MATH2070: Algebraic Structures

nablamath

October 31, 2021

Remarks

(1) Context of this document is based on university course *MATH2070: Algebraic Structures* from *Department of Mathematics, The Chinese University of Hong Kong (CUHK)*. The original source can be found at `https://www.math.cuhk.edu.hk/course`. The author does not own the source.

(2) This document is assumed unavailable for unauthorized parties that have not attended the university course. It is prohibited to share, including distributing or copying this document to unauthorized parties in any means for any non-academic purpose.

(3) Context of this doucment may not be completely accurate. The author assumes no responsibility or liability for any errors or omissions in the context of this document.

(5) Starting from academic year 2020-2021, a series of Honours courses (with coursecode ending with 8 instead of 0) are introduced. However, Honours courses are assumed to have equivalent contents to their corresponding courses in the past. Hence, current contents will not be modified unless significant difference is found. For more details to Honours courses, please visit `https://www.math.cuhk.edu.hk/undergraduates/honours-courses/overview-honours-courses`.

Prerequisites

This course requires prerequisites of *MATH1030: Linear Algebra I* and *MATH1050: Foundation of Modern Mathematics*.

Source

The latest version of this document can be found at `https://www.github.com/nablamath/notes`.

Contents

1 Group Theory

1.1 Groups

1.1.1 Definition of Groups

To start off with group theory, below is the definition of groups:

Definition 1.1. A **group** $(G, *)$ is a set G equipped with a binary operation

$$* : G \times G \to G$$

which can be called as the **group operation/product/multiplication** such that the following conditions are satisfied:

(a) The group operation is associative, which is

$$(a * b) * c = a * (b * c) \quad \text{for all } a, b, c \in G$$

(b) There exists an **identity element** $e \in G$ such that

$$a * e = e * a = a \quad \text{for all } a \in G$$

(c) For every $a \in G$, there exists an element $a^{-1} \in G$, which is the **inverse** of a, such that

$$a * a^{-1} = a^{-1} * a = e$$

Note that it is also allowed to express the group operation in ab or $a \cdot b$.

Definition 1.2. The group $(G, *)$ is **abelian** if the group operation $*$ is commutative, which is

$$a * b = b * a \quad \text{for all } a, b \in G$$

Otherwise, the group is **nonabelian**.

Note that if the group $(G, *)$ is abelian, the sign of the group operation $*$ is often replaced by $+$.

Definition 1.3. The **order** of the group $(G, *)$, denoted by $|G|$, is the cardinality of the set G. The set G is said to be **finite** if the order of the group $|G|$ is finite, or otherwise it is said to be **infinite**.

Below are some examples on identifying groups:

Example 1.4. Let $n \in \mathbb{Z}^+$, then

$$\begin{aligned} U_n &:= \{z \in \mathbb{C} \mid z^n = 1\} \\ &= \left\{ e^{\frac{2\pi i k}{n}} \mid 0 \leq k \leq n-1 \right\} \end{aligned}$$

is an abelian group under multiplication of complex numbers.

Proof. The well-definedness of the group operation has to be checked, thus first let $a, b \in U_n$, then

$$a^n = b^n = 1 \Rightarrow (ab)^n = a^n \cdot b^n = 1 \cdot 1 = 1 \Rightarrow a \cdot b \in U_n$$

After that, the three conditions of a group are checked one by one:

(a) Associtativity follows from that of multiplication of complex numbers.

(b) An identity element is given by $1 = e^{\frac{2\pi i \cdot 0}{n}} \in U_n$.

(c) Given $a \in U_n$, $a = e^{\frac{2\pi i k}{n}}$ for some $0 \leq k \leq n-1$. Then $\frac{1}{a} = e^{\frac{2\pi i (n-k)}{n}}$ is an inverse to a.

Hence $(U_n, \cdot)$ is a group. It follows from the fact that multiplication in $\mathbb{C}$ is commutative, which means $(U_n, \cdot)$ is abelian.

Example 1.5. Let X be a nonempty set. The set of all symmetries (or permutations) of X is defined as

$$S_X := \{\rho : X \to X \mid \rho \text{ is bijective}\}$$

Then S_X forms a group under composition of maps, for example

$$(\rho_1, \rho_2) \in S_X \mapsto \rho_1 \circ \rho_2 \in S_X$$

Proof. Again, the three conditions of a group are checked:

(a) Composition of maps is associative.

(b) The identity map $Id : x \mapsto x$ is an identity element.

(c) $\rho \in S_X$ is bijective, which means ρ^{-1} exists and is also bijective, which is an element of S_X.

Note that the group above is finite nonabelian group.

1.1.2 Linear Groups

Definition 1.6. The **General Linear Group** of $n \times n$ real matrices M, such that $\det(M) \neq 0$, and denoted by $\mathrm{GL}(n, \mathbb{R})$, is a group under matrix multiplication.

Definition 1.7. The **Special Linear Group** of $n \times n$ real matrices M, such that $\det(M) = 1$, and denoted by $\mathrm{SL}(n, \mathbb{R})$, is a group under matrix multiplication.

1.1.3 Basic Properties of Groups

Proposition 1.8. The identity element in a group is unique.

Proof. Suppose $e, e' \in G$ are two identity elements in G, then

$$e' = e' \cdot e = e$$

Therefore $e' = e$.

Proposition 1.9. Let G be a group, then for any $a \in G$, inverse of a is unique.

Proof. Suppose $a', a'' \in G$ are two inverses of a, then

$$\begin{aligned} a'' &= a'' \cdot e \\ &= a'' \cdot (a \cdot a') \\ &= (a'' \cdot a) \cdot a' \\ &= e \cdot a' \\ &= a' \end{aligned}$$

Therefore $a' = a''$.

Proposition 1.10. Let G be a group, then $(ab)^{-1} = b^{-1}a^{-1}$ for any $a, b \in G$.

Proof. Note that $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$, along with the uniqueness of inverse (by *Proposition 1.8*), $(ab)^{-1} = b^{-1}a^{-1}$.

Definition 1.11. Let G be a group with identity element e, for any $g \in G$, $n \in \mathbb{N}$, let

$$g^n = \begin{cases} \underbrace{g \cdots g}_{k \text{ times}} & , \text{if } k \in \mathbb{Z}^+ \\ \mathrm{e} & , \text{if } k = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{k \text{ times}} & , \text{if } k \in \mathbb{Z}_{<0} \end{cases}$$

Definition 1.12. The **Klein-4 group** is defined by $\mathbb{Z}_2 \times \mathbb{Z}_2$ with elements $(0,0),(0,1),(1,0)$ and $(1,1)$.

1.2 Cyclic Groups

1.2.1 Element Order

Definition 1.13. Let G be a group with identity element $e \in G$. The **order** of an element $g \in G$, denoted by $|g|$, is the smallest positive integer n such that $g^n = e$ if such integer exist. Otherwise, g has infinite order, which is $|g| = \infty$.

In other words, the order of an element can be found as follows:

$$|g| = \begin{cases} \min\left\{k \in \mathbb{Z}^+ \mid g^k = e\right\} & \text{, if such set is nonempty} \\ \infty & \text{, otherwise} \end{cases}$$

Proposition 1.14. Let G be a group with identity element $e \in G$, then for any $n \in \mathbb{Z}^+$ such that $g^n = e$ where $g \in G$, $|g| \mid n$.

Proof. Let $m := |g|$ (which is finite by assumption). Suppose $g^n = e$ for some $n \in \mathbb{Z}^+$. By the Division Algorithm in Z, there exists some $q, r \in \mathbb{Z}$ with $0 \leq r \leq m$ such that

$$\begin{aligned} & n = qm + r \\ \Rightarrow\ & e = g^n = g^{qm+r} = (g^m)^q g^r = g^r \end{aligned}$$

which means that $r = 0$ (otherwise there will be a contradiction based on the definition of $m = |g|$). Therefore $n = qm$, or $m \mid n$.

Theorem 1.15. Let G be a group. Fix an element $g \in G$. If $|g| = \infty$, then $\langle g \rangle$ is an infinite countable set. If $|g| = m < \infty$, then

$$\langle g \rangle = \left\{e, g, g^2, \cdots, g^{m-1}\right\}$$

Proof. Suppose $|g| = \infty$, then by defintion, the map $\varphi : \mathbb{Z} \to \langle g \rangle$ is surjective. Now if $g^{k_1} = g^{k_2}$ for $k_1, k_2 \in \mathbb{Z}$, and without the loss of generality, assume that $k_1 \geq k_2$. Then $g^{k_1 - k_2} = e$ and $|g| = \infty \Leftrightarrow \left\{k \in \mathbb{Z}^+ \mid g^k = e\right\} = \phi$. Hence φ is injective.

Suppose $|g| = m < \infty$, then it has to show that $\langle g \rangle \subset \{e, g, g^2, \cdots, g^{m-1}\}$. Let $g^k \in \langle g \rangle$ where $k \in \mathbb{Z}$. By *Proposition 1.14*, $g^r \in \{e, g, g^2, \cdots, g^{m-1}\}$.

1.2.2 Definition of Cyclic Groups

Definition 1.16. A group G is said to be **cyclic** if there exists $g \in G$ such that

every element of G is equal to g^n for some integers n. In this case, g is a **generator** of G, denoted by $G = \langle g \rangle$.

Note that a generator of a cyclic group is not unique, in other words, there may exist different elements g_1, g_2 such that $G = \langle g_1 \rangle = \langle g_2 \rangle$.

Theorem 1.17. If a group is cyclic, the group is also abelian.

Proof. Let G be a cyclic group, then $G = \langle g \rangle$ for some element $g \in G$ and every element is in the form g^n for some $n \in \mathbb{Z}$, then

$$g^{n_1} \cdot g^{n_2} = g^{n_1+n_2} = g^{n_2+n_1} = g^{n_2} \cdot g^{n_1}$$

1.3 Symmetric Groups

1.3.1 Definition of Symmetric Groups

Definition 1.18. Let X be a set. A permutation of the set X is the bijective map

$$\sigma : X \to X$$

Theorem 1.19. The set S of permutations of a set X is a group with respect to the composition of maps ($\circ$).

Proof. The following conditions of a group is satisfied:

(a) Let σ, γ be permutations of X. By definition, they are both bijective maps from X to itself. Then $\sigma \circ \gamma$ will also be a bijective map from X to itslef, hence $\sigma \circ \gamma$ is a permutation of X, and $\circ$ is a well-defined binary opeation on S.

(b) Composition of maps is associative.

(c) There exists a map $e(x) = x$ for all $x \in X$, which is an identity element in S.

(d) Let σ be an element in S. Since σ is bijective, there exists the inverse σ^{-1} which is also bijective.

Definition 1.20. If a set S_x of permutations of another set X is a group with respect to the composition of maps, then S_x is said to be the **symmetric group** on X.

An **n-th symmetric group** is the symmetric group on $I_n := \{1, 2, \cdots, n\}$ where n is a positive integer, denoted by S_n. Its element $\sigma \in S_n$, which is a bijective map, can be expressed as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

1.3.2 Cyclic Permutations

Definition 1.21. Let S be an n-th symmetric group, and σ be an element in S. $(i_1 i_2 \cdots i_k)$ is a **k-cycle** which denotes the permutation

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \cdots, i_k \mapsto i_1$$

and $j \mapsto j$ for all

$$j \in \{1, 2, \cdots, n\} \setminus \{i_1, i_2, \cdots, i_k\}$$

which is said to be **fixed** by σ.

Example 1.22. Consider the element σ in eighth symmetric group S_8:

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 6 & 4 & 2 & 1 & 3 & 5 & 7 \end{pmatrix} \\ &= (1\,8\,7\,5)(2\,6\,3\,4) \end{aligned}$$

and such factorization is essentially unique.

Note that a 2-cycle is often called a **transposition** as it switches two elements with each other.

Theorem 1.23. Every permutation in any symmetric group is either a cycle or a product of disjoint cycles.

1.4 Dihedral Groups

1.4.1 Definition of Dihedral Groups

Definition 1.24. A **dihedral group**, denoted by D_n, is a group containing elements of transformations of $\mathbb{R}^2$, which consists of all rotations (denoted by r) by fixed angles about the origin and reflections (denoted by s) over lines through the origin, of regular polygons with n sides.

