MATH 417

Wenxiao Yang*

*Department of Mathematics, University of Illinois at Urbana-Champaign

2021

Contents

1 Function and Set

1.1 Function

$A \times B = \{(a, b) | a \in A, b \in B\}$.
Function is a rule σ that assigns an element B to *every* element of A.

$$\sigma : A \to B$$
$$\forall a \in A, \sigma(a) \in B.$$
$$\sigma(a) = \textit{value of } \sigma \textit{ at } a. \textit{ (the } \underline{\textit{image}} \textit{ of } a)$$

A set $C \subset B$, we call $\sigma^{-1}(C) = \{a \in A | \sigma(a) \in C\}$ as the *preimage* of a.
An element $b \in B$, we call $\sigma^{-1}(b) = \{a \in A | \sigma(a) = b\}$ as the *fiber* of b.
A is the domain of σ, B is the range of σ.

1.1.1 Composition of functions

$\sigma : A \to B, \tau : B \to C$. The function $\tau \circ \sigma : A \to C$ is $\forall a \in A,\ (\tau \circ \sigma)(a) = \tau(\sigma(a))$

1.1.2 Proposition 1.1.3: Associativity of Functions

Proposition 1 (Proposition 1.1.3). *$\sigma : A \to B, \tau : B \to C, \rho : C \to D$ functions then,*

$$\rho \circ (\tau \circ \sigma) = (\rho \circ \tau) \circ \sigma$$

1.1.3 Injective, surjective, bijective

A function $\sigma : A \to B$ is called,
1. *Injective (1 to 1)*

$$\forall a_1, a_2 \in A, \sigma(a_1) = \sigma(a_2) \Rightarrow a_1 = a_2$$

2. *Surjective (onto)*

$$\forall b \in B, \exists a \in A, s.t. \sigma(a) = b$$

3. *Bijective* (if injective and surjective)

1.1.4 Lemma 1.1.7: injective/surjective/bijective is preserved in composition

Lemma 1 (Lemma 1.1.7). *Suppose $\sigma : A \to B, \tau : B \to C$ are functions,*
If σ, τ are injective, then $\tau \circ \sigma$ is injective.
If σ, τ are surjective, then $\tau \circ \sigma$ is surjective.
If σ, τ are bijective, then $\tau \circ \sigma$ is bijective.

1.1.5 Proposition 1.1.8: Inverse of Function

Proposition 2 (Proposition 1.1.8). *A function $\sigma : A \to B$ is a bijection if*
$\exists$ a function $\tau : B \to A$ such that

$$\sigma \circ \tau = id_B = \textit{identity on } B (id_B(x) = x, \forall x \in B)$$
$$\tau \circ \sigma = id_A$$

Such τ is unique, called inverse of σ, $\tau = \sigma^{-1}$.

1.2 Set

1.2.1 Well Defined Set

Definition 1. *A set S is **well defined** if an object a is either $a \in S$ or $a \notin S$.*

1.2.2 Power Set

Definition 2. *For any set A, we denote by $\mathcal{P}(A)$ the collection of all subsets of A. $\mathcal{P}(A)$ is the **power set** of A.*

1.2.3 Cardinalities of Sets, Pigeonhole Principle

Definition 3. *If A is a set, $|A| =$ cardinality of $A = \#$ of elements*

$n \in \mathbb{N}, |\{1, \ldots n\}| = n$; $|\emptyset| = 0(\emptyset =$ empty set $)$.
$|A| = |B|$ if there is a bijection $\sigma : A \to B$.
If there is an *injection* $\sigma : A \to B$, we can write $|A| \leq |B|$;
If there is a *surjection* $\sigma : A \to B$, we can write $|A| \geq |B|$.

Theorem 1 (Pigeonhole Principle)**.** *If A and B are sets and $|A| > |B|$, then there is no injective function $\sigma : A \to B$.*

1.2.4 B^A: Sets of Function

If A, B are sets, then $B^A = \{\sigma : A \to B | \sigma \text{ a function}\}$.

Example 1. *$n \in \mathbb{Z}$, we define a function $f : B^{\{1,\ldots,n\}} \to B^n (= B \times B \times B \times \cdots \times B)$ by the equation $f(\sigma) = \{\sigma(1), ..., \sigma(n)\}$, where $\sigma : \{1, \ldots, n\} \to B$. The f is a bijection.*

Proof.
1. *Injective*:

$$f(\sigma_1) = f(\sigma_2) \Rightarrow \{\sigma_1(1), ..., \sigma_1(n)\} = \{\sigma_2(1), ..., \sigma_2(n)\}$$
$$\text{Since } \sigma : \{1, \ldots, n\} \to B, \text{ it is sufficient to prove } \sigma_1 = \sigma_2.$$

2. *Surjective*:

$$\forall \{b_1, ..., b_n\}, \text{ we have } \sigma^*(x) = b_x, x = 1, ..., n. \text{ s.t. } f(\sigma^*) = \{b_1, ..., b_n\}$$

□

Example 2.

$$C(\mathbb{R}, \mathbb{R}) = \{\text{continuous functions } \sigma : \mathbb{R} \to \mathbb{R}\} \subset \mathbb{R}^{\mathbb{R}}$$

1.2.5 Operation definitions

Definition 4. *A <u>binary operation</u> on a set A is a function $* : A \times A \to A$.*
The <u>operation is associative</u> if $a * (b * c) = (a * b) * c, \forall a, b, c \in A$.
The <u>operation is commutative</u> if $a * b = b * a, \forall a, b \in A$.

Example 3. *$+, \circ$ are both associative and commutative operations on $\mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{R}$; $-$ is a neither associative nor commutative operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, but not $\mathbb{N}$.*

Definition 5. *A subset $H \subset S$ is <u>closed under $*$</u> if $a * b \in H$ for all $a, b \in H$.*

Definition 6. *$*$ has <u>identity element $e \in S$</u> if $a * e = e * a = a$ for all $s \in S$.*

2 Equivalence relations and Partition

2.1 Equivalence relations (rational equivalence in micro)

rational equivalence in micro Satisfy: (1)Reflexive, (2)Symmetric, (3)Transitive. Given a set X, a relation on X is a subset of $R \subset X \times X$. We write $a \sim b$.
A relation $\sim$ is said to be
1. *Reflexive* if $\forall x \in X$, we have $x \sim x$.
2. *Symmetric* if $\forall x, y \in X$, $x \sim y \Rightarrow y \sim x$.
3. *Transitive* if $\forall x, y, z \in X$, $x \sim y, y \sim z \Rightarrow x \sim z$.
The *sim* is called **equivalence relation** if it is *reflexive, Symmetric* and *Transitive.*

Example 4. *Set* $X = \{(a, b) \in \mathbb{Z}^2 | b \neq 0\}$*, satisfies* $(a, b) \sim (c, d)$ *if* $ad = bc$.

1. *Reflexive*: $(a, b) \sim (a, b), \forall (a, b) \in \mathbb{Z}^2$.
2. *Symmetric*: $\forall (a, b), (c, d) \in \mathbb{Z}^2, (a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$.
3. *Transitive*: $\forall (a, b), (c, d), (u, v) \in \mathbb{Z}^2, (a, b) \sim (c, d), (c, d) \sim (u, v) \Rightarrow ad = bc, cv = du \Rightarrow acv = adu = bcu \Rightarrow av = bu \Rightarrow (a, b) \sim (u, v)$.
So this is an equivalence relation.

Example 5. $f : X \to Y$ *is a function, define* $\sim_f$ *on* X *by* $a \sim_f b$ *if* $f(a) = f(b)$.

1. *Reflexive*: $a \sim a, \forall a \in X$.
2. *Symmetric*: $a, b \in X, a \sim b \Rightarrow b \sim a$.
3. *Transitive*: $\forall a, b, c \in X, a \sim b, b \sim c \Rightarrow f(a) = f(b) = f(c) \Rightarrow a \sim c$.
So $\sim_f$ is an equivalence relation.

2.2 Partition (separate a set into disjoint sets with no element left)

X a set, a partition of X is a collection ω of subsets of X s.t.

1) $\forall A, B \in \omega$ either $A = B$ or $A \cap B = \emptyset$.

2) $\cup_{A \in \omega} A = X$.

The subsets are the **cell**s of partition.

2.3 Equivalence class

2.3.1 $[x]$: equivalence class

Define the **equivalence class** of x to be the subset $[x] \subset X$:

$$[x] = \{y \in X | y \sim x\}$$

Where $\sim$ is an equivalence relation.
$\sim$ is reflexive $\Rightarrow x \in [x]$. We say that any $y \in [x]$ as a **representative** of the equivalence class.

2.3.2 $X/\sim$: set of equivalence classes

Set of equivalence classes is a **set** of division result of an *equivalence relation*
We write the set of equivalence classes

$$X/\sim = \{[x] | x \in X\}$$

2.4 Relationship of ***Equivalence relation***, ***Set of equivalence classes*** and ***Partitions***

2.4.1 Theorem 1.2.7: Equivalence relation $\sim \Leftrightarrow$ Set of equivalence classes $X/\sim$; $\{$all Sets of equivalence classes$\}$ = $\{$all Partitions$\}$

Theorem 2 (Theorem 1.2.7)**.** *$X/\sim$ is a partition of X. Conversely, given a partition ω of X, there exists a unique equivalence relation $\sim_\omega$ s.t. $X/\sim_\omega = \omega$.*

Proof.
(1)$X/\sim$ is a partition of X:

$$\begin{aligned}
&\forall x, y \in X \ s.t. \ [x] \cap [y] \neq \emptyset \\
&Let \ z \in [x] \cap [y] \Rightarrow z \sim x, z \sim y \\
&\forall w \in [x] \Rightarrow w \sim x \Rightarrow x \sim w \Rightarrow z \sim w \Rightarrow w \sim z \Rightarrow w \sim y \Rightarrow [x] \subset [y] \\
&Similarly \ we \ can \ prove \ [y] \subset [x] \Rightarrow [x] = [y]
\end{aligned}$$

(2)Given a partition ω of X, there exists a unique equivalence relation $\sim_\omega$ s.t. $X/\sim_\omega = \omega$:
(2.1) Prove there exists an equivalence relation s.t. $X/\sim_\omega = \omega$:
We define a relation: $x \sim_\omega y$ if there exists $A \in \omega$ s.t. $x, y \in A \Rightarrow \sim_\omega$ is symmetric and transitive. Since $\cup_{A\in\omega} A = X$, we know $\forall x \in X, \exists A \in \omega \ s.t. \ x \in A \Rightarrow \sim_\omega$ is reflexive. So $\sim_\omega$ is an equivalence relation.
We know $A = [x], \forall A \in \omega, \forall x \in A$ (by $\sim_\omega$), then $X/\sim_\omega = \{[x] | x \in \cup_{A\in\omega} A\} = \{\{A^* | x \in A^*\} | A^* \in \omega\} = \omega$.
(2.2) Prove the equivalence relation is unique:
Set $\sim$ be any equivalence relation that make $X/\sim = \omega$, then we know $\forall A \in \omega, \exists x \in X$ s.t. $[x] = A$. According to the definition of $[x]$, if $x \in A$, $y \sim x$ if and only if $y \in [x] = A$. Which is exactly the $\sim_\omega$. ☐

Example 6 (the same as example 5)**.** *$f : X \to Y$ is a function, define $\sim_f$ on X by $a \sim_f b$ if $f(a) = f(b)$. In this example the* ***equivalence classes*** *are precisely the fibers $[x] = f^{-1}(f(x))$. $y \sim_f x \Rightarrow y \in f^{-1}(f(x))$*

Example 7 (the same as example 4)**.** *Set $X = \{(a, b) \in \mathbb{Z}^2 | b \neq 0\}$, satisfies $(a, b) \sim (c, d)$ if $ad = bc$. i.e. we write the equivalence of (a, b) as $\frac{a}{b} = [(a, b)]$. Then $X/\sim = \mathbb{Q}$.*

2.4.2 Proposition 1.2.12: use $X/\sim = \{[x]|x \in X\}$ to infer $\sim_\pi$ equals to $\sim$.

Proposition 3 (Proposition 1.2.12)**.** *If $\sim$ is an equivalence relation on X, define a surjective function $\pi : X \to X/\sim$ by $\pi(x) = [x]$. Then $\sim_\pi = \sim$(the definition of $\sim_f$ in example 6.)*

Proof.
(1)Surjective:
$X/\sim = \{[x]|x \in X\} = \{\pi(x)|x \in X\}$, so $\forall y \in X/\sim$, $y \in \{\pi(x)|x \in X\}$, there exists $x \in X$ s.t. $\pi(x) = y$.
(2)$\sim_\pi = \sim$
$a \sim_\pi b$ if $\pi(a) = \pi(b) \Leftrightarrow [a] = [b]$, which is exactly the definition of $\sim$. ☐

1. Given $\sim$;
2. Get the corresponding $X/\sim = \{[x]|x \in X\}$;
3. $\pi(x) = [x]$;
4. $\sim_\pi$: $a \sim_\pi b$ iff $\pi(a) = \pi(b)$
5. $\sim_\pi = \sim$

Proposition 4 (Proposition 1.2.13). *Given any function $f : X \to Y$ there exists a unique function $\tilde{f} : X/\sim \to Y$ such that $\tilde{f} \circ \pi = f$, where $\pi : X \to X/\sim$ in proposition 3. Furthermore, $\tilde{f}$ is a bijection onto the image $f(X)$.*

Proof.
(1) Existence:
We define $x_1 \sim_f x_2$ if $f(x_1) = f(x_2)$. Set $\tilde{f} : X/\sim_f \to Y$, $\tilde{f}([x]) = f(x)$. Then $\tilde{f}[\pi(x)] = \tilde{f}([x]) = f(x)$. Exactly what we require.
(2) Uniqueness:
Set any $\tilde{f}'$ s.t. $\tilde{f}' \circ \pi = f$, then $\tilde{f}'[\pi(x)] = \tilde{f}'([x]) = f(x)$, i.e. the $\tilde{f}$ is unique.
(3) Bijection:
Surjective, which we proved before $\forall f, \exists \tilde{f}$ s.t.$\tilde{f} \circ \pi = f$;
Injective, we also have proved the uniqueness $f = \tilde{f} \circ \pi = \tilde{f}' \circ \pi \Rightarrow \tilde{f}' = \tilde{f}$. □

3 Permutations

Definition 7. *Let X be a finite set, a permutation is bijection $\sigma : X \to X$.*

Definition 8. *Let S_X $(Sym(X))$ be the set of all bijection $\sigma : X \to X$.*

If $|X| = n$, $|S_X| = n!$.

3.1 $Sym(X) = \{\sigma : X \to X | \sigma$ *is a bijection*$\}$: permutation group of X; elements in $Sym(X)$: permutations of X

We set $Sym(X) = \{\sigma : X \to X | \sigma \text{ is a bijection}\} \subset X^X$. We call it **symmetric group of X** or **permutation group of X**. We call the elements in $Sym(X)$ the **permutations of X** or the **symmetries of X**.

3.1.1 Properties of $\circ$ on $Sym(X)$

Proposition 5 (Proposition 1.3.1.). *For any nonempty set X, $\circ$ is an operation on $Sym(X)$ with the following properties:*
(i) $\circ$ is associative.
(ii) $id_X \in Sym(X)$, and for all $\sigma \in Sym(X)$, $id_X \circ \sigma = \sigma \circ id_X = \sigma$, and
(iii) For all $\sigma \in Sym(X)$, $\sigma^{-1} \in Sym(X)$.

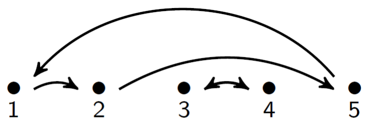
3.1.2 S_n: Permutation group on n elements, σ^i

Note 1. *When $X = \{1, ..., n\}, n \in \mathbb{Z}$, write $S_n = Sym(X)$ **symmetric/permutation group on n elements**.*

Note 2. *$\sigma \in Sym(X)$, write $\sigma^n = \sigma \circ \sigma \circ ... \circ \sigma$, $\sigma^0 = id_X$, $\sigma^{-1} = inverse$, $r > 0, \sigma^{-r} = (\sigma^{-1})^r$. So, $r, s \in \mathbb{Z}, \sigma^{r+s} = \sigma^r \circ \sigma^s = \sigma^s \circ \sigma^r$.*

3.1.3 k-cycle, cyclically permute/fix

Example 8.

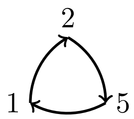


$$1 \overset{\sigma}{\mapsto} 2 \overset{\sigma}{\mapsto} 5 \overset{\sigma}{\mapsto} 1, \quad \tau_1$$

$$3 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 3, \quad \tau_2$$

Figure 1: Example of Cycle

In the example of *Figure 1*, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$, $\sigma = \tau_1 \circ \tau_2$, where $\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$. τ_1 is 3-cycle, τ_2 is 2-cycle. We could represent $\tau_1 = (1\ 5\ 2) = (5\ 2\ 1) = (2\ 1\ 5)$,

i.e. 

Similarly, we can represent $\tau_2 = (3, 4) = (4, 3)$, i.e. $3 \longleftrightarrow 4$

We can find that $\forall x \in \{1, 2, 3, 4, 5\}$, $\tau_1^3(x) = x, \tau_2^2(x) = x$, so we write τ_1 as a **3-cycle** in S_5, τ_2 as a **2-cycle** in S_5.

Given $k \geq 2$, a **k-cycle** in S_n is a permutation σ with the property that $\{1, ..., n\}$ is the union of two disjoint subsets, $\{1, ..., n\} = Y \cup Z$ and $Y \cap Z = \emptyset$, such that
1. $\sigma(x) = x$ for every $x \in Z$, and
2. $|Y| = k$, and for any$x \in Y$,$Y = \{\sigma(x), \sigma^2(x), \sigma^3(x) ... \sigma^k(x) = x\}$.

We say that σ **cyclically permutes** the elements of Y and **fixes** the elements of Z.
$\tau_1 = (1\ 2\ 5)$ **cyclically permutes** the elements of $Y = \{1, 2, 5\}$ and **fixes** the elements of $Z = \{3, 4\}$.
$\tau_2 = (3\ 4)$ **cyclically permutes** the elements of $Y = \{3, 4\}$ and **fixes** the elements of $Z = \{1, 2, 5\}$.

3.2 Disjoint cycles

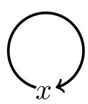
Since the sets are cyclically permuted by τ_1, τ_2 (i.e.Y) are disjoint. We call the **disjoint cycle notation** $\sigma = \tau_1 \circ \tau_2 = (1\ 2\ 5)(3\ 4)$. (Commute the order is irrelevant)

3.2.1 Theorem: Every permutation is a union of disjoint cycles, uniquely.

Given $\sigma \in S_n$, there exists a unique (possibly empty) set of pairwise disjoint cycles.

Theorem 3. *Let X be a finite set, the graph of permutation $\sigma \in S_X$ is a union of disjoint cycle.*

Proof. Prove by induction:

If $|X| = 1$, the graph is circle: 

For $|X| > 1$, let $i_1 \in X$ and let $\mathcal{O}(i_1) = \{\sigma^r(i_1), r \geq 0\} = \{i_1, \sigma(i_1), \sigma^2(i_1), ...\}$. $\mathcal{O}(i_1)$ is finite, and there is a smallest r s.t. $\sigma^r(i_1) \in \{i_1, \sigma(i_1), \sigma^2(i_1), ..., \sigma^{r-1}(i_1)\}$. Then $\sigma^r(i_1) = i_1$ because other elements already have a pre-change under σ.

Then $i_1 \to \sigma(i_1) \to \sigma^2(i_1) \to \cdots \to \sigma^{r-1}(i_1) \to i_1$ is a cycle of length r.
For $j \notin \mathcal{O}(i_1), \sigma(j) \notin \mathcal{O}(i_1), \sigma^{-1}(j) \notin \mathcal{O}(i_1)$. Let $Y = X/\mathcal{O}(i_1)$ then $\sigma : Y \to Y$ is a bijection. Then prove by induction.

