A FIRST COURSE

IN

ABSTRACT ALGEBRA

A FIRST COURSE

IN

ABSTRACT ALGEBRA

MAT3004 Notebook

Dr. Guang Rao

The Chinese University of Hongkong, Shenzhen

香 港 中 文 大 學（深 圳）

The Chinese University of Hong Kong, Shenzhen

Contents

Acknowledgments

This book is from the MAT3004 in fall semester, 2018.

CUHK(SZ)

Notations and Conventions

$\mathbb{R}^n$	n-dimensional real space
$\mathbb{C}^n$	n-dimensional complex space
$\mathbb{R}^{m\times n}$	set of all $m \times n$ real-valued matrices
$\mathbb{C}^{m\times n}$	set of all $m \times n$ complex-valued matrices
x_i	ith entry of column vector $\boldsymbol{x}$
a_{ij}	(i,j)th entry of matrix $\boldsymbol{A}$
$\boldsymbol{a}_i$	ith column of matrix $\boldsymbol{A}$
$\boldsymbol{a}_i^{\mathrm{T}}$	ith row of matrix $\boldsymbol{A}$
$\mathbb{S}^n$	set of all $n \times n$ real symmetric matrices, i.e., $\boldsymbol{A} \in \mathbb{R}^{n\times n}$ and $a_{ij} = a_{ji}$ for all i, j
$\mathbb{H}^n$	set of all $n \times n$ complex Hermitian matrices, i.e., $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ and $\bar{a}_{ij} = a_{ji}$ for all i, j
$\boldsymbol{A}^{\mathrm{T}}$	transpose of $\boldsymbol{A}$, i.e, $\boldsymbol{B} = \boldsymbol{A}^{\mathrm{T}}$ means $b_{ji} = a_{ij}$ for all i, j
$\boldsymbol{A}^{\mathrm{H}}$	Hermitian transpose of $\boldsymbol{A}$, i.e, $\boldsymbol{B} = \boldsymbol{A}^{\mathrm{H}}$ means $b_{ji} = \bar{a}_{ij}$ for all i, j
$\mathrm{trace}(\boldsymbol{A})$	sum of diagonal entries of square matrix $\boldsymbol{A}$
$\mathbf{1}$	A vector with all 1 entries
$\mathbf{0}$	either a vector of all zeros, or a matrix of all zeros
$\boldsymbol{e}_i$	a unit vector with the nonzero element at the ith entry
$\mathcal{C}(\boldsymbol{A})$	the column space of $\boldsymbol{A}$
$\mathcal{R}(\boldsymbol{A})$	the row space of $\boldsymbol{A}$
$\mathcal{N}(\boldsymbol{A})$	the null space of $\boldsymbol{A}$
$\mathrm{Proj}_{\mathcal{M}}(\boldsymbol{A})$	the projection of $\boldsymbol{A}$ onto the set $\mathcal{M}$

Chapter 1

Week1

1.1. Monday

1.1.1. Introduction to Abstract Algebra

The basic concepts include **groups, rings, fields**.

One topic is algebra, i.e., the solvability of polynomials. (From Galois Theory to analysis)

$$\text{Example: } \frac{\mathrm{d}\boldsymbol{y}}{\mathrm{d}\boldsymbol{x}} = g(\boldsymbol{x}) \implies D\boldsymbol{y} = g(\boldsymbol{x})$$

with operatior $D := \frac{\mathrm{d}}{\mathrm{d}\boldsymbol{x}}$. The operator D forms a ring, i.e.,

$$\{a_n(x)D^n + a_{n-1}(x)D^{n-1} + \cdots + a_0(x)\} \mapsto \text{ring}$$

Second topic is number theory

Third topic is geometry, including *algebraic geometry, differential geometry, topology, finite geometry, affine geometry, algebraic graph theory,, combinatorics*, with applications to coding theory, physics, crystallography chemestry.

1.1.2. Group

Definition 1.1 [Group] A group $\mathcal{G}$ is a set equipped with a binary operation, i.e.,

$$* : \quad \mathcal{G} \times \mathcal{G} \mapsto \mathcal{G}$$

such that:

1. Associativity: $(a * b) * c = a * (b * c)$ for $\forall a, b, c \in \mathcal{G}$.
2. Existence of Identity: $\exists$ an identity $e \in \mathcal{G}$ s.t. $e * g = g * e = g$ for $\forall g \in \mathcal{G}$.
3. Existence of Inverse: $\forall g \in \mathcal{G}$, there exists an inverse g^{-1} s.t. $g^{-1} * g = g * g^{-1} = e$.

The size(order) of $\mathcal{G}$ is denoted by $|\mathcal{G}|$. ∎

R

- If $a * b = b * a$ for $\forall a, b$, then $\mathcal{G}$ is called an **abelian group**.
- If $|\mathcal{G}| = 1$, then $\mathcal{G}$ is said to be **trivial**, otherwise $\mathcal{G}$ is **nontrivial**.
- Similarly, the ternary operation means:

$$* : \quad \mathcal{G} \times \mathcal{G} \times \mathcal{G} \mapsto \mathcal{G}$$

- The semigroup definition only requires the (1) condition; and the menoid requies the (1) and (2) conditions.
- Is $\emptyset$ a group? By the second condition, it is not a group.

Given a set $\mathcal{S}$ with its associated operation $*$, to check $(\mathcal{S}, *)$ is a group, we need to check:

1. $\mathcal{S}$ is **closed** under the operation $*$, i.e., $a * b \in \mathcal{S}$ for $\forall a, b \in \mathcal{S}$
2. **Associativity**.
3. **Existence of Identity**
4. **Existence of Inverse**

Proposition 1.1 $(\mathbb{Q}, +)$ is a group.

Proof. 1. For $\forall a, b \in \mathbb{Q}$, it is easy to show $a + b \in \mathbb{Q}$.

2. Associativity: $(a+b)+c=a+(b+c)$ for $\forall a,b\in\mathbb{Q}$
3. Existence of Identity: Take the identity $0\in\mathbb{Q}$, we have $0+a=a+0=a$ for $\forall a\in\mathbb{Q}$.
4. Existence of Inverse: For $\forall a\in\mathbb{Q}$, it follows that $(-a)\in\mathbb{Q}$ s.t. $(-a)+a=a+(-a)=0$.

■

Note that $(\mathbb{Q},\cdot)$ is not a group since inverse does not exist.

R Note that the existence of identity is unique, which will be shown in the future.

Proposition 1.2 $(u_m,\cdot)$ is a group, where

$$u_m=\{1,\xi^m,\ldots,\xi_m^{m-1}\}$$

with $\xi^m=1$ and $\xi\neq 1$.

Proof.
1. Note that for $\forall\xi^j,\xi^k\in u_m$, we have

$$\xi^j\cdot\xi^k:=\xi^{j+k}=\begin{cases}\xi^{j+k}, j+k\leq m-1\\ \xi^{j+k-m}, j+k\geq m\end{cases}$$

2. The associativity is easy to show.
3. Take the identity $e=1$.
4. For $\forall\xi^k\in u_m$, we take the inverse ξ^{m-k}.

■

Proposition 1.3 The set $\mathcal{G}=\{\text{bijections of }\mathbb{R}\}$ associated with the **conposition** operator is a group.

Definition 1.2 [bijection] The bijection contains **injective**, i.e., $f(x)=f(y)$ implies $x=y$; and **supjective**, i.e., $\forall y\in\mathcal{B},\exists x\in\mathcal{A}$ s.t. $f(x)=y$. ■

Proof.
1. $\forall f,g\in\mathcal{G}$,

- Injective: take $x, y \in \mathbb{R}$ s.t. $(f \odot g)(x) = (f \odot g)(y)$, it follows that

$$f(g(x)) = f(g(y)) \implies g(x) = g(y) \implies x = y.$$

- Subjective: take $y \in \mathbb{R}$ s.t. $f(z) = y$. Hence, $\exists x \in \mathbb{R}$ s.t. $g(x) = z$, which implies $f(g(x)) = y$.

2. For any functions $f, g, h \in \mathcal{G}$,

$$((f \odot g) \odot h)(x) = (f \odot g)(h(x)) = f(g(h(x))), \forall x \in \mathbb{R}$$

Similarly,

$$(f \odot (g \odot h))(x) = f((g \odot h)(x)) = f(g(h(x))), \forall x \in \mathbb{R}$$

3. Define $e : x \mapsto x$. Then $e \in \mathbb{G}$. It follows that

$$(e * g)(x) = e(g(x)) = g(x)$$

Similarly, $(g * e)(x) = g(x)$. Hence, e is the identity.

4. For $\forall f \in \mathcal{G}$, take $f^{-1} : f(x) \mapsto x$. Firstly verify f^{-1} is a bijection. Then we have

$$f^{-1} \odot f = f \odot f^{-1} = e.$$

■

Recall a definition from Linear Algebra:

$$\mathrm{GL}(n, \mathbb{R}) := \{\boldsymbol{A} \in \mathcal{M}_n(\mathbb{R}) \mid \det(\boldsymbol{A}) \neq 0\}$$

where $\mathcal{M}_n(\mathbb{R})$ denotes the set of $n \times n$ matrices over $\mathbb{R}$.

Proposition 1.4 The set $\mathrm{GL}(n, \mathbb{R})$ associated with the matrix multiplication operator is the general linear group.

Proof. 1. $\forall \boldsymbol{A}, \boldsymbol{B} \in \mathrm{GL}(n, \mathbb{R})$, we have $\boldsymbol{AB} \in \mathrm{GL}(n, \mathbb{R})$ since

$$\det(\boldsymbol{AB}) = \det(\boldsymbol{A}) \det(\boldsymbol{B}) \neq 0$$

2. Associativity of matrix multiplication is easy to verify
3. Take the identity $e := \boldsymbol{I}_n$
4. Inverse is $\boldsymbol{A}^{-1}$.

■

R $\mathrm{SL}(n, \mathbb{R}) := \{\boldsymbol{A} \in \mathcal{M}_n(\mathbb{R}) \mid \det(\boldsymbol{A}) = 1\}$ is a special linear group.

Proposition 1.5 Let $n \in \mathbb{Z}^+$, for the set

$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$

associated with the operation

$$+_n \text{ such that } \quad a +_n b = \begin{cases} a + b, \text{ if } a + b \leq n - 1 \\ a + b - n, \text{ if } a + b \geq n \end{cases}$$

Proof. 1. Closed under operation

2. Associativity:

$$(a +_n b +_n c) = a + b + c \in \mathbb{Z}_n \text{ or } a + b + c - n \in \mathbb{Z}_n \text{ or } a + b + c - 2n \in \mathbb{Z}_n$$

3. Identity?
4. Inverse?

■

In the future we abuse the operator $+$ to denote the $+_n$ for $\mathbb{Z}_n$.

Theorem 1.1 Given a sequence of elements $g_1, \ldots, g_n$ in the group $\mathcal{G}$ associated with $\cdot$, the product is independent from adding brackets.