1.4.2 Dihedral Groups and Transformations of Regular Polygons

Note that dihedral groups are subgroups of the group U of rigid motions on $\mathbb{R}^2$, where

$$U := \left\{\sigma : \mathbb{R}^2 \to \mathbb{R}^2 \mid \sigma(\|\mathbf{v} - \mathbf{w}\|) = \|\sigma(\mathbf{v}) - \sigma(\mathbf{w})\| \ \forall \mathbf{v}, \mathbf{w} \in \mathbb{R}^2\right\}$$

In fact, σ represents the distance in $\mathbb{R}^2$, and note that

$$\sigma(\mathbf{v}) = A\mathbf{v} + \mathbf{b}$$

for some orthogonal $A \in M_{2\times 2}(\mathbb{R})$ and $\mathbf{b} \in \mathbb{R}^2$. With this terminology,

$$T = \left\{\sigma \in U \mid \sigma \text{ fixes } \sigma \in \mathbb{R}^2\right\}$$

contains all rotations and reflections in *Definition 1.24*.

Now consider a regular n-gon $\Delta_n \subset \mathbb{R}^2$ centered at $\mathbf{O} \in \mathbb{R}^2$ with vertices $P_n := \{x_1, x_2, \cdots, x_n\} \subset \mathbb{R}^2$, then the dihedral group can be defined as

$$D_n := \{\sigma \in T \mid \sigma(P_n) = P(n)\}$$

1.4.3 Properties of Dihedral Groups

Theorem 1.25. A dihedral group D_n can be expressed as

$$D_n = \begin{Bmatrix} r_0, r_1, r_2, \cdots, r_{n-1} \\ s_1, s_2, s_3, \cdots, s_n \end{Bmatrix}$$

where r_k is a counterclockwise rotation by $\frac{2k\pi}{n}$ and $s_1, s_2, \cdots, s_n$ are reflections about the n symmetry axes of Δ_n. Then $|D_n| = 2n$.

Note that the rotations can be rewritten as $\{id, r, r^2, \cdots, r^{n-1}\}$ and reflections can be rewritten as $\{s, rs, r^2s, \cdots, r^{n-1}s\}$, since the composition of any two reflections is a rotation.

Proposition 1.26. For any rotation r and reflection s, $s^{-1}rs = r^{-1}$, then all dihedral groups D_n are nonabelian since $rs = sr^{-1}$.

1.5 Subgroups

1.5.1 Definition of Subgroups

Just like subsets as substructure of sets in set theory, there is also substructure of groups. The following are the definition of subgroups:

Definition 1.27. Let $(G, *)$ be a group. A nonempty subset $H \subset G$ is a **subgroup** of G, denoted by $H < G$, if H is also a group by itself under the induced structure of G. By induced structure, more precisely it means that:

(a) H is closed under $*$, which is $a*b \in H\ \forall a, b \in H$ (This shows that the restriction of $*$ to $H \times H$ gives a well-defined binary operation on H).

(b) H is a group using this induced operation.

Definition 1.28. For any group G, the singleton containing only the identity element $\{e\}$ is called the **trivial subgroup** of G.

A subgroup $H < G$ is said to be **nontrivial** if $H \neq \{e\}$. Since a group is a subgroup of itself, which is $G < G$, a subgroup $H < G$ is said to be **proper** if $H \neq G$.

Example 1.29. Below are various examples of subgroups:

(a) Since $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, then $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.

(b) Roots of unity $\mathrm{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ is a subgroup of $\mathrm{U} = \{z \in \mathbb{C} \mid |z| = 1\}$, for all positive integers n.

(c) The special linear group $\mathrm{SL}(n, F) = \{A \in \mathrm{GL}(n, F) \mid \det(A) = 1\}$ is a subgroup of general linear group $\mathrm{GL}(n, F)$.

1.5.2 Subgroups and Symmetric Groups

Proposition 1.30. Let an n-th symmetric group be S_n, then each permutation $\sigma \in S_n$ is a product of transpositions.

Proof. Notice that every cycle is a product of transpositions:

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2)$$

then the result follows from the fact that every permutation of the symmetric group is a product of cycles.

Proposition 1.31. Let an n-th symmetric group be S_n, then in every factorization of $\sigma \in S_n$ as a product of transpositions, then the number of factors is either always even or always odd.

Proof. The use of determinant is required to finish this proof. Observe that there exists an unique matrix $A \in M_{n\times n}(\mathbb{R})$ with only 0 or 1 as entries which sends any vector

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n \text{ to } \begin{bmatrix} x_{\sigma_1} \\ x_{\sigma_2} \\ \vdots \\ x_{\sigma_n} \end{bmatrix} \in \mathbb{R}^n$$

where A is given by permuting rows in the identity matrix I_n. Now if there are two factorizations of σ into products of transpositions, which is

$$\begin{cases} \sigma = \tau_1\tau_2\cdots\tau_k \\ \sigma = \mu_1\mu_2\cdots\mu_l \end{cases}$$

which can be determined that $\det(A) = (-1)^k \det(I_n) = (-1)^k$ in the first equation and $\det(A) = (-1)^l \det(I_n) = (-1)^l$. Hence $(-1)^k = (-1)^l$, and $k - l$ is divisible by 2.

Definition 1.32. Let an n-th symmetric group be S_n, then a permutation $\sigma \in S_n$ is called **even** (**odd**) if it is a product of an even (odd) number of transpositions.

Further let $A_n := \{\sigma \in S_n \mid \sigma \text{ is even}\}$, then $A_n < S_n$. A_n is called the **n-th alternating group**.

1.5.3 Techniques on Subgroups

Proposition 1.33. A nonempty subset H of a group G is a subgroup of G if and only if

$$ab^{-1} \in H \ \forall a, b \in H$$

Proof. Part (⇒) Suppose $H < G$, then given $a, b \in H$, we have $b^{-1} \in H$ because of the existence of inverse in groups. Along with the closedness of H under the group product, $ab^{-1} \in H$.

Part (⇐) Suppose $ab^{-1} \in H \ \forall a, b \in H$. Because H is nonempty, there exists some element within H, and for any element $a \in H$, $e = a \cdot a^{-1} \in H$. For any $b \in H$, $b^{-1} = e \cdot b^{-1} \in H$. Now, for $a, b \in H$, since $b^{-1} \in H$, then $a \cdot b = a(b^{-1})^{-1} \in H$, H is closed under the group opeation. Finally, with the associativity of the induced operation follows from that in G, it can be concluded that H is a group under the induced operation.

With the proposition above, it is much easier to determine whether a subset of a group is a subgroup or not.

Example 1.34. Prove example (b) and (c) in *Example 1.29*.

Answer. Part (b) Note that for any $z_1, z_2 \in U_n$,

$$\begin{aligned} & z_1^n = z_2^n = 1 \\ \Rightarrow & (z_1 z_2^{-1})^n = 1 \\ \Rightarrow & = z_1 z_2^{-1} \in U_n \end{aligned}$$

By *Proposition 1.33*, $U_n < U$.

Part (c) Note that for any $A, B \in \mathrm{SL}(n, F)$,

$$\begin{aligned} &\det(A) = \det(B) = 1 \\ \Rightarrow &\det(AB^{-1}) = \det(A)\det(B)^{-1} = 1 \\ \Rightarrow &AB^{-1} \in \mathrm{SL}(n, F) \end{aligned}$$

By *Proposition 1.33*, $\mathrm{SL}(n, F) < \mathrm{GL}(n, F)$.

1.5.4 Cyclic Subgroups

Proposition 1.35. Let G be a group and fix an element $g \in G$ where $\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\}$. $\langle g \rangle$ is the smallest subgroup of G containing g.

Proof. For $\langle g \rangle < G$, take $g^{k_1}, g^{k_2} \in \langle g \rangle$, then $g^{k_1} \cdot (g^{k_2})^{-1} = g^{k_1 - k_2} \in \langle g \rangle$, which means that $\langle g \rangle < G$. Now let $H < G$ be a subgroup of G containing g, then $g^k \in H \ \forall k \in \mathbb{Z}$. Therefore, $\langle g \rangle \subset H$.

With the proposition above, the following definition of cyclic subgroups can be introduced:

Definition 1.36. Let G be a group and fix an element $g \in G$. $\langle g \rangle$ is the **cyclic subgroup** generated by g.

Proposition 1.37. The intersection of any collection of subgroups of a group G is a subgroup of G, that is if $\{H_i \mid i \in I\}$ is a collection of subgroups of G, then

$$\bigcap_{i \in I} H_i < G$$

With the proposition above, it can be rewritten into

$$\langle g \rangle = \bigcap_{\{H \mid g \in H < G\}} H$$

Proposition 1.38. Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle g \rangle$ be a cyclic group, and $H < G$ be a subgroup. If H is trivial, then it is cyclic since it is generated by the identity element e. If H is nontrivial, then there exists $k \in \mathbb{Z}^+$ such that $g^k \in H$. Let

$$m := \min\left\{k \in \mathbb{Z}^+ \mid g^k \in H\right\}$$

Now claim that H is generated by g^m. First of all, it is obvious that $\langle g^m \rangle \subset H$. Conversely, let g^n be an arbitrary element in H. By the Division Algorithm, there exists unique integers q and $0 \leq r \leq m-1$ such that $n = mq + r$. Then $g^n = (g^m)^q g^r$ which leads to $g^r = (g^m)^{-q} g^n \in H$. If $r \neq 0$, then it contradicts to the Division

Algorithm, so it forces $r = 0$. With $r = 0$, $g^n \in \langle g^m \rangle$ and $H \subset \langle g^m \rangle$.

Corollary. Any subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

1.5.5 Greatest Common Divisor

With the corollary of *Proposition 1.38*, the greatest common divisor can be defined:

Definition 1.39. For any $a, b \in \mathbb{Z}$, the subset

$$\langle a, b \rangle := \{ma + nb \mid m.n \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$, and is of the form $d\mathbb{Z}$ for some $d \in \mathbb{Z}$. The **greatest common divisor** of a and b, defined by $\gcd(a, b)$, is the positive integer d mentioned above. Furthermore, d has to satisfies the following:

(a) **Definition**

$$d = ma + nb \; \exists m, n \in \mathbb{Z}$$

(b) **Divisibility**

$$d \mid a \text{ and } d \mid b$$

(c) **Common divisor**

$$\text{If } k \mid a \text{ and } k \mid b \text{ , then } k \mid d$$

Proposition 1.40. Let G be a cyclic group of order n and $g \in G$ be a generator of G, which is $G = \langle g \rangle$. Let $g^s \in G$ be an element in G, then the order of g^s

$$|g^s| = \frac{n}{\gcd(s, n)}$$

Moreover, $\langle g^s \rangle = \langle g^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof. Let $m = |g^s|$. Since $|G| = n$, $(g^s)^{\frac{n}{d}} = (g^n)^{\frac{s}{d}} = e$. By *Proposition 1.14*, $m \mid \frac{n}{d}$. On the other hand, $e = (g^s)^m$ and by the same proposition as above, $n \mid sm$. By dividing both sides by d, $\frac{n}{d} \mid \frac{sm}{d}$. However, $\frac{n}{d}$ and $\frac{s}{d}$ are relatively primes, so $\frac{n}{d} \mid m$ which proves that $|g^s| = \frac{n}{\gcd(s,n)}$.

To prove the second assertion, it has to be first shown that there is an equality of subgroups $\langle g^s \rangle = \langle g^d \rangle$ where $d = \gcd(s, n)$. Note that one inclusion is clear: as $d \mid s$, $g^s \in \langle g^d \rangle$ which implies $\langle g^s \rangle \subset \langle g^d \rangle$. Conversely, note that there exists $p, q \in \mathbb{Z}$ such that $d = ps + qn$, so $g^d = (g^s)^p (g^n)^q = (g^s)^p = \langle g^s \rangle$. Hence $\langle g^d \rangle \subset \langle g^s \rangle$ and the proof of equality is complete.

