

$$ma + ar + r'a + \sum_{i=1}^{n} r_i a r_i'$$

where $m \in \mathbb{Z}; r, r', r_i, r_i' \in R; n \geq 1$.

(iv) If R contains 1, then $(a) = RaR$, and an arbitrary element of (a) is of the form

$$\sum_{i=1}^{n} r_i a r_i'$$

where $r_i, r_i' \in R; n \geq 1$.

(v) If R is commutative and contains 1, then

$$(a) = aR = Ra = ra | r \in R$$

An arbitrary element of (a) is of the form ra where $r \in R$.

Proposition 3.3.0.18. *Let R be a ring with $1 \neq 0$ and I an ideal of R. Then the following are equivalent:*

(i) $I = R$

(ii) $1 \in I$

(iii) I contains a unit.

Proposition 3.3.0.19. *Suppose R is a ring with 1. Let $X \subseteq R$ be a subset, and $b_1, \ldots, b_n \in R$. Then*

(i) the ideal generated by X is

$$(X) = RXR = \left\{\sum_{i=1}^{s} r_i a_i r_i' | a_i \in X; r_i, r_i' \in R; s \geq 1\right\}$$

the smallest among all ideals of R containing X.

(ii) the ideal generated by $\{b_1, \ldots, b_n\}$ is given by

$$(b_1, \ldots, b_n) = (b_1) + \cdots + (b_n) = Rb_1R + \cdots + Rb_nR$$

the smallest among all ideals of R containing $\{b_1, \ldots, b_n\}$.

Proposition 3.3.0.20. *Let J_α $(\alpha \in \sum)$ be a family of left (resp. 2-sided) ideals of a ring R. Then the inclusion is*

$$R(\bigcup_{\alpha\in\sum} J_\alpha) \subseteq \left\{ \sum_{\alpha\in\sum} a_\alpha | a_\alpha \in J_\alpha; a_\alpha \neq 0 \ for\ only\ finitely\ many \alpha \right\}$$

where the RHS is a left (resp. 2-sided) ideal of R, and the smallest among those of R containing all J_α, where LHS = RHS when R contains 1.
If R contains 1 and $\sum$ is finite, then

$$R(\bigcup_{\alpha\in\sum} J_\alpha) = \sum_{\alpha\in\sum} J_\alpha$$

Proposition 3.3.0.21. *Let $J, J_1, \ldots, J_n$ be ideals of a ring. Then*

$$J_1 \cdots J_n = \left\{ \sum_{l=1}^{k} a_1(l) \cdots a_n(l) | a_i(l) \in J_i, k \geq 1 \right\}$$

and it is an ideal of R. In particular,

$$J^n = J \cdots J = \left\{ \sum_{l=1}^{k} a_1(l) \cdots a_n(l) | a_i(l) \in J, k \geq 1 \right\}$$

and it is an ideal of R.

Proposition 3.3.0.22. *Let $R = R_1 \times \cdots \times R_n$ be a direct product of rings. Then*

$$S_i = \{0_{R_1}\} \times \cdots \times \{0_{R_{i-1}}\} \times R_i \times \{0_{R_{i+1}}\} \times \cdots \times \{0_{R_n}\}$$

is an ideal (2-sided) of R. Furthermore,

$$R = \sum_{i=1}^{n} S_i$$

Proposition 3.3.0.23. *Let $\varphi : R \to S$ be a ring homomorphism. Then ker φ is an ideal of R.*

Definition 3.3.0.24. Let R e a ring and $I \subseteq R$ an ideal.
Then $(I, +)$ is a normal subgroup of additive group $(R, +)$. The *quotient additive group* is

$$R/I = \{\overline{r} = r + I | r \in R\}$$

with well-defined addition $\overline{r} + \overline{s} := \overline{r + s}$.

Theorem 3.3.0.25. *Let R be a ring and $I \subseteq R$ an ideal. Then*

(i) for cosets $\overline{r}, \overline{s} \in R/I$, the multiplication $\overline{r} \times \overline{S} := \overline{rs}$ is a well-defined binary operation on R/I, i.e., this multiplication does not depend on the choice of representatives r, s of the cosets.

(ii) $(R/I, +, \times)$ is a ring with $0_{R/I} = \overline{0_R}$.

(iii) $\overline{r} = 0_{R/I}$ $(= \overline{0_R})$ if and only if $r \in I$.

Definition 3.3.0.26. Let R be a ring and $I \subseteq R$ an ideal.
Then the ring $(R/I, +, \times)$ is the *quotient ring* of R by I.

Remark 3.3.0.27. Let R be a ring and $(I, +)$ a subgroup of the additive group $(R, +)$.
Then I is an ideal of R is and only if the multiplication $\times$ on the additive quotient group $(R/I, +)$ is well-defined so that $(R/I, +, \times)$ is a ring.

Definition 3.3.0.28. Let R be a ring, $I \subseteq R$ an ideal, and R/I the quotient ring.
The *surjective quotient map*

$$\gamma : R \to R/I$$
$$r \mapsto \overline{r} = r + I$$

from the additive group $(R, +)$ to the additive group $(R/I, +)$ is a ring homomorphism such that $ker\ \gamma = I$.
The *quotient ring homomorphism* refers to γ.

Remark 3.3.0.29. *(Equivalence concepts of kernel and ideal)*
The kernel of every ring homomorphism is an ideal.
Every ideal is equal to the kernel of some (surjective) homomorphism.

Definition 3.3.0.30. Let R be a commutative ring and I an ideal.
An element $a \in R$ is *nilpotent* if $a^n = 0$ for some $n \geq 1$ (depending on a).
The set of all nilpotent elements of R is the *nilradical of R*,

$$nil(R) := \{a \in R | a^n = 0,\ for\ some\ n \geq 1\}$$

In fact, $nil(R)$ is an ideal of R, and $nil(R/nil(R)) = 0$.

Definition 3.3.0.31. Let R be a commutative ring and I an ideal.
The set of *radical of I* is

$$rad(I) = \{r \in R | r^n \in I,\ for\ some\ n \geq 1\}$$

In fact, $rad(I)$ is an ideal of R containing I such that $rad(I)/I = nil(R/I)$.

Definition 3.3.0.32. Let R be a commutative ring and J an ideal.
J is a radical if $rad(J) = J$. Every prime idea of R is ideal.

Definition 3.3.0.33. Let R be a commutative ring and I an ideal. When R contains 1 and $I \subset R$, define

$$Jac(I) = \bigcap_{M:max, M \supseteq I} M$$

where M runs in the set of all maximal ideals of R containing I.
In fact, $Jac(I)$ is an ideal of R containing the radical $rad(I)$ of I.
$Jac(0)$ is the *Jacobson radical of R*.
Thus $Jac(I)$ is the pre-image of $Jac(0_{R/I})$ via $R \to R/I$.

Remark 3.3.0.34. Let R be a commutative ring and I an ideal. Then $nil(R/I^n) \supseteq I/I^n$, and $rad(I^n) \supseteq I$ (the inclusions might be strict).

Remark 3.3.0.35. For the polynomial ring $F[x]$ over field F, if $I = (x)$ is the principal ideal generated by x, then $I^n = (x^n)$. Hence $nil(F[x]/I^n) = I/I^n$ and $rad(I^n) = I$.

Remark 3.3.0.36. The Jacobson radical of $\mathbb{Z}/12\mathbb{Z}$ is $6\mathbb{Z}/12\mathbb{Z}$, included in the intersection (of two maximal ideals)

$$(2\mathbb{Z}/12\mathbb{Z}) \cap (3\mathbb{Z}/12\mathbb{Z})$$

The Jacobson radical of the polynomial ring $F[x]$ over field F is 0, which is contained in the intersection (of two maximal ideals) $(x) \cap (x - 1)$.

3.4 Ring Isomorphisms

Definition 3.4.0.1. *(First Isomorphism Theorem)* Let below be a ring homomorphism:

$$\varphi : R \to S$$

the (surjectve) quotient ring homomorphism:

$$\gamma : R \to R/ker\ \varphi$$

and a (well-defined) ring homomorphism:

$$\overline{\varphi} : R/ker\ \varphi \xrightarrow{\sim} \varphi(R)$$
$$\overline{r} \mapsto \overline{\varphi}(\overline{r}) := \varphi(r)$$

Then $\varphi = \overline{\varphi} \circ \gamma$.

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\gamma"'] & & \varphi(R) \\ & R/ker\ \varphi \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

Remark 3.4.0.2. Let R, S be a commutative ring with 1 and $\varphi : R \to S$ a ring homomorphism. Then φ induces a ring homomorphism

$$\begin{aligned} \tilde{\varphi} : R[x] &\to S[x] \\ f(x) = \sum a_i x^i &\mapsto \widetilde{\varphi}(f(x)) = \sum \varphi(a_i)x_i \end{aligned}$$

Furthermore, if $J = ker\ \varphi$, then

$$ker\ \widetilde{\varphi} = J[x] = \left\{ \sum_{i=1}^{n} a_i x^i | a_i \in J, n \geq 1 \right\}$$

is the polynomial ring with coefficients in J.
Finally, $J[x] = JR[x]$ and $J[x]$ is the ideal of $R[x]$ generated by J, i.e., $J[x] = (J)$.

Remark 3.4.0.3. Let R be a commutative ring with 1 and I an ideal of R.
Then there is an isomorphism $R[x]/I[x] \cong (R/I)[x]$.

Remark 3.4.0.4. If $\varphi : R \to S$ is a ring homomorphism, it induces a homomorphism (between matrix rings):

$$\begin{aligned} \varphi_n : M_n(R) &\to M_n(S) \\ A = (r_{ij}) &\mapsto \varphi_n(A) := (\varphi(r_{ij})) \end{aligned}$$

Remark 3.4.0.5. Let $G = g_1, , g_n$ be a multiplicative group of order $|G| = n$, R a ring, and $R[G] = Rg_1 + \cdots + Rg_n$ the group ring. Then the map

$$\begin{aligned} Tr : R[G] &\to R \\ \sum_{i=1}^{n} r_i g_i &\mapsto \sum_{i=1}^{n} r_i \end{aligned}$$

Remark 3.4.0.6. *(One-sided Ideals)*
Let $n \geq 2$ and $M_n(R)$ a matrix ring over a ring R. Let $L_k = \{A = (a_{ij}) \in M_n(R) | a_{ij} = 0, \forall j \neq k\}$.
Then L_k is a left ideal of $M_n(R)$, but not a right ideal of $M_n(R)$ when R contains 1_R.
Similarly, let $R_k = \{A = (a_{ij}) \in M_n(R) | a_{ij} = 0, \forall i \neq k\}$.
Then R_k is a right ideal of $M_n(R)$, but not a left ideal of $M_n(R)$ when R contains 1_R.
More generally, let $1 \leq k_1 < \cdots < k_r \leq n$ with $r < n$.
Let $L_{k_1,\ldots,k_r} = \{A = (a_{ij}) \in M_n(R) | a_{ij} = 0, \forall j \notin \{k_1, \ldots, k_r\}\}$.
Then $L_{k_1,\ldots,k_r}$ is a left ideal of $M_n(R)$, but not a right ideal of $M_n(R)$ when R contains 1_R.
Let $R_{k_1,\ldots,k_r} = \{A = (a_{ij}) \in M_n(R) | a_{ij} = 0, \forall i \notin \{k_1, \ldots, k_r\}\}$.
Then $R_{k_1,\ldots,k_r}$ is a right ideal of $M_n(R)$, but not a left ideal of $M_n(R)$ when R contains 1_R.