Proof. We show it by induction. Let $\mathcal{P}(n)$ denotes the product is the same whatever different ways of putting brackets on $g_1, \ldots, g_n$

1. Easy to verify $\mathcal{P}(1)$ is true.
2. Assume $\mathcal{P}(n)$ is true for $n \leq k$. Consider $n = k+1$. For $\forall m \leq n$, we have

$$\begin{aligned}
&(g_1 g_2 \cdots g_m)(g_{m+1} \cdots g_{k+1}) \\
&\qquad = (g_1(g_2 \cdots g_m))(g_{m+1} \cdots g_{k+1}) \\
&\qquad = g_1((g_2 \cdots g_m)(g_{m+1} \cdots g_{k+1})) \\
&\qquad = g_1(g_2 \cdots g_{k+1}) \\
&\qquad = g_1 \cdots g_{k+1}
\end{aligned}$$

■

R Theorem (1.1) shows that given a sequence of elements multiplied together, we do not need to specify the order of operations that performed.

Moreover, for **abelian** groups, the group is unqiue regardless of the ordering of elements.

Theorem 1.2 Each group $(\mathcal{G}, *)$ has the unique identity.

Proof. Let $e, e' \in \mathcal{G}$ be two identites. By definition,

$$e' = e' * e = e.$$

■

Theorem 1.3 Let $\mathcal{G}$ be a group, then g^{-1} is unique for any $g \in \mathcal{G}$.

Proof. Let h_1, h_2 be two inverses of $g \in \mathcal{G}$, by definition,

$$h_1 = h_1 \cdot e = h_1 \cdot (g h_2) = (h_1 g) h_2 = e \cdot h_2 = h_2.$$

■

R Due to Theorem(1.1) to (1.3), it makes sense to define

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}}, \qquad g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}, \qquad g^0 := e.$$

Proposition 1.6 Let $(\mathcal{G}, \cdot)$ be a group, then

1. $(g^{-1})^{-1} = g, \forall g \in \mathcal{G}$
2. $(ab)^{-1} = b^{-1}a^{-1}$, $\forall a, b \in \mathcal{G}$
3. $g^m \cdot g^n = g^{m+n}$, $\forall g \in \mathcal{G}, m, n \in \mathbb{Z}$.

In fact, we can redefine groups as the semigroups with a weaker condition.

Definition 1.3 [Group]

- A group $\mathcal{G}$ is a **semigroup** with a binary operation $\cdot$ such that
  - There exists a left identity $e \in \mathcal{G}$ s.t.

$$e \cdot a = a, \quad \forall a \in \mathcal{G}$$

  - For each $a \in \mathcal{G}$, there exists a left inverse $a^{-1} \in \mathcal{G}$ s.t.

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

- A set $\mathcal{G}$ equipped with a binary operation $\cdot$ is said to be a **semigroup** if
  1. It is closed under the operation $\cdot$
  2. It satisfies the associativity.

■

Proposition 1.7 The definition(1.1) adn definition(1.3) are equivalent.

Proof. It suffices to show that the left identity and left inverse are essentially identity and inverse, respectively.

1. Suppose a^{-1} is the left inverse of a, we have

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

   It follows that

$$\begin{aligned} aa^{-1} &= (a^{-1})^{-1}a^{-1}aa^{-1} \\ &= (a^{-1})^{-1}(a^{-1}a)a^{-1} \\ &= (a^{-1})^{-1}ea^{-1} \\ &= e \end{aligned}$$

2. Suppose e is the left identity, it follows that

$$ae = a(a^{-1}a) = (aa^{-1})a = ea = a$$

■

Similarly, we can define a group with help of right identities and right inverses; but we cannot define a group by left identities and right inverses. Here is a counterexample:

■ **Example 1.1** Let $(\mathcal{G}, *)$ be a group with at least 2 elements such that

$$a * b = b, \quad \forall a, b \in \mathcal{G}$$

Note that $\mathcal{G}$ is closed under $*$ and associative. The group $\mathcal{G}$ has left identities and rihgt inverses. But $\mathcal{G}$ is not a group by definition. ■

If a group is **finite**, then its operation can be described by its Cayley table, or multiplication table.

■ **Example 1.2** For a group $\mathcal{G} = \{e, a\}$ equipped with $*$, its Cayley table is given by:

$*$	e	a
e	e	a
a	a	e

For a group $(\mathbb{Z}_6, +)$, its Cayley table is given by:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

■

R Note that a group can be described by a cayley table. But not all cayley tables define a group.

R It is usually messy to check whether the cayley table defines a group. There are a few necessary conditions we can examine (to exclude Cayley Tables that don't define groups):

- It has a row and column that is identical to the list of the elements
- The elements in each row and each column must be all distinct.

Chapter 2

Week2

2.1. Tuesday

2.1.1. Review

Note that a group has the property of closeness, associatity, identity and its inverse

2.1.2. Cyclic groups

Definition 2.1 [Ablian] Let $(\mathcal{G},*)$ be a group, it is said to be **ablian** if

$$a*b=b*a, \quad \forall a,b\in\mathcal{G}$$

■

Definition 2.2 [Order] Let $\mathcal{G}$ be a group with the identity e. The **order** if an element $g\in\mathcal{G}$ is denoted by $|g|$, i.e., the smallest $n\in\mathbb{N}^+$ such that $g^n=e$. If $|g|=\infty$, then g has **infinite order**. ■

Definition 2.3 [Periodic Group] A group is said to be

1. **periodic** (torsion) if every element from this group is of finite order.
2. **torsion-free** if every non-identity has infinite order.

■

Note that not torsion is not equivalent to torsion-free; not torsion-free is not equivalent

to torsion.

Proposition 2.1 If $|\mathcal{G}| < \infty$, then $|g| < \infty$ for $\forall g \in \mathcal{G}$.

Proof. If $|g| = \infty$, then

$$\{e, g, g^2, \cdots, g^n, \ldots\} \subseteq \mathcal{G},$$

which implies $|\mathcal{G}| = \infty$. ■

Proposition 2.2 Let $\mathcal{G}$ be a group with identity e. If $g^n = e$ for some $n \in \mathbb{N}^+$, then $|g||n$.

Proof. Let $m := |g| \leq n$. Recall the ideas from discrete mathematics:

Theorem 2.1 — **well-ordering principle.** Any $S \subseteq \mathbb{N}$ has a least element (Axiom).

Theorem 2.2 — **Division Theorem.** For $\forall m \in \mathbb{Z}$ and $n \in \mathbb{N}^+$, there always $\exists\, q, r \in \mathbb{Z}$ such that

$$m = nq + r,$$

where $0 \leq r < n$.

Note that the power g^n can be rewritten as:

$$g^n := g^{mq+r} = (g^m)^q \cdot g^r = e.$$

Since $(g^m)^q$ equals to e, we imply $g^r = e, r < m$, i.e., $r = 0$. ■

R Not that the condition $n \in \mathbb{N}^+$ can be relaxed into $n \in \mathbb{Z}$.

Definition 2.4 [cyclic] A group $\mathcal{G}$ is **cyclic** if there $\exists g \in \mathcal{G}$ such that for $\forall x \in \mathcal{G}$, there always $\exists n \in \mathbb{Z}$ such that

$$x = g^n.$$

We rewrite the group as $\mathcal{G} = < g >$, we call g as the **generator** of $\mathcal{G}$. The notation $< g >$

means:

$$< g >:= \{\cdots, g^{-2}, g^{-1}, e.g, g^2, \cdots\}$$

Proposition 2.3 Given a group $\mathcal{G}$ and $g \in \mathcal{G}$, we have $| < g > | = |g|$.

Proof.

- If $|g| = \infty$, the result is trivial.
- If $|g| = n$, we imply $| < g > | = |\{e, g, \ldots, g^{n-1}\}| = n$.

■

Definition 2.5 Let $a, b \in \mathbb{Z}$ not all zero. The greatest common divisor is defined as:

$$\gcd(a,b) := \text{the greatest integer that divides } a \text{ and } b.$$

Theorem 2.3 — Bezout. Provided with $a, b \in \mathbb{Z}$ not all zero. Then there exists $s, t \in \mathbb{Z}$ such that

$$sa + tb = \gcd(a,b)$$

■ **Example 2.1**

1. $(\mathbb{Z}, +)$ is **cyclic** with generator ± 1
2. $(\mathbb{Z}_n, +) =< k >$, where $\gcd(k,n) = 1$. This is because we can always find $s > 0$ and $t < 0$ such that $sa + tb = 1$, i.e.,

$$1 = \underbrace{k + \cdots + k}_{s \text{ terms}} \in \mathbb{Z}_n$$

3. $(u_m, \cdot) =< \xi_m^k >$, where $\xi_m = \exp(\frac{2\pi i}{m})$ and $\gcd(k,m) = 1$. This is because we can similarly consturct $s > 0$ s.t. $(\xi_m^k)^s = \xi_m$.

Proposition 2.4 Every cyclic group is abelian.

Proof. As $\mathcal{G} =< g >$, for $\forall x, y \in \mathcal{G}$, we have

$$x \cdot y = g^m \cdot g^n = g^{m+n} = g^n \cdot g^m = y \cdot x.$$

■

R The converse of proposition(2.4) is not true. For example, $(\mathbb{Q}, +)$ is abelian, but it is not cyclic, i.e., if $(\mathbb{Q}, +) =< \frac{n}{m} >$, we find $\frac{n}{2m} \notin < \frac{n}{m} >$.

Definition 2.6 Let X be a set. A **permutation** of X is a **bijection** of X. We denote

$$\text{Sym}(X) = \{\text{all permutations of } X\}$$

■

Proposition 2.5 $\text{Sym}(X)$ is a group under composition operation.

Proof.

1. For $\forall \alpha, \beta \in \text{Sym}(X)$, we have $\alpha \circ \beta \in \text{Sym}(X)$ as the composition of bijections is also bijection.
2. For $\forall \alpha, \beta, \gamma \in \text{Sym}(X)$, we have $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.
3. identity = id$\in$Sym(X)
4. For $\forall \sigma \in \text{Sym}(X)$, we choose $\rho \in \text{Sym}(X)$ s.t.

$$\rho : \sigma(x) \mapsto x, \forall x \in X$$

It follows that $\rho \circ \sigma = \text{id}$, since

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

■

Let $X = \{1,2,\ldots,n\}$, we denote $\mathbb{S}_n = \mathrm{Sym}(X)$. Describe $\sigma \in \mathbb{S}_n$ by:

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

Note that $|\mathbb{S}_n| = n!$

■ **Example 2.2** Consider $\mathcal{G} := \mathbb{S}_3$, then $\sigma, \beta \in \mathcal{G}$:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} := (1,2,3) \qquad \beta := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} := (1,2)$$

Then we compute the composite $\sigma \circ \beta$:

$$\sigma \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

and $\beta \circ \sigma$:

$$\beta \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

and $\sigma \circ \sigma \circ \sigma$:

$$\sigma \circ \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}^3 = \mathrm{id},$$

which is said to be **3-cycle**, which will be talked in future. ■

R In general, $\mathbb{S}_n$ is not **ablian** for $n \geq 3$.

