# PMATH 347 - Groups and Rings

by Steven Cao

## Contents

# §1. Groups

## §1.1. Notations

In this course natural numbers $\mathbb{N}$ start with 1.

**Definition** ($\mathbb{Z}_n$).
Set of integers modulo $n$:

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

where the congruence class

$$[r] = \{z \in \mathbb{Z} : z \in (r \bmod n)\}$$

Note that for the sets $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$, $S$ consists of two operations: **addition** and **multiplication**.

**Definition** ($\mathcal{M}_n(\mathbb{F})$).
Set of all $n \times n$ matrices over field $\mathbb{F}$.

We can perform addition and multiplication on $\mathcal{M}_n(\mathbb{R}$.

## §1.2. Groups

**Definition** (Group).
Let $G$ be a set and $*$ be an operation on $G \times G$ (can be addition, multiplication, matrix addition, matrix multiplication etc.).

$G$ is a **group** of it satisfies:
1. Closure: if $a, b \in G$, then $a * b \in G$
2. Associativity: if $a, b, c \in G$, then $a * (b * c) = (a * b) * c$
3. Identity: there exists $e \in G$ (identity) such that $a * e = a = e * a \quad \forall a \in G$
4. Inverse: for all $a \in G$, there exists $b \in G$ (inverse) such that $a * b = e = b * a$

**Definition** (Abelian group).
$G$ is **abelian** if $a * b = b * a \quad \forall a, b \in G$.

**Problem 1.1**.
Prove that in the definition of a group, it suffices to only have $e * a = a$ in (3) and $b * a = e$ in (4). Note $e$ and $b$ must be on the same side.

**Theorem 1.1.**
Let $G$ be a group and $a \in G$.
1. The identity of $G$ is unique.
2. The inverse of $a$ is unique.

**Proof.**
1. If $e_1$ and $e_2$ are both identities, then $e_1 = e_1 * e_2 = e_2$
2. If $b_1, b_2$ are inverses of $a$, then $b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$

$\square$

**Example.**
The sets $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian groups, where the additive identity is 0 and the additive inerse of an element $r$ is $(-r)$.

$(\mathbb{N}, +)$ is not a group as it does not have an identity and inverse for all elements.

**Example.**
The sets $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ are not groups as 0 has no multiplicative inverse.

For a set $S = (\mathbb{F}, \cdot)$, let $S^*$ denote the subset of $S$ containing all elements with multiplicative inverse. For example, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Then $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}, \cdot)$ are abelian groups. The multiplicative identity is 1 and the multiplicative inverse is $\frac{1}{r}$.

**Problem 1.2.**
Let $\mathbb{Z}_n$ denote the set of integers mod $n$. What is $\mathbb{Z}_n^*$?

**Example.**
The set $(\mathcal{M}_n(\mathbb{R}), +)$ is an abelian group where the additive identity is the zero matrix and the additive inverse of $A$ is $-A$.

**Example.**
$(\mathcal{M}_n(\mathbb{R}), \cdot)$ is not a group because not all elements have a multiplicative inverse.

Let $GL_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) : \det(M) \neq 0\}$, which is the set of full-rank/invertible matrices. Note that:
- If $A, B \in GL_n(\mathbb{R})$, then $\det(AB) = \det(A)\det(B) \neq 0$
- $\det(A^{-1}) = \det(A)^{-1} \neq 0$

$(GL_n(\mathbb{R}), \cdot)$ is also known as the **general linear group** of degree $n$ over $\mathbb{R}$.

Note that if $n \geq 2$, then the group $(GL_n\mathbb{R}, \cdot)$ is not abelian.

**Problem 1.3 .**
What is $(GL_1(\mathbb{R}), \cdot)$?

**Example .**
Let $G, H$ be groups. The **direct product** is the set $G \times H$ with the component-wise operation defined by

$$(g_1, h_1) * (g_2, h_2) = (g_1 * g_2, h_1 * h_2)$$

$G \times H$ is a group with the identity $(e_G, e_H)$, and the inverse of $(g, h)$ is $(g^{-1}, h^{-1})$.

Similarly, if $G_1, G_2, ..., G_n$ are groups, then $G_1 \times G_2 \times \cdots \times G_n$ is also a group.

Notation: we often denote:
- $g_1 * g_2$ by $g_1 g_2$
- Its identity by 1
- The inverse of $g \in G$ by $g^{-1}$
- $g^n = g * \underbrace{\cdots}_{n \text{ times}} * g$

**Proposition 1.2 .**
Let $G$ be a group and $g, h \in G$. We have:
1. $(g^{-1})^{-1} = g$
2. $(gh)^{-1} = h^{-1}g^{-1}$
3. $g^n g^m = g^{n+m}$
4. $(g^n)^m = g^{nm}$

**Proof.**
1. $g^{-1}g = 1 = gg^{-1}$
2. $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = gg^{-1} = 1$

□

**Problem 1.4 .**
Prove the properties (3) and (4).

In general, it is **not** true that if $g, h \in G$, then $(gh)^n = g^n h^n$. For example, $(gh)^2 = ghgh$ and $g^2h^2 = gghh$ which is not equal unless $G$ is abelian.

**Theorem 1.3 .**
Let $G$ be a group and $g, h, f \in G$. Then,
1. Left and right cancellation:
   - If $gh = gf$, then $h = f$
   - If $hg = fg$, then $h = f$
2. Given $a, b \in G$, the equations $ax = b$ and $ya = b$ has unique solutions for $x, y \in G$.

**Proof.**

- Left cancellation:

$$gh = gf \iff g^{-1}(gh) = g^{-1}(gf) <> (g^{-1}g)h = (g^{-1}g)f \iff h = f$$

Proof for right cancellation is similar.

- Let $x = a^{-1}b$. Then,

$$ax = a(a^{-1})b = b$$

If $u$ is another solution, then $au = b = ax$. Then, $u = x$ by cancellation.

Similarly, $y = ba^{-1}$ is the unique solution of $ya = b$.

$\square$

## §1.3. Symmetric groups

**Definition** (Permutation).
Given $L \neq \emptyset$, a **permutation** of $L$ is a bijection from $L$ to $L$. The set of all permutations is denoted by $S_L$.

**Example.**
Consider the set $L = \{1, 2, 3\}$. It has the following different permutations:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

**Definition.**
For $n \in \mathbb{N}$, we denote $S_n = S_{\{1,2,\ldots,n\}}$ as the set of all permutations of $\{1, \ldots, n\}$.

We have seen that the order of $S_3 = 3! = 6$.

**Proposition 1.4.**
$|S_n| = n!$

Given $\sigma, \tau \in S_n$, we can *compose* them to get a third element $\sigma\tau$, where $\sigma\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$ given by $x \mapsto \sigma(\tau(x))$.

Since both $\sigma, \tau$ are bijections, so is $\sigma\tau$. Thus $\sigma\tau \in S_n$.

**Example.**
Given

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Then, the compositions are

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Note that $\sigma\tau \neq \tau\sigma$.

For any $\sigma, \tau \in S_n$, we have $\sigma\tau, \tau\sigma \in S_n$, but $\sigma\tau \neq \tau\sigma$ in general.

On the other hand, $\sigma(\tau\mu) = (\sigma\tau)\mu$.

The **identity permutation** $\varepsilon \in S_n$ is defined as

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Then for any $\sigma \in S_n$, we have $\sigma\varepsilon = \sigma = \varepsilon\sigma$.

Given $\sigma \in S_n$, there also exists a unique **inverse permutation** bijection $\sigma^{-1} \in S_n$, such that $\sigma^{-1}(x) = y$ iff $\sigma(y) = x$. This also satisfies $\sigma(\sigma^{-1}(x)) = \sigma(y) = x$ and $\sigma^{-1}(\sigma(y)) = y$.

To compute the inverse, find $y$ in $\sigma(y) = x$ for each $x \in [n]$.

**Problem 1.5.**
Find the inverse of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

**Proposition 1.5.**
$S_n$ is a group called the **symmetric group** of degree $n$.

**Problem 1.6.**
Write down all rotations and reflections that fix a equilateral triangle. Then check why it is the "same" as $S_3$.

Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 9 & 0 & 2 & 5 & 8 & 10 \end{pmatrix} \in S_{10}$.

Note that if we repeatedly apply $\sigma$, there are four cycles:
- $1 \to 3 \to 7 \to 2 \to 1$
- $4 \to 6 \to 4$
- $5 \to 9 \to 8 \to 5$
- $10 \to 10$

Thus $\sigma$ can be **decomposed** into one 4-cycle $(1\ 3\ 7\ 2)$, one 2-cycle $(4\ 6)$, one 3-cycle $(5\ 9\ 8)$, and one 1-cycle $(10)$ (usually omitted).

Note that these cycles are **pairwise disjoint** and we have

$$\sigma = (1\ 3\ 7\ 2)(4\ 6)(5\ 9\ 8)$$

We can also reorder the three cycles or rearranges the elements in each cycle. So these are also valid:

$$\sigma = (4\ 6)(5\ 9\ 8)(1\ 3\ 7\ 2) = (6\ 4)(9\ 8\ 5)(7\ 2\ 1\ 3)$$

**Theorem 1.6** (Cycle Decomposition Theorem).
If $\sigma \in S_n$ with $\sigma \neq \varepsilon$, then $\sigma$ is a product of one or more disjoint cycles of length at least 2.

This factorization is unique up to the order of the factors.

See Bonus 1 for proof.

Every permutation in $S_n$ can be regarded as a permutation in $S_{n+1}$ with the number $n+1$ fixed. Thus $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq S_{n+1} \subseteq \cdots$.

## §1.4. Cayley tables

For a finite group $G$, it is sometimes convenient to define its operation by a table.

Given $x, y \in G$, the product $xy$ is the entry of the table in row $x$ and column $y$. Such a table is a **Cayley table**.

**Proposition 1.7**.
The entries in each row or column $n$ of a Cayley table are all distinct.

**Example**.
Consider $(\mathbb{Z}_2, +)$. Its Cayley table is

| $\mathbb{Z}_2$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

**Example**.
Consider $(\mathbb{Z}^* = \{1, -1\}, \times)$. Its Cayley table is

| $\mathbb{Z}^*$ | $1$ | $-1$ |
|---|---|---|
| $1$ | $1$ | $-1$ |
| $-1$ | $-1$ | $1$ |

Note that if we replace $1$ by $[0]$ and $-1$ by $[1]$, the Cayley tables of $\mathbb{Z}^*$ and $\mathbb{Z}_2$ becomes the same.

In this case, we say $\mathbb{Z}^*$ and $\mathbb{Z}_2$ are isomorphic: $\mathbb{Z}^* \cong \mathbb{Z}_2$.

**Example.**
For $n \in \mathbb{N}$, the cyclic group of order $n$ is defined by $C_n = \{1, a, a^2, ..., a^{n-1}\}$ with $a^n = 1$ and $1, a, ..., a^{n-1}$.

The Cayley table of $C_n$ is

| $C_n$ | $1$ | $a$ | $a^2$ | ... | $a^{n-2}$ | $a^{n-1}$ |
|---|---|---|---|---|---|---|
| $1$ | $1$ | $a$ | $a^2$ | ... | $a^{n-2}$ | $a^{n-1}$ |
| $a$ | $a$ | $a^2$ | $a^3$ | ... | $a^{n-1}$ | $1$ |
| $a^2$ | $a^2$ | $a^3$ | $a^4$ | ... | $1$ | $a$ |
| $\vdots$ | | | | | | |
| $a^{n-2}$ | $a^{n-2}$ | $a^{n-1}$ | $1$ | ... | $a^{n-4}$ | $a^{n-3}$ |
| $a^{n-1}$ | $a^{n-1}$ | $1$ | $a$ | ... | $a^{n-3}$ | $a^{n-2}$ |

**Proposition 1.8.**
Let $G$ be a group. Up to isomorphism, we have
1. If $|G| = 1$, then $G \cong \{1\}$
2. If $|G| = 2$, then $G \cong C_2$
3. If $|G| = 3$, then $G \cong C_3$
4. If $|G| = 4$, then $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$, the Klein 4-group

**Proof.** (1) If $|G| = 1$, then trivially $G = \{1\}$

(2) If $|G| = 2$, then $G = \{1, g\}$ with $g = \pm 1$. Then $g^2 = g$ or $g^2 = 1$. If $g^2 = g$, then by cancellation $g = 1$ which is a contradiction. Thus $g^2 = 1$.

Hence the Cayley table of $G$ is

| $G$ | $1$ | $g$ |
|---|---|---|
| $1$ | $1$ | $g$ |
| $g$ | $g$ | $1$ |

(3) If $|G| = 3$, then $G = \{1, g, h\}$ with $g \neq 1$, $h \neq 1$, $g \neq h$.

By cancellation, we have $gh \neq g$, $gh \neq h$, thus $gh = 1$. Similarly, we have $hg = 1$.

Also, on the row for $g$, we have $g(1) = g$, $gh = 1$. Since all entries in the row are distinct, we have $g^2 = h$.

The Cayley table of $G$ is

| $G$ | $1$ | $g$ | $h$ |
|---|---|---|---|
| $1$ | $1$ | $g$ | $h$ |
| $g$ | $g$ | $h$ | $1$ |
| $h$ | $h$ | $1$ | $g$ |

$\square$

**Problem 1.7.**
Consider the symmetry group of a non-square rectangle. How is it related to $K_4$?

# §2. Subgroups

## §2.1. Subgroup tests

**Definition** (Subgroup).
Let $G$ be a group. Let $H \subseteq G$. If $H$ itself is a group, then we say $H$ is a subgroup of $G$.

Since $G$ is a group, for $h_1, h_2, h_3 \in H \subseteq G$, we have $h_1(h_2 h_3) = (h_1 h_2) h_3$. Thus, $H$ is a subgroup of $G$ if it satisfies the following conditions.

**Remark** (Subgroup test).
1. If $h_1, h_2 \in H$, then $h_1 h_2 \in H$
2. $I_h \in H$
3. If $h \in H$, then $h^{-1} \in H$

**Problem 2.1.**
Prove that $I_H = I_G$.

**Example.**
Given a group $G$, then $\{1\}$ and $G$ are subgroups of $G$.

**Example.**
We have a chain of groups:

$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$$

**Example.**
Recall the general linear group of order $n$ over $\mathbb{R}$:

$$GL_n(\mathbb{R}) = (GL_n(\mathbb{R}), \cdot) = \{M \in \mathcal{M}_n(\mathbb{R}) : \det(M) \neq 0\}$$

We can define

$$SL_n(\mathbb{R}) = (SL_n\mathbb{R}, \cdot) = \{M \in GL_n(\mathbb{R}) : \det(M) = 1\} \subseteq GL_n(\mathbb{R})$$

Note that the identity matrix is $I \in SL_n(\mathbb{R})$. Let $A, B \in SL_n(\mathbb{R})$. Then,

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$$

And

$$\det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$$

So $AB, A^{-1} \in SL_n(\mathbb{R})$. By subgroup test, $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

$SL_n(\mathbb{R})$ is the **special linear group** of order $n$ over $\mathbb{R}$.

**Example.**
Given a group $G$, we define the **center** of $G$ to be

$$Z(G) = \{z \in G : zg = gz \ \forall g \in G\}$$

Note that $Z(G) = G$ iff $G$ is abelian.

Claim: $Z(G)$ is an abelian subgroup of $G$.

Note that $I \in Z(G)$. Let $y, z \in Z(G)$. Then for all $g \in G$, we have

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz)$$

Thus $yz \in Z(G)$.

And, for $z \in Z(G)$ and $g \in G$, we have

$$zg = gz \iff z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} \iff (z^{-1}z)(gz^{-1}) = (z^{-1}g)(zz^{-1}) \iff gz^{-1} = z^{-1}g$$

**Proposition 2.1.**
Let $H, K \subseteq G$. Then their intersection $H \cap K = \{g \in G : g \in H, g \in K\}$ is also a subgroup of $G$.

**Problem 2.2.**
Prove the intersection of subgroups property.

**Theorem 2.2** (Finite subgroup test)**.**
If $H \subseteq G$ is finite and non-empty, then $H$ is a subgroup of $G$ iff $H$ is closed under its operation.

**Proof.** Let $H \subseteq G$ be finite and non-empty.

($\Longrightarrow$) Trivial.

($\Longleftarrow$) Let $h \in H$. Since $H$ is closed under its operation, we have $h, h^2, \ldots$ are all in $H$.

As $H$ is finite, these elements are not all distinct. Thus $h^n = h^{n+m}$ for some $n, m \in \mathbb{N}$. By cancellation, $h^m = 1$ and thus $1 \in H$.

Also, $1 = h^{m-1}h \Longrightarrow h^{-1} = h^{m-1}$, so $h^{-1} \in H$.

By the subgroup test, $H$ is a subgroup of $G$. □

## §2.2. Alternating groups

**Definition** (Transposition).
A **transposition** $\sigma \in S_n$ is a cycle of length 2.

**Example.**
Consider $(1\ 2\ 4\ 5) \in S_5$. The composition $(1\ 2)(2\ 4)(4\ 5)$ can be computed as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \\ 1 & 4 & 3 & 5 & 2 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

Thus we have

$$(1\ 2\ 4\ 5) = (1\ 2)(2\ 4)(4\ 5)$$

Also, we can show that

$$(1\ 2\ 4\ 5) = (2\ 3)(1\ 2)(2\ 5)(1\ 3)(2\ 4)$$

We can see from this example that the factorization into transpositions are not unique.

**Theorem 2.3** (Parity theorem).
If a permutation $\omega$ has two factorizations

$$\sigma = \nu_1\nu_2 \ldots \nu_r = \mu_1\mu_2 \ldots \mu_s$$

where each $\nu_i$ and $\mu_j$ is a transposition, then $r \equiv s \pmod 2$.

**Definition.**
A permutation is **even** (or **odd**) if it can be written as a product of an even (or odd) number of transpositions.

By parity theorem, a permutation is either even or odd, but not both.