□

Example 9. $\sigma_1 = (1\ 2\ 6\ 5)(3)(4)$, *can be written by* $\sigma_1 = (1\ 2\ 6\ 5)$, $\sigma_2 = (2\ 3\ 5\ 4)$

$\sigma_1 \circ \sigma_2 = (1\ 2\ 6\ 5) \circ (2\ 3\ 5\ 4)$

$$1 \xrightarrow{(2\ 3\ 5\ 4)} 1 \xrightarrow{(1\ 2\ 6\ 5)} 2$$
$$2 \xrightarrow{(2\ 3\ 5\ 4)} 3 \xrightarrow{(1\ 2\ 6\ 5)} 3$$
$$3 \xrightarrow{(2\ 3\ 5\ 4)} 5 \xrightarrow{(1\ 2\ 6\ 5)} 1$$
$$4 \xrightarrow{(2\ 3\ 5\ 4)} 2 \xrightarrow{(1\ 2\ 6\ 5)} 6$$
$$5 \xrightarrow{(2\ 3\ 5\ 4)} 4 \xrightarrow{(1\ 2\ 6\ 5)} 4$$
$$6 \xrightarrow{(2\ 3\ 5\ 4)} 6 \xrightarrow{(1\ 2\ 6\ 5)} 5$$

Then $\sigma_1 \circ \sigma_2 = (1\ 2\ 3) \circ (4\ 6\ 5)$
$\sigma_2 \circ \sigma_1 = (2\ 3\ 5\ 4) \circ (1\ 2\ 6\ 5)$

$$1 \xrightarrow{(1\ 2\ 6\ 5)} 2 \xrightarrow{(2\ 3\ 5\ 4)} 3$$
$$2 \xrightarrow{(1\ 2\ 6\ 5)} 6 \xrightarrow{(2\ 3\ 5\ 4)} 6$$
$$3 \xrightarrow{(1\ 2\ 6\ 5)} 3 \xrightarrow{(2\ 3\ 5\ 4)} 5$$
$$4 \xrightarrow{(1\ 2\ 6\ 5)} 4 \xrightarrow{(2\ 3\ 5\ 4)} 2$$
$$5 \xrightarrow{(1\ 2\ 6\ 5)} 1 \xrightarrow{(2\ 3\ 5\ 4)} 1$$
$$6 \xrightarrow{(1\ 2\ 6\ 5)} 5 \xrightarrow{(2\ 3\ 5\ 4)} 4$$

Then $\sigma_2 \circ \sigma_1 = (1\ 3\ 5) \circ (2\ 6\ 4)$
Note: $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$

Example 10 (Exercise 1.3.2.)**.** *Consider* $\sigma = (3\ 4\ 8)(5\ 7\ 6\ 9)$ *and* $\tau = (1\ 9\ 3\ 5)(2\ 7\ 4)$ *in* S_9 *expressed in disjoint cycle notation. Compute* $\sigma \circ \tau$ *and* $\tau \circ \sigma$ *expressing both in disjoint cycle notation.*

$$\begin{aligned}
&1 \to \sigma(\tau(1)) = \sigma(9) = 5;\ 2 \to \sigma(\tau(2)) = \sigma(7) = 6;\\
&3 \to \sigma(\tau(3)) = \sigma(5) = 7;\ 4 \to \sigma(\tau(4)) = \sigma(2) = 2;\\
&5 \to \sigma(\tau(5)) = \sigma(1) = 1;\ 6 \to \sigma(\tau(6)) = \sigma(6) = 9;\\
&7 \to \sigma(\tau(7)) = \sigma(4) = 8;\ 8 \to \sigma(\tau(8)) = \sigma(8) = 3;\\
&9 \to \sigma(\tau(9)) = \sigma(3) = 4;\\
\Rightarrow &\sigma \circ \tau = (1\ 5)(2\ 6\ 9\ 4)(3\ 7\ 8)
\end{aligned}$$

$$\begin{aligned}
&1 \to \tau(\sigma(1)) = \tau(1) = 9;\ 2 \to \tau(\sigma(2)) = \tau(2) = 7;\\
&3 \to \tau(\sigma(3)) = \tau(4) = 2;\ 4 \to \tau(\sigma(4)) = \tau(8) = 8;\\
&5 \to \tau(\sigma(5)) = \tau(7) = 4;\ 6 \to \tau(\sigma(6)) = \tau(9) = 3;\\
&7 \to \tau(\sigma(7)) = \tau(6) = 6;\ 8 \to \tau(\sigma(8)) = \tau(3) = 5;\\
&9 \to \tau(\sigma(9)) = \tau(5) = 1;\\
\Rightarrow &\tau \circ \sigma = (1\ 9)(2\ 7\ 6\ 3)(4\ 8\ 5)
\end{aligned}$$

Example 11. *Let $\sigma, \tau \in S_7$, given in disjoint cycle, notation by $\sigma = (1\ 5\ 4)(3\ 7), \tau = (1\ 3\ 2\ 6\ 4)$, Compute $\sigma^2, \sigma^{-1}, \tau \circ \sigma$*

$$\begin{aligned}
\sigma^2 &= (1\ 4\ 5), & \sigma^{-1} &= (4,5,1)(3,7),\\
1 &\to \tau(\sigma(1)) = \tau(5) = 5, & 2 &\to \tau(\sigma(2)) = \tau(2) = 6,\\
3 &\to \tau(\sigma(3)) = \tau(7) = 7, & 4 &\to \tau(\sigma(4)) = \tau(1) = 3,\\
5 &\to \tau(\sigma(5)) = \tau(4) = 1, & 6 &\to \tau(\sigma(6)) = \tau(6) = 4,\\
7 &\to \tau(\sigma(7)) = \tau(3) = 2, & &\\
\Rightarrow \tau \circ \sigma &= (1,5)(2,6,4,3,7) & &
\end{aligned}$$

3.2.2 Cycle Structure

- How many permutation $\sigma \in S_{12}$ has cycle structure $(1\ 2\ 3)(4\ 5\ 6)(7\ 8)(9\ 10)(11\ 12)$?

$$\frac{12!}{3^2 2^3 (2!)(3!)}$$

  12!: Arrange 12 elements in 12 slots.

  3^2: Every cycle with 3 element has 3 forms to represent a same permutation.

  2^3: Every cycle with 2 element has 2 forms to represent a same permutation.

  (2!): Due to the communicative of disjoint permutation, the arrange of cycles with three elements is 2! need to be divided.

  (3!): Due to the communicative of disjoint permutation, the arrange of cycles with two elements is 3! need to be divided.

- $(1\ 2\ 3)(4\ 5)(6) \in S_6$?

$$\frac{6!}{3 \times 2} = 120$$

- General situation: $\sigma \in S_n$, r_i category of length i, $i = 1, 2...$

$$\frac{n!}{[1^{r_1} 2^{r_2} 3^{r_3} \cdots][(r_1!)(r_2!)(r_3!) \cdots]}$$

3.3 Transposition

Definition 9. *A **transposition** is a cycle of length 2: $\sigma = (i\ j)$.*

3.3.1 Theorem: Every permutation can be represented by a product of transpositions (not require to be disjoint)

Theorem 4. *Every permutation σ of X is a product of transposition. (the product is not unique)*
Equivalent: *Given $n \geq 2$, any $\sigma \in S_n$ can be expressed as a composition of 2-cycles.(not require disjoint)*

Proof.

Version 1:

$$\begin{aligned}(x_1\ x_k)(x_1\ x_2, ...\ x_{k-1}\ x_k) &= (x_1\ x_2\ ...\ x_{k-1})\\ (x_1\ x_2\ ...\ x_{k-1}\ x_k) &= (x_1\ x_k)(x_1, x_2\ ...\ x_{k-1})\\ &= (\mathbf{x_1\ x_k})(\mathbf{x_1\ x_{k-1}})(\mathbf{x_1\ x_2\ ...\ x_{k-2}})\\ &\dots\\ &= (\mathbf{x_1\ x_k})(\mathbf{x_1\ x_{k-1}})(\mathbf{x_1\ x_{k-2}})\dots(\mathbf{x_1\ x_2})\end{aligned}$$

Version 2:

$$\begin{aligned}(x_1\ x_2, ...\ x_{k-1}\ x_k)(x_1\ x_k) &= (x_2\ x_3\ ...\ x_k)\\ (x_1\ x_2\ ...\ x_{k-1}\ x_k) &= (x_2\ x_3\ ...\ x_k)(x_1\ x_k)\\ &\dots\\ &= (\mathbf{x_{k-1}\ x_k})(\mathbf{x_{k-2}\ x_k})\dots(\mathbf{x_2\ x_k})(\mathbf{x_1\ x_k})\end{aligned}$$

□

Claim 1. *Cycle of length k can be written as a product of $k-1$ transpositions.*

3.3.2 Sign of Permutation

Theorem 5. *Although the product of transposition of a permutation is not unique, the parity (odd or even) of the n in a product is unique. We call it the **sign** of permutation.*

$$\begin{aligned}sign(\sigma) &= (-1)^{(\#\ \text{even-length cycles in } \sigma)}\\ &= (-1)^{(\#\ \text{transpositions in } \sigma)}\end{aligned}$$

Example 12.
$\sigma_1 = (1\ 4\ 7\ 9)(2\ 8)(6\ 10)$: $N = 3+1+1 = 5$ *is odd.*
$\sigma_2 = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$: $N = 4+4 = 8$ *is even*

What happens to a permutation σ's cycles if $\sigma \to (i\ j)\circ\sigma$?
1. i and j are not contained in σ.
2. i and j appear in the same cycle of σ.
3. i and j appear in disjoint cycles.

$$\begin{aligned}(i\ j)\circ(i - -j \sim\sim) &= (i - -)\circ(j \sim\sim)\\ (i\ j)\circ(i - -)\circ(j \sim\sim) &= (i - -j \sim\sim)\end{aligned}$$

Proposition 6. $sign((i\ j)\circ\sigma) = -1\cdot sign(\sigma)$

Proof.

Suppose $\sigma = (a_1\ a_2\ \cdots a_k\ b_1\ b_2\ \cdots b_l)$
Then $(a_1\ b_1)\circ\sigma = (a_1\ a_2\ \cdots a_k)(b_1\ b_2\ \cdots b_l)$

$$sign(\sigma) = \begin{cases}+1 & \text{if } k+l \text{ is odd}\\ -1 & \text{if } k+l \text{ is even}\end{cases}$$

$$sign((a_1\ b_1)\circ\sigma) = \begin{cases}-1 & \text{if } k+l \text{ is odd}\\ +1 & \text{if } k+l \text{ is even}\end{cases}$$

□

4 Integers

4.1 Proposition 1.4.1: Properties of integers $\mathbb{Z}$

Proposition 7 (Proposition 1.4.1.). *The following hold in the integers $\mathbb{Z}$:*

(i) *Addition* and *multiplication* are *commutative* and *associative* operations in $\mathbb{Z}$.
(ii) $0 \in \mathbb{Z}$ is an identity element for addition; that is, $\forall a \in \mathbb{Z}, 0 + a = a$.
(iii) Every $a \in \mathbb{Z}$ has an additive inverse, denoted $-a$ and given by $-a = (-1)a$, satisfying $a+(-a) = 0$.
(iv) $1 \in \mathbb{Z}$ is an identity element for multiplication; that is, for all $a \in \mathbb{Z}$, $1a = a$.
(v) The *distributive* law holds: $\forall a, b, c \in \mathbb{Z}, a(b + c) = ab + ac$.
(vi) Both $\mathbb{N} = \{x \in Z | x \geq 0\}$ and $\mathbb{Z}_+ = \{x \in \mathbb{Z} | x > 0\}$ are *closed* under *addition* and *multiplication*. That is, if x and y are in one of these sets, then $x + y$ and xy are also in that set.
(vii) For any two nonzero integers $a, b \in \mathbb{Z}, |ab| \geq \max\{|a|, |b|\}$. Strict inequality holds if $|a| > 1$ and $|b| > 1$.

From this we get cancellation.

$$ab = ac \Rightarrow b = c \text{ or } a = 0$$

4.2 Definition: Divide

Suppose $a, b \in \mathbb{Z}, b \neq 0$, <u>b divides a</u> if $\exists m \in \mathbb{Z}$, so that $a = bm, b|a$. Otherwise, write $b \nmid a$.

4.3 Proposition 1.4.2: properties of integer division

Proposition 8 (Proposition 1.4.2). $\forall a, b \in \mathbb{Z}$

(i) if $a \neq 0$, then $a|0$
(ii) if $a|1$, then $a = \pm 1$
(iii) if $a|b$ & $b|a$, then $a = \pm b$
(iv) if $a|b$ & $b|c$, then $a|c$
(v) if $a|b$ & $a|c$, then $a|(mc + nb) \forall m, n \in \mathbb{Z}$

4.4 Definitions: Prime, The Greatest common divisor $gcd(a, b)$

$p > 1, p \in \mathbb{Z}$ is called <u>*prime*</u> if the only divisors are $\pm 1, \pm p$.
Given $a, b \in \mathbb{Z}, a, b \neq 0$, the <u>*greatest common divisor*</u> of a and b is $c \in \mathbb{Z}, c > 0$ s.t.
(1) $c|a$ and $c|b$; (2) if $d|a, d|b$, then $d|c$
The c is unique, we write it $gcd(a, b)$.

4.5 Euclidean Algorithm

Proposition 9 (Proposition 1.4.7(Euclidean Algorithm)). *Given $a, b \in \mathbb{Z}, b \neq 0$, then $\exists q, r \in \mathbb{Z}$ s.t. $a = qb + r, 0 \leq r \leq |b|$.*

Example 13 (Exercise 1.4.3). *For the pair $(a, b) = (130, 95)$, find $gcd(a, b)$ using the Euclidean Algorithm and express it in the form $gcd(a, b) = sa + tb$ for $s, t \in Z$.*

$$\begin{aligned} &130 = 95 + 35; \quad 95 = 2 \times 35 + 25 \\ &35 = 25 + 10; \qquad 25 = 2 \times 10 + 5 \\ &10 = 2 \times 5 + 0 \end{aligned}$$

$$5 = 25 - 2 \times 10 = 25 - 2 \times (35 - 25) = 3 \times 25 - 2 \times 35 = 3 \times (95 - 2 \times 35) - 2 \times 35$$
$$= 3 \times 95 - 8 \times 35 = 3 \times 95 - 8 \times (130 - 95) = 11 \times 95 - 8 \times 130$$

$$gcd(130, 95) = gcd(95, 35) = gcd(35, 25) = gcd(25, 10) = gcd(10, 5) = gcd(5, 0) = 5$$

We can also express it by matrix

	q	r	s	t
-1		130	1	0
0	1	95	0	1
1	2	35	1	-1
2	1	25	-2	3
3	2	10	3	-4
4	2	5	-8	11

Hence $gcd(130, 95) = 5 = -8 \cdot 130 + 11 \cdot 95$

4.6 Proposition: $gcd(a, b)$ exists and is the smallest positive integer in the set $M = \{ma + nb | m, n \in \mathbb{Z}\}$

Theorem 6. *$d = gcd(a, b)$ is of the form $sa + tb$*

Proof. We may assume $0 \leq a \leq b$
For $a = 0$, $d = b = 0 \cdot a + 1 \cdot b$.
For $a > 0$, let $b = q \cdot a + r$ with $0 \leq r < a \leq b$. Then

$$\{sa + tb : s, t \in \mathbb{Z}\} = \{sa + t(q \cdot a + r) : s, t \in \mathbb{Z}\} = \{tr + ua : t, u \in \mathbb{Z}\}$$
$$= \ldots \{x \cdot 0 + y \cdot d : x, y \in \mathbb{Z}\} = \{..., -2d, -d, 0, d, 2d, ...\}$$

□

Proposition 10 (second form, second proof)**.** *$\forall a, b \in \mathbb{Z}$, not both 0, $gcd(a, b)$ exists and is the smallest positive integer in the set $M = \{ma + nb | m, n \in \mathbb{Z}\}$. i.e. $\exists m_0, n_0 \in \mathbb{Z}$ s.t. $gcd(a, b) = m_0 a + n_0 b$.*

Proof. Let c be the smallest positive integer in the set $M = \{ma + nb | m, n \in \mathbb{Z}\}$. $c = m_0 a + n_0 b > 0$.
Let $d = ma + nb \in M$, $d = qc + r$ where $0 \leq r < c$ (by Euclidean Algorithm).

$$r = d - qc = (m - qm_0)a + (n - qn_0)b \in M$$

Since c is the smallest integer in M and $r \in [0, c)$, so $r = 0$. $\Rightarrow d = qc$. So $c | d$.
$a = 1a + 0b \in M \Rightarrow c | a$, $b = 0a + 1b \in M \Rightarrow c | b$.
If $t | a, t | b$ then $t | m_0 a + n_0 b$ i.e. $t | c$. $\Rightarrow c = gcd(a, b)$. □

4.7 Well-Ordering Principle (Least Integer Axiom)

There is a smallest integer in every nonempty subset S of the natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$

4.8 Proposition 1.4.10: $gcd(b, c)$, $b | ac \Rightarrow b | a$

Proposition 11 (Proposition 1.4.10)**.** *Suppose $a, b, c \in \mathbb{Z}$. If b, c are relatively prime i.e. $gcd(b, c) = 1$ and $b | ac$, then $b | a$.*

Proof. $gcd(b, c) = 1 \Rightarrow \exists m, n \in \mathbb{Z}$ s.t. $1 = mb + nc \Rightarrow a = amb + anc$. Since $b | nac, b | amb \Rightarrow b | a$. □

4.8.1 Corollary: $p|ab \Rightarrow p|a$ or $p|b$

Corollary 1 (Corollary of Prop 1.4.10)**.** *$a, b, p \in \mathbb{Z}, p > 1$ prime. If $p|ab$, then $p|a$ or $p|b$.*

Proof. If $p|b$, done. Otherwise, $gcd(p, b) = 1$. By Prop 1.4.10, $p|a$. $\square$

4.9 Fundamental Theorem of Arithmetic: Any integer $a \geq 2$ has a unique prime factorization

4.9.1 Existence

Lemma 2. *Any integer $a \geq 2$ is either a prime or a product of primes.*

Proof. Set $S \subset \mathbb{N}$ be the set of all n without the given property.
Assume that S in nonempty and m is the least element in S.
Since m is not a prime, it can be written as $m = ab$ with $1 < a, b < m$. Since m is the least element in S, $a, b \notin S$. Then m is a product of primes. Contradiction. Thus, $S = \emptyset$. $\square$

4.9.2 Uniqueness

Theorem 7 (Fundamental Theorem of Arithmetic)**.**

Any integer $a > 1$ has a unique prime factorization: $a = p_1^{k_1} \cdot p_2^{k_2} \cdot ...p_n^{k_n}$ where $p_i > 1$ is prime, $k_i \in \mathbb{Z}_+, \forall i = 1, ..., n, p_i \neq p_j, \forall i \neq j$.

Proof.

a) Existence: (Previous Lemma)

b) Uniqueness:

1) Method 1:
Suppose $a = p_1^{n_1} \cdot p_2^{n_2} \cdot ...p_k^{n_k} = q_1^{r_1} \cdot q_2^{r_2} \cdot ...q_j^{r_j}$. Where $p_1 > p_2 > ... > p_k, q_1 > q_2 > ... > q_j, n_i, r_i \geq 1$.
$p_1|a \Rightarrow \exists\ q_i$ *s.t.* $p_1|q_i$. Similarly, $\exists\ q_i$ *s.t.* $q_1|p_{i'}$.
$q_1 \leq p_{i'} \leq p_1 \leq q_i \Rightarrow q_1 = p_{i'} = p_1 = q_i$
We can also know $n_1 = r_1$, otherwise we would have two prime factorization of the quotient where the largest primes are different by dividing $p_1^{\min\{n_1, r_1\}}$.
Then we can get $b = p_2^{n_2} \cdot ...p_k^{n_k} = q_2^{r_2} \cdot ...q_j^{r_j}$. Then prove it by induction.

2) Method 2:
Suppose $a = p_1 \cdot p_2 \cdot ...p_k = q_1 \cdot q_2 \cdot ...q_t$. For a p_i, there must exist a q_j s.t. $p_i = q_j$:
Assume that $p_i \neq q_t$, $gcd(p_i, q_t) = 1$. Then $\exists a, b$ such that $1 = ap_i + bq_t$. Multiplying both sides by $q_1 \cdot q_2 \cdot ...q_{t-1}$:

$$q_1 \cdot q_2 \cdot ...q_{t-1} = ap_iq_1 \cdot q_2 \cdot ...q_{t-1} + bq_1 \cdot q_2 \cdot ...q_t$$

Since $p_i|q_1 \cdot q_2 \cdot ...q_t$, we can conclude that $p_i|(ap_iq_1 \cdot q_2 \cdot ...q_{t-1} + bq_1 \cdot q_2 \cdot ...q_t)$

$$\text{i.e. } p_i|q_1 \cdot q_2 \cdot ...q_{t-1} \text{ if } p_i \neq q_t$$

Then prove by induction.

$\square$

5 Modular arithmetic

5.1 Congruences

5.1.1 Congruent modulo m: $a \equiv b$ mod m

Given $m \in \mathbb{Z}_+$, define a relation on $\mathbb{Z}$: **congruence modulo m**

$$a \equiv b \text{ mod } m, \text{ if } m|(a-b)$$

Read as "a is congruent to b mod n"; Notation: $a \equiv b$ mod m.
Equivalent to: a, b have the same remainder after division by m.

5.1.2 Proposition: For fixed $m \geq 2$, the relation "$a \sim b \Leftrightarrow a \equiv b$ mod m" is an equivalence relation

Proposition 12 (Proposition 1.5.1)**.** *For fixed $m \geq 2$, the relation "$a \sim b \Leftrightarrow a \equiv b$ mod m" is an equivalence relation*

Proof.

1) Reflexive: $\forall a \in \mathbb{Z}, m|0 = (a-a)$, so $a \equiv a$ mod m i.e. $a \sim a$.
2) Symmetric: $\forall a, b \in \mathbb{Z}$, $a \equiv b$ mod m, then $m|(a-b) \Rightarrow m|(b-a) \Rightarrow b \equiv a$ mod m. i.e. $a \sim b \Rightarrow b \sim a$.
3) Transitive: $\forall a, b, c \in \mathbb{Z}$, $a \equiv b$ mod m, $b \equiv c$ mod m. Then $m|(a-b), m|(b-c) \Rightarrow m|(a-b)+(b-c) = (a-c) \Rightarrow a \equiv c$ mod m.

□

5.1.3 Theorem: the equivalence relation "$a \sim b \Leftrightarrow a \equiv b$ mod m" partitions the integers into m disjoint sets $\Omega_i = \{a|a \sim i\}, i = 0, 1, ..., m-1$

Theorem 8. *the equivalence relation "$a \sim b \Leftrightarrow a \equiv b$ mod m" partitions the integers into m disjoint sets $\Omega_i = \{a|a \sim i\}, i = 0, 1, ..., m-1$*

Proof. Prove any $a \in \mathbb{Z}$ belongs to a unique Ω_i.

a) Existence: Division Algorithm $\Rightarrow a = qm + r$, $0 \leq r < m$. $a \in \Omega_r$.
b) Uniqueness: Assume a in two sets, $a \in \Omega_r \cap \Omega_{r^1}$, $0 \leq r^1 < r < m$.
   Then $m|a-r$ and $m|a-r^1 \Rightarrow m|r-r^1$, which is impossible because $0 < r-r^1 < m$. Contradiction.