In general, we write the k-cycle permutation as:

$$\alpha = (i_1, \ldots, i_k)$$

where $i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_k \mapsto i_1$.

■ **Example 2.3** Consider $\sigma = (15)(246) \in S_6$, i.e.,

$$\sigma = 1 \mapsto 5 \mapsto 1; \qquad 2 \mapsto 4 \mapsto 6 \mapsto 2; \qquad 3 \mapsto 3$$

and $\alpha = (13)(45) \in S_6$. We study the composition $\sigma \circ \alpha$:

$$\sigma \circ \alpha = [(15)(246)] \circ [(13)(45)] = (135624)$$

and

$$\alpha \circ \sigma = (13)(45)(15)(246) = (146253)$$

■

Proposition 2.6 Each $\sigma \in S_n$ is either a cycle or a product of disjoint cycle.

Disjoint cycles commute with one another.

Definition 2.7 2-cycle is called a **transposition** ■

Proposition 2.7 $\sigma \in S_n$ can be written as a product of transpositions.

Proof. Due to proposition(2.6) and

$$(i_1 i_2 \cdots i_k) = (i_1 i_k) \cdots (i_1 i_3)(i_1 i_2)$$

■

For $\sigma \in S_n$, we have

$$\sigma(i_1,\ldots,i_k)\sigma^{-1} = (\sigma(i_1),\ldots,\sigma(i_k))$$

Chapter 3

Week3

3.1. Tuesday

Definition 3.1 [Cartesian Product]

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in S_i\}$$

■

Theorem 3.1 $\prod_{i=1}^{n} G_i$ is a group under the operation

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

Proof.

- It's obvious that the operation is closed.
- Check inverse and identity.

$$\text{identity} = (e_1, e_2, \ldots, e_n)$$

- Check the operation is associate:

$$\begin{aligned}
[(g_1, \ldots, g_n)(h_1, \ldots, h_n)](k_1, \ldots, k_n) &= (g_1 h_1, \ldots, g_n h_n)(k_1, \ldots, k_n) \\
&= (g_1 h_1 k_1, \ldots, g_n h_n k_n) \\
&= (g_1, \ldots, g_n)(h_1 k_1, \ldots, h_n k_n) \\
&= (g_1, \ldots, g_n)[(h_1, \ldots, h_n)(k_1, \ldots, k_n)]
\end{aligned}$$

■

R If the operation of each G_i is the **addition**, then

$$\prod_{i=1}^{n} G_i := \oplus_{i=1}^{n} G_i$$

■ **Example 3.1**

1. $G = (S_3 \times \mathbb{Z}_2, \cdot)$ is not abelian, e.g.,

$$((12),0) \cdot ((23),0)$$

2. $G = (\mathbb{Z}_2 \times \mathbb{Z}_3, +) = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic

$$d(1,1) = (0,0) \implies d = 6k$$

3. The **Klein** 4-group $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic

$$d(x,y) = (0,0)$$

■

Theorem 3.2 $G = \mathbb{Z}_m \times \mathbb{Z}_n$ is **cyclic** iff $gcd(m,n) = 1$.

Proof. Let $k = lcn(m,n) = \frac{mn}{gcd(m,n)} \leq mn$.

Necessity. Consider $(a,b) \in G$:

$$k(a,b) = (ka,kb) := (msa,ntb) = (0,0),$$

i.e., $|(a,b)| \leq k$. In particular, $mn \leq k$, thus $k = mn$, i.e., $gcd(m,n) = 1$.

Sufficiency. Consider $(1,1) \in G$: $d(1,1) = (0,*) \implies d = xm$; and $d(1,1) = (*,0) \implies d = yn$. Thus $|(1,1)| = lcm(m,n) = mn$, i.e., this group is cyclic. ■

Corollary 3.1 $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic iff (m_i, m_j) are mutually coprime.

Definition 3.2 Let G be a group, S a non-empty subset.

$$< S >:= \{a_1^{m_1}, \ldots, a_n^{m_n} \mid n \in \mathbb{Z}^+, m_i \in \mathbb{Z}, a_i \in S\}$$

If S is finite, then $< S >$ is **finitely generated**. ■

Verify that this is a group, i.e., a subgroup of G. Note that a_i's need not to be distinct.

e.g.,

$$S = \{a, b\} \implies a^{-1}bab^2 \in < S >$$

Proposition 3.1

$$< S >= \bigcap_{\{H \mid S \subseteq H \subseteq G\}} H$$

■ **Example 3.2** 1. $<$ cycles in $S_n >= S_n =<$ transpositions $>$

2. $S_n =< (12), (1,2,\ldots,n) >$.

   hint: $(i, i+1) \in S_n, (i,j) \in S_n$

3. $D_n =< r, s >$

■

Proposition 3.2 $\mathbb{Q}$ is not finitely generated.

Theorem 3.3 — **Fundamental Theorem of Finitely Generated Abelian Groups.** Any finitely generated abelian group (is isomorphic to)

$$\prod_{i=1}^{m} \mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}^n,$$

$r_i, n \in \mathbb{N}$.

■ **Example 3.3** abelian group of order $360 = 2^3 3^2 5$:

$$G_2 \times G_3 \times G_5$$

$G_5 = \mathbb{Z}_5$, $G_3 = \mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_9$, $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_8$.

Thus there are 6 possible abelian groups of order 360. ■

How about abelian group of order 7^5?

Definition 3.3 [Partition] Let $S \neq \emptyset$. A **partition** P of S is $\{S_i \mid i \in I\}$ such that

1. $S_i \neq \emptyset, \forall i \in I$
2. $S_i \bigcap S_j = \emptyset, \forall i \neq j$
3. $\bigcup_{i \in I} S_i = S$

Also, we denote $S = \bigsqcup_{i \in I} S_i$ ■

Definition 3.4 [Equivalence Relation] An **equivalence relation** on S is a relation $\sim$ such that

1. Reflexive: $a \sim a, \forall a \in S$
2. Symmetric: $a \sim b$ implies $b \sim a$
3. Transitive: $a \sim b, b \sim c$ implies $a \sim c$.

■

Equivalence relation is essentially the same meaning of partition:

- Partition implies equivalence relation: Define $a \sim b$ if $a, b \in S_i$
- Equivalence relation implies partition: Define $C_a := \{b \in S \mid b \sim a\}$. (For the symmeticity part, show that $C_a \bigcap C_b \neq \emptyset$ implies $C_a = C_b$.)

We call C_a the **equivalence class** with the representative a. If $b \in C_a$, then $C_b = C_a$, so any element in an equivalence class can be its representative.

Proposition 3.3 Any $\sigma \in S_n$ is a product of disjoint cycles.

Proof. Given $a, b \in X = \{1, 2, \ldots, n\}$, define $a \sim b$ if $b = \sigma^k(a)$ for some $k \in \mathbb{Z}$. ■

3.2. Thursday

3.2.1. Cyclic Groups

Definition 3.5 [order] Let G be a group with **identity** e. The **order** of an element $g \in G$, denoted by $|g|$ is the smallest $n \in \mathbb{N}^+$ such that $g^n = e$; if no such n exists, we say g has **infinite order** and $|g| = \infty$. ∎

Proposition 3.4 If G has finite order, then every element of G has finite order. (The order of G is the number of elements in G).

Proof. Suppose $|G| = m$, consider the elements in G:

$$g^0 := e, g^1, \ldots, g^m,$$

thus there exists $0 \leq i < j \leq m$ such that $g^i = g^j$, otherwise there will be $m+1$ distinct elements in G. Therefore $g^{-i}g^i = e = g^{j-i}$. ■

R Note that the converse of this proposition is not true.

Definition 3.6 [Torsion] A group is said to be a **periodic group** (or **torsion group**) if all its elements all have **finite** order; A group is said to be **torsion-free** if none of its non-trivial elements has finite order. Finite groups are always periodic. ∎

Proposition 3.5 Let G be a group with identity e, and $g \in G$. If $g^n = e$ for some $n \in \mathbb{Z}$, then $|g|$ divides n, i.e., $|g||n$.

Proof. Let $m = |g|$. There exists $q, r \in \mathbb{N}^+$ such that

$$n = mq + r \quad 0 \leq r < m$$

It follows that $g^n = (g^m)^q \cdot g^r = e = g^r$, which follows that $r = 0$. ■

Definition 3.7 [Cyclic] A group G is said to be **cyclic** if there exists $g \in G$ such that every element of G is equal to g^n for some $n \in \mathbb{Z}$. In this case, we say g is a **generator** of G and write $G = \langle g \rangle$. ■

In general, $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Proposition 3.6 Let G be a group and $g \in G$. Then $|\langle g \rangle| = |g|$.

Question.

Proof. Note that $m := |g| \leq |\langle g \rangle|$, since $g^0, g^1, \ldots, g^{m-1}$ are distinct; and also $|\langle g \rangle| \leq |g|$, since $g^i = g^j$ iff $i \equiv j \pmod{m}$ ■

R The generator of a cyclic group may not be unique, i.e., there may exists distinct $g_1, g_2 \in G$ s.t. $G = \langle g_1 \rangle = \langle g_2 \rangle$.

Applications. To illustrate some examples, we introduce some results from discrete mathematics:

Definition 3.8 Let $a, b \in \mathbb{Z}$ s.t. $a^2 + b^2 \neq 0$. The **greatest common divisor** is defined as:

$$\gcd(a,b) := \text{greatest integer that divides both } a \text{ and } b$$

■

Theorem 3.4 — **Bezout's identity.** Let $a, b \in \mathbb{Z}$ s.t. $a^2 + b^2 \neq 0$. There exists $s, t \in \mathbb{Z}$ s.t.

$$sa + tb = \gcd(a,b)$$

■ **Example 3.4**

1. $(\mathbb{Z}, +)$ is cyclic, generated by 1 or -1.
2. $(\mathbb{Z}_n, +)$ is cyclic, generated by k with $\gcd(k,n) = 1$.
3. $(U_m, \cdot)$ is cyclic, generated by $\zeta_m^k = \exp(\frac{2k\pi}{m} i)$ with $\gcd(k,m) = 1$.

Note that $U_m := \{1, \zeta_m^1, \ldots, \zeta_m^{m-1}\}$.

Proposition 3.7 A cyclic group G has order n iff its generators have order n.

Question: Can we apply proposition(3.6) directly

Proof.

- Suppose g is a generator of G with order n, thus $|G| = |\langle g \rangle| = n$.
- Suppose G is a cyclic group with order n and g is a generator of G, then $|g| = |\langle g \rangle| = |G| = n$.

■

Proposition 3.8 Let p be a prime. Let $G = (\mathbb{Z}_p, +)$. Then $|g| = p$ for $\forall g \in G \setminus \{0\}$.

Proof.

