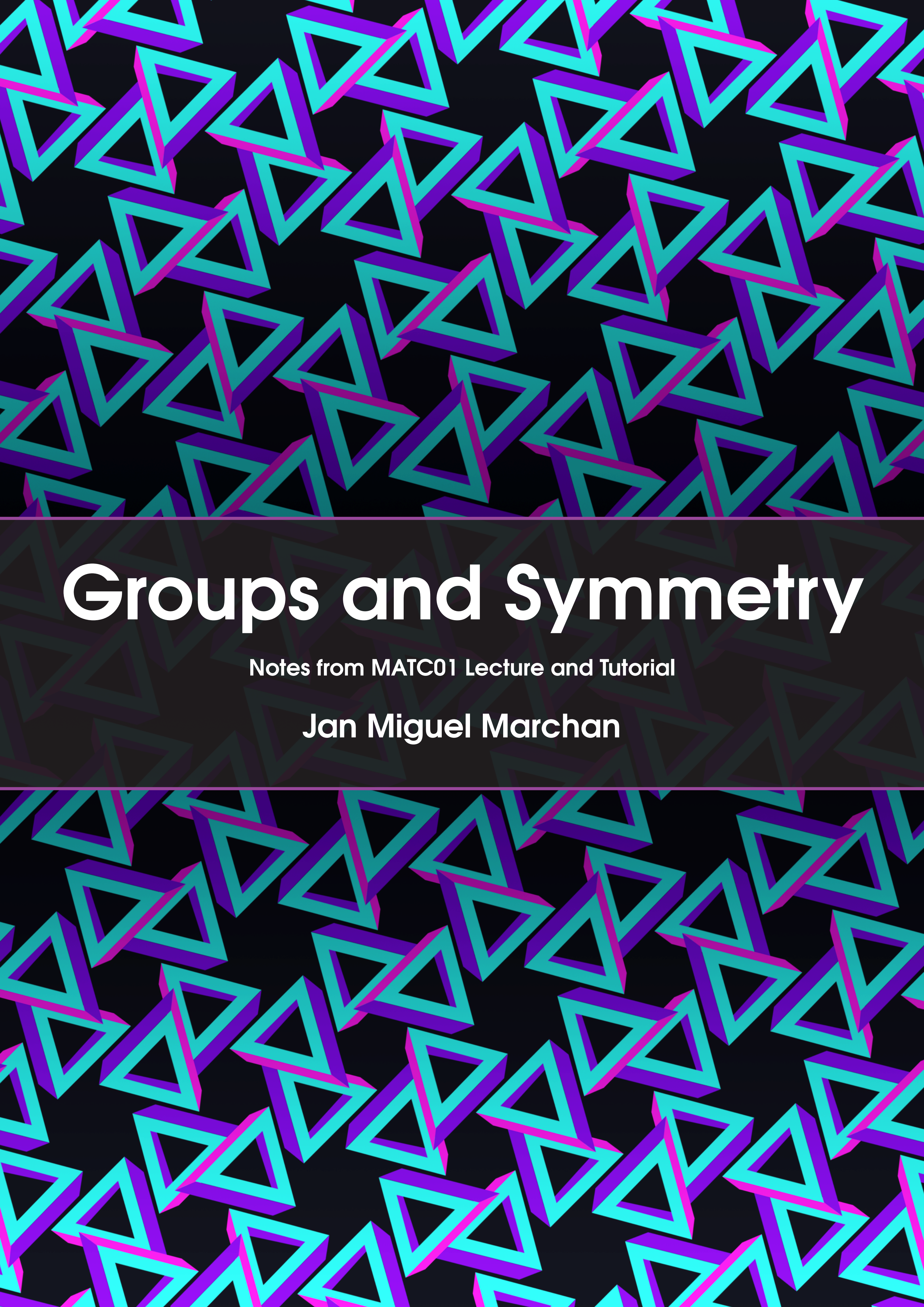


Groups and Symmetry

Notes from MATC01 Lecture and Tutorial

Jan Miguel Marchan

Contents

Part One

1. Groups

1.1 Introduction to groups

1.1.1 Symmetries of the equilateral triangle

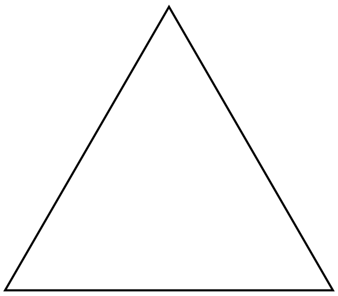


Figure 1.1: An equilateral triangle

Consider the equilateral triangle as shown 1.1. It has plenty of symmetries. You can reflect it about each of its three perpendicular bisectors, or you can rotate it some multiple of 120° about its center, both obtaining the original shape after the transformation.

Definition 1.1.1 — Plane symmetry. A *plane symmetry* is a bijection of an object to itself that preserves distances.

Consider the equilateral triangle's rotations.

■ **Example 1.1 — Rotations of the equilateral triangle.** The following transformations are all plane symmetries:

- R_{240}, the rotation of 240 degrees counterclockwise about the center;
- R_{120}, the rotation of 120 degrees counterclockwise about the center;
- R_0, the rotation of 0 degrees;

■

Notation 1.1. *Given a figure, R_d refers to a rotation d degrees counterclockwise about its center.*

Note that any rotation that is not $n(120°)$ for $n \in \mathbb{N}$ and about the center of the triangle is not a plane symmetry because these would not be surjective.

What about reflections?

■ **Example 1.2 — Reflections of the equilateral triangle.** The following transformations are all plane symmetries:

- V, the reflection about the vertical axis;
- D, the reflection about the main diagonal (going down and right);
- D', the reflection about the other diagonal;

■

Proposition 1.1.1 There are 6 distinct plane symmetries of the equilateral triangle, $\text{Sym}(\triangle) = \{R_{240°}, R_{120°}, R_{0°}, V, D, D'\}$

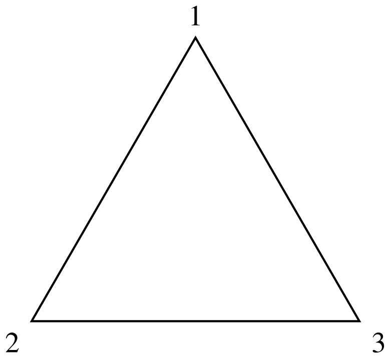


Figure 1.2: A labeled equilateral triangle

Proof. Use a combinatorial argument. Also think about function composition and how these functions are bijections. What happens if you compose any two plane symmetries? You will get one of these symmetries again.

Label the vertices of equilateral triangle. Without loss of generality, consider vertex 1. (That is, we can relabel any vertex to be vertex to create an equivalent solution.) By definition of plane symmetry, a vertex must map to a vertex. There are 3 possibilities for vertex 1. Given the final position of vertex 1, we can reflect (or not) through the vertex (the perpendicular bisector of the opposite side so we have 2 possibilities. We can do this for each of the 3 vertices.

$\therefore$ There are $3 \times 2 = 6$ distinct plane symmetries. □

1.1.2 Composition

Note that plane symmetries are functions with the same domain and range. Therefore, we can define the operation composition on $\text{Sym}(\triangle)$. That is, we can perform one plane symmetry after another.

Notation 1.2. *Function composition $f \circ g$ can be written as fg.*

■ **Example 1.3** $D' \circ R_{120} = D$. We can show this by showing where each vertex of the triangle maps: $123 \to 312 \to 213$. For example, this states that D' brings vertex 1 to vertex 3 then R_{120} brings it to vertex 2, equivalent to D bringing vertex 1 to vertex 2 in one transformation. ■

1.1.3 Cayley Table

A Cayley table is a table that defines all the compositions of functions. Note that the column function is applied first, then the row is applied second.