$\langle g^s \rangle = \langle g^t \rangle$ implies that $|g^s| = |g^t|$ which in turn gives $\gcd(s, n) = \gcd t, n$. Conversely, if $d := \gcd(s, n) = \gcd(t, n)$, then $\langle g^d \rangle = \langle g^s \rangle = \langle g^t \rangle$.

Corollary. All generators of a cyclic group $G = \langle g \rangle$ of order n are of the form g^r where r and n are relatively primes.

1.6 Generating Sets

1.6.1 Definition of Generating Sets

Definition 1.41. Let G be a group and S be a nonempty subset of G. Define

$$\langle S \rangle := \{a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n} \mid n \in \mathbb{N}, a_i \in S \ \forall i, m_i \in \mathbb{Z} \ \forall i\}$$

be the **smallest subgroup** of G containing the subset S, which is called the subgroup generated by S.

Proof. Let $a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n}, b_1^{l_1} b_2^{l_2} \cdots b_k^{l_k} \in \langle S \rangle$. Then $AB^{-1} = a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n} b_1^{-l_1} b_2^{-l_2} \cdots b_k^{-l_k} \in \langle S \rangle$. Then $\langle S \rangle < G$.

Furthermore, if $H < G$ is a subgroup containing S, then $a^k \in H \ \forall a \in S, \forall k \in \mathbb{Z}$ and thus $a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n} \in H \ \forall a_1, a_2, \cdots, a_n \in S, \forall k_1, k_2, \cdots, k_n \in \mathbb{Z}$. Therefore, $\langle S \rangle \subset H$.

Note that the subgroup generated by an empty set $\langle \phi \rangle = \{e\}$. Also note that

$$\langle S \rangle = \bigcap_{S \subset H < G} H$$

If $S = \{a_1, a_2, \cdots, a_n\}$, it is often written as $\langle a_1, a_2, \cdots, a_n \rangle$ instead of $\langle \{a_1, a_2, \cdots, a_n\} \rangle$.

Definition 1.42. A group G is said to be **finitely generated** if there exists a finite subset $S = \{a_1, a_2, \cdots, a_n\}$ such that $G = \langle a_1, a_2, \cdots, a_n \rangle$.

1.6.2 Equivalence Relations and Partitions

Recall the definition of partitions:

Definition 1.43. Let S be a set. A **partition** of S, denoted by P, is a collection of subsets $\{S_i \mid i \in I\}$ such that $S_i \neq \phi \ \forall i \in I, S_i \cap S_j = \phi$ if $i \neq j, S = \bigcap_{i \in I} S_i$. In this case, it is also said that S is a disjoin union of $\{S_i \mid i \in I\}$ written as $S = \bigsqcup_{i \in I} S_i$.

Definition 1.44. Let S be a set. An **equivalence relation** on S, is a relaion $\sim$ on S (which is a subset of $S \times S$) such that the following are true:

(a) **Reflexive**

$$a \sim a \; \forall a \in S$$

(b) **Symmetric**

$$\text{If } a \sim b \text{ then } b \sim a$$

(c) **Transitive**

$$\text{If } a \sim b \text{ and } b \sim c \text{ then } a \sim c$$

Definition 1.45. For any $a \in S$, the subset

$$C_a := \{b \in S \mid b \sim a\} \subset S$$

is called the **equivalence class** of a.

Proposition 1.46. The collection of equivalence classes $\{C_a \mid a \in S\}$ is a partition of S. More precisely, any two equivalence classes are either exactly the same subset or disjoint, which is

$$C_a \cap C_b \neq \phi \Rightarrow C_a = C_b$$

Then

$$S = \bigcup_{a \in S} C_a = \bigsqcup_{a \in I} C_a$$

for some index set I.

Proof. Suppose $c \in C_a \cap C_b \neq \phi$, then

$$c \in C_a \Rightarrow c \sim a \Rightarrow a \sim c$$

On the other hand,

$$c \in C_b \Rightarrow c \sim b \Rightarrow a \sim b$$

In order to show that $C_a \subset C_b$, let $d \in C_a$ where $d \sim a$ is always true. However $a \sim b$, and by transitivity, $d \sim b$ and so $d \in C_b$. By the symmetric property, $a \sim b \Rightarrow b \sim a$. Also note that C_a and C_b are interchangable, then $C_b \subset C_a$. Hence $C_a = C_b$.

1.6.3 Application of Equivalence Relations

Recall *Theorem 1.26*, below is the proof of the theorem:

Proof. Let $\sigma \in S_n$ be a permutation of $I_n = \{1, 2, \cdots, n\}$. Define a relation $\sim$ on I_n by $a \sim b$ if and only if $b = \sigma^k(a)$ for some $k \in \mathbb{Z}$, which is an equivalence relation.

Hence it induces a partition of I_n:

$$I_n = O_1 \sqcup O_2 \sqcup \cdots \sqcup O_m$$

where O_i is called an **orbit** of σ in I_n. Then for $j = 1, 2, \cdots, m$, define a cycle of length $|O_j|$ by

$$\mu_j(a) = \begin{cases} \sigma(a) & , \text{if } a \in O_j \\ a & , \text{if } a \notin O_j \end{cases}$$

Note that $\mu_1, \mu_2, \cdots, \mu_m$ are disjoint cycles because $\{O_1, O_2, \cdots, O_m\}$ is a partition of I_n.

Finally, check that $\sigma = \mu_1\mu_2 \cdots \mu_m$. By computing

$$\begin{aligned} (\mu_1\mu_2 \cdots \mu_m)(a) &= \mu_j(a) \quad \text{where } a \in O_j \\ &= \sigma(a) \end{aligned}$$

1.7 Cosets

1.7.1 Definition of Cosets

Proposition 1.47. Let G be a group and $H < G$ be a subgroup, then a relation $\sim_L$ on G can be defined as $a \sim_L b$ if and only if $b = a \cdot h$ for some $h \in H$, or in other words, $a^{-1}b \in H$, then $\sim_L$ is an equivalence relation.

Proof. In order to prove $\sim_L$ is an equivalence relation, check the following:

(a) **Reflexive**

$$\begin{aligned} &a^{-1}a = e \in H \ \forall a \in G \\ \Rightarrow &a \sim_L a \ \forall a \in G \end{aligned}$$

(b) **Symmetric**

$$\begin{aligned} a \sim_L b &\Leftrightarrow a^{-1}b \in H \\ &\Rightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \\ &\Rightarrow b \sim_L a \end{aligned}$$

(c) **Transitive**

$$\begin{aligned} \begin{cases} a \sim_L b \\ b \sim_L c \end{cases} &\Leftrightarrow \begin{cases} a^{-1}b \in H \\ b^{-1}c \in H \end{cases} \\ &\Rightarrow a^{-1}c = (a^{-1}b)(b^{-1}c) \in H \\ &\Rightarrow a \sim_L c \end{aligned}$$

Note that for any subset $H \subset G$, the relation $\sim$ on G defined by $a \sim b$ if and only if $a^{-1}b \in H$ is an equivalence relation, if and only if $H < G$.

Definition 1.48. Let G be a group and $H < G$ be a subgroup. Define $\sim_L$ be the relation mentioned above, then $\sim_L$ induces a partition of G into equivalence classes, where those classes are **left cosets** of H in G. Each left coset of H in G is of the form

$$\begin{aligned} aH &= \{b \in G \mid a \sim_L b\} \\ &= \{b \in G \mid b = ah \text{ for some } h \in H\} \end{aligned}$$

Similarly, define $\sim_R$ be another relation where $a \sim_R b \Leftrightarrow b = ha$ for some $h \in H$, then $\sim_R$ also induces a partition of G into equivalence classes, where those classes are **right cosets** of H in G. Each right coset of H in G is of the form

$$\begin{aligned} Ha &= \{b \in G \mid a \sim_R b\} \\ &= \{b \in G \mid b = ha \text{ for some } h \in H\} \end{aligned}$$

Note that left cosets and right cosets are equivalent if the group is abelian.

1.7.2 Theorem of Lagrange

With the definition of left cosets and right cosets, it can be related with the following:

Definition 1.49. The **index** of H in G is the number of left cosets (or right cosets) of H in G, denoted by $[G : H]$.

The definition above implies that the number, or cardinality to be exact, of left cosets and right cosets of H in G are equal. This leads to the **Theorem of Lagrange**:

Theorem 1.50. Let H be a subgroup of a group G, then for all $a \in G$,

$$|aH| = |H| = |Ha|$$

In particular, if $|G| < +\infty$, then $|H| \mid |G|$ or more precisely,

$$|G| = |H| \cdot [G : H]$$

Proof. For the first statement, consider the maps $\varphi_a : H \to aH$ and $\psi_a : H \to Ha$. In other words, for any $h \in H$, $\varphi_a : h \mapsto ah$ and $\psi_a : h \mapsto ha$. Claim φ_a (and ψ_a) is a bijection for all $a \in G$:

(a) **Injectivity**
For all $h_1, h_2 \in H$, $\varphi_a(h_1) = \varphi_a(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$. Hence φ_a is injective.

(b) **Surjectivity**
Let $g \in aH$, then by definition, there exists $h \in H$ such that $g = ah = \varphi_a(h)$. Hence φ_a is surjective.

For the second statement, note that the partition of G

$$G = \bigsqcup_{i \in I} a_i H$$

where $\{a_1 H, a_2 H, \cdots, a_k H\}$ enumerates the set of all left cosets of H in G. This implies that

$$\begin{aligned} |G| &= \sum_{i=1}^{k} |a_i H| \\ &= \sum_{i=1}^{k} |H| \\ &= k\,|H| = [G : H] \cdot |H| \end{aligned}$$

Below are some corollaries based on the Theorem of Lagrange:

Corollary. Let G be a finite group, then $|g| \mid |G|$ for all $g \in G$. In particular,

$$g^{|G|} = e \; \forall g \in G$$

Proof. By applying the Theorem of Lagrange to the cyclic subgroup $\langle g \rangle$ generated by $g \in G$, $|g| = |\langle g \rangle| \mid |G|$.

Corollary. If G is a finite group of prime order, then it is cyclic.

Proof. Suppose $|G| = p$ is a prime. Further let $g \in G \setminus \{e\}$, then $|g| \mid |G| = p$ by the corollary above, and $|g| = p$. Therefore $G = \langle g \rangle$.

Example 1.51. If $\{e\} < G$, then the set of left cosets and the set of right cosets are the same, which is $\{\{g\} \mid g \in G\}$. This means that $G = \bigsqcup_{g \in G} \{g\}$.

On the other hand, if $G < G$, then again the set of left cosets and the set of right cosets are the same, which is $\{G\}$. This leads to a trivial result $G = G$.

Example 1.52. Let D_n be a dihedral group, which is

$$D_n = \begin{Bmatrix} id, r_1, r_2, \cdots, r_{n-1} \\ s, r_1 s, r_2 s, \cdots, r_{n-1} s \end{Bmatrix}$$

For $\langle r \rangle < D_n$,

$$\begin{aligned} \text{left cosets} &= \{\langle r \rangle, s\langle r \rangle\} \Rightarrow D_n = \langle r \rangle \sqcup s\langle r \rangle \\ \text{right cosets} &= \{\langle r \rangle, \langle r \rangle s\} \Rightarrow D_n = \langle r \rangle \sqcup \langle r \rangle s \end{aligned}$$

In particular, $s\langle r \rangle = \langle r \rangle s$.

1.8 Group Homomorphisms

1.8.1 Definition of Group Homomorphisms

Definition 1.53. Let $G = (G, *)$ and $G' = (G, *')$ be groups. A **group homomorphism**, denoted by ϕ, is a map $G \to G'$ such that

$$\phi(a * b) = \phi(a) *' \phi(b)$$

for all $a, b \in G$. If ϕ is an addition bijective, then ϕ is called a **group isomorphism**, and G is **isomorphic** to G' as groups. In other words, G and G' have the same structure.

Definition 1.54. Let G be a group. An **automorphism** of G is an isomorphism from G onto itself

$$\phi : G \to G$$

Note that

$$\mathrm{Aut}(G) := \{\phi : G \to G \mid \phi \text{ is an isomorphism}\}$$

is a group itself under composition of maps.

