

## Contents

1	Groups .....	2
1.1	Notation .....	2
1.2	Groups .....	2
1.3	Symmetric Groups .....	7
1.4	Cayley Tables .....	10
2	Subgroups .....	12
2.1	Subgroups .....	12
2.2	Alternating Groups .....	14
2.3	Orders of Elements .....	15
2.4	Cyclic Groups .....	17
2.5	Non-cyclic Groups .....	19
3	Normal Subgroups .....	20
3.1	Homomorphisms and Isomorphisms .....	20
3.2	Cosets and Lagrange's Theorem .....	21

# 1 Groups

## 1.1 Notation

1.  $\mathbb{N} = \{1, 2, \dots\}$
2.  $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$
3.  $\mathbb{Q} = \left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\right\}$
4.  $\mathbb{R}$  = real numbers
5.  $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$

For  $n \in \mathbb{N}$ ,  $\mathbb{Z}_n$  = integers modulo  $n = \{[0], \dots, [n-1]\}$  where  $[r] = \{z \in \mathbb{Z} : z \equiv r \pmod{n}\}$

We note that the set  $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$  has 2 operations  $+$ ,  $\cdot$ .

For  $n \in \mathbb{N}$ , an  $n \times n$  matrix over  $\mathbb{R}$  (or  $\mathbb{Q}$  or  $\mathbb{C}$ ) is an  $n \times n$  array

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

with  $a_{ij} \in \mathbb{R}$ .

Note we can also do  $+$ ,  $\cdot$ . For  $A, B \in M_n(\mathbb{R})$

$$A + B := [a_{ij} + b_{ij}] \quad A \cdot B := \left[ \sum_{k=1}^n a_{ik} b_{kj} \right]$$

## 1.2 Groups

### Definition 1.2.1

Let  $G$  be a set and  $*$  :  $G \times G \rightarrow G$ . We say  $G$  is a *group* if the following are satisfied:

1. Associativity: if  $a, b, c \in G$ , then  $a * (b * c) = (a * b) * c$
2. Identity: there is  $e \in G$  such that  $a * e = e * a = a$  for all  $a \in G$
3. Inverses: for all  $a \in G$ , there is  $a^{-1} \in G$  such that  $a * a^{-1} = a^{-1} * a = e$

### Definition 1.2.2

A group is called *abelian* if  $a * b = b * a$  for all  $a, b \in G$

### Exercise 1.2.1

Prove in the definition of a group, 1-sided identity and inverses are enough to have 2-sided identity and inverses

**Proposition 1.2.1**[previous exercise](#)

Suppose  $G$  is a set,  $*$  :  $G \times G \rightarrow G$  is associative. Suppose there is  $e \in G$  such that  $e * a = a$  for all  $a \in G$ . Further suppose that for every  $a \in G$ , there is  $a^{-1} \in G$  such that  $a^{-1} * a = e$ . Then for all  $a \in G$ ,

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

**Proof of 1:** Let  $a \in G$ , then

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

Multiplying on the left by  $a^{-1-1}$  gives

$$\begin{aligned} a^{-1-1} * a^{-1} * a * e &= a^{-1-1} * a^{-1} * a \\ \implies e * a * e &= e * a \\ \implies a * e &= a \end{aligned}$$

□

**Proof of 2:** Let  $a \in G$ , then

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

Again multiplying on the left by  $a^{-1-1}$  gives

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

□

**Proposition 1.2.2**

Let  $G$  be a group, let  $a \in G$ . Then

1. The group identity is unique
2. The inverse of  $a$  is unique

**Proof of 1:** Suppose  $e_1, e_2$  are both identities. Then

$$e_1 = e_1 * e_2 = e_2$$

□

**Proof of 2:** Suppose  $b_1, b_2$  are inverses of  $a$ . Then

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

□

**Example 1.2.1**

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$  are all abelian groups

**Example 1.2.2**

$(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$  are not groups as 0 has no inverse

**Example 1.2.3**

but  $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$  are abelian groups

**Definition 1.2.3**

For a set  $(S, \cdot)$  let  $S^* \subseteq S$  denote the set of all elements with inverses.

**Exercise 1.2.2**

what is  $\mathbb{Z}_n^*$ ?

**Example 1.2.4**

$(M_n(\mathbb{R}), +)$  is an abelian group.

**Example 1.2.5**

Consider  $(M_n(\mathbb{R}), \cdot)$  The identity matrix is  $\begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} \in M_n(\mathbb{R})$  However, since not all  $M \in M_n(\mathbb{R})$  have multiplicative inverses,  $(M_n(\mathbb{R}), \cdot)$  is not a group.

**Notation**

$\text{GL}_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : \det(M) \neq 0\}$

**Note**

If  $A, B \in \text{GL}_n(\mathbb{R})$ , then  $\det(AB) = \det(A)\det(B) \neq 0$  Thus  $AB \in \text{GL}_n(\mathbb{R})$ . The associativity of  $\text{GL}_n(\mathbb{R})$  inherits from  $M_n(\mathbb{R})$ . Also the identity matrix satisfies  $\det(I) = 1 \neq 0$  and thus  $I \in \text{GL}_n(\mathbb{R})$ . Finally, for  $M \in \text{GL}_n(\mathbb{R})$ , there exists  $M^{-1} \in M_n(\mathbb{R})$  such that  $MM^{-1} = I = M^{-1}M$  since  $\det(M^{-1}) = \frac{1}{\det(M)} \neq 0$ , we have  $M^{-1} \in \text{GL}_n(\mathbb{R})$ . Thus  $(\text{GL}_n(\mathbb{R}), \cdot)$  is a group, called the *general linear group of degree  $n$  over  $\mathbb{R}$*

**Note**

if  $n \geq 2$ , then  $\text{GL}_n(\mathbb{R})$  is not abelian.