- One way is to apply proposition(3.7). The cyclic group G has order p and therefore its generators have order p. $g \in G \setminus \{0\}$ are generators since

$$sp + tg = \gcd(p, g) = 1 \implies (sk)p + (tk)g = k, \quad 1 \leq k \leq p$$

- Another way is to assume $|g| = y$ for $1 \leq y < p$, since $g^i = g^j$ iff $i \equiv j \pmod{p}$ and $g^p \equiv 0 \pmod{p}$. Since $sp + tg = \gcd(p, g) = 1$, we derive for $1 \leq y < p$,

$$(sy)p + (ty)g = y \implies y \equiv 0 \pmod{p},$$

which is a contradiction

■

Proposition 3.9 Every cyclic group is abelian.

Recall that abelian means a group has commucative operation.

Proof. Suppose $G = \langle g \rangle$ for some $g \in G$, thus for any elements g^{n_1}, g^{n_2}:

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

since the product of the elements is independent from adding parentheses. ■

R The converse is not true, e.g., the group $(\mathbb{Q},+)$.

Verification: Assume $\mathbb{Q} = \langle \frac{p}{q} \rangle$, i.e., Choose $k > 1$ such that $(k,q) = 1$ and set $y = \frac{1}{k} \in G$. There exists $r \in \mathbb{Z}$ such that $(\frac{p}{q})^r = \frac{rp}{q} = y$, which implies $rp = qy = \frac{y}{k}$, which is a contradiciton since RHS is not an integer.

3.2.2. Symmetric Groups

Definition 3.9 Let X be a set. A **permutation** of X is a bijection $\sigma : X \mapsto X/$ ■

Proposition 3.10 The set of all permutations of a set X forms a group under the operation $\circ$ (composition), denoted by $\mathrm{Sym}(X)$. (**symmetric group**)

Proof.

- Note that $\alpha \circ \beta$ is a bijection of X, hence permutation of X
- $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
- e is a permutation such that $e(x) = x$, $\forall x \in X$. Then

$$e \circ \sigma = \sigma \circ e = \sigma, \quad \forall \sigma \in \mathrm{Sym}(X)$$

- For a given $\sigma \in \mathrm{Sym}(X)$, there exixts a bijection $\rho \in \mathrm{Sym}(X)$ such that

$$\rho \circ \sigma = \sigma \circ \rho = e$$

■

Notations. For $X = \{1,2,\ldots,n\}$, we write $\mathrm{Sym}(X)$ as S_n (n-th symmetric group). The element $\sigma \in S_n$ is denoted as:

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

Proposition 3.11 $|S_n| = n!$.

Proof. $\sigma(1) \in \{1,\dots,n\}$; for fixed $\sigma(1)$, $\sigma(2) \in \{1,\dots,n\} \setminus \{\sigma(1)\}$; so on and so forth. Hence, there are totoal $n * (n-1) * \cdots * 1 = n!$ choices of permutations. ■

■ **Example 3.5** For $\alpha, \beta \in S_3$ given by:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

we find

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Thus $\alpha\beta \neq \beta\alpha$, i.e., S_3 is non-abelian. ■

Note that S_n is non-abelian for $n \geq 3$: To show this property, construct

$$\alpha' = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & 4 & \cdots & n \end{pmatrix} \quad \beta' = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ \beta(1) & \beta(2) & \beta(3) & 4 & \cdots & n \end{pmatrix}$$

Also, note that $|\alpha| = 3$. Thus S_3 is not cyclic.

More on S_n. Consider the element σ in S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix}$$

We re-write σ as

$$\sigma = (15)(246),$$

where $(i_1,\dots,i_k)$ denotes the permutation

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

and $j \mapsto j$ for all remaining j.

Definition 3.10 [cycle] We call $(i_1,\dots,i_k)$ as a k-cycle or a **cycle of length** k. In particular, we use $()$ to denote the identity $\epsilon \in S_n$, meaning that it fixes all numbers in $\{1,\dots,n\}$. ■

Proposition 3.12 Each permutation $\sigma \in S_n$ is either a cycle or a product of disjoint cycles.

We will prove proposition(3.12) later.

Proposition 3.13 Disjoint cycles commute with each other.

Proof. Suppose $\tau = (i_1,\dots,i_k)$ and $\rho = (j_1,\dots,j_l)$. Show that for $i_m \in \{i_1,\dots,i_k\}$, $\tau(\rho(i_m)) = \rho(\tau(i_m))$ and similarly for j_n; also show $\tau(\rho(s)) = \rho(\tau(s))$ for $s \in \text{dom} \setminus (I \bigcup J)$ ■

Definition 3.11 [Transposition] A 2-cycle is called a transposition, for it swaps two elements with each other. ■

Proposition 3.14 Each element of S_n is a product of transpositions (not necessarily disjoint).

Proof. Consider $(i_1 \dots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_3)(i_1 i_2)$; ■

■ **Example 3.6**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (15)(246) = (15)(26)(24) = (15)(46)(26)$$

■

Proposition 3.15 Let $n \in \mathbb{N}^+$ and $\sigma \in S_n$. Show that

$$\sigma(i_1 \cdots i_k)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_k))$$

Proof. For $x := \sigma(i_m)$, $1 \le m \le k$, we have

$$\sigma^{-1}(x) = i_m \implies (i_1 \cdots i_k)\sigma^{-1}(x) = \begin{cases} i_1, & \text{if } m = k \\ i_{m+1}, & \text{otherwise} \end{cases}$$

adn thus $\sigma(i_1 \cdots i_k)\sigma^{-1}(x) = \sigma(i_1)$ if $m = k$, and equals $\sigma(i_{m+1})$ otherwise.

For $x \in \{1,\ldots,n\} \setminus \{\sigma(i_1),\ldots,\sigma(i_k)\}$, we have $\sigma^{-1}(x) \notin \{i_1,\ldots,i_k\}$, and thus

$$(i_1 \cdots i_k)(\sigma^{-1}(x)) = \sigma^{-1}(x) \implies \sigma(i_1 \cdots i_k)(\sigma^{-1}(x)) = x.$$

■

Proposition 3.16 In every factorization of σ as a product of transpositions, the number of factors is either always even or always odd.

Proof. There is a one-to-one coorespondence between σ and binary matrix A_σ, e.g.,

$$\sigma = (15)(246) \Leftrightarrow A_\sigma = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Also, if σ is a transposition then $\det(A_\sigma) = -1$. ■

3.2.3. Dihedral Groups

Let $\mathcal{T}$ denote the set of **transformations** of $\mathbb{R}^2$, consisting of all rotations by fixed angles about the origin, and all reflections over lines through the origin.

Definition 3.12 Consider a regular n-th polygon P_n in $\mathbb{R}^2$ centered at origin. We represent the polygon by its vertices, e.g., $P_n = \{x_1,\ldots,x_n\} \subseteq \mathbb{R}^2$. If $\tau(P_n) = P_n$ for some $\tau \in \mathcal{T}$, we say that P_n is **symmetric** w.r.t. τ. ■

R Intuitively, P_n is symmetric w.r.t. n rotations $\{r_0,\ldots,r_{n-1}\}$ and n reflections $\{s_1,\ldots,s_n\}$ in $\mathcal{T}$.

Theorem 3.5 The set

$$D_n := \{r_0, r_1, \ldots, r_{n-1}, s_1, \ldots, s_n\}$$

forms the n-th **dihedral group**, under the transformation composition operation $\tau * \gamma = \tau \circ \gamma$. In particular, $|D_n| = 2n$.

Proof. The set of rotations:

$$\langle r \rangle = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}\}$$

The set of reflections:

$$\{s, rs, r^2 s, \ldots, r^{n-1} s\}$$

Thus the elements in D_n:

$$D_n = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, rs, r^2 s, \ldots, r^{n-1} s\}$$

■

Proposition 3.17 Show that $D_3 = S_3$.

3.2.4. Free Groups

Definition 3.13 [Free Groups]

1. Let S be a non-empty set (not necessarily finite). Let 1 be an **empty word**, i.e., a string of elements from S with length 0. For each $a \in S$, define an element $a^{-1} \notin S$ s.t. their juxtaposition is 1:

$$a^{-1}a = aa^{-1} = 1 \quad a^{-1}b \neq 1 \neq ba^{-1}, \forall b \neq a$$

2. Define $S^{-1} := \{a^{-1} \mid a \in S\}$. A **reduced word** w of S is a **finite** string of elements from $S \bigcup S^{-1}$ s.t. no substring of w contains $a^{-1}a$ or aa^{-1} for $\forall a \in S$. Define an

operation $*$ on the set of all reduced words F_S:

$$w_1 * w_2 = w := \begin{cases} w_1 w_2, & \text{if } w_1 w_2 \text{ is a reduced word} \\ & \text{obtained by repeatedly removing } a^{-1}a \text{ or } aa^{-1} \end{cases},$$

$\forall w_1, w_2 \in F_S$. It can be verified that $(F_S, *)$ forms a group, called the **free group** generated by S.

■

Notations. For convenience,

$$a^n := \underbrace{a \cdots a}_{n} \quad a^{-n} := \underbrace{a^{-1} \cdots a^{-1}}_{n}$$

■ **Example 3.7** Let $S = \{a, b, c\}$, then

$$w_1 = ac^{-4}b^2c, w_2 = c^{-1}b^{-2}c^2a^{-3}, w_3 = a^3c^{-2}b^3$$

are reduced words of S, while $w_1 w_2$ and $w_2 w_3$ are not. Also,

$$(w_1 * w_2) * w_3 = ac^{-4}b^3 = w_1 * (w_2 * w_3)$$

■

■ **Example 3.8** Let $S = \{a\}$ be a singleton. then the free group F_S can be viewed as the group $(\mathbb{Z}, +)$ ■

In fact, any group can be viewed as a free group with some additional conditions. For instance, a cyclic group G of order 6 can be viewed as the group F_S with the condition that $a^6 = 1$, which is sometimes written as $G = \langle a | a^6 = 1 \rangle$

Chapter 4

Week4

4.1. Subgroups

Definition 4.1 Let G be a group. A **non-empty** subset $H \subseteq G$ is a **subgroup** of G (denoted by $H \leq G$) if it satisfies the following:

1. If $a, b \in H$, then $a * b \in H$
2. If $a \in H$, then $a^{-1} \in H$

Particularly, if H is a **proper subset** of G, then H is a **proper subgroup** of G, denoted by $H < G$. ■

R Any subgroup H is a subgroup iff H is a subset of G, and H forms a group w.r.t. the induced binary operation from G (called the induced operation on H)

■ **Example 4.1**

1. Any group G contains the trivial subgroup $\{e\}$, (sometimes writeen as 1 for such group). Any subgroup $H \neq 1$ is **non-trivial**
2. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ under addition; $\mathbb{Z}^{\#} < \mathbb{Q}^{\#} < \mathbb{R}^{\#} < \mathbb{C}^{\#}$ under multiplication
3. For any $n \in \mathbb{Z}$, we have $n\mathbb{Z} \leq \mathbb{Z}$ under addition
4. Define $\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathbb{R}^{n \times n} \mid \det(A) = 1\}$ and $\mathrm{GL}(n, \mathbb{R}) := \{A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0\}$, then $\mathrm{SL}(n, \mathbb{R}) < \mathrm{GL}(n, \mathbb{R})$
5. The set of all rotations (including the trivial rotation) in a dihedral group D_n is a subgroup of D_n
6. Viewing the elements in D_n as permutations of the vertices of a regular n-gon P_n,

we regard D_n as a subgroup of S_n

7. For any $n \in \mathbb{N}^+$, a permutation $\sigma \in S_n$ is **even** (**odd**) if it is a product of an even (odd) number of transpositions. The set of all even permutations in S_n forms the n-th **alternating group** $A_n \leq S_n$.