□

5.1.4 Proposition: Addition and Mutiplication of Congruences

Proposition 13. *Fix integer $m \geq 2$. If $a \equiv r$ mod m and $b \equiv s$ mod m, then $a+b \equiv r+s$ mod m and $ab \equiv rs$ mod m*

Proof.

a) Addition: $m|(a-r), m|(b-s) \Rightarrow m|(a-c)+(b-d) \Rightarrow m|(a+b)-(c-d)$.
b) Mutiplication: $m|(a-r)b + r(b-s) \Rightarrow m|ab - rs$.

□

5.2 Solving Linear Equations on Modular m

5.2.1 Theorm: unique solution of $aX \equiv b$ mod m if $gcd(a, m) = 1$

Theorem 9. *If $gcd(a, m) = 1$, then $\forall b \in \mathbb{Z}$ the congruence $aX \equiv b$ mod m has a unique solution.*

Proof.

1) Existence: Since $gcd(a, m) = 1$, $\exists s, t$ such that

$$
\begin{aligned}
1 &= sa + tm \\
&\text{(Version 1)} \\
&\text{(Mutiplying } X\text{)} \\
X &= saX + tmX \\
aX \equiv b \text{ mod } m &\Leftrightarrow aX = km + b \\
&\Leftrightarrow X = s(km + b) + b \\
&\Leftrightarrow X \equiv sb \text{ mod } m \\
&\text{(Version 2)} \\
&\text{(Mutiplying } s\text{)} \\
saX &\equiv sb \text{ mod } m \\
(1 - tm)X &\equiv sb \text{ mod } m \\
X &\equiv sb \text{ mod } m
\end{aligned}
$$

$X \equiv sb$ mod m is the solution to $aX \equiv b$ mod m.

2) Uniqueness: Assume x, y are two solutions,

$$ax \equiv b \text{ mod } , ay \equiv b \text{ mod } m \Rightarrow a(x - y) \equiv 0 \text{ mod } m$$

Since $gcd(a, m) = 1$, $m|(x - y) \Rightarrow x = y$, $(x, y \in \{0, 1, ..., m - 1\})$

Example 14. *Solve $3X \equiv 5$ mod 11.*

$gcd(3, 11) = 1$, $1 = 4 * 3 - 1 * 11$,

$$
\begin{aligned}
X &\equiv 4 * 5 \\
X &\equiv 9
\end{aligned}
$$

□

5.3 Chinese Remaindar Theorem (CRT): unique solution for x modulo mn

Theorem 10 (Chinese Remaindar Theorem (CRT))**.**
If $gcd(m, n) = 1$. Then $\begin{cases} x \equiv r \text{ mod } m & (1) \\ x \equiv s \text{ mod } n & (2) \end{cases}$ have a unique solution for x modulo mn.

Proof.
$(1) \Rightarrow x = km + r$ for some $k \in \mathbb{Z}$.

$$
\begin{aligned}
\text{substitute (2) } &\Rightarrow km + r \equiv s \text{ mod } n \\
&\Leftrightarrow mk \equiv s - r \text{ mod } n \quad (3)
\end{aligned}
$$

According to previous theorem, $gcd(m, n) = 1$, (3) has a **unique** solution.
We say $k \equiv t$ mod n, $k = ln + t$ for some $l \in \mathbb{Z}$
$\Rightarrow x = (ln + t)m + r = lnm + tm + r$, where $tm + r$ is the unique solution to x modulo mn. □

Example 15. *(Similar to CRT) Find the smallest integer x such that*

$$x \equiv 1 \ mod \ 11 \ and \ x \equiv 9 \ mod \ 13$$

$gcd(11, 13) = 1$ and $1 = 6 * 11 - 5 * 13$
Write $x = 11k + 1$. Substitute in $x \equiv 9$ mod 13:

$$\begin{aligned} 11k &\equiv 8 \text{ mod } 13 \\ 6 * 11k &\equiv 6 * 8 \equiv 9 \text{ mod } 13 \\ (1 + 5 * 13)k &\equiv 9 \text{ mod } 13 \\ k &\equiv 9 \text{ mod } 13 \end{aligned}$$

Then $x = 11k + 1 = 100$.

5.4 Congruence Classes: $[a]_n = \{a + kn | k \in \mathbb{Z}\}$

Fix $n \in \mathbb{Z}_+$, we call $[a]_n = [a]$ the **congruence class** of a modulo n.

$$[a] = \{b \in \mathbb{Z} | b \equiv a \ mod \ n\} = \{a + kn | k \in \mathbb{Z}\}$$

5.4.1 Set of congruence classes of mod n: $\mathbb{Z}_n = \{[a]_n | a \in \mathbb{Z}\} = \{[0], [1], ..., [n-1]\}$

The set of *congruence classes* of mod n is denoted $\mathbb{Z}_n = \{[a]_n | a \in \mathbb{Z}\}$

Proposition 14 (Proposition 1.5.2.). *For any $n \geq 1$ there are exactly n congruences classes modulo n, which we may write as*

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$$

Proof.
For any $a \in \mathbb{Z}$. By Euclidean algorithm, $a = qn + r$, $q, r \in \mathbb{Z}$, $0 \leq r < n \Rightarrow a \in [r]$. So, $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$.
When $0 \leq a < b \leq n - 1$, $n \nmid (b - a)$, so $[a] \neq [b]$ the n congruence classes listed are all distinct. Hence, there are exactly n congruence classes. □

5.4.2 Proposition 1.5.5: Addition and Multiplication on Congruence Classes

Fix $n \in \mathbb{Z}$, we define addition+ and multiplication· on $\mathbb{Z}_n$:

$$\begin{aligned} [a] + [b] &= [a + b] = \{a + b + (k + j)n | k, j \in \mathbb{Z}\} \\ [a] \cdot [b] &= [ab] = \{ab + (aj + bk + kjn)n | k, j \in \mathbb{Z}\} \end{aligned}$$

This is well defined, follows Lemma 1.5.3.

Proposition 15 (Proposition 1.5.5.). *Let $a, b, c, d, n \in \mathbb{Z}, n \geq 1$, then*
(i) Addition and multiplication are commutative and associative operations in $\mathbb{Z}_n$.
(ii) $[a] + [0] = [a]$.
(iii) $[-a] + [a] = [0]$.
(iv) $[1][a] = [a]$.
(v) $[a]([b] + [c]) = [a][b] + [a][c]$.

Proof.

□

5.4.3 Units(i.e. invertible) in Congruence Classes

Say $[a] \in \mathbb{Z}_n$ is a **unit** or is **invertible** if $\exists [b] \in \mathbb{Z}_n$ so that $[a][b] = [1]$.

5.4.4 Proposition 1.5.6: Set of units in congruence classes: $\mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n | [a] \textit{ is a unit}\} = \{[a] \in \mathbb{Z}_n | gcd(a,n) = 1\}$

The set of **invertible** elements in $\mathbb{Z}_n$ will be denoted $\mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n | [a] \textit{ is a unit}\}$.

Proposition 16 (Proposition 1.5.6.). *For all $n \geq 1$, we have $\mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n | gcd(a,n) = 1\}$.*

Proof.
By Proposition 1.4.8, we know there exists b, c s.t. $ab + cn = 1$. So, $ab \equiv 1 \ mod \ n$, $[1] = [ab] = [a][b]$. So, $\{[a] \in \mathbb{Z}_n | gcd(a,n) = 1\} \subset \mathbb{Z}_n^\times$
$[a]$ *is a unit* $\Rightarrow \exists [b] \in \mathbb{Z}_n$ so that $[a][b] = [ab] = [1] \Rightarrow ab = 1 + kn, k \in \mathbb{Z} \Rightarrow ab - kn = 1, k \in \mathbb{Z} \Rightarrow gcd(a,n) = 1$. So, $\mathbb{Z}_n^\times \subset \{[a] \in \mathbb{Z}_n | gcd(a,n) = 1\}$. □

Note 3. *Inverse of $[a]$ is unique, i.e. $[b] = [a]^{-1}$ is unique.*

$[a][b] = 1, [a][b'] = 1 \Rightarrow [b] = [b][1] = [b][a][b'] = [b']$

5.4.5 Corollary 1.5.7: if p is prime, $\varphi(p) = \mathbb{Z}_p^\times = \{[1], [2], ..., [p-1]\}$

Corollary 2 (Corollary 1.5.7). *If $p \geq 2$ is prime, $\mathbb{Z}_p^\times = \{[1], [2], ..., [p-1]\}$.*

5.5 Euler phi-function: $\varphi(n) = |\mathbb{Z}_n^\times|$

Euler phi-function: $\varphi(n) = |\mathbb{Z}_n^\times|$.
p prime, $\varphi(p) = p - 1$.

5.5.1 $m|n$, $\pi_{m,n}([a]_n) = [a]_m$

Example 16 (Exercise 1.5.4). *If $m|n$, we can define $\pi_{m,n} : \mathbb{Z}_n \to \mathbb{Z}_m$ by $\pi_{m,n}([a]_n) = [a]_m$. Prove it is well-defined.*

Proof.
We write $[a]_n = [c]_n$, verify that $[a]_m = [c]_m$.
Since $m|n$, there exists $k \in \mathbb{Z}$ s.t. $n = km$.
$[a]_n = [c]_n \Rightarrow \exists j \in \mathbb{Z}$ s.t. $c = a + jn$.
$[c]_m = [a + jn]_m = [a + jkm]_m = [a]_m$ □

5.6 Theorem 1.5.8(Chinese Remainder Theorem): $n = mk, gcd(m,k) = 1$, $F([a]_n) = (\pi_{m,n}([a]_n), \pi_{k,n}([a]_n)) = ([a]_m, [a]_k)$

Theorem 11 (Theorem 1.5.8(Chinese Remainder Theorem)). *If $m, n, k > 0, n = mk, gcd(m,k) = 1$, then $F : \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_k$ which is given by $F([a]_n) = (\pi_{m,n}([a]_n), \pi_{k,n}([a]_n)) = ([a]_m, [a]_k)$, then F is a bijection.*

Proof.
(1)Injective: $F([a]_n) = F([b]_n) \Rightarrow [a]_m = [b]_m, [a]_k = [b]_k$ i.e. $a \equiv b \ mod \ m, a \equiv b \ mod \ n$. $\exists i, j \in \mathbb{Z}$ s.t. $b = a + im = a + jk \Rightarrow k|im$. Since $gcd(m,k) = 1$, $k|i \Rightarrow n = mk|im$. Then $[b]_n = [a]_n + [im]_n = [a]_n$.
(2)Surjective: prove $\forall u, v \in \mathbb{Z}$, $\exists a\mathbb{Z}$ s.t. $[a]_m = [u]_m, [a]_k = [v]_k$.

Since $gcd(m,k)=1$, $\exists s,t\in\mathbb{Z}$ so that $1=sm+tk$.
Let $a=(1-tk)u+(1-sm)v$, $[a]_m=[(u-v)sm+v]_m=[v]_m$, $[a]_k=[(v-u)tk+u]_k=[u]_k$. □

Note 4. $F([a]_n[b]_n)=F([ab]_n)=([ab]_m,[ab]_k)=([a]_m[b]_m,[a]_k[b]_k)$

Since F is a bijection, $[ab]_n=[1]_n$ iff $([a]_m[b]_m,[a]_k[b]_k)=([1]_m,[1]_k)$.

5.6.1 Proposition 1.5.9+Corollary 1.5.10: $m,n,k>0,n=mk,gcd(m,k)=1$, then $F(\mathbb{Z}_n^\times)=\mathbb{Z}_m^\times\times\mathbb{Z}_k^\times$, then $\varphi(n)=\varphi(m)\varphi(k)$

Proposition 17 (Proposition 1.5.9+Corollary 1.5.10)**.** *If $m,n,k>0,n=mk,gcd(m,k)=1$, then $F(\mathbb{Z}_n^\times)=\mathbb{Z}_m^\times\times\mathbb{Z}_k^\times$, then $\varphi(n)=\varphi(m)\varphi(k)$.*

5.7 prime factorization: $n=p_1^{r_1}...p_k^{r_k}$, then $\varphi(n)=(p_1-1)p_1^{r_1-1}...(p_k-1)p_k^{r_k-1}$

Proposition 18. *If $n\in\mathbb{Z}$ is positive integre with prime factorization $n=p_1^{r_1}...p_k^{r_k}$, then $\varphi(n)=(p_1-1)p_1^{r_1-1}...(p_k-1)p_k^{r_k-1}$*

Proof.
$\mathbb{Z}_{p^r}=\{[0],[1],...,[p^r-1]\}$, the number of multiples of p is $\frac{p^r}{p}=p^{r-1}$. Then $\varphi(p^r)=|\mathbb{Z}_{p^r}^\times|=p^r-p^{r-1}=(p-1)p^{r-1}$. So,

$$\varphi(n)=\varphi(p_1^{r_1})...\varphi(p_k^{r_k})=(p_1-1)p_1^{r_1-1}...(p_k-1)p_k^{r_k-1}$$

□

6 Group

6.1 Group $(G,*)$: a set with a binary operation(associative, identity, inverse)

6.1.1 Definition

A *group* is a nonempty set G with a binary operation $*:G\times G\to G$ s.t.

(1) Binary operation on G, $*:G\times G\to G$

(2) $*$ is **associative**

(3) G contains an **identity** element e for $*$: $\exists e\in G$ s.t. $e*g=g*e=g\ \forall g\in G$

(4) Each element $a\in G$ has an **inverse** $b\in G$ s.t. $a*b=b*a=e$.
A Group is **abelian** if moreover

(5) $*$ is **commutative**.

$|G|$ =Order of a group $(G,*)$
$(\mathbb{Z},+)$ is a group and $+$ is commutative, we call this kind of groups(statify commutative) *abelian group*.

Example 17. *If $\mathbb{F}$ is a field, then $(\mathbb{F},+)$ and $(\mathbb{F}^\times,\cdot)$ are abelian group.*

Example 18. *If V is a vector space over $\mathbb{F}$, then $(V,+)$ abelian group.*

As we know a V is a vector space over $\mathbb{F}$ means V is a field whose subfields include $\mathbb{F}$.

6.1.2 Uniqueness of identity and inverse

Lemma 3. *1. Identity of a group is unique. 2. Inverse of any element in a group is also unique.*

Proof.
1. Let e, e' be two identities in G, then $e * e' = e = e'$.
2. Suppose b, c are both inverse of a, then

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

□

6.1.3 Examples: Permutation group $Sym(X)$, Klein 4-group, alternating group A_n, Dihedral group

Example 19. *If X is any nonempty set, permutation group of X : $\{\sigma : X \to X | \sigma$ is a bijection$\}$, then*

1. $\circ$ is associative;
2. $id : X \to X,\ id(x) = x\ \forall x \in X$ is the idenity;
3. $\sigma \in Sym(X), \sigma^{-1} \in Sym(X)$ is the inverse function.

$(Sym(X), \circ)$ **is a group called the symmetric group of** X

Example 20. *The Klein four-group is a group with four elements, in which each element is self-inverse (composing it with itself produces the identity) and in which composing any two of the three non-identity elements produces the third one. For example, $K \leq S_4$*

$$K = \{(1), (12)(34), (13)(24), (14)(23)\}$$

Example 21. *An alternating group is the group of even permutations of a finite set. An alternating group of degree n, A_n.*

The cycle structure of A_5,
(1) $(abcde)$ - even
(3) (abc) - even
(4) $(ab)(cd)$ - even (odd permutation $\times$ odd permutation)
(6) e - even

Example 22 (Dihedral group)**.**

The dihedral group of order $2n$, denoted D_{2n}, is the group of symmetries of a regular n-gon $A_1A_2 \ldots A_n$, which includes rotations and reflections. It consists of the $2n$ elements

$$\left\{1, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\right\}.$$

The element ρ corresponds to rotating the n-gon by $\frac{2\pi}{n}$, while σ corresponds to reflecting it across the line OA_1 (here O is the center of the polygon). So $\rho\sigma$ mean "reflect then rotate" (like with function composition, we read from right to left). In particular, $\rho^n = \sigma^2 = 1$. You can also see that $\rho^k\sigma = \sigma\rho^{-k} = \sigma\rho^{n-k}$.

6.1.4 Cancelation Laws

Theorem 12. *Let G be a group. The left and right cancelation laws hold in G:*

1. $a * x = a * y \Rightarrow x = y$
2. $x * a = y * a \Rightarrow x = y$

Proof.
Let $a*x = a*y$. $\exists a'$ s.t. $a'*a = e$. $a'*(a*x) = a'*(a*y) \Rightarrow (a'*a)*x = (a'*a)*y \Rightarrow e*x = e*y \Rightarrow x = y$
Similar for the right cancel law. □

6.1.5 Unique Solution of Linear Equation

Theorem 13. *The linear equation $a * x = b$ and $y * a = b$ has unique solution.*

Proof.

1. Existence: Multiply by a': $a' * (a * x) = a' * b \Rightarrow x = a' * b$ is a solution.
2. Uniqueness: if x' is another, $a * x = a * x' = b \Rightarrow x = x'$

□

6.2 Subgroup: $H \leq G$

Definition 10. *A subset $H \subseteq G$ is a subgroup of G if H is itself a group.*

write $H \leq G$, $H < G$ if H is a subgroup of $(G, *)$. (If $H = G$, H is an improper subgroup. If $H \subsetneq G$, H is an proper subgroup.)
If $H = \{e\}$, then H is a trivial subgroup.
If $H \neq \{e\}$, then H is a nontrivial subgroup.

Theorem 14. *A subset $H \subseteq G$ is a subgroup of G if and only if*

1. *H is closed under $*$. ($\forall\ g, h \in H$, $g * h \in H$)*
2. *identity $e \in H$.*
3. *Each $a \in H$, the inverse $a' \in H$*

Proof.
"$\Rightarrow$": if $H \leq G$ be a subgroup.

1. H is a group $\Rightarrow *$ is a binary operation on H, $* : H \times H \to H$ i.e. H is closed under $*$.
2. Identity of H, e_H is also a identity of G, due to the uniqueness of identity, $e_H = e_G$.
3. $a \in H$, a's inverse $a'_H \in H$ is also an inverse in G, due to the uniqueness of identity, $a'_H = a'_G$.

"$\Leftarrow$":

1. H is closed under $* \Rightarrow *$ is a binary operation on H.
2. 2,3 fufill the requirement of identity and inverse.
3. $*$ is operation of group $G \Rightarrow *$ is associative.
   Hence H is itself a group.
4. H is a subeset of G, then H is s subgroup of G.

□

6.2.1 Proposition 2.6.8: $H < G$, $(H, *)$ is a group: A group's operation with its any subgroup is also a group

Proposition 19 (Proposition 2.6.8)**.** *If $(G, *)$ is a group, $H \subset G$ is a subgroup, then $(H, *)$ is a group.*

Example 23. *$(G, *)$ is a group, then $e < G$, $G < G$.*

Example 24. *$\mathbb{K} \subset \mathbb{F}$ is a subfield, then $\mathbb{K} < \mathbb{F}$, $\mathbb{K}^\times < \mathbb{F}^\times$.*

Example 25. *$W \subset V$ is a vector subspace, $W < V$.*

Example 26. *$1 \in S^1 \subset \mathbb{C}^\times$, $S^1 = \{z \in \mathbb{C} | |z| = 1\}$. S^1 is a subgroup.*

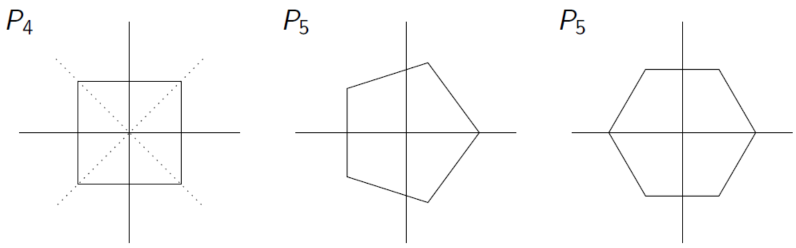
Proof.
$S^1 = \{e^{i\theta} | \theta \in \mathbb{R}\}$. For any $e^{i\theta}, e^{i\psi} \in S^1$, $e^{i\theta}e^{i\psi} = e^{i(\theta+\psi)} \in S^1, e^{-i\theta} \in S^1$. □

Example 27. *$Isom(\mathbb{R}^n) < Sym(\mathbb{R}^n)$*

Example 28. *If $\mathbb{F}$ is a field, $Aut(\mathbb{F}) = \{\sigma : \mathbb{F} \to \mathbb{F} \in Sym(\mathbb{F}) | \sigma(a + b) = \sigma(a) + \sigma(b), \sigma(ab) = \sigma(a)\sigma(b)\} < Sym(\mathbb{F})$*

Example 29. *Dihedral Groups:*

Let $P_n \subset \mathbb{R}^2$ be a regular $n - gon$



$D_n < Isom(\mathbb{R}^2)$, $D_n = \{\Phi \in Isom(\mathbb{R}^2) | \Phi(P_n) = P_n\}$

6.3 Some Properties of Group Operation

Proposition 20 (Proposition 3.1.1)**.** *Let $(G, *)$ be a group with identity $e \in G$, then*

(1) if $g, h \in G$ and either $g * h = h$ or $h * g = h$, then $g = e$
(2) if $g, h \in G$ and $g * h = e$ then $g = h^{-1}$ and $h = g^{-1}$

Corollary 3 (Corollary 3.1.2)**.** *$e^{-1} = e$, $(g^{-1})^{-1} = g$, $(g * h)^{-1} = h^{-1} * g^{-1}$*

6.4 Power of an Element

We define g^n recursively for $n \geq 0$ by setting $g^0 = e$ and for $n \geq 1$, we set $g^n = g^{n-1} * g$. For $n \leq 0$, we define $g^n = (g^{-1})^{-n}$.