**Theorem 2.4.**
For $n \geq 2$, let $A_n$ denote the set of all even permutations in $S_n$. Then,
1. $\varepsilon \in A_n$
2. If $\sigma, \tau \in A_n$, then $\sigma\tau \in A_n$ and $\sigma^{-1} \in A_n$
3. $|A_n| = \frac{1}{2}n!$

**Proof.** (1) We can write $\varepsilon = (1\ \ 2)(1\ \ 2)$. Thus $\varepsilon$ is even.

(2) Let $\sigma, \tau \in A_n$. We can write $\sigma = \sigma_1 \cdots \sigma_r$ and $\tau = \tau_1 \cdots \tau_s$ where $\sigma_i, \tau_j$ are transpositions and $r, s$ are even.

Then,

$$\sigma\tau = \sigma_1 \cdots \sigma_r \tau_1 \cdots \tau_s$$

is a product of $r + s$ transpositions, so it is even.

Also, since $\sigma_i$ is a transposition, we have $\sigma_i^2 = \varepsilon$ and thus $\sigma_i^{-1} = \sigma_i$. It follows that

$$\sigma^{-1} = (\sigma_1 \cdots \sigma_r)^{-1} = \sigma_r^{-1} \cdots \sigma_1^{-1} = \sigma_r \cdots \sigma_1$$

which is an even permutation.

(3) Let $O_n$ denote the set of odd permutations in $S_n$, such that $S_n = A_n \cup O_n$, and the parity theorem implies $A_n \cap O_n = \emptyset$.

Since $|S_n| = n!$, to prove $|A_n| = \frac{1}{2}n!$, it suffices to show that $|A_n| = |O_n|$.

Let $\nu = (1\ \ 2)$ and let $f : A_n \to O_n$ be defined by $f(\sigma) = \nu\sigma$.

Since $\sigma$ is even, we have that $\nu\sigma$ is odd. Thus the map is well-defined.

Also, if we have $\nu\sigma_1 = \nu\sigma_2$, by cancellation we get $\sigma_1 = \sigma_2$. So, $f$ is one-to-one.

Let $\tau \in O_n$. Then, $\sigma = \nu\sigma \in A_n$ and

$$f(\sigma) = \nu\sigma = \nu(\nu\tau) = \nu^2\tau = \tau$$

So $f$ is onto

Putting together, $f$ is a bijection. Thus, $|n| = |O_n|$. □

From (1) and (2), we see that $A_n$ is a subgroup of $S_n$.

$A_n$ is called the **alternating group** of degree $n$.

## §2.3. Order of elements

**Definition.**
If $G$ is a group and $g \in G$, we denote

$$\langle g \rangle = \{g^\beta : \beta \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, g^0, g^1, g^2, \ldots\}$$

Note that $1 = g^0 \in \langle g \rangle$. Also, if $x \in g^m$, $y \in g^n \in \langle g \rangle$ with $m, n \in \mathbb{Z}$, then

$$xy = g^m g^n = g^{m+n} \in \langle g \rangle$$

and $x^{-1} = g^{-m} \in \langle g \rangle$. By the subgroup test, we have

**Proposition 2.5.**
If $G$ is a group and $g \in G$, then $\langle g \rangle$ is a subgroup of $G$.

**Definition.**
Let $G$ be a group and $g \in G$. We call $\langle g \rangle$ the **cyclic subgroup** of $G$ generated by $g$.

If $G = \langle g \rangle$ for some $g \in G$, then we say $G$ is **cyclic** and $g$ is a **generator** of $G$.

**Example.**
Consider $(\mathbb{Z}, +)$. Note that for all $k \in \mathbb{Z}$, we can write $k = k \cdot 1$. Thus $(\mathbb{Z}, +) = \langle 1 \rangle$.

Similarly, $(\mathbb{Z}, +) = \langle -1 \rangle$.

For any $n \in \mathbb{Z}$ with $n \neq \pm 1$, there exists no $k \in \mathbb{Z}$ such that $k \cdot n = 1$, thus $\pm 1$ are the only generators of $(\mathbb{Z}, +)$.

Let $G$ be a group a $g \in \mathbb{G}$ suppose that there exists $k \in \mathbb{Z}, k \neq$ such that $g^k = 1$. Then $g^{-k} = (gk)^{-1} = 1$. Thus we can assume that $k \geq 1$. By the well-ordering principle, there exists the "smallest" positive integer $n$ such that $g^n = 1$.

**Definition (Order).**
Let $G$ be a group and $g \in G$. If $n \in \mathbb{N}$ is the smallest value such that $g^n = 1$, then we say the **order** of $g$ is $n$, denoted by $o(g) = n$.

If no such $n$ exist, then we say $g$ has **infinite order** and write $o(g) = \infty$.

**Proposition 2.6.**
Let $G$ be a group and $g \in G$ such that $o(g) = n \in \mathbb{N}$. For $k \in \mathbb{Z}$, we have
1. $g^k = 1$ iff $n \mid k$ (divides)
2. $g^k = g^m$ iff $k \equiv m \pmod n$
3. $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$ where $g, g^2, ...g^{n-1}$ are all distinct, and $|\langle g \rangle| = o(g)$

**Proof.** (1) ($\Longleftarrow$) If $n \mid k$, then $k = nq$ for some $q \in \mathbb{Z}$. Thus

$$g^k = g^{nz} = (g^n)^z = 1^z = 1$$

($\Longrightarrow$) By division algorithm, we can write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Since $g^k = 1$ and $g^n = 1$, we have

$$g^r = g^{k-nq} = g^k (g^n)^{-q} = 1(1)^{-q} = 1$$

As $0 \leq r < n$ and $o(g) = n$, we have $r = 0$ and hence $n \mid k$.

(2) Note that $g^k = g^m$ iff $g^{k-m} = 1$. By (1), we have $n \mid (k - m)$, so $k \equiv m \pmod n$.

(3) From (2), it follows that $1, g, g^2, ..., g^{n-1}$ are all distinct. So, we have $\{1, g, g^2, ..., g^{n-1}\} \subseteq \langle g \rangle$.

Let $g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. Write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then,

$$g^k = g^{nq} g^r = 1^q g^r = g^r \in \{1, g, g^2, ..., g^{n-1}\}$$

Thus we have $\langle g \rangle = \{1, g, ..., g^{n-1}\}$. □

**Proposition 2.7.**
Let $G$ be a group and $g \in G$ satisfying $o(g) = \infty$. For $k \in \mathbb{Z}$, we have
1. $g^k = 1$ iff $k = 0$
2. $g^k = g^m$ iff $k = m$
3. $\langle g \rangle = \{..., g^{-1}, g^{=}, g^1, ...\}$ where $g^i$ are all distinct

**Proposition 2.8.**
Let $G$ be a group and $g \in G$ with $o(g) = n \in \mathbb{N}$. If $d \in \mathbb{N}$, then $o(g^d) = \frac{n}{\gcd(n,d)}$ where $\gcd(n, d)$ is the gcd of $n$ and $d$.

In particular, if $d \mid n$, then $o(g^d) = \frac{n}{d}$.

**Proof.** Let $n_1 = \frac{n}{\gcd(n,d)}$ and $d_1 = \frac{d}{\gcd(n,d)}$. By (divide by GCD from MATH 135) we have $\gcd(n_1, d_1) = 1$. Note that

$$(g^d)^{n_1} = (g^d)^{\frac{n}{\gcd(n,d)}} = (g^n)^{\frac{d}{\gcd(n,d)}} = 1$$

Now we will show that $n_1$ is the smallest such possible integer.

Suppose $(g^d)^r = 1$ with $r \in \mathbb{N}$. Since $o(g) = n$, we have $n \mid dr$. Thus there exists $q \in \mathbb{Z}$ such that $dr = nq$.

Dividing both sides by $\gcd(n, d)$, we have

$$d_1 r = \frac{d}{\gcd(n, d)} r = \frac{n}{\gcd(n, d)} q = n_1 q$$

Since $n_1 \mid d_1 r$ and $\gcd(n_1, d_1) = 1$, we get $n_1 \mid r$, so $r = n_1 l$ for some $l \in \mathbb{Z}$. As $l \geq 1$, we get $r \geq n_1$. □

## §2.4. Cyclic groups

For a group $G$, if $G = \langle g \rangle$ for some $g \in G$, then $G$ is a cyclic group. For $a, b \in G$, we have $a = g^m$ and $b = g^n$ for some $m, n \in \mathbb{Z}$, which means

$$ab = g^m g^n = ba$$

**Proposition 2.9.**
Every cyclic group is abelian.

The converse of this is not true! For example, $K_4$ is ablian, but it is not cyclic.

**Proposition 2.10.**
Every subgroup of a cyclic group is cyclic.

**Proof.** Let $G = \langle g \rangle$ be cyclic. Let $H$ be a subgroup of $G$.

If $H = \{1\}$, then trivially $H$ is cyclic. Otherwise, there exists $g^k \in H$ with $k \in \mathbb{Z}, k \neq 0$. Since $H$ is a group, we have $g^{-k} \in H$. Thus we can assume $k \in \mathbb{N}$.

Let $m \in \mathbb{N}$ be the smallest such that $g^m \in H$. We can show that $H = \langle g^m \rangle$ using division algorithm. □

**Proposition 2.11.**
Let $G = \langle g \rangle$ be cyclic with $o(g) = n$. Then $G = \langle g^k \rangle$ iff $\gcd(k, n) = 1$.

**Proof.** By earlier proposition, $o(g^k) = \frac{n}{\gcd(n,k)}$. □

**Theorem 2.12** (Fundamental theorem of finite cyclic groups).
Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n$.
1. If $H$ is a subgroup of $G$, then $H = \langle g^d \rangle$ for some $d \mid n$. It follows that $|H| \mid |G|$
2. If $k \mid n$, then $g^{\frac{n}{k}}$ is a unique subgroup of $G$ of order $k$.

**Proof.**

1. Let $H$ be a subgroup of $G$. Then $H$ is cyclic, so $H = \langle g^m \rangle$ for some $m \in \mathbb{N} \cup \{0\}$.

   Let $d = \gcd(m, n)$. We will show $H = \langle g^d \rangle$.

   ($\subseteq$) Since $d \mid m$, we have $m = dk$ for some $k \in \mathbb{Z}$. Then $g^m = g^{dk} \in \langle g^d \rangle$. Thus $H = \langle g^m \rangle \subseteq \langle g^d \rangle$.

   ($\supseteq$) As $d = \gcd(mn)$, there exists $x, y \in \mathbb{Z}$ such that $d = mx + ny$. Then,
   $$g^d = g^{mx+ny} = g^{mx}(g^n)^y = g^{mx} \in \langle g^m \rangle$$
   Thus $\langle g^d \rangle \subseteq \langle g^m \rangle = H$. It follows that $H = \langle g^d \rangle$.

   Since $d = \gcd(m, n)$, we have $d \mid n$. So,
   $$|H| = o(g^d) = \frac{n}{\gcd(n, d)} = \frac{n}{d}.$$
   Thus, $|H| \mid |G|$.

2. The cyclic subgroup $\langle g^{\frac{n}{k}} \rangle$ is of order
   $$o(g^{\frac{n}{k}}) = \frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k$$
   To show uniqueness, let $K$ be a subgroup of $G$ of order $k$, possible as $k \mid n$. By (1), let $K = \langle g^d \rangle$ with $d \mid n$. Then, we have
   $$k = |k| = o(g^d) = \frac{n}{\gcd(n, d)} = \frac{n}{d}$$
   It follows that $d = \frac{n}{k}$ and thus $K = \langle g^{\frac{n}{k}} \rangle$.

□

## §2.5. Non-cyclic groups

Let $X$ be a non-empty subset of a group $G$, and let

$$\langle X\rangle = \left\{x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m} : m \in \mathbb{N}, x_i \in X, k_i \in \mathbb{Z}\right\}$$

denote the set of all products of powers of (not necessarily distinct) elements of $X$. Note that if $x_1^{k_1}\cdots x_m^{k_m} \in \langle X\rangle$ and $y_1^{r_1}, \cdots y_n^{r_n} \in \langle X\rangle$, then

$$x_1^{k_1}\cdots x_m^{k_m}y_1^{r_1}\cdots y_n^{r_n} \in \langle X\rangle$$

Also, $x_1^0 \in \langle X\rangle$ and $\left(x_1^{k_1}\cdots x_m^{k_m}\right)^{-1} = x_m^{-k_1}\cdots x_1^{-k_m}$. Hence $\langle X\rangle$ is a subgroup of $G$ containing $X$, called the subgroup of $G$ generated by $X$.

**Example.**
$K_4 = \{1, a, b, c\}$ with $a^2 = b^2 = c^2 = 1$ and $ab = c$. Thus

$$K_4 = \{a, b \cdot a^2 = b^2 = 1, \}$$

**Definition** (Dihedral group).
For $n \geq 2$, the **dihedral group** of order $2n$ is defined by

$$D_{2n} = \{1, a, ..., a^{n-1}, b, ba, ..., ba^{n-1}\}$$

where $a^n = 1 = b^2$ and $aba = b$.

Note that $D_4 \cong K_4$ and $D_6 \cong S_3$.

**Problem 2.3.**
For $n \geq 3$, consider a regular $n$-gon and its group of symmetries. How is it related to $D_{2n}$?

# §3. Normal subgroups

## §3.1. Homomorphisms and isomorphisms

**Definition** (Homomorphism).
Let $G, H$ be groups. A mapping $\alpha : G \to H$ is a **homomorphism** (HM) if

$$\alpha(a *_G b) = \alpha(a) *_H \alpha(b) \ \forall a, b \in G$$

We often omit the group specific operation for simplicity.

**Example.**
Consider the determinant map

$$\det : (GL_n(\mathbb{R}), \cdot) \to \mathbb{R}^*$$

given by $A \mapsto \det(A)$.

Since $\det(AB) = \det(A)\det(B)$, the mapping det is a homomorphism.

**Proposition 3.1.**
Let $\alpha : G \to H$ be a group HM. Then,
1. $\alpha(I_G) = I_H$
2. $\alpha(g^{-1}) = \alpha(g)^{-1}\ \forall g \in G$
3. $\alpha(g^k) = \alpha(g)^k\ \forall g \in G, k \in \mathbb{Z}$

**Problem 3.1.**
Prove Proposition 3.1.

**Definition** (Isomorphism)**.**
A mapping $\alpha : G \to H$ is an isomorphism (IM) if $\alpha$ is HM and $\alpha$ is bijective.

**Proposition 3.2.**
We have
1. The identity map id is an IM
2. If $\sigma : G \to H$ is an IM, then the inverse map $\sigma^{-1} : H \to G$ os also an IM
3. If $\sigma : G \to H$ and $\tau : H \to K$ are IM, then $\sigma\tau : G \to K$ is also an IM

Thus, we see that $\cong$ is an equivalence relation.

**Problem 3.2.**
Problem Proposition 3.2.

**Example.**
Let $\mathbb{R}^+ + \{r \in \mathbb{R} : r > 0\}$. We will show that $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$.

Define $\sigma : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ by $\sigma(r) = e^r$. Note that the exponential map from $\mathbb{R}$ to $\mathbb{R}^+$ is bijective. Also, for $r, s \in \mathbb{R}$, we have

$$\sigma(r + s) = e^{r+s} = e^r e^s = \sigma(r)\sigma(s)$$

Thus, $\sigma$ is an IM.

**Example.**
We will show $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$

Suppose $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an IM. Then, $\tau$ is onto, so there exists $q \in \mathbb{Q}$ such that $\tau(g) = 2$.

Consider $\tau(\frac{q}{2}) = a \in \mathbb{Q}$. Since $\tau$ is an HM, we have

$$a^2 = \tau\left(\frac{q}{2}\right)\tau\left(\frac{q}{2}\right) = \tau\left(\frac{q}{2} + \frac{q}{2}\right) = \tau(q) = 2$$

which contradicts $a \in \mathbb{Q}$. Thus such $\tau$ does not exist and $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$.

## §3.2. Cosets and Lagrange's theorem

**Definition** (Coset).
Let $H$ be a subgroup of group $G$. If $a \in G$, we define

$$Ha = \{ha \mid h \in H\}$$

to be the **right coset** of $H$ generated by $a$.

Similarly, we define

$$aH = \{ah \mid h \in H\}$$

to be the **left coset** of $H$ generated by $a$.

Since $1 \in H$, we have $H1 = H = 1H$ and $a \in Ha$ and $a \in aH$.

However in general, $Ha$ and $aH$ are not subgroups of $G$ and $aH \neq Ha$. But if $G$ is abelian, then $Ha = aH$.

**Example.**
Let $K_4 = \{1, a, b, ab\}$ with $a^2 = 1 = b^2$ and $ab = ba$. Let $H = \{1, a\}$ be a subgroup of $K_4$. Note that since $K_4$ is abelian, we have $gH = Hg \; \forall g \in K_4$. Then the right/left cosets of $H$ are

$$H1 = \{1, a\} = 1H \quad Hb = \{b, ab\} = bH$$

Thus there are exactly two cosets of $H$ in $K_4$.

**Example.**
Let $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ with $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau\sigma = \tau$. Let $H = \{\varepsilon, \tau\}$ which is a subgroup of $S_3$. Since $\sigma\tau = \tau\sigma^{-1} = \tau\sigma^2$, the right cosets of $H$ are

$$\begin{aligned} H\varepsilon &= \{\varepsilon, \tau\} = H\tau \\ H\sigma &= \{\sigma, \tau\sigma\} = H\tau\sigma \\ H\sigma^2 &= \{\sigma^2, \tau\sigma^2\} = H\tau\sigma^2 \end{aligned}$$

And, the left cosets of $H$ are

$$\begin{aligned} \varepsilon H &= \{\varepsilon, \tau\} = \tau H \\ \sigma H &= \{\sigma, \tau\sigma^2\} = \tau\sigma^2 H \\ \sigma^2 H &= \{\sigma^2, \tau\sigma\} = \tau\sigma H \end{aligned}$$

Note that $H\sigma \neq \sigma H$ and $H\sigma^2 \neq \sigma^2 H$.

**Proposition 3.3.**
Let $H$ be a subgroup of a group $G$ and let $a, b \in G$.

1. $Ha = Hb$ iff $ab^{-1} \in H$.
   - In particular, $Ha = H$ iff $a \in H$.
2. If $a \in Hb$, then $Ha = Hb$.
3. Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Thus, the right cosets of $H$ forms a partition of $G$.

**Proof.**

1. ($\Longrightarrow$) Suppose $Ha = Hb$. Then $a = 1a \in Ha = Hb$. Thus $a = hb$ for some $h \in H$ and we have $ab^{-1} = h \in H$.