Definition 3.4.0.7. *(Second Isomorphism Theorem)* Let R be a ring, $R_1 \subseteq R$ subring, and $J \subseteq R$ ideal. Then:

(i) $R_1 + J$ is a subring of R

(ii) $R_1 \cap J$ is an ideal of R

(iii) There is an isomorphism

$$\begin{aligned} \varphi : R_1/(R_1 \cap J) &\xrightarrow{\sim} (R_1 + J)/J \\ \overline{r} = r + (R_1 \cap J) &\mapsto \varphi(\overline(r)) := \overline{r} = r + J \end{aligned}$$

Definition 3.4.0.8. *(Third Isomorphism Theorem)* Let R be a ring, and $I \subseteq J$ ideals of R. Then:

(i) J/I is an ideal of the quotient ring R/I

(ii) There is an isomorphism

$$\varphi : R/J \xrightarrow{\sim} (R/I)/(J/I)$$
$$\overline{r} = r + J \mapsto \overline{r} + J/I = (r + I) + J/I$$

Definition 3.4.0.9. *(Fourth Isomorphism Theorem)* Correspondence Theorem for Rings
Let R be a ring, $I \subseteq R$ an ideal, and $\gamma : R \to R/I$ the (surjective) quotient ring homomorphism.
Let $\sum_1$ be the set of subrings of R containing $I = ker\ \gamma$, and $\sum_2$ be the set of subrings of R/I. Then:

(i) if $R_1 \in \sum_1$, then $\gamma(R_1) = R_1/I \in \sum_2$. Conversely, if $R_1' \in \sum_2$, then $R_1' = R_1/I$ with

$$R_1 := \gamma^{-1}(R_1') = \{r \in R | \gamma(r) \in R_1'\} \in \sum{}_1$$

(ii) The map below is a well-defined bijection:

$$f : \sum{}_1 \to \sum{}_2$$
$$R_1 \mapsto R_1/I$$

(iii) $J_1 \in \sum_1$ is an ideal of R if and only if J_1/I is an ideal of R/I. If this is the case, then

$$R/J_1 \cong (R/I)/(J_1/I)$$

(iv) For $R_i \in \sum_1$, $R_1 \subseteq R_2$ holds if and only if $R_1/I \subseteq R_2/I$ holds.

3.5 Ideals, Rings of Fractions, Local Rings

Proposition 3.5.0.1. *Let R be a ring with $1 \neq 0$. Let $I \subseteq R$ be an ideal.
Then $I = R$ is and only if I contains a unit, if and only if $1 \in I$.*

Proposition 3.5.0.2. *Let R be a commutative ring with $1 \neq 0$.
Then R is a field if and only if R has only two ideals: 0 and R.*

Corollary 3.5.0.3. *If R is a field with $1 \neq 0$, then every nonzero ring homomorphism $f : R \to S$ is an injection.*

Definition 3.5.0.4. An ideal M of a ring S with $1 \neq 0$ is a *maximal ideal* if:

(i) $M \neq S$; and

(ii) for every ideal J of S with $M \subseteq J \subseteq S$, that $J = M$ or $J = S$.

Proposition 3.5.0.5. *If J is a proper ideal of R (commutative with 1), i.e, $J \subset R$, then $J \subseteq M$ for some maximal ideal M of R.*

Corollary 3.5.0.6. *Apply $J = 0$ to above. If R is a commutative ring with $1 \neq 0$, then R has a maximal ideal.*

Proposition 3.5.0.7. *Assume the ring R is commutative with 1 and $M \subseteq R$ an ideal, then these are equivalent:*

(i) M is a maximal ideal

(ii) The quotient ring R/M is a field

Definition 3.5.0.8. Assume the ring R is commutative with 1. An ideal P is a prime ideal if:

(i) $P \neq R$; and

(ii) $ab \in P \Rightarrow a \in P,$ *or* $b \in P$

Proposition 3.5.0.9. *Assume R is commutative with 1 and $P \subseteq R$ an ideal. Then the following are equivalent:*

(i) P is a prime ideal

(ii) The quotient ring R/P is an integral domain

Corollary 3.5.0.10. *Assume the ring R is commutative with 1. Then every maximal ideal is a prime ideal.*

Proposition 3.5.0.11. *Let R be a commutative ring with 1 and I an ideal of R. Then:*

(i) The ideal of $R[x]$ generated by I is

$$I[x] = \{\sum a_i x^i \in R[x] | a_i \in I\}$$

i.e., $(I) = I[x]$. Furthermore, $I[x] = I\ R[x]$

(ii) I is a prime ideal of R if and only if $I[x]$ is a prime ideal of $R[x]$

Example 3.5.0.12. Consider the polynomial ring $\mathbb{Z}[x]$. The principal idea (x) is a prime ideal of $\mathbb{Z}[x]$ but it nos not a maximal ideal as $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.

Example 3.5.0.13. Consider the polynomial ring $\mathbb{Z}[x]$. For every prime number p, the ideal $(p, x) = \mathbb{Z}[x]p + \mathbb{Z}[x]x$ generated by p and x is a maximal idea. This is because

$$\begin{aligned} &\mathbb{Z}[x] \to \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z} \\ &f(x) \mapsto \mathbf{f}(0) \mapsto \overline{f(0)} = f(0) + p\mathbb{Z} \end{aligned}$$

induces $\mathbb{Z}[x]/(p, x) \cong \mathbb{Z}/p\mathbb{Z}$.

Example 3.5.0.14. Consider the polynomial ring $F[x]$ over a field F. The principal ideal (x) is a maximal ideal of $F[x]$. This is because of isomorphism (via evaluation map $f(x) \mapsto f(0)$): $F[x]/(x) \cong F$.

Example 3.5.0.15. Consider the polynomial ring $F[x, y]$ in two variables x, y over a field F. The principal ideal (x) is a prime ideal of $F[x, y]$, but it is not a maximal ideal of $F[x, y]$.
This is because of the isomorphism (via evaluation map $f(x, y) \mapsto f(0, y)$): $F[x, y]/(x) \cong F[y]$

Proposition 3.5.0.16. *(Inverse of a prime ideal)*
Let $\varphi : R \to S$ be a ring isomorphism of commutative rings. Then

(i) If $P \subseteq S$ is a prime ideal, then $\varphi^{-1}(P)$ is either a prime ideal of R or equal to R (this latter case will not happen when φ is onto, or when $1_R \in R and \varphi(1_R) = 1_S$. In particular, if $\varphi : R \to S$ is the inclusion map, then either $P \subseteq R$ (hence $P \bigcap R = R$), or $P \bigcap R$ is a prime ideal of the subring R.

(ii) If both R and S contain 1, φ is surjective and M is a maximal ideal of S, then $\varphi^{-1}(M)$ is a prime ideal of R.

Theorem 3.5.0.17. *Let R be a commutative ring and let D be a set with $\emptyset \neq D \subseteq R \backslash \{0\}$ which does not contain any zero divisors and is closed under multiplication (i.e., $a, b \in D \Rightarrow ab \in D$). Then there is a commutative ring with $Q = D^{-1}R$ with 1 such that:*

(i) Q contains R as a subring

(ii) Every element of D is a unit in Q.

(iii) Every element of Q is the form rd^{-1} for some $r \in R$ and $d \in D$.

Definition 3.5.0.18. The ring $Q = D^{-1}R$ is the *ring of fractions of D with respect to R*.

Definition 3.5.0.19. If R is an integral domain and $D = R \backslash \{0\}$, then $D^{-1}R$ is the *fractional field of R* and denoted as $Q(R)$.

$$Q(R) = D^{-1}R$$

Corollary 3.5.0.20. *Suppose R is a nonzero subring of a field F. Then the fractional field $Q(R)$ of R is the subfield of F generated by R. Namely,*

$$Q(R) = \{\alpha \in F | \alpha = \frac{r_1}{r_2}, r_i \in R, r_2 \neq 0\}$$

Corollary 3.5.0.21. *Suppose R is an integral domain and $Q = Q(R)$ its fraction field. If $\sigma : R \to F$ is an injective ring homomorphism to a field F, then σ extends to an injective homomorphism.*

$$\sigma' : Q(R) \to E =: \{\alpha \in F | \alpha = \frac{\alpha(r_1)}{\alpha(r_2)}, r_i \in R, r_2 \neq 0\} \subseteq F$$

Here $E = Q(\alpha(R))$ is the fraction field of the integral domain $\sigma(R)$ and is the subfield of F generated by $\sigma(R)$.

Definition 3.5.0.22. A commutative ring R with $1 \neq 0$ is a *local ring* if it has a unique maximal ideal (say M).

Definition 3.5.0.23. Let R be an integral domain and P a prime ideal.
Then $D =: R \backslash P$ satisfies the condition of Theorem 4.5.17.
The *localisation of R at P* is denoted $R_P := D^{-1}R$.
Then $PR_P = \{a/d \mid a \in P, d \notin P\}$ is the only maximal ideal in R_P so that R_P is a local ring. Note that $d \in D$ if and only if $d \notin P$.

Definition 3.5.0.24. Let R be an integral domain. if $n1_R = 1_R + \cdots + 1_R$ (n times) is equal to 0_R for some $n \geq 1$, let $p \geq 1$ be the minimum of such integer with $p1_R = 0$.
Then the *characteristic of R* is defined as $char\ R := p$, a prime number.
If no such $n \geq 1$ exists, then set $char\ R := 0$.
Hence either $char\ R = p$ is prime and R contains a subring isomorphic to $\mathbb{Z}/(p)$ (a field), or $char\ R = 0$ and R contains a subring isomorphic to $\mathbb{Z}$.

Definition 3.5.0.25. Let R be an integral domain. When $R = F$ is a field, either F contains a subfield F_0 isomorphic to $\mathbb{Z}/(p)$, or F contains a subfield F_0 isomorphic to $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$.
Such a subfield F_0 is the *prime subfield* of F.

Remark 3.5.0.26. Every subfield F of $\mathbb{R}$ or $\mathbb{C}$ has characteristic equal to 0 and contains the prime field $\mathbb{Q}$.
Indeed, F contains $\mathbb{Q}(\mathbb{Z}1_F) \cong \mathbb{Q}(\mathbb{Z}) = \mathbb{Q}$.

Proposition 3.5.0.27. *Let F be a field of characteristic $p > 0$, e.g., $F = \mathbb{Z}/(p)$.
The $(x+y)^p = x^p + y^p$ holds for any $x, y \in F$.
This is by binomial expansion of left hand side and nothing that $p = 0$ in F.*

Definition 3.5.0.28. Let R be a commutative ring with $1 \neq 0$.
Two ideals I, J of R is *comaximal* if $I + J = R$.

Theorem 3.5.0.29. *(Chinese Remainder Theorem) Let $J_1, \ldots, J_n$ be ideals of R. Then*

(i) The map

$$\begin{aligned} \varphi : R &\to (R/J_1) \times \cdots \times (R/J_n) \\ r &\mapsto (\overline{r} = r + J_1, \ldots, \overline{r} = r + J_n) \end{aligned}$$

is a ring homomorphism with

$$ker\ \varphi = J_1 \cap \cdots \cap J_n$$

(ii) Suppose that J_i, J_j are comaximal for all $i \neq j$. Then φ is surjective and

$$J_1 \cap \cdots \cap J_n = J_1 \cdots J_n$$

Hence we have the isomorphism:

$$\overline{\varphi} : R/(J_1 \cdots J_n) \to R/(J_1) \times \cdots \times R/(J_n)$$

Corollary 3.5.0.30. *let $n \geq 2$ be an integer.*

(i) Factorise n as a product, $n = p_1^{r_1} \cdots p_t^{r_t}$ of powers of distinct primes. Then there is an isomorphism

$$\begin{aligned} r : \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} (\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_t^{r_t}\mathbb{Z}) \\ \overline{s} &\mapsto (\overline{s}, \ldots, \overline{s}) \end{aligned}$$

(ii) In particular, τ induces isomorphism of multiplicative unit groups:

$$U(\mathbb{Z}/n\mathbb{Z}) \cong U(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/p_t^{r_t}\mathbb{Z})$$

Hence Euler's φ-functions satisfy

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_t^{r_t}) = (p^{r_1} - p^{r_1 - 1}) \cdots (p^{r_t} - p^{r_t - 1})$$

3.6 Euclidean Domains, PID, UFD

Definition 3.6.0.1. An integral domain is said to be a *(Euclidean Domain)* (or possesses a *(Euclidean / Division Domain)*) if there is a function

$$N : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$$

on R such that for any two elements $a, b \in R$ with $b \neq 0$, there exist element $q \in R$ such that

$$a = qb + r$$

where $r = 0$ or $N(r) < N(b)$.
The *norm function* is N, and the *norm of a* is defined as $N(a)$.