$\circ$	R_0	R_{120}	R_{240}	V	$D‘$	D
R_0	R_0	R_{120}	R_{240}	V	$D‘$	D
R_{120}	R_{120}	R_{240}	R_0	D	V	$D‘$
R_{240}	R_{240}	R_0	R_{120}	$D‘$	D	V
V	V	$D‘$	D	R_0	R_{120}	R_{240}
$D‘$	$D‘$	D	V	R_{240}	R_0	R_{120}
D	D	V	$D‘$	R_{120}	R_{240}	R_0

Table 1.1: Cayley table for $\mathrm{Sym}(\triangle)$

Looking at Table 1.1, we can note that $\mathrm{Sym}(\triangle)$ is closed, ie $\forall A, B \in \mathrm{Sym}(\triangle), AB \in \mathrm{Sym}(\triangle)$ and that each member of $\mathrm{Sym}(\triangle)$ appears exactly once in each row and column.

Observe:

- Each $A \in \mathrm{Sym}(\triangle)$ has an inverse. (In fact, the inverse is 2-sided, ie, the inverse can be composed from the left or right $A^{-1}A = AA^{-1} = R_0$.)
- R_0 is a 2-sided identity $R_0A = AR_0 = A$.
- $\circ$ is associative.

These properties along with closure on a binary operation create a group.

1.2 Groups

1.2.1 Binary Operation

Definition 1.2.1 — Binary Operation. [Gal17, page 42] Let G be a set. A *binary operation*, $*$, is a function $* : G \times G \to G$.

This gives $(g,h) \mapsto g*h, \forall g,h \in G$. That is, $*$ maps each ordered pair of elements in G to an element in G, which means the function must be closed.

■ **Example 1.4** The following are examples of binary operations:

- $G = \mathbb{R}, * = +, + : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (g,h) \mapsto g+h$;
- $G = M_n(\mathbb{R}) = \{n \times n$ real-valued matrices$\}$, $* = \cdot$, matrix multiplication;

■

1.2.2 Group

Definition 1.2.2 — Group. [Gal17, page 43] A *group* is a pair $(G, *)$ consisting of a set $G \neq \varnothing$ and $*$ is a binary operation defined on G satisfying:

1. $*$ is associative, $\forall g_1, g_2, g_3 \in G, (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$
2. An identity element exists, $\exists e \in G, \forall g \in G, e * g = g = g * e$
3. Each element in G has a 2-sided inverse, $\forall g \in G, \exists g^{-1} \in G, g * g^{-1} = e = g^{-1}g$

Notation 1.3. *By convention, we can often write the set G on its own instead of* $(G, *)$ *if we know the context. Also, we write* $g, h \in G, g*h$ *as gh.*

When checking that a pair is a group, we have to check five things: the nonempty set, the closure of the binary operation, along with associativity, identity, and inverse. To show a pair is not a group, we show one of these is not true.

R We will use that $\mathbb{N} = \mathbb{Z}_{\geq 0}$

Proposition 1.2.1 $(\mathbb{N}, -)$ is not a group.

Proof. We can show $(\mathbb{N}, -)$ is not a group by showing that $-$ is not a binary operation on $\mathbb{N}$.

$$\forall g, h \in \mathbb{N}, g - h \in \mathbb{N} \text{ is false} \Leftrightarrow \neg(\forall g, h \in \mathbb{N}, g - h \in \mathbb{N}) \text{ is true} \tag{1.1}$$

$$\Leftrightarrow \exists g, h \in \mathbb{N}, g - h \in \mathbb{N} \text{ is true} \tag{1.2}$$

For example, choose $g = 0 \in \mathbb{N}, h = 1 \in \mathbb{N}$. Consider $1 - 2 = -1 \notin \mathbb{N}$. Then $-$ is not a binary operation, and $(N, -)$ is not a group. □

1.3 Examples of groups

1.3.1 Sets of numbers

Some sets of numbers with addition $+$ are groups.

■ **Example 1.5** $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ are groups. ■

Proposition 1.3.1 The set of real numbers equipped with addition $(\mathbb{R}, +)$ is a group.

Proof. We prove $(\mathbb{R}, +)$ is a group by showing it satisfies the five properties of a group.

NON-EMPTINESS Since $0 \in \mathbb{R}$, $\mathbb{R} \neq \varnothing$.

CLOSURE Let $g, h \in \mathbb{R}$ be arbitrary. By axioms of $\mathbb{R}$, $g + h \in \mathbb{R}$. Therefore, $\forall g, h \in \mathbb{R}, g + h \in \mathbb{R}$.

ASSOCIATIVITY Let $g_1, g_2, g_3 \in \mathbb{R}$. By axioms of $\mathbb{R}$, $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$.

IDENTITY Choose $e = 0 \in \mathbb{R}$. Let $g \in \mathbb{R}$. Then $g + 0 = g$ and $0 + g = g$.

INVERSE Let $g \in \mathbb{R}$. Choose $g^{-1} = -g \in \mathbb{R}$ by axioms of $\mathbb{R}$. Then $g + g^{-1} = g + (-g) = 0$ and $g^{-1} + g = (-g) + g = 0$.

□

Some sets of numbers of numbers with multiplication $\cdot$ are groups. We don't include 0 since it does not have a multiplicative inverse.

Notation 1.4. *We denote the real numbers without 0 as* $\mathbb{R}^{\times} = \mathbb{R} - \{0\} = (-\infty, 0) \cup (0, \infty)$

■ **Example 1.6** $(\mathbb{R}^{\times}, \cdot), (\mathbb{C}^{\times}, \cdot)$ are groups. ■

1.3.2 Sets of symmetries

Some symmetries with the operation composition $\circ$ are groups. For example, we have the plane symmetries of the equilateral triangle.

■ **Example 1.7** The plane symmetries of any 2-D figure with composition $\circ$ is a group. ■

Definition 1.3.1 — Dihedral Group. The plane symmetries of the n-gon (the polygon with n equal length sides and equal interior angles) are called the *dihedral group* D_n.

■ **Example 1.8** The rotational symmetries of any 3-D object with composition $\circ$ is a group. ■

We can consider a subset of groups as a group, for example, just rotational symmetries. One way to describe these elements would be to label the vertices.

1.3.3 General linear group

Some sets of matrices with matrix multiplication are a group.

Definition 1.3.2 — General linear group. The *general linear group* $GL(2,\mathbb{R})$ is the set of 2×2 real-valued, invertible matrices with matrix multiplication.

Exercise 1.1 Show that $GL(2,\mathbb{R})$ is a group.

We prove $GL(2,\mathbb{R})$ is a group by showing it satisfies the five properties of a group.

NON-EMPTINESS $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$

CLOSURE Show that matrix multiplication results in a matrix that is still invertible.

ASSOCIATIVITY Use matrix multiplication theorems.

IDENTITY I is the identity.

INVERSE Two-sided inverse also exists from invertibility.

1.3.4 Permutations

Notice how there's a correspondence between the image of vertices upon the transformations of $D_3 = \{R_{240^\circ}, R_{120^\circ}, R_{0^\circ}, V, D, D'\}$ and the permutations on a set of 3 objects.

Definition 1.3.3 — Permutation. [Gal17, page 93] A *permutation* on a non-empty set X is a bijection from X to X.

Definition 1.3.4 — Permutation group. Let $X \neq \varnothing$ be a set. The set $\text{Perm}(X) = \{f : X \to X \mid f \text{ is a bijection}\}$ with composition $\circ$ is a *permutation group*.

Exercise 1.2 Show that $\text{Perm}(X)$ with $\circ$ is a group.

We prove $(\mathbb{R},+)$ is a group by showing it satisfies the five properties of a group.