Example 1.55. Below are various examples of group homomorphisms:

(a) The exponential function

$$\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$$

is a group homomorphism, which is $\exp(a+b) = \exp(a)\exp(b)$.

(b) The determinant

$$\det : \mathrm{GL}(n, \mathbb{R}) \to (\mathbb{R}^x, \cdot)$$

is a group homomorphism, which is $\det(AB) = \det(A)\det(B)$.

(c) Fix any $n \in \mathbb{Z}^x$, then $n\mathbb{Z} < \mathbb{Z}$ and the map

$$\phi : n\mathbb{Z} \to \mathbb{Z}$$

is a group isomorphism.

Note that if $\phi : G \to G'$ is a group isomorphism, then $\phi^{-1} : G' \to G$ is automatically a group isomorphism. For example, the logarithmic function is the inverse of the exponential function in example (a) of *Example 1.55*, and it is an isomorphism, which is $\log(ab) = \log(a) + \log(b)$.

Also note that in example (c) of *Example 1.55*, if $|n| \neq 1$, then $n\mathbb{Z} \neq \mathbb{Z}$ and $n\mathbb{Z} < \mathbb{Z}$ but $n\mathbb{Z} \cong \mathbb{Z}$. In general, given a group G and two subgroups $H, H' < G$, then $H = H'$ as subsets in G, and $H \cong H'$ as groups, which are usually not equivalent. On the other hand, for any $n \in \mathbb{Z}$, the map $\phi' : \mathbb{Z} \to n\mathbb{Z}$ is a group homomorphism but not an isomorphism unless $|n| = 1$.

Example 1.56. The remainder map

$$\phi : \mathbb{Z} \to \mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$$

is well-defined because of the Division Theorem, and surjective. Let $k_1, k_2 \in \mathbb{Z}$, and check that $\phi(k_1 + k_2) = \phi(k_1) + \phi(k_2)$ for homomorphism. By the Division Theorem, for $i = 1, 2$, there exists unique $q_i, r_i \in \mathbb{Z}$ with $0 \leq r_i \leq n-1$ such that $k_i = q_i n + r_i$.

Now by definition, $\phi(k_i) = r_i$ for $i = 1, 2$. Consider $k_1 + k_2$,

$$k_1 + k_2 = (q_1 + q_2)n + (r_1 + r_2) = (q_1 + q_2 + 1)n + (r_1 + r_2 - n)$$

which leads to

$$\begin{aligned}\phi(k_1 + k_2) &= \begin{cases} r_1 + r_2 & \text{if } 0 \leq r_1 + r_2 \leq n - 1 \\ r_1 + r_2 - n & \text{if } n \leq r_1 + r_2 \end{cases} \\ &= r_1 +_n r_2 = \phi(k_1) +_n \phi(k_2)\end{aligned}$$

1.8.2 Basic Properties of Group Homomorphisms

Proposition 1.57. Let $\phi : G \to G'$ be a group homomorphism, then the following applies:

(a)
$$\phi(e_G) = \phi(e_{G'})$$

(b)
$$\phi(g^{-1}) = \phi(g)^{-1} \ \forall g \in G$$

(c)
$$\phi(g^n) = \phi(g)^n \ \forall g \in G, \forall n \in Z$$

Proof. Part (a)

$$\begin{aligned} e_G \cdot e_G &= e_G \\ \phi(e_G \cdot e_G) &= \phi(e_G) \\ \phi(e_G)^{-1}\phi(e_G)\phi(e_G) &= \phi(e_G)^{-1}\phi(e_G) \\ \phi(e_G) &= e_{G'} \end{aligned}$$

Part (b) For any $g \in G$,

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = e_{G"}$$

by part (a). Similarly, $\phi(g)\phi(g^{-1}) = e_{G'}$, and so $\phi(g^{-1}) = \phi(g)^{-1}$ by uniqueness of inverses in G'.
Part (c) Can be proven by using part (a), part (b) and induction.

1.8.3 Images and Kernels

Proposition 1.58. Let $\phi : G \to G'$ be a group homomorphism, then the following applies:

(a)
$$H < G \Rightarrow \phi(H) < G'$$

(b)
$$H' < G' \Rightarrow \phi^{-1}(H') < G$$

Proof. Part (a) Recall the criterion where $\phi \neq H \subset G$ is a subgroup if and only if $ab^{-1} \in H$ for all $a, b \in H$. First, $H \neq \phi$ implies $\phi(H) \neq \phi$. Let $a', b' \in \phi(H)$ be two arbitrary elements. By definition, there exists $a, b \in H$ such that $a' = \phi(a)$ and $b' = \phi(b)$, then

$$(a')(b')^{-1} = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1})$$

Since $H < G$ and $ab^{-1} \in H$, $(a')(b')^{-1} \in \phi(H)$, which means that $\phi(H) < G'$.

Part (b) First, $\phi^{-1}(H') \neq \phi$ since $H' \neq \phi$. Let $a, b \in \phi^{-1}(H')$, which is $\phi(a), \phi(b) \in H'$. $H' < G'$ implies that

$$\phi(a)\phi(b)^{-1} = \phi(ab^{-1}) \in H'$$

meaning that $ab^{-1} \in \phi^{-1}(H')$, and so $\phi^{-1}(H') < G$.

Corollary. Let $\phi : G \to G'$. The **image** of ϕ

$$\operatorname{im} \phi := \phi(G) = \{\phi(g) \mid g \in G\}$$

is a subgroup of G'. The **kernel** of ϕ

$$\ker \phi := \phi^{-1}(e_{G'}) = \{g \in G \mid \phi(g) = e_{G'}\}$$

is a subgroup of G.

1.8.4 Applications of Group Homomorphisms

Proposition 1.59. Let $\phi : G \to G'$ be a surjective group homomorphism, then the following applies:

(a) If G is cyclic, G' is also cyclic.

(b) If G is abelian, G' is also abelian.

Proof. Part (a) Note that the fact that ϕ is injective implies $G' = \phi(G)$. If $G = \langle g \rangle$ for some $g \in G$, then $G' = \phi(G) = \langle \phi(G) \rangle$.

Part (b) For $\phi(a), \phi(b) \in G' = \phi(G)$,

$$\phi(a)\phi(b) = \phi(ab) \quad = \phi(ba) = \phi(b)\phi(a)$$

Therefore G' is abelian.

Corollary. If $G \cong G'$, then G is cyclic (abelian) if and only if G' is cyclic (abelian).

Example 1.60. Below are various examples based on *Proposition 1.59*:

(a) $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$ since $\mathbb{Z}_4$ is cyclic but $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not. In fact, $\mathbb{Z}_4$ and $\mathbb{Z}$ are the only two groups of order 4 up to isomorphism.

(b) Although $|S_3| = |\mathbb{Z}_6| = 6$, but $S_3 \ncong \mathbb{Z}_6$ since $\mathbb{Z}_6$ is abelian but S_3 is not. However, $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ with $(1, 1)$ as generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

1.8.5 Group Homomorphisms and Orders

Proposition 1.61. If $\phi : G \to G'$ is an isomorphism, then

$$|\phi(g)| = |g| \ \ \forall g \in G$$

Proof. If $\phi : G \to G'$ is a group homomorphism and $H < G$, then $\phi|_H \colon H \to G'$ is also a group homomorphism. Also, if ϕ is injective, then $\phi|_H$ is also injective.

Apply this to $H = \langle g \rangle$, which gives an injective homomorphism

$$\phi|_{\langle g \rangle} \colon \langle g \rangle \to G'$$

whose image is given by

$$\operatorname{im}(\phi|_{\langle g \rangle}) = \left\{ \phi(g^k) = \phi(g)^k \mid k \in \mathbb{Z} \right\} = \langle \phi(g) \rangle$$

Hence $\phi|_{\langle g \rangle}$ gives an isomorphism from $\langle g \rangle$ onto $\langle \phi(g) \rangle$. In particular, $|g| = |\phi(g)|$.

Example 1.62. Consider $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_3 \times \mathbb{Z}_8$. They are not isomorphic because $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ has an order 12 element $(0, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_{12}$, but $\mathbb{Z}_3 \times \mathbb{Z}_8$ does not.

1.9 Classification of Groups

1.9.1 Classification of Cyclic Groups

Theorem 1.63. Let G be a cyclic group. If $|G| = +\infty$, then $G \cong \mathbb{Z}$. Otherwise, if $|G| = n < +\infty$, then $G \cong \mathbb{Z}_n$.

Proof. Let $G = \langle g \rangle$ for some $g \in G$. The proof is split into two cases:

(a) **Case I:** $|G| = +\infty$

For ϕ to be a homomorphism, note that

$$\begin{aligned}\phi(k_1 + k_2) &= g^{k_1+k_2} = g^{k_1} g^{k_2} \\ &= \phi(k_1)\phi(k_2)\ \forall k_1, k_2 \in \mathbb{Z}\end{aligned}$$

For ϕ to be injective, if $\phi(k_1) \neq \phi(k_2)$ and without the loss of generality, $k_1 \geq k_2$, then

$$\begin{aligned}g^{k_1} = g^{k_2} &\Rightarrow g^{k_1-k_2} = e \\ &\Rightarrow k_1 - k_2 = 0 \quad \text{since } |g| = +\infty \\ &\Rightarrow k_1 = k_2\end{aligned}$$

Since G is generated by g, ϕ is surjective. With all the requirements, ϕ is an isomorphism.

(b) **Case II:** $|G| = n < +\infty$

Note that

$$\begin{cases} G = \langle G \rangle \\ |G| = n \end{cases} \Rightarrow G = \left\{e, g, g^2, \cdots, g^{n-1}\right\}$$

Then there is a bijection

$$\phi : G \to \mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$$

Again, for ϕ to be a homomorphism, note that

$$\begin{aligned}\phi(g^{k_1}+g^{k_2}) &= \phi(g^{k_1+k_2}) \\ &= \begin{cases}\phi(g^{k_1+k_2}) & \text{if } k_1+k_2 \le n-1 \\ \phi(g^{k_1+k_2-n}) & \text{if } n \le k_1+k_2 \le 2n-2\end{cases} \\ &= \begin{cases}k_1+k_2 & \text{if } k_1+k_2 \le n-1 \\ k_1+k_2-n & \text{if } n \le k_1+k_2 \le 2n-2\end{cases} \\ &= \phi(g^{k_1})+\phi(g^{k_2})\end{aligned}$$

With all the requirements, ϕ is an isomorphism.

Note that for any fixed order, there is a unique cyclic group up to isomorphisms.

Corollary. Let G be a cyclic group. If $|G| = p$ where p is a prime number, then $G \cong \mathbb{Z}_p$.

Proof. By the corollary of the Theorem of Lagrange, if $|G| = p$ is prime, then G is cyclic. The result follows from this, together with the second statement above.

Example 1.64. For any positive integer n, the subgroup

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} \subset U = \{z \in \mathbb{C} \mid |z| = 1\} = \left\langle e^{\frac{2\pi i}{n}} \right\rangle$$

Since $|U_n| = n$, by *Theorem 1.63*, $U_n \cong \mathbb{Z}_n$, and an isomorphism is given by $e^{\frac{2\pi i}{n}} \mapsto k$ for $k = 0, 1, 2, \cdots, n-1$.

2 Ring Theory and General Field Theory

2.1 Rings

2.1.1 Definition of Rings

Definition 2.1. A **ring** $(R, +, *)$ is a set R equipped with two binary operations

$$+, * : R \times R \to R$$

such that the following conditions are satisfied:

(a) $(R, +)$ is an abelian group.

(b) $(R, *)$ satisfies the following conditions:

(i) The multiplication $*$ is associative, which is

$$(a * b) * c = a * (b * c) \quad \text{for all } a, b, c \in R$$

(ii) There exists an element $1 \in R$ (which is called the **multiplicative identity**) such that

$$1 * a = a * 1 = a \quad \text{for all } a \in R$$

(c) $(R, +, *)$ satisfies the distributive laws:

(i)
$$a * (b + c) = a * b + a * c \quad \text{for all } a, b, c \in R$$

(ii)
$$(a + b) * c = a * c + b * c \quad \text{for all } a, b, c \in R$$

Note that in the literature, $(R, +, *)$ without part (b)(ii) is also called a ring. In that case, if part (b)(ii) is also satisfied, then $(R, +, *)$ is called a **ring with unity**. For example, $(2\mathbb{Z}, +, *)$ is a ring without unity.