■

Proposition 4.1 Let H be a non-empty subset of a group G. Then $H \leq G$ iff $ab^{-1} \in H$ whenever $a, b \in H$

Proof. Necessity:

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

Sufficiency: Let e be the identity of G. As H is non-empty, there exists $h \in H$ s.t.

$$e = hh^{-1} \in H$$

- Since $e \in H$, for any $a \in H$, we have $a^{-1} = e \cdot a^{-1} \in H$
- For any $a, b \in H$, we have $b^{-1} \in H$.

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

■

4.1.1. Cyclic subgroups

Given a group G and any element g, we have subset

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

It is indeed the cyclic subgroup generated by g.

Proposition 4.2 The intersection of any collection of subgroups of a group G is also a subgroup of G.

Corollary 4.1 Let G be a group. Then for any $g \in G$, we have

$$\langle g \rangle = \bigcap_{\{H | g \in H \leq G\}} H,$$

i.e., $\langle g \rangle$ is the smallest subgroup of G containing g.

Proof. Note that $\bigcap_{\{H|g\in H\leq G\}} H \subseteq \langle g \rangle$.

On the other hand, note that $\bigcap_{\{H|g\in H\leq G\}} H$ is a subgroup,

$$\langle g \rangle \subseteq \bigcap_{\{H | g \in H \leq G\}} H$$

■

Proposition 4.3 Every subgroup of a cyclic group is cyclic

Proof. Let $G = \langle g \rangle$ and $H \leq G$

- If $H = 1$, then $H = \langle e \rangle$ is cyclic
- Otherwise, there exists a samllest $m \in \mathbb{N}^+$ s.t. $g^m \in H$. It suffices to show $H = \langle g^m \rangle$
  - It's clear that $\langle g^m \rangle \subseteq H$
  - Take $g^n \in H$, there exists $q, r \in \mathbb{Z}$ s.t.

$$n = mq + r, \quad 0 \leq r < m$$

Therefore, $g^n = (g^m)^q \cdot g^r \implies g^r = (g^m)^{-q} \cdot g^n \in H \implies r = 0$. Thus $g^n \in \langle g^m \rangle$, i.e., $H \subseteq \langle g^m \rangle$.

■

Corollary 4.2 Any subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{N}$.

R For $a, b \in \mathbb{Z}$, it's easy to verify

$$\langle a, b \rangle := \{ma + nb \mid m, n \in \mathbb{Z}\} \leq \mathbb{Z} \tag{4.1}$$

Thus following corollary(4.2), $\langle a,b\rangle = d\mathbb{Z}$ for some $d \in \mathbb{N}^+$. In fact, d is the greatest common divisor of a and b. (proof relies on Bezout's identity.)

Theorem 4.1 — **Bezout's identity.** Let $a,b \in \mathbb{Z}$ such that $a^2+b^2 \neq 0$. Then there exists $s,t \in \mathbb{Z}$ s.t.

$$sa+tb = \gcd(a,b)$$

Proof. Consider the case that $ab \neq 0$.

Note that $\langle a,b\rangle = d\mathbb{Z}$, there exists s,t such that

$$sa+tb = d \tag{4.2}$$

Since $a,b \in d\mathbb{Z}$, we derive d divides both a and b. From (4.2), for any x dividing both a and b, we have $x|d$, which implies $\gcd(a,b)|d$, which implies $d = \gcd(a,b)$. ■

Proposition 4.4 Let $a,b \in \mathbb{Z}$ be such that $a^2+b^2 \neq 0$ and $k \in \mathbb{Z}^{\#}$. Show that

$$\gcd(ak,bk) = \gcd(a,b)k$$

Proof. First, since $\gcd(a,b)$ divides both a and b, we imply $\gcd(a,b)k$ divides both ak and bk. It follows that

$$\gcd(a,b)k | s(ak)+t(bk) = \gcd(ak,bk),$$

for some s,t.

Second,

$$\gcd(ak,bk) | s(ak)+t(bk) = k\gcd(a,b)$$

■

Let $a,b \in \mathbb{Z}$ s.t. $a^2+b^2 \neq 0$. The **least common multiple** is

$$\operatorname{lcm}(a,b) = \begin{cases} \text{least positive integer divisible by } a \text{ and } b, & ab \neq 0 \\ 0, & \text{otherwise} \end{cases}$$

Theorem 4.2 Let $a, b \in \mathbb{Z}$ s.t. $a^2 + b^2 \neq 0$. Then

$$\operatorname{lcm}(a,b) = \frac{|ab|}{\gcd(a,b)}$$

Proof. w.l.o.g., $a, b > 0$.

Note that a and b divides $\frac{ab}{\gcd(a,b)}$, and thus $k \leq \frac{ab}{\gcd(a,b)}$.

On the other hand, note that ab divides both $a\operatorname{lcm}(a,b)$ and $b\operatorname{lcm}(a,b)$, which implies

$$ab \leq \gcd(a\operatorname{lcm}(a,b), b\operatorname{lcm}(a,b)) = \operatorname{lcm}(a,b)\gcd(a,b)$$

■

Proposition 4.5 Let $G = \langle g \rangle$ be a cyclic group of order n. Let $g^s \in G$, then

$$|g^s| = \frac{n}{d},$$

where $d = \gcd(s,b)$. Moreover, $\langle g^s \rangle = \langle g^t \rangle$ iff $\gcd(s,n) = \gcd(t,n)$.

Proof. The idea is to transform the order of element into the order of a cyclic group.

- For some $x, y \in \mathbb{Z}$,

$$g^d = g^{xs+yn} = (g^s)^x \in \langle g^s \rangle \implies \langle g^d \rangle \subseteq \langle g^s \rangle$$

On the other hand, g^s is the power of g^d since d divides s:

$$g^s = (g^d)^{s/d} \implies \langle g^s \rangle \subseteq \langle g^d \rangle \implies \langle g^s \rangle = \langle g^d \rangle$$

it follows that

$$|g^s| = |\langle g^s \rangle| = |\langle g^d \rangle| = |g^d| = \frac{n}{d}$$

- For second assrtion, the converse is clear. For the forward direction,

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

■

Corollary 4.3 All generators of a cyclic group $G = \langle g \rangle$ of order n are of the form g^r with $\gcd(r,n) = 1$.

■ **Example 4.2** Given the **cyclic group** $G = \mathbb{Z}_{12} = \langle g \rangle$, then all the generators of G are g, g^5, g^7, g^{11}; since $\gcd(9,12) = \gcd(3,12) = 3$, we have $\langle g^3 \rangle = \langle g^9 \rangle$ ■

4.1.2. Direct Products

Definition 4.2 [Cartesian Product] The **Cartesian product** of given sets $S_1, \ldots, S_n$ is

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n := \{(a_1, \ldots, a_n) \mid a_i \in S_i\}$$

If $S_1 = S_2 = \cdots = S_n$, we write $\prod_{i=1}^{n} S_i = S^n$ ■

Proposition 4.6 The product of groups also forms a group, under the operation induced from those groups.

(R) If the operations of G_i are all addition, then $\prod_{i=1}^{n} G_i$ is said to be the **direct sum** of groups of G_i:

$$\bigoplus_{i=1}^{n} G_i = G_1 \oplus \cdots \oplus G_n$$

Note that $\bigoplus_{i=1}^{n} G_i$ is always abelian.

■ **Example 4.3**

1. The group $G = S_3 \times \mathbb{Z}_2$ is not abelian.
2. The group $G = (\mathbb{Z}_2 \times \mathbb{Z}_3, +) = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic
3. The **Klein 4-group** $V = \mathbb{Z}_2^2$ is **not** cyclic.

■

Theorem 4.3 The group $G = \mathbb{Z}_m \times \mathbb{Z}_n$ is **cyclic** iff $\gcd(m,n) = 1$.

Proof. Let $k = \text{lcm}(m,n) = mn/\gcd(m,n)$, then

$$k(a,b) = (ka,kb) = (0,0), \forall a \in \mathbb{Z}_m, b \in \mathbb{Z}_n,$$

since m and n both divide k. Thus $|g| \leq k, \forall g \in G$. Thus G is cyclic implies $k = mn$, i.e., $\gcd(m,n) = 1$

To show the converse, consider the element $(1,1) \in G$:

$$\begin{aligned} d(1,1) = (0,*), &\implies d = xm \\ d(1,1) = (*,0), &\implies d = ym \end{aligned}$$

thus $|(1,1)| = \text{lcm}(m,n) = mn$, i.e., G is cyclic. ■

Corollary 4.4 The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic iff m_i, m_j are mutually co-prime.

4.1.3. Generating Sets

Definition 4.3 [Generating Set] Let G be a group, S be a non-empty subset of G, the set

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

is a subgroup of G, called the subgroup of G generated by S. If $G = \langle S \rangle$, then S is the genreating set for G. ■

R The elements a_i do not have to be distinct, e..g, if $S = \{a,b\}$, then $a^3 b^{-1} a^{-1} \in \langle S \rangle$.

Proposition 4.7

$$\langle S \rangle = \bigcap_{\{H \mid S \subseteq H \leq G\}} H,$$

i.e., $\langle S \rangle$ is the smallest subgroup in G containing the subset S.

Proof. It's clear that $\langle S \rangle \supseteq \bigcap_{\{H | S \subseteq H \leq G\}} H$.

For any element a in $\langle S \rangle$, we find $a \in \bigcap_{\{H | S \subseteq H \leq G\}} H$, since $S \subseteq \bigcap_{\{H | S \subseteq H \leq G\}} H$.

■

When $S = \{a_1, \ldots, a_l\}$ is a finite set, we write

$$\langle S \rangle = \langle a_1, \ldots, a_l \rangle$$

■ **Example 4.4**

1. The set of cycles and the set of transpositions are two examples of generating sets for S_n
2. $S_n = \langle (12)(12\cdots n) \rangle$
3. $D_n = \langle r, s \rangle$, where r is the rotation by angle $\frac{2\pi}{n}$ in the anti-clock wise direction; and s is any reflection

■

A group is said to be **finitely generated** if there are finite number of elements $a_1, \ldots, a_l \in G$ s.t.

$$G = \langle a_1, \ldots, a_l \rangle$$

Every finite group is finitely generated.

Proposition 4.8 The group $(\mathbb{Q}, +)$ is not finitely generated.