   ($\Longleftarrow$) Suppose $ab^{-1} \in H$. Then, for all $h \in H$,
   $$ha = (ha)(b^{-1}b) = h(ab^{-1})b \in Hb$$
   so $Ha \subseteq Hb$.

   Note that if $ab^{-1} \in H$, since $H$ is a subgroup, then $(ab^{-1})^{-1} = ba^{-1} \in H$. Thus for all $h \in H$,
   $$hb = h(ba^{-1}) \in Ha$$
   so $Hb \subseteq Ha$. It follows that $Ha = Hb$.
2. If $a \in Hb$, then $ab^{-1} \in H$. Thus by (1), we have $Ha = Hb$.
3. If $Ha \cap Hb = \emptyset$, then we are done. Otherwise, there exists $x \in Ha \cap Hb$. Since $x \in Ha$, by (2), we have $Ha = Hx$. And since $x \in Hb$, similarly we have $Hb = Hx$. Thus $Ha = Hx = Hb$.

$\square$

The analogues of Proposition 3.3 also holds for left cosets.

**Problem 3.3.**
Let $G$ be a group and $Ha$ be a subset of $G$. For $a, b \in G$, do we still have $Ha = Hb$ or $Ha \cap Hb = \emptyset$ if $H$ s not a subgroup of $G$?

From Proposition 3.3 we see that $G$ can be written as a disjoint union of right cosets of $H$.

**Definition** (Index).
The **index** $[G : H]$ is the number of disjoint right (or left) cosets of $H$ in $G$.

**Theorem 3.4** (Lagrange's theorem).
Let $H$ be a subgroup of a finite group $G$. We have $|H| \mid |G|$ and $[G : H] = \frac{|G|}{|H|}$.

**Proof.** Let $k = [G : H]$ and let $Ha_1, Ha_2, \ldots, Ha_k$ be the distinct right cosets of $H$ in $G$. By Proposition 3.3,

$$G = Ha_1 \cup \cdots \cup Ha_k$$

is a disjoint union. Since $|Ha_i| = |H|$ for each $i$, we have

$$|G| = |Ha_1| + \cdots + |Ha_k| = k|H|$$

It follows that $|H| \mid |G|$ and $[G : H] = k = \frac{|G|}{|H|}$. □

**Corollary 3.5.**
Let $G$ be a finite group.
1. If $g \in G$, then $o(g) \mid |G|$.
2. If $|G| = n$, then for all $g \in G$, we have $g^n = 1$.

**Proof.**

1. Take $H = \langle g \rangle$. Note that $|H| = o(G)$.
2. Let $o(g) = m$. Then by (1) we have $m \mid n$. Thus

$$g^n = (g^m)^{\frac{n}{m}} = 1^{\frac{n}{m}} = 1$$

□

**Example.**
For $n \in \mathbb{N}, n \geq 2$, let $\mathbb{Z}_n^*$ be the set of (multiplicative) invertible elements in $\mathbb{Z}_n$. Let the **Euler's $\varphi$-function**, $\varphi(n)$, denote the order of $\mathbb{Z}_n^*$:

$$\varphi(n) = |\{[k] \in \mathbb{Z}_n : k \in \{0, \ldots, n-1\}, \gcd(k, n) = 1\}|$$

As a direct consequence of the previous corollary, we see that if $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. This is Euler's thoerem. If $n = p$ is a prime number, then Euler's theorem implies $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's little theorem.

Recall that $|G| = 2 \implies G \cong C_2$ and $|G| = 3 \implies G \cong C_3$.

**Corollary 3.6.**
If $G$ is a group with $|G| = p$, a prime number, then $G \cong C_p$, the cyclic group of order $p$.

**Proof.** Let $g \in G$ with $g \neq 1$. Then we have $o(g) \mid p$. Since $g \neq 1$ and $p$ is prime, we have $o(g) = p$. Thus, $|\langle g \rangle| = o(g) = p$. It follows that $G = \langle g \rangle \cong C_p$. $\square$

**Corollary 3.7.**
Let $H, K$ be finite subgroups of $G$. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

## §3.3. Normal subgroups

**Definition** (Normal).
Let $H$ be a subgroup of $G$. If $gH = Hg$ for all $g \in G$, then we say $H$ is **normal**, denoted by $H \lhd G$.

**Example.**
We have $\{1\} \lhd G$ and $G \lhd G$.

**Example.**
The center of $G$, $Z(G) = \{z \in g : zg = gz \ \forall g \in G\}$ is an abelian subgroup of $G$. By its definition, $Z(G) \lhd G$. Thus every subgroup of $Z(G)$ is normal in $G$.

**Example.**
If $G$ is an abelian group, then every subgroup of $G$ is normal in $G$. The converse is false.

**Proposition 3.8** (Normality test).
Let $H$ be a subgroup of a $G$. The following are equivalent:
1. $H \lhd G$
2. $gHg^{-1} \subseteq H \ \forall g \in G$ (conjugate of $H$)
3. $gHg^{-1} = H \ \forall g \in G$

**Remark.**
To prove normality by the normality test, showing (2) is enough.

**Proof.** (1) $\implies$ (2). Let $ghg^{-1} \in gHg^{-1}$ for some $h \in H$. Then, by (1), $gh \in gH = Hg$. Suppose $gh = h_1 g$ for some $h_1 \in H$. Then

$$ghg^{-1} = h_1 gg^{-1} = h_1 \in H$$

(2) $\implies$ (3). If $g \in G$, then by (2), $gHg^{-1} \subseteq H$. Taking $g^{-1}$ in place of $g$ in (2), we get $g^{-1}Hg \subseteq H$. Then $H \subseteq gHg^{-1}$ so $H = gHg^{-1}$.

(3) $\implies$ (1) If $gHg^{-1} = H$, then $gH = Hg$. □

**Example.**
Let $G = GL_n(\mathbb{R})$ and $H = SL_n(\mathbb{R})$. For $A \in G, B \in H$, we have

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(B) = 1$$

Thus $ABA^{-1} \in H$ and it follows that $AHA^{-1} \subseteq H \ \forall A \in G$. By normality test, $H \lhd G$, which means $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

**Proposition 3.9.**
If $H$ is a subgroup of $G$ with $[G : H] = 2$, then $H \lhd G$.

**Proof.** Let $g \in G$. If $g \in H$, then $Hg = H = gH$.

If $g \notin H$, since $[G : H] = 2$, then $G = H \cup Hg$, a disjoint union. Then $Hg = G \setminus H$. Similarly, $gH = G \setminus H$. Thus $gH = Hg \ \forall g \in G$, so $H \lhd G$. □

**Example.**
Let $A_n$ be the alternating group contained in $S_n$. Since $[S_n : A_n] = 2$, we have $A_n \lhd S_n$.

**Example.**
Let $D_{2n}$ be the dihedral group of order $2n$. Since $[D_{2n} : \langle a \rangle] = 2$, we have $\langle a \rangle \lhd D_{2n}$.

Let $H, K$ be subgroups of $G$. The intersection $H \cap K$ is the "largest" subgroup of $G$ contained in both $H$ and $K$. What is the "smallest" subgroup containing $H$ and $K$?

Note that $H \cup K$ is the "smallest subset" containing $H$ and $K$, but $H \cup K$ is a subgroup of $G$ iff $H \subseteq K$ or $K \subseteq H$. A more useful subset to consider is the **product** $HK$ of $H$ and $K$ defined as follows:

$$HK = \{hk : h \in H, k \in K\}$$

Note this is still not always a subgroup of $G$.

**Lemma 3.10.**
Let $H$ and $K$ be subgroups of $G$. The following are equivalent:
1. $HK$ is a subgroup of $G$
2. $HK = KH$
3. $KH$ is a subgroup of $G$

**Proof.** We will prove (1) $\iff$ (2), then (2) $\iff$ (3) follows.

(2) $\implies$ (1). We have $1 = 1(1) \in HK$. Also, if $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. And, for $hk, h_1, k_1 \in HK$, we have $kh_1 \in KH = HK$, say $kh_1 = h_2k_2$. It follows that

$$(hk)(h_1k_1) = h(kh_1)k_1 = h(h_2k_2)k_1 = (hh_2)(k_2k_1) \in HK$$

By subgroup test, $HK$ is a subgroup of $G$.

(1) $\Longrightarrow$ (2). Let $kh \in KH$ with $k \in K$ and $h \in H$. Since $H$ and $K$ are subgroups of $G$, we have $h^{-1} \in H$ and $k^{-1} \in K$. As $HK$ is a subgroup of $G$, we have

$$(kh) = (h^{-1}k^{-1})^{-1} \in HK$$

Thus $KH \subseteq HK$. Similarly, we can show $HK \subseteq KH$, so $HK = KH$. □

**Proposition 3.11.**
Let $H$ and $K$ be subgroups of $G$.
1. If $H \lhd G$ or $K \lhd G$, then $HK = KH$ is a subgroup of $G$.
2. If $H \lhd G$ and $K \lhd G$, then $HK \lhd G$.

**Proof.**

1. Suppose $H \lhd G$. Then,
$$HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kH = KH$$
Then, $HK = KH$ is a subgroup of $G$.
2. If $g \in G$ and $hk \in HK$, since $H \lhd G$ and $K \lhd G$, we have
$$g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$$

Thus $g^{-1}HKg \subseteq HK$ and $HK \lhd G$. □

**Definition** (Normalizer).
Let $H$ be a subgroup of $G$. The **normalizer** of H, $N_G(H)$, is defined to be

$$N_G(H) = \{g \in G : gH = Hg\}$$

which has that $H \lhd G$ iff $N_G(H) = G$.

In the previous proof, we do not need the full assumption that $H \lhd G$. We only need $kH = Hk$ for all $k \in K$, that is $k \in N_G(H)$.

**Corollary 3.12.**
Let $H$ and $K$ be subgroups of a group $G$. If $K \subseteq N_G(H)$ (or $H \subseteq N_G(K)$), then $HK = KH$ is a subgroup of $G$.

**Theorem 3.13.**
If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $HK \cong H \times K$.

**Proof.** We first will show that, (1) if $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$, then $hk = kh$ for all $h \in H$ and $k \in K$.

Consider $x = hk(kh)^{-1} = hkh^{-1}k^{-1}$. Note that $kh^{-1}k^{-1} \in kHk^{-1} = H$ (since $H \lhd G$). Thus $x = h(kh^{-1}k) \in H$. Similarly, since $hkh^{-1} \in hKh^{-1} = K$, we have $x = (hkh^{-1})k^{-1} \in K$.

Since $x \in H \cap K = \{1\}$, we have $hkh^{-1}k^{-1} = 1$, so $hk = kh$. As $H \lhd G$, by property of normality, we have that $HK$ is a subgroup of $G$.

Now, define $\sigma : H \times K \to HK$ by $\sigma((h,k)) = hk$. We will show that (2) $\sigma$ is an IM.

Let $(h,k), (h_1,k_1) \in H \times K$. By (1), we have $h_1 k = k h_1$. Thus

$$\begin{aligned}\sigma((h,k)(h_1,k_1)) &= \sigma((hh_1, kk_1)) = (hh_1)(kk_1) = h(h_1k)k_1 \\ &= h(kh_1)k_1 = (hk)(h_1k_1) = \sigma((h,k))\sigma((h_1,k_1))\end{aligned}$$

so $\sigma$ is a HM.

Note that by the definition of $HK$, $\sigma$ is onto. Also, if $\sigma((h,k)) = \sigma((h_1,k_1))$, we have $hk = h_1k_1$. Thus $h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$. So, $h_1^{-1}h = 1 = k_1k^{-1}$ ($h_1 = h$ and $k_1 = k$). Thus $\sigma$ is one-to-one.

Thus, $\sigma$ is an IM and we have $HK \cong H \times K$. □

**Corollary 3.14.**
Let $G$ be a finite group, and $H, K$ be normal subgroups of $G$ such that $H \cap K = \{1\}$ and $|H||K| = |G|$. Then $G \cong H \times K$.

**Example.**
Let $m, n \in \mathbb{N}$ and $\gcd(m,n) = 1$. Let $G = \langle a \rangle$ be the cyclic group with $\mathrm{O}(G) = mn$.. Let $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$.

Then, $|H| = \mathrm{O}(a^n) = m$ and $|K| = \mathrm{O}(a^m) = n$. It follows that $|H||K| = mn = |G|$. Since $\gcd(m,n) = 1$, we have $H \cap K = \{1\}$. Also, since $G$ is cyclic (abelian), we have $H \lhd G$ and $K \lhd G$

Then, we have $G \cong H \times K$. That is, $C_{mn} \cong C_m \times C_n$.

Hence to consider finite cyclic groups, it suffices to consider cyclic groups of prime power order.

# §4. Isomorphism theorems

## §4.1. Quotient groups

Let $K$ be a subgroup of $G$. Consider the set of right cosets of $K$, $\{Ka : a \in G\}$. To make it a group, a natural way is to define

$$Ka \cdot Kb = Kab \quad \forall a, b \in G$$

Note that we could have $Ka = Ka_1$ and $Kb = Kb_1$ with $a \neq a_1$ and $b \neq b_1$. Thus in order for the previous equation to make sense, a necessary condition is

$$Ka = Ka_1, Kb = Kb_1 \implies Kab = Ka_1b_1$$

In this case, we say that the multiplication $KaKb = Kab$ is well-defined.

**Lemma 4.1 .**
Let $K$ be a subgroup of $G$. The following are equivalent:
1. $K \lhd G$.
2. For $a, b \in G$, the multiplication $KaKb$ is well-defined.

**Proof.** (1) $\implies$ (2). Let $Ka = Ka_1$ and $Kb = Kb_1$. Thus $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$.

To get $Kab = Ka_1b_1$, we need $ab(a_1b_1)^{-1} \in K$. Note that since $K \lhd G$, we have $aKa^{-1} = K$. Thus,

$$ab(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1} = (abb_1^{-1}a^{-1})(aa_1^{-1}) \in K$$

so $Kab = Ka_1b_1$.

(2) $\implies$ (1). If $a \in G$, to show $K \lhd G$, we need $aka^{-1} \in K, \forall k \in K$. Since $Ka = Ka$ and $Kk = K1$, by (2), we have $Kak = Ka1$, i.e. $Kak = Ka$. It follows that $aka^{-1} \in K$. Thus $K \lhd G$. $\square$

**Proposition 4.2 .**
Let $K \lhd G$ and write $G/K = \{Ka : a \in G\}$ for the set of all cosets of $K$. Then,
1. $G/K$ is a group under the operation $KaKb = Kab$.
2. The mapping $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is an onto HM.
3. If $[G : K]$ is finite, then $|G/K| = [G : K] = \frac{|G|}{|K|}$.

**Definition** (Quotient group)**.**
Let $K \lhd G$. The group $G/K$ of all cosets $K$ in $G$ is called the **quotient group** of $G$ by $K$. And, the mapping $\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is called the **coset map**.

Remark .
$G/K$ represents the set of **all distinct cosets** (left or right) of $K$ generated by $G$. It is not a subgroup of $G$.

**Problem 4.1 .**
List all normal subgroups of $D_{10}$ and all quotient groups of $D_{10}/K$.

## §4.2. Isomorphism theorems

**Definition** (Kernel)**.**
Let $\alpha : G \to H$ be a group HM. The **kernel** of $\alpha$ is defined by

$$\ker(\alpha) = \{g \in G : \alpha(g) = I_H\} \subseteq G$$

which is the set of all elements in $G$ for which $\alpha$ maps to the identity in $H$.

**Definition** (Image).
The **image** of $\alpha$ is defined by

$$\mathrm{im}(\alpha) = \alpha(G) = \{\alpha(g) : g \in G\} \subseteq H$$

**Proposition 4.3**.
Let $\alpha : G \to H$ be a group HM. Then,
1. $\mathrm{im}(\alpha)$ is a subgroup of $H$.
2. $\ker(\alpha) \lhd G$.

**Proof.**

1. Note that $I_H = \alpha(I_G) \in \alpha(G)$. Also, for $h_1 = \alpha(g_1), h_2 = \alpha(g_2) \in \alpha(G)$, we have

$$h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G)$$

   Also, $\alpha(g)^{-1} = \alpha(g^d) \in \alpha(G)$. By the subgroup test, $\alpha(G)$ is a subgroup of $H$.
2. For $\ker(\alpha)$, note that $\alpha(I_G) = I_H$. And, for $k_1, k_2 \in \ker(\alpha)$, we have

$$\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1 \cdot 1 = 1$$

   and

$$\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1$$

   By the subgroup test, $\ker(\alpha)$ is a subgroup of $G$. Note that if $g \in G$ and $k \in \ker(\alpha)$, then

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g) \cdot 1 \cdot \alpha(g)^{-1} = 1$$

   Thus $g \ker(\alpha) g^{-1} \subseteq \ker(a)$. By the normality test, $\ker(\alpha) \lhd G$.

$\square$

**Example**.
Consider the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ defined by $A \mapsto \det(A)$.

Then, $\ker(\det) = SL_n(\mathbb{R})$ and $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

**Example**.
Define the **sign** of a permutation $\sigma \in S_n$ by

$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

Note that $\mathrm{sgn} : S_n \to (\pm 1, \cdot)$ defined by $\sigma \mapsto \mathrm{sgn}(\sigma)$ is a HM. Also, $\ker(\mathrm{sgn}) = A_n$. Thus we have another example that $A_n \lhd S_n$.

**Theorem 4.4** (1st IM).
Let $\alpha : G \to H$ be a group HM. We have $G/\ker(\alpha) \cong \operatorname{im}(\alpha)$.

**Proof.** Let $K = \ker(\alpha)$. Since $K \lhd G$, $G/K$ is a group. Define the group map $\bar{\alpha} : G/K \to \operatorname{im}(\alpha)$ by

$$\bar{\alpha}(Kg) = \alpha(g) \quad \forall Kg \in G/K.$$

Note that

$$Kg = Kg_1 \iff gg_1^{-1} \in K = \ker(\alpha) \iff \alpha(gg_1^{-1}) = 1 \iff \alpha(g) = \alpha(g_1)$$

Thus $\bar{\alpha}$ is well-defined and one-to-one. Also, $\bar{\alpha}$ is clearly onto.