Proposition 21 (Proposition 3.1.5)**.** *(1) $g^n * g^m = g^{n+m}$; (2) $(g^n)^m = g^{nm}$*

6.5 $(G \times H, \circledast)$: <u>Direct Product</u> of G and H

$(G, *)$ a group $(H, \star)$ a group. Define an operation on $G \times H$, $\circledast$:

$$(h, k) \circledast (h', k') = (h * h', k * k')$$

6.5.1 Proposition 3.1.7: $(G \times H, \circledast)$ is a group

Proposition 22 (Proposition 3.1.7)**.** *$(G \times H, \circledast)$ is a group. The identity is (e_G, e_H), inverse is (g^{-1}, h^{-1})*

usually written as

$$(h, k)(h', k') = (hh', kk')$$

6.6 Subgroups and Cyclic Groups

6.6.1 Intersection of Subgroups is a Subgroup

Proposition 23 (Proposition 3.2.2)**.** *Let G be a group and suppose $\mathcal{H}$ is any collection of subgroups of G. Then $K = \cap_{H \in \mathcal{H}} H < G$ is a subgroup of G.*

6.6.2 Subgroup Generated by A: $\langle A \rangle$

We define **Subgroup Generated by A:**

$$\langle A \rangle = \cap_{H \in \mathcal{H}(A)} H$$

where $\mathcal{H}(A)$ is the set of all subgroups of G containing the set A:

$$\mathcal{H}(A) = \{H < G | A \subset H \textit{ and } H \textit{ is a subgroup of } G\}$$

6.6.3 Cyclic Group: group generated by an element

A group G is <u>cyclic</u> if exists g (an element), $\langle g \rangle = G$.
g is called a <u>generator</u> for G in this case.
Easy to prove

$$G = \langle g \rangle = \{...g^{-2}, g^{-1}, e, g^1, g^2...\}$$

6.6.4 Cyclic Subgroup

If A is a subgroup of G, and $A = \langle \{a\} \rangle = \langle a \rangle$. Then A is the <u>cyclic subgroup</u> generated by a: $A = \langle a \rangle \leq G$

$$\langle a \rangle = \{...a^{-2}, a^{-1}, e, a^1, a^2...\}$$

6.6.5 Subgroups of a Cyclic Group must be Cyclic

Theorem 15. *A subgroup of a cyclic group is cyclic.*

Proof.
Let $G = \{a^n : n \in \mathbb{Z}\}$ be a cyclic group. Let $H \leq G$ be a subgroup.

1. If $H = \{e\}$, then H is cyclic.

2. If $H \neq \{e\}$, then $a^n \in H$ for some $n > 0$. Check m be the minimal among all n.

   Claim: $H = \langle a^m \rangle$

   Proof: Clearly $\langle a^m \rangle \subset H$. $\forall a^n \in H$, $n = qm + r, 0 \leq r < m$. Then $a^r = a^n (a^m)^{-q}$. Since m is the minimal positive integer s.t. $a^m \in H$, $r = 0$. $\Rightarrow n = qm \Rightarrow a^n \in \langle a^m \rangle$. Hence $H = \langle a^m \rangle$ which is cyclic.

□

Example 30 (Subgroups of $(\mathbb{Z}, +)$)**.**

$\mathbb{Z}$ is a cyclic group $\langle 1 \rangle$. Its subgroups are $\langle n \rangle \leq \mathbb{Z}$ for some $n \geq 0$. (which is a multiplier of n. $(n\mathbb{Z})$)
$n = 0, H = \{0\}; n = 1, H = \mathbb{Z}; n = 2, H = 2\mathbb{Z}$

6.6.6 Theorem: $\langle a^v \rangle < \{1, a, a^2, ..., a^{n-1}\} \Rightarrow \langle a^v \rangle = \langle a^d \rangle, d = gcd(v, n), |\langle a^v \rangle| = \frac{n}{d}$

Theorem 16. *Let G be a cyclic group of order n. ($G = \{1, a, a^2, ..., a^{n-1}\}$, where $a^n = 1$.). Let $H = \langle a^v \rangle$ be a subgroup of G. Then H is generated by a^d (i.e. $H = \langle a^d \rangle$), $d = gcd(v, n)$ and $|H| = \frac{n}{d}$.*

Proof.
Let $H' = \langle a^d \rangle$, we need to show that $H = H'$. $d = gcd(v, n) = d|v \Rightarrow a^v \in \langle a^d \rangle \Rightarrow H \subset H'$.
While $d = sv + tn$ for some s, t. $\Rightarrow a^d = (a^v)^s (a^n)^t$. Since $a^n = 1$, $a^d = (a^v)^s \Rightarrow H' \subset H$.
Hence, $H = H' = \langle a^v \rangle$. $H = \{1, a^d, a^{2d}, ..., a^{n-d}\}, |H| = \frac{n}{d}$ □

6.6.7 Corollary 3.2.4: G is a cyclic group $\Rightarrow$ G is abelian

Corollary 4 (Corollary 3.2.4)**.** *If G is a cyclic group (i.e. exits $g \in G$ s.t. $\langle g \rangle = G$), then G is abelian (i.e. commutative).*

6.6.8 Equivalent properties of order of g: $|g| = |\langle g \rangle| < \infty$

Proposition 24 (Proposition 3.2.6)**.** *Let G be a group for $g \in G$, the following are equivalent:*

(i) $|g| < \infty$
(ii) $\exists n \neq m$ in $\mathbb{Z}$ so that $g^n = g^m$
(iii) $\exists n \in \mathbb{Z},\ n \neq 0$ so that $g^n = e$
(iv) $\exists n \in \mathbb{Z}_+$so that $g^n = e$
If $|g| < \infty$, then $|g| =$ smallest $n \in \mathbb{Z}_+$so that $g^n = e$, and $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\} = \{g^n \mid n = 0, \ldots, n-1\}$

6.6.9 $(\mathbb{Z}, +)$ Theorem 3.2.9: $\langle a \rangle < \langle b \rangle$ if and only if $b|a$

Theorem 17 (Theorem 3.2.9)**.** *If $H < \mathbb{Z}$ is a subgroup, then either $H = \{0\}$, or else $H = \langle d \rangle$, where*

$$d = \min\{h \in H | h > 0\}$$

*Consequently, $a \to \langle a \rangle$ defines a **bijection** from $N = \{0, 1, 2, ...\}$ to the set of subgroups of $\mathbb{Z}$. Furthermore, for $a, b \in \mathbb{Z}_+$, we have $\langle a \rangle < \langle b \rangle$ if and only if $b|a$.*

6.6.10 $(\mathbb{Z}_n, +)$ Theorem 3.2.10: $\langle [d] \rangle < \langle [d'] \rangle$ if and only if $d'|d$

Theorem 18 (Theorem 3.2.10)**.** *For any $n \geq 2$, if $H < \mathbb{Z}_n$ is a subgroup, then there is a positive divisor d of n so that*

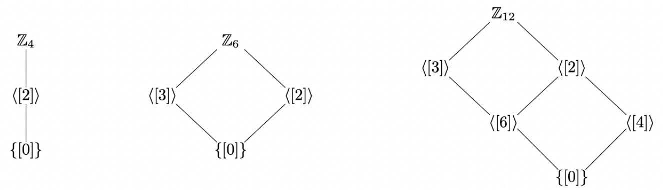
$$H = \langle [d] \rangle$$

Furthermore, this defines a bijection between divisors of H and subgroups of $\mathbb{Z}_n$. Furthermore, if $d, d' > 0$ are two divisors of n, then $\langle [d] \rangle < \langle [d'] \rangle$ if and only if $d'|d$.

If $H = \langle [d] \rangle$ is a subgroup of H, then $[n] \in H$, so $d|n$. And $|H| = |\langle [d] \rangle| = \frac{n}{d}$, so $|H||d$

6.6.11 Subgroup Lattice

The set of all subgroups of a group of G, together with the data of which subgroups contain which others is called the **subgroup lattice**. We often picture the subgroup lattice in a diagram with the entire group at the top, the trivial subgroup $\{e\}$ at the bottom, and the intermediate subgroups in the middle, with lines drawn from subgroups up to larger groups.



Writing down the subgroup lattice is as easy as writing down the divisibility lattice in which n is placed at the bottom, 1 at the top, and all intermediate divisors in between, connected by edges when there is divisibility. The congruence class of the divisor generates the corresponding subgroup in the subgroup lattice.

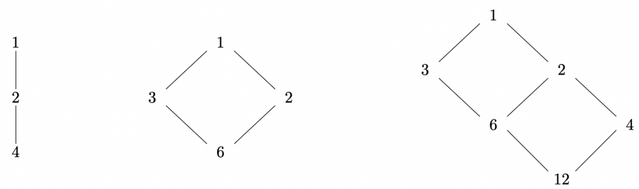


Figure 2:

6.7 Homomorphism

6.7.1 Def: Homomorphism, Image

Definition 11. *If $(G, *)$ and $(H, \circ)$ are groups, then a function $f : G \to H$ is a **homomorphism** if*

$$f(x * y) = f(x) \circ f(y), \ \forall x, y \in G$$

*If f is also a bijection, then f is called an **isomorphism**.*

Example 31. *Let S_n be the symmetric group on n letters, and let $\phi : S_n \to \mathbb{Z}_2$ be defined by*

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation,} \\ 1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Show that ϕ is a homomorphism.

Example 32. *Let $GL(n,\mathbb{R})$ be the multiplicative group of all invertible $n \times n$ matrices. Recall that a matrix A is invertible if and only if its determinant, $\det(A)$, is nonzero. Recall also that for matrices $A, B \in GL(n.\mathbb{R})$ we have*

$$\det(AB) = \det(A)$$

Example 33.

1. $\phi : (\mathbb{R}, +) \to (\mathbb{R}^*, x) \quad \phi(x) = 2^x$. Then

$$\phi(x + y) = 2^{x+y} = 2^x 2^y = \phi(x)\phi(y)$$

   ϕ is a homonorphism.

2. $\phi : G \to G \quad \phi(g) = g^{-1}$. Then

$$\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = \phi(h)\phi(g)$$

   ϕ is not a homonorphism in general; but it is homomorpgism if it is abelian.

Definition 12. *Let ϕ be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The image $\phi[A]$ of A in Y under ϕ is $\{\phi(a) \mid a \in A\}$. The set $\phi[X]$ is the range of ϕ. The inverse image $\phi^{-1}[B]$ of B i is $\{x \in X \mid \phi(x) \in B\}$*

6.7.2 Properties of Homomorphism

Theorem 19. *Let ϕ be a homomorphism of a group G into a group G', then*

1. if $e \in G$ is an identity in G, then $\phi(e) \in G'$ is the identity in G'.
2. if $a \in G$ has inverse $a' \in G$, then $\phi(a) \in G'$ has inverse $\phi(a') \in G'$.
3. if $H \leq G$ is a subgroup of G, then the image $\phi(H) = \{\phi(h) : h \in G\} \leq G'$ is a subgroup of G'.
4. if $K' \leq G'$ then the inverse image $\phi^{-1}(K') = \{x \in G : \phi(x) \in K'\} \leq G$.

6.7.3 Kernel of Homomorphism

Definition 13. *Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}(e') = \{x \in G : \phi(x) = e'\}$ is the kernel of ϕ, denoted by $Ker(\phi)$.*

$$Ker(\phi) \stackrel{def}{=} \phi^{-1}(e') = \{x \in G : \phi(x) = e'\}$$

Theorem 20 ($Ker\phi$ is normal)**.** *Let $\phi : G \to G'$ be a homomorphism. $H = Ker\phi$, then for all $a \in G$, $\phi^{-1}[\phi(a)] = \{x \in G : \phi(x) = \phi(a)\}$ is the left coset aH of H, and is also the right coset Ha of H.*

$$aH = Ha = \{x \in G : \phi(x) = \phi(a)\}$$

Proof.

$$\begin{aligned}
& \phi(x) = \phi(a) \\
\Leftrightarrow \quad & \phi(x)\phi(a)^{-1} = e' \\
\Leftrightarrow \quad & \phi(x)\phi(a^{-1}) = e' \\
\Leftrightarrow \quad & \phi(xa^{-1}) = e' \\
\Leftrightarrow \quad & xa^{-1} \in H \\
\Leftrightarrow \quad & x \in Ha
\end{aligned}$$

Similarity, we can prove $x \in aH$. $\square$

Theorem 21. *A homomorphism is injective if and only if $Ker(\phi) = \{e\}$.*

Proof.

$$\begin{aligned}\phi(x) = \phi(y) \Leftrightarrow & \phi(x)\phi^{-1}(y) = e' \\ & \phi(x)\phi(y^{-1}) = e' \\ & \phi(xy^{-1}) = e' \\ \Leftrightarrow & xy^{-1} \in Ker(\phi)\end{aligned}$$

Hence, we can also prove that

$$xy^{-1} \in Ker(\phi) \Leftrightarrow x = y \text{ if and only if } Ker(\phi) = \{e\}$$

□

6.8 Isomorphism

6.8.1 Definition: Isomorphism

Definition 14. *We say that G and H are* ***isomorphic*** *if exists an* ***isomorphism*** *f, denoted by $G \cong H$ or $G \simeq H$. (since f is bijection, $G \cong H \Leftrightarrow H \cong G$)*

Isomophic means these two pathes are the same.

$$\begin{aligned} G \times G \xrightarrow{*} \qquad & G \xrightarrow{f} \quad H \\ G \times G \xrightarrow{(f,f)} \quad & H \times H \xrightarrow{\circ} \quad H \end{aligned}$$

Example 34. $(\mathbb{Z}_2, +)$, $(\{-1, 1\}, \times)$ *and* $\phi : 0 \to 1;\ 1 \to -1$.

$$\begin{aligned}\phi(0+0) = 1 = \phi(0) \times \phi(0) \\ \phi(0+1) = -1 = \phi(0) \times \phi(1) \\ \phi(1+1) = 1 = \phi(1) \times \phi(1)\end{aligned}$$

6.8.2 Theorem: $\begin{cases} \sigma : G \to G' \textbf{ injective} \\ \sigma(xy) = \sigma(x)\sigma(y)\ \forall x, y \in G \end{cases} \Rightarrow \sigma(G) \le G'$, G is isomorphic to $\sigma(G)$

Theorem 22. *Let $\sigma : G \to G'$ be an injective map s.t.*

$$\sigma(xy) = \sigma(x)\sigma(y),\ \forall x, y \in G$$

Then the image $\sigma(G) = \{\sigma(x) : x \in G\}$ is a subgroup of G' that is isomorphic to G.

Proof.

1. Closed: $\forall a = \sigma(x), b = \sigma(y) \in \sigma(G)$, then $ab = \sigma(x)\sigma(y) = \sigma(xy) \in \sigma(G)$.
2. Identity: $\sigma(e) \in \sigma(G)$ is an identity for $\sigma(G)$: $\sigma(e)\sigma(x) = \sigma(ex) = \sigma(x) = \sigma(xe) = \sigma(x)\sigma(e)$
3. Inverse: $\sigma(x^{-1})$ is an inverse in $\sigma(G)$ for $\sigma(x)$: $\sigma(x^{-1})\sigma(x) = \sigma(e) = \sigma(x)\sigma(x^{-1})$

□

6.8.3 Cayley Theorem: G is isomorphic to a subgroup of S_G

Theorem 23 (Cayley Theorem)**.** *Let G be a group and S_G is the symmetric group of G (the group of all permutation of G: $S_G = \{Bijection\ \sigma : G \to G\}$) Then G is isomorphic to a subgroup of S_G.*

Proof.
Set a bijection $\phi : G \to S_G$ such that $\phi(g) = \lambda_g, \forall g \in G$, where λ_g is a permutation $\lambda_g : x \to gx$.
Claim: $\lambda_g \in S_G$ (i.e. λ_g is a permutation of G, a bijection $G \to G$).

1. $\lambda_g : G \to G$ is injective
$$\begin{aligned} &\lambda_g(x) = \lambda_g(y) \\ &\Leftrightarrow gx = gy \\ &\Leftrightarrow x = y \end{aligned}$$
2. $\lambda_g : G \to G$ is surjective. Let $y \in G$
$$\begin{aligned} &\lambda_g(x) = y \\ &\Leftrightarrow gx = y \\ &\Leftrightarrow x = g^{-1}y \end{aligned}$$

Claim: $\phi(x)\phi(y) = \phi(xy)$

$$\begin{aligned} \phi(x)\phi(y) &= \lambda_x \circ \lambda_y \\ (\lambda_x \circ \lambda_y)(z) = \lambda_x(yz) = xyz &= \lambda_{xy}(z),\ \forall z \in G \\ \Rightarrow \phi(x)\phi(y) &= \phi(xy) \end{aligned}$$

According to previous theorem, $\phi(G) \leq G$ and G is isomorphic to $\phi(G)$.

□

6.9 Coset and Order

Definition 15. *If H is a subgroup of a group G and $a \in G$, then $aH = \{ah | h \in H\} \leq G$ is called left coset of H.*

Theorem 24. *Let $H \leq G$, $a, b \in G$,*

1. *$aH = bH$ if and only if $a^{-1}b \in H$*
2. *$aH \cap bH = \emptyset$ or $aH = bH$*
3. *$|aH| = |H|\ \forall a \in G$*

Proof.

1. Assume that $aH \cap bH \neq \emptyset$ and let $ah = bk \in aH \cap bH$ with $h, k \in H$.
$ah = bk \Leftrightarrow h = a^{-1}bk \Leftrightarrow a^{-1}b = hk^{-1} \in H$, thus $a^{-1}b \in H$.
2. When $aH \cap bH \neq \emptyset$ $\exists k_1, h \in H$ such that $ak_1 = bh \in bH$. Then $\forall k_2 \in H$ $a = bhk_1^{-1} \Rightarrow ak_2 = bhk_1^{-1}k_2$ where $hk_1^{-1}k_2 \in H$ so $ak_2 \in bH$, $\forall k_2 \in H$.
3. $x \to ax$ is bijection $\Rightarrow |aH| = |H|$.

□

Claim 2. *Coset can generate a partition of group:*

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

6.9.1 index of a subgroup

Definition 16. *Let H be a subgroup of a group G. The number of left cosets of H in G is the **index**.*

Note: Since $|aH| = |H|\ \forall a \in G$, the index of a subgroup is the number of subgroups which have order $|H|$.

6.9.2 Lagrange Theorem: Order of subgroup divides the order of group

Theorem 25 (Lagrange Theorem)**.** *Let $H \leq G$ be a subgroup of finite group G. Then the order $|H|$ divides the order $|G|$.*

Proof.
Give a partition

$$\begin{aligned} G &= a_1H \cup a_2H \cup \cdots \cup a_rH \\ |G| &= |a_1H| + |a_2H| + \cdots + |a_rH| \\ &= r|H| \to |H| \Big| |G| \end{aligned}$$

□

6.9.3 Theoerm: Order of element $a \in G = |\langle a \rangle|$ divides $|G|$

Theorem 26 (Order of element/cyclic subgroup)**.** *For $a \in G$, the order of a (the smallest m such that $a^m = e$) divides $|G|$. The order of a is the order of cyclic subgroup $\langle a \rangle$ with generator a.*

Proof.
For $a \in G$, $H = \{a^n, n \in \mathbb{Z}\} \leq G$. H is the size of m. With lagrange theorm, $|H| = m \Big| |G|$ □

Corollary 5. *Every group of prime order is cyclic.*

6.9.4 Theorem: Order n cyclic group is isomorphic to $(\mathbb{Z}_n, +_n)$

Theorem 27. *Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$. If G has finite order n, then G is isomorphic to $(\mathbb{Z}_n, +_n)$.*

6.10 Direct Products

6.10.1 Cartesian product

Let $G_1, G_2, ..., G_n$ be n groups. Let $G = G_1 \times G_2 \times \cdots \times G_n$ be the Cartesian product.
For $g \in G$, $g = (g_1, ..., g_n)$, $g_i \in G_i$.

Theorem 28. *Then $(G, *)$ becomes a group with operation $*$ defined as*

$$a * b = (a_1, ..., a_n) * (b_1, ..., b_n) = (a_1b_2, ..., a_nb_n) \quad a, b \in G$$

Proof.

(1) Binary operation $* : G \times G \to G$.

(2) $*$ is associative:

$$(a * b) * c = a * (b * c) = (a_1b_1c_1, ..., a_nb_nc_n)$$

(3) Identity: $e = (e_1, ..., e_n) \in G$
$$e * a = a = a * e$$

(4) Inverse: $a^{-1} = (a_1^{-1}, ..., a_n^{-1}) \in G$
$$a * a^{-1} = a^{-1} * a = e$$

□

6.10.2 Theorem: $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn} \Leftrightarrow gcd(m, n) = 1$

Theorem 29. *The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if $gcd(m, n) = 1$.*

Proof.
Claim: $(1, 1)$ generate $\mathbb{Z}_m \times \mathbb{Z}_n$
$k(1, 1) = (k, k) = (0, 0)$ if and only if $m|k$ and $n|k$. The smallest such k is $k = lcm(m, n) = mn$. Hence, $\mathbb{Z}_m \times \mathbb{Z}_n$ is a cyclic group with order mn. Then $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$.
We can define an isomorphism
$$\phi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$$
and its inverse
$$\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$
Since $\mathbb{Z}_{mn} \langle 1 \rangle$, $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (1, 1) \rangle$, we can write
$$\psi(x \bmod mn) = (x \bmod m, x \bmod n)$$
ψ is well-defined.
To describe $\phi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$ at $1 = sm + tn$ and let
$$\phi(a \bmod m, b \bmod n) = (atn + bsm \bmod mn)$$
$$\begin{aligned}\psi(atn + bsm \bmod mn) &= (atn + bsm \bmod m, atn + bsm \bmod n)\\ &= (atn \bmod m, bsm \bmod n)\\ &= (a(1 - sm) \bmod m, b(1 - tn) \bmod n)\\ &= (a \bmod m, b \bmod n)\end{aligned}$$
Hence ψ is the inverse of ϕ. □

Corollary 6. *The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and is isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ if and only if the numbers m_i for $i = 1, ..., n$ are such that the gcd of any two of them is 1.*

Example 35. *If n is written as a product of powers of distinct prime numbers, as it*
$$n = (p_1)^{n_1}(p_2)^{n_2} \cdots (p_r)^{n_r}$$
then $\mathbb{Z}_n$ is isomorphic to
$$\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \cdots \times \mathbb{Z}_{(p_r)^{n_r}}$$

6.10.3 Finitely Generated Abelian Groups

Theorem 30 (Primary Factor Version of the Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The number of factors of $\mathbb{Z}$ and the prime powers $(p_i)^{r_i}$ are unique.