NON-EMPTINESS $f(x) = x$ is 1-1 and onto, and $f(x) \in \text{Perm}(X)$, so $\text{Perm}(X) \neq \varnothing$.

CLOSURE Let $f, g \in \text{Perm}(X)$.

First, we show that $f \circ g : X \to X$ is injective, ie. $h : A \to B, \forall a, b \in \text{dom}(h)$, if $h(a) = h(b)$ then $a = b$.

Let $x_1, x_2 \in X$. Suppose $(f \circ g)(x_1) = (f \circ g)(x_2)$. Since $f \in \text{Perm}(X)$, by injectivity of f, then $g(x_1) = g(x_2)$. Since $g \in \text{Perm}(X)$, by injectivity of g, $x_1 = x_2$. So $f \circ g$ is injective.

Now, we show that $f \circ g : X \to X$ is surjective, ie. $h : A \to B, \forall y \in B, \exists x \in A h(x) = y$.

Let $x \in X$. Since $f \in \text{Perm}(X)$, it is surjective, ie. $\exists y \in X, f(y) = x$. Since $g \in \text{Perm}(X)$, it is surjective, ie. $\exists z \in X, g(z) = y$. Then $\exists z \in X, f(g(z)) = f(y) = x$. So $f \circ g$ is surjective.

Since $f \circ g$ is bijective, $f \circ g \in \text{Perm}(X)$.

ASSOCIATIVITY Show associativity with sets A, B, C, D and functions f, g, h.

IDENTITY Show identity using the identity function.

INVERSE Show inverse exists from bijectivity.

Example 1.9 Let $X = \{1,2,3\}$. What are the elements in $\mathrm{Perm}(X)$?

We can describe the functions of $\mathrm{Perm}(X)$ with mapping notation. One element is $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. The following list describes all the elements:

$$p_1 : 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3 \tag{1.3}$$
$$p_2 : 1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2 \tag{1.4}$$
$$p_3 : 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3 \tag{1.5}$$
$$p_4 : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1 \tag{1.6}$$
$$p_5 : 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2 \tag{1.7}$$
$$p_6 : 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1 \tag{1.8}$$

■

Definition 1.3.5 — Cycle. [Gal17, page 102] Let $n \in Z^+$ and $X = \{1,2,\dots,n\}$. Let $a_1, a_2, \dots, a_k$ be distinct numbers in X. A *cycle* (or k-cycle) is denoted $(a_1\ a_2\ \dots\ a_k)$ represents the mapping $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\dots, a_{k-1} \mapsto a_k$, $a_k \mapsto a_1$.

Consider the mapping in Example 1.9. We can describe it in cycle notation. $\beta_1 : (1)(2)(3)$, $\beta_2 : (1)(2\ 3)$, $\beta_3 : (1\ 2)(3)$, $\beta_4 : (1\ 2\ 3)$, $\beta_5 : (1\ 3\ 2)$, $\beta_6 : (1\ 3)(2)$.

Since these are functions, we can compose them.

Example 1.10 We can calculate $(1\ 2\ 3) \circ (1\ 2\ 3)$ by finding what each input outputs, and we take those outputs as the next input to give the cycle.

$$f(g(1)) = f(2) = 3 \tag{1.9}$$
$$f(g(3)) = f(1) = 2 \tag{1.10}$$
$$f(g(2)) = f(3) = 1 \tag{1.11}$$

That is $(1\ 2\ 3) \circ (1\ 2\ 3) = (1\ 3\ 2)$. ■

R Only order matters in cycle notation, not the starting value, eg., $(3\ 2\ 1)$ and $(2\ 1\ 3)$ are equivalent to $(1\ 3\ 2)$. Also, cycles which aren't written are assumed to be fixed, eg., $(1)\ (2)\ (3)$ is equivalent to (1).

Consider the permutation group of $\{1,2,3\}$, $\mathrm{Perm}(X) = \{(1),(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\}$.

1.3.5 Symmetric group

Definition 1.3.6 — Symmetric group. The group of permutations on the set $X = \{1,2,\dots,n\}$ is called the *symmetric group* of degree n, S_n.

1.3.6 Integers modulo n

Recall modular arithmetic.

Let $a, n \in \mathbb{Z}, n \geq 0$. Our division algorithm gives that $\exists q, r \in \mathbb{Z}$ such that $a = qn + r$ where $0 \leq r < n$. (For example, $4 \equiv 0 \pmod 2$, $7 \equiv 1 \pmod 2$.)

We want to consider addition modulo n, $a + b \pmod n$ and multiplication modulo n, $a \cdot b \pmod n$.

$\circ$	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 2 3)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 3 2)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

Table 1.2: Cayley table for S_3

Definition 1.3.7 — Integers modulo n. Let $n \in Z^+$. The set $\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$ is the *integers modulo n*.

$+ \pmod{4}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 1.3: Cayley table for $(\mathbb{Z}_4, + \pmod{4})$

$\cdot \pmod{4}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Table 1.4: Cayley table for $(\mathbb{Z}_4, \cdot \pmod{4})$

■ **Example 1.11** We have $(\mathbb{Z}_4, + \pmod{4})$ and $(\mathbb{Z}_4, \cdot \pmod{4})$ represented in Table 1.3 and 1.4 respectively. Observe that $(\mathbb{Z}_4, + \pmod{4})$ is a group but $(\mathbb{Z}_4, \cdot \pmod{4})$ is not a group. ■

If we want $(\mathbb{Z}_4, \cdot \pmod{4})$ to be a group, we could consider a subset $\{1,3\}$ and show that $(\{1,3\}, \cdot \pmod{4})$ is a group. Some sets of numbers with modular arithmetic are a group.

1.3.7 Units modulo n

Definition 1.3.8 — Units modulo n. Let $n \in \mathbb{Z}$. The set $U(n) = \{a \in Z_n \mid \gcd(a,n) = 1\}$ is the *units modulo n*.

■ **Example 1.12** $U(12) = \{1,5,7,11\}$. ■

Proposition 1.3.2 For $n \in Z^+$, $(\mathbb{Z}_n, + \pmod{n})$ and $(U(n), \cdot \pmod{n})$ are groups.

2. Properties of groups

2.1 Properties of groups

2.1.1 Uniqueness of identity

Note that we don't specify the uniqueness of the identity or the inverse in the definition of a group. These are theorems that follow from these definitions.

Theorem 2.1.1 — Uniqueness of identity. [Gal17, page 50] If G is a group, then the identity element e is unique.

Proof. Suppose G is a group, and $e, e' \in G$ are both identities.

We are given the following from identity axioms:

$$\forall g \in G, eg = ge = g \tag{2.1}$$

and

$$\forall g \in G, e'g = ge' = g \tag{2.2}$$

By 2.1, set $g = e'$, then $ee' = e'e = e'$.
By 2.2, set $g = e$, then $e'e = ee' = e$.
Then $e' = ee' = e$. □

2.1.2 Cancellation laws

Theorem 2.1.2 — Cancellation laws. [Gal17, page 50] If G is a group, then

$$\forall a, b, c \in G, ab = ac \Rightarrow b = c \tag{2.3}$$
$$\forall a, b, c \in G, ba = ca \Rightarrow b = c \tag{2.4}$$

2.3 is the left cancellation law and 2.4 is the right cancellation law.

Proof. Suppose G is a group. We want to show the left cancellation law.

Let $a,b,c \in G$ and $ab = ac$.

By the inverse axiom of groups, every element has an inverse, ie., $\exists a^{-1} \in G$ such that $a^{-1}a = e$. By the identity axiom of groups, $\exists e \in G$ such that $eb = b$ and $ec = c$.

$$\begin{aligned} ab = ac &\Rightarrow a^{-1}(ab) = a^{-1}(ac) && \text{(Closure)} \\ &\Rightarrow (a^{-1}a)b = (a^{-1}a)b && \text{(Associativity)} \\ &\Rightarrow eb = ec && \text{(Inverse)} \\ &\Rightarrow b = c && \text{(Identity)} \end{aligned}$$

The right cancellation law follows similarly.