Remark 3.6.0.2. For a, b in Euclidean domain R with $b \neq 0$, apply Division Algorithm:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where r_n is the last nonzero remainder. Such an r_n exists since

$$N(b) > N(r_0) > N(r_1) > \cdots > N(r_n)$$

is a strictly decreasing sequence of nonnegative integers

Example 3.6.0.3. Every field F is a Euclidean domain with respect to any function $N : F \to \mathbb{Z}_{\geq 0}$

Example 3.6.0.4. The integer ring $\mathbb{Z}$ is a Euclidean domain with the modules as the norm function:

$$N(s) : \ |s|, s \in \mathbb{Z}$$

Example 3.6.0.5. The polynomial ring $F[x]$ over a field F is a Euclidean domain where

$$N(f) : \ \deg f, \forall f \in F[x]\backslash\{0\}$$

Example 3.6.0.6. The *Gaussian Integer* ring

$$\mathbb{Z}[i] := \mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

is a Euclidean domain where the norm function is the square of the usual modules of $\mathbb{C}$:

$$N(a+bi) := |a+bi|^2 = (a+bi)(a-bi) = a^2 + b^2, \ \forall \ a+bi \in \mathbb{Z}[i]\backslash\{0\}$$

Example 3.6.0.7. The *Eisenstein Integer* ring is a Euclidean domain:

$$\mathbb{Z}[\zeta_3] = \mathbb{Z} + \mathbb{Z}\zeta_3$$

where $\zeta_3 = (-1 + \sqrt{-3})/2$ is a primitive cube root of unity: $\zeta_3^n = 1$ if and only if $3|n$.
The norm function is the square of the usual modulus:

$$N(a + b\zeta_3) = |a + b\zeta_3|^2 = (a + b\zeta_3)(a - b\zeta_3) = a^2 - ab + b^2$$

Definition 3.6.0.8. An integral domain R is a *Principal Ideal Domain (PID)* if every ideal $I \subseteq R$ is a principal: $I = (a)$ for some $a \in I$.

Proposition 3.6.0.9. *A Euclidean domain R is a PID.*

Example 3.6.0.10. Consider the polynomial ring $\mathbb{Z}[x]$. The ideal $(2, x) = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$ is not principal. Hence $\mathbb{Z}[x]$ is neither a PID, nor a Euclidean domain.

Example 3.6.0.11. The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID.
Indeed, the ideal $I = (3, 2 + \sqrt{-5})$ is not a principal.
Alternatively, show that 3 is an irreducible element but not a prime element in the quadratic integer ring.

Definition 3.6.0.12. Let $a, b \in R$ with $b \neq 0$.

(i) a is a *multiple* of b if $a = bc$ for some $c \in R$.
In this case, b is said to divide a,or to be a *divisor of a*, written $b|a$.

(ii) $d \in R$ is the *greatest common divisor of a and b*, denoted as $d = \gcd(a, b)$ if

a. $d|a$, and $d|b$; and

b. $d'|a$, and $d'|b \Rightarrow d'|d$.

c. Inductively, for $a_i \in R \backslash \{0\}$ $(1 \leq i \leq n)$, define their greatest common divisor as:

$$\gcd(a_1, \dots, a_n) := \gcd(\gcd(a_1, \leq, a_{n-1}), a_n)$$

This is a multi-symmetric function in $a_1, \leq, a_n$.

Proposition 3.6.0.13. *Assume R is commutative and has 1.*
Let a, b be nonzero elements in R such that $(a, b) = (d)$ for some $d \in R$.
Then d is a greatest common divisor of a and b, i.e., $d = \gcd(a, b)$

Proposition 3.6.0.14. *Suppose R is an integral domain.*

(i) Let $d, d' \in R$. Then $(d) = (d') \Leftrightarrow d' = ud$ for some unit u.

(ii) Let d be a greatest common divisor of a and b. Then d' is another greatest common divisor of a and b is and only if $d' = ud$ for some unit u.

Theorem 3.6.0.15. *Suppose R is a Euclidean domain. Let a, b be nonzero elements in R.*
Let $d = r_n$ be the last nonzero remainder in the Division Algorithm. Then

(i) $d = \gcd(a, b)$.

(ii) $(d) = (a, b)$. In particular, $d = ax + by$ for some $x, y \in R$.

Proposition 3.6.0.16. *Assume that R is a PID. Let a, b be nonzero elements.*
Let $d \in R$ such that $(d) = (a_1, \dots, a_n)$. Then

(i) $d = \gcd(a_1, \dots, a_n)$.

(ii) $d = a_1x_1 + \cdots + a_nx_n$ for some $x_i \in R$

(iii) Such d above is unique up to multiplication by a unit of R.

Proposition 3.6.0.17. *Assume that R is a PID.*
Then every nonzero prime ideal P of R is a maximal ideal of R.

Corollary 3.6.0.18. *Let R be a commutative ring with 1 such that the polynomial ring $R[x]$ is a PID.*
Then R is a field.

Definition 3.6.0.19. Assume R is an integral domain. An element $r \in R$ is *irreducible* in R if:

(i) $r \neq 0$,

(ii) r is not a unit, and

(iii) $r = ab \Rightarrow a$ or b is a unit in R

Definition 3.6.0.20. Assume R is an integral domain. An element $r \in R \backslash \{0\}$ is *reducible* in R if $r = ab$ where neither a nor b is a unit of R.

Definition 3.6.0.21. Assume R is an integral domain. A nonzero element $p \in R$ is *prime* in R if the ideal (p) is a prime ideal, or equivalently if p is a non-unit and $p|ab \Rightarrow p|a$, or $p|b$.

Definition 3.6.0.22. Assume R is an integral domain.
Elements $a, b \in R$ is *associate* in R if $a = ub$ for some unit $u \in R$.

Proposition 3.6.0.23. *Let R be an integral domain and a, b nonzero elements of R.*

(i) If $a|b$ and $b|a$, then a and b are associate in R.

(ii) Suppose $a = bc$. Then a and b are associate in R if and only if c is a unit.

Proposition 3.6.0.24. *Assume R is an integral domain. Then a prime element is always irreducible.*

Proposition 3.6.0.25. *Assume that R is PID. Let $p \in R \backslash \{0\}$. Then the following are equivalent:*

(i) (p) *is a maximal ideal*

(ii) p *is a prime element, i.e.,* (p) *is a prime ideal*

(iii) p *is an irreducible element*

Definition 3.6.0.26. An integral domain R is a *Unique Factorisation Domain (UFD)* if every element $r \in R \backslash \{0\}$ which is not a unit, satisfies:

(i) *(Factorisation)* $r = p_1 \cdots p_n$ where p_i's are irreducible (but not necessarily distinct), and

(ii) *uniqueness* The factorisation in (i) is unique up to associates if $r = q_1 \cdots q_m$ is another factorisation, with q_i irreducible. Then $m = n$, and after relabelling $q_i = u_i p_i$ for some units u_i (i.e., q_i is associate to p_i).

Proposition 3.6.0.27. *For r in Definition 4.6.26(i) above, we can write $r = up_i^{s_1} \cdots p_c^{s_c}$ where p_i are irreducible, $s_i \geq 0$, u is a unit, and p_i and p_j are not associate for all $i \neq j$.*
If $r' = vp_i^{t_1} \cdots p_c^{t_c}$ is as in Definition 4.6.26(i) and r' is associate to r (but with $s_i \geq 0$, $t_i \geq 0$, and with v a unit), then $s_i = t_i$ for all i.

Proposition 3.6.0.28. *Assume that R is a UFD. Then $p \in R$ is irreducible if and only if it is prime.*

Proposition 3.6.0.29. *Assume that R is a UFD and a, b are nonzero elements. Then*

(i) $\gcd(a, b)$ *exists.*

(ii) Precisly, factorise

$$a = up_1^{e_1} \cdots p_n^{e_n}$$
$$b = vp_1^{f_1} \cdots p_n^{f_n}$$

where p_i's are irreducible, u and v are units, and $e_i \geq 0$, $f_i \geq 0$. Then

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$$

Here, set $\gcd(a, b) = 1$ *if* $\min(e_i, f_i) = 0$ $(\forall i)$.

(iii) For a, b in (ii), $a|b$ if and only if $e_i \leq f_i$ for all $i = 1, \leq, n$.

Definition 3.6.0.30. Suppose R is a PID. Then R satisfies *ACC = Ascending Chain Condition* (or *Noetherian* condition): every increasing sequence of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ must stabilise, i.e., $I_N = I_{N+1} = I_{N+2} = \cdots$ for some $N \geq 1$.

Proposition 3.6.0.31. *Euclidean Domain $\Rightarrow$ PID $\Rightarrow$ UFD*

Corollary 3.6.0.32. *(Fundamental Theorem of Arithmetic) The integer ring $\mathbb{Z}$ is UFD.*

Definition 3.6.0.33. Let R be a commutative ring with 1 and let $a, b \in R$ be nonzero elements. A *least common multiple (lcm)* of a and b, denoted lcm(a, b), is an element c or R such that:

(i) $a|b$, $b|c$, and

(ii) $a|c'$, $b|c' \Rightarrow c|c'$

Proposition 3.6.0.34. *Assume that R is a UFD and a, b are nonzero elements. Then*

(i) lcm*(a,b) exists.*

(ii) Precisely, factorise

$$a = up_1^{e_1} \cdots p_n^{e_n}$$
$$b = vp_1^{f_1} \cdots p_n^{f_n}$$

where p_i's are prime, u and v are units, and $e_i \geq 0$, $f_i \geq 0$. Then

$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} \cdots p_n^{\max(e_n, f_n)}$$

Here, set $\operatorname{lcm}(a, b) = 1$ *if* $\max(e_i, f_i) = 0$ $(\forall i)$

3.7 Polynomial rings

Assume for this section that R is a commutative ring with $1 \neq 0$

Definition 3.7.0.1. A *polynomial of degree $n \geq 0$, in one variable x and with coefficients $a_i \in R$ with leading coefficient $a_n \neq 0$* is defined as:

$$g(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

By convention, for zero polynomial 0, define its degree as $\deg 0 = -\infty$. If $g(x)$ has no positive-degree term, i.e., if $g(x) = a_0$ with $a_0 \in R$, then this $g(x)$ is a *constant polynomial*.

Remark 3.7.0.2. Let the following be the set of all polynomials in one variable x and with coefficients in R:

$$R[x] := \{\sum_{j=0}^{d} b_j x^j \mid d \geq 0, b_j \in R\}$$

There are natural addition and multiplication operations for polynomials

$$g(x) = \sum_{i=0}^{r} a_i x^i,\ h(x) = \sum_{i=0}^{s} a_i x^i$$

defined as

(i) $g(x) + h(x) = \sum_{i\geq 0}(a_i + b_i)x^i$

(ii) $g(x)h(x) = \sum_{k\geq 0} c_k x^k$, where $c_k = \sum_{i+j=k} a_i b_j = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$ such that $(R[x], +, \times)$ is a ring called the *polynomial ring with coefficients in R*.

Proposition 3.7.0.3. *Assume that R is an integral domain. then*

(i) For any $f(x)$, $g(x) \in R[x]$, we have $\deg(fg) = \deg\ f + \deg\ g$.

(ii) The units of $R[x]$ are just the units of R. Namely, $U(R[x]) = U(R)$.

(iii) $R[x]$ is an integral domain.

Proposition 3.7.0.4. *Let I be an ideal of R, let $(I) = I[x]$ $(= I\ R[x])$ be the ideal of $R[x]$ generated by I. Then:*

(i) $R[x]/I[x] \cong (R/I)[x]$

(ii) If I is a prime ideal of R, then $I[x]$ is a prime ideal of $R[x]$.