- $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if $gcd(m,n) = 1$.
- Abelian $\Leftrightarrow \mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_n \times \mathbb{Z}_m$

Example 36. *Find all abelian group of order 16*

5 nonisomorphic abelian group.

$$\begin{cases} \mathbb{Z}_{16} \\ \mathbb{Z}_8 & \times\mathbb{Z}_2 \\ \mathbb{Z}_4 & \times\mathbb{Z}_4 \\ \mathbb{Z}_4 & \times\mathbb{Z}_2 & \times\mathbb{Z}_2 \\ \mathbb{Z}_2 & \times\mathbb{Z}_2 & \times\mathbb{Z}_2 & \times\mathbb{Z}_2 \end{cases}$$

Example 37.

$$\mathbb{Z}_6 \times \mathbb{Z}_{40} \times \mathbb{Z}_{49} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_{49}$$
$$\mathbb{Z}_{210} \times \mathbb{Z}_{56} \simeq \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_8$$

6.11 Def: Normal Subgroup $H \lhd G : aH = Ha, \forall a \in G$

Definition 17. *A subgroup $H \leq G$ is* ***normal*** *if its left and right cosets coincide, that is, if*

$$aH = Ha, \quad \forall a \in G$$

Notation: $H \lhd G$

Note that all subgroups of abelian groups are normal.

6.11.1 Thm: Three ways to check if H is normal

Theorem 31. *"$H < G$ is a normal subgroup of G ($H \lhd G$)" is equivalent to*

(1) $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$

(2) $gHg^{-1} = H$ for all $g \in G$

(3) $gH = Hg$ for all $g \in G$

6.11.2 Thm: A subgroup is "Well-defined Left Cosets Multiplication" $\Leftrightarrow$ "Normal"

Theorem 32. *Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation*

$$(aH)(bH) = (ab)H$$

if and only if $H \lhd G$ (H is a normal subgroup of G).
i.e. '$x \in aH$ and $y \in bH \Rightarrow xy \in abH$' <u>if and only if</u> '$aH = Ha, \quad \forall a \in G$'

Proof.

- "$\Rightarrow$": $\forall x \in aH$, $a^{-1} \in a^{-1}H \Rightarrow xa^{-1} \in H \Leftrightarrow x \in Ha \Rightarrow aH \subset Ha$;
  Similarly $a^{-1}H \subset Ha^{-1} \Leftrightarrow Ha \subset aH \Rightarrow aH = Ha$
- "$\Leftarrow$": Let $x \in aH$, $y \in bH$. Say $x = ah_1, y = bh_2$

$$\begin{aligned} xy &= (ah_1)(bh_2) \\ &= a(h_1 b)h_2 \\ &= a(bh_3)h_2 \quad \text{(Since } bH = Hb\text{)} \\ &= (ab)(h_3 h_2) \in abH \end{aligned}$$

□

6.12 Factor Group $G/H = \{aH : a \in G\}$

Definition 18. *The group $G/H = \{aH : a \in G\}$ with $(aH)(bH) = abH$ is the factor group (or quotient group) of G by H.*

6.12.1 Def: kernel H forms a factor group G/H

Definition 19. *Let $\phi : G \to G'$ be a homomorphism of groups with <u>kernel H</u>. Then the cosets of H form a **factor group**, $G/H = \{aH : a \in G\}$. where $(aH)(bH) = (ab)H$.*

Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.

6.12.2 Cor: $ker\phi$ is a normal subgroup

Corollary 7. *$ker\phi$ is a normal subgroup: $ker\phi \lhd G$ for all homonorphisms.*

6.12.3 Corollary: normal subgroup H forms a group G/H

By the Thm: A subgroup is "Well-defined Left Cosets Multiplication" $\Leftrightarrow$ "Normal".

Corollary 8. *Let $H \lhd G$ be a **normal subgroup** of G. Then the cosets of H form a group $G/H = \{aH : a \in G\}$ under the binary operation $(aH)(bH) = (ab)H$.*

Proof.

(1) $*$ is associative.

(2) G/H has an identity H.

$$H * aH = aH * H = aH$$

(3) $aH \in G/H$ has inverse $a^{-1}H$

$\square$

Note: This corollary contains the defintion because kernel is normal subgroup(kernel $\Rightarrow$ normal subgroup). (We can then prove they are exactly the same in the next theorem (kernel $\Leftarrow$ normal subgroup))

6.12.4 Thm: normal subgroup is a kernel of a surjective homomorphism $\gamma : G \to G/H$

For any normal subgroup $H \lhd G$, we can define $\gamma(x) = xH$ which is surjective with $ker\gamma = H$

Theorem 33. *Let $H \lhd G$ be a normal subgroup of G. Define $\gamma : G \to G/H$, $\gamma(x) = xH$. Then γ is a surjective homomorphism with $ker\gamma = H$.*

Proof.

1. γ is surjective homomorphism: $\gamma(ab) = abH = (aH)(bH) = \gamma(a)\gamma(b)$
2. $ker\gamma = H$: The identity in G/H is the coset H.

$$\begin{aligned} ker\gamma = \gamma^{-1}(H) &= \{a \in G : \gamma(a) = aH = H\} \\ &= \{a \in G : a \in H\} = H \end{aligned}$$

$\square$

6.12.5 The Fundamental Homomorphism Theorem: Every homomorphism ϕ can be factored to a homomorphism $\gamma : G \to G/H$ and isomorphism $\mu : G/H \to \phi[G]$

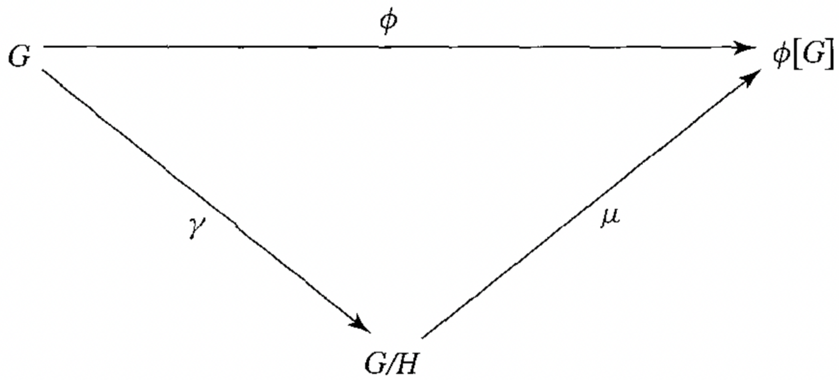


Figure 3: The Fundamental Homomorphism Theorem

Theorem 34 (The Fundamental Homomorphism Theorem)**.**

> *Homomorphism $\phi : G \to G'$ with kernel H* can be ***factored***
>
> $$\phi = \mu\gamma$$
>
> *where $\gamma : G \to G/H$ is a homomorphism, $\mu : G/H \to \phi[G]$ is an isomorphism*
> *where $\gamma(g) = gH$, $\mu(gH) = \phi(g)$*

Let $\phi : G \to G'$ be a group homomorphism with kernel H.
Then $\phi[G]$ is a group isomorphic to G/H, and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. (If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for each $g \in G$.)

Proof. i.e. prove μ is (1) well-deifined, (2) isomorphism.

(1) well-defined: if $aH = bH$, then $a^{-1}b \in H$,

$$\mu(bH) = \mu((a(a^{-1}b))H) = \phi(a(a^{-1}b)) = \phi(a)\phi(a^{-1}b) = \phi(a) = \mu(aH)$$

(2) homomorphism:

$$\mu(aHbH) = \mu(abH) = \phi(ab) = \phi(a)\phi(b) = \mu(aH)\mu(bH)$$

(3) isomorphism i.e. prove $ker(\mu)$ is exactly the identity in G/H:

$$\begin{aligned}\mu(aH) = e' = \phi(a) &\Leftrightarrow a \in ker(\mu), a \in ker(\phi) = H \\ &\Leftrightarrow aH = H, \quad aH \text{ is the identity in } G/H\end{aligned}$$

□

Corollary 9. *Let $\phi : G \to G'$ be a homomorphism for finite group G, G'.*
Then (1).$|\phi(G)| \Big| |G|$; (2).$|\phi(G)| \Big| |G'|$

Proof.

(1) According to the Fundamental Homomorphism theorem, $\phi(G)$ is one-to-one corresponse to G/H (H is the kernel of G), then $|\phi(G)| = |G/H| = |\{aH : a \in G\}| \Rightarrow |\phi(G)| = |G|/|H|$

(2) Proved by Lagrange theorem.

□

6.12.6 Thm: $(H \times K)/(H \times e) \simeq K$ and $(H \times K)/(e \times K) \simeq H$

Theorem 35. *Let $G = H \times K$ be the direct product of groups H and K. Then $\bar{H} = \{(h, e) \mid h \in H\}$ is a normal subgroup of G. Also $G/\bar{H}$ is isomorphic to K in a natural way. Similarly, $G/\bar{K} \simeq H$ in a natural way.*

Proof. $\pi : H \times K \to K$ where $\pi(h, k) = k$ has kernal $\bar{H} = \{(h, e) \mid h \in H\}$, then $H \times K/\bar{H}$ is isomorphic to K. Prove $G/\bar{K} \simeq H$ in the same way. □

6.12.7 Thm: factor group of a cyclic group is cyclic [a]/N=[aN]

Theorem 36. *A factor group of a cyclic group is cyclic.* $[a]/N = [aN]$

6.12.8 Ex: 15.11 example $\mathbb{Z}_4 \times \mathbb{Z}_6/(\langle(2, 3)\rangle) \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$ or $\mathbb{Z}_{12}$

6.12.9 Thm: Homomorphism $\phi : G \to G'$ preserves normal subgroups between G and $\phi[G]$.

Theorem 37. *Let $\phi : G \to G'$ be a group homomorphism. If N is a normal subgroup of G, then $\phi[N]$ is a normal subgroup of $\phi[G]$. Also, if N' is a normal subgroup of $\phi[G]$, then $\phi^{-1}[N']$ is a normal subgroup of G.*

Note: $\phi[N]$ is a normal subgroup of $\phi[G]$ not G'. Counterexample: $\phi : \mathbb{Z}_2 \to S_3$, where $\phi(0) = \rho_0$ and $\phi(1) = \mu_1$ is a homomorphism, and $\mathbb{Z}_2$ is a normal subgroup of itself, but $\{\rho_0, \mu_1\}$ is not a normal subgroup of S_3.

6.13 Def: automorphism, inner automorphism

Definition 20.
An isomorphism $\phi : G \to G$ of a group G with itself is an automorphism of G.
The automorphism $\phi_g : G \to G$, where $\phi_g(x) = gxg^{-1}$ for all $x \in G$, is the inner automorphism of G by g. Performing ϕ_g on x is called conjugation of x by g.

6.14 Simple Groups

Definition 21. *A group G is simple if it is nontrivial ($G \neq \{e\}$) and has no proper nontrivial normal subgroups. ($\nexists H \neq \{e\} \lhd G$)*

Theorem 38. *The alternating group A_n is simple for $n \geq 5$*
(alternating group is a group of even permutations on a set of length n)

6.15 The Center and Commutator Subgroups

6.15.1 Def: center and commutator subgroup

Theorem 39. *All finite subgroup G have two normal subgroups,*

(1) The *center* of G, $Z(G) = \{z \in G : za = az, \forall a \in G\} \lhd G$

(2) The *commutator* subgroup of G, $C(G) = [G, G] = \{[a, b] : a, b \in G\}$.

Definition 22. $[a, b] = aba^{-1}b^{-1}$ *is the commutator of a and b. $[a, b] \in G$ is the unique element such that $ab = [a, b]ba$.*

6.15.2 Thm: commutator subgroup is normal

Theorem 40. $[G, G] \lhd G$

Proof. Consider $[a, b] \in [G, G]$, prove that $\forall g \in G, g[a, b]g^{-1} \in [G, G]$

$$\begin{aligned} g[a, b]g^{-1} &= g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}] \in [G, G] \end{aligned}$$

□

Example 38.

(1) For abelian group, $Z(G) = G$, $C(G) = \{e\}$

(2) $G = S_6$, $Z(G) = \{e\}$, $C(G) = \{1, \rho, \rho^2\}$

(3) $G = D_8 = \{1, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$, $Z(G) = \{1, \rho^2\}$, $C(G) = \{1, \rho^2\}$

(4) $G = D_{12}$, $Z(G) = \{1, \rho^3\}$, $C(G) = \{1, \rho^2, \rho^4\}$

(5) $G = A_4$, $Z(G) = \{(1)\}$, $C(G) = \{(1), (12)(34), (13)(24), (14)(23)\}$

(6) $G = S_4$, $Z(G) = \{(1)\}$, $C(G) = A_4$

Commutator subgroup of S_n is A_n.
Commutator subrgoup of D_{2n} is $\{1, \rho^2, ..., \rho^{n-2}\}$
$\sigma\rho^a = \rho^{n-a}\sigma = \rho^{n-2a}(\rho^a\sigma) \Rightarrow \rho^{n-2a}$ is a commutator $\forall a \in \mathbb{Z} \Rightarrow C(D_{2n}) = \{1, \rho^2, ...\rho^{n-2}\}$ if n is even.

6.15.3 Thm: if $N \lhd G$, "G/N is abelian" $\Leftrightarrow$ "$[G,G] \leq N$"

Theorem 41. *If N is a normal subgroup of G, then G/N is abelian if and only if $[G,G] < N$.*

Proof.
If N is a normal subgroup of G and G/N is abelian, then $\left(a^{-1}N\right)\left(b^{-1}N\right) = \left(b^{-1}N\right)\left(a^{-1}N\right)$; that is, $aba^{-1}b^{-1}N = N$, so $aba^{-1}b^{-1} \in N$, and $C \leq N$. Finally, if $C \leq N$, then

$$\begin{aligned}(aN)(bN) &= abN = ab\left(b^{-1}a^{-1}ba\right)N \\ &= \left(abb^{-1}a^{-1}\right)baN = baN = (bN)(aN)\end{aligned}$$

□

6.16 Group Action on a Set

6.16.1 Def: action of group G on set X

Definition 23. *Let X be a set and G a group. An **action of** G **on** X is a map $* : G \times X \to X$ such that*

(1) $ex = x$ for all $x \in X$.

(2) $(g_1g_2)(x) = g_1(g_2x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

*Under these conditions, X **is a** G**-set**.*

Example: Let X be any set, and let H be a subgroup of the group S_x of all permutations of X. Then X is an H-set.

6.16.2 Thm: If G acts on X, $\phi : G \to S_X$ as $\phi(g) = \sigma_g$ is a homomorphism (where $\sigma_g(x) = gx$)

Theorem 42. *Let group G act on the set X,*

(1) *$\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is well-defined.*
($\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X)

(2) *$\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.*

Special case: Let G act on itself, we get the **Cayley Theorem**: G is isomorphic to a subgroup of S_G
In general, for a group G act on the set X, the homomorphism $\phi : G \to S_X$ is not injective. We say that G acts faithfully on X if ϕ is injective.

6.16.3 Examples of Group Actions

(Let $H \leq G$ be a subgroup of G)

(1) $G \times G \to G$, $(g_1, g_2) \to g_1g_2$

(2) $G \times G \to G$, $(g_1, g_2) \to g_1g_2g_1^{-1}$ (conjugation)

(3) $G \times G/H \to G/H$, $(g, aH) \to gaH$ (when H is not normal, $X = G/H$ is just a set.)

6.17 Orbits

6.17.1 Thm: Equivalence Relation: X is a G-set, $x_1 \sim x_2 \Leftrightarrow x_2 = gx_1,\ \exists g \in G$

Theorem 43. *For G acting on X, define a relation $\sim$ on X via*

$$x_1 \sim x_2 \Leftrightarrow x_2 = gx_1 \quad \textit{for some } g \in G$$

Definition 24. *A group G is **transitive** on a G-set X if for each $x_1, x_2 \in X$, there exists $g \in G$ such that $gx_1 = x_2$.*

6.17.2 Def: $Gx = \{gx|g \in G\}$ is the orbit of x

Definition 25. *For a group action G on X, X partitions into equivalence classes. Denote the class containing x by Gx. $Gx = \{gx|g \in G\}$ is called the orbit of $x \in X$.*

Denote: the partition of X as equivalence classes takes the form

$$X = Gx_1 \cup Gx_2 \cup \cdots Gx_r$$

r disjoint orbits.

6.17.3 Def: $G_x = \{g \in G|gx = x\}$ is the stabilizer of x

Definition 26. *Let G act on X, for $x \in X$, define $G_x = \{g \in G|gx = x\}$, then G_x is a subgroup of G called the **stabilizer** of x. (or the **isotropy subgroup** of x)*

6.17.4 Thm: if X is a G-set, stabilizer $G_x = \{g \in G|gx = x\}$ is subgroup of G, $\forall x \in X$

Let

$$X^g = \{x \in X|gx = x\};\ G_x = \{g \in G|gx = x\}$$

Theorem 44. *Let X be a G-set then G_x is a subgroup of G, $\forall x \in X$.*

Proof.

(1) Closed: $\forall g_1, g_2 \in G_x$, $(g_1 g_2)x = g_1(g_2 x) = g_1 x = x \Rightarrow g_1 g_2 \in G_x$.

(2) Identity: $ex = x$.

(3) Inverse: $gx = x$, $x = ex = g^{-1}gx = g^{-1}(gx) = g^{-1}x$.

□

6.17.5 Orbit-Stabilizer Theorem: $|Gx| = \frac{|G|}{|G_x|}$

Theorem 45. *Let G act on X, and let $x \in X$, then $|Gx| = [G : G_x] = |G/G_x| = \frac{|G|}{|G_x|}$*

Proof. Since G_x is the subgroup of G, according to largrange theorem we know $|G_x| \Big| |G|$.

For a $x_1 = g_1 x \in Gx$ with $g_1 \notin G_x = \{g \in G|gx = x\}$. $G_{x_1} = \{g \in G|gx_1 = x_1\} = \{g \in G|g_1^{-1}gg_1 x = x\}$.

Prove $g \to g_1^{-1}gg_1$ is one to one: assume $g_1^{-1}gg_1 = g_1^{-1}g'g_1$, $\Rightarrow g = g'$.

Hence, $|G_{x_1}| = |G_x| \Rightarrow \frac{|G|}{|G_x|} = |Gx|$ □

6.18 Applications of $G-$sets to Counting

As we showed before, the partition of X as equivalence classes takes the form

$$X = Gx_1 \cup Gx_2 \cup \cdots Gx_r$$

where r is the number of orbits in X.

6.18.1 Burnside's Formula: number of orbits in X: $r = \frac{1}{|G|}\sum_{g\in G}|X^g|$

Theorem 46. *Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G, then*

$$r = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

i.e. r equals to the average $|X^g|$, where $X^g = \{x : gx = x\}$

Proof. Since $G_{x_0} = \{g \in G | gx = x\} = \{(g, x)|gx = x, g \in G, x = x_0\}$,

$$\sum_{x\in X}|G_x| = |\{(g, x)|gx = x, g \in G, x \in X\}|$$

At the same time, $|X^{g_0}| = \{x \in X : gx = x\} = \{(g, x)|gx = x, g = g_0, x \in X\}$, then

$$\sum_{g\in G}|X^g| = |\{(g, x)|gx = x, g \in G, x \in X\}| = \sum_{x\in X}|G_x|$$

As we shoed before, $|G_x| = |G_y|, \forall x, y \in X$

$$\Rightarrow \sum_{x\in X}|G_x| = |G|\sum_{x\in X}\frac{1}{|Gx|} = |G|\sum_{i=1}^{r}\sum_{x\in Gx_i}\frac{1}{|Gx|} = |G|\sum_{i=1}^{r}\frac{|Gx_i|}{|Gx_i|} = |G|r$$
$$\Rightarrow r = \frac{\sum_{x\in X}|G_x|}{|G|} = \frac{\sum_{g\in G}|X^g|}{|G|}$$

□

6.18.2 Example: Counting

Example 39. *How many distinguishable necklaces (with no clasp) can be made using 7 different-colored beads of the same size?*

If two necklaces are transitive ($\exists g \in D_14$ s.t. $gx_1 = x_2$), they are in the same necklace. Hence, we want to count the number of orbits. $|X^1| = 7!$ and $|X^g| = 0, \forall g \neq 1 \in D_{14}$ Then,

$$r = \frac{|X^1|}{|D_14|} = \frac{7!}{14} = 360$$

Example 40. *Let X be the set of all 4-edge-colored equivalent triangle. Count the number of different coloring.*

$D_6 = \{(1), (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}$

$$\begin{array}{rcr} g & \# & |X^g| \\ (1) & 1 & 4^3 \\ \left.\begin{array}{r}(1,2)\\(2,3)\\(1,3)\end{array}\right\} & 3 & 4^2\text{(two points must be the same color, the other can be any color)} \\ \left.\begin{array}{r}(1,2,3)\\(1,3,2)\end{array}\right\} & 2 & 4\text{(three points must be the same color)} \end{array}$$

$$r = \frac{1 \cdot 4^3 + 3 \cdot 4^2 + 2 \cdot 4}{6} = 20$$

7 Ring and Field

7.1 Ring $(R, +, \cdot)$: $+$ is associative, commutative, identity, inverse $\in R$; $\cdot$ is associative, distributes over $+$

7.1.1 Def, Prop

Definition 27. *A ring is a nonempty set with two operations, called addition and multiplication, $(R, +, \cdot)$ such that*

(1): $(R, +)$ is an abelian group: i.e. $+$ is associatve and commucative. $0, -a \in R$
(2): $\cdot$ is associative.
(3): $\cdot$ distributes over $+$: $\forall a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$

Theorem 47. *If R is a ring with additive identity 0 , then for any $a, b \in R$ we have*
1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$.