**Exercise 1.2.3**

What is  $(\text{GL}_1(\mathbb{R}), \cdot)$ ?

**Example 1.2.6**

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

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

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

**Note**

One can show by induction that if  $G_1, \dots, G_n$  are groups, then  $G_1 \times \dots \times G_n$  is also a group.

**Notation**

Given a group  $G$  and  $g_1, g_2 \in G$ , we often denote  $g_1 * g_2$  by  $g_1 g_2$  and its identity by 1. Also the unique inverse of an element  $g \in G$  is denoted by  $g^{-1}$ . Also for  $n \in \mathbb{N}$ , we define  $g^n = g * g * \dots * g$  ( $n$ -times) and  $g^{-n} = (g^{-1})^n$ . Finally, we denote  $g^0 = 1$ .

**Proposition 1.2.3**

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.  $g^n g^m = g^{n+m}$  for all  $n, m \in \mathbb{Z}$
4.  $(g^n)^m = g^{nm}$  for all  $n, m \in \mathbb{Z}$

**Proof of 1:** Since

$$g^{-1}g = 1 = gg^{-1}$$

so  $g^{-1-1} = g$  □

**Proof of 2:**

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g1g^{-1} = 1$$

Similarly,

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

Thus  $(gh)^{-1} = h^{-1}g^{-1}$  □

**Proof of 3:** We proceed by considering cases:

1. if  $n = 0$  then

$$g^n g^m = g^0 g^m = 1g^m = g^m = g^{0+m} = g^{n+m}$$

2. if  $n > 0$ , we will proceed by induction on  $n$ . Case 1 establishes the base case. Let  $m \in \mathbb{Z}$ ,  $n \in \mathbb{Z}_{\geq 0}$ . Suppose that  $g^n g^m = g^{n+m}$  Then

$$g^{n+1}g^m = gg^n g^m = gg^{n+m} = g^{n+m+1}$$

3. if  $n < 0$ , then  $n = -k$  for some  $k \in \mathbb{N}$ . We have

$$g^k g^n g^m = g^{k+n} g^m = g^0 g^m = g^m$$

also

$$g^k g^{n+m} = g^{k+n+m} = g^m$$

Thus

$$g^k g^n g^m = g^k g^{n+m}$$

So

$$g^n g^m = g^{n+m}$$

as desired. □

**Proof of 4:** We proceed by considering cases:

1. if  $m = 0$ , then  $(g^n)^m = (g^n)^0 = 1 = g^0 = g^{n0} = g^{nm}$
2. if  $m > 0$ , then

$$(g^n)^m = \underbrace{g^n g^n \cdots g^n}_{m \text{ times}} = g^{nm}$$

3. if  $m < 0$ , then  $m = -k$  for some  $k \in \mathbb{N}$ . We will induct on  $k$ . For  $k = 1$  we see that  $(g^n)^{-1} = g^{-n}$  since

$$g^n g^{-n} = g^{n-n} = g^0 = 1$$

Suppose  $(g^n)^{-\ell} = g^{-n\ell}$  for all  $1 \leq \ell \leq k$ . Then

$$(g^n)^{-k-1} = (g^n)^{-k} (g^n)^{-1} = g^{-nk} g^{-n} = g^{-nk-n} = g^{-n(k+1)}$$
□

#### Exercise 1.2.4

prove 3,4

#### Warning

In general, it is not the case that if  $g, h \in G$  then  $(gh)^n = g^n h^n$ , this is not true unless  $G$  is abelian

**Proposition 1.2.4**

Let  $G$  be a group and  $g, h, f \in G$  Then

1. They satisfy the left and right cancellation. More precisely,
  - a. if  $gh = gf$  then  $h = f$
  - b. if  $hg = fg$  then  $h = f$
2. Given  $a, b \in G$  the equations  $ax = b$  and  $ya = b$  have unique solutions for  $x, y \in G$

**Proof of 1-a:** By left-multiplying by  $g^{-1}$ , we have

$$gh = gf \iff g^{-1}gh = g^{-1}gf \iff h = f$$

□

**Proof of 1-b:** similar to 1-a

□

**Proof of 2:** Let  $x = a^{-1}b$  then

$$ax = aa^{-1}b = b$$

If  $u$  is another solution, then  $au = b = ax$ . By 1-a,  $u = x$ . Similarly,  $y = ba^{-1}$  is the unique solution of  $ya = b$

□

**1.3 Symmetric Groups****Definition 1.3.1**

Given a non-empty set  $L$ , a *permutation* of  $L$  is a bijection from  $L$  to  $L$ . The set of all permutations of  $L$  is denoted by  $S_L$

