Graduate Algebra

Arthur Li

September 25, 2022

Introduction

This collection of notes serve as a guide to mastering abstract algebra with content from undergraduate to graduate level course. The notes combine knowledge from different sources, including course notes and textbooks used in the courses.

The proofs for Theorems, Propositions and Lemmas will be added after completion of the skeleton.

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.

Contents

1 Preliminaries 3

1.1 Introductory Ideas and Definitions . . . 3

2 Group Theory 5

2.1 Basic Axioms . . . 5

2.2 Homomorphisms and Subgroups . . . 5

2.3 Cyclic Groups . . . 5

2.4 Cosets . . . 5

2.5 Normality, Quotient Groups . . . 5

2.6 Isomorphism Theorems . . . 5

2.7 Symmetric, Alternating and Dihedral Groups . . . 5

2.8 Categories, Products, Coproducts, Free Objects . . . 5

2.9 Direct Products, Direct Sums . . . 5

2.10 Free Groups, Free Products . . . 5

2.11 Matrix Groups . . . 5

3 Group Structures 6

3.1 Free Abelian Groups . . . 6

3.2 Finitely Generated Abelian Groups . . . 6

3.3 Krull-Schmidt Theorem . . . 6

3.4 Group Action . . . 6

3.5 The Sylow Theorems . . . 6

3.6 Semidirect Products . . . 6

3.7 Normal and Subnormal Series . . . 6

4 Ring Theory 7

4.1 Basic Axioms . . . 7

4.2 Examples of Rings . . . 10

4.3 Ring Homomorphisms . . . 11

4.4 Ring Isomorphisms . . . 16

4.5 Ideals, Rings of Fractions, Local Rings . . . 17

4.6 Euclidean Domains, PID, UFD . . . 20

4.7 Polynomial rings . . . 23

5 Modules 27

5.1 Basic Axioms . . . 27

5.2 Module Homomorphisms . . . 30

6 Category Theory 31

6.1 Basic Axioms . . . 31

1 Preliminaries

1.1 Introductory Ideas and Definitions

Definition 1.1.1. *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 1.1.2. *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 1.1.3. 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 1.1.4. *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 1.1.5. 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 1.1.6. *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 1.1.7. 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 1.1.8. 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 1.1.9. 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 $domf$, 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 1.1.10. 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 1.1.11. 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 1.1.12. 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 1.1.13. 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 1.1.14. 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 1.1.15. 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

2.1 Basic Axioms

2.2 Homomorphisms and Subgroups

2.3 Cyclic Groups

2.4 Cosets

2.5 Normality, Quotient Groups

2.6 Isomorphism Theorems

2.7 Symmetric, Alternating and Dihedral Groups

2.8 Categories, Products, Coproducts, Free Objects

2.9 Direct Products, Direct Sums

2.10 Free Groups, Free Products

2.11 Matrix Groups

3 Group Structures

3.1 Free Abelian Groups

3.2 Finitely Generated Abelian Groups

3.3 Krull-Schmidt Theorem

3.4 Group Action

3.5 The Sylow Theorems

3.6 Semidirect Products

3.7 Normal and Subnormal Series

4 Ring Theory

4.1 Basic Axioms

Definition 4.1.1. 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 4.1.2. 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 4.1.3. 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 4.1.4. 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 4.1.5. 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 4.1.6. 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 4.1.7. 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 4.1.8. 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 4.1.9. 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 4.1.10. 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

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

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

Remark 4.1.11. 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 4.1.12. 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 4.1.13. An *Integral Domain* is a commutative ring with $1 \neq 0$ such that $\forall a, b, \in R,\ ab = 0 \Rightarrow a = 0 \ or \ b = 0$, 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 4.1.14. 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 4.1.15. *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 4.1.16. *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 4.1.17. *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 4.1.18. 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 4.1.19. *(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 4.1.20. 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 4.1.21. *(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 4.1.22. *(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 4.1.23. *(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 4.1.24. *(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 4.1.25. *(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 4.1.26. *(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

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

4.2 Examples of Rings

Definition 4.2.1. 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 4.2.2. 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 4.2.3. *(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 4.2.4. 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 4.2.5. 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 4.2.6. 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 4.2.7. 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 4.2.8. *(Group Rings $R[G]$)*
Let R be a commutative ring with $1 \neq 0$. Let $G = \{g_1, \dots, g_n\}$ 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 4.2.9. 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 4.2.10. 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 4.2.11. 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 $\{g_1, \dots, g_n\} = G$. 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.

4.3 Ring Homomorphisms

Definition 4.3.1. 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 4.3.2. 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 4.3.3. The *kernel* of a ring homomorphism φ is defined as $ker\ \varphi = \varphi^{-1}(0_S) = \{a \in R | \varphi(a) = 0_S\}$.