7.1.2 $S \subset R$: Subring (closed under $+$ and $\cdot$; addictive inverse $-a \in S$)

Proposition 25 (Proposition 2.6.27)**.** *If $S \subset R$ is a subring, then $+, \cdot$ make S into a ring.*

7.1.3 Def: Commutative ring: ring's $\cdot$ is commutative

If "$\cdot$" is commutative, we call $(R, +, \cdot)$ a commutative ring.

7.1.4 Def: A ring with 1: the ring exists multiplication identity $1 \in R$

If there exists an element $1 \in R\backslash\{0\}$ such that $a1 = 1a = a$, $\forall a \in R$,then we say that R is a ring with 1 (a ring with unity).
Note: We usually discuss $1 \neq 0$. If $1 = 0$, $a = 1a = 0 \Rightarrow R = \{0\}$.

7.1.5 Def: In a ring R with 1, u is a <u>unit</u> if $\exists v \in R$ s.t. $uv = vu = 1$

Definition 28. *In a ring R with 1, u is a <u>unit</u> if it has a <u>multiplicative inverse</u> in R i.e. $\exists v \in R$ s.t. $uv = vu = 1$*

Example 41. *units in $\mathbb{Z}$ are $\{-1, +1\}$; in $\mathbb{Z}_n$ are $\{a \in \mathbb{Z}_n : gcd(a, n) = 1\}$*

7.1.6 Def: A ring with 1, R is a division ring if every nonzero element of R is a unit

Definition 29. *A ring with* 1*,* R *is a division ring if every nonzero element of* R *is a unit. This is equalivalent to* R *has identity and inverse in mutiplication.*

7.1.7 Def: Ring Homomorphism: $\phi(a+b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$

Definition 30. *Let* R, R' *be rings. A map* $\phi : R \to R'$ *is a ring homomorphism if*

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

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

7.1.8 Def: zero divisor: a $a \neq 0 \in R$ if $\exists b \neq 0 \in R$ s.t. $ba = 0$ or $ab = 0$

Definition 31. *A nonzero element* $a \in R$ *is called a zero divisor if there exists a nonzero* $b \in R$ *s.t.* $ba = 0$ *or* $ab = 0$

Note: Mutiplication cancellation law holds when no zero divisors.

7.1.9 Remark: In $\mathbb{Z}_n$, an element is either 0 or unit or zero divisor

Remark: In $\mathbb{Z}_n$, an element is either (1) 0, (2) a unit, (3) a zero divisor.
$0 \neq a \in \mathbb{Z}_n$ is a $\begin{cases} \text{unit} & \text{if } gcd(a,n) = 1 \\ \text{zero divisor} & \text{if } gcd(a,n) \neq 1 \end{cases}$
In $M_n(R)$ $\begin{cases} \text{unit} & \text{if } rank(A) = n \\ \text{zero divisor} & \text{if } rank(A) < n \end{cases}$
In $R = \mathbb{Z}$, $a \notin \{0, +1, -1\}$ is neither unit nor zero divisor.

7.1.10 Thm: $a \in \mathbb{Z}_n$ is a zero divisor $\Leftrightarrow gcd(a,n) \neq 1$.

Theorem 48. *In the ring* $\mathbb{Z}_n$*, the zero divisors are precisely those nonzero elements that are not relatively prime to* n*.*

7.1.11 Cor: $\mathbb{Z}_p$ has no zero divisors if p is prime.

7.1.12 Def: An integral domain is a commutative ring with $1 \neq 0$ that has no zero divisors

Definition 32. *An integral domain is a commutative ring with* $1 \neq 0$ *that has no zero divisors.*

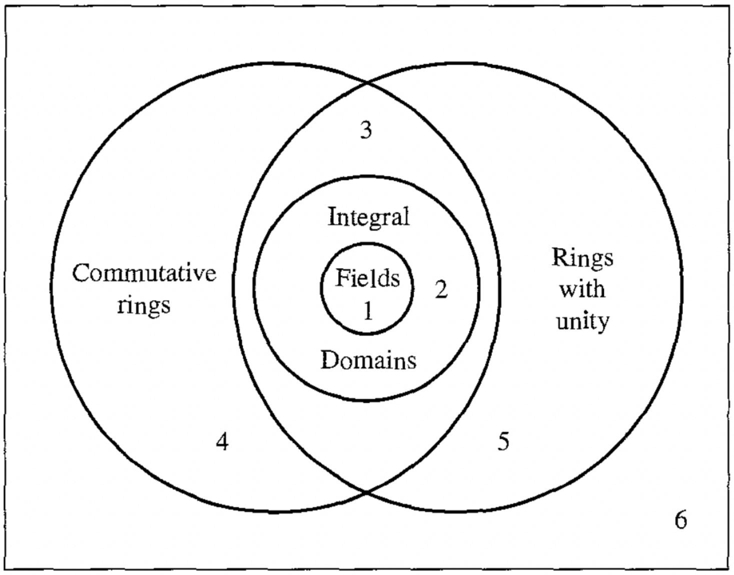
$\mathbb{Z}$ and $\mathbb{Z}_p$ for any prime p are integral domains, but $\mathbb{Z}_p$ is not an integral domain if n is not prime.

7.2 Field $\mathbb{F}$

7.2.1 Def: A field is a commutative division ring.

Definition 33. *A field is a commutative division ring.*

Which is equal to a ring satifies identity, inverse and commutative in multiplication. Field $(\mathbb{F}, +, \cdot)$ (close, associative, commutative, distributive(M over A), identity & inverse(M,A))
Note: nonzero elements of a finite field can form a cyclic (sufficient for abelian) mutiplication group.



19.10 Figure A collection of rings.

Figure 4: example: 1.$\mathbb{Z}_2, \mathbb{Q}$, 2.$\mathbb{Z}$, 3.$\mathbb{Z}_4$, 4.$2\mathbb{Z}$ 5.$M_2(\mathbb{Z})$,$M_2(\mathbb{R})$, 6.upper-triangular matrices with integer entries and all zeros on the main diagonal

7.2.2 Differences between "Field" and "Integral Domain"

Def: An integral domain is a commutative ring with $1 \neq 0$ that has no zero divisors
Def: A field is a commutative ring with $1 \neq 0$ that every nonzero element of R is a unit.

7.2.3 Lemma: A unit is not zero divisor

Proof. $a \in R$ is a unit and $\frac{1}{a}$ is its inverse.
Assume there exists $b \neq 0$ s.t. $ab = 0$, then

$$\begin{aligned}\frac{1}{a}(ab) &= \frac{1}{a}0 = 0\\ &= (\frac{1}{a}a)b = b\end{aligned}$$

Contradiction!
Assume there exists $b \neq 0$ s.t. $ba = 0$, then

$$\begin{aligned}(ba)\frac{1}{a} &= 0\frac{1}{a} = 0\\ &= b(a\frac{1}{a}) = b\end{aligned}$$

Contradiction! □

7.2.4 Lemma: A field doesn't has zero divisors

Since a field is a division ring, its nonzero elements are unit which is not zero divisor.

7.2.5 Thm: Every field is an integral domain

Theorem 49. *Every field is an integral domain.*

prove by previous lemma.

7.2.6 Thm: Every finite integral domain is a field

Theorem 50. *Every finite integral domain is a field.*

Proof. The only thing we need to show is that a typical element $a \neq 0$ has a multiplicative inverse. Consider $a, a^2, a^3, ...$ Since there are only finitely many elements we must have $a^m = a^n$ for some $m < n$.
Then $0 = a^m - a^n = a^m(1 - a^{n-m})$. Since there are no zero-divisors we must have $a^m \neq 0$ and hence $1 - a^{n-m} = 0$ and so $1 = aa^{n-m-1}$ and we have found a multiplicative inverse for a. □

7.2.7 Note: Finite Integral Domain $\subset$ Field $\subset$ Integral Domain

$\mathbb{Z}_p$ is a field.
$\mathbb{Z}$ is an integral domain but not a field.

7.3 The Characteristic of a Ring

7.3.1 Def: characteristic n is the least positive integer s.t. $n \cdot a = 0, \forall a \in R$

Definition 34. *If for a ring R a positive integer n exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the characteristic of the ring R. If no such positive integer exists, then R is of characteristic 0.*

Example 42. *The ring $\mathbb{Z}_n$ is of characteristic n, while $\mathbb{Z}, \mathbb{Q}, \mathbb{M}$, and $\mathbb{C}$ all have characteristic 0.*

7.3.2 Thm: In a ring with 1, characteristic $n \in \mathbb{Z}^+$ s.t. $n \cdot 1 = 0$

Theorem 51. *Let R be a ring with 1. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{Z}^+$, then the smallest such integer n is the characteristic of R.*

8 The Ring $\mathbb{Z}_n$ (Fermat's and Euler's Theorems)

8.1 Fermat's Theorem

8.1.1 Thm: nonzero elements in $\mathbb{Z}_p$ (p is prime) form a group under multiplication

Theorem 52. *The nonzero elements in $\mathbb{Z}_p$ (p is prime) form a group under multiplication.*

Proof. $\mathbb{Z}_p$ is a finite field. □

8.1.2 Cor: (Little Theorem of Fermat) $a \in \mathbb{Z}$ and p is prime not dividing a, then $a^{p-1} \equiv 1 \bmod p$ (p divides $a^{p-1} - 1$)

Corollary 10 (Little Theorem of Fermat)**.** *$a \in \mathbb{Z}$ and p is prime not dividing a, then $a^{p-1} \equiv 1 \bmod p$ (p divides $a^{p-1} - 1$)*

Proof. Let $G_p = \{a \in \mathbb{Z}_p : a \neq 0\}$, by previous theorem, we know the G_p is a group under multiplication of size $|G_p| = p - 1$.
Then the order of a should divde $|G_p| = p - 1$, then

$$a^{p-1} = 1 \in G_p \Rightarrow a^{p-1} \equiv 1 \bmod p$$

□

8.1.3 Cor: (Little Theorem of Fermat) If $a \in \mathbb{Z}$, then $a^p \equiv a \bmod p$ for any prime p

8.2 Euler's Theorem

Euler's Theorem is more general form of Fermat's Theorem.

8.2.1 Thm: $G_n = \{a \in \mathbb{Z}_n : gcd(a, n) = 1\}$ forms a group under multiplication

Theorem 53. *The set G_n of nonzero elements of $\mathbb{Z}_n$ that are not zero divisors ($G_n = \{a \in \mathbb{Z}_n : gcd(a, n) = 1\}$) forms a group under multiplication modulo n.*

8.2.2 Def: Euler phi function $\phi(n) = |G_n|$, where $G_n = \{a \in \mathbb{Z}_n : gcd(a, n) = 1\}$

More generally, any $n \in \mathbb{Z}^+$, $a^{p-1} \equiv 1 \bmod p$. Then G_n is a group under mutiplication of size $|G_n| = \phi(n)$, we set $\phi(n)$ be the Euler phi function. E.g.

$$\phi(8) = \#\{a \in \mathbb{Z}_8 : gcd(a, 8) = 1\} = 4$$
$$\phi(15) = \#\{1, 2, 4, 7, 8, 11, 13, 14\} = 8$$

8.2.3 Thm: (Euler's Theorem) If $a \in \mathbb{Z}$, $n \geq 2$ s.t. $gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \bmod n$

Theorem 54. *If a is an integer relatively prime to n, then $a^{\phi(n)} - 1$ is divisible by n, that is $a^{\phi(n)} \equiv 1 \bmod n$.*

Proof. order of a should divide $|G_n| = \phi(n)$ then $a^{\phi(n)} = 1 \in G_n \Rightarrow a^{\phi(n)} \equiv 1 \bmod n$ □

8.3 Application to $ax \equiv b \pmod m$

8.3.1 Thm: find solution of $ax \equiv b \pmod m$, $gcd(a, m) = 1$

Theorem 55. *$a, b \in \mathbb{Z}_m, gcd(a, m) = 1$, then $ax = b$ has a unique solution in $\mathbb{Z}_m$*

Proof. By Euler's Theorem, $a^{\phi(m)} \equiv 1 \bmod m$, which means a is a unit of $\mathbb{Z}_m$, there exists a unique $a^{-1} \in \mathbb{Z}_m$.
Mutiply $a^{-1} \in \mathbb{Z}_m$ on both side, we can get $x = a^{-1}b$ is the solution. □

8.3.2 Thm: $ax \equiv b \pmod m$, $d = gcd(a, m)$ has solutions if $d|b$, the number of solutions is d

Theorem 56. *Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let $d = gcd(a, m)$. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.*

8.3.3 Cor: $ax \equiv b$ (mod m), $d = gcd(a, m)$, $d|b$, then solutions are $((\frac{a}{d})^{\phi(\frac{m}{d})-1}\frac{b}{d} + k\frac{m}{d}) + (m\mathbb{Z})$, $\quad k = 0, 1, ..., d-1$

Corollary 11. *Let $d = gcd(a, m)$. The congruence $ax \equiv b$ (mod m) has a solution if and only if d divides b. When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m.*

Steps:

(1) let $a_1 = a/d$, $b_1 = b/d$, $m_1 = m/d$, solve

$$a_1 s \equiv b_1 \text{ mod } m_1 \Rightarrow s = a_1^{-1} b_1$$

where $a_1^{-1} = a_1^{\phi(m_1)-1}$

(2) Solutions are

$$(s + km_1) + (m\mathbb{Z}), \quad k = 0, 1, ..., d-1$$

Example 43. *Find all solutions of* $12x \equiv 27$ *mod* 18

d=gcd(12,18)=6, $d \nmid 27 \Rightarrow$ no solutions.

Example 44. *Find all solutions of* $15x \equiv 27$ *mod* 18

d=gcd(15,18)=3, $a_1 = 5, b_1 = 9, m_1 = 6$. Then $s = a_1^{-1} b_1 = 5 \cdot 9 = 3$, then solutions are $3 + 18\mathbb{Z}$, $9 + 18\mathbb{Z}$, $15 + 18\mathbb{Z}$

9 Ring Homomorphisms and Factor Rings

9.1 Ring Homomorphism

9.1.1 Def: Ring Homomorphism: $\phi(a+b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$

Definition 35. *Let R, R' be rings. A map $\phi : R \to R'$ is a <u>ring homomorphism</u> if*

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

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

Example 45 (Projection Homomorphisms)**.** *Let $R_1, R_2, ..., R_n$ be rings. For each i, the map π_i: $R_1 \times R_2 \times ... \times R_n \to R_i$ defined by $\pi_i(r_1, r_2, ..., r_n) = r_i$ is a homomorphism.*

9.1.2 Properties of Ring Homomorphism

1. $\phi(0) = 0'$.
2. $\phi(-a) = -\phi(a)$.
3. $S \subseteq R$ is a subring $\Rightarrow \phi(S) \subseteq R'$ is a subring.
4. $S' \subseteq R'$ is a subring $\Rightarrow \phi^{-1}(S') \subseteq R$ is a subring.
5. If $1 \in R$ is a unity of $R \Rightarrow \phi(1)$ is a unity of $\phi(R)$.

9.1.3 Def: kernel of ring homomorphism (the same as group homomorphism)

$$Ker(\phi) = \phi^{-1}[0'] = \{r \in R : \phi(r) = 0'\}$$

9.1.4 Thm: one-to-one map $\Leftrightarrow Ker(\phi) = \{0\}$

Similiarly, a ring homomorphism is one-to-one map if and only if $Ker(\phi) = \{0\}$.

9.2 Factor(Quotient) Rings

9.2.1 Thm: R/H is a ring for $H = ker\phi$ if operations well defined

Theorem 57. *Let $\phi : R \to R'$ be a ring homomorphism and let $H = ker\phi$. Then R/H is a ring under the operation.*

$$(a + H) + (b + H) = (a + b) + H$$
$$(a + H)(b + H) = ab + H$$

Also, $\mu : R/H \to \phi[R]$ defined by $\mu(a + H) = \phi(a)$ is an isomorphism.

9.2.2 Thm: $(a + H) + (b + H) = (a + b) + H$ well defined $\Leftrightarrow ah \in H, hb \in H, \forall a, b \in R, b \in H$

Theorem 58. *$(a + H) + (b + H) = (a + b) + H$ is well defined if and only if $ah \in H$ and $hb \in H$, $\forall a, b \in R, \forall h \in H$*

9.2.3 Def: $N < R$ is ideal $aN \subseteq N$ and $Nb \subseteq N$ $\forall a, b \in R$

Definition 36. *An addive subgroup N of a ring R is an **ideal** if $aN \subseteq N$ and $Nb \subseteq N$ $\forall a, b \in R$*

Example 46. *$n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$.*

9.2.4 Thm: N is ideal $\Rightarrow R/N$ is a ring

Theorem 59. *Let N be an ideal of a ring R. R/N is a ring with operations*

$$(a + H) + (b + H) = (a + b) + H$$
$$(a + H)(b + H) = ab + H$$

*We call this ring R/N is the **factor ring of** R **by** N*

9.2.5 Fundamental Homomorphism Theorem

Theorem 60. *Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then*

1. *$\phi[R]$ is a ring.*
2. *$\mu : R/N \to \phi[R]$ given by $\mu(x + N) = \phi(x)$ is an isomorphism.*
3. *$\gamma : R \to R/N$ given by $\gamma(x) = x + N$ is a homomorphism.*
4. *$\phi(x) = \mu\gamma(x), \quad \forall x \in R$*

9.2.6 Thm: $I, J \subset R$ be $R - ideals$ and $I + J = R \Rightarrow R/_{I\cap J} \cong R/_I \times R/_J$

Theorem 61. *Let R be a commutative ring with $1 \neq 0$, and $I, J \subset R$ be $R - ideals$ such that $I + J = R$ (I and J are relatively prime). Then,*

$$R/_{I\cap J} \cong R/_I \times R/_J$$

Moreover, $IJ = I \cap J$ and $R/_{IJ} \cong R/_I \times R/_J$

Proof. Using that $I + J = R$ and $1 \in R$, we can write $1 = x + y$, $x \in I, y \in J$.
The natural map (direct product of two projections) $R \to R/I \times R/J$ is a ring homomorphism. $(r \to (r + I, r + J))$.
The ring $R/I \times R/J$ is generated by the element $(1 + I, J), (I, 1 + J)$:

$$(a + I, b + J) = a(1 + I, J) + b(I, 1 + J)$$

Let $x + y = 1, x \in I, y \in J$

$$\begin{aligned} x &\to (x + I, x + J) = (I, 1 - y + J) = (I, 1 + J) \\ y &\to (y + I, y + J) = (1 - x + I, J) = (1 + I, J) \end{aligned}$$

Then $bx + ay = a(1 + I, J) + b(I, 1 + J)$. And $R \to R/I \times R/J$ is surjective.
We can prove that $I \cap J$ is the kernel of the ring $R/I \times R/J$:

$$\begin{aligned} r \to (r + I, r + J) \text{ maps } r \text{ to } (I, J) = 0 \in R/I \times R/J \\ \Leftrightarrow r \in I \text{ and } r \in J. \\ \Leftrightarrow r \in I \cap J. \end{aligned}$$

Then, according to the FHT $R/_{I \cap J} \cong R/_I \times R/_J$ if $I + J = R$.
Moreover, we can prove $I + J = R \Rightarrow IJ = I \cap J$.

1. $(IJ \subset I \cap J)$: From the definition of ideal $IJ \subset I$ and $IJ \subset J \Rightarrow IJ \subset I \cap J$
2. $(I \cap J \subset IJ)$: Let $1 = x + y, x \in I, y \in J, r \in I \cap J$, then

$$r = r \cdot 1 = r(x + y) = rx + ry = xr + ry \in IJ$$

□

10 Prime and Maximal Ideals

Every nonzero ring R has at least two ideals, the **improper ideal** R and the **trivial ideal** $\{0\}$. For these ideals, the factor rings are R/R, which has only one element, and $R/\{0\}$, which is isomorphic to R. These are uninteresting cases. Let's consider **proper nontrivial ideal** $N \subset R$.

10.1 Thm: N is R-ideal has a unit $\Rightarrow N = R$

Theorem 62. *If R is a ring with 1, and N is an ideal of R containing a unit, then $N = R$.*

Proof. Since N is ideal, $rN \subseteq N, \forall r \in R$. $r^{-1} \in N \Rightarrow 1 \in N \Rightarrow r \cdot 1 \in N, \forall r \in R \Rightarrow N = R$ □

10.1.1 Cor: Ideal of field F is $\{0\}$ or F

Corollary 12. *A field F contains no proper nontrivial ideals, i.e., ideal is $\{0\}$ or F.*

Proof. Every nonzero element of field is unit. □

10.2 Def: Maximal ideal: no other ideal properly contains it

Definition 37. *A proper ideal $M \subsetneq R$ is called **maximal** if*

$$M \subseteq I \subseteq R \Rightarrow M = I \text{ or } I = R \text{ (for } R\text{−ideal } I).$$

i.e, there is no other ideal properly containing M.