**Example 1.3.1**

Consider the set  $L = \{1, 2, 3\}$  which has the following different permutations

$$\begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}$$

Where  $\begin{pmatrix} 123 \\ 123 \end{pmatrix}$  denotes the bijection

$$\sigma : \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$$

$$\sigma(1) = 1, \sigma(2) = 2, \sigma(3) = 3$$

**Notation**

For  $n \in \mathbb{N}$  we denote by  $S_n = S_{\{1, 2, \dots, n\}}$  the set of all permutations of  $\{1, 2, \dots, n\}$ . We have seen that the order of  $S_3 = 3! = 6$ . To consider the general  $S_n$ , we note that for a permutation  $\sigma \in S_n$ , there are  $n$  choices for  $\sigma(1)$ ,  $n - 1$  choices for  $\sigma(2)$ , ..., 1 choice for  $\sigma(n)$ . Thus

**Proposition 1.3.1**

$$|S_n| = n!$$

**Note**

For Möbius quizzes, use “9 dots” for permutations.

**Remark**

Given  $\sigma, \tau \in S_n$  we can compose them to get a new element  $\sigma\tau$ , where  $\sigma\tau = \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  given by  $x \mapsto \sigma(\tau(x))$ . Since both  $\sigma, \tau$  are bijections,  $\sigma\tau \in S_n$ .

**Example 1.3.2**

Compute  $\sigma\tau$  and  $\tau\sigma$  if

$$\sigma = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1234 \\ 2431 \end{pmatrix}$$

Then  $\sigma\tau(1) = \sigma(2) = 4, \dots$  Then  $\sigma\tau = \begin{pmatrix} 1234 \\ 4213 \end{pmatrix}$ , and  $\tau\sigma = \begin{pmatrix} 1234 \\ 3124 \end{pmatrix}$

We note that  $\sigma\tau \neq \tau\sigma$

**Note**

For any  $\sigma, \tau \in S_n$  we have that  $\tau\sigma, \sigma\tau \in S_n$  but  $\sigma\tau \neq \tau\sigma$  in general on the other hand, for any  $\sigma, \tau, \mu$  we have  $\sigma(\tau\mu) = (\sigma\tau)\mu$ . Also note the *identity permutation*  $\varepsilon \in S_n$  is defined as

$$\varepsilon = \begin{pmatrix} 12 \cdots n \\ 12 \cdots n \end{pmatrix}$$

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

Finally, for  $\sigma \in S_n$ , since it is a bijection, there is a unique bijection  $\sigma^{-1} \in S_n$  called the *inverse permutation* of  $\sigma$  such that for all  $x, y \in \{1, 2, \dots, n\}$

$$\sigma^{-1}(x) = y \iff \sigma(y) = x$$

It follows that

$$\sigma(\sigma^{-1}(x)) = \sigma(y) = x$$

and

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

i.e we have

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = \varepsilon$$



**Example 1.3.3**

$$\sigma = \begin{pmatrix} 12345 \\ 45123 \end{pmatrix}$$

Then

$$\sigma^{-1} = \begin{pmatrix} 12345 \\ 34512 \end{pmatrix}$$

From the above we have

**Proposition 1.3.2**

$(S_n, \circ)$  is a group, called the *symmetric group of degree  $n$*

**Exercise 1.3.1**

Write down all rotations and reflections that fix an equilateral triangle. Then check why it is the “same” as  $S_3$

**Example 1.3.4**

Consider

$$\sigma = \begin{pmatrix} 123456789(10) \\ 317694258(10) \end{pmatrix} \in S_{10}$$

We note that  $1 \rightarrow 3 \rightarrow 7 \rightarrow 2 \rightarrow 1$  and  $4 \rightarrow 6 \rightarrow 4$  and  $5 \rightarrow 9 \rightarrow 8$  and  $10 \rightarrow 10$ . Thus  $\sigma$  can be *decomposed* into one 4-cycle (1372), one 2-cycle (46), and one 3-cycle (598) and one 1-cycle (10) (we usually do not write 1-cycles). Note that these cycles are *pairwise disjoint* and we have

$$\sigma = (1372)(46)(598)$$

We can also write  $\sigma = (46)(598)(1372)$ , or  $\sigma = (64)(985)(7213)$

**Theorem 1.3.3****Cycle Decomposition**

If Given  $\sigma \in S_n$  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.

**Proof:** See bonus 1. □

**Convention**

Every permutation of  $S_n$  can be regarded as a permutation in  $S_{n+1}$  by fixing the number  $n+1$ , thus

$$S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq S_{n+1}$$

## 1.4 Cayley Tables

### Definition 1.4.1

For a finite group  $G$ , defining its operation by means of a table is sometimes convenient. Given  $x, y \in G$ , the product  $xy$  is the entry of the table in the row corresponding to  $x$  and the column corresponding to  $y$ , such a table is a *Cayley table*.