Let G be a group, $a,b,c \in G$, and $ba = ca$.

By the inverse axiom of groups, every element has an inverse, ie., $\exists a^{-1} \in G$ such that $aa^{-1} = e$. By the identity axiom of groups, $\exists e \in G$ such that $be = b$ and $ce = c$.

$$\begin{aligned} ba = ca &\Rightarrow (ba)a^{-1} = (ca)a^{-1} && \text{(Closure)} \\ &\Rightarrow b(aa^{-1}) = b(aa^{-1}) && \text{(Associativity)} \\ &\Rightarrow be = ce && \text{(Inverse)} \\ &\Rightarrow b = c && \text{(Identity)} \end{aligned}$$

□

2.1.3 Uniqueness of inverse

Theorem 2.1.3 — Uniqueness of inverse. If g is a group, then the inverse of an element is unique to that element.

Proof. Let $g \in G$. Suppose $\exists g_1, g_2 \in G, g_1g = gg_1 = g_2g = gg_2 = e$. Then we can use the identity element e.

$$\begin{aligned} g_1 &= g_1e && \text{(Identity)} \\ &= g_1(g_2g) && \text{(Since } g_2 \text{ is inverse)} \\ &= g_1(gg_2) && (g_2g = gg_2) \\ &= (g_1g)g_2 && \text{(Associativity)} \\ &= eg_2 && \text{(Since } g_1 \text{ is inverse)} \\ &= g_2 && \text{(Identity)} \end{aligned}$$

□

2.1.4 Commutativity

A group's binary operation need not be commutative for G to be a group. Thus we have a separate definition for when a group is commutative.

Definition 2.1.1 — abelian Group. A group $(G,*)$ is an *abelian group* if $*$ is commutative, ie $\forall g,h \in G, gh = hg$

■ **Example 2.1** Any of $\mathbb{Z},\mathbb{Q},\mathbb{R}$ with addition is an abelian group. However, $GL(\mathbb{R},2)$ with matrix multiplication is non-abelian. ■

We could check commutativity with a Cayley table: an abelian group will have diagonal symmetry. To show a group is non-abelian, we only need to find a counterexample.

Proposition 2.1.4 D_3 is not abelian.

Proof. We can show that $\exists g,h \in G, gh \neq hg$, which is the negation of the definition.
Choose $g = V$, $h = R_{120}$. Note $g,h \in D_3$.
$gh = VR_{120} = D'$ and $hg = R_{120}V = D$. Thus $hg \neq gh$. □

2.1.5 Order

Definition 2.1.2 — Order of a group. [Gal17, page 60] The *order of a group* G, $|G|$, is the total number of elements in G.

The order of a group may be finite, $|G| < \infty$, or infinite, $|G| = \infty$.

■ **Example 2.2** $D_3 = \{R_0, R_{120}, R_{240}, V, D, D'\}$, $|D_3| = 6$. The group $\mathbb{R}$ with multiplication has infinite order. ■

Definition 2.1.3 — Order of a element. [Gal17, page 60] The *order of an element* $g \in G$ is the smallest positive integer n, $g^n = ggg\cdots g = e$, where e is the identity. If no such n exists, we say that g has infinite order. We denote $n = |g|$.

To find the order of an element g in G, we only need to calculate $g, g^2, g^3, \ldots$ until we get the identity. It follows immediately from the definition that the identity has order 1, and by the uniqueness of identity, it is the only element with order 1.

■ **Example 2.3** The order of each element in $D_3 = \{R_0, R_{120}, R_{240}, V, D, D'\}$:

- $|R_0| = 1$;
- $|V| = 2$, since $V \neq e, VV = e$;
- $|D| = |D'| = 2$, similarly to V;
- $|R_{120}| = 3$, since $R_{120} \neq e$, $R_{120}R_{120} \neq e$, $R_{120}R_{120}R_{120} = e$;
- $|R_{240}| = 3$, similarly to R_{120};

■

Exercise 2.1 Let $g \in G$ be an element of a group G, $|g| = n$. Prove that $g^{-1} = g^{n-1}$.

Proof. We are given that $|g| = n$, so $g^n = e$ by definition of order of an element.
By associativity, $g^n = g(g^{n-1}) = e$.
By inverse axiom, $g^{-1}(gg^{n-1}) = (g^{-1}g)g^{n-1} = g^{-1}e$. Then $eg^{n-1} = g^{-1}$.
$\therefore g^{-1} = g^{n-1}$. □

Exercise 2.2 Let $g \in G$. Prove that g and g^{-1} have the same order.

First, consider g with finite order.

Let $n = |G|$, so $g^n = e = g^{-n}g^n$. For contradiction, suppose $|g^{-1}| = k$ where $k \neq n$. why?

If $k < n$, them $g^{-k} = e$. Hence $e = g^k g^{-k} = g^k e = g^k$. Contradiction to definition of the order of g.

If $k > n$, then this is clearly (why?) a contradiction.

Also, what happens when order of g is infinite?

Exercise 2.3 Suppose $\forall x \in G, x^2 = e$. Prove that G is an abelian group.

Proof. We want to show that $\forall x, y \in G, xy = yx$.

Let $x, y \in G$.

By closure, we can consider $(xy)^2 = e = xyxy$. Then $xe = xxyxy = eyxy$. So $yx = yyxy = y^2xy = exy = xy$. □

■ **Example 2.4** Examples of finite abelian groups:

- $(\mathbb{Z}_n, + \pmod n)$
- $(U_n(\mathbb{Z}), \cdot \pmod n)$

■

■ **Example 2.5** Examples of finite non-abelian groups:

- D_n, the group of symmetries on a regular n-sided polygon
- S_n, the permutation group on the set $\{1, \ldots, n\}$
- $GL(\mathbb{Z}_5, 2)$, the set of 2×2, $\mathbb{Z}_5$-valued, invertible matrices.

■

Exercise 2.4 What is the order of $GL(\mathbb{Z}_5, 2)$? Consider that we need to check for non-zero determinant.

Exercise 2.5 Let X, Y be sets and $f : X \to Y$ a function on X and Y. How many functions f exist?

For each element in X, we have $|Y|$ possibilities to map that element. That is, we have $|Y|^{|X|}$ functions.

Exercise 2.6 $G = \{\phi \mid \phi : X \to X \text{ is a bijection}\}$ with composition $\circ : G \times G \to G$. Prove $(G, \circ)$ is a group.

Consider $X = \{1, \ldots, n\}$. Then $G = S_n$, the permutation group, and $|G| = n!$. This is stating that bijective functions restricts the choices from which x maps to y.

3. Subgroups

3.1 Subgroups and Subgroup Tests

We can consider subsets of groups.

Definition 3.1.1 — Subgroup. [Gal17, page 61]

Let G be a group. If $H \subseteq G$ such that $H \neq \varnothing$ is itself a group under the operation of G, then H is a *subgroup*, $H \leqslant G$.

If $H \leqslant G$ and $H \neq G$, then H is a *proper subgroup*, $H < G$.

For any group G, we always have a subgroup. For example, $G \leqslant G$. We also have the following subgroup.

Definition 3.1.2 — Trivial Subgroup. Let G be a group. $\{e\} \leqslant G$ is the *trivial subgroup*.

■ **Example 3.1** $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$. However, $(\mathbb{R}^{\times}, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$ since the binary operation is not the same. ■

There are ways we can test whether a subset of a group is a subgroup.