Proof. Otherwise assume

$$\mathbb{Q} = \langle \frac{p_1}{q_1}, \ldots, \frac{p_l}{q_l} \rangle$$

Construct number $\frac{1}{q_1 \ldots q_l} \in \mathbb{Q}$, which is a contradiction. ■

Theorem 4.4 — Fundamental Theorem of Finitely Generated Abelian Groups. Any

finitely generated **abelian** group is isomorphic to

$$\prod_{i=1}^{m} \mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}^n$$

where $m \in \mathbb{N}^+, n, r_i \in \mathbb{N}$, and p_i are primes not necessarily distinct. This direct product is unique after re-arrangement.

■ **Example 4.5** The abelian groups of order $360 = 2^3 3^2 5$ up to isomorphism are

1. $\mathbb{Z}_2^3 \times \mathbb{Z}_3^2 \times \mathbb{Z}^5$
2. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2 \times \mathbb{Z}^5$
3. $\mathbb{Z}_8 \times \mathbb{Z}_3^2 \times \mathbb{Z}^5$
4. $\mathbb{Z}_2^3 \times \mathbb{Z}_9 \times \mathbb{Z}^5$
5. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}^5$
6. $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}^5$

The abelian groups of order 7^5 up to isomorphism are

1. $\mathbb{Z}_7^5$
2. $\mathbb{Z}_7 \times \mathbb{Z}_{2401}$
3. $\mathbb{Z}_{49} \times \mathbb{Z}_{343}$
4. $\mathbb{Z}_{16807}$

■

Chapter 5

Week4

5.1. Reviewing

Definition 5.1 [partition] Let S be a non-empty set. A **partition** P of S is a collection of subsets $\{S_i \mid i \in I\}$ of S such that

1. $S_i \neq \emptyset$ for all $i \in I$
2. $S_i \bigcap S_j = \emptyset$ whenever $i \neq j$
3. $\bigcup_{i \in I} S_i = S$

We also say P is a sub-division of S into a **disjoint union** of non-empty subsets, denoted as $S = \sqcup_{i \in I} S_i$ ∎

Definition 5.2 [Equivalence Relation] An **equivalence relation** on S is a relation $\sim$ such that

1. Reflexive: $a \sim a$ for all $a \in S$
2. Symmetric: if $a \sim b$, then $b \sim a$
3. Transitive: if $a \sim b$ and $b \sim c$, then $a \sim c$.

∎

Partition and equivalence relation are essentially two equivalent concepts.

1. Given partition $\{S_i \mid i \in I\}$ of S, we define $a \sim b$ whenever $a, b \in S_i$ for some $i \in I$.
2. Suppose there is an equivalence relation $\sim$ on S, for each $a \in S$, we define the

equivalence class with the representative a, i.e., partition as:

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

- Non-empty: since $a \sim a$, $a \in C_a$, i.e., C_a is non-empty.
- $\bigcup_{a \in S} C_a = S$
- disjoint: we show that $C_a \bigcap C_b \neq \emptyset$ implies $C_a = C_b$:

  Suppose $c \in C_a \bigcap C_b$, we imply $a \sim b$. Thus for any $d \in C_a$, $d \sim b$, i.e., $C_a \subseteq C_b$. Similarly, $C_a \supset C_b$.

R If $b \in C_a$, then $C_b = C_a$, i.e., **any eleemebt in an equivalence class can be its representative**.

Proposition 5.1 Any permutation $\sigma \in S_n$ is a product of disjoint cycles.

Proof. Let $\sigma \in S_n$ be an permutation on $X = \{1, \ldots, n\}$. For any $a, b \in X$, define an equivalence relation

$$a \sim b \text{ whenever } b = \sigma^k(a), \text{ for some } k \in \mathbb{Z}$$

Thus X is paritioned into disjoint union of equivalence classes:

$$X = O_1 \sqcup Q_2 \sqcup \cdots \sqcup O_m,$$

here O_j's are called orbits of σ. For each $j \in \{', \ldots, m\}$, construct $\mu_j \in S_n$:

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

These μ_j are mutually disjoint cycles, and thus $\sigma = \mu_1 \cdots \mu_m$. ■

5.1.1. Theorem of Lagrange

Let G be a group and $H \leq G$. We are interested in the size of H compared with G.

Proposition 5.2 For any $a, b \in G$, define a relation $\sim_L$ on G:

$$a \sim_L b \text{ whenever } b = ah \text{ for some } h \in H, \text{ i.e., } a^{-1}b \in H$$

The operator $\sim_L$ is an equivalence relation.

Thus the group G is partitioned into a disjoint union of equivalence classes w.r.t. $\sim_L$. We call these equivalence classes the **left cosets** of H in G, and each has form $aH = \{ah \mid h \in H\}$. Every $a \in G$ is a representative of the left coset aH.

Also, we define $\sim_R$ as:

$$a \sim_R b \text{whenever } b = ha \text{ for some } h \in H$$

and $Hb = \{hb \mid h \in H\}$.

■ **Example 5.1** Let $G = (\mathbb{Z}, +)$ and $H = 3\mathbb{Z} \leq G$. The left cosets of H in G are:

$$3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$$

The coset representatives are generally not unique. ■

In general, if $n \in \mathbb{N}^+$, the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are:

$$i + n\mathbb{Z}, \quad i = 0, \ldots, n-1$$

Definition 5.3 Let G be a group, and $H \leq G$. Denote the collection of the left cosets of H in G by $[G : H]$. We call the size of $[G : H]$ the **index** of H in G, denoted as $|G : H|$. ■

R The number of left cosets and right cosets are always equal to each other, if finite.

■ **Example 5.2** Let $G = \mathsf{GL}(n,\mathbb{R})$, and

$$H = \mathsf{GL}^+(n,\mathbb{R}) := \{h \in G \mid \det(h) > 0\} \leq G.$$

Take $a = \mathrm{diag}(-1,1,\ldots,1) \in G$ and thus $\det(a) = -1$. Take $g \in G$, then

1. If $\det(g) > 0$, then $g \in H$
2. If $\det(g) < 0$, then $\det(a^{-1}g) > 0$, i.e., $g \in aH$

Thus $[G : H] = \{H, aH\}$ and $|G : H| = 2$. Note that both G and H are infinite, but $|G : H|$ are finite. ■

■ **Example 5.3** Let $G = \mathsf{GL}(n,\mathbb{R})$ and $H = \mathsf{SL}(n,\mathbb{R})$. For each $x \in \mathbb{R}^\#$, take $a_x = \mathrm{diag}(x,1,\ldots,1) \in G$ and $\det(a_x) = x$. Thus for each $g \in G$,

$$g = a_{\det(g)} \left[a_{\det(g)}^{-1} g \right] \in a_{\det(g)} H$$

Moreover, we show that the constructed cosets are non-trivial:

$$a_x H \bigcap a_y H = \emptyset, \forall x, y \in \mathbb{R}^\#$$

and therefore $G = \sqcup_{x \in \mathbb{R}^\#} a_x H$, and $|G : H|$ is infinite. ■

Proposition 5.3 For the additive subgroup $\mathbb{Z} < \mathbb{R}$, we have

$$\mathbb{R} = \sqcup_{t \in [0,1)} (t + \mathbb{Z})$$

Proof. For the subgroup $H := \mathbb{Z}$, construct left cosets tH for $t \in [0,1)$. Thus for $\forall h_1 \in t_1 H$ and $h_2 \in t_2 H$ with distinct t_1 and t_2, we have

$$h_1 = t_1 + z_1 \neq t_2 + z_2, \quad h_2 = t_2 + z_3 \neq t_1 + z_4$$

Thus tH's are disjoint. Moreover, for $\forall x \in \mathbb{R}$, $t_x := x - \lceil x \rceil$, and thus $x \in t_x H$. ■

Proposition 5.4 For vector subspace $W \subseteq V$, consider the subgroup $(W,+) \leq (V,+)$. The set of cosets are the translations $v+W$, $v \in V$. Let $W' \subseteq V$ be a subspace complementary to W such that

1. $\dim(W) + \dim(W') = \dim(V)$
2. $W \bigcap W' = \{0\}$

Show that $V = \sqcup_{v \in W'}(v+W)$.

■ **Example 5.4** Consider the dihedral group D_n, we have

$$D_n = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$$

Thus we have $D_n = \langle r \rangle \sqcup \langle r \rangle s$. ■

Question,

■ **Example 5.5** Consider S_n with its subgroup A_n, we have $S_n = A_n \sqcup \tau A_n$ ■

■ **Example 5.6** Recall that $S_3 = \langle \rho, \mu \rangle$ with $\rho = (123)$ and $\mu = (12)$. For the cyclic subgroup $H = \langle \mu \rangle$, we have $[S_3 : H] = \{H, \rho H, \rho^2 H\}$ ■

Theorem 5.1 Let G be a finite group and $H \leq G$, then $|G:H| = |G|/|H|$

Proof. Suppose $G = H \sqcup a_1 H \sqcup \cdots \sqcup a_m H$. It suffces to show $|a_k H| = |H|$ for $k \in \{1, \ldots, m\}$.

Suppose $H = \{h_1, \ldots, h_n\}$, then immediately $|a_k H| = |\bigcup_{i=1}^n \{a_k h_i\}| \leq n$. For distinct $h_{i,j} \in H$, $a_k h_i = a_k h_j$ implies $h_i = h_j$, contradiciton. ■

This theorem also works for right cosets.

Proposition 5.5 Let G be a group and $H \leq G$ s.t.

$$G = H \sqcup a_1 H \sqcup a_2 H \sqcup \cdots \sqcup a_m H,$$

show that $G = H \sqcup H a_1^{-1} \sqcup H a_2^{-1} \sqcup \cdots \sqcup H a_m^{-1}$.

Proof. It's clear that $H, Ha_1^{-1}, \ldots, Ha_m^{-1}$ are disjoint. Also, for $\forall g \in G$, consider g^{-1}:

$$g^{-1} = a_i h \implies g = h^{-1} a_i^{-1} \in Ha_i^{-1}$$

■

Proposition 5.6 Let G be a finite group and $g \in G$, then $|g| \mid |G|$.

Proof. Since $|g| = |\langle g \rangle|$ ■

Proposition 5.7 Let G be a finite group of prime order, then G is cyclic.

Proof. Let $p = |G| \geq 2$. There exists non-trivial element a s.t. $|a|$ divides p, and $|a| \neq 1$, i.e., $|a| = p$. ■

Proposition 5.8 Let G be a finite group. For each $g \in G$, we have

$$g^{|G|} = e$$

Proof. SInce $|g|$ divides $|G|$, there exists k s.t.

$$g^{|G|} = (g^{|g|})^k = e$$

■

Then we give a generalization of cosets:

Definition 5.4 [Product of H by K] For a group G and $H, K \subseteq G$, the **product** of H by K is

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

■

Note that $(HK)L = H(KL), \forall H, K, L \subseteq G$

If $H \leq G$, it's clear that $HH = H$; the converse is not true in general, e.g., $H = \{\mathrm{id}, (12)\}$ and $G = S_3$.