### Remark

By cancellation, the entries in each row or column of a Cayley table are all distinct

### Example 1.4.1

Consider  $(\mathbb{Z}_2, +)$  its Cayley table is

$\mathbb{Z}_2$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

### Example 1.4.2

Consider the group  $\mathbb{Z}^* = \{1, -1\}$ . Its Cayley table is

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

### Note

If we replace 1 by [0] and -1 by [1] the Cayley tables of  $\mathbb{Z}^*$  and  $\mathbb{Z}_2$  become the same. In this case, we say  $\mathbb{Z}^*$  and  $\mathbb{Z}_2$  are *isomorphic* denoted by

$$\mathbb{Z}^* \cong \mathbb{Z}_2$$

**Example 1.4.3**

For  $n \in \mathbb{N}$ , the *cyclic group of order  $n$*  is defined by

$$C_n = \{1, a, a^2, \dots, a^{n-1}\} \text{ with } a^n = 1 \text{ and } 1, a, \dots, a^{n-1} \text{ are distinct}$$

The Cayley table of  $C_n$  is as follows

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

**Proposition 1.4.1**

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  $G \cong K_4 \cong C_2 \times C_2$

**Proof of 1:** obviously □

**Proof of 2:** If  $|G| = 2$  then  $G = \{1, g\}$  with  $g \neq 1$ . Then  $g^2 = g$  or  $g^2 = 1$ . We note that if  $g^2 = g$ , then  $g = 1$  contradiction. thus  $g^2 = 1$ . Thus the Cayley table is as follows

$G$	1	$g$
1	1	$g$
$g$	$g$	1

which is the same as  $C_2$  □

**Proof of 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  $g1 = g, gh = 1$ . Since all entries in this row are distinct, we have  $g^2 = h$ . Similarly, we have  $h^2 = g$ . Thus we obtain the following Cayley table

$G$	1	$g$	$h$
1	1	$g$	$h$
$g$	$g$	$h$	1
$h$	$h$	1	$g$

Which is the same as  $C_3$ . □

**Proof of 4:** See assignment 1 □

**Exercise 1.4.1**

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

## 2 Subgroups

### 2.1 Subgroups

**Definition 2.1.1**

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

**Note**

We note that since  $G$  is a group, for  $h_1, h_2, h_3 \in H \subseteq G$ , we have

$$h_1(h_2h_3) = (h_1h_2)h_3$$

Thus

**Proposition 2.1.1****Subgroup Test**

Let  $G$  be a group,  $H \subseteq G$ . Then  $H$  is a subgroup of  $G$  if

1. If  $h_1, h_2 \in H$ , then  $h_1h_2 \in H$
2.  $1_H \in H$
3. If  $h \in H$ , then  $h^{-1} \in H$

**Exercise 2.1.1**

Prove that  $1_H = 1_G$

**Example 2.1.1**

Given a group  $G$ , then  $\{1\}, G$  are subgroups of  $G$

**Example 2.1.2**

We have a chain of groups

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

**Example 2.1.3**

Define

$$\mathrm{SL}_n(\mathbb{R}) = (\mathrm{SL}_n(\mathbb{R}), \cdot) := \{M \in M_n(\mathbb{R}), \det(M) = 1\} \subseteq \mathrm{GL}_n(\mathbb{R})$$

Note that the identity matrix  $I \in \mathrm{SL}_n(\mathbb{R})$ . Let  $A, B \in \mathrm{SL}_n(\mathbb{R})$ , then

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

and

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

i.e.  $AB, A^{-1} \in \mathrm{SL}_n(\mathbb{R})$ . By the subgroup test ([Proposition 2.1.1](#)),  $\mathrm{SL}_n(\mathbb{R})$  is a subgroup of  $\mathrm{GL}_n(\mathbb{R})$ . We call  $\mathrm{SL}_n(\mathbb{R})$  the *special linear group of order  $n$  over  $\mathbb{R}$*

**Definition 2.1.2**

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

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

**Remark**

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

**Proposition 2.1.2**

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

**Proof:** Note that  $1 \in Z(G)$ . 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  $yz \in Z(G)$ . Also, for  $z \in Z(G)$ ,  $g \in G$  we have

$$\begin{aligned} zg = gz &\iff z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} \\ &\iff gz^{-1} = z^{-1}g \end{aligned}$$

Thus  $z^{-1} \in Z(G)$ . By the subgroup test ([Proposition 2.1.1](#)),  $Z(G)$  is a subgroup of  $G$ . Also, by the definition of  $Z(G)$ , we see that it is abelian. □

**Proposition 2.1.3**

Let  $H, K$  be subgroups of a group  $G$ . Then  $H \cap K$  is also a subgroup.

**Proof:** Exercise □

**Proposition 2.1.4****Finite Subgroup Test**

If  $H \neq \emptyset$  is a finite subset of a group  $G$ , then  $H$  is a subgroup of  $G$  iff  $H$  is closed under its operation.

**Proof:**

( $\implies$ ) obvious

( $\impliedby$ ) For  $H \neq \emptyset$ , let  $h \in H$ . Since  $H$  is closed under its operation, we have  $h, h^2, h^3, \dots \in H$ . Since  $H$  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,  $1 = h^{m-1}h$  implies that  $h^{-1} = h^{m-1}$  and thus  $h^{-1} \in H$ . By the subgroup test,  $H$  is a subgroup of  $G$ .  $\square$

## 2.2 Alternating Groups

**Definition 2.2.1**

A *transposition*  $\sigma \in S_n$  is a cycle of length 2. i.e.  $\sigma = (ab)$  with  $a, b \in \{1, 2, \dots, n\}$  and  $a \neq b$ .