For $g, h \in G$, we have

$$\bar{\alpha}(KgKh) = \bar{\alpha}(K(gh)) = \alpha(gh) = \alpha(g)\alpha(h) = \bar{\alpha}(Kg)\bar{\alpha}(Kh)$$

Thus $\bar{\alpha}$ is a group IM and we have $G/\ker(\alpha) \cong \operatorname{im}(\alpha)$. $\square$

Let $\alpha : G \to H$ be a group HM and $K = \ker(\alpha)$. Let $\varphi : G \to G/K$ be the coset map and let $\bar{\alpha}$ be defined as in the previous proof. We have the following relationship:

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & \operatorname{im}(\alpha) \\ G/\ker(\alpha) \arrow[ur, "\bar{\alpha}"] & \end{tikzcd}$$

Note that for $g \in G$, we have

$$\bar{\alpha}\varphi(g) = \bar{\alpha}(Kg) = \alpha(g)$$

Thus $\alpha = \bar{\alpha}\varphi$.

On the other hand, if we have $\alpha = \bar{\alpha}\varphi$, then the action of $\bar{a}$ is determined by $\alpha$ and $\varphi$ as

$$\bar{\alpha}(Kg) = \bar{\alpha}(\varphi(g)) = \alpha(g)$$

Thus $\bar{\alpha}$ is the *only* HM $G/K \to H$ satisfying $\bar{\alpha}\varphi = \alpha$.

**Proposition 4.5**.
Let $\alpha : G \to H$ be a group HM and $K = \ker(\alpha)$. Then $\alpha$ factors uniquely as $\alpha = \bar{\alpha}\varphi$ where $\varphi : G \to G/K$ is the coset map and $\bar{\alpha} : G/K \to H$ is defined by $\bar{\alpha}(Kg) = \alpha(g)$.

Note that $\varphi$ is onto and $\bar{\alpha}$ is one to one.

**Example.**
We have seen that $(\mathbb{Z}, +) = \langle \pm 1 \rangle$ and for $n \in \mathbb{N}$, $(\mathbb{Z}_n, +) = \langle [1] \rangle$ are cyclic groups. We will show that these two together represent all cyclic groups.

Let $G = \langle g \rangle$ be a cyclic group. Consider $\alpha : (\mathbb{Z}, +) \to G$ defined by $\alpha(k) = g^k$ for all $k \in \mathbb{Z}$, which is a group HM. By the definition of $\langle g \rangle$, $\alpha$ is onto. Note that $\text{im}(\alpha) = G$ and $\ker(\alpha) = \{k \in \mathbb{Z} : g^k = 1\}$. We have two cases.

Suppose $o(g) = \infty$. Then $\ker(\alpha) = \{0\}$. By 1st IM, we have $G \cong \mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$.

Suppose $o(g) = n$. Then, by Proposition 2.6, $\ker(\alpha) = n\mathbb{Z}$. By 1st IM, we have $G \cong \mathbb{Z}/(n\mathbb{Z}) \cong \mathbb{Z}_n$.

Thus, we can conclude that if $G$ is cyclic, then $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_n$.

**Theorem 4.6** (2nd IM).
Let $H, K$ be subgroups of $G$ with $K \lhd G$. Then,
- $HK$ is a subgroup of $G$.
- $K \lhd HK$.
- $H \cap K \lhd H$.
- $HK/K \cong H/H \cap K$.

**Proof.** Since $K \lhd G$, by Proposition 3.11, $HK$ is a subgroup, $HK = KH$ and $K \lhd HK$.

Consider $\alpha : H \to HK/K$ defined by $\alpha(h) = Kh$ (note that $h \in H \subseteq HK$). Then $\alpha$ is a HM. Also, if $x \in HK = KH$, say $x = kh$, then

$$Kx = K(kh) = kh = \alpha(h)$$

Thus $\alpha$ is onto.

Finally, by Proposition 3.3,

$$\ker(\alpha) = \{h \in H : Kh = K\} = \{h \in H : h \in K\} = H \cap K$$

By 1st IM, $H/H \cap K \cong HK/K$. $\square$

**Theorem 4.7** (3rd IM).
Let $K \subseteq H \subseteq G$ be groups with $K \lhd G$ and $H \lhd G$. Then,
- $H/K \lhd G/K$.
- $(G/K)/(H/K) \cong G/H$.

**Proof.** Define $\alpha : G/K \to G/H$ by $\alpha(Kg) = Hg$ for all $g \in G$. Note that if $Kg = Kg_1$, then $gg_1^{-1} \in K \subseteq H$. Thus $Hg = Hg_1$, and $\alpha$ is well-defined and onto.

Note that

$$\ker(\alpha) = \{Kg : Hg = H\} = \{Kg : g \in H\} = H/K$$

By 1st IM,

$$(G/K)/(H/K) \cong G/H$$

□

# §5. Group actions

## §5.1. Cayley's theorem

**Theorem 5.1** (Cayley's theorem).
If $G$ is a finite group of order $n$, then $G$ is isomorphic to a subgroup of $S_n$.

**Proof.** Let $G = \{g_1, ..., g_n\}$. Let $S_G$ be the permutation group of $G$. By identifying $g_i$ with $i$, we see that $S_G \cong S_n$. Thus it suffices to find a one-to-one HM $\sigma : G \to S_G$.

For $a \in G$, define $\mu_a : G \to G$ by $\mu_a(g) = ag$ for all $g \in G$. Note that $ag = ag \Longrightarrow g = g$, and $a(a^{-1}g) = g$. Hence $\mu_a$ is a bijection and $\mu_a \in S_G$.

Now define $\sigma : G \to S_G$ by $\sigma(a) = \mu_a$. For $a, b \in G$, we have $\mu_a \mu_b = \mu_{ab}$ and $\sigma$ is HM. Also, if $\mu_a = \mu_b$, then $a = \mu_a(1) = \mu_b(1) = b$. Thus $\sigma$ is a one-to-one HM.

By 1st IM, we have $G \cong \mathrm{im}(\sigma)$, which is a subgroup of $S_G \cong S_n$. □

**Example.**
Let $H$ be a subgroup of $G$ with $[G : H] = m < \infty$. Let $X = \{g_1 H, g_2 H, ..., g_m H\}$ be the set of all distinct left cosets of $H$ in $G$.

For $a \in G$, define $\lambda_a : X \to X$ by

$$\lambda_a(gH) = agH \quad \forall gH \in X$$

Note that $agH = ag_1 H$ implies $gH = g_1 H$ and $a(a_{-1} gH) = gH$. Hence $\lambda_a$ is a bijection and thus $\lambda_a \in S_x$.

Consider $\tau : G \to S_x$ defined by $\tau(a) = \lambda_a$. For $a, b \in G$, we have $\lambda_{ab} = \lambda_a \lambda_b$, thus $\tau$ is a HM. Note that if $a \in \ker(\tau)$, then $\lambda_a$ is the identity permutation. In particular, $aH = \lambda_a(H) = H$ and $a \in H$. Thus, $\ker(\tau) \subseteq H$.

**Theorem 5.2** (Extended Cayley's theorem).
Let $H$ be a subgroup of $G$ with $[G : H] = m < \infty$. If $G$ has a normal subgroup contained in $H$ except for $\{1\}$, then $G$ is isomorphic to a subgroup of $S_m$.

**Proof.** Let $X$ be the set of all distinct left cosets of $H$ in $G$. Then we have $|X| = m$ and $S_x \cong S_m$.

We have seen from the above example that there exists a group HM $\tau : G \to S_x$ with $K = \ker(\tau) \subseteq H$. By 1st IM, we have $G/K \cong \mathrm{im}(\tau)$. Since $K \subseteq H$ and $K \lhd G$, by the assumption, we have $K = \{1\}$. It follows that $G \cong \mathrm{im}(\tau)$, a subgroup of $S_x \cong S_m$. □

**Corollary 5.3**.
Let $G$ be a finite group and $p$ be the smallest prime dividing $|G|$. If $H$ is a subgroup of $G$ with $[G : H] = p$, then $H \lhd G$.

**Proof.** Let $X$ be the set of all distinct left cosets of $H$ in $G$. Then we have $|X| = p$ and $S_x \cong S_p$.

Let $\tau : G \to S_x \cong S_p$ be the group HM defined in the previous example with $K = \ker(\tau) \subseteq H$. By 1st IM, we have $G/K \cong \mathrm{im}(\tau) \subseteq S_p$. Thus $G/K$ is isomorphic to a subgroup of $S_p$.

By Lagrange's theorem, $|G/K| \mid |S_p| = p!$. Also, since $K \subseteq H$, if $[H : k] = k$, then $|G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = k$. Thus $pk \mid p!$ and hence $k \mid (p-1)!$. Since $k \mid |H|$ which divides $|G|$ and $p$ is the smallest prime dividing $|G|$, we see that every prime divisor of $k$ must be $\geq p$ unless $k = 1$. Combining this with $k \mid (p-1)!$, this forces $k = 1$, which implies $K = H$. Thus $H \lhd G$. □

## §5.2. Group actions

**Definition** (Group action).
Let $X$ be a non-empty set. A (left) **group action** of $G$ on $x$ is a mapping $G \times X \to X$, denoted $(a, x) \mapsto a \cdot x$ such that
1. $1 \cdot x = x \ \forall x \in X$
2. $a \cdot (b \cdot x) = (ab) \cdot x \ \forall a, b \in G, x \in X$

In this we say $G$ *acts on* $X$.

**Remark**.
Let $G$ be a group acting on a set $X \neq \emptyset$. For $a, b \in G$ and $x, y \in X$, by (1) and (2), we have

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y$$

In particular, we have $a \cdot x = a \cdot y \iff x = y$.

**Example**.
If $G$ is a group, let $G$ act on itself ($X = G$), by

$$a \cdot x = axa^{-1} \quad \forall a, x \in G$$

Note that

$$1 \cdot x = 1x1^{-1} = x$$

and

$$a(b \cdot x) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = (ab) \cdot x$$

In this case, we say $G$ acts on itself by *conjugation*.

**Definition** (Stabilizer).
Let $G$ act on $X \neq \emptyset$ and $x \in X$.

$$G \cdot x = \{g \cdot x : g \in G\} \subseteq X$$

is the **orbit** of $x$. And,

$$S(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

is the **stabilizer** of $x$.

Remark.
Orbit is like the image of $x$ under the action of $G$, and stabilizer is like the kernel of $x$ under the action of $G$.

**Proposition 5.4.**
1. $S(x)$ is a subgroup of $G$.
2. There exists a bijection $G \cdot x \to \{gS(x) : g \in G\}$, and thus $|G \cdot x| = [G : S(x)]$.

**Proof.**

1. Since $1 \cdot x = x$, we have $1 \in S(x)$. Also, if $g, h \in S(x)$, then

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

and

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x$$

thus $gh, g^{-1} \in S(x)$. By the subgroup test, $S(x)$ is a subgroup of $G$.

2.

□

**Theorem 5.5** (Orbit decomposition theorem).
Let $G$ be a group acting on set $X \neq \emptyset$. Let

$$X_f = \{x \in X : a \cdot x = x \ \forall a \in G\}$$

Note that $x \in X_f \iff |G \cdot x| = 1$.

Let $G \cdot x_1, ..., G \cdot x_n$ denote the distinct non-singleton orbits (i.e. $|G \cdot x_i| > 1$). Then,

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

**Proof.** Note that for $a, b \in G$ and $x, y \in X$,

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y \iff y \in G \cdot x \iff G \cdot y = G \cdot x$$

Thus two orbits are either disjoint or the same, so the orbits form a disjoint union of $X$.

Since $x \in X_f$ iff $|G \cdot x| = 1$, the set $X \setminus X_f$ contain all non-singleton orbits, which are disjoint. Thus, by Proposition 5.4, we have

$$\begin{aligned} |X| &= |X_f| + \sum_{i=1}^{n} |G \cdot x_i| \\ &= |X_f| + \sum_{i=1}^{n} [G : S(x_i)] \end{aligned}$$

□

Let $G$ be a group acting on itself by conjugation ($g \cdot x = gxg^{-1}$). Then,

$$\begin{aligned} G_f &= \{x \in G : gxg^{-1} = x \ \forall g \in G\} \\ &= \{x \in G : gx = xg \ \forall g \in G\} \\ &= Z(G) \end{aligned}$$

Also, for $x \in G$,

$$\begin{aligned} S(x) &= \{g \in G : gxg^{-1} = x\} \\ &= \{g \in G : gx = xg\} \end{aligned}$$

This set is called the **centralizer** of $x$ and is denoted by $S(x) = C_G(x)$.

Finally, in this case, the orbit

$$G \cdot x = \{gxg^{-1} : g \in G\}$$

is called the **conjugacy class** of $x$.

By Theorem 5.5, we get

**Corollary 5.6** (Class equation).
Let $G$ be a finite group and let $\{gx_1g^{-1} : g \in G\}, \ldots, \{gx_ng^{-1} : g \in G\}$ denote the distinct non-singleton conjugacy classes. Then,

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)]$$

**Lemma 5.7**.
Let $p$ be prime and $m \in \mathbb{N}$. Let $G$ be a group of order $p^m$ acting on a finite set $X \neq \emptyset$. Let $X_f$ be denoted as in Theorem 5.5. Then we have

$$|X| \equiv |X_f| \pmod{p}$$

**Proof.** By Theorem 5.5, we have

$$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$$

with $[G : S(x_i)] > 1$ for $1 \leq i \leq n$.

Since $[G : S(x_i)]$ divides $|G| = p^m$ and $[G : S(x_i)] > 1$, we have $p \mid [G : S(x_i)]$ for all $i$. It follows that

$$|X| \equiv |X_f| \pmod{p}$$

□

**Theorem 5.8** (Cauchy's Theorem).
Let $p$ be prime and $G$ be a finite group. If $p \mid |G|$, then $G$ contains an element of order $p$.

**Proof.** Define

$$X = \{(a_1, ..., a_p) : a_i \in G, a_1 \cdots a_p = 1\}$$

Since $a_p$ is uniquely determined by $a_1, ..., a_{p-1} \in G$, if $|G| = n$, we have $|X| = n^{p-1}$. Since $p \mid n$, we have $|X| \equiv 0 \pmod{p}$.

Let the group $\mathbb{Z}_p = (\mathbb{Z}_p, +)$ act on $X$ by *cycling*, that is for $k \in \mathbb{Z}_p$,

$$k \cdot (a_1, ..., a_p) = (a_{k+1}, ..., a_p, a_1, ..., a_k)$$

One can verify that this action is well-defined.

Let $X_f$ be defined as in Theorem 5.5. Then $(a_1, ..., a_p) \in X_f$ iff $a_1 = a_2 = \cdots = a_p$. Clearly, $(1, ..., 1) \in X_f$ and hence $|X_f| \geq 1$. Since $|\mathbb{Z}_p| = p$, by Lemma 5.7, we have

$$|X_f| \equiv |X| \equiv 0 \pmod{p}$$

And since $|X| \equiv 0 \pmod{p}$ and $|X_f| \geq 1$, it follows that $|X_f| \geq p$. Therefore, there exists $a \neq 1$ such that $(a, ..., a) \in X_f$, which implies that $a^p = 1$. Since $p$ is a prime and $a \neq 1$, the order of $a$ is $p$. □

# §6. Sylow theorems

## §6.1. p-groups

**Definition** ($p$-group).
Let $p$ be prime. A group in which every element has order of a non-negative power of $p$ is called a ***p*-group**.

As a direct corollary of Cauchy's theorem (Theorem 5.8), we have

**Corollary 6.1**.
A finite group $G$ is a $p$-group iff $|G|$ is a power of $p$.

**Lemma 6.2**.
The center $Z(G)$ of a non-trivial finite $p$-group $G$ contains more than one element.

**Proof.** The class equation of $G$ (Corollary 5.6) states that

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $[G : C_G(x_i)] > 1$.

Since $G$ is a $p$-group, by Corollary 6.1, $p \mid |G|$. By Lemma 5.7, $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$. It follows that $p \mid |Z(G)|$.

Since $1 \in Z(G)$ and $Z(G) \geq 1$, $Z(G)$ has at least $p$ elements. □

Recall that if $H$ is a subgroup of $G$, then

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

is the normalizer of $H$ in $G$. In particular, $H \lhd N_G(H)$.

**Lemma 6.3**.
If $H$ is a $p$-subgroup of a finite group $G$, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}$$

**Proof.** Let $X$ be the set of all left cosets of $H$ in $G$. Hence $|X| = [G : H]$. Let $H$ act on $X$ by left multiplication. Then for $x \in G$, we have

$$\begin{aligned} xHx^{-1} &\iff hxH = xH \quad \forall h \in H \\ &\iff x^{-1}hxH = H \quad \forall h \in H \\ &\iff x^{-1}Hx = H \\ &\iff x \in N_G(H) \end{aligned}$$

Thus $|X_f|$ is the number of cosets $xH$ with $x \in N_G(H)$, and hence $|X_f| = [N_G(H) : H]$.

By Lemma 5.7,

$$[N_G(H) : H] = |X_f| \equiv |X| = [G : H] \pmod{p}$$

□

**Corollary 6.4**.
Let $H$ be a $p$-subgroup of a finite group $G$. If $p \mid [G : H]$, then $p \mid [N_G(H) : H]$ and $N_G(H) \neq H$.

**Proof.** Since $p \mid [G : H]$, by Lemma 6.3, we have

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$$

Since $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq 1$, we have $[N_G(H) : H] \geq p$. Thus $N_G(H) \neq H$. □

## §6.2. Sylow's three theorems

Recall Cauchy's theorem (Theorem 5.8) that states if $p \mid |G|$, then $|G|$ contains an element $a$ of order $p$. Thus $|\langle a \rangle| = p$. The following first Sylow theorem can be viewed as a generalization of Cauchy's theorem.

**Theorem 6.5** (1st Sylow theorem).
Let $G$ be a group of order $p^n m$ where $p$ is a prime, $n \geq 1$ and $\gcd(p, m) = 1$. Then $G$ contains a subgroup of order $p^i$ for all $1 \leq i \leq n$.

Moreover, every subgroup of $G$ of order $p^i$ $(i < n)$ is normal in some subgroup of order $p^{i+1}$.