10.2.1 Thm: R comm ring with 1, M maximal ideal $\Leftrightarrow R/M$ is a field

Theorem 63. *Let R be a commutative ring with $1 \neq 0$. Then M is a maximal ideal of R if and only if R/M is a field.*

Example 47. *Since $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ and $\mathbb{Z}_n$ is a field if and only if n is prime. Then we see that maximal ideals are $p\mathbb{Z}$ where p is any positive prime.*

Example 48. *Let $R = \mathbb{Z}[x]$ has ideals $(2) = 2\mathbb{Z}[x] \subseteq R$, $(x) = x\mathbb{Z}[x] \subseteq R$, $(2, x) = 2\mathbb{Z}[x] + x\mathbb{Z}[x] \subseteq R$*

(1) *$R/(2) \cong \mathbb{Z}_2[x]$, $\mathbb{Z}_2[x]$ is not a field $\Rightarrow (2)$ is not maximal ideal.*

(2) *$R/(x) \cong \mathbb{Z}$, $\mathbb{Z}$ is not a field $\Rightarrow (x)$ is not maximal ideal.*

(3) *$R/(2, x) \cong \mathbb{Z}_2$, $\mathbb{Z}_2$ is a field $\Rightarrow (2, x)$ is maximal ideal.*

10.3 Def: Prime ideal: $ab \in P \Rightarrow a \in P$ or $b \in P$

Definition 38. *An ideal $P \subsetneq R$ in a commutative ring R is a **prime** ideal if $ab \in P \Rightarrow a \in P$ or $b \in P$.*

Note: $\{0\}$ is a prime ideal in $\mathbb{Z}$, and indeed in any integral domain.

Example 49. *$\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$, for if $(a, b)(c, d) \in \mathbb{Z} \times \{0\}$, then we must have $bd = 0$, then either $(a, b) \in \mathbb{Z} \times \{0\}$ or $(c, d) \in \mathbb{Z} \times \{0\}$*

10.3.1 Thm: N prime ideal $\Leftrightarrow R/N$ is an integral domain

Theorem 64. *Let R be a commutative ring with 1, and let $N \subsetneq R$ be an ideal in R. Then R/N is an integral domain if and only if N is a prime ideal in R.*

R/N is an integral domain: $(aN)(bN) = 0, (an_1)(bn_2) = 0, a, b \in R, \forall n_1, n_2 \in N$ where $an_1 \in N, bn_2 \in N$ since N is an ideal.

10.3.2 Cor: maximal ideal $\Rightarrow$ prime ideal

Corollary 13. *Every maximal ideal in a commutative ring R with 1 is a prime ideal.*

10.4 Relation Summary

$$\begin{array}{lcl} I \text{ is maximal} & \Leftrightarrow & R/I \text{ is a field} \\ \Downarrow & & \Downarrow \\ I \text{ is prime} & \Leftrightarrow & R/I \text{ is an integral domain} \end{array}$$

10.5 Thm: homomorphism $\phi : \mathbb{Z} \to R$, $\phi(n) = n \cdot 1$

Theorem 65. *If R is a ring with unity 1, then the map $\phi : \mathbb{Z} \to R$ given by*

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

for $n \in \mathbb{Z}$ is a homomorphism of $\mathbb{Z}$ into R.

10.5.1 Cor: Ring R 1. characteristic $n > 1 \Rightarrow$ has subring isomorphic to $\mathbb{Z}_n$ 2. characteristic $0 \Rightarrow$ has subring isomorphic to $\mathbb{Z}$

Corollary 14. *If R is a ring with 1 and characteristic $n > 1$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If R has characteristic 0, then R contains a subring isomorphic to $\mathbb{Z}$.*

Review: Characteristic n is the least positive integer s.t. $n \cdot a = 0, \forall a \in R$

10.5.2 Thm: Field F 1. prime characteristic $p \Rightarrow$ has subfield isomorphic to $\mathbb{Z}_p$ 2. characteristic $0 \Rightarrow$ has subfield isomorphic to $\mathbb{Q}$

Theorem 66. *A field F is either of prime characteristic p and contains a subfield isomorphic to $\mathbb{Z}_p$ or of characteristic 0 and contains a subfield isomorphic to $\mathbb{Q}$.*

Definition 39. *We define $\mathbb{Z}_p$ and $\mathbb{Q}$ are prime fields.*

10.6 Def: Pricipal ideal (of comm ring R) generated by a: $\langle a \rangle = \{ra | r \in R\}$

Definition 40. *If R is a commutative ring with 1 and $a \in R$, the ideal $\{ra | r \in R\}$ of all multiples of a is the **principal ideal generated by** a and is denoted by $\langle a \rangle$. An ideal N of R is a **principal ideal** if $N = \langle a \rangle$ for some $a \in R$.*

Example 50. *Every ideal of the ring $\mathbb{Z}$ is of the form $k\mathbb{Z}$, which is generated by k, so every ideal of $\mathbb{Z}$ is a principal ideal.*

Example 51. *The ideal $\langle x \rangle$ in $F[x]$ consists of all polynomials in $F[x]$ having zero constant term.*

10.6.1 Thm: field F, every ideal in $F[x]$ is principal

Theorem 67. *If F is a field, every ideal in $F[x]$ is principal.*

Proof. Let N be an ideal of $F[x]$.

1. If $N = \{0\}$, then $N = \langle 0 \rangle$.
2. If $N \neq \{0\}$, and let $g(x)$ be a nonzero element of N of minimal degree.

   If $g(x)$ is constant (degree 0), then $g(x) \in F$ is a unit $\Rightarrow N = \langle 1 \rangle = F[x]$.

   If degree of $g(x) \geq 1$, then for all $f(x) \in N$, $\exists q(x), r(x)$ s.t. $f(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or degree $r(x) <$ degree $g(x)$. Since $g(x)$ has minimal degree, $r(x) = 0 \Rightarrow f(x) = g(x)q(x) \Rightarrow N = \langle g(x) \rangle$

□

10.6.2 Thm: principal ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal $\Leftrightarrow p(x)$ is irreducible

Theorem 68. *An ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is irreducible over F.*

Proof.

1. "$\Rightarrow$": Suppose $\langle p(x) \rangle$ is a maximal ideal of $F[x]$. Then $\langle p(x) \rangle \neq F[x]$, so $p(x) \notin F$. Assume $p(x)$ can be factorizaed $p(x) = f(x)g(x)$. Since $\langle p(x) \rangle$ is a maximal idea, it is also a prime ideal. Then $f(x) \in \langle p(x) \rangle$ or $g(x) \in \langle p(x) \rangle$, which is impossible since degree of $f(x)$ and $g(x)$ are both less than the degree of $p(x)$. Hence, $p(x)$ is irreducible.

2. "$\Leftarrow$": $p(x)$ is irreducible over F. Suppose N is an ideal of $F[x]$ s.t. $\langle p(x)\rangle \subseteq N \subseteq F[x]$. According to previous theorem, we know that N is a principal ideal. So, $N = \langle g(x)\rangle$ for some $g(x) \in F$. Since $p(x) \in F[x]$, $p(x) = g(x)q(x)$ for some $q(x) \in F[x]$. As we set $p(x)$ is irreducible, so degree $g(x) = 0$ or degree $q(x) = 0$. If degree $g(x) = 0$, $g(x) \in F$, $g(x)$ is a unit in $F[x] \Rightarrow N = \langle g(x)\rangle = F[x]$. If degree $q(x) = 0$, $q(x) \in F$ is a unit, so $q^{-1}(x) \in F$ $\Rightarrow g(x) = p(x)q^{-1}(x) \Rightarrow N = \langle g(x)\rangle = \langle p(x)\rangle$

□

11 The Field of Quotients of an Integral Domain

Let D be an integral domain (a ring with 1 has no zero divisors) that we desire to enlarge to a field of quotients F. A coarse outline of the steps we take is as follows:

11.1 Step 1. Define what the elements of F are to be. (Define $S/\sim$)

D is the given integral domain, $S = \{(a,b)|a,b \in D, b \neq 0\} < D \times D$

11.1.1 Def: equivalent relation $(a,b) \sim (c,d) \Leftrightarrow ad = bc$

Definition 41. *Two elements (a,b) and (c,d) in S are equivalent, denoted by $(a,b) \sim (c,d)$, if and only if $ad = bc$.*
Note: we can image it as $\frac{a}{b} = \frac{c}{d}$, but don't use this form.

Lemma 4. *$\sim$ defines an equivalence relation on S.*

Proof. easy to prove (1) reflexive, (2) symmetric, (3) transitive. □

11.2 Step 2. Define the binary operations of addition and multiplication on $S/\sim$.

The relation $\sim$ can define a set of all equvalence classes on $[(a,b)], (a,b) \in S$, $S/\sim = \{[(a,b)]|(a,b) \in S\}$

11.2.1 lemma: well-defined operations $+, \times$

Lemma 5. *For $[(a,b)]$ and $[(c,d)]$ in $S/\sim$, the equations*

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$

and

$$[(a,b)][(c,d)] = [(ac, bd)]$$

give well-defined operations of addition and multiplication on $S/\sim$.

Proof. Assume $(a_1,b_1) \sim (a,b)$, $(c_1,d_1) \sim (c,d)$.
Verify $+ : (ad + bc, bd) \sim (a_1d_1 + b_1c_1, b_1d_1)$

□

11.3 Step 3. Check all the field axioms to show that F is a field under these operations.

11.3.1 Thm: $S/\sim$ is a field with $+, \times$

Theorem 69. *With operation $+, \times$. $S/\sim$ is a field.*

Proof. Check all field axioms:

$$\begin{aligned} Associative :+ : & \quad \checkmark \quad && \times : \checkmark \\ Identity :+ : & \quad [(0,1)] \quad && \times : [(1,1)] \end{aligned}$$

$[(a,b)] + [(0,1)] = [(a,b)]$, $[(a,b)][(1,1)] = [(a,b)]$

$$Inverse :+ : \quad [(-a,b)] \qquad \times : [(b,a)], \forall a \neq 0$$

$[(a,b)] + [(-a,b)] = [(0,b^2)] = [(0,1)]$, where $(0,b^2) \sim (0,1) \Leftrightarrow 0 * 1 = b^2 * 0$;
$[(a,b)][(b,a)] = [(ab,ab)] = [(1,1)]$

$$\begin{aligned} Commucative :+ : & \quad \checkmark \qquad \times : \checkmark \\ \text{Distributive laws :} & \quad \checkmark \end{aligned}$$

□

11.4 Step 4. Show that F can be viewed as containing D as an integral subdomain.

11.4.1 Lem: $\phi(a) = [(a,1)]$ is an isomorphism between D and $\{[(a,1)] | a \in D\}$

Lemma 6. *The map $\phi : D \to F = S/\sim$ given by $\phi(a) = [(a,1)]$ is an isomorphism of D with a subring of $F (= S/\sim)$.*

Proof.

$$\begin{aligned} \phi(a+b) &= [(a+b,1)] = [(a,1)] + [(b,1)] \\ \phi(ab) &= [(ab,1)] = [(a,1)][(b,1)] \end{aligned}$$

Injective: assume $\phi(a) = \phi(b)$, then

$$[(a,1)] = [(b,1)] \Leftrightarrow (a,1) \sim (b,1) \Leftrightarrow a = b$$

Surjective: $\forall [(a,1)]$ is mapped from a
We prove that ϕ is an isomorphism between D and $\{[(a,1)] | a \in D\}$. □

11.4.2 Thm: every element of F can be expressed as a quotient of two elements of D: $[(a,b)] = \frac{\phi(a)}{\phi(b)}$

$\forall [(a,b)] \in F$,

$$[(a,b)] = [(a,1)][(1,b)] = \frac{[(a,1)]}{[(1,b)]^{-1}} = \frac{[(a,1)]}{[(b,1)]} = \frac{\phi(a)}{\phi(b)}$$

Theorem 70. *Any integral domain D can be enlarged to (or embedded in) a field $F = S/\sim$ such that every element of F can be expressed as a quotient of two elements of D. (Such a field F is a* ***field of quotients*** *of D.)*

12 Polynomials

12.1 Def: Polynomials

Let R be any field. A polynomial over R in variable x is a formal sum:

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n = \sum_{i=0}^{n} a_ix^i$$

where $n \geq 0$ is an integer, $a_1, a_1, ..., a_n \in \mathbb{F}$.
Polynomial is a squence $\{a_k\}_{k=0}^{\infty}$ with $a_m = 0, \forall m > n$.
Remark: $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ If $a_d \neq 0$ and $a_i = 0, \forall i > d$, d is the degree of $f(x)$.

12.2 Rings of Polynomials

12.2.1 Thm: $R[x]$ is a ring under addition and multiplication

Theorem 71. *The set $R[x]$ of all polynomials in an indeterminate x with coefficients in a ring R is a ring under polynomial addition and multiplication.*
Note: If R is commutative, then so is $R[x]$, and if R has unity $1 \neq 0$. then 1 is also unity for $R[x]$.

Let $R[x]$ denote the set of all polynomials with coefficients in the ring R.

$$R[x] = \{\sum_{i=0}^{n} a_ix^i | n \geq 0, n \in \mathbb{Z}, a_0, ..., a_n \in R\}$$

We call the $R[x]$ *polynomial ring* over the ring R.

$$f = \sum_{i=0}^{n} a_ix^i, g = \sum_{j=0}^{n} a_jx^j \in R[x]$$
$$f + g = \sum_{i=0}^{n} (a_i + b_i)x^i \in R[x]$$
$$fg = (\sum_{i=0}^{n} a_ix^i)(\sum_{j=0}^{n} a_jx^j) = \sum_{i=0}^{2n}(\sum_{j=0}^{i} a_jb_{i-j})x^i$$

12.2.2 Def: evaluation homomorphism

Definition 42. *Let F be a field, and let $\alpha \in F$. Define an evaluation map. $EV_{x=\alpha} : F[x] \to F$, $\phi_\alpha(\sum_{i=0}^{\infty} a_ix^i) = \sum_{i=0}^{\infty} a_i\alpha^i$. Then,*

$$\phi_\alpha(f(x) + g(x)) = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$$
$$\phi_\alpha(f(x)g(x)) = \phi_\alpha(f(x))\phi_\alpha(g(x))$$

ϕ_α is a ring homomorphism. We call it evaluation homomorphism.

Example 52. *Consider $EV_{x=2} : \mathbb{Q}[x] \to \mathbb{Q}$. $EV_{x=2}$ is a ring homomorphism. In particular it is a group homomorphism for addition.*

$$\phi_2\left(a_0 + a_1x + \cdots + a_nx^n\right) = a_0 + a_12 + \cdots + a_n2^n$$

Note that

$$\phi_2\left(x^2 + x - 6\right) = 2^2 + 2 - 6 = 0.$$

Thus $x^2 + x - 6$ is in the kernel N of ϕ_2. Of course,

$$x^2 + x - 6 = (x - 2)(x + 3),$$

and the reason that $\phi_2\left(x^2 + x - 6\right) = 0$ is that $\phi_2(x - 2) = 2 - 2 = 0$.

Example 53. *Compute $EV_{x=4}(3x^{106} + 5x^{99} + 2x^{53}) \in \mathbb{Z}_7[x]$*

$$EV_{x=4}(3x^{106} + 5x^{99} + 2x^{53}) =$$

According to the little Theorem of Fermat, $x^6 \equiv 1$ mod 7.

$$= 3x^4 + 5x^3 + 2x^5 = 0 \in \mathbb{Z}_7$$

12.2.3 Def: α is zero if $EV_{x=\alpha}(f(x)) = 0$

Definition 43. *We say that α is a zero of $f(x)$ if $EV_{x=\alpha}(f(x)) = 0$.*

Example 54. *Find all zeros of $f(x) = x^3 + 2x + 2$ in $\mathbb{Z}_7$.*
Solve by checking all value $f(x), x = 0, 1, ..., 6 \Rightarrow$ zeros are $x = 2$, $x = 3$.

12.3 Degree of a Polynomial: $deg(f)$

$f = \sum_{i=0}^{n} a_i x^i$, $deg(f) =$ degree of f is,

$$deg(f) = \begin{cases} 0 & \text{if } f \text{ is constant, } f \neq 0 \\ n & \text{if } a_n \neq 0 \text{ in above } (a_n = \text{leading coefficent}) \\ -\infty & \text{if } f = 0 \end{cases}$$

Define $-\infty + a = a + (-\infty) = -\infty \ \forall a \in \mathbb{Z} \cup \{-\infty\}$

12.3.1 Lemma 2.3.3: $deg(fg) = deg(f) + deg(g)$, $deg(f + g) \leq \max\{deg(f), deg(g)\}$

Lemma 7 (Lemma 2.3.3)**.** *For any field $\mathbb{F}$ and f , $g \in \mathbb{F}[x]$,*

$$deg(fg) = deg(f) + deg(g)$$
$$deg(f + g) \leq \max\{deg(f), deg(g)\}$$

12.4 Corollary 2.3.5: Unit(invertible) in $\mathbb{F}[x]$: constant$\neq 0$ iff $deg(f) = 0$

Corollary 15 (Corollary 2.3.5)**.** *For any field $\mathbb{F}$ and $f \in \mathbb{F}[x]$, Then f is a unit(i.e. invertible) in $\mathbb{F}[x]$ iff $deg(f) = 0$.*

Proof.
Obviously, $deg(f) = 0 \Rightarrow$ f is a unit.
Suppose f is a unit, i.e. $\exists g \in \mathbb{F}[x]$ s.t. $fg = 1$.
$0 = deg(fg) = deg(f) + deg(g) \Rightarrow deg(f), deg(g) \geq 0 \Rightarrow deg(f) = 0, deg(g) = 0$. □

12.5 Irreducible Polynomials:

A nonconstant polynomial f is irreducible if $f = uv$, $u, v \in \mathbb{F}[x]$, then either u or v is a unit(i.e., constant$\neq 0$)

12.6 Theorem 2.3.6: nonconstant polynomials can be reduced uniquely

Theorem 72 (Theorem 2.3.6). *Suppose $\mathbb{F}$ is a field and $f \in \mathbb{F}[x]$ is any nonconstant. Then $f = ap_1p_2 \dots p_k$ where $a \in \mathbb{F}$, $p_1, \dots p_k \in \mathbb{F}[x]$ are irreducible monic polynomials (monic = i.e. leading coeff. 1). If $f = bq_1q_2 \dots q_r$ with $b \in \mathbb{F}$ and $q_1, q_2, \dots, q_r \in \mathbb{F}[x]$ monic irreducible, then $a = b, k = r$, and after reindexing $p_i = q_i$, $\forall i$*

Lemma 8 (Lemma 2.3.7). *Suppose $\mathbb{F}$ is a field and $f \in \mathbb{F}[x]$ is nonconstant monic polynomial. Then $f = p_1p_2 \dots p_k$ where each p_i is monic irreducible.*

Proof.
Prove it by induction. When $deg(f) = 1$, $f = uv$, $u, v \in \mathbb{F}[x]$, $deg(f) = deg(u) + deg(v) \Rightarrow$ one of these is 0.
Suppose the lemma holds for all degree$< n$. When $deg(f) = n$,
Either f is irreducible, done.
Suppose $f = uv$ with/ $deg(u), deg(v) \geq 1$
$\Rightarrow deg(u), deg(v) < n \Rightarrow u = p_1p_2 \dots p_k, v = q_1q_2 \dots q_j$ So, $f = p_1p_2 \dots p_kq_1q_2 \dots q_j$. □

Example 55. *$x^2 - 1 \in \mathbb{Q}[x]$ reducible*
$x - 1, x + 1 \in \mathbb{Q}[x]$ irreducible
$x^2 + 1 \in \mathbb{Q}[x]$ irreducible
$x^2 + 1 \in \mathbb{C}[x]$ reducible
$x^2 - 1 = x^2 + 1 = [1]x^2 + [1] \in \mathbb{Z}_2[x]$ reducible

13 Divisibility of Polynomials

Proposition 26 (Proposition 2.3.8). *$f, h, g \in \mathbb{F}[x]$, then*

(i) If $f \neq 0, f|0$
(ii) If $f|1$, f is nonzero constant
(iii) If $f|g$ and $g|f$, then $f = cg$ for some $c \in \mathbb{F}$
(iv) If $f|g$ and $g|h$, then $f|h$
(v) If $f|g$ and $f|h$, then $f|(ug + vh)$ for all $u, v \in \mathbb{F}[x]$.

13.1 Thm: Euclidean Algorithm of polynomials

Theorem 73. *For nonzero elements in $\mathbb{F}[x]$, $m > 0$*

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0$$
$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \dots + b_0$$

Then there are unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Simplify: Given $f, g \in \mathbb{F}[x]$, $g \neq 0$, then $\exists q, r \in \mathbb{F}[x]$ s.t. $deg(r) < deg(g)$ and $f = qg + r$

Example 56.

$$f = 3x^3 - 5x^2 - 3x + 5, g = x^3 - 2x^2 + 1 \in \mathbb{Q}[x]$$
$$f = 3g + x^2 - 3x + 2$$

$f, g \in \mathbb{F}[x], f \neq 0$, f divides g, $f|g$ means $\exists u \in \mathbb{F}[x]$ s.t. $g = fu$.