**Example 2.2.1**

Consider  $(1245) \in S_5$ . Also the composition  $(12)(24)(45)$  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  $(1245) = (12)(24)(45)$  Also we can show that

$$(1245) = (23)(12)(25)(13)(24)$$

We see from this example that the factorization into transpositions are NOT unique. However, one can prove (see Bonus 2)

**Theorem 2.2.1****Parity Theorem**

If a permutation  $\sigma$  has two factorizations

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r = \mu_1 \mu_2 \cdots \mu_s$$

Where each  $\gamma_i$  and  $\mu_j$  is a transposition, then  $r \equiv s \pmod{2}$

**Definition 2.2.2**

A permutation  $\sigma$  is *even* (or *odd*) if it can be written as a product of an even (or odd) number of transpositions. By the previous theorem, a permutation is either even or odd, but not both.

**Theorem 2.2.2**

For  $n \geq 2$ , let  $A_n$  denote the set of all even permutations in  $S_n$

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.  $|A_n| = \frac{1}{2}n!$

From (1) and (2), we see  $(A_n)$  is a subgroup of  $S_n$  called the *alternating group of degree  $n$* .

**Proof of 1:** We can write  $\varepsilon = (12)(12)$ . Thus  $\varepsilon$  is even. □

**Proof of 2:** if  $\sigma, \tau \in A_n$  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 integers. Then

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

is a product of  $(r + s)$  transpositions and thus  $\sigma\tau \in A_n$ . Also, we note that  $\sigma_i$  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. □

**Proof of 3:** Let  $O_n$  denote the set of odd permutations in  $S_n$ . Thus  $S_n = A_n \cup O_n$  and the parity theorem implies that  $A_n \cap O_n = \emptyset$ . Since  $|S_n| = n!$ , to prove  $|A_n| = \frac{1}{2}n!$ , it suffices to show that  $|A_n| = |O_n|$ . Let  $\gamma = (12)$  and let  $f : A_n \rightarrow O_n$  be defined by  $f(\sigma) = \gamma\sigma$ . Since  $\sigma$  is even, we have  $\gamma\sigma$  is odd. Thus the map is well-defined. Also, if we have  $\gamma\sigma_1 = \gamma\sigma_2$ , then by cancellation, we get  $\sigma_1 = \sigma_2$ , thus  $f$  is injective. Finally, if  $\tau \in O_n$ , then  $\sigma = \gamma\tau \in A_n$  and  $f(\sigma) = \gamma\sigma = \gamma(\gamma\tau) = \gamma^2\tau = \tau$ . Thus  $f$  is surjective. It follows that  $f$  is a bijection, thus  $|A_n| = |O_n|$ . It follows that  $|A_n| = \frac{1}{2}n! = |O_n|$  □

## 2.3 Orders of Elements

### Notation

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

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} = \{\dots, g^{-1}, g^0 = 1, g, g^2, \dots\}$$

Note that  $1 = g^0 \in \langle g \rangle$ . Also, if  $x = g^m, y = g^n \in \langle g \rangle$  With  $m, n \in \mathbb{Z}$ , then  $xy = g^n g^m = g^{n+m} \in \langle g \rangle$  and  $x^{-1} = g^{-m} \in \langle g \rangle$ . By the subgroup test, we have

### Proposition 2.3.1

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

### Definition 2.3.1

Let  $G$  be a group with  $g \in G$ . 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  $g$  a *generator* of  $G$ .

**Example 2.3.1**

Consider  $(\mathbb{Z}, +)$ . Note that for all  $k \in \mathbb{Z}$ , we can write  $k = k \cdot 1$ . Thus we can see  $\langle \mathbb{Z}, + \rangle = \langle 1 \rangle$ . Similarly,  $\langle \mathbb{Z}, + \rangle = \langle -1 \rangle$ . We observe, for any integer  $n \in \mathbb{Z}$  with  $n \neq \pm 1$  there exist no  $k \in \mathbb{Z}$  such that  $k \cdot n = 1$ . Thus  $\pm 1$  are the only generators of  $(\mathbb{Z}, +)$ .

**Remark**

Let  $G$  be a group and  $g \in G$ . Suppose there is  $k \in \mathbb{Z}$   $k \neq 0$  such that  $g^k = 1$  then  $g^{-k} = (g^k)^{-1} = 1$ . Thus we can assume  $k \geq 1$ . Then by the well-ordering principle, there exists the smallest positive integer  $n$  such that  $g^n = 1$

**Definition 2.3.2**

Let  $G$  be a group and  $g \in G$ . If  $n$  is the smallest positive integer such that  $g^n = 1$ , then we say the *order* of  $g$  is  $n$ , denoted  $o(g) = n$ . If no such  $n$  exists, we say  $g$  has *infinite order* and write  $o(g) = \infty$

**Proposition 2.3.2**

Let  $G$  be a group and  $g \in G$  with  $o(g) = n \in \mathbb{N}$ . For  $k \in \mathbb{Z}$  we have

1.  $g^k = 1$  iff  $n \mid k$
2.  $g^k = g^m$  iff  $k \equiv m \pmod{n}$
3.  $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$  where  $1, g, \dots, g^{n-1}$  are all distinct. In particular, we have  $|\langle g \rangle| = o(g)$

**Proof of 1:**

( $\Leftarrow$ ) if  $n \mid k$ , then  $k = nq$  for some  $q \in \mathbb{Z}$ . Thus

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

( $\Rightarrow$ ) By the 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

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

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

**Proof of 2:** Note that  $g^k = g^m$  iff  $g^{km} = 1$ . By (1), we have  $n \mid (km)$  i.e.  $k \equiv m \pmod{n}$  □

**Proof of 3:** It follows from (2) that  $1, g, \dots, g^{n-1}$  are all distinct. Clearly, we have  $\{1, g, \dots, g^{n-1}\} \subseteq \langle g \rangle$ .