Example 2.2. The following sets equipped with their corresponding usual operations of addition and multiplication are rings:

(a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$, which represents the set of all polynomials with integer, rational, real and complex coefficients respectively.

(c) $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\} \subset \mathbb{R}$.

(d) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Such ring is called the **ring of Gaussian integers**.

(e) $\mathbb{Q}[\alpha] := \{f(\alpha) \mid f(x) \in \mathbb{Q}[x]\} \subset \mathbb{C}, \mathbb{Z}[\alpha] := \{g(\alpha) \mid g(x) \in \mathbb{Z}[x]\} \subset \mathbb{C}$ for any $\alpha \in \mathbb{C}$.

(f) $M_{n\times n}(\mathbb{R})$ for any fixed positive integer n with usual matrix addition and multiplication.

(g) $C[a,b] = \{f : [a,b] \to \mathbb{R} \mid f \text{ is continuous}\}, D[a,b] = \{g : [a,b] \to \mathbb{R} \mid g \text{ is differentiable}\}$.

(h) $\text{Map}(X,R) := \{f : X \to R\}$ for any set X and ring R.

2.1.2 Properties of Rings

Proposition 2.3. Let R be a ring, then R has a unique additive identity and also a unique multiplicative identity.

Proof. The additive identity is automatically unique by the definition of rings. The uniqueness of 0 is also given. Now suppose there are two multiplicative identities $1, 1' \in R$, then $1 = 1 \cdot 1' = 1'$.

Proposition 2.4. Let R be a ring. For any $r \in R$, its **additive inverse** $-r \in R$ is unique. If $r \in R$ has a **multiplicative inverse**, denoted by $r' \in R$ such that $r \cdot r' = r' \cdot r = 1$, then the multiplicative inverse is unique.

Proof. The part about additive inverse is automically true by the definition of rings. For multiplicative inverses, if $r', r'' \in R$ are multiplicative inverses to $r \in R$, then

$$r' = r' \cdot 1 = r' \cdot (r \cdot r'') = (r' \cdot r) \cdot r'' = r''$$

Proposition 2.5. Let R be a ring, then the following equations can be applied:

(a)
$$0 \cdot r = r \cdot 0 = 0 \; \forall r \in R$$

(b)
$$(-1)(-r) = (-r)(-1) = r \; \forall r \in R$$

(c)
$$(-1)r = r(-1) = -r \; \forall r \in R$$

Proof. Part (a)

$$0 \cdot r = (0+0) \cdot r = 0 \cdot r + 0 \cdot r \Rightarrow 0 \cdot r = 0$$

Similarly, $r \cdot 0 = 0$.

Part (b)

$$(-1)(-r) + (-r) = ((-1) + 1)(-r) = 0(-r) = 0$$

thus uniqueness of additive inverse $-r$ implies that $(-1)(-r) = r$. Similarly, $(-r)(-1) = r$.

Proposition 2.6. If R is a ring where the multiplicative identity is the additive identity, which is $1 = 0$, then $R = \{0\}$ which is called the **zero ring**.

Proof. For any $r \in R$, $r = r \cdot 1 = r \cdot 0 = 0$.

2.1.3 Commutative Rings

Definition 2.7. A ring R is said to be **commutative** if

$$ab = ba \; \forall a, b \in R$$

Example 2.8. The following sets equipped with their corresponding usual operations of addition and multiplication are commutative rings:

(a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$.

(c) $\mathbb{Z}[i], \mathbb{Q}[\sqrt{2}], C[a, b], D[a, b]$.

(d) $\mathrm{Map}(X, R)$ where X is a set and R is a commutative ring.

2.2 Common Types of Rings

2.2.1 Modulo Arithmetic

Recall how the remainder is defined in groups:

Definition 2.9. Let n be a positive integer. Consider the group

$$(\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}, +_m)$$

For any $k \in \mathbb{Z}$, the **remainder** of k divided by m, denoted by $\overline{k}$, is equal to $r \in \mathbb{Z}_m$ where $k = mq + r$.

Now define an operation of multiplication $\cdot_m$ on $\mathbb{Z}_m$ by $a \cdot_m b = \overline{a \cdot b}$. Note that $+_m$ and $\cdot_m$ are addition and multiplication defined modulo m. Note that

$$\begin{aligned} &a \equiv c (\text{mod } m) \text{ and } b \equiv d (\text{mod } m) \\ \Rightarrow &a + b \equiv c + d (\text{mod } m) \text{ and } a \cdot b \equiv c \cdot d (\text{mod } m) \end{aligned}$$

the the following proposition can be applied:

Proposition 2.10. $(Z_m, +_m, \cdot_m)$ is a commutative ring.

Proof. Note that $(Z_m, +_m)$ is an abelian group. Let $a, b, c \in \mathbb{Z}_m$, then

$$\begin{aligned} a \cdot_m (b \cdot_m c) &= a \cdot_m \overline{bc} = \overline{a \cdot \overline{bc}} \\ &= \overline{\overline{a} \cdot \overline{bc}} = \overline{abc} \end{aligned}$$

and

$$\begin{aligned} (a \cdot_m b) \cdot_m c &= \overline{ab} \cdot_m c = \overline{\overline{ab} \cdot c} \\ &= \overline{\overline{ab} \cdot \overline{c}} = \overline{abc} \end{aligned}$$

Therefore $\cdot_m$ is associative. With $1 \in \mathbb{Z}_m$ as the multiplicative identity, then

$$\begin{aligned} a \cdot_m (b +_m c) &= a \cdot_m \overline{b + c} = \overline{a \cdot \overline{b + c}} \\ &= \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} \\ &= \overline{a \cdot b} + \overline{a \cdot c} = a \cdot_n b + a \cdot_n c \end{aligned}$$

2.2.2 Polynomial Rings

Definition 2.11. Let R be a nonzero ($1 \neq 0$) commutative ring. A **polynomial** with coefficients in R (in one variable) is a formal sum

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_i \in R$ and $a_i \neq 0$ only for finitely many i.

Note that a polynomial with coefficients in R is essentially a finite sequence of elements in R.

Definition 2.12. Let $f(x)$ be a polynomial defined in *Definition 2.11*. The **degree** of $f(x)$ is defined as

$$\deg f(x) := \begin{cases} \max \{i \in \mathbb{Z}_{\geq 0} \mid a_i \neq 0\} & \text{if } f(x) \not\equiv 0 \\ -\infty & \text{if } f(x) \equiv 0 \end{cases}$$

The notation $R[x]$ is the set of all polynomials with coefficients in R. With such notation, the following proposition can be introduced:

Proposition 2.13. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[x]$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i \in R[x]$ be polynomials defined in *Definition 2.11*, then the following can be applied:

(a) **Equality of Polynomials**

$f(x) = g(x)$ if and only if $a_i = b_i$ for all i as elements in $R[x]$.

(b) **Addition of Polynomials**

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

(c) **Multiplication of Polynomials**

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} c_i x^i$$

where $c_i = \sum_{k=0}^{i} a_k b_{i-k}$.

Note that the addition operation is well-defined since $a_i + b_i \neq 0$ only for finitely many i. With the binary operations required, there is the following proposition:

Proposition 2.14. $(R[x], +, \cdot)$ is a nonzero commutative ring.

Proof. Note that the following are true:

(a) $(R[x], +)$ is an abelian group with additive identity $0 \in R[x]$, which is the zero polynomial.

(b) $1 \in R[x]$ is the multiplicative identity.

(c) For associativity for multiplication, let $f(x) = \sum_i a_i x^i, g(x) = \sum_i b^i x^i, h(x) = \sum_i c^i x^i \in R[x]$, then

$$\begin{aligned} f \cdot (g \cdot h) &= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i \left(\sum_{m+n=j} b_m c_n \right)_j \right) x^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} \sum_{m+n=j} a_i b_m c_n \right) x^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{i+m+n=k} a_i b_m c_n \right) x^k \end{aligned}$$

On the other hand,

$$\begin{aligned}(f \cdot g) \cdot h &= \left(\sum_{l=0}^{\infty} \left(\sum_{i+m=l} a_i b_m\right) x^l\right) \cdot \left(\sum_i c_i x^i\right) \\ &= \sum_{k=0}^{\infty} \left(\sum_{l+n=k} \sum_{i+m=l} a_i b_m c_n\right) x_k \\ &= \sum_{k=0}^{\infty} \left(\sum_{i+m+n=k} a_i b_m c_n\right) x^k\end{aligned}$$

(d) The binary operation satisfies the distributive laws.

Definition 2.15. Given a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$, define a **function** as

$$\phi_f : \alpha \in R \mapsto f(\alpha) = \sum_{i=0}^{n} a_i x^i \in R$$

Proposition 2.16. Given polynomials $f, g \in R[x]$ with functions $\phi_f, \phi_g : R \to R$, if $\phi_f = \phi_g$ as functions of $R \to R$, then $f = g$ as polynomials in $R[x]$.

For example, $f(x) \in \mathbb{R}[x]$ defines a function $\phi_f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$. Moreover, if $g(x) \in \mathbb{R}[x]$ where $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{R}$, then $f = g$ in $R[x]$. This means that f and g have exactly the same coefficients.

However, this may not be true in general, especially when the cardinality of R is finite. Consider $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ and $g = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$, then $f \neq g$ in $\mathbb{Z}_2[x]$ but $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{Z}_2$.

2.3 Integral Domains and Fields

2.3.1 Integral Domains

Definition 2.17. An **integral domain** is a nonzero commutative ring R where the product of any two nonzero elements is always nonzero.

Definition 2.18. A nonzero element r in a ring R is called a **zero divisor** if there exists nonzero element $s \in R$ such that $rs = 0$.

With the definitions above, it can be shown that a nonzero commutative ring R is an integral domain if and only if it has no zero divisors.

Proposition 2.19. A commutative ring R is an integral domain if and only if the cancellation law holds for multiplication, which is $ca = cb$ and $c \neq 0$ implies $a = b$.

Proof. ($\Rightarrow$) Suppose R is an integral domain. If $ca = cb$, then by distributive laws, $c(a-b) = c(a+(-b)) = 0$. Since R is an integral domain, either $c = 0$ and $a - b = 0$. Given that $c \neq 0$, so $a = b$.

($\Leftarrow$) Suppose cancellation law holds. Suppose there are nonzero $a, b \in R$ such that $ab = 0$, then by the previous result, $0 = a0$ and this will give out $ab = a0$. Cancellation leads to $b = 0$, which contradicts the assumption.

2.3.2 Units

Definition 2.20. Let R be a ring, then an element $a \in R$ is said to be a **unit** if it has a multiplicative inverse. In other words, there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Example 2.21. Below are various examples of units:

(a) 1 and -1 are the only units of $\mathbb{Z}$.

(b) Let R be the ring of all real-valued functions on $\mathbb{R}$, then any function $f \in R$ satisfying $f(x) \neq 0$ for all x is a unit.

(c) Let R be the ring of all continuous real-valued functions on $\mathbb{R}$, then $f \in R$ is a unit if and only if it is either strictly positive or strictly negative.

Proposition 2.22. The only units of $\mathbb{Q}[x]$ are nonzero constants.

Proof. Given any $f \in \mathbb{Q}[x]$ such that $\deg f > 0$, for all nonzero $g \in \mathbb{Q}[x]$,

$$\deg fg \geq \deg f > 0 = \deg 1$$

and hence $fg \neq 1$. If $g = 0$, then $fg = 0 \neq 1$, so f has no multiplicative inverse.

If f is a nonzero constant, then $f^{-1} = \frac{1}{f}$ is a constant polynomial in $\mathbb{Q}[x]$ and

$$f\left(\frac{1}{f}\right) = \frac{1}{f}(f) = 1$$

Therefore f is a unit.

Finally, if $f = 0$, then $fg = 0 \neq 1$ for all $g \in \mathbb{Q}[x]$, so the zero polynomial has no multiplicative inverse.