Example 3.7.0.5. If $I = (a) = aR$ is a principal ideal of R, then $aR[x]$ is the ideal of $R[x]$ generated by aR, i.e., $aR[x] = I[x]$. Thus $R[x]/aR[x] = R[x]/I[x] \cong (R/I)[x] = (R/aR)[x]$

Example 3.7.0.6. Consider the integer ring $\mathbb{Z}$ and its ideal $n\mathbb{Z}$. We have $\mathbb{Z}[x]/n\mathbb{Z}[x] \cong (\mathbb{Z}/n\mathbb{Z})[x]$.
Hence if $n = p$ is a prime number, then $p\mathbb{Z}[x]$ is a prime ideal of $\mathbb{Z}[x]$.
So p is a prime element of $\mathbb{Z}$ and also of $\mathbb{Z}[x]$

Definition 3.7.0.7. The polynomial ring $R[x_1, \ldots, x_n]$ in n variables $x_1, \ldots, x_n$ can be inductively defined as:

$$R[x_1, x_2] = (R[x_1])[x_2], \ldots, R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$$

In a slightly more concrete formulation, a nonzero polynomial in $R[x_1, \ldots, x_n]$ is the finite sum of nonzero monomial terms, i.e., a finite sum of elements of the form $ax_1^{d_1} \cdots x_n^{d_n}$ where $a \in R$ (the coefficient of the term), and the d_i are nonnegative integers.
A monic term $x_1^{d_1} \cdots x_n^{d_n}$ is a *monomial* and is the monomial part of the term $ax_1^{d_1} \cdots x_n^{d_n}$.
The exponent d_i is the *degree in x_i* of the term.
The sum $d = d_1 + d_2 + \cdots + d_n$ is the *degree of the term*.
The ordered n-tuple $(d_1, d_2, \ldots, d_n)$ is the *multidegree of the term*.
The *degree of a nonzero polynomial* is the largest degree of any of its monomial terms.
If f is a nonzero polynomial in n variables, the sum of all the monomial terms in f of degree k is the *homogeneous component* of f of degree k. If f has degree d then f may be written uniquely as the sum $f = f_0 + f_1 + \cdots + f_d$ where f_k is the homogeneous component of f of degree k, for $0 \leq k \leq d$ (where some f_k may be zero).

Theorem 3.7.0.8. *Let F be a field. Then the polynomial ring $F[x]$ is a Euclidean domain with the norm function $N : F[x] \to \mathbb{Z}_{\geq 0}$ given as $N(f) = \deg f$.*

Corollary 3.7.0.9. *The polynomial ring $F[x]$ over a field F is a PID and also UFD.*

Lemma 3.7.0.10. *(i) We have equality for sets of units: $U(R[x]) = U(R)$.*

(ii) Let $r \in R \backslash \{0\}$. Then r is irreducible as element of R if and only if r is irreducible as an element of $R[x]$.

Definition 3.7.0.11. Let R be a UFD with $F = Q(R)$ its fraction field.

(i) Let $f(x) \in R[x]$ be a nonconstant polynomial. Write $f(x) = c(f)f_1(x)$ so that $c(f) \in R\backslash\{0\}$ and gcd of cofficients of $f_1(x)$ is 1.
This $c(f)$ is unique up to a unit factor of R and is the *content* of f.
The *primitive polynomial* is $f(x) \in R[x]$ if its content $c(f)$ is a unit in R. Then $c(f) = 1$ in this case.
In the above notation, the content $c(f_1) = 1$ and f_1 is a primitive polynomial.

(ii) In general, when $g(x) \in F(x)$ is a nonconstant polynomial, write $g(x) = c(g)g_1(x)$ such that $c(g) \in F^\times$ and $g_1(x) \in R[x]$ is a primitive polynomial.
This $c(g)$ is unique up to a unit factor of R ad is the *content* of g.

Remark 3.7.0.12. Let R be a UFD and $F = Q(R)$ its fraction field.

(i) For nonconstant $g(x) \in F[x]$ as above, write $g(x) = c(g)g_1(x)$ with $c(g)\ inF$ the content of $g(x)$, and $g_1(x) \in R[x]$ a primitive polynomial.
Then $g(x) \in R[x]$ if and only if the content $c(g) \in R$

(ii) If $f(x) \in R[x]$ is irreducible as an element and $\deg f \geq 1$, then $f(x)$ is primitive.

Proposition 3.7.0.13. *(Gauss Lemma 1) Let R be a UFD and $f(x), g(x) \in R[x]$ primitive polynomials. Then $f(x)g(x) \in R[x]$ is still a primitive polynomial.*

Corollary 3.7.0.14. *(Contents Relation) Let R be a UFD with $F = Q(R)$ its fraction field, and $f(x), g(x) \in F[x]$ nonconstant polynomials. Then there is contents relation: $c(fg) = c(f)c(g)$.*

Proposition 3.7.0.15. *(Gauss Lemma 2) Assume R is UFD with $F = Q(R)$ its fraction field, and $f(x) \in R[x]$.*
If $f(x)$ is reducible in $F[x]$ then $f(x)$ is reducible in $R[x]$.
More precisely, if

$$f(x) = g(x)h(x)$$

for some nonconstant polynomials $g(x), h(x) \in F[x]$, and $g(x) = c(g)g_1(x)$, $h(x) = c(h)h_1(x)$, then $c(g)c(h) = c(f) \in R$ and

$$f(x) = c(f)g_1(x)h_1(x)$$

is the factorisation in $R[x]$ with $g_1, h_1, g_1h_1 \in R[x]$ all primitive polynomials.

Proposition 3.7.0.16. *(Gauss Lemma 3) Let R be a UFD with F its fraction field and let $p(x) \in R[x]$. Then:*

(i) Suppose $p(x)$ is a primitive polynomial.
Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

(ii) Suppose $p(x)$ is a monic polynomial.
Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

Theorem 3.7.0.17. *The ring R is a UFD if and only if the polynomial ring $R[x]$ is a UFD.*

Corollary 3.7.0.18. *Assume that R is a UFD. Then polynomial ring $R[x_1, \ldots, x_n]$ is also a UFD for any $n \geq 1$.*

Proposition 3.7.0.19. *Let F be a field and $f \in F[x]$. Then f has a factor of degree 1 in $F[x]$ if and only if f has a root in F (i.e., there is an $\alpha \in F$ such that $f(\alpha) = 0$).*

Proposition 3.7.0.20. *(Irreducibility criterion in small degree)*
Let F be a field. Suppose $f \in F[x]$ has $\deg f = 2$ or 3.
Then f is reducible in $F[x]$ if and only if f has a root in F.

Proposition 3.7.0.21. *Assume $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$ has $\deg f = n$. Assume r/s (with $r, s \in \mathbb{Z}$ co-prime) is a rational root of $f(x)$. Then:*

$$r|a_0, \ s|a_n$$

In particular, if $f(x) \in \mathbb{Z}[x]$ is a monic polynomial and $f(d) \neq 0$ for all integers d dividing the constant term of $f(x)$, then $f(x)$ has no roots in $\mathbb{Q}$.

Proposition 3.7.0.22. *(Irreducibility criterion, modulo ideal)*
Let R be an integral domain, $I \subset R$ a proper ideal and $f(x) \in R[x]$ a nonconstant monic polynomial. Suppose that the image of $f(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller positive degrees. Then $f(x)$ is irreducible in $R[x]$.

Proposition 3.7.0.23. *(Eisenstein's Criterion)*
Let R be an integral domain, $P \subset R$ a prime ideal, and

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

a polynomial in $R[x]$ (with $n \geq 2$). Suppose

$$a_i \in P (0 \leq i \leq n-1), \ a_0 \notin P^2$$

Then $f(x)$ is irreducible in $R[x]$.

Proposition 3.7.0.24. *(Eisenstein's Criterion over UFD)*
Let R be a UFD with $F = Q(R)$ its fraction field, P a prime ideal of R and

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

in $R[x]$ with $n \geq 2$ such that

$$a_n \notin, \ a_i \in P (0 \leq i \leq n-1), \ a_0 \notin P^2$$

Then $f(x)$ is irreducible in $R[x]$, and also in $F[x]$ by Gauss lemma.

Proposition 3.7.0.25. *(Eisenstein's Criterion for $\mathbb{Z}[x]$)*
Let p be a prime in $\mathbb{Z}$ and let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

a polynomial in $\mathbb{Z}[x]$ (with $n \geq 2$). Suppose

$$p|a_i (0 \leq i \leq n-1), \ p^2 \nmid a_0$$

Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Proposition 3.7.0.26. *Let $F[x]$ be the polynomial ring over a field F and $f(x)$ a nonconstant polynomial. Then the following are equivalent:*

(i) (f) is a maximal ideal of $F[x]$

(ii) (f) is a prime ideal of $F[x]$

(iii) The quotient ring $F[x]/(f)$ is a field

Proposition 3.7.0.27. *Let $F[x]$ be polynomial ring over a field F and $g(x)$ a nonconstant polynomial such that:*

$$cg(x) = f_1(x)^{n_1} \cdots f_k(x)^{n_k}$$

where c is nonzero constant, the f_i are distinct monic irreducible polynomials in $F[x]$ and $n_i \geq 1$. Then

$$F[x]/(g) \cong (F[x]/(f_1^{n_1})) \times \cdots \times (F[x]/(f_k^{n_k}))$$

Definition 3.7.0.28. Let $F[x]$ be the polynomial ring over a field F and $f(x)$ a nonconstant polynomial. Note that $\alpha \in F$ is a root of $f(x)$ (i.e., $f(\alpha) = 0$) if and only if $(x-a)|f(x)$.
Then $\alpha \in F$ is a root of $f(x)$ of *multiplicity m* if

$$(x-a)^m | f(x), \ \text{but} \ (x-a)^{m+1} \nmid f(x)$$

Proposition 3.7.0.29. *Let $F[x]$ be the polynomial ring over a field F and $f(x)$ a nonconstant polynomial such that $\alpha_i \in F$ $(1 \le i \le k)$ are all the distinct roots of $f(x)$ of multiplicity $m_i \ge 1$. Then*

$$f(x) = (x - \alpha_1)^{m_1} \cdots (x - \alpha_k)^{m_k} q(x)$$

for some $q(x) \in F[x]$. In particular, $\sum_{i=1}^{k} m_i \le \deg f(x)$, and $f(x)$ has at most $\deg f(x)$ of roots in F, even counted with multiplicity.

Remark 3.7.0.30. The *fundamental theorem of algebra* from Gauss states: every complex polynomial

$$f(x) = c(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)$$

of deg $n \ge 1$ has at least one complex root α_1.
Thus $f(x) = (x - \alpha_1)q(x)$ for some complex polynomial $q(x) \in \mathbb{C}[x]$.
Applying it n times, $f(x)$ can be factorised as product of linear ones:

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$$

where $\alpha_1, \ldots, \alpha_n$ are all the roots of $f(x)$ with multiplicity counted.
Conversely, if

$$g(x) = c(x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)$$

is a deg n complex polynomial, and $\beta_1, \ldots, \beta_n$ are all of the roots of $g(x)$ (with multiplicity counted), then $g(x)$ can be recovereed from its roots:

$$g(x) = c(x - \beta_1) \cdots (x - \beta_n)$$

Remark 3.7.0.31. Let $p \in \mathbb{Z}$ be a prime number. Let $f(x) = x^p - a$ with $a \ne 0$.
In the complex field $\mathbb{C}$, $f(x)$ has exactly p distinct roots.
Indeed, let α be one complex root of $f(x)$ (exist by Fundamental Theorem of Algebra). Then below are all the p distinct roots of $f(x)$:

$$x_k = \alpha \exp(2k\pi i/p) = \cos(2k\pi/p) + i\sin(2k\pi/p) \ (0 \le k < n)$$

Indeed, for any $n \ge 1$, the $\exp(2k\pi i/p)$ $(0 \le k < n)$ are all the n distinct roots of the polynomial $x^n - 1$.
The monic polynomial $f(x)$ of degree p can be recovered from its p roots:

$$f(x) = x^p - a = (x - x_0) \cdots (x - x_p)$$

Remark 3.7.0.32. Let $p \in \mathbb{Z}$ be a prime number. Let $f(x) = x^p - a$ with $a \ne 0$.
If F is a field of characteristic p, say over some field of $\mathbb{Z}/(p)$, and $a \in F$, then whenever $\beta \in F$ is a root of $f(x)$ (so that $0 = f(\beta) = \beta^p - a$) it is a multiple root of multiplicity p. Indeed,

$$f(x) = x^p - a = x^p + (-1)^p a = x^p + (-\beta)^p = (x - \beta)^p$$

Proposition 3.7.0.33. *Let F be a field, and $G \subseteq (F \backslash \{0\}, \times)$ a finite multiplicative subgroup. Then G is cyclic.*

Proposition 3.7.0.34. *If F is a finite field, then $F \backslash \{0\}$ is a cyclic multiplicative group.*

Corollary 3.7.0.35. *Let p be a prime.*
Then $U(\mathbb{Z}/(p)) = \mathbb{Z}/(p) \backslash \{[0]_p\}$ is a cyclic multiplicative group of order $p - 1$.