**Proof.** We prove this theorem by induction on $i$.

For $i = 1$, since $p \mid |G|$, by Cauchy's theorem, $G$ contains an element $a$ such that $|\langle a \rangle| = p$.

Suppose the statement holds for some $i \leq i < n$, say $H$ is a subgroup of $G$ of order $p^i$. Then $p \mid [G : H]$. By Corollary 6.4, $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq p$. Then, by Cauchy's theorem, $N_G(H)/H$ contains a subgroup of order $p$. Such a group is of the form $H_1/H$, where $H_1$ is a subgroup of $N_G(H)$ containing $H$. Since $H \lhd N_G(H)$, we have $H \lhd H_1$. Finally,

$$|H_1| = |H||H_1/H| = p^i \cdot p = p^{i+1}$$

$\square$

**Definition** (Sylow $p$-subgroup).
A subgroup $P$ of $G$ is a **Sylow $p$-subgroup** of $G$ if $P$ is a maximal $p$-subgroup of $G$.

That is, if $P \subseteq H \subseteq G$ with $H$ a $p$-group, then $P = H$.

As a direct consequence of Theorem 6.5, we have

**Corollary 6.6**.
Let $G$ be a group of order $p^n m$ where $p$ is a prime, $n \geq 1$ and $\gcd(p, m) = 1$. Let $H$ be a $p$-subgroup of $G$. Then,
1. $H$ is a Sylow $p$-subgroup iff $|H| = p^n$.
2. Every conjugate of a Sylow $p$-subgroup is also a Sylow $p$-subgroup.
3. If there is only one Sylow $p$-subgroup $P$, then $P \lhd G$.

**Theorem 6.7** (2nd Sylow theorem).
If $H$ is a $p$-subgroup of a finite group $G$ and $P$ is any Sylow $p$-subgroup of $G$, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$.

In particular, any two Sylow $p$-subgroups of $G$ are conjugate.

**Proof.** Let $X$ be the set of all left cosets of $P$ in $G$, and let $H$ act on $X$ by left multiplication. By Lemma 5.7, we have $|X_f| \equiv |X| = [G : P] \pmod{p}$.

Since $p \nmid [G : P]$, we have $|X_f| \neq 0$. Thus there exists $gP \in X_f$ for some $g \in G$. Note that

$$\begin{aligned} gP \in X_f &\iff hgP = gP \quad \forall h \in H \\ &\iff g^{-1}hgP = P \quad \forall h \in H \\ &\iff g^{-1}Hg \subseteq P \\ &\iff H \subseteq gPg^{-1} \end{aligned}$$

If $H$ is a Sylow $p$-subgroup, then $|H| = |P| = |gHg^{-1}|$. Thus $H = gPg^{-1}$. $\square$

**Theorem 6.8** (3rd Sylow theorem).
If $G$ is a finite group and $p$ is prime with $p \mid |G|$, then the number of Sylow $p$-subgroups of $G$ divides $|G|$ and is of the form $kp + 1$ for some $K \in \mathbb{N} \cup \{0\}$.

**Proof.** By Theorem 6.7, the number of Sylow $p$-subgroups of $G$ is the number of conjugates of any of them, say $P$.

This number is $[G : N_G(P)]$ where $N_G(P) = \{g \in G : gP : Pg\}$, which is a divisor of $|G|$. Let $X$ be the set of all Sylow $p$-subgroups of $G$ and let $P$ act on $X$ by conjugation. Then $Q \in X_f$ iff $gQg^{-1} = G$ $\forall g \in P$. The latter condition holds iff $P \subseteq N_G(Q)$. Both $P$ and $Q$ are Sylow $p$-subgroups of $G$ and hence $N_G(Q)$.

Thus by Corollary 6.6, they are conjugate in $N_G(Q)$. Since $Q \lhd N_G(Q)$, this can only occur if $Q = P$ and $X_f = \{P\}$. By Lemma 5.7, $|X| \equiv |X_f| \equiv 1 \pmod p$. Thus $|X| = kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$. $\square$

Remark.
Suppose that $G$ is a group with $|G| = p^n m$ and $\gcd(p, m) = 1$. Let $n_p$ be the number of Sylow $p$-subgroups of $G$.

By the 3rd Sylow theorem, we have $n_p \mid p^n m$ and $n_p \equiv 1 \pmod p$. And since $p \nmid n_p$, we have $n_p \mid m$.

**Example.**
We will show that every group of order 15 is cyclic.

Let $G$ be a group of order $15 = 3 \cdot 5$. Let $n_p$ be the number of Sylow $p$-subgroups of $G$.

By Theorem 6.8 (3rd Sylow theorem), we have $n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$. Thus $n_3 = 1$. Similarly, we have $n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5$. Thus $n_5 = 1$.

It follows that there is only one Sylow 3-subgroup $P_3$ and one Sylow 5-subgroup $P_5$. Thus $P_3 \lhd G$ and $P_5 \lhd G$.

Consider $|P_3 \cap P_5|$, which divides 3 and 5. Thus $|P_3 \cap P_5| = 1$ and $P_3 \cap P_5 = \{1\}$. Also, $|P_3 P_5| = 15 = |G|$. Thus

$$G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$$

**Problem 6.1.**
Construct a cyclic group of order $> 100$.

**Example.**
There are two isomorphism classes of groups of order 21.

Let $G$ be a group of order $21 = 3 \cdot 7$. By 3rd Sylow theorem, $n_3 \mid 7$ and $n_3 \equiv 1 \pmod 3$. Thus $n_3 = 1$ or $7$. Also, we have $n_7 \mid 3$ and $n_7 \equiv 1 \pmod 7$. Thus, $n_7 = 1$.

It follows that $G$ has a unique Sylow 7-subgroup $P_7$. Note that $P_7 \in G$ and $P_7 = \langle x : x^7 = 1 \rangle$. Let $H$ be a Sylow 3-subgroup. Since $|H| = 3$, $H$ is cyclic and $H = \langle y : y^3 = 1 \rangle$. Since $P_7 \lhd G$, we have $gxg^{-1} = x^i$ for some $0 \leq i \leq 6$. Hence,

$$x = y^3 x y^{-3} = y^2 (yxy^{-1}) y^{-2} = y^2 (x^i) y^{-2} = x^{i^3}$$

Since $x^{i^3} = x$ and $x^7 = 1$, we have $i^3 = -i \equiv 0 \pmod 7$.

Since $0 \leq i \leq 6$, we have $i = 1, 2, 4$. If $i = 1$, then $yxy^{-1} = x \implies yx = xy$. Thus $G$ is an abelian group. Since $P_3 \lhd G$ $P_7 \lhd G$, $P_3 \cap P_7 = \{1\}$ and $|G| = |P_3 P_7|$. We have

$$G \cong P_3 \times P_7 \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$$

If $i = 2$, then $yxy^{-1} = x^2$. Thus

$$G = \{x^i y^i : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}$$

If $i = 4$, then $yxy^{-1} = x^4$. Note that

$$y^2 x y^{-2} = x^{16} = x^2$$

Note that $g^2$ is also a generator of $H$. Thus by replacing $y$ by $g^2$, we get back to case $i = 2$. It follows that there are two isomorphism classes of groups of order 21.

# §7. Finite abelian groups

## §7.1. Primary decomposition

Let $G$ be a group and $m \in \mathbb{Z}$, we define

$$G^{(m)} = \{g \in G : g^m = 1\}$$

**Proposition 7.1.**
Let $G$ be an abelian group. Then $G^{(m)}$ is a subgroup of $G$.

**Proof.** We have $1 = 1^m \in G^{(m)}$. Also, if $g, h \in G^{(m)}$, since $G$ is abelian, we have

$$(gh)^m = g^m h^m = 1$$

Finally, if $g \in G^{(m)}$ we have

$$g^{(-1)^m} = (g^m)^{-1} = 1$$

and thus $g^{-1} \in G^{((m)}$. By the subgroup test, $G^{(m)}$ is a subgroup of $G$. $\square$

**Proposition 7.2.**
Let $G$ be a finite abelian group and $|G| = mk$ with $\gcd(m, k) = 1$. Then,
1. $G \cong G^{(m)} \times G^{(k)}$
2. $\left|G^{(m)}\right| = m$ and $\left|G^{(k)}\right| = k$

**Proof.**

1. Since $G$ is abelian, we have $G^{(m)} \lhd G$ and $G^{(k)} \lhd G$. We will show that $G^{(m)} \cap G^{(k)} = \{1\}$ and $G = G^{(m)}G^{(k)}$.

   Let $g \in G^{(m)} \cap G^{(k)}$. Then $g^m = 1 = g^k$. We have
   $$g = g^{mx+ky} = (g^m)^x \left(g^k\right)^y = 1$$
   Let $g \in G$. Then,
   $$1 = g^{mk} = (g^m)^k = \left(g^k\right)^m$$
   It follows that $g^k \in G^{(m)}$ and $g^m \in G^{(k)}$. Thus
   $$g = g^{mx+ky} = (g^m)^x \left(g^k\right)^y \in G^{(m)}G^{(k)}$$
   Combining the two results, by Theorem 3.13, we have
   $$G \cong G^{(m)} \times G^{(k)}$$
2. Write $\left|G^{(m)}\right| = m'$ and $\left|G^{(k)}\right| = k'$. By (1), we have
   $$mk = |G| = m'k'$$
   We will show that $\gcd(m, k') = 1$.

   Suppose $\gcd(m, k') \neq 1$. Then there exists prime $p$ such that $p \mid m$ and $p \mid k'$. By Cauchy's theorem (Theorem 5.8), there exists $g \in G^{(k)}$ such that $o(g) = p$. Since $p \mid m$, we have
   $$g^m = (g^p)^{\frac{m}{p}} = 1$$
   that is, $g \in G^{((m)}$.

   By (1), we have $g \in G^{(m)} \cap G^{(k)} = \{1\}$, which gives a contradiction since $o(g) = p$. Thus we have $\gcd(m, k') = 1$.

   Note that since $m \mid m'k'$ and $\gcd(m, k') = 1$, we have $m \mid m'$. Similarly, we have $k \mid k'$. Since $mk = m'k'$, it follows that $m = m'$ and $k = k'$.

□

As a direct consequence of Proposition 7.2, we have

**Theorem 7.3** (Primary decomposition theorem).
Let $G$ be a finite abelian group and $|G| = p_1^{n_1} \cdots p_k^{n_k}$ where $p_1, \ldots, p_k$ are distinct primes and $n_1, \ldots, n_k \in \mathbb{N}$. Then,
1. $G \cong G^{\left(p_1^{n_1}\right)} \times \cdots \times G^{\left(p_k^{n_k}\right)}$
2. $\left|G^{\left(p_i^{n_i}\right)}\right| = p_i^{n_i}$ for all $1 \leq i \leq k$

**Example.**
Let $G = \mathbb{Z}_{13}^*$. Then $|G| = 12 = 2^2 \cdot 3$. Note that

$$G^{(3)} = \{a \in \mathbb{Z}_{13}^* : a^3 = 1\} = \{1, 3, 9\}$$
$$G^{(4)} = \{a \in \mathbb{Z}_{13}^* : a^4 = 1\} = \{1, 5, 8, 12\}$$

By Theorem 7.3, we have

$$\mathbb{Z}_{13}^* \cong \{1, 5, 8, 12\} \times \{1, 3, 9\}$$

## §7.2. Structure theorem of finite abelian groups

We have seen that if $|G| = p$ where $p$ is a prime, then $G \cong C_p$. Also, if $|G| = p^2$, then $G \cong C_{p^2} \cong C_p \times C_p$. What about abelian groups of order $p^n$ for general $n \in \mathbb{N}$?

**Proposition 7.4.**
Let $G$ be a finite abelian $p$-group that contains only one subgroup of order $p$. Then $G$ is cyclic.

In other words, if a finite abelian $p$-group $G$ is not cyclic, then $G$ has at least two subgroups of order $p$.

**Proof.** Let $y \in G$ be of maximal order ($o(y) \geq o(x)\ \forall x \in G$). We will show that $G = \langle y \rangle$.

Suppose that $G \neq \langle y \rangle$. Then the quotient group $G/\langle y \rangle$ is a non-trivial $p$-group, which contains an element $z \neq 1$ of order $p$ by Cauchy's theorem (Theorem 5.8).

Consider the coset map $\pi : G \to G/\langle y \rangle$. Let $x \in G$ such that $\pi(x) = z$. Since $\pi(x^p) = \pi(x)^p = z^p = 1$, we see that $x^p \in \langle y \rangle$. Thus $x^p = y^m$ for some $m \in \mathbb{Z}$. We have two cases.

If $p \nmid m$, since $o(y) = p^r$ for some $r \in \mathbb{N}$, by Proposition 2.11, $o(y^m) = o(y)$. Since $y$ is of maximal order, we have

$$o(x^p) < o(x) \leq o(y) = o(y^m) = o(x^p)$$

which leads to a contradiction.

If $p \mid m$, then $m = pk$ for some $k \in \mathbb{Z}$. Thus we have $x^p = y^m = y^{pk}$. Since $G$ is abelian, we have $(xy^{-k})^p = 1$. Thus $xy^{-k}$ belongs to the one and only subgroup of order $p$, say $H$. On the other hand, the cyclic group $\langle y \rangle$ contains a subgroup of order $p$, which must be $H$. Thus $xy^{-k} \in \langle y \rangle \implies x \in \langle y \rangle$. It follows that $z = \pi(x) = 1$, a contradiction.

Combing the two cases, we conclude that $G = \langle y \rangle$. □

**Proposition 7.5.**
Let $G \neq \{1\}$ be a finite abelian $p$-group. Let $C$ be a cyclic subgroup of max order. Then $G$ contains a subgroup $B$ such that $G = CB$ and $C \cap B = \{1\}$.

**Theorem 7.6.**
Let $G \neq \{1\}$ be a finite abelian $p$-group. Then $G$ is isomorphic to a direct product of cyclic groups.

**Proof.** By Proposition 7.5, there exists a cyclic group $C_1$ and a subgroup $B_1$ of $G$ such that $G \cong C_1 \times B_1$. Since $|B_1| \mid |G|$ by Lagrange's theorem, the group $B_1$ is also a $p$-group. Thus if $B_1 \neq \{1\}$, by Proposition 7.5, there exists a cyclic group $C_2$ and a subgroup $B_2$ such that $B_1 \cong C_2 \times B_2$. Continue in this way to get cyclic groups $C_1, ..., C_k$ until we get $B_k = \{1\}$ for some $k \in \mathbb{N}$. Then, $G \cong C_1 \times \cdots \times C_k$. □

**Remark.**
One can show that the decomposition of a finite abelian $p$-group into a direct product of cyclic group is unique up to its order.

Combining this remark, Theorem 7.6 and Theorem 7.3, we have

**Theorem 7.7** (Structure theorem of finite abelian groups).
If $G$ is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p_k}^{n_k}$$

where $\mathbb{Z}_{p_i}^{n_i} = \left(\mathbb{Z}_{p_i}^{n_i}, +\right) \cong C_{p_i}^{n_1}$ are cyclic groups of order $p_i^{n_i}$, $1 \leq i \leq k$.

Note that $p_i$ are not necessarily distinct. The numbers $p_i^{n_i}$ are uniquely determined up to their order.

Note that if $p_1$ and $p_2$ are distinct primes, then $C_{p_1}^{n_1} \times C_{p_2}^{n_2} \cong C_{p_1^{n_1} p_2^{n_2}}$. Thus by combining suitable coprime factors together,

**Theorem 7.8** (Invariant factor decomposition of finite abelian group).
Let $G$ be a finite abelian group. Then,

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$$

where $n_i \in \mathbb{N}$, $n_i > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_r$.

**Example.**
Let $G$ be an abelian group of order 48. Since $48 = 2^4 \cdot 3$, by Theorem 7.3, $G \cong H \times \mathbb{Z}_3$ where $H$ is an abelian group of order $2^4$. The options for $H$ are $\mathbb{Z}_{2^4}$, $\mathbb{Z}_{2^3} \times \mathbb{Z}_2$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Thus, we have:
1. $G \cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48}$
2. $G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24}$
3. $G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_{12}$
4. $G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$
5. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$

There are 5 non-isomorphic groups in total.

# §8. Rings

## §8.1. Rings

**Definition** (Ring).
A set $R$ is a (unitary) **ring** if it has two operations, addition $+$ and multiplication $\cdot$, such that $(R, +)$ is an abelian group and $(R, \cdot)$ satisfies the closure, associativity and identity properties of a group, and distributive law.

More precisely, for all $a, b, c \in R$,
1. $a + b \in R$
2. $a + (b + c) = (a + b) + c$
3. There exists $0 \in R$ (zero of $R$) such that $a + 0 = a = 0 + a$
4. There exists $-a \in R$ (negative of $R$) such that $a + (-a) = 0 = (-a) + a$
5. $a + b = b + a$
6. $ab = a \cdot b \in R$
7. $a(bc) = (ab)c \in R$
8. There exists $1 \in R$ (unity of $R$) such that $a \cdot 1 = 1 \cdot a$
9. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

**Definition** (Commutative ring).
Ring $R$ is a **commutative ring** if it also satisfies
10. $ab = ba$

**Example**.
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings with the zero being $0$ and the unity being $1$.

**Example**.
For $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a commutative ring with the zero being $[0]$ and the unity being $[1]$.

**Example**.
For $n \in \mathbb{N}$ with $n \geq 2$, the set $M_n(\mathbb{R})$ is a ring using matrix addition and matrix multiplication with the zero being the zero matrix and the unity being the identity matrix. Note that $\mathbb{M}_n(\mathbb{R})$ is not commutative.

**Remark**.
Note that since $(R, \cdot)$ is not a group, there is no left/right cancellation.

For example, $0 \cdot x = 0 \cdot y$ does not imply $x = y$.