2.3.3 Fields

Definition 2.23. A **field** is a commutative ring with $1 \neq 0$ where every nonzero element is a unit.

In other words, a nonzero commutative ring F is a field if and only if every nonzero element $r \in F$ has a multiplicative inverse r^{-1}, which is $rr^{-1} = r^{-1}r = 1$.

Example 2.24. With the definition of fields, it can be shown that:

(a) $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not.

(b) Polynomial rings, including $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$, are not fields.

Note that if every nonzero element of a commutative ring has a multiplicative inverse, then the ring is an integral domain since

$$ca = cb \Rightarrow c^{-1}ca = c^{-1}cb \Rightarrow a = b$$

and this leads to the following proposition:

Proposition 2.25. A field is an integral domain.

Proposition 2.26. Let $k \in \mathbb{Z}_m \setminus \{0\}$. If $\gcd(k, m) > 1$, then k is a zero divisor. If $\gcd(k, m) = 1$, then k is a unit.

Proof. Let $d = \gcd(k, m)$. If $d > 1$, then $\frac{m}{d}$ is a nonzero element in $\mathbb{Z}_m$, and

$$k \cdot_m \frac{m}{d} = \overline{\frac{k}{d} \cdot m} = 0$$

so k is a zero divisor. On the other hand, if $d = 1$, then there exists $a, b \in \mathbb{Z}$ such that $ak + bm = 1$, but this means $\overline{a}k = 1$ in $\mathbb{Z}_m$, so k is a unit.

2.4 Ring Homomorphisms

2.4.1 Definition of Ring Homomorphisms

Definition 2.27. Let R and R' be rings. A **ring homomorphism** from R to R' is a map $\phi : R \to R'$ such that the following are satisfied:

(a) **Multiplicative Identity**

$$\phi(1_R) = 1_{R'}$$

(b) **Addition**

$$\phi(a+b) = \phi(a) + \phi(b)$$

(c) **Multiplication**

$$\phi(ab) = \phi(a)\phi(b)$$

Note that part (a) of the definition above is not imposed in some textbooks.

2.4.2 Properties of Ring Homomorphisms

Proposition 2.28. Let R and R' be rings. If $\phi : R \to R'$ is a ring homomorphism, then $\phi : (R, +) \to (R', +')$ is a homomorphism between abelian groups.

In particular, $\phi(0_R) = 0_{R'}$ and $\phi(-a) = -\phi(a)$ for all $a \in R$. Note that the converse of the above proposition is not true. For example, $\psi : \mathbb{Z} \to \mathbb{Z}$ where $k \mapsto 2k$ is a group homomorphism, but it is not a ring homomorphism.

Proposition 2.29. Let R and R' be rings. If $\phi : R \to R'$ is a ring homomorphism and $u \in R^x$ is an element from the set of all units in R, then $\phi(u^{-1}) = \phi(u)^{-1}$.

Proof. By the definition of ring homomorphism,

$$\phi(u^{-1})\phi(u) = \phi(u^{-1}u) = \phi(1_R) = 1_{R'}$$

then $\phi(u^{-1}) = \phi(u)^{-1}$.

2.4.3 Examples of Ring Homomorphisms

Example 2.30. Below are various examples of ring homomorphisms:

(a) For any positive integer n, the remainder map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where $k \mapsto \overline{k}$ is a ring homomorphism, since the following conditions are satisfied:

(i) **Multiplicative Identity**

$$\phi(1) = \overline{1} = 1$$

(ii) **Addition**

$$\phi(k_1 + k_2) = \overline{k_1 + k_2} = \overline{\overline{k_1} + \overline{k_2}} = \phi(k_1) + \phi(k_2)$$

(iii) **Multiplication**

$$\phi(k_1 k_2) = \overline{k_1 k_2} = \overline{(\overline{k_1})(\overline{k_2})} = \phi(k_1)\phi(k_2)$$

Note that the zero map $\phi : R \to R'$ where $r \mapsto 0_{R'}$ is not a ring homomorphism because of part (a) of *Definition 2.27*.

(b) For any ring R, the map $\phi : \mathbb{Z} \to R$ where

$$n \mapsto n \cdot 1_R = \begin{cases} \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} & \text{if } n > 0 \\ 0_R & \text{if } n = 0 \\ \underbrace{(-1_R) + \cdots + (-1_R)}_{n \text{ times}} & \text{if } n < 0 \end{cases}$$

is a ring homomorphism, since the following conditions are satisfied:

(i) **Multiplicative Identity**

$$\phi(1) = 1 \cdot 1_R = 1_R$$

(ii) **Addition**

$$\phi(n_1 + n_2) = (n_1 + n_2)1_R = n_1 1_R + n_2 1_R = \phi(n_1) + \phi(n_2)$$

(iii) **Multiplication**

$$\phi(n_1 n_2) = (n_1 n_2)1_R = (n_1 1_R)(n_2 1_R) = \phi(n_1)\phi(n_2)$$

Note that for any ring R, ϕ is the only ring homomorphism from $\mathbb{Z}$ to R. If $\theta : \mathbb{Z} \to R$ is a ring homomorphism, then $\phi(1) = 1_R$ and this implies

$$\begin{aligned} \theta(n) &= \theta(\underbrace{1 + \cdots + 1}_{n \text{ times}}) \\ &= \underbrace{\theta(1) + \cdots + \theta(1)}_{n \text{ times}} \\ &= n\theta(1) = n \cdot 1_R = \phi(n) \end{aligned}$$

for all $n \in \mathbb{Z}$.

2.4.4 Characteristics of Integral Domains

Definition 2.31. Let D be an integral domain. If there does not exist $n \in \mathbb{Z}_{>0}$ such that $\phi(n) = 0$, then D is said to have **characteristic** 0, denoted as $\text{char}(D) = 0$.

On the other hand, if there exists $n \in \mathbb{Z}_{>0}$ such that $\phi(n) = 0$, then D is said to have **positive characteristic**, and $\text{char}(D) = \min\{n \in \mathbb{Z}_{>0} \mid n \cdot 1_D = 0\}$.

Proposition 2.32. If D is an integral domain of positive characteristic, then $\text{char}(D)$ is a prime number.

Example 2.33. Below are various examples of characteristics of integral domains:

(a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all of characteristic 0.

(b) $\mathbb{Z}_n$ is not an integral domain if n is composite, then $n = p$ where p is a prime and $\text{char}(\mathbb{Z}_n) = p$.

(c) The **natrual inclusion**

$$\phi : \mathbb{Z} \to \mathbb{Q} = \underset{\sim}{\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})}$$

where $n \mapsto \frac{n}{1}$ is a ring homomorphism.

More generally, if D is an integral domain, and

$$F = \underset{\sim}{D \times (D \setminus \{0\})}$$

is the field of fractions, then the map $\phi : D \to F$ where $a \mapsto [(a, 1)]$ is an injective ring homomorphism, since the following conditions are satisfied:

(i) **Multiplicative Identity**

$$\phi(1) = [(1, 1)]$$

(ii) **Addition**

$$\phi(a_1 + a_2) = [(a_1 + a_2, 1)] = [(a_1, 1)] + [(a_2, 1)] = \phi(a_1) + \phi(a_2)$$

(iii) **Multiplication**

$$\phi(a_1 a_2) = [(a_1 a_2, 1)] = [(a_1, 1)][(a_2, 1)] = \phi(a_1)\phi(a_2)$$

(iv) **Injectivity**

To show that ϕ is injective,

$$\ker \phi = \{a \in D \mid [(a, 1)] = [(0, 1)]\} = \{a \in D \mid a \cdot 1 = 1 \cdot 0\} = \{0\} \subset D$$

(d) Let R be a commutative ring. For any $a \in R$, the **evaluation map**

$$\phi_a : R[x] \to R$$

where $f(x) \mapsto f(a)$ is a surjective ring homomorphism.

2.5 Subrings and Ideals

2.5.1 Definition of Subrings

Definition 2.34. Let R be a ring. A subset $S \subset R$ is called a **subring** if it is closed under the addition $+$ and multiplication $\cdot$ in R and S itself is a ring with unity 1_R under the induced operations. In other words, $S \subset R$ is a subring of R if it satisfies the conditions in *Definition 2.2*.

Note that for any ring R, $\{0\} \subset R$ is not a subring. Below is a practical criterion for checking whether a subset is a subring:

Proposition 2.35. Let R be a ring, then a subset $S \subset R$ is a subring if and only if the following conditions are satisfied:

(a)
$$1_R \in S$$

(b)
$$a - b \in S \; \forall a, b \in S$$

(c)
$$a \cdot b \in S \; \forall a, b \in S$$

Proposition 2.36. Let $\phi : R \to R'$ be a ring homomorphism, then the following are true:

(a) If $S < R$ is a subring of R, then $\phi(S) < R'$.

(b) If $S' < R'$ is a subring of R', then $\phi^{-1}(S') < R$.

Proof. Note that the following are true:

(i)
$$\phi(1_R) = 1_{R'} \in S' \Rightarrow 1_R \in \phi^{-1}(S')$$

(ii) Let $a, b \in \phi^{-1}(S')$, then $\phi(a), \phi(b) \in S'$.

Since S' is a subring, then

$$\begin{cases} \phi(a-b) = \phi(a) - \phi(b) \in S' \\ \phi(ab) = \phi(a)\phi(b) \in S' \end{cases} \Rightarrow a - b, ab \in \phi^{-1}(S')$$

hence $\phi^{-1}(S')$ is a subring of R.

Corollary. For any ring homomorphism $\phi : R \to R'$, its image

$$\operatorname{im} \phi = \phi(R) = \{\phi(a) \mid a \in R\}$$

is a subring of R'.

Note that $\ker \phi$ is not a subring unless R' is the zero ring, because $\phi(1_R) = 1_{R'} \neq 0$ unless $R' = \{0_{R'}\}$.

Example 2.37. Consider an integral domain D contained inside a field F, which is $D \subset F$. Let $\alpha \in F$, then this defines the evaluation map $\phi_\alpha : D[x] \to F$ where $f(x) \mapsto f(\alpha)$ is a ring homomorphism. By the corollary of *Proposition 2.36*,

$$D[\alpha] := \operatorname{im} \phi_\alpha = \{f(\alpha) \mid f \in D[x]\}$$

is a subring of F. In particular, $D[\alpha]$ is an integral domain.

2.5.2 Definition of Ideals

Definition 2.38. A subset I of a commutative ring R is said to be an **ideal** if the following properties are satisfied:

(a) $0 \in I$.

(b) If $a, b \in I$, then $a + b \in I$.

(c) For all $a \in I$, $ar \in I$ for all $r \in R$.

2.6 Quotient Rings

2.6.1 Residues

Definition 2.39. Let R be a commutative ring and $I \subset R$ be an ideal. Consider the set $R/I = \{a + I \mid a \in R\}$, then $a + I \in R/I$ is said to be the **residue** of $a \in R$, denoted by $\overline{a}$.

2.6.2 Construction of Quotient Rings

Recall that $\overline{a}$ is the equivalence class containing a with respect to the relation $a \sim b \Leftrightarrow a - b \in I$. In particular, for any $a, b \in R$, $\overline{a} = \overline{b} \Leftrightarrow a - b \in I$. In this case, a is said to be congruent to b modulo I, denoted by $a \equiv b (\mathrm{mod}\ I)$.

Now define an operation $+$ on R/I such that

$$(a+I)+(b+I) := (a+b)+I$$

and the binary operation above is well-defined. More precisely, it has to be checked if

$$\begin{cases} a'+I = a+I \\ b'+I = b+I \end{cases}$$

then $(a'+b')+I = (a+b)+I$. Suppose

$$\begin{cases} a'+I = a+I \\ b'+I = b+I \end{cases} \Leftrightarrow \begin{cases} a'-a \in I \\ b'-b \in I \end{cases}$$

and since $(I,+) < (R,+)$,

$$\begin{aligned} &(a'-a)+(b'-b) \in I \\ \Rightarrow &(a'+b')-(a+b) \in I \\ \Rightarrow &(a'+b')+I = (a+b)+I \end{aligned}$$

so $+$ on R/I is well-defined. Furthermore, check if the binary operation can form an abelian group:

Proposition 2.40. $(R/I,+)$ is an abelian group.