Remark 3.7.0.36. Let F be a field, $a, b \in F$ with $a \ne 0$. Let $f(x) \in F(x)$ be a nonconstant polynomial. Then:

$$\begin{aligned} \varphi : F &\to F \\ x &\mapsto ax + b \end{aligned}$$

is a bijection with its inverse given by

$$\begin{aligned} \psi : F &\to F \\ x &\mapsto (x - b)/a \end{aligned}$$

Thus $f(x)$ is irreducible in $F[x]$ if and only if $g(x) := f(ax + b)$ is irreducible.

Remark 3.7.0.37. Let F be a field, $a, b \in F$ with $a \neq 0$. Let $f(x) \in F(x)$ be a nonconstant polynomial. Suppose deg $f(x) = n \geq 1$ and let $h(x) = x^n f(x^{-1})$ which is the *reverse of $f(x)$*, and which is a polynomial in $F[x]$ with deg $h(x) \leq n$. Then $f(x)$ can be recovered from its inverse via:

$$f(x) = x^n h(x^{-1})$$

Further, $f(x)$ is irreducible in $F[x]$ if and only if its inverse $h(x)$ is irreducible.

Example 3.7.0.38. Let $p \in \mathbb{Z}$ be a prime number. Then the *cyclotomic polynomial* below is irreducible over $\mathbb{Q}$:

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

4 Modules and Vector Spaces

4.1 Basic Axioms

Definition 4.1.0.1. Let R be a ring. A *left R-module* or a *left module over R* is a nonempty set M with:

(i) a binary operation $+$ so that $(M, +)$ is an abelian additive group, and

(ii) a (left) action of R on M, i.e., a map

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

that satisfies:

a. *(Distributive Law)* $\forall r, s \in R$, $\forall m, n \in M$

$$\begin{aligned} (r + s)m &= rm + sm \\ r(m + n) &= rm + rn \end{aligned}$$

b. *(Associative Law)* $\forall r, s \in R$, $\forall m \in M$,

$$(rs)m = r(sm)$$

If the ring R has 1_r, the additional axiom is imposed

c. *(Trivial Action by 1_R)*

$$1_R m = m, \forall m \in M$$

Remark 4.1.0.2. *(Unital Module)*

(i) The right R-module can be defined similarly

(ii) A left R-module is *unital* if R has 1 and Definition 5.1.1(2c) holds.

(iii) When R is commutative, a left R-module M can eb made into a right R-module by defining:

$$mr := rm, \ \forall r \in R, m \in M$$

(iv) When R is a field (or division ring), a left module over R is just a vector space over R

From here onwards, whenever R has 1, every left R-module is assumed to be unital.

Example 4.1.0.3. Every additive abelian group M is a natural $\mathbb{Z}$-module:

$$\begin{aligned} Z \times M &\to M \\ (n, m) &\mapsto nm \end{aligned}$$

Here $0_{\mathbb{Z}} m := 0_M$, $nm := m + \cdots + m$ (n times) when integer $n > 0$, and $nm := -((-n)m)$ when integer $n > 0$. Thus $\mathbb{Z}$-modules are just (additive) abelian groups.

Example 4.1.0.4. *(Ring as a module over itself)*
Let R be a ring. Then $M = R$ is naturally a left R-module via the natural multiplication:

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

Left R-submodules of $M = R$ are just left ideals of R.
Assuming R is commutative, $M = R$ is naturally a right R-module.

Definition 4.1.0.5. Let R be a ring and M a left R-module.
A nonempty subset $N \subseteq M$ is a *left R-submodule of M* if:

(i) $(N, +)$ is a subgroup of the additive group $(M, +)$, and

(ii) N is closed under the action of R:

$$r \in R, \ n \in N \Rightarrow rn \in N$$

Remark 4.1.0.6. A left R-submodule N of M is just a subset of M which itself is a left R-module under the addition $+N \times N \to N$ and the action $R \times N \to N$ as the restrictions of the addition $+ : M \times M \to M$ and the action $R \times M \to M$, respectively.

Remark 4.1.0.7. When R is a field (or division ring), a left R-submodule is just an R-subspace.

Example 4.1.0.8. Let R be a ring, $I \subseteq R$ a left ideal of R, and M a left R-module. Then define:

$$IM := \{\sum_{i=1}^{s} a_i m_i \mid a_i \in I,\ m_i \in M,\ s \geq 1\}$$

which is a left R-submodule of M.

Example 4.1.0.9. *(Free module R^n)* Let R be a ring with 1. Let

$$R^n := \{(a_1, \dots, a_n) \mid a_i \in R\}$$

Define addition to be

$$\begin{gathered} + : R^n \times R^n \to R^n \\ (X = (x_1, \dots, x_n), Y = (y_1, \dots, y_n)) \mapsto X + Y := (x_1 + y + 1, \dots, x_n + y_n) \end{gathered}$$

Define the R-action as

$$\begin{gathered} R \times R^n \to R^n \\ (r, Y = (y_1, \dots y_n)) \mapsto rY := (r_y 1, \dots, r y_n) \end{gathered}$$

Then R^n is a left R-module called the *free left module of rank n over R*.

Example 4.1.0.10. Let R^n be the free left R-module of rank n over R.

(i) Let $I_1, \dots, I_n$ be left ideals of R. Then

$$I_1 \times \cdots \times I_n := \{(a_1, \dots, a_n) \mid a_i \in I\}$$

is a left R-submodule of R^n.

(ii) This is a left R-submodule of R^n:

$$\{(x_1, \dots, x_n) \mid x_i \in R,\ \sum_{i=1}^{n} x_i = 0\}$$

Definition 4.1.0.11. *($F[x]$-modules)* Let F be a field and V a vector space over F.
Fix a linear transformation $T : V \to V$. Then V has a natural $F[x]$-module structure, depending on T.
Note that for linear transformations $T_i : V \to V$ $(i = 1, 2, \dots)$ and scalars $\alpha_i \in F$, the *linear combination*

$$\begin{aligned} \alpha_1 T_1 + \alpha_2 T_2 &: V \to V \\ v &\mapsto (\alpha_1 T_1 + \alpha_2 T_2)(v) := \alpha_1 T_1(v) + \alpha_2 T_2(v) \end{aligned}$$

is a well defined linear transformation. Inductively, $\alpha_1 T_1 + \ldots + \alpha_k T_k$ is a well defined linear transformation.
For a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$, define

$$f(T) = \sum_{i=0}^{n} a_i T^i = a_0 I_v + a_1 T + \cdots + a_n T^n$$

The *identity map* is as follows:

$$\begin{aligned} T^0 = I_V &: V \to V \\ v &\mapsto I_V(v) := v \end{aligned}$$

The compositions are then linear transformations:

$$\begin{aligned} T^2 &:= T \circ T \\ T^3 &:= T \circ T \circ T \\ &\dots \\ T^n &:= T \circ \cdots \circ T (n \text{ times}) \end{aligned}$$

Define the action:

$$\begin{aligned} F[x] \times V &\to V \\ (f(x), v) &\mapsto f(x)v := f(T)(v) \end{aligned}$$

This action makes V a left $F[x]$-module, depending on linear transformation $T : V \to V$.
Hence given a vector space V over F, there may be different left $F[x]$-module structures. If $W \subseteq V$ is a *T-invariance subspace*, i.e. $T(W) \subseteq W$, then W is a left $F[x]$-submodule of V since

$$f(x)(w) = f(T)(w) \in W, \ \forall f(x) \in F[x], \ \forall w \in W$$

Proposition 4.1.0.12. *(Submodule Criterion) Let R be a ring with 1 and M a left R-module. let $N \subseteq M$ be a nonempty subset. Then the following are equivalent:*

(i) N is a left R-submodule of M.

(ii) $\forall r \in R$, $\forall x, y \in N \Rightarrow x + ry \in N$

Definition 4.1.0.13. An element m of a left R-module is a *torsion element* if $rm = 0$ for some nonzero $r \in R$.

$$\mathrm{Tor}(M) := \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}$$

is the set of all torsion elements in M.

Proposition 4.1.0.14. *If R is an integral domain, then* Tor*(M) is a R-submodule of M called the torsion submodule of M.*

Definition 4.1.0.15. Le R be a ring. The *centre $Z(R)$ of the ring R* is defined and denoted

$$Z(R) := \{z \in R \mid zr = rz, \ \forall r \in R\}$$

Remark 4.1.0.16. The centre $Z(R)$ is a commutative subring of R.

Remark 4.1.0.17. A ring R is commutative if and only if $Z(R) = R$.

Definition 4.1.0.18. Let R be a commutative ring with 1_R. A *R-algebra* is a ring A with 1_A and ring homomorphism $f : R \to A$ such that

(i) $f(1_R) = 1_A$; and

(ii) $f(R) \subseteq Z(A)$

For simplicity, write $ra := f(r)a$. Note that $\forall r \in R$, $\forall a, b \in A$

$$\begin{aligned} ra &= ar \\ r(ab) = (ra)b &= a(rb) = a(br) = (ab)r \end{aligned}$$

A R-algebra A has natural left (resp. right) R-module structure given as:

$$\begin{aligned} R \times A \to A \ ; \quad A \times R &\to A \\ (r, a) \mapsto ra \ ; \quad (a, r) &\mapsto ar = ra \end{aligned}$$

Definition 4.1.0.19. Let A and B be two R-algebras.
An *R-algebra homomorphism* is a ring homomorphism $\varphi : A \to B$ such that $\forall r \in R, \forall a \in A$

(i) $\varphi(1_A) = 1_B$, and

(ii) $\varphi(ra) = r\varphi(a)$

An *R-algebra isomorphism* $\varphi : A \to B$ is a R-algebra homomorphism which is bijective.
In this case, the inverse $\varphi^{-1} : B \to A$ is also an R-algebra isomorphism.

Remark 4.1.0.20. If A is an R-algebra, then A is a ring with 1_A which is a unital left R-module satisfying

$$(*) \qquad r(ab) = (ra)b = a(rb), \ \forall r \in R, \ \forall a, b \in A$$

Conversely, if R is a commutative ring with 1_r and A is a ring with 1_A which is a unital left R-module satisfying the condition $(*)$ above, then A is an R-algebra by defining

$$\begin{aligned} f : R &\to A \\ r &\mapsto r1_A \end{aligned}$$

The condition $(*)$ is used as the defining axiom for A to be an R-algebra.

4.2 Module Homomorphisms

Assume for this section that ring R has 1. Modules are assumed to be left R-modules.

Definition 4.2.0.1. Let R be a ring, and M, N be left R-modules. A map $\varphi : M \to N$ is a (left) R-module homomorphism if it respects the R-module structures of M and N, i.e.,

(i) $\varphi(x + y) = \varphi(x) + \varphi(y),\ \forall x, y \in M$; and

(ii) $\varphi(rx) = r\varphi(x),\ \forall r \in R,\ \forall x \in M$

Definition 4.2.0.2. Let R be a ring, and M, N be left R-modules. A (left) R-module homomorphism $\varphi : M \to N$ is an isomorphism (of R-modules) if it is bijective. In this case, M and N are *isomorphic*, denoted

$$\varphi : M \xrightarrow{\sim} N, \text{ or}$$
$$M \cong N, \text{ or } \ M \simeq N$$

Definition 4.2.0.3. Let R be a ring, and M, N be left R-modules.
If $\varphi : M \to N$ is a left R-module isomorphism, define and denote the *kernel of φ* as

$$\ker \varphi = \varphi^{-1}(0_N) = \{m \in M \mid \varphi(m) = 0\}$$

The *image* is defined as

$$\varphi(M) := \{n \in N \mid n = \varphi(m), \text{ for some } m \in M\}$$

Definition 4.2.0.4. Let R be a ring, and M, N be left R-modules.
Let below be the set of all left R-module homomorphisms from M into N:

$$\mathrm{Hom}_R(M, N) := \{\varphi : M \to N \mid \varphi \text{ is a left } R\text{-module homomorphism}\}$$

When $M = N$, a left R-module $\varphi : M \to M$ is an *endomorphism* of the left R-module M.
This is denoted $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$

Remark 4.2.0.5. Let $\varphi : M \to N$ be a left R-module homomorphism.
Then $\ker \varphi$ is a left R-submodule of N, while the image $\varphi(M)$ is a left R-submodule of N.
Moe generally, for any left R-submodule M_i of M, the image $\varphi(M_i)$ is a left R-submodule of N.