Theorem 5.2 Let G be a group and $H, G \leq G$ be finite, then

$$|HK| = \frac{|H||K|}{|H \bigcap K|}$$

Proof. It suffices to show $|H||K| = |HK||H \bigcap K|$, e.g., construct a map $\phi : H \times K \mapsto HK$, it suffices to show ϕ is $|H \bigcap K|$-to-1 map.

- For $h_1, h_2 \in H$ and $k_1, k_2 \in K$, if the output of the mapping is the same,

$$h_1 k_1 = h_2 k_2 \implies h_2^{-1} h_1 = k_2 k_1^{-1} := d \in H \bigcap K$$

  and therefore $h_2 = h_1 d^{-1}$ and $k_2 = d k_1$.

- On the other hand, for any $h \in H, k \in K, d \in H \bigcup K$, if $h' = h d^{-1}$ and $k' = dk$, we find $h'k' = hk$.

■

question.

Theorem 5.3 Let G be a group and $H, K \leq G$. Then HK is a group iff $HK = KH$

Proof. Let $h \in H, k \in K$

Necessity. $kh = (h^{-1}k^{-1})^{-1} \in HK$, i.e., $KH \subseteq HK$. On the other hand, $(hk)^{-1} \in HK$ implies $(hk)^{-1} := h_1 k_1$, i.e., $hk = k_1^{-1} h_1^{-1} \in KH$.

Sufficiency. For any $h_1 k_1, h_2 k_2 \in HK$, we have

$$(h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} \in HKKH = HKHK = HHKK = HK.$$

■

Chapter 6

Week5

6.1. Monday

Let G be a finite group with $H \leq G$. Then G can be partitioned into the left cosets or the right cosets of H. However, the left cosets and the right cosets are usually different.

■ **Example 6.1** Let $G = S_3$ and $H = \{(), (12)\}$, it is eaily seen that

$$G = H \sqcup (13)H \sqcup (23)H = H \sqcup H(13) \sqcup H(23)$$

However, we see that

$$(13)H \neq H(13), \quad (23)H \neq H(23)$$

We are interested in the case when the left coset of H and the right coset of H are always the same.

■

Definition 6.1 [normal subgroup] Let G be a group. A subgroup $H \leq G$ is **normal** if

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

We denote this by $H \trianglelefteq G$ and $H \triangleleft G$ when $H < G$. ■

Normal subgroups have several equivalent definitions:

Theorem 6.1 Let G be a group and $H \leq G$. The following statements are equivalent:

1. $H \trianglelefteq G$
2. $a^{-1}Ha \subseteq H$, for $\forall a \in G, h \in H$
3. $a^{-1}Ha = H$, for $\forall a \in G$.

Proof. The non-trivial case is (2) implies (3). Since (2) holds for all $a \in G$, it holds for a^{-1}, i.e.,

$$(a^{-1})^{-1}Ha^{-1} \subseteq H \implies aHa^{-1} \subseteq H \implies H \subseteq a^{-1}Ha$$

■

■ **Example 6.2**

1. Any group G contains the trivial normal subgroups, i.e. ,1 and G
2. Let $G = S_3, N = \{(), (123), (132)\}, H_1 = \{(), (12)\}, H_2 = \{(), (13)\}, H_3 = \{(), (23)\}$, then $N \triangleleft G$ but H_i's are not.
3. Let $n \in \mathbb{N}^+$, then $\mathrm{SL}(n, \mathbb{R}) \triangleleft \mathrm{GL}(n, \mathbb{R})$
4. Let $n \in \mathbb{N}^+$, then $A_n \triangleleft S_n$. (question)
5. Let H, K be groups and $G = H \times K$. Then $H \times 1$ and $1 \times K$ are normal subgroups of G.

■

Proposition 6.1 Let i, j, k be such that

$$i^2 = j^2 = k^2 = ijk = -1 \in \mathbb{R},$$

show that the **quaternion group**

$$Q_8 = \langle i, j, k \rangle$$

has order 8, and every its subgroup is normal.

Proof. Since $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$, any element from the set Q_8 can be written as the form $\pm i^{m_1} j^{m_2} k^{m_3}$ for $m_i \in \mathbb{N}$ with $m_1 + m_2 + m_3 = 1$. Hence, the set Q_8

has at most 8 elements, i.e., the order should be no more than 8. Furthermore, note that $\pm 1, \pm i, \pm j, \pm k \in Q_8$, which means the $|Q_8| = 8$.

Also, due to Lagrange's theorem, every subgroup can only have order 1,2,4,8, and the subgroup with order 1 or 8 are trivial normal subgroups; the subgroup with order 4 has index 2, i.e., is normal. After computation, we find the only one subgroup with order 2 is $\{1, -1\}$, which is normal obviously. ■

R Every subgroup of an abelian group is normal, but the converse is not true (e.g., see example above). In general, a group G is **Dedekind** if every its subgroups is normal; and if G is non-abelian but with all normal subgroups, then G is **Hamiltonian group**.

Theorem 6.2 Let G be a group with $H \trianglelefteq G$, then the set $[G : H]$ forms a **quotient group** (factor group) G/H under the operation defined as:

$$(aH)(bH) := (ab)H, \qquad \forall a, b \in G$$

Note that the proof is incomplete, we need to check the well-defineness of operation.

Proof. To examine that G/H is indeed a group:

- $(ab)H$ is also a left cosets
- associative
- H is identity
- $a^{-1}H$ is inverse

■

■ **Example 6.3** For $n \in \mathbb{N}^+$, the abelian group $\mathbb{Z}$ contains a normal subgroup $n\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n. ■

Proposition 6.2 Let G be a group, then the **center**

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

forms a normal subgroup of G.

Question for Proposition 3.5

Proof. First, show that $z_1, z_2 \in Z(G)$ implies $z_1 z_2^{-1} \in Z(G)$. Next, show that $g^{-1}zg = z$ for all $g \in G$ and $z \in Z(G)$. ■

■ **Example 6.4**

1. Let G be an abelian group, then $Z(G) = G$, i.e., $Z(G)$ is essentially the largest abelian subgroup of G
2. Let $n \geq 3$ be an integer, then $Z(S_n) = 1$.
3. Let $n \geq 3$ be an integer, then $Z(\mathbb{Z}_n \times S_n) = \mathbb{Z}_n \times 1$.
4. $$Z(\mathrm{GL}(2,\mathbb{R})) = \{\mathrm{diag}(a,b) : ab \neq 0\}$$

■

6.1.1. Derived subgroups

Definition 6.2 [derived subgroup] Let G be a group and $a, b \in G$. The **commutator** of a, b is:

$$[a,b] := a^{-1}b^{-1}ab$$

The **derived subgroup** (**commutator subgroup**) of G is

$$G' := \langle [a,b] | a,b \in G \rangle$$

■

Proposition 6.3 The G'-coset partition defines an equivalence relation on G such that $ab \sim_{G'} ba$ for $\forall G$.

Proof. First show that $x \sim_{G'} y$ iff $xy^{-1} \in G'$.

Then it's trivial that $aba^{-1}b^{-1} \in G'$. ■

Note that the L-coset parititon $a \sim_L b$ means that $aH = bH$.

R If $G' \triangleleft G$, then G/G' is an abelian group. Note that G' is normal since

$$a^{-1}ha = [a, h^{-1}]h \in G'$$

Theorem 6.3 Let G be a group, then $G' \triangleleft G$ and G/G' is abelian.

Corollary 6.1 Let G be a group such that $G'' = 1$, then G is abelian

Proof. $\{\{a\} \mid a \in G\}$ is abelian implies G is abelian. ■

R The derived subgroup is the smallest normal subgraoup such that the quotient group G/G' is abelian, i.e., any quotient group G/H is abelian iff H contains G'.

Theorem 6.4 Let G be a group and $H \triangleleft G$, then G/H is abelian iff $G' \leq H$.

Proof. Necessity. Since G/H is abelian, we have

$$abH = baH \implies abh_1 = bah_2 \implies [a,b] = h_2h_1' \in H \implies \langle [a,b] | a,b \in G \rangle \in H$$

Suffiency. Note that

$$a^{-1}b^{-1}ab \in G' \subseteq H \implies a^{-1}b^{-1}ab = h \implies ab \sim_H ba, \forall a,b \in G$$

■

Theorem 6.5 Let $n \in \mathbb{N}^+$, then $A_n = S_n'$ (A_n denotes the group of even permutations). Moreover, when $n \geq 5$, $A_n' = A_n$.

Recall that a permutation is called an even permutation if it can be written as a product of an even number of transpositions.

Proof. Note that $S_n / A_n = A_n \sqcup \tau A_n$, and therefore abelian. Thus $A_n \geq S_n'$. It suffices to show $S_n' \geq A_n$, Note that

$$A_n = \langle (12i) | i = 3, \ldots, n \rangle$$

Therefore $(12i) = (12)^{-1}(1i)^{-1}(12)(1i) \in S_n'$ implies $A_n \leq S_n'$.

When $n \geq 5$, note that $A_n' \leq A_n$. On the other hand,

$$(12i) = (1a2)^{-1}(1bi)^{-1}(1a2)(1bi) \in A_n' \implies A_n \leq A_n'$$

■

R In general, a group satisfying $G' = G$ is perfect. The alternating groups are concrete examples of perfect groups.

Proposition 6.4 The group $\mathrm{SL}(2, \mathbb{R})$ is perfect.

Proof. Note that any element is a product of $\begin{pmatrix} 1 & x \\ 0 & x \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$ and these two basis can be written as the form $[a, b]$.,e.g.,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = [\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (\sqrt{2})^{-1} & 0 \\ 0 & \sqrt{2} \end{pmatrix}]$$

■

Definition 6.3 [Simple] Every group G contains the trivial normal subgroups 1 and G. If these are only normal subgroups contained in G, then we say G is **simple**. ■

Definition 6.4 [Conjugacy Class] Let G be a group and $a,b \in G$. If there exists $g \in G$ such that $g^{-1}ag = b$, then a,b are **conjugate**, and b is a conjugate of a. The conjugacy class with representative a is a collectio nof all conjugates of a:

$$\mathrm{Cl}(a) = \{g^{-1}ag \mid g \in G\}$$

■

Proposition 6.5 The conjugacy class defines an equivalence relation on G; and $\mathrm{Cl}(z) = \{z\}$ for each $z \in G$.

Theorem 6.6 Let G be a finite group with r disjoint conjugacy classes of size $c_1,\ldots,c_r \geq 2$. Let $|Z(G)| = c_0$, then

$$|G| = \sum_{i=0}^{r} c_i$$

Proof. Note that $x \in Cl(z)$ with $z \in Z(G)$ iff $x = z$. Hence the conjugacy class with only one element must be of the form $\{z\}$, $z \in Z(G)$. Thererfore,

$$|G| = \sum_{i=0}^{r} c_i$$

■

Theorem 6.7 The alternating group A_5 is simple.

Solution. Let $\sigma \in N \triangleleft A_5$ be non-identity, then if we can show that $N = A_5$, which is a contradiction, then we show that A_5 is simple.

Note that A_5 is generated by the $3-$cycles, i.e., every element σ of A_n can be written as

$$\sigma = C_1 C_2 \cdots C_k,$$

with C_i to be 3-cycles.