To prove the other inclusion, let  $g^k \in \langle g \rangle$  for some  $k \in \mathbb{Z}$ . Write  $k = nq + r$  with  $n, r \in \mathbb{Z}$  and  $0 \leq r < n$ . Then

$$g^k = g^{nq+r} = g^{nq} g^r = (g^n)^q g^r = 1^q g^r = g^r \in \{1, g, \dots, g^{n-1}\}$$

Thus  $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$  □



**Proposition 2.3.3**

Let  $G$  be a group and  $g \in G$  with  $o(g) = \infty$ . For  $k \in \mathbb{Z}$  we have

1.  $g^k = 1$  iff  $k = 0$
2.  $g^k = g^m$  iff  $k = m$
3.  $\langle g \rangle = \{\dots, g^{-1}, g^0 = 1, g, \dots\}$  where  $g^i$  are all distinct

**Proposition 2.3.4**

Let  $G$  be a group and  $g \in G$  with  $o(g) = n \in \mathbb{N}$ . If  $d \in \mathbb{N}$ , then  $o(g^d) = \frac{n}{\gcd(n, d)}$ . In particular, if  $d \mid n$ , then  $\gcd(n, d) = d$  and  $o(g^d) = \frac{n}{d}$

**Proof:** Let  $n_1 = \frac{n}{\gcd(n, d)}$  and  $d_1 = \frac{d}{\gcd(n, d)}$ . By a result from Math 135, we have  $\gcd(n_1, d_1) = 1$ . Note that

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

Thus it remains to show that  $n_1$  is the smallest such positive integer. Suppose  $(g^d)^r = 1$  with  $r \in \mathbb{N}$ . Since  $o(g) = n$ , by prop, we have  $n \mid dr$ . Thus there is  $q \in \mathbb{Z}$  such that  $dr = nq$ . Dividing both sides by  $\gcd(n, d)$  we get

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

Since  $n_1 \mid d_1 r$  and  $\gcd(n_1, d_1) = 1$ , by a result from Math 135, we get  $n_1 \mid r$  i.e.  $r = n_1 \ell$  for some  $\ell \in \mathbb{Z}$ . Since  $r, n_1 \in \mathbb{N}$ , it follows that  $\ell \in \mathbb{N}$ . Since  $\ell \geq 1$ , we get  $r \geq n_1$  □

**2.4 Cyclic Groups****Remark**

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  $a = g^n, b = g^m$  for some  $m, n \in \mathbb{Z}$ . We have

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba$$

**Proposition 2.4.1**

Every cyclic group is abelian

**Warning**

The converse of the above prop is not true. For example the Klein 4 group is abelian, but not cyclic.

**Proposition 2.4.2**

Every subgroup of a cyclic group is cyclic.

**Proof:** Let  $G = \langle g \rangle$  be cyclic and  $H \subseteq G$  a subgroup. If  $H = \{1\}$ , then  $H$  is cyclic. Otherwise, there is  $g^k \in H$  with  $k \in \mathbb{Z} \setminus \{0\}$ . Since  $H$  is a group, we have  $g^{-k} \in H$ . Thus we can assume that  $k \in \mathbb{N}$ . Let  $m$  be the smallest positive integer such that  $g^m \in H$ .

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

Proof is exercise, by division algorithm. □

### Proposition 2.4.3

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

**Proof:** By prop,

$$o(g^k) = \frac{n}{\gcd(n, k)} = n$$

□

### Theorem 2.4.4

### Fundamental Theorem of Finite Cyclic Groups

Let  $G = \langle g \rangle$  be a cyclic group with  $o(g) = n \in \mathbb{N}$ .

1. If  $H$  is a subgroup of  $G$ , then  $G = \langle g^d \rangle$  for some  $d \mid n$ . It follows that  $|H| \mid |G|$ .
2. Conversely, if  $k \mid n$ , then  $g^{\frac{n}{k}}$  is the unique subgroup of  $G$  with order  $k$ .

**Proof of 1:** By prop,  $H$  is cyclic. Write  $H = \langle g^n \rangle$  for some  $m \in \mathbb{N} \cup \{0\}$ . Let  $d = \gcd(m, n)$ .