Theorem 3.1.1 — One-Step Subgroup Test. [Gal17, page 62]

Let G be a group. Let $H \subseteq G$ such that $H \neq \varnothing$.

If $h_1 h_2^{-1} \in H, \forall h_1, h_2 \in H$, then $H \leqslant G$.

Exercise 3.1 (a) Prove this using the two-step subgroup test.
(b) Prove without the two-step subgroup test. (That is, use the definition.)

Theorem 3.1.2 — Two-Step Subgroup Test. [Gal17, page 63]

Let G be a group. Let $H \subseteq G$ such that $H \neq \varnothing$.

$$h_1h_2 \in H, \forall h_1,h_2 \in H \tag{3.1}$$
$$h^{-1} \in H, \forall h \in H \tag{3.2}$$

If 3.1 and 3.2, then $H \leqslant G$.

Proof. Let G be a group. Let $H \subseteq G$ such that $H \neq \varnothing$. Suppose 3.1 and 3.2.

NON-EMPTINESS: H is assumed nonempty.

CLOSURE: By 3.1, $\forall h_1,h_2 \in H, h_1h_2 \in H$.

ASSOCIATIVITY: $H \subseteq G$ and G is a group, so G is associative. $\therefore H$ inherits associativity from G.

INVERSE: Follows from 3.2.

IDENTITY: Let $h \in H$. (We know $\exists h \in H$ because $H \neq \varnothing$.)

From 3.2, $h^{-1} \in H$. From 3.1, $hh^{-1} \in H$, so $e \in H$. Since $H \subseteq G$, H has the same identity as G. $\therefore \forall h \in H, eh = he = h$.

$\therefore H \leqslant G$. □

3.1.1 Special linear group

■ **Example 3.2** Let $H = \{A \in GL(2,\mathbb{R}) \mid \det(A) = 1\}$. Then $H \leqslant GL(2,\mathbb{R})$. (This subgroup is named $SL(2,\mathbb{R})$ the special linear group.) ■

Proof. We can prove this with the one-step subgroup test.

We have $H \subseteq GL(2,\mathbb{R})$ by definition of H. We have $H \neq \varnothing$ because $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$ and $\det(A) = 1$.

We want to show $\forall A,B \in H, AB^{-1}$. Let $A,B \in H$. So $A,B \in GL(2,\mathbb{R})$ and $\det(A) = 1 = \det(B)$.

Consider AB^{-1}. Since $GL(2,\mathbb{R})$ is a group, by inverse, $B^{-1} \in GL(2,\mathbb{R})$, then by closure, $AB^{-1} \in GL(2,\mathbb{R})$.

We can use determinant rules.

$$\begin{aligned}
\det(AB^{-1}) &= \det(A)\det(B^{-1}) && (3.3)\\
&= \det(A)\frac{1}{\det(B)} && (3.4)\\
&= 1 \cdot \frac{1}{1} \quad (A,B \in H) && (3.5)\\
&= 1 && (3.6)
\end{aligned}$$

$\therefore AB^{-1} \in H$, and by the one-step subgroup test, $H \leqslant GL(2,\mathbb{R})$. □

3.1.2 Cyclic subgroup

We have more examples of subgroups where we can use the subgroup test. Also, the following subgroup will be important.

Notation 3.1. $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, *where, in multiplicative notation*

- *if* $n > 0$, *then* $\underbrace{a^n = aaa\cdots a}_{n \text{ times}}$
- *if* $n = 0$, *then* $a^0 = e$
- *if* a^{-n}, *then* $a^{-|n|} = (a^{-1})^{|n|} = a^{-1}a^{-1}a^{-1}\cdots a^{-1}$

(In additive notation, $na = \underbrace{a+a+a+\cdots+a}_{n \text{ times}}$*.)*

Proposition 3.1.3 Let G be a group. Let $a \in G$. Then $\langle a \rangle$ is a subgroup of G.

Proof. We can apply the one-step subgroup test.
$\langle a \rangle \subseteq G$ by definition of $\langle a \rangle$ and G is a group (so $a^n \in G$ by closure).
$\langle a \rangle \neq \varnothing$ because $a \in G$.
Let $m, n \in \mathbb{Z}$. So $a^m, a^n \in \langle a \rangle$.
Consider $a^m (a^n)^{-1}$.

$$\begin{aligned}
a^m (a^n)^{-1} &= \underbrace{aaa\cdots a}_{|m| \text{ times}} \underbrace{(aaa\cdots a)^{-1}}_{|n| \text{ times}} && && (3.7)\\
&= \underbrace{aaa\cdots a}_{|m| \text{ times}} \underbrace{a^{-1}a^{-1}a^{-1}\cdots a^{-1}}_{|n| \text{ times}} && \text{(Shoes and socks theorem)} && (3.8)\\
&= a^m (a^{-1})^{|n|} && && (3.9)\\
&= a^{m-n} \in \langle a \rangle && m-n \in \mathbb{Z} && (3.10)\\
& && && (3.11)
\end{aligned}$$

$\therefore$ By the one-step subgroup test, $\langle a \rangle \leqslant G$. □

Definition 3.1.3 — Cyclic subgroup. [Gal17, page 65]
Let $a \in G$ and G be a group.
The subgroup $\langle a \rangle$ is called the *cyclic subgroup* generated by a.
If $\langle a \rangle = G$, then G is cyclic.

We use the term cyclic because of the way succesive powers cycle back to the original element. Look at the following example.

■ **Example 3.3** Consider $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$. Then $\langle 2 \rangle = \{2n \pmod 6 \mid n \in \mathbb{Z}\}$.

$$\begin{aligned}
2 &= 2 \pmod 6\\
2+2 &= 4 \pmod 6\\
2+2+2 &= 0 \pmod 6\\
2+2+2+2 &= 2 \pmod 6\\
2+2+2+2+2 &= 4 \pmod 6
\end{aligned}$$

and for $n \leq 0$,

$$\begin{aligned}
0 &= 0 \pmod 6\\
-2 &= 4 \pmod 6\\
(-2)+(-2) &= 2 \pmod 6
\end{aligned}$$

Then $\langle 2 \rangle = \{2,4,0\} < \mathbb{Z}_6$.
Note that $\langle 5 \rangle = \{0,1,2,3,4,5,6\} = \mathbb{Z}_6$. So $\mathbb{Z}_6$ is cyclic, generated by 5. See that $\langle 1 \rangle = \mathbb{Z}_6$ ■

R If a group is cyclic, its generator does not need to be unique.

Note cyclic groups do not need to have infinite order.

■ **Example 3.4** Consider $GL(2,\mathbb{R})$. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$. What is $\langle A \rangle$?

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \frac{1}{1}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

This leads to the claim, $\langle A \rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$. ■

We need to consider the natural numbers and the negative integers.

We can use induction to prove that $\langle A \rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{N} \right\}$.

BASE CASE: Let $n = 0$. Then $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

INDUCTION HYPOTHESIS: Let $k \in \mathbb{N}$. Assume $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$.

INDUCTION STEP: We want to show $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}$.

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} && \text{(Induction Hypothesis)} \\ &= \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

By principle of mathematical induction, $\langle A \rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$.

Now we want to show this holds for $n < 0$.

We can use induction to prove $\langle A \rangle = \left\{ \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{N} - \{0\} \right\}$.

BASE CASE: Let $n = 1$. Then $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$.

Exercise 3.2 Complete the proof for $\langle A \rangle = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$, in particular, the inductive step for negative integers.

3.1.3 Center of a group

Definition 3.1.4 — Center. [Gal17, page 66]
Let G be a group. The *center* of G, $Z(G)$, is

$$Z(G) = \{g \in G \mid xg = gx, \forall x \in G\}$$

that is, the set of elements that commute with every element of G.

Proposition 3.1.4 [Gal17, page 67]
Let G be a group. Then $Z(G) \leqslant G$.