Given a ring $R$, to distinguish the difference between multiples in addition and multiplication, for $n \in \mathbb{N}$ and $a \in R$ we write

$$na = a + \dots + a$$

and

$$a^n = a \cdot \dots \cdot a$$

Note that for a group $G$ and $g \in G$, we have $g^0 = 1$, $g^1 = g$ and $(g^{-1})^{-1}$. Thus for addition, we have

$$0 \cdot a = 0 \quad 1a = a \quad -(-a) = a$$

For $n \in \mathbb{N}$, we define

$$(-n)a = (-a) + \cdots + (-a)$$

Also, we define

$$a^0 = 1$$

If the multiplicative inverse of $a$ ($a^{-1}$) exists, we define

$$a^{-n} = (a^{-1})^n$$

Also, by Proposition 1.2, for $n, m \in \mathbb{Z}$, we have

$$(na) + (ma) = (n + m)a$$
$$n(ma) = (nm)a$$
$$n(a + b) = na + nb$$

We can also prove that

**Proposition 8.1.**
Let $R$ be a ring and $r, s \in R$.
1. If $0$ is the zero of $R$, then $0r = 0 = r0$ (all zeroes are the same zero of $R$)
2. $(-r)s = r(-s) = -(rs)$
3. $(-r)(-s) = rs$
4. For any $m, n \in \mathbb{Z}$, $(mr)(ns) = (mn)(rs)$

**Definition** (Trivial ring).
A **trivial ring** is a ring with only one element. In this case, we have $1 = 0$.

**Remark.**
If $R$ is a ring with $R \neq \{0\}$, since $r = r1$ for all $r \in \mathbb{R}$, we have $1 \neq 0$. Otherwise $r = r1 = r0 = 0$ by Proposition 8.1 for all $r \in R$.

**Example.**
Let $R_1, ..., R_n$ be rings. Define component-wise operations on the product $R_1 \times \cdots \times R_n$ as

$$(r_1, ..., r_n) + (s_1, ..., s_n) = (r_1 + s_1, ..., r_n + s_n)$$
$$(r_1, ..., r_n) \cdot (s_1, ...s_n) = (r_1 \cdot s_1, ..., r_n \cdot s_n)$$

One can check that $R_1 \times \cdots \times R_n$ is a ring with the zero being $\left(0_{R_1}, ..., 0_{R_n}\right)$ and the unity being $\left(1_{R_1}, ..., 1_{R_n}\right)$.

This set $R_1 \times \cdots \times R_n$ is called the **direct product** of $R_1, ..., R_n$.

**Definition** (Characteristic).
Let $R$ be a ring. We define the **characteristic** of $R$, $\mathrm{ch}(R)$, in terms of the order of $1_R$ in the additive group $(R, +)$:

$$\mathrm{ch}(R) = \begin{cases} n & o(1_R) = n \in \mathbb{N} \text{ in } (R,+) \\ 0 & o(1_R) = \infty \text{ in } (R,+) \end{cases}$$

For $k \in \mathbb{Z}$, we write $kR = 0$ to mean that $kr = 0\ \forall r \in R$. By Proposition 8.1, we have

$$kr = k(1_R r) = (k1_R)r$$

Thus $kR = 0$ iff $k1_R = 0$. By Proposition 2.6 and Proposition 2.7,

**Proposition 8.2**.
Let $R$ be a ring and $k \in \mathbb{Z}$.
1. If $\mathrm{ch}(R) = n \in \mathbb{N}$, then $kR = 0$ iff $n \mid k$.
2. If $\mathrm{ch}(R) = 0$, then $kR = 0$ iff $k = 0$.

**Example**.
Each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ has a characteristic 0.

For $n \in \mathbb{N}$ with $n \geq 2$, the ring $\mathbb{Z}_n$ has characteristic $n$.

## §8.2. Subrings

**Definition** (Subring).
A subset $S \subseteq R$ of ring $R$ is a **subring** if $S$ is a ring itself with $1_S = 1_R$ with the same addition and multiplication.

Note that properties (2), (3), (7), (9), are automatically satisfied. Thus to show that $S$ is a subring, it suffices to show

**Remark** (Subring test).
1. $1_R \in S$.
2. If $s, t \in S$, then $s + t \in S$ and $st \in S$.

Note that if (2) holds, then $0 = s - s \in S$ and $-t = 0 - t \in S$.

**Example**.
We have a chain of commutative rings $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

**Example.**
If $R$ is a ring, the center $Z(R)$ of $R$ is defined to be

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

Note that $1_R \in Z(R)$. Also, if $s, t \in Z(R)$, then for $r \in R$,

$$(s-t)r = sr - tr = rs - rt = r(s-t)$$
$$(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$$

By the subring test, $Z(R)$ is a subring of $R$.

**Example.**
Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\} \subseteq \mathbb{C}$. Then one can show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, called the **ring of Gaussian integers**.

## §8.3. Ideals

Let $R$ be a ring and $A$ be an additive subgroup of $(R, +)$. Since $(R, +)$ is abelian, we have $A \lhd R$. Thus we have the additive quotient group

$$R/A = \{r + A : r \in R\} \text{ with } r + A = \{r + a : a \in A\}$$

Using the known properties about cosets and quotient groups, we have

**Proposition 8.3.**
Let $R$ be a ring and $A$ an additive subgroup of $R$. For $r, s \in R$, we have
1. $r + A = s + A$ iff $(r - s) \in A$.
2. $(r + A) + (s + A) = (r + s) + A$.
3. $0 + A = A$ is the additive identity of $R/A$.
4. $-(r + A) = (-r) + A$ is the additive inverse of $r + A$.
5. $k(r + A) = kr + A \ \forall k \in \mathbb{Z}$.

To make $R/A$ a ring, a natural way to define multiplication in $R/A$ is

$$(r + A)(s + A) = rs + A \quad \forall r, s \in R$$

Note that we could have $r + A = r_1 + A$ and $s + A = s_1 + A$ with $r \neq r_1$ and $s \neq s_1$. In order for multiplication to make sense, a necessary condition is

$$r + A = r_1 + A \text{ and } s + A = s_1 + A \Longrightarrow rs + A = r_1 s_1 + A$$

In this case, we say the multiplication $(r + A)(s + A)$ is **well-defined**.

**Proposition 8.4.**
Let $A$ be an additive subgroup of ring $R$. For $a \in A$, define

$$Ra = \{ra : r \in R\}, \quad aR = \{ar : r \in R\}$$

The following are equivalent:
1. $Ra \subseteq A$ and $aR \subseteq A$ for all $a \in A$.
2. For $r, s \in R$, the multiplication $(r + A)(s + A) = rs + A$ is well-defined in $R/A$.

**Proof.** (1) $\Longrightarrow$ (2). Suppose $r + A = r_1 + A$ and $s + A = s_1 + A$. We need to show that $rs + A = r_1 s_1 + A$.

Since $(r - r_1) \in A$ and $(s - s_1) \in A$, by (1), we have

$$\begin{aligned} rs - r_1 s_1 &= rs - r_1 s + r_1 s - r_1 s_1 \\ &= (r - r_1)s + r_1(s - s_1) \in (r - r_1)R + R(s - s_1) \subseteq A \end{aligned}$$

By Proposition 8.3, $rs + A = r_1 s_1 + A$, so the multiplication is well-defined.

(2) $\Longrightarrow$ (1). Let $r \in R$ and $a \in A$. By Proposition 8.1, we have

$$ra + A = (r + A)(a + A) = (r + A)(0 + A) = r0 + A = 0 + A = A$$

Thus $ra \in A$ and we have $Ra \subseteq A$. Similarly, we can show $aR \subseteq A$. $\square$

**Definition (Ideal).**
An additive subgroup $A$ of ring $R$ is an **ideal** of $R$ if $Ra \subseteq A$ and $aR \subseteq A$ for all $a \in A$.

**Remark (Ideal test).**
1. $0 \in A$.
2. For $a, b \in A$ and $r \in R$, we have $a - b \in A$ and $ra, ar \in A$.

**Example.**
if $R$ is a ring, then $\{0\}$ and $R$ are ideals of $R$.

**Example.**
Let $R$ be a commutative ring and $a_1, \ldots, a_n \in R$. Consider the set $I$ generated by $a_1, \ldots, a_n$:

$$I = \langle a_1,\ldots,a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R\}$$

Then one can show that $I$ is an ideal of $R$.

**Proposition 8.5.**
Let $A$ be an ideal of a ring $R$. If $1_R \in A$, then $A = R$.

**Proof.** Let $r \in R$. Since $A$ is an ideal and $1_R \in A$, we have $r = r1_R \in A$. It follows that $R \subseteq A \subseteq R$, and hence $A = R$. $\square$

From the above discussion, we have

**Proposition 8.6.**
Let $A$ be an ideal of ring $R$. Then the additive quotient group $R/A$ is a ring with multiplication $(r + A)(s + A) = rs + A$. The unity of $R/A$ is $1 + A$.

**Definition** (Quotient ring).
Let $A$ be an ideal of a ring $R$. The ring $R/A$ is called the **quotient ring** of $R$ by $A$.

**Definition** (Principle).
Let $R$ be a commutative ring and $A$ an ideal of $R$. If $A = aR = \{ar : r \in R\} = Ra$ for some $a \in R$, we say $A$ is a principle ideal generated by $a$ and is denoted by $A = \langle a \rangle$.

**Example.**
If $n \in \mathbb{Z}$, then $\langle n \rangle = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

**Proposition 8.7.**
All ideals of $\mathbb{Z}$ are of form $\langle n \rangle$ for some $n \in \mathbb{Z}$. If $\langle n \rangle \neq \{0\}$ and $n \in \mathbb{N}$, then the generator is uniquely determined.

**Proof.** Let $A$ be an ideal of $\mathbb{Z}$. If $A = \{0\}$, then $A = \langle 0 \rangle$. Otherwise, choose $a \in A$ with $a \neq 0$ and $|a|$ minimum. Clearly $\langle a \rangle \subseteq A$.

To prove the other inclusion, let $b \in A$. By division algorithm, we have $b = qa + r$ with $q, r \in \mathbb{Z}$ and $0 < r < |a|$. If $r \neq 0$, since $A$ is an ideal and $a, b \in A$, we have $r = b - qa \in A$ with $|r| < |a|$, a contradiction. Thus $r = 0$ and $b = qa$, which means $b \in \langle a \rangle$. It follows that $A = \langle a \rangle$. $\square$

## §8.4. Isomorphism theorems

**Definition** (Ring homomorphism mapping).
Let $R, S$ be rings. A mapping $\theta : R \to S$ is a **ring homomorphism** if for all $a, b \in R$,
1. $\theta(a + b) = \theta(a) + \theta(b)$
2. $\theta(ab) = \theta(a)\theta(b)$
3. $\theta(1_R) = 1_S$

**Example.**
The mapping $k \to [k]$ from $\mathbb{Z} \to \mathbb{Z}_n$ is an onto ring HM.

**Example.**
If $R_1, R_2$ are rings, the projection $\pi_1 : R_1 \times R_2 \to R_1$ defined by $\pi_1(r_1, r_2) = r_1$ is an onto ring HM. Similarly, $\pi_2 : R_1 \times R_2 \to R_2$ defined by $\pi_2(r_1, r_2) = r_2$ is also an onto ring HM.

**Proposition 8.8.**
Let $\theta : R \to S$ be a ring HM and let $r \in R$. Then,
1. $\theta(0_R) = 0_S$
2. $\theta(-r) = -\theta(r)$
3. $\theta(kr) = k\theta(r)\ \forall k \in \mathbb{Z}$
4. $\theta(r^n) = (\theta(r))^n\ \forall n \in \mathbb{Z}^+$
5. If $a \in R^*$ (set of elements in $R$ with multiplicative inverse), then $\theta(u^k) = \theta(u)^k\ \forall k \in \mathbb{Z}$.

**Definition** (Ring isomorphism).
A mapping of ring $\theta : R \to S$ is a **ring isomorphism** if $\theta$ is a homomorphism and $\theta$ is bijective. In this case, we say $R$ and $S$ are isomorphic and write $R \cong S$.

**Problem 8.1.**
Let $\theta : R \to S$ be a bijection of rings with $\theta(rr') = \theta(r)\theta(r')$ for all $r, r' \in R$. Write $\theta(1_R) = 0$.

Prove that $se = es$ for all $s \in S$, hence condition (3) for ring HM can be omitted.

**Definition** (Kernel and image).
Let $\theta : R \to S$ be a ring HM. The **kernel** of $\theta$ is defined by

$$\ker(\theta) = \{r \in R : \theta(r) = 0\} \subseteq R$$

and the **image** of $\theta$ is defined by

$$\operatorname{im}(\theta) = \theta(R) = \{\theta(r) : r \in R\} \subseteq S$$

We ave seen earlier that $\ker(\theta)$ and $\operatorname{im}(\theta)$ are additive subgroups of $R$ and $S$ respectively.

**Proposition 8.9.**
Let $\theta : R \to S$ be a ring HM. Then,
1. $\operatorname{im}(\theta)$ is a subring of $S$
2. $\ker(\theta)$ is an ideal of $R$

**Proof.** (1). Since $\operatorname{im}(\theta) = \theta(R)$ is an additive subgroup of $S$, it suffices to show that $\theta(R)$ is closed under multiplication and $1_S \in \theta(R)$.

Note that $1_S = \theta(1_R) \in \theta(R)$. Also, if $s_1 = \theta(r_1)$ and $s_2 = \theta(r_2)$, then

$$s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) \in \theta(R)$$

By the subring test, $\operatorname{im}(\theta)$ is a subring of $S$.

(2). Since $\ker(\theta)$ is an additive subgroup of $S$, it suffices to show that $ra, ar \in \ker(\theta)$ for all $r \in R$ and $a \in \ker(\theta)$. If $r \in R$ and $a \in \ker(\theta)$, then

$$\theta(ra) = \theta(r)\theta(a) = \theta(r)0 = 0$$

Then $ra \in \ker(\theta)$. Similarly, we can show that $ar \in \ker(\theta)$. Thus $\ker(\theta)$ is an ideal of $R$. □

**Theorem 8.10** (1st IM).
Let $\theta : R \to S$ be a ring HM. We have $R/\ker(\theta) \cong \text{im}(\theta)$.

**Proof.** Let $A = \ker(\theta)$. Since $A$ is an ideal of $R$, $R/A$ is a ring. Define the ring map $\bar{\theta} : R/A \to \text{im}(\theta)$ by

$$\bar{\theta}(r + A) = \theta(r) \quad \forall r + A \in R/A$$

Note that

$$r + A = s + A \iff r - s \in A \iff \theta(r - s) = 0 \iff \theta(r) = \theta(s)$$

Thus $\bar{\theta}$ is well-defined and one-to-one. And, $\bar{\theta}$ is clearly onto. One can show that $\bar{\theta}$ is a HM.

It follows that $\bar{\theta}$ is a ring IM and $R/\ker(\theta) \cong \text{im}(\theta)$. □

Let $A$ and $B$ be two subsets of ring $R$. If $A$ and $B$ are both subrings, then $A \cap B$ is the "largest" subring of $R$ contained in both $A$ and $B$.

To consider the "smallest" subring of $R$ containing both $A$ and $B$, we define

$$A + B = \{a + b : a \in A, b \in B\}$$

**Proposition 8.11**.
If $R$ is a ring, then we have
1. If $A$, $B$ are both subrings of $R$ with $1_A = 1_B = 1_R$, then $A \cap B$ is a subring of $R$
2. If $A$ is a subring and $B$ is an ideal of $R$, then $A + B$ is a subring of $R$
3. If $A$, $B$ are ideals of $R$, then $A + B$ is an ideal of $R$

**Theorem 8.12** (2nd IM).
Let $A$ be a subring and $B$ an ideal of ring $R$. Then,

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

**Theorem 8.13** (3rd IM).
Let $A$, $B$ be ideals of ring $R$ with $A \subseteq B$. Then $B/A$ is an ideal in $R/A$ and

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

**Example**.
Combining the 3rd IM theorem and the fact that all ideals of $\mathbb{Z}$ are principle, all ideals of $\mathbb{Z}_n$ are principle.

**Corollary 8.14** (Correspondence theorem / 4th IM).
Let $R$ be a ring and $A$ an ideal. There exists a bijection between the set of ideals $B$ of $R$ that contains $A$ and the set of ideals of $R/A$.

**Theorem 8.15** (Chinese remainder theorem).
Let $A$, $B$ be ideals of $R$.
1. If $A+B=R$, then $R/(A\cap B)\cong R/A\times R/B$
2. If $A+B=R$ and $A\cap B=\{0\}$, then $R\cong R/A\times R/B$

**Proof.** Note that (2) is a direct consequence of (1), so we will prove just (1).

Define $\theta : R\to R/A\times R/B$ by $\theta(r)=(r+A, r+B)$. Then $\theta$ is a ring HM with $\ker(\theta)=A\cap B$.

Since $A+B=R$, there exists $a\in A$ and $b\in B$ such that $a+b=1$. Let $r=sb+ta$. Then,

$$s-r=s-sb-ta=s(1-b)-ta=sa-ta=(s-t)a\in A$$

Thus $s+A=r+A$. Similarly, we can have $t+B=r+B$. Thus $\theta(r)=(r+A,r+B)=(s+A,t+B)$. Therefore, $\mathrm{im}(\theta)=R/A\times R/B$. By 1st IM, we have

$$R/(A\cap B)\cong R/A\times R/B$$

□

Let $m,n\in\mathbb{N}$ with $\gcd(m,n)=1$. By Euclid's lemma, we have $1=mr+ns$ for some $r,s\in\mathbb{Z}$. Thus $1\in m\mathbb{Z}+n\mathbb{Z}$ and hence $m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$. And since $\gcd(m,n)=1$, we have $m\mathbb{Z}\cap n\mathbb{Z}=mn\mathbb{Z}$. By CRT (Theorem 8.15),

**Corollary 8.16**.
Let $m,n\in\mathbb{N}$ with $\gcd(m,n)=1$. Then,
1. $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$
2. If $m,n\geq 2$, then $\varphi(mn)=\varphi(m)\varphi(n)$, where $\varphi(m)=|\mathbb{Z}_m|$ is the Euler $\varphi$-function

**Proof.** (2). From (1), we have

$$(\mathbb{Z}_{mn})^*\cong(\mathbb{Z}_m\times\mathbb{Z}_n)^*\cong\mathbb{Z}_m^*\times\mathbb{Z}_n^*$$

Since $|\mathbb{Z}_m^*|=\varphi(m)$, we have $\varphi(mn)=\varphi(m)\varphi(n)$. □

Remark.
Let $m,n\in\mathbb{Z}$ with $\gcd(m,n)=1$. For $a,b\in\mathbb{Z}$, by Corollary 8.16 and the proof of Theorem 8.15, for $[a]\in\mathbb{Z}_m$ and $[b]\in\mathbb{Z}_n$, there exists a unique $[c]\in\mathbb{Z}_{mn}$ such that $[c]=[a]$ in $\mathbb{Z}_m$ and $[c]=[b]$ in $\mathbb{Z}_n$.