Claim:  $H = \langle g^d \rangle$

Since  $d \mid m$  we have  $m = dk$  for some  $k \in \mathbb{Z}$ . Then

$$g^m = g^{dk} = (g^d)^k \in \langle g^d \rangle$$

Thus  $H = \langle g^m \rangle \subseteq \langle g^d \rangle$ . To prove the other inclusion, since  $d = \gcd(m, n)$ , there is  $x, y \in \mathbb{Z}$  such that  $d = mx + ny$ . Then

$$g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x 1^y = (g^m)^x \in \langle g^m \rangle$$

Thus  $\langle g^d \rangle \subseteq \langle g^m \rangle = H$ . It follows that  $H = \langle g^d \rangle$ . Note that since  $d = \gcd(m, n)$ , we have  $d \mid n$ . By prop, we have

$$|H| = o(g^d) = \frac{n}{\gcd(n, d)} = \frac{n}{d}$$

Thus  $|H| \mid |G|$  □

**Proof of 2:** By prop, the cyclic subgroup  $\langle g^{\frac{n}{k}} \rangle$  is of order

$$\frac{n}{\gcd(n, \frac{n}{k})} = \frac{n}{n/k} = k$$

To show uniqueness, let  $K$  be a subgroup of  $G$  with order  $k \mid n$ . By 1, let  $K = \langle g^d \rangle$  where  $d \mid n$ . Then by props, 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

### Definition 2.5.1

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

$$\langle X \rangle := \{x_1^{k_1} \cdots x_m^{k_m} \mid x_i \in X, k_i \in \mathbb{Z}, m \geq 1\}$$

denote the set of all products of powers of (not necessarily distinct) elements of  $X$ . Note that this is clearly a group.  $\langle X \rangle$  is called the *subgroup of  $G$  generated by  $X$* .

### Example 2.5.1

The Klein-4 group  $K_4 = \{1, a, b, c\}$  with  $a^2 = b^2 = c^2 = 1$  and  $ab = c$ . Thus

$$K_4 = \langle a, b \mid a^2 = 1 = b^2 \text{ and } ab = ba \rangle$$

### Example 2.5.2

The symmetric group of order 3  $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$  where  $\sigma^3 = \varepsilon = \tau^2$  and  $\sigma\tau = \tau\sigma^2$  (one can take  $\tau = (12)$  and  $\sigma = (123)$ ) Thus

$$\langle \sigma, \tau \mid \sigma^3 = \varepsilon = \tau^2 \text{ and } \sigma\tau = \tau\sigma^2 \rangle$$

We can also replace  $\sigma, \tau$  with  $\sigma, \tau\sigma$  or  $\sigma, \tau\sigma^2, \dots$ , etc

### Definition 2.5.2

For  $n \geq 2$  the *dihedral group of order  $2n$*  is defined by

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

Where  $a^n = 1 = b^2$  and  $aba = b$ . Thus

$$D_{2n} = \langle a, b \mid a^n = 1 = b^2 \text{ and } aba = b \rangle$$

### Note

For  $n = 2$  or  $3$  we have

$$D_4 \cong K_4 \quad \text{and} \quad D_6 \cong S_3$$

### Exercise 2.5.1

For  $n \geq 3$ , consider a regular  $n$ -gon and its group of symmetries. How does it relate to  $D_{2n}$ ?

## 3 Normal Subgroups

### 3.1 Homomorphisms and Isomorphisms

#### Definition 3.1.1

Let  $G, H$  be groups. A mapping  $\alpha : G \rightarrow H$  is a *homomorphism* if

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

To simplify notation, we often write

$$\alpha(ab) = \alpha(a)\alpha(b) \quad \forall a, b \in G$$

#### Example 3.1.1

Consider the determinant map

$$\begin{aligned} \det : \mathrm{GL}_n(\mathbb{R}) &\longrightarrow \mathbb{R}^* \\ A &\longmapsto \det A \end{aligned}$$

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

#### Proposition 3.1.1

Let  $\alpha : G \rightarrow H$  be a group homomorphism. Then

1.  $\alpha(1_G) = 1_H$
2.  $\alpha(g^{-1}) = \alpha(g)^{-1} \quad \forall g \in G$
3.  $\alpha(g^k) = \alpha(g)^k \quad \forall k \in \mathbb{Z}$

#### Definition 3.1.2

Let  $\alpha : G \rightarrow H$  be a mapping between groups. If  $\alpha$  is a homomorphism and  $\alpha$  is bijective, we say  $\alpha$  is an *isomorphism*. In this case, we say  $G, H$  are *isomorphic* and write  $G \cong H$ .

#### Proposition 3.1.2

We have

1. The identity map  $\mathrm{id} : G \rightarrow G$  is an isomorphism.
2. If  $\sigma : G \rightarrow H$  is an isomorphism, then the inverse map  $\sigma^{-1} : H \rightarrow G$  is also an isomorphism.
3. If  $\sigma : G \rightarrow H$  and  $\tau : H \rightarrow K$  is an isomorphism, the composite map  $\tau\sigma : G \rightarrow K$  is also an isomorphism.

So  $\cong$  is (sort-of) an equivalence relation

**Proof:** Exercise. □

**Example 3.1.2**

Let  $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$ . Then  $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$  since we see that

$$\begin{aligned}\sigma : \mathbb{R} &\rightarrow \mathbb{R}^+ \\ x &\mapsto e^x\end{aligned}$$

is a bijection. Moreover,  $\sigma(x + y) = e^{x+y} = e^x \cdot e^y = \sigma(x)\sigma(y)$  thus  $\sigma$  is an isomorphism.

**Example 3.1.3**

Claim:  $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$  Suppose  $\tau : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}^*, \cdot)$  is an isomorphism. Thus  $\tau$  is surjective. So there is some  $q \in \mathbb{Q}$  such that  $\tau(q) = 2$ . Then

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

Thus  $\tau\left(\frac{q}{2}\right)$  is a rational number whose square is 2, a contradiction.