Proof. Note that associativity and commutativity of $+$ follow from those in R. The additive identity is $0+I=I$, and the additive inverse of $a+I$ is $(-a)+I$.

Note that the above only involves the addition in R. In particular, given any subgroup H in an abelian group G, the quotient abelian group G/H is constructed as above. If $|G| < +\infty$, then

$$|G/H| = [G:H] = \frac{|G|}{|H|}$$

Theorem 2.41. Let R be a commutative ring and $(I,+) < (R,+)$ is an additive subgroup, then the binary operation

$$(a+I)\cdot(b+I) := (ab)+I$$

is well-defined if and only if I is an ideal.

Proof. ($\Leftarrow$) Suppose I is an ideal. Also suppose that

$$\begin{cases} a'+I = a+I \\ b'+I = b+I \end{cases}$$

then it has to be checked that $a'b' + I = ab + I$. Note that the above implies that there exists $i, j \in I$ such that

$$\begin{cases} a' = a + i \\ b' = b + j \end{cases}$$

then

$$a'b' = (a + i)(b + j) = ab + aj + bi + ij$$

where $aj+bi+ij \in I$ since I is an ideal. This means that $a'b' = ab$ and $a'b'+I = ab+I$.

($\Rightarrow$) Suppose the multiplication is well-defined. Let $a \in R$ and $i \in I$, then $i + I = 0 + I$ and the well-definedness of the multiplication implies that

$$\begin{aligned} (0 + I)(a + I) &= (i + I)(a + I) \\ I &= (ai) + I \end{aligned}$$

so $ai \in I$ and I is an ideal.

Corollary. $(R/I, +, \cdot)$ is a ring.

Proof. Associtativity of $\cdot$ and the distributive laws are inherited from R. The multiplicative identity is $1 + I$.

2.6.3 Quotient Rings

With the construction above, the definition of quotient rings is as below:

Definition 2.42. Let R be a commutative ring and $I \subset R$ be an ideal, then R/I is called the **quotient ring** of R by the ideal I.

Proposition 2.43. Consider the map $\pi : R \to R/I$ where $a \mapsto a + I$, then π is a surjective map homomorphism.

Proof. For any $a, b \in R$,

$$\pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b)$$

and

$$\pi(ab) = (ab) + I = (a + I)(b + I) = \pi(a)\pi(b)$$

2.6.4 First Isomorphism Theorem

Below the **First Isomorphism Theorem** is introduced:

Theorem 2.44. Let $\phi : R \to R'$ be a ring homomorphism, then

$$R/\ker\phi \cong \text{im}\phi$$

More precisely, the map

$$\overline{\phi} : R/\ker\phi \to \text{im}\phi \quad \text{where } a + \ker\phi \mapsto \phi(a)$$

is a ring homomorphism such that $\phi = \overline{\phi} \circ \pi$.

Proof.

(a) **Well-definedness of $\overline{\phi}$**

Let $a, a' \in R$ such that $a + \ker\phi = a' + \ker\phi$, and this means that $\phi(a - a') = 0$. With some evaluations, $\overline{\phi}(a + \ker\phi) = \phi(a) = \phi(a') = \overline{\phi}(a' + \ker\phi)$. Therefore $\overline{\phi}$ is well-defined.

(b) **Homomorphism Property of $\overline{\phi}$**

Let $a + \ker\phi, b + \ker\phi \in R/\ker\phi$, then

$$\begin{aligned}
&\overline{\phi}((a + \ker\phi) + (b + \ker\phi)) \\
=&\overline{\phi}((a + b) + \ker\phi) \\
=&\phi(a + b) = \phi(a) + \phi(b) \\
=&\overline{\phi}(a + \ker\phi) + \overline{\phi}(b + \ker\phi)
\end{aligned}$$

and

$$\begin{aligned}
&\overline{\phi}((a + \ker\phi) \cdot (b + \ker\phi)) \\
=&\overline{\phi}((ab) + \ker\phi) \\
=&\phi(ab) = \phi(a)\phi(b) \\
=&\overline{\phi}(a + \ker\phi)\overline{\phi}(b + \ker\phi)
\end{aligned}$$

(c) **Isomorphism Property of $\overline{\phi}$**

By definition, every element of $\text{im}\phi$ is of the form $\phi(a) = \overline{\phi}(a + \ker\phi)$ for some $a \in R$. Then $\overline{\phi}$ is surjective. Also note that

$$\begin{aligned}\ker \overline{\phi} &= \{a + \ker \phi \mid \phi(a) = 0\} \\ &= \{a + \ker \phi \mid a \in \ker \phi\} \\ &= \{\ker \phi\}\end{aligned}$$

therefore $\overline{\phi}$ is injective and $\overline{\phi}$ is an isomorphism for rings.

Finally, for any $a \in R$,

$$(\overline{\phi} \circ \pi)(a) = \overline{\phi}(a + \ker \phi) = \phi(a)$$

therefore $\phi = \overline{\phi} \circ \pi$.

In fact, π is called the **canonical map** (or **projection map**).

Example 2.45. Below are various examples of quotient rings:

(a) For any positive integer n, the remainder map

$$\phi : \mathbb{Z} \to \mathbb{Z}_n$$

is a surjective ring homomorphism with

$$\ker \phi = \left\{k \in \mathbb{Z} \mid \overline{k} = 0\right\} = n\mathbb{Z}$$

so by the First Isomorphism Theorem, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(b) Consider the map

$$\phi : \mathbb{Z} \to \mathbb{Z}[i] \setminus (1 + 3i) \quad \text{where } n \mapsto \overline{n} = n + (1 + 3i)$$

Note that $\mathbb{Z}[i]$ is also a PID, so every ideal in it is a principal ideal. ϕ is a surjective ring homomorphism and

$$\ker \phi = 10\mathbb{Z}$$

Proof. Let $m, n \in \mathbb{Z}$, then

$$\phi(n + m) = (n + m) + (1 + 3i) = (n + (1 + 3i)) + (m + (1 + 3i)) = \phi(n) + \phi(m)$$

and

$$\phi(nm) = (nm) + (1+3i) = (n + (1+3i))(m + (1+3i)) = \phi(n)\phi(m)$$

To show that ϕ is surjective, observe that in $\mathbb{Z}[i] \setminus (1+3i)$, $\overline{1+3i} = \overline{0}$. Let $I = (1+3i)$, then

$$\begin{aligned} 1 + 3i &\equiv 0 (\mathrm{mod} I) \\ 1 &\equiv -3i (\mathrm{mod} I) \\ i &\equiv 3 (\mathrm{mod} I) \end{aligned}$$

For an arbitrary element $\overline{a+bi} \in \mathbb{Z}[i] \setminus (1+3i)$,

$$\overline{a+bi} = \overline{a+3b} = \phi(a+3b)$$

and hence ϕ is surjective. Now consider

$$\ker \phi = \left\{ n \in \mathbb{Z} \mid \overline{n} = \overline{0} \right\}$$

note that $\overline{n} = \overline{0}$ implies $n = (a-3b)+(b+3a)i$ for some $a+bi \in \mathbb{Z}[i]$. Solving the system of equations, $n = 10a$, and the above argument shows that if $\overline{n} \in \ker \phi$, then $n \in 10\mathbb{Z}$ and $\ker \phi \subset 10\mathbb{Z}$. On the other hand, $10 = (1+3i)(1-3i)$ leads to $= 10 \in \ker \phi$ and hence $10\mathbb{Z} \subset \ker \phi$.

As a result, $\ker \phi = 10\mathbb{Z}$. By the First Isomorphism Theorem, $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}[i] \setminus (1+3i)$.

2.7 Factorization of Polynomials

2.7.1 Principal Ideal Domains

Recall an ideal $(a) = \{ar \mid r \in R\}$ generated by one element $a \in R$ is called a principal ideal. Note that $R = (1)$ and $\{0\} = (0)$ are both principal ideals.

Definition 2.46. Let R be an integral domain, then R is a **principal ideal domain** (**PID**) if every ideal in R is principal.

Note that the definition of principal ideal domains brings out an interesting fact: any field is a principal ideal domain. However, the following proposition needs to be established first.

Proposition 2.47. Let R be a commutative ring, then for all $d, f \in R[x]$ where the leading coefficient of d is a unit in R, there exists $q, r \in R[x]$ such that

$$f = qd + r,\ \deg(r) < \deg(d)$$

Proof. The proof is using induction to complete. For the base case, if $\deg(f) < \deg(d)$, take $r = f$, then $f = 0d + r$ and $\deg(r) < \deg(d)$. For inductive step, let

$$d = \sum_{i=0}^{n} a_i x^i \in R[x]$$

be fixed where a_n is a unit in R. For any given

$$f = \sum_{i=0}^{m} b_i x^i \in R[x]$$

where $m \geq n$, suppose the claim holds for all f' with $\deg(f') < \deg(f)$, let

$$f' = f - a_n^{-1} b_m x^{m-n} d$$

By hypothesis there exists $q', r' \in R[x]$ with $\deg(r') < \deg(d)$ such that

$$\begin{aligned} f - a_n^{-1} b_m x^{m-n} d &= q'd + r' \\ f &= (a_n^{-1} b_m x^{m-n} + q')d + r' \end{aligned}$$

which is in the form $f = qd + r'$ where $q \in R[x]$ and $\deg(r') < \deg(d)$.

Theorem 2.48. Let F be a field, then $F[x]$ is a principal ideal domain.

Proof. Let I be an ideal of $F[x]$ and d be a nonzero polynomial in I with the least leading degree. Such d can be found since the leading degree of a polynomial is a nonnegative integer. I is ideal implies $(d) \subset I$.

By division theorem, $f = qd + r$ for some $q, r \in F[x]$ where $\deg(r) < \deg(d)$. Note that $r = f - qd$ lies in I. Since d is a nonzero element of I with the least degree, $r = 0$, leaving $f = qd$. Finally, $f \in (d)$ and $I \subset (d)$, so $I = (d)$ can be concluded.

2.7.2 Factor Theorem for Polynomials

Definition 2.49. Let F be a field and $f = \sum_{i=0}^{n} c_i x^i$ be a polynomial in $F[x]$. An element $a \in F$ is a **root** of f if

$$f(a) = \sum_{i=0}^{n} c_i a^i = 0$$

In fact the above definition is just a small recall from secondary school mathematics, but with the introduction of fields.

Proposition 2.50. For all polynomials $f \in F[x]$ and elements $a \in F$, there exists $q \in F[x]$ such that

$$f = q(x - a) + f(a)$$

With the proposition above, **Factor Theorem** can be introduced:

Theorem 2.51. Let F be a field and f be a polynomial in $F[x]$, then $a \in F$ is a root in f if and only if $(x - a)$ divides f in $F[x]$.

Theorem 2.52. Let F be a field and f be a nonzero polynomial in $F[x]$ with degree n, then f has at most n roots in F. Moreover, if $a_1, a_2, \cdots, a_n \in F$ are distinct roots of f, then

$$f = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

where c is a constant in F.

Corollary. Let F be a field, and f, g be nonzero polynomials in $F[x]$ with maximum degree of n, or $n = \max\{\deg(f), \deg(g)\}$, then if $f(a) = g(a)$ for $n + 1$ distinct elements $a \in F$, then $f = g$.

2.7.3 Monic Polynomials

Definition 2.53. Let f be a polynomial in $F[x]$, then f is **monic** if its leading coefficient is 1.

Proposition 2.54. Let F be a field, and f, g be nonzero polynomials in $F[x]$, then there exists a unique monic polynomial $d \in F[x]$ with the following properties:

(a) $(f, g) = (d)$.

(b) d divides f and g, or there exists $a, b \in F[x]$ such that $f = ad$ and $g = bd$.

(c) There exists $p, q \in F[x]$ such that $d = pf + qg$.

(d) If $h \in F[x]$ is a divisor of f and g, then h divides d.

Note that the polynomial d in the proposition above is called the **greatest common divisor** (**gcd**) of f and g. If $d = 1$, f and g are **relatively prime**.