Proof. We can prove this with the two-step subgroup test.

SUBSET: $Z(G) \subseteq G$ by definition of $Z(G)$.

NON-EMPTINESS: $Z(G) \neq \varnothing$ because $e \in G$ and $ex = xe = x, \forall x \in G$ by group axiom. $\therefore e \in Z(G)$.

CLOSURE: We want to show $\forall g_1, g_2 \in Z(G), g_1g_2 \in Z(G)$.
Let $g_1, g_2 \in Z(G)$. We know $g_1g_2 \in G$ by closure group axiom.
Now we need to show $\forall x \in G, (g_1g_2)x = x(g_1g_2)$.
Let $x \in G$.

$$\begin{aligned}
(g_1g_2)x &= g_1(g_2x) && \text{(Associativity)}\\
&= g_1(xg_2) && (g_2 \in Z(G))\\
&= (g_1x)g_2 && \text{(Associativity)}\\
&= (xg_1)g_2 && (g_1 \in Z(G))\\
&= x(g_1g_2) && \text{(Associativity)}
\end{aligned}$$

INVERSE: We want to show $\forall g \in Z(G), g^{-1} \in Z(G)$.
Let $g \in Z(G)$. We know $g^{-1} \in G$ by inverse group axiom.
Now we need to show $\forall x \in G, g^{-1}x = xg^{-1}$.
Let $x \in G$. We have $gx = xg$ since $g \in Z(G)$.

$$\begin{aligned}
gx = xg &\Rightarrow g^{-1}(gx)g^{-1} = g^{-1}(xg)g^{-1}\\
&\Rightarrow (g^{-1}g)xg^{-1} = g^{-1}x(gg^{-1}) && \text{(Associativity)}\\
&\Rightarrow e(xg^{-1}) = (g^{-1}x)e && \text{(Inverse)}\\
&\Rightarrow xg^{-1} = g^{-1}x && \text{(Identity)}
\end{aligned}$$

$\therefore$ By two-step subgroup test, $Z(G) \subseteq G$. □

Exercise 3.3 Find $Z(GL(2,\mathbb{R}))$.

Let $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(GL(2,\mathbb{R}))$, $x_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL(2,\mathbb{R})$ since $\det(x_1) \neq 0$. Then g commutes with x_1 iff:

$$gx_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix} \qquad x_1g = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

We need $gx_1 = x_1g$, so $\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$. Then $b = c$ and $a = d$.

Let $x_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$ since $\det(x_2) \neq 0$. Then g commutes with x_2 iff

$$gx_2 = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & a+b \\ b & b+a \end{bmatrix} \qquad x_1 g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ b & a \end{bmatrix} = \begin{bmatrix} a+b & b+a \\ b & a \end{bmatrix}$$

We need $gx_2 = x_2 g$, so $\begin{bmatrix} a & a+b \\ b & b+a \end{bmatrix} = \begin{bmatrix} a+b & b+a \\ b & a \end{bmatrix}$. Then $a = a+b \Rightarrow b = 0$.
$\therefore Z(GL(2,\mathbb{R})) \subseteq \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| \, a \neq 0, a \in \mathbb{R} \right\}$
Recall $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$.
Let $W := \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| \, a \neq 0, a \in \mathbb{R} \right\}$. To show $W \subseteq Z(GL(2,\mathbb{R}))$, let $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in W$.
Let $\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in Z(GL(2,\mathbb{R}))$.

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax & ay \\ az & aw \end{bmatrix} \qquad \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} ax & ay \\ az & aw \end{bmatrix}$$

Since $A \in W \Rightarrow A \in Z(GL(2,\mathbb{R}))$, $W \subseteq Z(GL(2,\mathbb{R}))$.
$\therefore Z(GL(2,\mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| \, a \neq 0, a \in \mathbb{R} \right\}$.

Exercise 3.4 Find $Z(SL(2,\mathbb{R}))$.

4. Cyclic Groups

4.1 Properties of Cyclic Groups

4.1.1 Order of Cyclic Groups

Recall from 3.1.3 the definition of a cyclic group.

Let G be a group. Let $a \in G$. If $G = \langle a \rangle$, then G is cyclic. We say a generates G.

■ **Example 4.1** $\mathbb{Z}$ is cyclic because $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. ■

Proposition 4.1.1 Let G be a group. Let $a \in G$ such that $|a| = n$.
(i) If $a^k = e$ for some $k \in \mathbb{Z}$, then $n \mid k$;
(ii) $|a| = |\langle a \rangle|$.

Proof. Let G be a group. Let $a \in G$ such that $|a| = n$.

(i) Suppose $a^k = e$ for some $k \in \mathbb{Z}$.
By division algorithm, $\exists q, r \in \mathbb{Z}, k = qn + r$ such that $0 \leq r < n$.
We know $a^k = e$, and $a^k = a^{qn+r}$.

$$\begin{aligned}
a^k &= a^{qn+r} \\
&= a^{qn}a^r \\
&= (a^n)^q a^r && \text{(Associativity)} \\
&= e^q a^r && (|a| = n) \\
&= ea^r = a^r && \text{(Identity)}
\end{aligned}$$

So $a^r = e$. But $|a| = n$. SS $r = 0$. Otherwise, we contradict definition of order. (Recall, $0 \leq r < n$.) Thus $k = qn + 0 = qn$.
$\therefore n \mid k$.

(ii) Consider $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$
Let $m \in \mathbb{Z}$.

By division algorithm, $\exists q, r \in \mathbb{Z}, m = qn + r$ such that $0 \leq r < n$.

$$\begin{aligned} a^m &= a^{qn+r} \\ &= a^{qn}a^r \\ &= (a^n)^q a^r && \text{(Associativity)} \\ &= e^q a^r && (|a| = n) \\ &= ea^r = a^r && \text{(Identity)} \end{aligned}$$

Hence $\langle a \rangle = \{e, a, a^2, a^3, \dots, a^{n-1}\}$. We need to show the elements of $\langle a \rangle$ are distinct. Assume $a^l = a^m$ for some $l, m \in \mathbb{Z}$. WLOG, $0 \leq m \leq l < n$. Since a^m is a group element, there exists inverse a^{-m}.

$$\begin{aligned} a^l = a^m &\Rightarrow a^l a^{-m} = a^m a^{-m} \\ &\Rightarrow a^{l-m} = e && \text{(Inverse)} \\ &\Rightarrow n \mid l - m && \text{(By 4.1.1(i), since } l - m \in \mathbb{Z}) \\ &\Rightarrow l - m = 0 && (l - m < n, |a| = n) \\ &\Rightarrow l = m \end{aligned}$$

$\therefore \{e, a, a^2, a^3, \dots, a^{n-1}\}$ has all distinct elements, and $|\langle a \rangle| = n = |a|$.

□

Exercise 4.1 Let a be an element of a group. Suppose $a^{180} = e$ and $a^{143} = e$. Prove $a = e$.

Proof. Suppose $|a| = n, n \in \mathbb{Z}^+$.

By 4.1.1, $n \mid 180$ and $n \mid 143$. But $\gcd(180, 143) = 1$ because $180 = 2^2 \cdot 3^2 \cdot 5$ and $143 = 11 \cdot 13$.

Then $n \mid gcd(180, 143)$, so $n = 1$, i.e., $|a| = 1$ and by uniqueness of identity, $a = e$. □

Theorem 4.1.2 [Gal17, page 78]

Let G be a group. Let $a \in G$ such that $|a| = n$. Let $k \in Z^+$.

(i) $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(ii) $|a^k| = \frac{n}{\gcd(n,k)}$

Proof. Let G be a group. Let $a \in G$ such that $|a| = n$. Let $k \in Z^+$. Also, let $d = \gcd(n, k)$.