Remark 4.3.4. *(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 4.3.5. *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) $ker \; \varphi$ is a subring of R such that $\forall a \in R$, $\forall k \in ker \; \varphi \Rightarrow ak \in ker \; \varphi$. In other words, $ker \; \varphi$ is a subring of R, $R(ker \; \varphi) \subseteq ker \; \varphi$ and $(ker \; \varphi)R \subseteq ker \; \varphi$.

Definition 4.3.6. 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 4.3.7. 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 4.3.8. 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 4.3.9. *(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 4.3.10. *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 4.3.11. *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 4.3.12. *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 4.3.13. 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 $X = \{r_1, \dots, r_n\}$, then write $(X) = (r_1, \dots, r_n)$.

Definition 4.3.14. For $r \in R$, the ideal (r) generated by a single element r is the *principal ideal of ring R*.

Definition 4.3.15. Let R be a ring. An ideal I is *finitely generated* if $I = (r_1, \dots, r_n)$ for some $r_i \in R$.

Proposition 4.3.16. *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: $(X_1 \cup \dots \cup X_n) = (X_1) + \dots + (X_n)$.

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

Proposition 4.3.17. *Let R be a ring. Let $B \subseteq R$ and $a, a_1, \dots, a_n \in R$.*

(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,

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

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 4.3.18. *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 4.3.19. *Suppose R is a ring with 1. Let $X \subseteq R$ be a subset, and $b_1, \dots, b_n \in R$. 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 4.3.20. *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 4.3.21. *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 4.3.22. *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 4.3.23. *Let $\varphi : R \to S$ be a ring homomorphism.*
Then ker φ is an ideal of R.

Definition 4.3.24. 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 4.3.25. *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 4.3.26. 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 4.3.27. 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 4.3.28. Let R be a ring, $I \subseteq R$ an ideal, and R/I the quotient ring.
The *surjective quotient map*

$$\begin{aligned} \gamma : R &\to R/I \\ r &\mapsto \overline{r} = r + I \end{aligned}$$

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 4.3.29. *(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 4.3.30. 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 4.3.31. 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 4.3.32. 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 4.3.33. 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 4.3.34. 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 4.3.35. 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 4.3.36. 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) $(x) \cap (x - 1)$.

4.4 Ring Isomorphisms

Definition 4.4.1. *(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:

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

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 4.4.2. 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 4.4.3. 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 4.4.4. 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 4.4.5. 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 4.4.6. *(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 4.4.7. *(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

$$\varphi : R_1/(R_1 \cap J) \xrightarrow{\sim} (R_1 + J)/J$$
$$\overline{r} = r + (R_1 \cap J) \mapsto \varphi(\bar{(}r)) := \overline{r} = r + J$$

Definition 4.4.8. *(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 4.4.9. *(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.

4.5 Ideals, Rings of Fractions, Local Rings

Proposition 4.5.1. *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 4.5.2. *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 4.5.3. *If R is a field with $1 \neq 0$, then every nonzero ring homomorphism $f : R \to S$ is an injection.*

Definition 4.5.4. 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 4.5.5. *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 4.5.6. *Apply $J = 0$ to above. If R is a commutative ring with $1 \neq 0$, then R has a maximal ideal.*

Proposition 4.5.7. *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 4.5.8. 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 4.5.9. *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 4.5.10. *Assume the ring R is commutative with 1. Then every maximal ideal is a prime ideal.*

Proposition 4.5.11. *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 4.5.12. 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 4.5.13. 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 4.5.14. 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 4.5.15. 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 4.5.16. *(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 4.5.17. *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 4.5.18. The ring $Q = D^{-1}R$ is the *ring of fractions of D with respect to R.*

Definition 4.5.19. 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 4.5.20. *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 4.5.21. *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 4.5.22. A commutative ring R with $1 \neq 0$ is a *local ring* if it has a unique maximal ideal (say M).

Definition 4.5.23. 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 4.5.24. 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 4.5.25. 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 4.5.26. 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 4.5.27. *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 4.5.28. Let R be a commutative ring with $1 \neq 0$.
Two ideals I, J of R is *comaximal* if $I + J = R$.

Theorem 4.5.29. *(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 4.5.30. *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

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

4.6 Euclidean Domains, PID, UFD

Definition 4.6.1. 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 4.6.2. 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 4.6.3. Every field F is a Euclidean domain with respect to any function $N : F \to \mathbb{Z}_{\geq 0}$

Example 4.6.4. The integer ring $\mathbb{Z}$ is a Euclidean domain with the modules as the norm function:

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

Example 4.6.5. 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 4.6.6. 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 4.6.7. 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 4.6.8. An integral domain R is a *Principal Ideal Domain (PID)* if every ideal $I \subsetneq R$ is a principal: $I = (a)$ for some $a \in I$.

Proposition 4.6.9. *A Euclidean domain R is a PID.*

Example 4.6.10. 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 4.6.11. 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 4.6.12. 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 4.6.13. *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 4.6.14. *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 4.6.15. *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 4.6.16. *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) $d = a_1 x_1 + \cdots + a_n x_n$ for some $x_i \in R$

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

Proposition 4.6.17. *Assume that R is a PID.*
Then every nonzero prime ideal P of R is a maximal ideal of R.