Definition 2.55. Let p be a nonconstant polynomial in $F[x]$, then p is **irreducible** if there do not exist $f, g \in F[x]$ such that $\deg(p) > \max\{\deg(f), \deg(g)\}$ and $p = fg$.

2.7.4 Unique Factorization Domain

Definition 2.56. Let D be an integral domain, then D is a **unique factorization domain** (**UFD**) if any nonzero nonunit $r \in D$ can be factorized into a unique finite product of irreducible elements.

Proposition 2.57. If F is a field, then F is also a principal ideal domain and a unique factorization domain.

Proposition 2.58. A polynomial $f \in F[x]$ is a unit if and only if it is a nonzero constant polynomial.

Proof. If $f, g \in F[x]$ are nonzero polynomials satisfying $fg = 1$, then by comparing degrees on both sides gives $\deg(f) + \deg(g) = 0$, which means $\deg(f) = \deg(g) = 0$ and f, g are constant polynomials.

Corollary. Every nonconstant polynomial $f \in F[x]$ can be expressed as

$$f = cp_1p_2 \cdots p_n$$

where c is a nonzero constant, and each p_i is a monic irreducible polynomial in $F[x]$. The factorization is unique up to reordering of the factors.

With the proposition above, the greatest common divisor of two polynomials can be computed using the Euclidean Algorithm as in the case of $\mathbb{Z}$.

Theorem 2.59. Let F be a field and p be a polynomial in $F[x]$, then the following statements are equivalent:

(a) $F[x]/(p)$ is a field.

(b) $F[x]/(p)$ is an integral domain.

(c) p is irreducible in $F[x]$.

2.7.5 Rational Polynomials

Proposition 2.60. Let $f = \sum_{i=0}^{n} a_i x^i$ be a polynomial in $\mathbb{Q}[x]$ with $a_i \in \mathbb{Z}$, then every rational root r of f in $\mathbb{Q}$ has the form $r = \frac{b}{c}$, where $\gcd\{b, c\} = 1$, $b \mid a_0$ and $c \mid a_n$.

Proof. Let $r = \frac{b}{c}$ be a root of f, then

$$\sum_{i=0}^{n} a_i \left(\frac{b}{c}\right)^i = 0$$

Multiply both sides with c^n and rearrange gives

$$a_0 c^n = -b(a_1 c^{n-1} + a_2 c^{n-2} b + \cdots + a_n b^{n-1})$$

and given that b and c are relatively prime, b divides a_0. Similarly,

$$a_n b^n = -c(a_0 c^{n-1} + a_1 c^{n-2} b + \cdots + a_{n-1} b^{n-1})$$

shows that c divides a_n.

The proposition above is useful to determine whether a polynomial (especially with degree 3 or greater) because such a polynomial is reducible only if it has a root in $\mathbb{Q}$.

Example 2.61. Check whether $f(x) = x^3 + 3x + 2 \in \mathbb{Q}[x]$ is reducible or not.

Answer. By *Proposition 2.60*, only ± 1 and ± 2 are possible roots. However, none of the possible roots satisfies the equation $f(x) = 0$. Therefore, $f(x)$ is irreducible.

Definition 2.62. Let f be a polynomial in $\mathbb{Z}[x]$, then f is **primitive** if the greatest common divisor of its coefficients is 1.

By the definition above, a monic polynomial is primitive. Moreover, if d is the greatest common divisor of coefficients of f, then $(1/d)f$ is primitive. Below is the **Gauss' Lemma**:

Proposition 2.63. If $f, g \in \mathbb{Z}[x]$ are both primitive, then fg is also primitive.

Proof. Let $f = \sum_{k=0}^{m} a_k x^k$, $g = \sum_{k=0}^{n} b_k x^k$, then $fg = \sum_{k=0}^{m+n} c_k x^k$ where

$$c_k = \sum_{i+j=k} a_i b_j$$

Assume fg is not primitive, then there exists a prime p such that p divides any c_k. Since f is primitive, there exists a least $0 < u < m$ such that a_u is not divisible by p. Similarly, since g is primitive, there exists a least $0 < v < n$ such that b_v is not divisible by p. Now

$$c_{u+v} = \sum_{\substack{i+j=u+v \\ (i,j)\neq(u,v)}} a_i b_j + a_u b_v$$

Hence

$$a_u b_v = c_{u+v} - \sum_{\substack{i+j=u+v \\ i<u}} a_i b_j - \sum_{\substack{i+j=u+v \\ j<v}} a_i b_j$$

shows that every term on the right hand side are divisible by p. By Euclid's Lemma, p divides either a_u or b_v, which leads to a contradiction. Therefore, fg is primitive.

Definition 2.64. Let f be a nonzero polynomial in $\mathbb{Q}[x]$, then there exists a **content** of f, denoted by $c(f)$, and a primitive polynomial $f_0 \in \mathbb{Z}[x]$ such that

$$f = c(f) f_0$$

Below are some propositions about contents of polynomials:

Proposition 2.65. If $f \in \mathbb{Z}[x]$, then $c(f) \in \mathbb{Z}$.

Proof. Let d be the greatest common divisor of the coefficients of f, then naturally $(1/d)f$ is a primitive polynomial and

$$f = d\left(\frac{1}{d} f\right)$$

is a factorization of f into a product of a positive rational number and a primitive polynomial in $\mathbb{Z}[x]$. Therefore by the uniqueness of $c(f)$ and f_0, $c(f) = d \in \mathbb{Z}$.

Proposition 2.66. Let f, g, h be nonzero polynomials in $\mathbb{Q}[x]$ such that $f = gh$, then $c(f) = c(g)c(h)$ and $f_0 = g_0 h_0$.

Proof. The equation $f = gh$ implies

$$c(f) f_0 = c(g)c(h) g_0 h_0$$

where $c(f), c(g), c(h)$ are positive rational numbers, and f_0, g_0, h_0 are primitive polynomials. By Gauss' Lemma, $g_0 h_0$ is also primitive. Finally, the uniqueness of content and primitive polynomial shows that $c(f) = c(g)c(h)$ and $f_0 = g_0 h_0$.

Theorem 2.67. Let f be a nonzero polynomial in $\mathbb{Z}[x]$. If $f = GH$ for some $G, H \in \mathbb{Q}[x]$, then $f = gh$ for some $g, h \in \mathbb{Z}[x]$, where $\deg(g) = \deg(G)$ and $\deg(h) = \deg(H)$.

For the following theorem, let p be a prime, and $\mathbb{Z}_p \cong \mathbb{Z}/\mathbb{Z}$. Note that $\mathbb{Z}_p$ is a field since p is a prime. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the residue of a in $\mathbb{Z}_p$.

Theorem 2.68. Let $f = \sum_{k=0}^{n} a_k x^k$ be a monic polynomial in $\mathbb{Z}[x]$. If $\overline{f} := \sum_{k=0}^{n} \overline{a_k} x^k$ is irreducible in $\mathbb{Z}_p[x]$ for some prime p, then f is irreducible in $\mathbb{Q}[x]$.

Below is the **Einstein's Criterion**:

Theorem 2.69. Let $f = \sum_{k=0}^{n} a_k x^k$ be a polynomial in $\mathbb{Z}[x]$. If there exists a prime p such that $p \mid a_i$ for $0 \leq i < n$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Q}[x]$.

Example 2.70. The polynomial $x^5 + 3x^4 - 6x^3 + 12x + 3$ is irreducible in $\mathbb{Q}[x]$ by the Einstein's Criterion using $p = 3$.

2.8 Field Extensions

2.8.1 Definition of Field Extensions

Definition 2.71. Let E, F be fields, then F is said to be a **subfield** if F is a subring of E. In this case, E is an extension of F, or E/F is a **field extension**.

Note that E/F does not mean a quotient ring. Further let α be an element of E, then consider the evaluation map

$$\phi_\alpha : F[x] \to E, f \mapsto f(\alpha)$$

which is a homomorphism such that $\phi_\alpha \mid_F = \mathrm{id}_F$. The image of ϕ_α is the subring

$$F[\alpha] := \mathrm{im}\phi_\alpha = \{f(\alpha) \mid f \in F[x]\}$$

in E. Since E is a field, $F[\alpha]$ is an integral domain. Also, the subfield

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in F[x], g(\alpha) \neq 0 \right\}$$

in E is precisely the field of fractions of $F[\alpha]$. There are two scenarios:

(1) $\ker \phi_\alpha = \{0\}$, which means α is not a root of any nonzero polynomial $f \in F[x]$. In this case, $\alpha \in E$ is **transcendental** over F. Then ϕ_α gives an isomorphism $F[x] \cong F[\alpha]$.

(2) $\ker \phi_\alpha \neq \{0\}$, which means α is a root of some nonzero polynomial $f \in F[x]$. In this case, $\alpha \in E$ is **algebraic** over F. Since $F[x]$ is a principal ideal domain, $\ker \phi_\alpha = (p)$ for some $p \in F[x]$. By the First Isomorphism Theorem,

$$\overline{\phi_\alpha} : F[x]/(p) \cong F[\alpha]$$

Since $F[\alpha]$ is an integral domain, p is irreducible and $\overline{\phi_\alpha}$ is a field. Therefore $\overline{\phi_\alpha} = F(\alpha)$ where $F(\alpha)$ is the smallest subfield of E containing F and α. $F(\alpha)$ is said to be obtained from F by **adjoining** α.

Theorem 2.72. Let E/F be a field extension and α be an element of E, then the following applies:

(a) If α is algebraic over F, then α is a root of an irreducible polynomial $p \in F[x]$, such that $p \mid f$ for any $f \in F[x]$ with $f(\alpha) = 0$.

(b) For p be an irreducible polynomial $F[x]$ of which α is a root, then the map $\overline{\phi_\alpha} : F[x]/(p) \to F(\alpha)$ is defined by

$$\phi\left(\sum_{i=0}^{n} c_i x^i + (p)\right) = \sum_{i=0}^{n} c_i \alpha^i$$

which is also a ring homomorphism mapping $x + (p)$ to α and $a + (p)$ to a for any $a \in F$.

(c) Let p be an irreducible polynomial in $F[x]$ of which α is a root. Then, each element in $F(\alpha)$ has a unique expression of the form

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

where $c_i \in F$ and $n = \deg(p)$.

(d) If $\alpha, \beta \in E$ are both roots of an irreducible polynomial $p \in F[x]$, then there exists a ring homomorphism $\rho : F(\alpha) \to F(\beta)$ with $\rho(\alpha) = \beta$ and $\rho(s) = s$ for all $s \in F$.

2.8.2 Finite Fields

Below is the **Kronecker's Theorem**:

Theorem 2.73. Let F be a field, and f be a nonconstant polynomial in $F[x]$, then there exists a field extension E of F, such that $f \in F[x] \subset E[x]$ is a product of linear polynomials in $E[x]$. In other words, there exists a field extension E of F such that

$$f = c(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

for some $c, \alpha_i \in E$.

Definition 2.74. Let D be an integral domain, then the **characteristic** of D, denoted by $\text{char}(D)$ is the smallest positive integer n such that the sum of 1 n times is 0. If the integer does not exist, D has **characteristic zero**.

Proposition 2.75. Let F be a finite field, then the number of elements of F is equal to p^n for some prime p and $n \in \mathbb{N}$.

Proof. Since F is finite, it has finite characteristic, and since F is a field, $\text{char}(F)$ must be a prime p.

With the proposition, below is the **Galois' Theorem**:

Theorem 2.76. Given any prime p and $n \in \mathbb{N}$, there exists a finite field F with p^n elements.

Proposition 2.77. Let F be a field, and f be a nonzero irreducible polynomial in $F[x]$, then $F[x]/(f)$ is a vector space of dimension $\deg(f)$ over F.

Corollary. If F is a finite field with $|F|$ elements, and f is a irreducible polynomial of degree n in $F[x]$, then the field $F[x]/(f)$ has $|F|^n$ elements.

References

The following are the references of the context of this document:

(a) Professor(s) associated to *MATH2070: Algebraic Structures*

(b) Michael Artin, *Algebra*, Pearson (2nd Edition), 2010.

(c) John B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley (7th Edition), 2003.