13.2 Cor: a is a zero of $f(x) \Leftrightarrow (x-a)|f(x)$

Corollary 16. *An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $(x-a)|f(x)$.*

Proof method 2. Suppose surjective homomorphism $\phi_a : F(x) \to F$ with $f(x) \to f(a)$
By defition of kernel $f(a) = 0 \Leftrightarrow f(x) \in ker\phi_a$.
Then we have $\langle (x-a) \rangle \subseteq ker\phi_a \subsetneq F[x]$, where $\langle (x-a) \rangle = \{ra | r \in F[x]\}$. Since $x-a$ is irreducible, then $\langle (x-a) \rangle$ is a maximal ideal of $F[x]$. Then $\langle (x-a) \rangle = ker\phi_a$
Thus

$$\begin{aligned} & f(a) = 0 \\ \Leftrightarrow & f(x) \in ker\phi_a \\ \Leftrightarrow & f(x) \in \langle (x-a) \rangle \\ \Leftrightarrow & (x-a)|f(x) \end{aligned}$$

□

13.3 Cor: Finite subgroup of multiplicative $F \backslash \{0\}$ is cyclic

Corollary 17. *If G is a finite subgroup of the multiplicative group $F^* = F \backslash \{0\}$ of a field F, then G is cyclic. (In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.)*

Proof. □

13.3.1 Greatest common divisor of f and g: is not unique, we denote monic Greatest common divisor as $gcd(f, g)$

If $f, g \in \mathbb{F}[x]$ are nonzero polynomials, a greatest common divisor of f and g is a polynomial $h \in \mathbb{F}[x]$ such that
(i) $h|f$ and $h|g$, and
(ii) if $k \in \mathbb{F}[x]$ and $k|f$ and $k|g$, then $k|h$.
the gcd is not unique, but the monic gcd is unique. We call it **the monic greatest common divisor**, denote it $gcd(f, g)$.

Example 57.

$$\begin{aligned} & x^2 - 1, x^2 - 2x + 1 \in \mathbb{Q}[x] \\ & (x-1)(x+1), (x-1)^2 \in \mathbb{Q}[x] \\ & x - 1 = gcd(x^2 - 1, x^2 - 2x + 1) \end{aligned}$$

13.3.2 Proposition 2.3.10:

Proposition 27 (Proposition 2.3.10)**.** *Any 2 nonzero polynomials $f, g \in \mathbb{F}[x]$ have a gcd in $\mathbb{F}[x]$. In fact among all polynomials in the set $M = \{uf + vg | u, v \in \mathbb{F}[x]\}$ any nonconstant of minimal degree are gcds.*

Proof.
$h \in M$, $deg(h) = d$ minimal. Let $k|f$ and $k|g \Rightarrow k|uf + vg, \ \forall u, v \Rightarrow k|h$.
Suppose $h' \in M$ is any nonzero element. $deg(h') \geq deg(h) \Rightarrow \ \exists q, r \in \mathbb{F}, deg(r) < deg(h) \ h' = qh + r$. $r = h' - qh \in M$. Since $deg(h) = d$ is nonconstant minimal degree, $r = 0 \Rightarrow h' = qh$. So $\exists q_1, q_2 \in \mathbb{F}[x], \ 1f + 0g = q_1 h, 0f + 1g = q_2 h \Rightarrow h|g, h|f$. □

Example 58.

$$
\begin{aligned}
&f = 3x^3 - 5x^2 - 3x + 5, g = x^3 - 2x^2 + 1 \in \mathbb{Q}[x] \\
&f = 3g + x^2 - 3x + 2 \\
&g = (x+1)(x^2 - 3x + 2) + x - 1 \\
&x^2 - 3x + 2 = (x-2)(x-1) \\
&\Rightarrow gcd(f, g) = x - 1 \\
&x - 1 = g - (x+1)(x^2 - 3x + 2) = g - (x+1)(f - 3g) = (3x+4)g - (x+1)f
\end{aligned}
$$

Example 59. *Find a greatest common divisor of $f = x^3 - x^2 - x + 1$ and $g = x^2 - 3x + 2$ in $\mathbb{Q}[x]$, and express it in form $uf + vg,\ u, v \in \mathbb{Q}[x]$.*

$$
\begin{aligned}
&f = (x+2)g + 3x - 3 \\
&g = \frac{1}{3}(x-2)(3x-3) \\
&gcd(f, g) = 3x - 3 \\
&3x - 3 = f - (x+2)g
\end{aligned}
$$

13.3.3 Proposition 2.3.12: $gcd(f, g) = 1, f|gh \Rightarrow f|h$

Proposition 28 (Proposition 2.3.12)**.** *If $f, g, h \in \mathbb{F}[x]$, $gcd(f, g) = 1$, and $f|gh$, then $f|h$.*

13.3.4 Corollary 2.3.13: irreducible f, $f|gh \Rightarrow f|g$ or $f|h$

Corollary 18 (Corollary 2.3.13)**.** *If $f \in \mathbb{F}[x]$ is irreducible, and $f|gh$, then $f|g$ or $f|h$.*

Since f is irreducible, we have two possible situations:
1. $gcd(f, g) = f$, i.e. $f|g$ done.
2. $gcd(f, g) = 1$, then according to Prop 2.3.12, we can know $f|h$.

13.4 Roots

Root:$\alpha \in \mathbb{F}$ is a root of f if $f(\alpha) = 0$.

13.4.1 Corollary 2.3.16(of Euclidean Algorithm): f can be divided into $(x-\alpha)q+f(\alpha)$i.e. if α is a root, then $(x-\alpha)|f$

Corollary 19 (Corollary 2.3.16(of Euclidean Algorithm))**.** *$\forall f \in \mathbb{F}[x]$ and $\alpha \in \mathbb{F}$, there exists a polynomial $q \in \mathbb{F}[x]$ s.t. $f = (x-\alpha)q + f(\alpha)$. In particular , if α is a root, then $(x-\alpha)|f$.*

13.5 Multiplicity

If α is a root of f , say its *multiplicity* is m, if $x - \alpha$ appears m times in irreducible factorization.

13.5.1 *Sum of multiplicity* $\leq deg(f)$

Proposition 29 (Proposition 2.3.17)**.** *Given a nonconstant polynomial $f \in \mathbb{F}[x]$, the number of roots of f, counted with multiplicity, is at most $deg(f)$.*

13.6 Roots in a filed may not in its subfield

Note if $\mathbb{F} \subset \mathbb{K}$, then $\mathbb{F}[x] \subset \mathbb{K}$. $f \in \mathbb{F}[x]$ may have no roots in $\mathbb{F}$, but could have roots in $\mathbb{K}$

Example 60. *$x^n - 1 \in \mathbb{Q}[x]$ has a root in $\mathbb{Q}$: 1; has 2 roots if n even: ± 1*
roots in $\mathbb{C}$: $\zeta_n = e^{\frac{2\pi i}{n}}$, then $\zeta_n^n = e^{2\pi i} = 1$; $(\zeta_n^k)^n = e^{2\pi k i} = 1$ So, the roots: $\{e^{\frac{2\pi k i}{n}} | k = 0, ..., n-1\}$
The roots of $x^n - d$: $\{e^{\frac{2\pi k i}{n}} \sqrt{d} | k = 0, ..., n-1\}$

14 Sylow Theorems

14.1 Def: $p-$group

Definition 44. *A group of order p^n, p is prime, for some $\alpha > 0$, is called $p-$group.*

14.2 Sylow Theorems

1) **First Sylow Theorem:** If G is a finite group of order $p^\alpha m$, $gcd(p, m) = 1$, then it conatins a subgroup H of order p^α. H is called a Sylow $p-$subgroup.

2) **Second Sylow Theorem:** Any two Sylow $p-$subgroups of group G are conjugate.
   (H_1 and H_2 are conjugate of G if $\exists g \in G$ s.t. $H_1 = gH_2g^{-1}$)

3) **Third Sylow Theorem:** The number of Sylow $p-$subgroups of a group G is 1 modulo p.

Example 61. $G = S_4, |G| = 4! = 2^3 \cdot 3$

1. *First Sylow Theorem:* Contains subgroup of order 8. (D_8)
2. *Second Sylow Theorem:* There are three kinds of D_8: begin with $(1, 3, 2, 4)/(1, 2, 3, 4)/(1, 2, 4, 3)$ are conjugate to each other.
3. *Third Sylow Theorem:* $3 \equiv 1 \bmod 2$

14.3 Thm: finite $H, K \leq G$, $|HK| = \frac{|H||K|}{|H \cap K|}$

Proposition 30. *For finite subgroups $H, K \leq G$, define $HK = \{hk : h \in H, k \in K\}$.*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

14.4 Group action by conjugation

Definition 45 (Group action by conjugation)**.** *Let X be the set of all subgroups of a group G, G acts on X by conjugation*

$$(g, H) \to gHg^{-1} \in X$$

$g \in G, \ H \in X$

The **stabilizer** of this action is called the **normalizer** of H in G

$$N_G(H) = \{g \in G : gHg^{-1} = H\} = \{g \in G : gH = Hg\}$$

14.5 Lemma: $K \leq N_G(H) \Rightarrow HK \leq G$

Lemma 9. *If $K \leq N_G(H)$, then HK is a subgroup of G*

Proof. Let $a = h_k k_1$, $b = h_2 k_2$, then

$$ab = h_1 k_1 h_2 k_2 = h_1(k_1 h_2 k_1^{-1}) k_1 k_2, \text{ where } k_1 h_2 k_1^{-1} \in H \Rightarrow ab \in HK$$
$$a^{-1} = (h_1 k_1)^{-1} = (k_1^{-1} h_1^{-1} k_1) k_1^{-1}, \text{ where } k_1^{-1} h_1^{-1} k_1 \in H \Rightarrow ab \in HK$$

□

14.6 Cor: if $H \lhd N_g(H) \leq G$, # subgroups of G conjugate to H is $[G : N_G(H)]$

Corollary 20. *By the Orbit-Stabilizer Theorem, if $H \lhd N_g(H) \leq G$, then the number of subgroups in G conjugate to H is $[G : N_G(H)]$.*

Example 62. $H = \langle (1, 2, 3, 4) \rangle \lhd D_8 \leq S_4$, $[S_4 : D_8] = 3$

S_4 has 3 subgroups conjugate to H: $\langle (1, 2, 3, 4) \rangle, \langle (1, 3, 4, 2) \rangle, \langle (1, 4, 2, 3) \rangle$

14.7 Center $Z(G) = \{a \in G : ag = ga, \forall g \in G\} = \{a \in G : gag^{-1} = a, \forall g \in G\}$

Size of orbit of a is 1 $\Leftrightarrow a \in Z(G)$

14.8 Class Equation: $|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(g_i)|}$

Let G act on itself by conjugate and $C_G(g_i)$ is the stabilizer of $g_i \in G$ under conjugation. Orbits of g_i of size > 1.

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(g_i)|}$$

Prove by Orbit-Stabilizer Theorem. Every element $a \in Z(G)$, $|Ga| = \frac{|G|}{|C_G(a)|} = 1$. G is the union of all orbits.

15 Euclidean geometry basics

15.1 Euclidean distance, inner product

Euclidean distance on $\mathbb{R}^n$:

$$|x - y| = \sqrt{(x_1 - y_1)^2 + ... + (x_n - y_n)^2}$$

Euclidean inner product:

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n = x^T y$$

15.2 Isometry of $\mathbb{R}^n$: a bijection $\mathbb{R}^n \to \mathbb{R}^n$ preserves distance

An **isometry** of $\mathbb{R}^n$ is a bijection $\Phi : \mathbb{R}^n \to \mathbb{R}^n$ that preserves distance, which means,

$$|\Phi(x) - \Phi(y)| = |x - y|, \ \forall x, y \in \mathbb{R}^n$$

15.2.1 $Isom(\mathbb{R}^n)$: set of all isometries of $\mathbb{R}^n$

We use $Isom(\mathbb{R}^n)$ denotes the set of all isometries of $\mathbb{R}^n$,

$$Isom(\mathbb{R}^n) = \{\Phi : \mathbb{R}^n \to \mathbb{R}^n || \Phi(x) - \Phi(y)| = |x - y|, \ \forall x, y \in \mathbb{R}^n\}$$

15.2.2 $Isom(\mathbb{R}^n)$ is closed under $\circ$ and inverse

Proposition 31. *$\Phi, \Psi \in Isom(\mathbb{R}^n)$, then $\Phi \circ \Psi, \Phi^{-1} \in Isom(\mathbb{R}^n)$*

Proof.
Since Φ, Ψ are bijections, so is $\Phi \circ \Psi$. Moreover,

$$|\Phi \circ \Psi(x) - \Phi \circ \Psi(y)| = |\Phi(\Psi(x)) - \Phi(\Psi(y))| = |\Psi(x) - \Psi(y)| = |x - y|$$

Since $id \in Isom(\mathbb{R}^n)$,

$$|x - y| = |id(x) - id(y)| = |\Phi \circ \Phi^{-1}(x) - \Phi \circ \Phi^{-1}(y)| = |\Phi^{-1}(x) - \Phi^{-1}(y)|$$

□

15.3 $A \in GL(n, \mathbb{R})$, $T_A(v) = Av$: $A^tA = I \Leftrightarrow T_A \in Isom(\mathbb{R}^n)$

There is a matrix $A \in GL(n, \mathbb{R})$ i.e. a *invertible linear transofrmations* $T_A : \mathbb{R}^n \to \mathbb{R}^n$ is given by $T_A(v) = Av$.

$$T_A(v) \cdot T_A(w) = (Av) \cdot (Aw) = (Av)^t(Aw) = v^tA^tAw$$

$$A^tA = I \Leftrightarrow T_A(v) \cdot T_A(w) = v \cdot w \Leftrightarrow_{(HW4)} T_A \in Isom(\mathbb{R}^n)$$

15.4 Linear isometries i.e. orthogonal group $O(n) = \{A \in GL(n, \mathbb{R}) | A^tA = I\}$

We define the all isometries in *invertible linear transofrmations* $\mathbb{R}^n \to \mathbb{R}^n$ as **orthogonal group**

$$O(n) = \{A \in GL(n, \mathbb{R}) | A^tA = I\} \subset GL(n, \mathbb{R})$$

15.4.1 Special orthogonal group $SO(n) = \{A \in O(n) | det(A) = 1\}$: orthogonal group with $det(A) = 1$

$O(n)$ are the matrices representing linear isometries of $\mathbb{R}^n$. $1 = det(I) = det(A^tA) = det(A^t)det(A) = det(A)^2 \Rightarrow det(A) = 1$ or $det(A) = -1$. We use **special orthogonal group** represents A with $det(A) = 1$,

$$SO(n) = \{A \in O(n) | det(A) = 1\}$$

15.5 translation: $\tau_v(x) = x + v$

Define a *translation* by $v \in \mathbb{R}^n$,

$$\tau_v : \mathbb{R}^n \to \mathbb{R}^n, \ \tau_v(x) = x + v$$

15.5.1 translation is an isometry

Note 5 (Exercise 2.5.3)**.** *$\forall v \in \mathbb{R}^n, \tau_v$ is an isometry.*

Proof. $|\tau_v(x) - \tau_v(y)| = |(x + v) - (y + v)| = |x - y|$ □

15.6 The composition of a translation and an orthogonal transformation is an isometry $\Phi_{A,v}(x) = \tau_v(T_A(x)) = Ax + v$

Since *the composition of isometries is an isometry,* $\forall A \in O(n)$ and $v \in \mathbb{R}^n$, the composition

$$\Phi_{A,v}(x) = \tau_v(T_A(x)) = Ax + v$$

is an isometry. **which could account for all isometries**.

15.6.1 Theorem 2.5.3: All isometries can be represented by a composition of *a translation* and *an orthogonal transformation*, $Isom(\mathbb{R}^n) = \{\Phi_{A,v} | A \in O(n), v \in \mathbb{R}^n\}$

Theorem 74 (Theorem 2.5.3)**.** *$Isom(\mathbb{R}^n) = \{\Phi_{A,v} | A \in O(n), v \in \mathbb{R}^n\}$*

16 Complex numbers

$\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$, $\mathbb{R} = \{a + 0i | a \in \mathbb{R}\} \subset \mathbb{C}$
Addition & multiplication

$$\begin{aligned}(a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi)(c + di) &= ac + bci + adi + bdi^2 \\ &= (ac - bd) + (bc + ad)i\end{aligned}$$

Complex conjugation: $z = a + bi, \bar{z} = a - bi, \overline{zw} = \bar{z}\bar{w}$
Absolute value: $|z| = \sqrt{a^2 + b^2}$, $|z|^2 = z\bar{z}$
Additive inverse: $-z = -a - bi$
Multiplicative inverse: $z^{-1} = \frac{1}{z} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{\bar{z}}{|z|^2}$

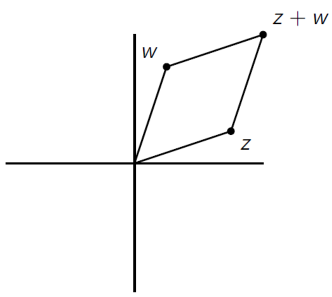
$$z \in \mathbb{C}, \overline{z + \bar{z}} = \bar{z} + \bar{\bar{z}} = z + \bar{z}$$

$$\textit{Real part: } Re(z) = \frac{z + \bar{z}}{2}$$

$$\textit{Imaginary part: } Im(z) = \frac{z - \bar{z}}{2i}$$

16.1 Geometric Meaning of Addition and Multiplication

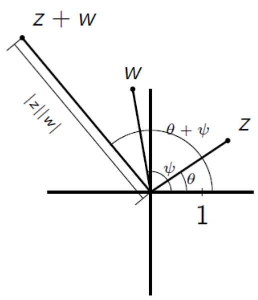
Addition: parallelogram law



Multiplication:

$$\begin{aligned}z &= a + bi \neq 0 \\ &= r\cos\theta + r\sin\theta i \\ &= r(\cos\theta + i\sin\theta) \\ |z|^2 &= a^2 + b^2 = r^2\end{aligned}$$

$$
\begin{aligned}
z =& r(\cos\theta + i\sin\theta) \\
w =& s(\cos\phi + i\sin\phi) \\
zw =& rs[\cos\theta\cos\phi - \sin\theta\sin\phi + i(\cos\theta\sin\phi + \cos\phi\sin\theta)] \\
=& rs[cos(\theta+\phi) + i\sin(\theta+\phi)] \\
=& |z||w|[cos(\theta+\phi) + i\sin(\theta+\phi)]
\end{aligned}
$$



We will write,

$$
\begin{aligned}
&\cos\theta + i\sin\theta = e^{i\theta} \\
&e^{i\theta}e^{i\phi} = e^{i(\theta+\phi)} \\
&z = |z|e^{i\theta}
\end{aligned}
$$

16.2 Theorem 2.1.1: $f(x) = a_0 + a_1x + ... + a_nx^n$ with coefficients $a_0, a_1, ..., a_n \in \mathbb{C}$. Then f has a <u>root</u> in $\mathbb{C}$: $\exists\alpha \in \mathbb{C}$ s.t. $f(\alpha) = 0$

Theorem 75 (Theorem 2.1.1)**.** *Supose a nonconstant polynomial $f(x) = a_0 + a_1x + ... + a_nx^n$ with coefficients $a_0, a_1, ..., a_n \in \mathbb{C}$. Then f has a <u>root</u> in $\mathbb{C}$: $\exists\alpha \in \mathbb{C}$ s.t. $f(\alpha) = 0$.*

16.2.1 Corollary 2.1.2: $f(x) = a_n\prod_{i=1}^{n}(x-k_i) = a_n(x-k_1)(x-k_2)...(x-k_n)$, where $k_1, k_2, ..., k_n$ are roots of $f(x)$

Corollary 21 (Corollary 2.1.2)**.** *Every nonconstant polynomial with coefficients $a_0, a_1, ..., a_n \in \mathbb{C}$ can be factored as $f(x) = a_n\prod_{i=1}^{n}(x-k_i) = a_n(x-k_1)(x-k_2)...(x-k_n)$, where $k_1, k_2, ..., k_n$ are roots of $f(x)$.*

16.2.2 Corollary 2.1.3: $a_i \in \mathbb{R}$, f can be expresses as a product of linear and quadratic polynomials

Corollary 22 (Corollary 2.1.3)**.** *If $f(x) = a_0 + a_1x + ... + a_nx^n$ is a nonconstant polynomial $a_0, a_1, ..., a_n \in \mathbb{R}, a_n \neq 0$. Then f can be expresses as a product of linear and quadratic polynomials.*

$a_0, a_1, ..., a_n$ is real number here!

Proof.
(1)Obviously, the corollary holds at $n = 1$ and $n = 2$.
(2)Suppose the corollary holds for all situations that $n < k$.
When $n = k$, $f(x) = a_0 + a_1x + ... + a_kx^k, a_k \neq 0$.
By F.T.A., f has a root α in $\mathbb{C}$.
If $\alpha \in \mathbb{R}$, long division $f(x) = q(x)(x-\alpha)$. q has real coefficients, *degree of* $q = k-1$. Since the corollary holds at $n = k-1$, $q(x)$ is a product of linear and quadratics. Then, the corollary also holds

at $n = k$.
If $\alpha \notin \mathbb{R}$

$$0 = f(\alpha) = a_0 + a_1\alpha + ... + a_k\alpha^k$$
$$0 = \overline{f(\alpha)} = a_0 + a_1\bar{\alpha} + ... + a_n\bar{\alpha}^n = f(\bar{\alpha})$$

Since $\bar{\alpha} \neq \alpha$, $(x-\alpha)(x-\bar{\alpha})|f$.
$(x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + |\alpha|^2$ is a polynomial with coefficients in $\mathbb{R}$. So $f(x) = q(x)(x^2 - (\alpha+\bar{\alpha})x + |\alpha|^2)$, q has real coefficients with degree $k-2$. The corollary also holds at $n = k-2$, $q(x)$ is a product of linear and quadratics. Then, the corollary also holds at $n = k$.

$\square$

References

[1] Christopher J Leininger Introduction to Abstract Algebra (Draft) 2017.

[2] Fraleigh, J. B. (2003). A first course in abstract algebra. Pearson Education India.