Example 4.2.0.6. Let M be a left R-module and N a left R-submodule of M. Then the inclusion map

$$\iota : N \to M$$
$$n \mapsto n$$

is a homomorphism of left R-modules.

Proposition 4.2.0.7. *Let R be a ring with 1. Let M, N be left R-modules.*
A map $\varphi : M \to N$ is a left R-module homomorphism if and only if:

$$\varphi(rx + y) = r\varphi(x) + \varphi(y),\ \forall r \in R;\ \forall x, y \in M$$

Proposition 4.2.0.8. *Let R be a ring with 1. Let M, N be left R-modules.*
Let $\varphi_i \in \mathrm{Hom}_R(M, N)$ and $\alpha_i \in R$. Then the linear combination belongs to $\mathrm{Hom}_R(M, N)$:

$$\alpha_1\varphi_1 + \alpha_2\varphi_2 : M \to N,$$
$$m \mapsto (\alpha_1\varphi_1 + \alpha_2\varphi_2)(m) := \alpha_1\varphi_1(m) + \alpha_2\varphi_2(m)$$

In particular,

$$\varphi_1 + \varphi_2 \in \mathrm{Hom}_R(M, N)$$
$$\alpha_1\varphi_1 \in \mathrm{Hom}_R(M, N)$$

The addition is defined as

$$+ : R \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$$
$$(\varphi_1, \varphi_2) \mapsto \varphi_1 + \varphi_2$$

The action is defined as

$$R \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$$
$$(\alpha, \varphi) \mapsto \alpha\varphi$$

Hence we get a left R-module structure on the additive group $(\mathrm{Hom}_R(M, N), +)$.

Proposition 4.2.0.9. *Let R be a ring with 1. Let M, N, L be left R-modules. If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$, then the composition is*

$$\psi \circ \varphi \in \mathrm{Hom}_R(L, N)$$

Proposition 4.2.0.10. *Let R be a ring with 1. Let M, N be left R-modules. The natural ring structure (with multiplicative identity 1) is $(\mathrm{Hom}_R(M, M), +, \circ)$ on the set $\mathrm{Hom}_R(M, M)$, where the addition $+$ is defined above, and $\circ$ is a composition (Note that $\varphi \circ \psi$ is not $\varphi \times \psi$). The identity map*

$$\begin{aligned} I_M : M &\to M \\ m &\mapsto I_M(m) := m \end{aligned}$$

serves as the multiplicative identity of the ring $\mathrm{Hom}_R(M, M)$. The Endomorphism ring of the left R-module M is $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$.

Proposition 4.2.0.11. *Let R be a ring with 1. Let M, N be left R-modules. Suppose that R is commutative. Then for $\alpha \in R$, the scalar map below belongs to $\mathrm{Hom}_R(M, M)$:*

$$\begin{aligned} \alpha I_M : M &\to M \\ m &\mapsto \alpha M \end{aligned}$$

The map below is a ring homomorphism

$$\begin{aligned} f : R &\to \mathrm{Hom}_R(M, M) \\ \alpha &\mapsto \alpha I_M \end{aligned}$$

with $f(R) \subseteq Z(\mathrm{Hom}_R(M, M))$ (the centre) with which $\mathrm{Hom}_R(M, M)$ becomes an R-algebra.

Proposition 4.2.0.12. *Let R be a ring, M a left R-module, N a left R-submodule, and M/N the quotient additive abelian group. The action*

$$\begin{aligned} R \times (M/N) &\to M/N \\ (r, \overline{m} = m + N) &\mapsto \overline{rm} \end{aligned}$$

is well-defined and makes M/N into a left R-module, called the quotient left R-module of M by N.

Proposition 4.2.0.13. *Let R be a ring, M a left R-module, N a left R-submodule, and M/N the quotient additive abelian group. The quotient map*

$$\begin{aligned} \gamma : M &\to M/N \\ m &\mapsto \overline{m} = m + N \end{aligned}$$

is a left R-module surjective homomorphism with $\ker \gamma = N$.

Remark 4.2.0.14. Let $N_1, \ldots, N_k$ be left R-submodules of a left R-module M. Then the addition $N_1 + \cdots + N_k$ is a left R-submodule of M, and is the smallest among all left R-submodules of M containing all N_i. The sum is defined as

$$N_1 + \cdots + N_k := \{\sum_{i=1}^{k} n_i \mid n_i \in N_i\}$$

4.3 Module Isomorphism Theorems

Assume for this section that ring R has 1. Modules are assumed to be left R-modules.

Theorem 4.3.0.1. *(First Isomorphism Theorem) Let M, N be left R-modules and let $\varphi : M \to N$ be a left R-module homomorphism. Then $\ker \varphi$ is a left R-submodule of M and*

$$M/(\ker \varphi) \cong \varphi(M)$$

Theorem 4.3.0.2. *(Second Isomorphism Theorem) Let A, B be left R-submodules of the left R-module M. Then*

$$A/(A \cap B) \cong (A + B)/B$$

Theorem 4.3.0.3. *(Third Isomorphism Theorem) Let M be a left R-module, and let A, B be left R-submodules of M with $A \subseteq B$. Then*

$$M/B \cong (M/A)/(B/A)$$

Theorem 4.3.0.4. *(Fourth Isomorphism Theorem)/ Corresponding Theorem for Modules*
Let N be a left R-submodule of the left R-module M. There is a bijection between the left R-submodules of M which contains N and the left R-submodules of M/N. The correspondence is given by

$$A \leftrightarrow A/N$$

for all $A \supseteq N$. This correspondence commutes with the processes of taking additions and intersections.

4.4 Module Generation

Definition 4.4.0.1. Let M be a left R-module and let $N_1, \ldots, N_n$ be left R-submodules of M.
Addition is defined as

$$N_1 + \cdots + N_n = \{\sum_{i=1}^{n} a_i \mid a_i \in N_i\}$$

which is a left R-submodule of M.

Definition 4.4.0.2. Let M be a left R-module and let $N_1, \ldots, N_n$ be left R-submodules of M.
For any subset $A \subseteq M$, let

$$RA := \{\sum_{i=1}^{s} r_i a_i \mid r_i \in R,\ a_i \in A,\ s \geq 1\}$$

RA is a left R-submodule of M and is the smallest among all left R-submodules of M containing A.
RA is the *submodule of M generated by A*. If $A = \{a_i, \ldots, a_t\}$, then

$$RA = Ra_1 + \cdots + Ra_t = \{\sum_{i=1}^{t} \mid r_i \in R\}$$

If N is a left R-submodule of M and $N = RA$ for some subset $A \subseteq M$, then A is a *set of generators* or *generating set for N*. Then N is *generated by A*.

Definition 4.4.0.3. Let M be a left R-module and let $N_1, \ldots, N_n$ be left R-submodules of M.
A submodule N of M (possibly $N = M$) is *finitely generated* if there is some finite subset A of M such that $N = RA$, that is, if N is generated by some finite subset.

Definition 4.4.0.4. Let M be a left R-module and let $N_1, \ldots, N_n$ be left R-submodules of M.
A left R-submodule N of M (possibly $N = M$) is *cyclic* if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element:

$$N = Ra = \{ra \mid r \in R\}$$

Definition 4.4.0.5. Let $M_1, \ldots, M_k$ be a finite collection of left R-modules. The direct product

$$M := M_1 \times \cdots \times M_k := \{(m_1, \ldots, m_k) \mid m_i \in M_i\}$$

has a natural left R-module structure. Define the addition

$$+ : M \times M \to M$$
$$(X = (x_1, \ldots, x_k), Y = (y_1, \ldots, y_k)) \mapsto X + Y := (x_1 + y_1, \ldots, x_k + y_k)$$

Define the R-action as:

$$R \times M \to M$$
$$(r, Y = (y_1, \ldots, y_k)) \mapsto rY := (ry_1, \ldots, ry_k)$$

Then $M = M_1 \times \cdots \times M_k$ is a left R-module called the *direct product* of $M_1, \ldots, M_k$.
More generally, the direct product can be defined as $\Pi_{\alpha \in \sum}$, any collection of left R-modules M_α ($\alpha \in \sum$, where $\sum$ may not be finite or countable).

Proposition 4.4.0.6. *Let $N_1, \ldots, N_k$ be submodules of the left R-module M. Then the following are equivalent:*

(i) The map

$$\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$$
$$(a_1, \ldots, a_k) \mapsto a_1 + \cdots + a_k$$

is an isomorphism of left R-modules. Namely, $N_1 \times \cdots \times N_k \cong N_1 + \cdots + N_k$.

(ii) $N_j \ \cap \ (N_1 + \cdots + \mathbb{N}_{j-1}) = 0$, $(\forall 2 \leq j \leq k)$.

(iii) $N_k \ \cap \ (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots +_k) = 0$, $(\forall 1 \leq j \leq k)$

(iv) Every $r \in N_1 + \cdots + N_k$ can be written uniquely in the form $r = a_1 + \cdots + a_k$ with $a_i \in N_i$.

Definition 4.4.0.7. If a left R-module $M = N_1 + \cdots + N_k$ is the sum of left R-submodules $N_1, \ldots, N_k$ satisfying the equivalent conditions in Proposition 4.4.0.6, then M is the *(internal) direct sum* of $N_1, \ldots, N_k$, and is denoted as $M = N_1 \oplus \cdots \oplus N_k$.

Remark 4.4.0.8. Let $M := M_1 \times \cdots \times M_k := \{(m_1, \ldots, m_k) \mid m_i \in M_i\}$ be the product of left R-modules M_i as in Definition 4.4.0.5. Let

$$N_i = \{(0, \ldots, 0, a_i, 0, \ldots, 0) \mid a_i \in M_i \text{ is at } i\text{-th positiion}\}$$

Then $M_i \cong N_i$ (as left R-module), and $M = N_1 \oplus \cdots \oplus N_n$.
Similarly, identify $M_i = N_i$ and write $M = M_1 \oplus \cdots \oplus M_n$.
So the direct product $M = M_1 \times \cdots \times M_n$ of finitely many modules M_i is just the direct sum $M_1 \oplus \cdots \oplus M_n$ of M_i identified with the submodule of M:

$$\{0_{M_1}\} \times \cdots \times \{0_{M_{i-1}}\} \times \{0_{M_i}\} \times \{0_{M_{i+1}}\} \times \cdots \times \{0_{M_n}\}$$

Theorem 4.4.0.9. *(Chinese Remainder Theorem for Modules) Let R be a commutative ring with 1, and A_i ideals of R which are pairwise comaximal (i.e., $A_i + A_j = R$, $\forall i \neq j$). Then*

$$A_1 \ \cap \cdots \cap \ A_k = A_1 \cdots A_k$$
$$M/(A_1, \ldots, A_k)M \cong M/(A_1 M) \times \cdots \times M/(A_k M)$$

Definition 4.4.0.10. A left R-module F is *free on the subset* A of F if for every nonzero $x \in F$, there exists unique nonzero elements $r_1, \ldots, r_n \in R$ and unique $a_1, \ldots, a_n \in A$ such that

$$x = r_1 a_1 + \cdots + r_n a_n$$

In this situation, A is a *basis or set of free generators* for F.
If R is a commutative ring, the *rank* of F is defined as $|A|$, the cardinality of A.

Theorem 4.4.0.11. *For any set A there is a free left R-module $F(A)$ on the set A and $F(A)$ satisfies the universal property: If M is any left R-module and $\varphi : A \to M$ is any map of sets, then there is a unique left R-module homomorphism such that $\varphi = \Phi \circ \iota$ where $\iota : A \to F(A)$ is the inclusion map.*
When $A = \{a_1, \ldots, a_n\}$ is a finite set, $F(a) = Ra_1 \oplus \cdots \oplus Ra_N \cong R^n$ (as left R-modules).