Corollary 4.6.18. *Let R be a commutative ring with 1 such that the polynomial ring $R[x]$ is a PID.*
Then R is a field.

Definition 4.6.19. 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 4.6.20. 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 4.6.21. 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 4.6.22. 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 4.6.23. *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 4.6.24. *Assume R is an integral domain. Then a prime element is always irreducible.*

Proposition 4.6.25. *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 4.6.26. 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 4.6.27. *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 4.6.28. *Assume that R is a UFD. Then $p \in R$ is irreducible if and only if it is prime.*

Proposition 4.6.29. *Assume that R is a UFD and a, b are nonzero elements. Then*

(i) $\gcd(a, b)$ *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 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 4.6.30. 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 4.6.31. *Euclidean Domain $\Rightarrow$ PID $\Rightarrow$ UFD*

Corollary 4.6.32. *(Fundamental Theorem of Arithmetic) The integer ring $\mathbb{Z}$ is UFD.*

Definition 4.6.33. 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 4.6.34. *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

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

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

4.7 Polynomial rings

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

Definition 4.7.1. 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 4.7.2. 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 4.7.3. *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 4.7.4. *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 4.7.5. 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 4.7.6. 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 4.7.7. 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 4.7.8. *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 4.7.9. *The polynomial ring $F[x]$ over a field F is a PID and also UFD.*

Lemma 4.7.10. *(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 4.7.11. 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 4.7.12. 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 4.7.13. *(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 4.7.14. *(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 4.7.15. *(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 4.7.16. *(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 4.7.17. *The ring R is a UFD if and only if the polynomial ring $R[x]$ is a UFD.*

Corollary 4.7.18. *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 4.7.19. *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 4.7.20. *(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 4.7.21. *Assume $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$ 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 4.7.22. *(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 4.7.23. *(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 4.7.24. *(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 4.7.25. *(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

$$p | a_i (0 \leq i \leq n-1),\ p^2 \not| a_0$$

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

Proposition 4.7.26. *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 4.7.27. *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 4.7.28. 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

$$(x-a)^m | f(x),\ but\ (x-a)^{m+1} \not| f(x)$$

Proposition 4.7.29. *Let $F[x]$ be the polynomial ring over a field F and $f(x)$ a nonconstant polynomial such that $\alpha_i \in F$ $(1 \leq i \leq k)$ are all the distinct roots of $f(x)$ of multiplicity $m_i \geq 1$. 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, $\sum_{i=1}^k m_i \leq \deg f(x)$, and $f(x)$ has at most $\deg f(x)$ of roots in F, even counted with multiplicity.

Remark 4.7.30. 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 $n \geq 1$ 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 4.7.31. Let $p \in \mathbb{Z}$ be a prime number. Let $f(x) = x^p - a$ with $a \neq 0$.
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 $f(x)$:

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

Indeed, for any $n \geq 1$, the $\exp(2k\pi i/p)$ $(0 \leq k < n)$ 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 4.7.32. Let $p \in \mathbb{Z}$ be a prime number. Let $f(x) = x^p - a$ with $a \neq 0$.
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 4.7.33. *Let F be a field, and $G \subseteq (F \backslash \{0\}, \times)$ a finite multiplicative subgroup. Then G is cyclic.*

Proposition 4.7.34. *If F is a finite field, then $F\backslash\{0\}$ is a cyclic multiplicative group.*

Corollary 4.7.35. *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 4.7.36. Let F be a field, $a, b \in F$ with $a \neq 0$. 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 4.7.37. 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 4.7.38. Let $p \in \mathbb{Z}$ be a prime number. Then the *cyclotomic polynomial* below is irreducible over $\mathbb{Q}$:

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

5 Modules

5.1 Basic Axioms

Definition 5.1.1. 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 5.1.2. *(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 5.1.3. 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 5.1.4. *(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 5.1.5. 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 5.1.6. 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 5.1.7. When R is a field (or division ring), a left R-submodule is just an R-subspace.

Example 5.1.8. 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 5.1.9. *(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

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

Define the R-action as

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

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

Example 5.1.10. 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 5.1.11. *($F[x]$-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 5.1.12. *(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 5.1.13. 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 5.1.14. *If R is an integral domain, then* Tor*(M) is a R-submodule of M called the torsion submodule of M.*

Definition 5.1.15. 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 5.1.16. The centre $Z(R)$ is a commutative subring of R.

Remark 5.1.17. A ring R is commutative if and only if $Z(R) = R$.

Definition 5.1.18. 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:

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

Definition 5.1.19. 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 5.1.20. 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.

5.2 Module Homomorphisms

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

Definition 5.2.1. 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 5.2.2. 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 5.2.3. 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 5.2.4. 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 $_M$

6 Category Theory

6.1 Basic Axioms