(i) First, show $\langle a^k \rangle \subseteq \langle a^d \rangle$.

Consider $a^k \in \langle a^k \rangle$. (That is, we only consider the generator, since the rest of the cyclic subgroup can be obtained from it.)

By definition of d, we know $d \mid k$, i.e., $k = dq$ for some $q \in \mathbb{Z}$.

Then, using associativity, $a^k = a^{dq} = (a^d)^q \in \langle a^d \rangle$ by definition of $\langle a^d \rangle$.

$\therefore \langle a^k \rangle \subseteq \langle a^d \rangle$.

Now, show $\langle a^d \rangle \subseteq \langle a^k \rangle$.

Consider $a^d \in \langle a^d \rangle$. (Again, we only consider the generator.)

Since $d = \gcd(n,k)$, we may write $d = sn + kt$ for some $s,t \in \mathbb{Z}$.

$$\begin{aligned}
a^d &= a^{sn+kt} \\
&= a^{sn}a^{kt} \\
&= (a^n)^s a^{kt} && \text{(Associativity)} \\
&= e^s a^{kt} && (|a| = n) \\
&= ea^{kt} = a^{kt} && \text{(Identity)} \\
&= a^{k^t} \in \left\langle a^k \right\rangle && \text{(By definition of } \left\langle a^d \right\rangle\text{)}
\end{aligned}$$

$\therefore \left\langle a^d \right\rangle \subseteq \left\langle a^k \right\rangle$.
$\therefore \left\langle a^d \right\rangle = \left\langle a^k \right\rangle$.

(ii) We want to show $|a^k| = \frac{n}{d}$. (Note that $\frac{n}{d} \in \mathbb{Z}^+$ because $d \mid n$.)

$$\begin{aligned}
|a^k| &= |\left\langle a^k \right\rangle| && \text{(by 4.1.1(ii))} \\
&= |\left\langle a^d \right\rangle| && \text{(by 4.1.2(i))} \\
&= |a^d| && \text{(by 4.1.1(ii))}
\end{aligned}$$

Now we only need to show $|a_d| = \frac{n}{d}$.

$$\begin{aligned}
e &= a^n && \text{(|a| = n)} \\
&= (a^d)^{\frac{n}{d}} && (\tfrac{n}{d} \in \mathbb{Z}^+)
\end{aligned}$$

Then $|a^d| \leq \frac{n}{d}$.
Let $i \in Z^+$ such that $i \leq \frac{n}{d}$ and $(a^d)^i = e$.
Since $i \leq \frac{n}{d}$, $di \leq n$. Also, since $(a^d)^i = e$ and $|a| = n$ (so n is the smallest positive integer satisfying $a^n = e$), $n \leq di$.
Then $di = n \Leftrightarrow i = \frac{n}{d}$.
$\therefore |a^k| = |a^d| = \frac{n}{d}$.

□

Exercise 4.2 Let a be an element of a group. Let $|a| = 30$. Find $|a^{22}|$.

4.2 Subgroups of Cyclic Groups

4.2.1 Fundamental Theorem of Cyclic Groups

This next theorem helps us find subgroups of a cyclic group can have and how many there of them are.

Theorem 4.2.1 — Fundamental Theorem of Cyclic Groups. [Gal17, page 81]

(i) Every subgroup of a cyclic group is cyclic.

(ii) If $|\langle a \rangle| = n, n \in \mathbb{Z}^+$ and any $H \leqslant G$, then $|H| \Big| n$.

(iii) Let $n \in \mathbb{Z}^+$. Suppose $|a| = n$. For each positive divisor k of n, $\langle a \rangle$ has exactly one subgroup of order k. Namely, $\left\langle a^{n/k} \right\rangle$.

Often, we can use the division algorithm in a proof when working with integer multiples.

Proof. (i) Suppose $G = \langle a \rangle$ for some $a \in G$. Let $H \leqslant \langle a \rangle$.

If $H = \{e\}$, then done because $\{e\} = \langle e \rangle$.

If $H \neq \{e\}$, we want to show $\exists m \in \mathbb{Z}, H = \langle a^m \rangle$.

$H \leq \langle a \rangle \Rightarrow$ every element in H has the form $a^k, k \in \mathbb{Z}$.

By well-ordering, we can choose m to be least positive integer k so that $a^m \in H$.

First, we have $\langle a^m \rangle \subseteq H$ since $a^m \in H$ by choice of m and since H is closed.

Now, we show $H \subseteq \langle a^m \rangle$.

Let $a^k \in H$. By the division algorithm, $\exists q, r \in \mathbb{Z}, k = qm + r, 0 \leq r < m$.

$$\begin{aligned}
a^k &= a^{qm+r} \\
&= a^{qm}a^r && (*) \\
&= (a^m)^q a^r && \text{(Associativity)} \\
\Leftrightarrow a^r &= ((a^m)^q)^{-1} a^k && ((a^m)^q \in H, \text{ so its inverse exists}) \\
&= a^{-mq} a^k \\
&= \underbrace{(a^m)^{-q}}_{\in H} \underbrace{a^k}_{\in H} \\
\Leftrightarrow a^r &\in G && \text{(Closure of } H\text{)} \\
\Leftrightarrow r &= 0 && \text{(By supposition, } m \text{ is least positive integer)}
\end{aligned}$$

By $(*)$, $a^k = a^{qm}a^r$. Then $r = 0$ gives $a^k = a^{qm}a^0 = a^{qm}e = a^{qm} = (a^m)^q \in \langle a^m \rangle$ by definition of cyclic group generated by a^m.

$\therefore H \subseteq \langle a^m \rangle$.

$\therefore H = \langle a^m \rangle$.

(ii) Suppose $|\langle a \rangle| = n$. Let $H \leqslant \langle a \rangle$.

We know from the proof of (i), H is cyclic and $H = \langle a^m \rangle$ where m is the least positive integer such that $a^m \in H$. So $|H| = |\langle a^m \rangle|$.

By Proposition 4.1.1(ii) and Theorem 4.1.2(ii), $|H| = |a^m| = \frac{n}{\gcd(n,m)}$. Then $n = |H| \gcd(n,m)$.

$\therefore |H| \mid n$

(iii) Suppose $|\langle a \rangle| = n$. Let k be any positive divisor of n.

WLOG, suppose $H = \langle a^m \rangle$ has order k (using the same m as before).

We want to show $H = \langle a^{n/k} \rangle$.

By Theorem 4.1.1(i), $H = \langle m \rangle = \langle a^{\gcd(m,n)} \rangle$.

From the proof of (ii), $n = |H| \gcd(n,m) = k \gcd(n,m) \Rightarrow \gcd(n,m) = \frac{n}{k}$. So $H = \langle a^{\gcd(m,n)} \rangle = \langle a^{n/k} \rangle$.

Note this subgroup is unique because we chose m to be least positive integer.

□

Exercise 4.3 Prove uniqueness in 4.2.1(iii) by choosing two distinct examples and showing they are the same.

The following corollary is an example of FTOCG applied to a specific group $G = \mathbb{Z}_n$.

Corollary 4.2.2 [Gal17, page 82] For each positive divisor k of $n \in \mathbb{Z}^+$, the set $\langle \frac{n}{k} \rangle$ is a subgroup of $\mathbb{Z}_n$; moreover, the only subgroups of $\mathbb{Z}_n$ are these $\langle \frac{n}{k} \rangle$.

■ **Example 4.2** We want to find the subgroups of $\mathbb{Z}_{21}$ and their orders.