Corollary 4.4.0.12. *If F_1, F_2 are free left R-modules on the same set A, then there is a unique isomorphism $\varphi : F_1 \to F_2$ such that the restriction $\varphi|_A$ equals the identity map*

$$Id_A : A \to A$$
$$a \mapsto Id_A(a) = a$$

Corollary 4.4.0.13. *If F is any free left R-module with basis A, then $F \cong F(A)$ (as left R-modules). In particular, F enjoys the same universal property with respect to A as $F(A)$ does in Theorem 4.4.0.11.*

Remark 4.4.0.14. More generally, let A_1, A_2 be two sets and $\varphi_0 : A_1 \to A_2$ a bijection.
Then there is a unique isomorphism (of left R-modules):

$$\varphi : F(A_1) \to F(A_2)$$

such that $\varphi|_{A_1} = \varphi_0$.

Remark 4.4.0.15. Let M_i $(1 \leq i \leq n)$ be left R-submodules of M.
Suppose that $M_1 + \cdots + M_n = M_1 \oplus \cdots \oplus M_n$ is a direct sum and each M_i is a free left R-module with basis A_i, then $M_1 + \cdots + M_n$ is a free left R-module with a basis $\Pi_{i=1}^n A_i$ (a disjoint union).

Remark 4.4.0.16. If F is a free left R-module with basis A, then define the left R-module homomorphism $\varphi : F \to N$ from F into other left R-module N by simply specifying their φ-values on the elements of A and then extend by linearity (apply Theorem 4.4.0.11 to $F = F(A)$).

Remark 4.4.0.17. When $R = \mathbb{Z}$, the free module on set A is the *free abelian group on A*.
If $A = a_1, \dots, a_n$, then $F(A)$ is the free abelian group of rank n (with basis A). Then

$$F(A) = \mathbb{Z}a_i \times \cdots \times \mathbb{Z}a_n \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \ (n \text{ times})$$

4.5 Modules over PID

Definition 4.5.0.1. Let R be a ring and M a left R-module.
The left R-module M is said to be a *Noetherian* R-module or to satisfy the Ascending Chain Condition on submodules (or *ACC* on submodules) if there are no infinite ascending chains of submodules, ie., whenever

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

is an ascending chain of left R-submodules of M, then there is a positive integer m such that

$$M_m = M_{m+1} = M_{M+2} = \cdots$$

The ring R is said to be *Noetherian* if it is Noetherian as a left module over itself, i.e., there are no infinite ascending chains of left ideals in R.

Theorem 4.5.0.2. *Let R be a ring with 1 and M a left R-module. Then the following are equivalent:*

(i) M is a Noetherian left R-module

(ii) Every nonempty set of submodules of M contains a maximal element under inclusion

(iii) Every submodule of M is finitely generated.

Corollary 4.5.0.3. *A PID is Noetherian ring*

Proposition 4.5.0.4. *Let R be an integral domain and M a free R-module of rank $n < \infty$.
Then any $n+1$ elements of M are R-linearly dependent, i.e. for any $y_1, \dots, y_{n+1} \in M$, there are elements $r_1, \dots r_{n+1} \in R$, not all zero, such that*

$$r_1 y_1 + \cdots + r_{n+1} y_{n+1} = 0$$

Definition 4.5.0.5. Let R be an integral domain and M an R-module.

(i) *R-linearly (in)dependent* subset A of M can be defined as in linear algebra.

(ii) The *rank* of an R-module M is the maximal number of R-linearly independent elements of M. Hence it is either a finite number or infinity.

Remark 4.5.0.6. If A is a linearly independent subset of M, then the R-submodule

$$RA = \{\sum_{i=1}^{n} r_i a_i \mid r_i \in R, a_i \in A, n \geq 1\}$$

of M is a free R-module with a basis A.
Thus, if M has a rank $r \in \mathbb{Z}_{>0}$ then M contains an R-submodule isomorphic to R^r.

Theorem 4.5.0.7. *Let R be a PID, M a free R-module of finite rank n, and N a R-submodule of M. Then*

(i) N is a free R-module of rank $m \leq n$, and

(ii) There exist a basis $\{y_1, \leq, y_n\}$ of M such that $\{a_1 y_1, \dots, a_m y_m\}$ is a basis of N, where $a_1, \leq, a_m$ are nonzero elements of R with the divisibility relations $a_1 \mid a_2 \mid \cdots \mid a_m$.

Proposition 4.5.0.8. *Let M be a left R-module, and N_i, M_i submodules such that $N_i \subseteq M_i$.
Suppose that $M_1 + \cdots + M_k = M_1 \oplus \cdots \oplus M_k$. Then $N_1 + \cdots + N_k = N_1 \oplus \cdots \oplus N_k$.*

Definition 4.5.0.9. Note that a left R-module C is cyclic if $C = Ra$ for some $a \in C$.
In this case, the surjective homomorphism

$$\begin{aligned} \gamma : R &\to C \\ r &\mapsto ra \end{aligned}$$

induces an isomorphism $R/\ker\varphi \cong C$.
Conversely, for every left ideal I of R, the quotient ring R/I is a cyclic left R-module since $R/I = R\overline{1_R}$ with $\overline{1_R} = 1_R + I \in R/I$.

Definition 4.5.0.10. Let M be a left R-module.

(i) An element $m \in M$ is a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of all torsion elements in M is denoted

$$\mathrm{Tor}(M) := \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}$$

(ii) The left R-module M is *torsion free* if $\mathrm{Tor}(M) = \{0\}$.

(iii) M is a *torsion module* if $\mathrm{Tor}(M) = M$.

(iv) Suppose R is an integral domain. Then $\mathrm{Tor}(M)$ is a left R-submodule of M, and every free module $N = R^n$ has $\mathrm{Tor}(N) = 0$.

(v) If R is a field, then $\mathrm{Tor}(M) = 0$.

Theorem 4.5.0.11. *Let R be PID and M a finitely generated R-module. Then*

(i) $M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$ for some $r \geq 0$ and nonzero elements $a_1, \ldots, a_m$ of R which are not units in R and which satisfies the divisibility relations $a_1 \mid a_2 \mid \cdots \mid a_m$.

(ii) M is torsion free if and only if M is a free left R-module.

*(iii) In the decomposition in (i), $\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$ so that $M/\mathrm{Tor}(M) \cong R^r$.
In particular, M is a torsion module if and only if $r = 0$, and in this case $aM = 0 \Leftrightarrow a_m \mid a$.
The annihilator is defined $\mathrm{Ann}(M) := \{r \in R \mid rM = 0\}$ equals (a_m).*

Definition 4.5.0.12. The integer r in Theorem 4.5.0.11 is the *free rank* or *Betti number* of M.
The elements $a_1, \ldots, a_m \in R$ (defined up to multiplication by units in R) are the *invariant factors of M*.

Theorem 4.5.0.13. *Let R be a PID and M a finitely generated R-module. Then*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where $r \geq 0$ is an integer and $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are positive powers of (not necessarily distinct or non-associate primes in R). Furthermore,

$$\mathrm{Tor}(M) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

and $M/\mathrm{Tor}(M) \cong R^r$.

Definition 4.5.0.14. Let R be a PID and M a finitely generated R-module as in Theorem 4.5.0.13. The prime powers $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ (defined up to multiplication by units in R) are *elementary divisors of M*.

Theorem 4.5.0.15. *Let R be a PID. Then*

(i) Two finitely generated R-modules M_1 and M_2 are isomorphic if and only if they have the same free rank and the same list of invariance factors.

(ii) Two finitely generated R-modules M_1 and M_2 are isomorphic if and only if they have the same free rank and the same list of elementary factors.

Theorem 4.5.0.16. *(Fundamental Theorem of Finitely Generated Abelian Groups: Invariant Factor Form)
Let G be a finitely generated abelian group. Then*

(i) $G \cong \mathbb{Z}^r \times \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_u)$ for some integers $r, n_1, \ldots, n_u$ satisfying the following conditions

a. $r \geq 0$; $n_j \geq 2$ $(\forall j)$; and

b. the divisibility relations $n_1 \mid n_2 \mid \cdots \mid n_u$

(ii) The expression in (i) is unique if $G \cong \mathbb{Z}^t \times \mathbb{Z}/(nm1) \times \cdots \times \mathbb{Z}/(m_v)$ where t and $m_1, \ldots, m_v$ satisfy (i)(a) and (i)(b), then $t = r$, $v = u$, and $m_i = n_i$ $(\forall i)$.

Definition 4.5.0.17. The integer r in Theorem 4.5.0.16 is the *free rank* or *Betti number of G* and the integers $n_1, \ldots, n_u$ are *invariant factors of G*.
The description of G in Theorem 4.5.0.16 is the *invariant factor decomposition of G*.

Theorem 4.5.0.18. *(Fundamental Theorem of Finitely Generated Abelian Groups: Elementary Divisor Form)*
Let G be an abelian group of order $n \geq 1$ and let the unique factorisation of n into distinct prime powers be $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then

(i) $G \cong A_1 \times \cdots \times A_k$ where $|A_i| = p_i^{\alpha_i}$

(ii) For each $A = A_i \in \{A_1, \ldots, A_k\}$ with $|A| = p^\alpha$,

$$A \cong \mathbb{Z}/(p^{\beta_1}) \times \cdots \times \mathbb{Z}/(p^{\beta_t}$$

with $1 \leq \beta_1 \leq \cdots \leq \beta_t$ and $\beta_1 + \cdots + \beta_t = \alpha$, where t and $\beta_1, \ldots, \beta_t$ depend on i.

(iii) The decomposition in (i) and (ii) is unique if $G \cong B_1 \times \cdots \times B_t$ with $|B_i| = p_i^{\alpha_i}$ for all i, then $B_i \cong A_i$ and B_i and A_i have the same invariant factors.

Definition 4.5.0.19. The integers p^{β_j} in Theorem 4.5.0.18 are the *elementary divisors of G*.
The description of G in Theorem 4.5.0.18 is the *elementary divisor decomposition of G*.

4.6 Rational Canonical Form of a Matrix

Definition 4.6.0.1. A monic polynomial $m_T(x) = x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0 \in R = F[x]$ is a *minimal polynomial* of the linear transformation $T : V \to V$ if:

(i) $m_T(T) = 0$, the zero map (i.e., $m_T(x)V = 0$), and

(ii) every nonzero $g(x) \in R$ with $g(T) = 0$ (i.e., $g(x)V = 0$ has degree $\deg g(x) \geq \deg m_T(x)$)

For any polynomial $g(x) \in R$, $g(T) = 0 \Rightarrow m_T(x)|g(x)$.
Minimal polynomial $m_T(x)$ is unique.

Theorem 4.6.0.2. *(Minimal Polynomial as the Annihilator)*

(i) V is a torsion $R = F[x]$-module

(ii) More precisely, $r(x)V = 0$ if and only if $m_T(x) \mid r(x)$.

Theorem 4.6.0.3. *(Fundamental Theorem for Vector Space, Existence: Invariant Factor Form)*
Let V be a finite-dimensional vector space over a field F and $T : V \to V$ a linear transformation, so that V is an $R = F[x]$-module: $f(x)v := f(T)(v)$. Then:

(i) $V \cong R/(a_1(x)) \oplus \cdots \oplus R/(a_m(x))$ where (the invariant factors) $a_i(x) \in R = F[x]$ are non-constant monic polynomials such that $a_1(x) \mid \cdots \mid a_m(x)$.

(ii) For any $r(x) \in R$, $r(x)V = 0 \Leftrightarrow a_m(x) \mid r(x)$.

(iii) There is equality $a_m(x) = m_T(x)$, the minimal polynomials of T.

Theorem 4.6.0.4. *(Invariant Factors via Row Operations)*
Let V be an n-dimensional vector space over a field F. Let $T : V \to V$ be a linear transformation.
Let $A = [T]_B$ be the representation matrix of T relative to a basis B of V.
Then the matrix $xI - A \in M_n(R)$ in the matrix ring $M_n(R)$ (with entries in $R = F[x]$) is row equivalent to the following diagonal matrix: $\mathrm{Diag}[1, \ldots, 1, a_1(x), \ldots, a_m(x)] \in M_n(R)$ by the usual three types of row operations:

(i) interchanging two rows

(ii) adding a multiple of a row by some $f(x) \in R = F[x]$ to another row

(iii) multiplying a row by a nonzero scalar $\alpha in F$

where $a_1(x) \mid \cdots \mid a_m(x)$ is the list of invariant factors in Theorem 4.6.0.3.