In other words, the simultaneous congruences $x\equiv a\pmod m$ and $x\equiv b\pmod n$ has a unique solution $x\equiv c\pmod{mn}$. This is the standard CRT.

**Proposition 8.17.**
If $R$ is a ring with $|R| = p$ where $p$ is prime, then

$$R \cong \mathbb{Z}_p$$

**Proof.** Define $\theta : \mathbb{Z}_p \to R$ by $\theta(k) = k1_R$. Note that since $R$ is an additive group and $|R| = p$, by Lagrange's theorem, $o(1_R) \in \{1, p\}$. Since $1_R \neq 0$, we have $o(1_R) = p$. Thus,

$$[k] = [m] \iff p \mid (k - m) \iff (k - m)1_R = 0 \iff k1_R = m1_R \text{ in } R$$

So $\theta$ is well-defined and one-to-one. Since $|\mathbb{Z}_p| = p = |R|$ and $\theta$ is one-to-one, $\theta$ is onto. Finally, we can prove that $\theta$ is a ring HM (exercise). It follows that $\theta$ is a ring IM and $R \cong \mathbb{Z}_p$. $\square$

**Problem 8.2.**
What are the possible rings $R$ with $|R| = p^2$?

# §9. Commutative rings

## §9.1. Integral domains and fields

**Definition (Unit).**
Let $R$ be a ring. We say $a \in R$ is a unit if $u$ has a multiplicative inverse in $R$, denoted by $u^{-1}$.

We have that $uu^{-1} = u^{-1}u = 1$. Note that if $u$ is a unit in $R$ and $r, s \in R$, we have

$$ur = us \implies r = s, \quad ru = su \implies r = s$$

Let $R^*$ denote the set of all units in $R$. One an show $(R^*, \cdot)$ is a group, called the **group of units** of $R$.

**Example.**
Note that 2 is a unit in $\mathbb{Q}$, but not a unit in $\mathbb{Z}$ We have $\mathbb{Q}^* = \mathbb{Q} \setminus \{n\}$ and $\mathbb{Q}^* = \{\pm 1\}$.

**Problem 9.1.**
Consider the ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = 1\} \subseteq \mathbb{C}$$

Show that $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Hint: define norm $N(a + bi) = a^2 + b^2$ and prove that $N(xy) = N(x)N(y)$ and $N(x) = 1$ iff $x$ is a unit.

**Definition (Division ring).**
A ring $R \neq \{0\}$ is a **division ring** if $R^* = R \setminus \{0\}$. That is, every non-zero element of $R$ is a unit in $R$.

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

**Example.**
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.

**Example.**
Recall that $[a][x] = [1]$ has a solution in $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$. Thus if $n = p$ is a prime, then $\gcd(a, p) = 1 \ \forall a \geq 1$, so $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ and hence $\mathbb{Z}_p$ is a field.

However, if $n$ is not a prime, say $n = ab$ with $1 < a, b < n$, then the non-zero congruence claims $[a]$, $[b]$ are not units in $\mathbb{Z}_n$ as there is no solution for $[a][x] = 1$ and hence $\mathbb{Z}_n^* \neq \mathbb{Z}_n \setminus \{0\}$. Thus $\mathbb{Z}_n$ is a field iff $n$ is a prime.

**Remark.**
If $R$ is a division ring or a field, then its only ideals are $\{0\}$ and $R$ since if $A \neq \{0\}$ is an ideal of $R$, then $0 \neq a \in A$ implies that $1 = aa^{-1} \in A$. By Proposition 8.5, $A = R$.

As a consequence, if we have a ring HM $\theta$ from a field $F$ to a ring $S$, since $\ker(\theta)$ is an ideal, $\ker(\theta) = \{0\}$ or $\ker(\theta) = F$. Hence $\theta$ is either injective or a zero map.

**Problem 9.2.**
Prove that every finite division ring is a field (Wedderburn's little theorem).

Note that for $r, s \in \mathbb{R}$, we have if $rs = 0$ then $r = 0$ or $s = 0$. This property is useful for solving equations, say if $x^2 - x - 6 = (x-3)(x+2) = 0$, then $x = 3$ or $x - 2$. However, this property is not always true. For example, $[2][3] = [6] = [0]$ in $\mathbb{Z}_6$, but $[2] \neq [0]$ or $[3] \neq [0]$.

**Problem 9.3.**
Solve $[(x-3)(x-2)] = [0]$ in $\mathbb{Z}_6$.

**Definition** (Zero divisor).
Let $R \neq \{0\}$ be a ring. For $0 \neq a \in R$, $a$ is a **zero divisor** if there exists $0 \neq b \in R$ such that $ab = 0$.

**Example.**
In $\mathbb{Z}_6$, $[2]$, $[3]$, $[4]$ are zero divisors since $[2][3] = [0] = [4][3]$.

**Example.**
In $\mathcal{M}_2(\mathbb{R})$, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Thus $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is a zero divisor.

**Proposition 9.1.**
Given a ring $R$ and $a, b, c \in R$. The following are equivalent:
1. If $ab = a$ in $R$, then $a = 0$ or $b = 0$.
2. If $ab = ac$ in $R$ and $a \neq 0$, then $b = c$
3. If $ba = ca$ in $R$ and $a \neq 0$, then $b = c$

**Proof.** (1) $\implies$ (2). Let $ab = ac$ with $a \neq 0$. Then $a(b-c) = 0$. By (1), since $a \neq 0$, we have $b - c = 0$, so $b = c$.

(2) $\implies$ (1). Let $ab = 0$. If $a = 0$, then we are done. If $a \neq 0$, then $ab = 0 = a0$. By (2), since $a \neq 0$, we have $b = 0$.

The proof of (1) $\iff$ (3) is similar. □

**Definition** (Integral domain).
A commutative ring $R \neq \{0\}$ is an **integral domain** (ID) if it has no zero divisor. That is, if $ab = 0$ in $R$, then $a = 0$ or $b = 0$.

**Example.**
$\mathbb{Z}$ is an integral domain since for $a, b \in \mathbb{Z}$, $ab = 0$ implies $a = 0$ or $b = 0$.

**Example.**
Note that if $p$ is a prime, then $p \mid ab$ then $p \mid a$ or $p \mid b$. That is, $[a][b] = [0]$ in $\mathbb{Z}_p$ implies $[a] = [0]$ or $[b] = [0]$. Thus $\mathbb{Z}_p$ is an ID.

However, if $n = ab$ with $1 < a, b < n$, then $[a][b] = [0]$ in $\mathbb{Z}_n$ with $[a] \neq [0]$ and $[b] \neq [0]$. Thus $\mathbb{Z}_n$ is an ID iff $n$ is a prime.

**Proposition 9.2.**
Every field is an ID.

**Proof.** Let $ab = 0$ in field $R$. If $a = 0$, then we are done. If $a \neq 0$, since $R$ is a field, $a \in R^*$ thus $a^{-1} \in R$ exists. Then,

$$b = 1 \cdot b = a^{-1}ab = a^{-1}0 = 0$$

Thus $R$ is an ID. □

Remark.
Using the above proof, one can show that every subring of a field is an ID.

Remark.
The converse of Proposition 9.2 is not true. For example, $\mathbb{Z}$ is an ID but not a field.

Example.
The Gaussian ring $\mathbb{Z}[i]$ is an ID, but not a field.

Proposition 9.3.
Every finite ID is a field.

**Proof.** Let $R$ be a finite ID and $a \in R$ with $a \neq 0$. Consider the map $\theta : R \to R$ defined by $\theta(r) = ar$. Since $R$ is an ID, $ar = as$ (and $a \neq 0$) implies $= s$. Hence $\theta$ is injective.

Since $R$ is finite, $\theta$ is also surjective. Hence there exists $s \in R$ such that $1 = \theta(s) = as$. □

Proposition 9.4.
The characteristic of an ID is either $0$ or a prime $p$.

**Proof.** Let $R$ be an ID. If $\mathrm{ch}(R) = 0$, then we are done. If $\mathrm{ch}(R) \neq 0$, note that since $R \neq \{0\}$, we have $\mathrm{ch}(R) \neq 1$.

If $\mathrm{ch}(R) = n \in \mathbb{N} \setminus \{1\}$, suppose $n$ is not prime, say $n = ab$ where $1 < ab < n$. If $1$ is the unity of $R$, then by Proposition 8.1, we have

$$(a \cdot 1)(b \cdot 1) = (ab) \cdot 1 = n \cdot 1 = 0$$

Since $R$ is an ID, we have $a \cdot 1 = 0$ or $b \cdot 1 = 0$, which contradicts $\mathrm{ch}(R) = o(1) = n$. Therefore, $n$ is prime. □

Remark.
Let $R$ be an ID with $\mathrm{ch}(R) = p$, a prime. For $a, b \in R$, we have

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

Since $p$ is prime, $p \mid \binom{p}{k}$ for all $1 \leq k \leq (p - 1)$. And since $\mathrm{ch}(R) = p$, we have

$$(a + b)^p = a^p + b^p$$

## §9.2. Prime ideals and maximal ideals

Let $p$ be prime and $a, b \in \mathbb{Z}$. Recall from MATH 135 that $p \mid ab$ implies $p \mid a$ or $p \mid b$. In other words, if $ab \in p\mathbb{Z}$, then $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

**Definition** (Prime ideal).
Let $R$ be a commutative ring. An ideal $P \neq R$ of $R$ is a prime ideal if whenever $r, s$ satisfy $rs \in P$, then $r \in P$ or $s \in P$.

**Example.**
$\{0\}$ is a prime ideal of $\mathbb{Z}$.

**Example.**
For $n \in \mathbb{N}$ with $n \geq 2$, $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ iff $n$ is prime.

**Proposition 9.5.**
If $R$ is a commutative ring, then an ideal $P$ of $R$ is a prime ideal iff $R/P$ is an ID.

**Proof.** Since $R$ is commutative, so is $R/P$. Note that

$$R/P \neq \{0\} \iff 0 + P \neq 1 + P \iff 1 \notin P \iff P \neq R$$

Also, for $r, s \in R$, we have $P$ is a prime ideal iff $r, s \in P$ implies $r \in P$ or $s \in P$. Equivalently, $(r + P)(s + P) = 0 + P$ implies $r + P = 0 + P$ or $s + P = 0 + P$. So by definition, $R/P$ is an ID. $\square$

**Definition** (Maximal ideal).
If $R$ is commutative, an ideal $M$ of $R$ is a **maximal ideal** iff $R/M$ is a field.

**Proof.** Let $M$ be a maximal ideal of $R$ and $r \notin M$. Then, $M \subseteq \langle r \rangle + M \subseteq R$. Since $M \neq \langle r \rangle + M$, we have $\langle r \rangle + M = R$. $\square$

**Proposition 9.6.**
If $R$ is a commutative ring, then an ideal $M$ of $R$ is a maximal ideal iff $R/M$ is a field.

**Proof.** Since $R$ is commutative, so is $R/M$. Note that

$$R/M \neq \{0\} \iff 0 + M \neq 1 + M \iff 1 \notin M \iff M \neq R$$

Also for $r \in R$, note that $r \neq M \iff r + M \neq 0 + M$. Thus, we have

$$\begin{aligned}
M \text{ is maximal} &\iff \langle r \rangle + M = R \ \forall r \notin M \\
&\iff 1 \in \langle r \rangle + M \ \forall r \notin M \\
&\iff \forall r \notin M, \exists s \in R, 1 + M = rs + M \\
&\iff \forall r + M \neq 0 + M, \exists s + M \in R/M, (r + M)(s + M) = 1 + M \\
&\iff R/M \text{ is a field}
\end{aligned}$$

$\square$

Combining Proposition 9.2, Proposition 9.5, and Proposition 9.6, we have

**Corollary 9.7.**
Every maximal ideal of a commutative ring is a prime ideal.

Remark.
The converse of Corollary 9.7 is not true. For example, $\{0\}$ is a prime ideal in $\mathbb{Z}$, but not a maximal ideal.

Example.
Consider the ideal $\langle x^2+1\rangle$ in the ring $\mathbb{Z}[x]$. Let $\theta : \mathbb{Z}[x] \to \mathbb{Z}[i]$ be defined by $\theta(f(x)) = f(i)$. Then $\theta$ is surjective as $\theta(a+bx) = a+bi$. Also, one can check that $\ker(\theta) = \langle x^2+1\rangle$.

By 1st IM (Theorem 8.10), we have $\mathbb{Z}[x]/\langle x^2+1\rangle \cong \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is an ID but not a field, the ideal $\langle x^2+1\rangle$ is prime but not maximal.

## §9.3. Fields of fractions

Let $R$ be an ID and let $D = R \setminus \{0\}$. Consider the set

$$X = R \times D = \{(r,s) : r \in R, s \in D\}$$

We say $(r,s) \equiv (r',s')$ iff $rs' = r's$. One can show $\equiv$ is an equivalence relation. In particular,
1. $(r,s) \equiv (r,s)$
2. If $(r,s) \equiv (r',s')$, then $(r',s') \equiv (r,s)$
3. If $(r,s) \equiv (r',s')$ and $(r',s') \equiv (r'',s'')$, then $(r,s) \equiv (r'',s'')$

Motivated by the case $R = \mathbb{Z}$, we can now define the fraction $\frac{r}{s}$ to be the equivalence class $[(r,s)]$ of the pairs $(r,s)$ on $X$. Let $F$ denote the set of all such fractions:

$$F = \left\{\frac{r}{s} : r \in R, s \in D\right\} = \left\{\frac{r}{s} : r, s \in R, s \neq 0\right\}$$

The addition and multiplication in $F$ are defined by

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$$
$$\left(\frac{r}{s}\right)\left(\frac{r'}{s'}\right) = \frac{rr'}{ss'}$$

Since $R$ is an ID, these operations are well-defined. Then one can show that with the above defined addition and multiplication, $F$ becomes a field with the zero being $\frac{0}{1}$, the unity $\frac{1}{1}$, and the negative of $\frac{r}{s}$ being $-\frac{r}{s}$. Moreover, if $\frac{r}{s} \neq 0$, then $r \neq 0$ and its multiplicative inverse is $\frac{s}{r}$.

In addition, we have $R \cong R'$ where $R' = \{\frac{r}{1} : r \in R\} \subseteq F$. Thus we have

**Theorem 9.8.**
Let $R$ be an ID. Then there exists a field $F$ consisting of fractions $\frac{r}{s}$ with $r, s \in R$ and $s \neq 0$. By identifying $r = \frac{r}{1}$ for all $r \in R$, we can view $R$ as a subring of $F$.

The field $F$ is called the **field of fractions** of $R$.

# §10. Polynomial rings

## §10.1. Polynomials

**Definition** (Polynomial).
Let $R$ be a ring and $x$ be a variable. Let

$$R[x] = \{f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m : m \in \mathbb{Z}^+, a_i \in R \ \forall 0 \leq i \leq m\}$$

Such $f(x)$ is called a **polynomial** in $x$ over $R$.

If $a_m \neq 0$, we say $f(x)$ has degree $m$, denoted by $\deg(f) = m$, and we say $a_m$ is the leading coefficient of $f(x)$.

If the leading coefficient $a_m = 1$, we say $f(x)$ is **monic**.

If $\deg(f) = 0$, then $f(x) = a_0 \in \mathbb{R} \setminus \{0\}$. In this case, we say $f(x)$ is a **constant polynomial**.

Note that

$$f(x) = 0 \Longleftrightarrow a_0 = a_1 = \cdots = a_m = 0$$

0 is also a constant polynomial and we define $\deg(0) = -\infty$.

Let $f(x) = \sum_{i=0}^{m} a_i x^i, g(x) = \sum_{i=0}^{n} b_i x^i \in R[x]$ with $m \leq n$. Then we write $a_i = 0 \ \forall (m+i) \leq i < n$.

We can define addition and multiplication on $R[x]$ as follows:

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

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k, \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

**Proposition 10.1**.
Let $R$ be a ring and $x$ be a variable.
1. $R[x]$ is a ring
2. $R$ is a subring of $R[x]$
3. If $Z = Z(R)$ denotes the center of $R$, then $Z(R[x]) = Z[x]$

**Proof.** (3). Let $f(x) = \sum_{i=0}^{m} a_m x^m \in Z[x]$ and $g(x) = \sum_{j=0}^{n} b_n x^n \in R[x]$. We have

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k$$

with $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

Since $a_i \in Z$, we have $a_i b_j = b_j a_i$ for all $i, j$. Thus we get $f(x)g(x) = g(x)f(x)$ for all $g(x) \in R[x]$, and hence $Z[x] \subseteq Z(R[x])$.

To show the other inclusion, if $h(x) = \sum_{i=0}^{s} c_i x^i \in Z(R[x])$, then for all $r \in R$, we have $h(x)r = rh(x)$. Thus $c_i r = rc_i$ for all $r \in R$ and $0 \le i \le s$. Hence $c_i \in Z$ and $Z(R[x]) \subseteq Z[x]$. It follows that $Z(R[x]) = Z[x]$. □

**Proposition 10.2.**
Let $R$ be an ID. Then,
1. $R[x]$ is an ID
2. If $f \neq 0$ and $g \neq 0$ in $R[x]$, then $\deg(fg) = \deg(f) + \deg(g)$ (product formula)
3. The units in $R[x]$ are $R^*$, the units of $R$

**Proof.** Suppose $f(x) = \sum_{i=0}^{m} a_i x^i \neq 0$ and $g(x) = \sum_{i=0}^{n} b_i x^i \neq 0$ are polynomials in $R[x]$ with $a_m \neq 0$, $b_n \neq 0$. Then,

$$f(x)g(x) = (a_m b_n)x^{m+n} + \cdots + a_0 b_0$$

Since $R$ is an ID, $a_m b_n \neq 0$ and thus $f(x)g(x) \neq 0$. It follows that $R[x]$ is an ID, and $\deg(fg) = \deg(f) + \deg(g)$.