**3.2 Cosets and Lagrange's Theorem****Definition 3.2.1**

Let  $H$  be a subgroup of a group  $G$ . If  $a \in G$ , we define

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

to be the *right coset of  $H$  generated by  $a$* . We define the left coset similarly.

**Remark**

Since  $1 \in H$ , we have  $H1 = H = 1H$ . Also  $a \in Ha$  and  $a \in aH$ . Note that in general  $Ha$  and  $aH$  are not subgroups of  $G$ , and  $aH \neq Ha$ . However, if  $G$  is abelian, then  $Ha = aH$ .

**Example 3.2.1**

Let  $K_4 = \{1, a, b, ab\}$ . Let  $H = \{1, a\}$  which is a subgroup of  $K_4$ . Note that since  $K_4$  is abelian, we have  $gH = Hg$  for all  $g \in K_4$ . Then the (right or left) cosets of  $H$  are

$$H1 = \{1, a\} = 1H$$

and

$$Hb = \{b, ab\} = Hab$$

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

**Example 3.2.2**

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

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

Notice that  $H\sigma \neq \sigma H$  and  $H\sigma^2 \neq \sigma^2 H$

**Proposition 3.2.1**

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

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

**Proof of 1:**

( $\implies$ ) If  $Ha = Hb$ , then  $a = 1a \in Ha = Hb$ . Thus  $a = hb$  for some  $h \in H$  and we have  $ab^{-1} = h \in H$ .

( $\impliedby$ ) Suppose  $ab^{-1} \in H$  for all  $h \in H$ . Then for all  $h \in H$ ,

$$ha = hab^{-1}b = h(ab^{-1})b \in H$$

Thus  $Ha \subseteq Hb$ . Note that if  $ab^{-1} \in H$ , since  $H$  is a subgroup, then

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

Thus for all  $h \in H$ ,

$$hb = h(ba^{-1})a \in Ha$$

Thus  $Hb \subseteq Ha$ . It follows that  $Ha = Hb$ . □

**Proof of 2:** If  $a \in Hb$ , then  $ab^{-1} \in H$ . Thus, by (1), we have  $Ha = Hb$ . □

**Proof of 3:** Two cases:

1. If  $Ha \cap Hb = \emptyset$ , then we are done.
2. If  $Ha \cap Hb \neq \emptyset$ , then there exists  $x \in Ha \cap Hb$ . Since  $x \in Hb$ , by (2), we have  $Hb = Hx$ . Thus

$$Ha = Hx = Hb$$

□

**Remark**

The analogues of the previous prop also holds for left cosets

1.  $aH = bH$  if and only if  $b^{-1}a \in H$

**Exercise 3.2.1**

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

**Definition 3.2.2**

By the previous prop, we see that  $G$  can be written as a disjoint union of right cosets of  $H$ . We define the *index*  $[G : H]$  to be the number of disjoint right (or left) cosets of  $H$  in  $G$ . (Note that  $[G : H]$  could be infinite).

**Theorem 3.2.2****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:** Write  $k = [G : H]$  and let  $Ha_1, \dots, Ha_k$  be the distinct right cosets of  $H$  in  $G$ . By prop

$$G = Ha_1 \sqcup \dots \sqcup Ha_k$$

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

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

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

**Corollary 3.2.3**

1. If  $G$  is a finite group and  $g \in G$  then  $o(g) \mid |G|$
2. If  $G$  is a finite group with  $|G| = n$ , then for all  $g \in G$ , we have  $g^n = 1$

**Proof of 1:** Take  $H = \langle g \rangle$  in the theorem. Note that  $|H| = o(g)$  □

**Proof of 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 3.2.3**

For  $n \in \mathbb{N}$  with  $n \geq 2$ , 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  $\mathbb{Z}_n^*$ . i.e.

$$\varphi(n) = |\{[k] \in \mathbb{Z}_n \mid k \in \{0, 1, \dots, n-1\} \text{ and } \gcd(k, n) = 1\}|$$

As a direct consequence of the 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 Theorem. If  $n = p$ , a prime number, then Euler's Theorem implies that  $a^{p-1} \equiv 1 \pmod{p}$ , which is Fermat's little theorem.

**Recall**

If  $|G| = 2$  then  $G \cong C_2$ , and  $|G| = 3$  then  $G \cong C_3$ .

**Corollary 3.2.4**

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

**Proof:** Let  $g \in G$  with  $g \neq 1$ . Then by corollary, we have  $o(g) \mid p$ . Since  $g \neq 1$  and  $p$  is a prime, we have  $o(g) = p$ . By prop, we have

$$|\langle g \rangle| = o(g) = p$$

It follows that  $G \cong \langle g \rangle \cong C_p$  □

**Corollary 3.2.5**

Let  $H$  and  $K$  be finite subgroups of a group  $G$ . If  $\gcd(|H|, |K|) = 1$ , then  $H \cap K = \{1\}$ .

**Proof:** Note  $H \cap K$  is a subgroup of  $H$  and  $K$ . So by Lagrange's Theorem, we have  $|H \cap K| \mid |H|$  and  $|H \cap K| \mid |K|$ . It follows that  $|H \cap K| \mid \gcd(|H|, |K|)$ , i.e.  $|H \cap K| = 1$  Thus  $H \cap K = \{1\}$ . □