Note that N contains a non-trivial even permutation σ, which must be of the form $(abcde)$ or $(ab)(cd)$ or (abc).

- When $\sigma = (abcde)$, let $\alpha = (ab)(cd)$. then N also contains:

$$\alpha\sigma\alpha^{-1} = (ab)(cd)(abcde)(ab)(cd) = (adceb)$$

  and therefore contains

$$\sigma\sigma^{-1} = (aec)$$

- When $\sigma = (ab)(cd)$, let $\beta = (abe)$, then N also contains

$$\sigma' = \beta\sigma\beta^{-1} = (becd)$$

  and therefore contains

$$\sigma\sigma^{-1} = (abe)$$

If N contains a signle 3-cycles, since 3-cycles are mutually conjugate, N will contain any other 3-cycles. Therefore $N = A$, which is a contradiction. ■

Solution 2. Let N be a normal subgroup of A_5, then it is a union of some of the conjugacy classes of A_5. Since the order of N must divide 60, a short calculation shows that no union of some of these conjugacy classes that includes $\{e\}$ has order a divisor of 60, unless $A_5 = \{e\}$ or A_5. ■

Theorem 6.8 Let $n \geq 5$, then A_n is simple,and A_n is the only non-trivial proper normal subgroup of S_n.

It suffices to show that $1 < H \triangleleft S_n$ implies $H = A_n$.

6.2. Thursday

6.2.1. Homomorphisms

Definition 6.5 [Homomorphisms] Let $G = (G, *)$ and $\hat{G} = (\hat{G}, \odot)$, then a **homomorphisms** is a map $\phi : G \mapsto \hat{G}$ such that

$$\phi(a * b) = \phi(a) \bigodot \phi(b), \quad \forall a, b \in G$$

If ϕ is a **bijection**, then ϕ is said to be a **isomorphism**. We denote $G \cong^{\phi} \hat{G}$. ■

R

- homomorphisms is not necessarily injective or surjective.
- The isomorphism from G to $\hat{G}$ is not unique;
- isomorphism admits symmetry, i.e., $G \cong \hat{G}$ iff $\hat{G} \cong G$.

■ **Example 6.5**

- Let V, W be vector spaces over $\mathbb{R}$ (or $\mathbb{C}$), then ant linear transformation $\phi : V \mapsto W$ is a **homomorphism** $\phi : (V, +) \mapsto (W, +)$.

  $$\phi(\lambda \boldsymbol{u} + \mu \boldsymbol{v}) = \lambda \phi(\boldsymbol{u}) + \mu(\boldsymbol{v}),$$

  and let $\lambda = \mu = 1$, we derive the homomorphismness.

- The determinant $\det : \mathrm{GL}(n, \mathbb{R}) \mapsto \mathbb{R}^{\#} := \mathbb{R} \setminus \{0\}$ is a group homomorphism:

  $$\phi : g \mapsto \det(g) \implies \phi(gh) = \phi(g) * \phi(h)$$

- For any $n \in \mathbb{Z}^+$, we have $n\mathbb{Z} \leq \mathbb{Z}$. Define the map $\phi : n\mathbb{Z} \mapsto \mathbb{Z}$ as $nk \mapsto k$, then

$$\phi(nh + nk) = \phi(n(h + k)) = h + k = \phi(nh) + \phi(nk)$$

  Then we need to show it is bijection. Each element on the range has its input, i.e., surjective. Also, take $\phi(nh) = \phi(nk)$, then $n = k$, i.e., injective.

  For $n > 1$, we have $n\mathbb{Z} < \mathbb{Z}$, i.e., a proper subgroup can be isomorphic to its parent group.

- The map $\mathbb{Z} \mapsto \mathbb{Z}$ defined by $k \mapsto nk$ is a homomorphism but not isomorphism unless $n = \pm 1$:

$$\phi(h + k) = n(h + k) = \phi(h) + \phi(k)$$

- The remainder map $\phi : \mathbb{Z} \mapsto \mathbb{Z}_n$ is defined as mapping k to its remainder $\bar{k}$divided by n. It is a surjective homomorphism: $\bar{k} \in \{0, \ldots, n-1\}$ always has its input

- The map ϕ defined as $k \mapsto k + 1$ is not a homomorphism:

$$\phi(0) = 1, \phi(1) = 2, \phi(0 + 1) = 2$$

■

Proposition 6.6 The group

$$G = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} | \theta \in \mathbb{R} \right\}$$

is isomorphic to $H = \{z \in \mathbb{C} || z| = 1\}$ under the map

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mapsto e^{i\theta}$$

Proof. First is to check the well-defineness of ϕ. i.e., different expression of the same

input leads to the same output:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{pmatrix} \implies \theta' = \theta + 2n\pi \implies e^{i\theta} = e^{i\theta'}$$

Then check homomorphism and bijection.

■

Proposition 6.7 Let $\phi : G \mapsto H$ be a group homomorphism, then

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = [\phi(g)]^{-1}$ for $\forall g \in G$
3. $\phi(g^n) = [\phi(g)]^n$ for $\forall g \in G$ and $n \in \mathbb{Z}$

Proof.

$$H \ni \phi(e_G) = \phi(e_G)\phi(e_G) \implies e_H = \phi(e_G)$$

■

Definition 6.6 [image] Let $\phi : G \mapsto H$ be a group homomorphism, then the **image** of ϕ is

$$\text{Im } \phi = \phi(G) = \{\phi(g) \mid g \in G\}$$

The **kernel** of ϕ is

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}$$

In particular, if $\ker \phi = G$, then we say the homomorphism is **trivial**. ■

R im $\phi \leq H$ and ker $G \triangleleft G$.

Proposition 6.8 Let ϕ defined above, then im $\phi \leq H$ and ker $\phi \leq G$

Proof.

$$a, b \in \text{im } \phi \implies ab^{-1} = \phi(g)[\phi(h)]^{-1} = \phi(gh^{-1}) \in \text{im } \phi$$

■

Proposition 6.9 A group homomorphism $\phi : G \mapsto H$ is injective iff $\ker \phi = \{e_G\}$

Proof. Necessity.

Assume $a \neq e_G$ and $a \in \ker \phi$, then

$$\phi(g) = \phi(g)e_H = \phi(g)\phi(a) = \phi(g * a),$$

but $g \neq g * a$, which is a contradiction.

Sufficiency.

For any $\phi(g) = \phi(h)$, it suffices to show $g = h$:

$$\phi(g)[\phi(h)]^{-1} = e_H \implies \phi(gh^{-1}) = e_H \implies gh^{-1} = e_G \implies g = h.$$

■

Proposition 6.10 Let G, H be isomorphic groups, if G is cyclic, then so is H

Proof. Let $G = \langle g_0 \rangle \cong H$ and $\phi : G \mapsto H$. Define $h_0 = \phi(g_0)$. Take $h \in H$, there exists $n \in \mathbb{Z}$ s.t.

$$h = \phi(g_0^n) = [\phi(g_0)]^n := h_0^n$$

It follows that $H \subseteq \langle h_0 \rangle \subseteq H$, i.e., $H = \langle h_0 \rangle$ ■

Proposition 6.11 Let G, H be isomorphic groups, if G is abelian, then so is H

Proof. For any $h_1, h_2 \in H$, there exists $g_1, g_2 \in G$ such that

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_2)\phi(g_1) = h_2h_1.$$

■

Note that D_6 is not isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$, since D_6 is not abelian.

R These two propositions above still remains true if replacing isomorphism by a surjective homomorphism.

Proposition 6.12 The restriction of a homomorphism $\phi : G \mapsto \hat{G}$ to a subgroup $H \leq G$ gives a homomorphism $\phi|_H : H \mapsto \hat{G}$ as well.

Proof. $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$ for $g_1, g_2 \in H$ ■

Proposition 6.13 Let G, H be groups s.t. $G \cong_\phi H$, then $|\phi(g)| = |g|$ for each $g \in G$.

Proof. Note that $n = |g|$ implies

$$[\phi(g)]^n = e_H,$$

i.e., $|\phi(g)| \leq n$. On the other hand, assume we can take a positive integer $m < n$ s.t.

$$[\phi(g)]^m = e_H \implies \phi(g^m) = e_H,$$

with $g^m \neq e_G$, which implies ϕ is not one-to-one, which is a contradiction. ■

6.2.2. Classification of cyclic groups

Proposition 6.14 Let r_1 denote the anti-clockwise rotation by $\frac{2\pi}{n}$, then $H = \langle r_1 \rangle \leq D_n$. Then $H \cong \mathbb{Z}_n$.

Proof. Define $\phi : H \mapsto \mathbb{Z}_n$ with $\phi(r_1^k) = \bar{k}$, $k \in \mathbb{Z}$

- ϕ is well-defined:

  $$r_1^{k_1} = r_1^{k_2} \implies k_2 = k_1 + nd,$$

  which is well-defined since $\overline{k_1 + nd} = \overline{k_1}$.

- ϕ is a homomorphism: for $i, j \in \{0, \ldots, n-1\}$

  $$\phi(r_1^i r_1^j) = \phi(r_1^{i+j}) = \overline{i+j} = i +_n j = \phi(r_1^i) +_n \phi(r_1^j)$$

- To show ϕ is a bijection. It suffices to show $\ker \phi = \{e_H\}$:

  $$\phi(r_1^i) = 0 \implies i = nd, d \in \mathbb{Z} \implies r_1^i = r_0$$

■

Theorem 6.9 Let G be a cyclic group, then

1. If $|G| = \infty$, then $G \cong \mathbb{Z}$
2. If $|G| = n$, then $G \cong \mathbb{Z}_n$

Proof. Define $\phi : G \mapsto \mathbb{Z}$ with $g_0^k \mapsto k$

First show the well-defineness of ϕ; then show ϕ is homomorphic:

$$\phi(g_0^m * g_0^n) = \phi(g_0^m) + \phi(g_0^n)$$

Then show that ϕ is bijection, i.e., $\ker \phi = \{e_G\}$.

For the second case, define the map $\phi : \mathbb{Z}_n \mapsto G$ with $k \mapsto g_0^k$:

Check the well-defineness, which is clear since the expresison for k is unique.

ϕ is homomorphism:

$$\phi(h +_n k) = \phi(\overline{h+k}) = g_0^{\overline{h+k}} = g_0^{h+k} = g_0^h g_0^k = \phi(h)\phi(k)$$

Then show that it is bijection. A one-to-one function from a finite set to itself is onto. Then check one-to-one mapping.

■

Corollary 6.2 Let $G, \hat{G}$ be cyclic groups of the same order, then $G \cong \hat{G}$.

6.2.3. Isomorphism Theorems

The first and seond theorem is required in exam. (can we apply the corresponding theorem in the exam?)

Theorem 6.10 — **The First Isomorphism Theorem.** Let $G \mapsto H$ be a **surjective** group homomorphism, then $\ker \phi \triangleleft G$ and $G/\ker \phi \cong \text{im } \phi$