Let $u(x) \in R[x]$ be a unit with inverse $v(x) \in R[x]$. Since $u(x)v(x) = 1$, by (1) we have $u(x) \neq 0, v(x) \neq 0$ and by (2), we have $\deg(u) + \deg(v) = \deg(1) = 0$, meaning $\deg(u) = \deg(v) = 0$. Thus $u(x), v(x)$ are units in $R$ and hence $R[x]^* \subseteq R^*$. Since trivially $R^* \subseteq R[x]^*$, we have $R[x]^* = R^*$. □

**Remark.**
Note that in $\mathbb{Z}_4[x]$, we have $2x \cdot 2x = 4x^2 = 0$. Thus $\deg(2x) + \deg(2x) \neq \deg(4x^2)$, hence the product formula in Proposition 10.2 only applies when $R$ is an ID.

**Remark.**
To extend the product formula to 0, we define $\deg(0) = \pm\infty$.

## §10.2. Polynomials over a field

**Definition** (Divides).
Let $F$ be a field and $f(x), g(x) \in F[x]$. We say $f(x)$ divides $g(x)$, denoted by $f(x) \mid g(x)$, if there exists $q(x) \in F[x]$ such that $g(x) = f(x)q(x)$.

**Proposition 10.3.**
Let $F$ be a field and $f(x), g(x), h(x) \in F[x]$.
1. If $f(x) \mid g(x)$ and $g(x) \mid h(x)$, then $f(x) \mid h(x)$ (transitivity of divisibility)
2. If $f(x) \mid g(x)$ and $f(x) \mid h(x)$, then $f(x) \mid (g(x)u(x) + h(x)v(x))$ for any $u(x), v(x) \in F[x]$ (division of integer combinations)

Recall for $a, b \in \mathbb{Z}$, if $a \mid b, b \mid a$ and $a, b$ are positive, then $a = b$. The following is its analogue in $F[x]$.

**Proposition 10.4.**
Let $F$ be a field and $f(x), g(x) \in F[x]$ be monic. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = g(x)$.

**Proof.** Since $f(x) \mid g(x)$ and $g(x) \mid f(x)$, we have $g(x) = r(x)f(x)$ and $f(x) = s(x)g(x)$ for some $r(x), s(x) \in F[x]$. Then, $f(x) = s(x)r(x)f(x)$. By Proposition 10.2, we have $\deg(f) = \deg(s) + \deg(r) + \deg(f)$, so $\deg(s) = \deg(r) = 0$. Thus, $f(x) = sg(x)$ for some $s \in F$.

Since both $f(x)$ and $g(x)$ are monic, we have $s = 1$ and hence $f(x) = g(x)$. □

**Proposition 10.5** (Division algorithm)**.**
Let $F$ be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq 0$. Then there exists unique $q(x), r(x) \in F[x]$ such that

$$g(x) = f(x)q(x) + r(x), \quad \deg(r) < \deg(f)$$

Note that this includes the case for $r = 0$, which explains why we define $\deg(0) = -\infty$.

**Proof.** Let $m = \deg(f)$ and $n = \deg(g)$. If $n < m$, then $g(x) = 0 \cdot f(x) + g(x)$.

Otherwise suppose $n \geq m$. Write $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$ with $a_m \neq 0$.

Since $F$ is a field, $a_m^{-1}$ exists. Consider

$$\begin{aligned} g_1(x) &= g(x) - b_n a_m^{-1} x^{n-m} f(x) \\ &= 0 \cdot x_n + (b_{n-1} - b_n a_m^{-1} a_{m-1}) x^{n-1} + \cdots \end{aligned}$$

Since $\deg(g_1) < n$, by the other case, there exists $q_1(x), r_1(x) \in F[x]$ such that

$$g_1(x) = q_1(x)f(x) + r_1(x), \quad \deg(r_1) < \deg(f)$$

It follows that

$$\begin{aligned} g(x) &= g_1(x) + b_n a_m^{-1} x^{n-m} f(x) \\ &= (q_1(x) + b_n a_m^{-1} x^{n-m}) f(x) + r_1(x) \end{aligned}$$

By taking $q(x) = q_1(x) + b_n a_m^{-1} x^{n-m}$ and $r(x) = r_1(x)$, we have that $g(x) = q(x)f(x) + r(x)$ with $\deg(r) < \deg(f)$.

For uniqueness, suppose there exist $q'(x), r'(x) \in F[x]$ such that $g(x) = q_1 f(x) + r_1(x)$ with $\deg(r_1) < \deg(f)$. Then, $r(x) - r_1(x) = (q_1(x) - q(x))f(x)$. If $q_1(x) \neq q(x)$, we get

$$\deg(r - r_1) = \deg(q_1 - q) + \deg(f) \geq \deg(f)$$

which contradicts $\deg(r - r_1) < \deg(f)$. Thus $q_1(x) = q(x)$ and hence $r_1(x) = r(x)$. □

For $a, b \in \mathbb{Z} \setminus \{0\}$, Bezout's lemma states that $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.

**Proposition 10.6.**
Let $F$ be a field and $f(x), g(x) \in F[x] \setminus \{0\}$. Then there exists $d(x) \in F[x]$ which satisfies
- $d(x)$ is monic
- $d(x) \mid f(x)$ and $d(x) \mid g(x)$
- If $e(x) \mid f(x)$ and $e(x) \mid g(x)$, then $e(x) \mid d(x)$
- $d(x) = u(x)f(x) + v(x)g(x)$ such that $u(x), v(x) \in F[x]$

Note that if both $d(x)$ and $d_1(x)$ satisfy the above conditions, since $d(x) \mid d_1(x)$ and $d_1(x) \mid d(x)$ and both of them are monic, by Proposition 10.4, we have $d(x) = d_1(x)$. We call such unique $d(x)$ the GCD of $f(x)$ and $g(x)$, denoted by $d(x) = \gcd(f(x), g(x))$.

**Proof.** Let $X = \{u(x)f(x) + v(x)g(x) : u(x), v(x) \in F[x]\}$. Since $f(x) \in X$, the set $X$ contains non-zero polynomials and thus monic polynomials. Among all monic polynomials in $X$, let $d(x) = u(x)f(x) + v(x)g(x)$ of minimum degree. Then, (1) and (4) are satisfied.

For (3), if $e(x) \mid f(x)$ and $e(x) \mid g(x)$, since $d(x) = u(x)f(x) + v(x)g(x)$, by Proposition 10.3, we have $e(x) \mid d(x)$.

For (2), by division algorithm (Proposition 10.5), write $f(x) = q(x)d(x) + r(x)$ with $\deg(r) < \deg(d)$. Then,

$$\begin{aligned} r(x) &= f(x) - q(x)d(x) \\ &= f(x) - q(x)(u(x)f(x) + v(x)g(x)) \\ &= (1 - q(x)u(x))f(x) - q(x)v(x)g(x) \end{aligned}$$

Note that if $r(x) \neq 0$, let $c \neq 0$ be the leading coefficient of $r(x)$. Since $F$ is a field, $c^{-1}$ exists. The above expression shows that $c^{-1}r(x)$ is a monic polynomial with $X$ with $\deg(c^{-1}r) = \deg(r) < \deg(d)$, which contradicts the minimum degree property of $d(x)$. Thus $r(x) = 0$ and we have $d(x) \mid f(x)$. Similarly, we can show that $d(x) \mid g(x)$. Thus, (2) follows. □

Recall that $p \in \mathbb{Z}$ is a prime if $p \geq 2$ and whenever $p = ab$, then $a = \pm 1$ or $b = \pm 1$, where $\pm 1$ are units in $\mathbb{Z}$.

**Definition** (Irreducible).
$l(x) \neq 0$ is **irreducible** if $\deg(l) \geq 1$ and whenever $l(x) = l_1(x)l_2(x)$, then $\deg(l_1) = 0$ or $\deg(l_2) = 0$.

**Example.**
If $l(x) \in F[x]$ satisfies $\deg(l) = 1$, then $l(x)$ is irreducible.

Given prime $p \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$, Euclid's Lemma shows that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

**Proposition 10.7.**
Let $F$ be a field and $f(x), g(x) \in F[x]$. If $l(x) \in F[x]$ is irreducible and $l(x) \mid f(x)g(x)$, then $l(x) \mid f(x)$ or $l(x) \mid g(x)$.

**Proof.** Suppose $l(x) \mid f(x)g(x)$. If $l(x) \mid f(x)$, then we are done.

If $l(x) \nmid f(x)$, then $d(x) = \gcd(l(x), f(x)) = 1$. By Proposition 10.6, we have $1 = l(x)u(x) + f(x)v(x)$ for some $u(x), v(x) \in F[x]$. Then,

$$g(x) = g(x)l(x)u(x) + g(x)f(x)v(x)$$

Since $l(x) \mid l(x)$ and $l(x) \mid g(x)f(x)$, by Proposition 10.3, we have $l(x) \mid g(x)$. $\square$

> Remark.
> Let $f_1(x), \cdots, f_n(x) \in F[x]$ and let $l(x) \in F[x]$ be irreducible. If $l(x) \mid f_1(x) \cdots f_n(x)$, by applying Proposition 10.7 repeatedly, we have $l(x) \mid f_i(x)$ for some $1 \le i \le n$.

For an integer $n \in \mathbb{Z}$ with $|n| \ge 2$, up to $\pm\operatorname{sgn}(n)$, $n$ can be written uniquely as a product of primes.

By induction and Proposition 10.7, we have the following analogous result in $F[x]$.

**Theorem 10.8** (Unique factorization theorem).
Let $F$ be a field and $f(x) \in F[x]$ with $\deg(f) \ge 1$. Then we can write

$$f(x) = cl_1(x)l_2(x) \cdots l_m(x)$$

where $c \in F^*$ and $l_i(x)$ are monic irreducible polynomials (not necessarily distinct).

The factorization is unique up to the order of $l_i$.

**Problem 10.1**.
Use Theorem 10.8 to prove that there are infinitely many irreducible polynomials in $F[x]$.

Recall in $\mathbb{Z}$, all ideals are of the form $\langle n \rangle = n\mathbb{Z}$ and if $n \in \mathbb{N}$, then $n$ is uniquely determined.

**Proof.** Let $A$ be an ideal of $F[x]$. If $A = \{0\}$, then $A = \langle 0 \rangle$. If $A \ne \{0\}$, since $F$ is a field, if $f \in A$ with leading coefficient $a$, then $a^{-1}f \in A$. Thus $A$ contains a monic polynomial.

Among all monic polynomials in $A$, choose $h(x) \in A$ of minimum degree. Then $\langle h(x) \rangle \subseteq A$.

To prove the other inclusion, let $f(x) \in A$. By division algorithm, we have $f(x) = q(x)h(x) + r(x)$ with $q(x), r(x) \in F[x]$ and $\deg(r) < \deg(h)$. If $r(x) \ne 0$, let $u \ne 0$ be its leading coefficient. Since $A$ is an ideal and $f(x), h(x) \in A$, we have

$$u^{-1}r(x) = u^{-1}(f(x) - q(x)h(x)) = u^{-1}f(x) - u^{-1}q(x)h(x) \in A$$

which is a monic polynomial in $A$ with $\deg(u^{-1}r(x)) < \deg(h)$. This contradicts the minimum degree property of $h$. Thus $r(x) = 0$ and $f(x) = q(x)h(x)$. It follows that $f(x) \in \langle h(x) \rangle$ and hence $A = \langle h(x) \rangle$.

To prove uniqueness, suppose $A = \langle h(x) \rangle = \langle h_1(x) \rangle$. Since $h(x) \mid h_1(x)$ and $h_1(x) \mid h(x)$, by Proposition 10.4, we have $h(x) = h_1(x)$. $\square$

**Proposition 10.9**.
Let $F$ be a field. Then all ideals of $F[x]$ are of the form $\langle h(x) \rangle = h(x)F[x]$ for some $h(x) \in F[x]$. If $\langle h(x) \rangle \ne 0$ and $h(x)$ is monic, then the generator is uniquely determined.

We have seen in $\mathbb{Z}$ that all ideals are of the form $\langle n \rangle$ for some $n \in \mathbb{Z}$. For $n \geq 2$, if we divide an integer by $n$, the remainder is $0 \leq r \leq n-1$. Then we have

$$\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle = \{r + \langle n \rangle : 0 \leq r \leq n-1\} = \{[i] : 0 \leq i \leq n-1\}$$

We now consider its analogue in $F[x]$.

Let $F$ be a field. By Proposition 10.9, all ideals of $F[x]$ are of the form $\langle h(x) \rangle$. Suppose that $h(x)$ is monic and $\deg(h) = m \geq 1$.

Consider the quotient ring $R = F[x]/\langle h(x) \rangle$.

$$R = \left\{ \overline{f(x)} := f(x) + \langle h(x) \rangle : f(x) \in F[x] \right\}$$

Write $t = \overline{x} = x + \langle h(x) \rangle$. We have $h(t) = 0$ in $R$. By the division algorithm, we can write $f(x) = q(x)h(x) + r(x)$ with $\deg(r) < \deg(h) = m$. Thus we can show that

$$R = \left\{ \sum_{i=0}^{m-1} \overline{a_i} t^i : a_i \in F, h(t) = 0 \right\}$$

Consider the map $\theta : F \to R$ given by $\theta(a) = \overline{a}$. Since $\theta$ is not the zero map and $\ker(\theta)$ is an ideal of $F$, we have $\ker(\theta) = \{0\}$. Thus $\theta$ is a one-to-one ring HM. Since $F \cong \theta(F)$, by identifying $F$ with $\theta(F)$, we have

$$R = \left\{ \sum_{i=0}^{m-1} a_i t^i : a_i \in F, h(t) = 0 \right\}$$

Note that in $R$, we have

$$\sum_{i=0}^{m-1} a_i t^i = \sum_{i=0}^{m-1} b_i t^i \iff a_i = b_i \ \forall 0 \leq i \leq m-1$$

Hence this representation of elements in $R$ is unique.

**Proposition 10.10.**
Let $F$ be a field and $h(x) \in F[x]$ be monic with $\deg(h) = m \geq 1$. Then the quotient ring $F[x]/\langle h(x) \rangle$ is given by

$$R = \left\{ \sum_{i=0}^{m-1} a_i t^i : a_i \in F, h(t) = 0 \right\}$$

in which an element of $R$ can be uniquely represented in the above form.

**Example.**
Consider the ring $\mathbb{R}[x]$. Let $h(x) = x^2 + 1 \in \mathbb{R}[x]$. By Proposition 10.10, we have

$$\mathbb{R}[x]/\langle x^2 + 1 \rangle = \{a + bt : a, b \in \mathbb{R}, t^2 + 1 = 0\} \cong \{a + bi : a, b \in \mathbb{R}, i^2 = -1\} = \mathbb{C}$$

**Proposition 10.11.**
Let $F$ be a field and $h(x) \in F[x]$ with $\deg(h) \geq 1$. The following are equivalent:
1. $F[x]/\langle h(x)\rangle$ is a field
2. $F[x]/\langle h(x)\rangle$ is an ID
3. $h(x)$ is irreducible in $F[x]$

**Proof.** Let $A = \langle h(x)\rangle$.

(1) $\implies$ (2). A field is an ID.

(2) $\implies$ (3). If $h(x) = f(x)g(x)$ with $f(x), g(x) \in F[x]$, then

$$(f(x) + A)(g(x) + A) = h(x) + A = 0 + A \in F[x]/A$$

By (2), either $f(x) + A = 0 + A$ or $g(x) + A = 0 + A$. If $f(x) \in A$, then $f(x) = q(x)h(x)$ for some $q(x) \in F[x]$. Thus $h(x) = f(x)g(x) = q(x)h(x)g(x)$. Since $F[x]$ is an ID, this implies that $q(x)g(x) = 1$, so $\deg(g) = 0$. Similarly, if $g(x) \in A$, then $\deg(f) = 0$. Thus $h(x)$ is irreducible in $F[x]$.

(3) $\implies$ (1). Note that $F[x]/A$ is a commutative ring. Thus to show that $F[x]/A$ is a field, it suffices to show that every non-zero element of $F[x]/A$ has an inverse.

Let $f(x) + A \neq 0 + A$ with $f(x) \in F[x]$. Then $f(x) \neq A$ and hence $h(x) \nmid f(x)$. Since $h(x)$ is irreducible and $h(x) \nmid f(x)$, we have $\gcd(f(x), h(x)) = 1$.

By Proposition 10.6, there exist $u(x), v(x) \in F[x]$ such that

$$1 = u(x)h(x) + v(x)f(x) \implies (v(x) + A)(f(x) + A) = 1 + A$$

It follows that $f(x) + A$ has an inverse $v(x) + A$ in $F[x]/A$, and hence $F[x]/A$ is a field. □

**Example.**
Since $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$, which is a field, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$.

**Example.**
Since $x^2 + x + 1$ has no root in $\mathbb{Z}_2$, it is irreducible in $\mathbb{Z}_2$. Thus

$$\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle = \{a + bt : a, b \in \mathbb{Z}_2, t^2 + t + 1 = 0\}$$

is a field with 4 elements.

**Remark.**
Before the previous example, the only finite fields we know are of the form $\mathbb{Z}_p$ where $p$ is prime. We have seen before that there are infinitely many irreducible polynomials in $\mathbb{Z}_p[x]$.

One can show that for any $n \in \mathbb{N}$, there exists at least one irreducible polynomial $f_n(x)$ of degree $n$ in $\mathbb{Z}_p[x]$. Since $f_n(x)$ is irreducible, $\mathbb{Z}_p[x]/\langle f_n(x)\rangle$ is a field of order $p^n$.

Note that $\mathbb{Z}_{p^n}$ is not a field if $n \geq 2$.

| | $\mathbb{Z}$ | $F[x]$ |
|---|---|---|
| Elements | $m$ | $f(x)$ |
| Size | $\|m\|$ | $\deg(f)$ |
| Units | $\pm 1$ | $F^*$ |
| Unique factorization | $m = \pm p_1 p_2 \cdots p_k$ | $f(x) = c l_1(x) l_2(x) \cdots l_k(x)$ |
| Ideals | $\langle n \rangle$ | $\langle h(x) \rangle$ |
| Prime ideal generators | Primes | Irreducible polynomials |

Table 1: Analogies between $\mathbb{Z}$ and $F[x]$