Definition 4.6.0.5. The *companion matrix* of the polynomial
$a_i(x) = x^{s_i} + c(i)_{s_i-1}x^{s_i-1} + \cdots + c(i)_1 x + c(i)_0$ is the representation matrix

$$[T|_{V_{\alpha_i}}]_{B_i} = C_{\alpha_i(x)} = \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -c_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -c_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -c_2 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & 1 & -c_{s_i-1} \end{pmatrix}$$

Definition 4.6.0.6. A matrix is in *canonical form* if it is of the form $\mathrm{Diag}[C_{\alpha_1(x)}, \ldots, C_{\alpha_m(x)}]$ where $a_i(x)$ are nonconstant monic polynomials with $a_1(x) \mid \cdots \mid a_m(x)$, and $C_{\alpha_i(x)}$ is the companion matrix of the polynomial $a_i(x)$. The polynomials $a_i(x)$ are the *invariant factors* of the matrix.
A rational canonical form for a linear transformation $T : V \to V$ is a representation matrix $[T]_B$ which is in rational canonical form.

Theorem 4.6.0.7. *(Existence of the Rational Canonical Form of a Linear Transformation)*
Let V be a finite-dimensional vector space over a field F, and let $T : V \to V$ be a linear transformation. Then

(i) V has a basis B such that the representation matrix $[T]_B$ is in rational canonical form:

$$[T]_B = \mathrm{Diag}[C_{\alpha_1(x)}, \ldots, C_{\alpha_m(x)}]$$

where $a_i(x)$ are nonconstant monic polynomials, $C_{\alpha_i(x)}$ is the companion matrix of polynomial $a_i(x)$, and

$$a_1(x) \mid \cdots \mid a_m(x)$$

(ii) The rational canonical form for T is unique.

5 Category Theory

Category theory provides the language and mathematical foundations for discussion of properties of large classes of mathematical objects, such as the class of 'all class' or 'all groups'. With this framework, we can explore commonality across classes of concepts and methods used in the study of each class, and introduce tools for studying relations between classes.

5.1 Categories, Functors, and Natural Transformations

5.1.1 Introduction

Observe that many properties of mathematical systems can be unified and simplified with diagrams of arrows, where each arrow $f : X \to Y$ represents a function from a set X to a set Y, and a rule $x \mapsto fx$ which assigns each element $x \in X$ to an element $fx \in Y$.
A diagram of sets and functions is commutative when h is $h = g \circ f$, where $g \circ f$ is the usual composite function $g \circ f : X \to Z$, defined by $x \mapsto g(fx)$.

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[dr, "f"'] & Z \arrow[d, "g"] \\ & Y \end{tikzcd}$$

Figure 4: An example of a commutative diagram.

Many other properties of mathematical constructions may be represented by universal properties of diagrams. Consider the cartesian product $X \times Y$ of two sets, consisting of ordered pairs $\langle x, y\rangle$ of elements $x \in X, y \in Y$. The projections $\langle x, y\rangle \mapsto x$, $\langle x, y\rangle \mapsto y$ of the product on the axes X, Y are functions $p : X \times Y \to X$, $q : X \times Y \to Y$. Any function $h : W \to X \times Y$ from a third set W is uniquely determined by its composites $p \circ h$, $q \circ h$. Conversely, given W and two functions f, g as in diagram below, there is a unique function h which makes the diagram commute, namely $hw = \langle fw, gw\rangle$ for each $w \in W$:

$$\begin{tikzcd} & W \arrow[dl, "f"'] \arrow[d, "h"] \arrow[dr, "g"] & \\ X & X \times Y \arrow[l, "p"] \arrow[r, "q"'] & Y \end{tikzcd}$$

Figure 5: Cartesian product on the sets.

Definition 5.1.1.1. A *category* $\mathfrak{C}$ consists of a *class of objects* $Ob(\mathfrak{C})$ and sets of morphisms between these objects. For every ordered pair A, B of objects there is a set $\hom_{\mathfrak{C}}(A, B)$ morphisms from A to B, and for every ordered triple A, B, C of objects there is a *law of composition* of morphisms (i.e., a map)

$$\hom_{\mathfrak{C}}(A, B) \times \hom_{\mathfrak{C}}(B, C) \to \hom_{\mathfrak{C}}(A, C)$$

where $(f, g) \mapsto gf$, and gf is the composition of g with f. The objects and morphism satisfy the following axioms for objects A, B, C, D:

(i) if $A \neq B$ or $C \neq D$, then $\hom_{\mathfrak{C}}(A, B)$ and $\hom_{\mathfrak{C}}(C, D)$ are disjoint sets;

(ii) Associative Law: $h(gf) = (hg)f \quad \forall f \in \hom_{\mathfrak{C}}(A, B)$, $g \in \hom_{\mathfrak{C}}(B, C)$, $h \in \hom_{\mathfrak{C}}(C, D)$

(iii) Identity Law: $1_B \circ f = f$, $g \circ 1_B = g \quad \forall f \in \hom_{\mathfrak{C}}(A, B)$, $g \in \hom_{\mathfrak{C}}(B, C)$ given identity $1_B \in \hom_{\mathfrak{C}}(B, B)$

Definition 5.1.1.2. A morphism from A to B will be denoted by $f : A \to B$ or $A \xrightarrow{f} B$.
The object A is the *domain* of f, and B is the *codomain* of f.
A morphism from A to A is an *endomorphism* of A.
A morphism $f : A \to B$ is an *isomorphism* if there is a morphism $g : B \to A$ such that $gf = 1_A$ and $gf = 1_B$.
A *subcategory* category $\mathfrak{C}$ of $\mathfrak{D}$ is such that every object of $\mathfrak{C}$ is also an object in $\mathfrak{D}$, and for objects $A, B \in \mathfrak{C}$, we have $\hom_{\mathfrak{C}}(A, B) \subseteq \hom_{\mathfrak{D}}(A, B)$.

Example 5.1.1.3.

(i) **Set** is the category of all sets. For any two sets A, B, $\hom(A, B)$ is the set of all functions from A to B. Composition of morphisms is the composition of functions $gf = g \circ f$. The identity in $\hom(A, A)$ is the map $1_A(a) = a \ \forall a \in A$. This category contains the category of all finite sets as a subcategory.

(ii) **Grp** is the category of all groups, and morphisms are group homomorphisms. The composition of group homomorphisms are group homomorphisms. A subcategory of **Grp** is **Ab**, category of all abelian groups.

(iii) **Ring** is the category of all nonzero rings with 1, where morphism are ring homomorphisms that send 1 to 1. The category **CRing** of all commutative rings with 1 is a subcategory of **Ring**. For a fixed ring R, the category R-**mod** consists of all left R-modules with morphisms being R-module homomorphisms.

(iv) **Top** is the category whose objects are topological spaces, and morphisms are continuous maps between topological spaces. The identity (set) map from a space to itself is continuous in every topology, so $\hom(A, A)$ always have an identity.

(v) If G is a group, we can form the category $\mathbf{G}$ where the only object is G, and $\hom(G, G) = G$. The composition of two functions f, g is the product gf in group G. The identity morphism is identity of G.

Definition 5.1.1.4. Let $\mathfrak{C}$ and $\mathfrak{C}$ be categories. Then $\mathcal{F}$ is a *covariant functor* from $\mathfrak{C}$ to $\mathfrak{D}$ if:

(i) for every object A in $\mathfrak{C}$, $\mathcal{F}A$ is an object in $\mathfrak{D}$, and

(ii) for every $f \in \hom_{\mathfrak{C}}(A, B)$ we have $\mathcal{F}(f) \in \hom_{\mathfrak{D}}(\mathcal{F}A, \mathcal{F}B)$ such that the following axioms are satisfied:

1. if gf is a composition of morphisms in $\mathfrak{C}$, then $\mathcal{F}(gf) = \mathcal{F}(g)\mathcal{F}(f)$ in $\mathfrak{D}$, and
2. $\mathcal{F}(1_A) = 1_{\mathcal{F}A}$.

Definition 5.1.1.5. Let $\mathfrak{C}$ and $\mathfrak{C}$ be categories. Then $\mathcal{F}$ is a *contravariant functor* from $\mathfrak{C}$ to $\mathfrak{D}$ if:

(i) for every object A in $\mathfrak{C}$, $\mathcal{F}A$ is an object in $\mathfrak{D}$, and

(ii) for every $f \in \hom_{\mathfrak{C}}(A, B)$ we have $\mathcal{F}(f) \in \hom_{\mathfrak{D}}(\mathcal{F}B, \mathcal{F}A)$ such that the following axioms are satisfied:

1. if gf is a composition of morphisms in $\mathfrak{C}$, then $\mathcal{F}(gf) = \mathcal{F}(f)\mathcal{F}(g)$ in $\mathfrak{D}$, and
2. $\mathcal{F}(1_A) = 1_{\mathcal{F}A}$.

Contravariant functors reverse the arrows.

Example 5.1.1.6.

(i) The identity function $\mathcal{I}_{\mathcal{C}}$ maps any category $\mathfrak{C}$ to itself by sending objects and morphisms to themselves. If $\mathfrak{C}$ issubcategory of $\mathfrak{D}$, *inclusion functor* maps $\mathfrak{C}$ into $\mathfrak{D}$ by sending objects, morphisms to themselves.

(ii) Let $\mathcal{F}$ be the function from **Grp** to **Set** that maps any group G to the same set G and any group homomorphism φ to the same set map φ. This is the *forgetful functor* as it 'removes' or 'forgets' the structure of the groups and the homomorphism between them.

(iii) The *abelianizing functor* maps **Grp** to **Ab** by sending each group G to the abelian group $G^{ab} = G/G'$, where G' is the commutator subgroup of G. Each group homomorphism $\varphi : G \to H$ is mapped to the induced homomorphism on quotient groups:

$$\overline{\varphi} : G^{ab} \to H^{ab} \quad \text{by} \quad \overline{\varphi}(xG') = \varphi(x)H'$$

The definition of commutator subgroup ensures $\overline{\varphi}$ is well defined and he axioms for a functor are satisfied.

(iv) Let R be a ring and let D be a left R-module. For each left R-module N, the set $\hom_R(D, N)$ is an abelian group, and is an R-module if R is commutative
If $\varphi : N_1 \to N_2$ is an R-module homomorphism, then $\forall f \in \hom_R(D, N_1)$ we have $\varphi \circ f \in \hom_R(D, N_2)$
Thus $\varphi' : \hom_R(D, N_1) \to \hom_R D, N_2$ by $\varphi'(f) = \varphi \circ f$. The map

$$\begin{aligned} \hom(D, \_) &: N \to \hom_R(D, N) \\ \hom(D, \_) &: \varphi \to \varphi' \end{aligned}$$

is a *covariant functor* from R-**Mod** to **Grp**. If R is commutative, it maps R-**Mod** to itself.

(v) If $\varphi : N_1 \to N_2$ is an R-module homomorphism, then $\forall g \in \hom_R(N_2, D)$, we have $g \circ \varphi \in \hom_R(N_1, D)$. Thus $\varphi' : \hom_R(N_2, D) \to \hom_R(N_1, D)$ by $\varphi'(g) = g \circ \varphi$. The map

$$\begin{aligned} \hom(\_, D) &: N \to \hom_R(N, D) \\ \hom(\_, D) &: \varphi \to \varphi' \end{aligned}$$

is a *contravariant functor* from R-**Mod** to **Grp**. If R is commutative, it maps R-**Mod** to itself.

(vi) If D is a right R-module map, the map $D \otimes_R \_ : N \to D \otimes_R N$ is a covariant functor from R-**Mod** to **Ab** (or to R-**Mod** when R is commutative). The morphism $\varphi : N_1 \to N_2$ maps to morphism $1 \otimes_\varphi$.

Definition 5.1.1.7.