We know $\mathbb{Z}_2 1 = \langle 1 \rangle$ and $|\mathbb{Z}_{21}| = 21 < \infty$. Also, the positive divisors k of 21 are $\{1,3,7,21\}$. We can use Corollary 4.2.2 to get the following list of subgroups:

$$\left\langle \frac{21}{1} \right\rangle = \langle 21 \rangle = \{21k \pmod{21}\} = \{0\} \qquad \left| \left\langle \frac{21}{1} \right\rangle \right| = 1$$

$$\left\langle \frac{21}{3} \right\rangle = \langle 7 \rangle = \{0,7,14\} \qquad \left| \left\langle \frac{21}{3} \right\rangle \right| = 3$$

$$\left\langle \frac{21}{7} \right\rangle = \langle 3 \rangle = \{0,3,6,9,12,15,18\} \qquad \left| \left\langle \frac{21}{7} \right\rangle \right| = 7$$

$$\left\langle \frac{21}{21} \right\rangle = \langle 1 \rangle = \mathbb{Z}_{21} \qquad \left| \left\langle \frac{21}{21} \right\rangle \right| = 21$$

■

Definition 4.2.1 — Lattice Diagram. A *lattice diagram* is a diagram that represents the relationship between a group G and its subgroups, with each relation given by the set inclusion between two subgroups.

We put the biggest group at the top of the diagram and the trivial subgroup at the bottom. The other groups are arranged according to decreasing order in cardinality.

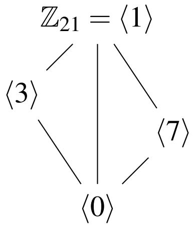


Figure 4.1: The lattice diagram of $\mathbb{Z}_{21}$

Exercise 4.4 Let G be a group. Let $a,b \in \mathbb{Z}_n$. Prove $\langle a \rangle \leqslant \langle b \rangle$ if $b \mid a$.

Exercise 4.5 Find all subgroups of $\mathbb{Z}_{45}$ and draw the lattice diagram.

5. Permutation Groups

5.1 Properties of Permutations

5.1.1 Symmetric Group

We've seen earlier $(\mathrm{Perm}(X), \circ)$ is a group. We also have the symmetric group S_n of degree n, $X = \{1, 2, \dots, n\}$. Its order is $|S_n| = n!$, and we use cycle notation to notate permutations.

5.1.2 k-cycle

Definition 5.1.1 — k-cycle. [Gal17, page 102] A *length k cycle* (or k-cycle) is an expression of the form $(a_1\ a_2\ \dots\ a_k)$ where $a_1, \dots, a_k$ are distinct elements in X, $k \le n$.

R A 2-cycle is also called a transposition.

■ **Example 5.1** $(1\ 2\ 3)$ has length 3, so it is a 3-cycle. ■

5.1.3 Disjoint Cycles

Definition 5.1.2 — Disjoint cycles. A pair of cycles $\alpha = (a_1\ a_2\ \dots\ a_k), \beta = (b_1\ b_2\ \dots\ b_k)$ are *disjoint* if $a_i \neq b_j, \forall i, j$, i.e., α and β have no common elements.

■ **Example 5.2** Let $\alpha = (1\ 2\ 3)$, $\beta = (7\ 10\ 1\ 21)$, and $\gamma = (4\ 6)$.

α and β are not disjoint because of 1.

γ and α are disjoint, and γ and β are disjoint. ■

■ **Example 5.3** Let $\alpha \in S_6$ such that $\alpha = (2\ 4\ 5)(6\ 1\ 2)(5\ 3\ 2\ 4)(4\ 5)$. We want to express α as a product of disjoint cycles.

We can consider each element one by one. For example, we see that $1 \mapsto 2 \mapsto 4$.

So $\alpha = (1436)(25)$ ■

We will have the following two theorems about the products of disjoint cycles, and we can use the former to prove the latter.

Theorem 5.1.1 [Gal17, page 99] Disjoint cycles commute; that is, if $\alpha, \beta \in S_n$ are disjoint, then $\alpha\beta = \beta\alpha$.

Proof. Let $\alpha, \beta \in S_n$.

WLOG, consider $\alpha = (a_1\ a_2\ \dots\ a_k), \beta = (b_1\ b_2\ \dots\ b_l)$ such that $a_i \neq b_j, \forall i, j$. (That is, they are disjoint.)

Note that $X = \{1, 2, \dots, n\}$ can be partitioned into

$$\{\ \underbrace{a_1, \dots, a_k}_{\text{fixed by only }\beta}\ ,\ \overbrace{b_1, \dots, b_l}^{\text{fixed by only }\alpha}\ ,\ \underbrace{c_1, \dots, c_s}_{\text{fixed by both }\alpha,\beta}\ \}$$

We want to show $\forall x \in X, (\alpha \circ \beta)(x) = (\beta \circ \alpha)(x)$.
Consider $a_i \in X$ fixed only by β.
By definition of β, $\alpha(\beta(a_i)) = \alpha(a_i)$. By definition of α, $\alpha(a_i) = a_{i+1}$.
By definition of α, $\beta(\alpha(a_i)) = \beta(a_{i+1})$. By definition of β, $\beta(a_{i+1}) = a_{i+1}$.
So $\alpha(\beta(a_i)) = \beta(\alpha(a_i))$
Consider $b_i \in X$ fixed only by α.
By definition of β, $\alpha(\beta(b_j)) = \alpha(a_{j+1})$. By definition of α, $\alpha(b_{j+1}) = b_{j+1}$.
By definition of α, $\beta(\alpha(b_j)) = \beta(b_j)$. By definition of β, $\beta(b_j) = b_{j+1}$.
So $\alpha(\beta(b_j)) = \beta(\alpha(b_j))$.
Consider $c_s \in X$ fixed by both α, β.
By definition of β, $\alpha(\beta(c_s)) = \alpha(c_s)$. By definition of α, $\alpha(c_s) = c_s$.
By definition of α, $\beta(\alpha(c_s)) = \beta(c_S)$. By definition of β, $\beta(c_s) = c_s$.
So $\alpha(\beta(c_s)) = \beta(\alpha(c_s))$.

□

Theorem 5.1.2 [Gal17, page 98] Every element in S_n is either a cycle or can be expressed uniquely (up to order) of disjoint cycles.

Proof. Let $\alpha \in S_n$.
If α is a cycle, nothing to prove.
Therefore, consider α which is not a single cycle. □

This proof is incomplete. We can use commutativity of disjoint cycles.

Exercise 5.1 Prove Theorem 5.1.2 by expanding out two cycles.

Theorem 5.1.3 [Gal17, page 100] Let $\alpha \in S_n$.

If α is written as a product of disjoint cycles, $\alpha = \alpha_1\alpha_2\cdots\alpha_m$, then $|\alpha| = \text{lcm}(\{l_1, l_2, \dots, l_m\})$, where l_i is the length of α_i.

Proof. If α is a cycle, then simple to prove by definition that $|\alpha|$ is its length.
Let $\alpha \in S_n$ be a product of disjoint cycles. Say $\alpha = \alpha_1\alpha_2\cdots\alpha_m$, and l_i is the length of α_i.

R Let $z \in \mathbb{Z}^+$. Since we have disjoint cycles, all α_i commute, and by repetitively commuting, we can rearrange.

$$\begin{aligned}\alpha^z &= \underbrace{\alpha\alpha\cdots\alpha}_{z \text{ times}}\\ &= \alpha_1\alpha_2\cdots\alpha_m\alpha_1\alpha_2\cdots\alpha_m\cdots\alpha_1\alpha_2\cdots\alpha_m\\ &= \alpha_1^z\alpha_2^z\cdots\alpha_m^z\end{aligned}$$

We know $\exists k \in \mathbb{Z}^+$ such that $\alpha^k = (1)$ because $|S_n| < \infty$.

Consider that $\alpha^k = \alpha_1^k\alpha_2^k\cdots\alpha_m^k = (1)$. So, we get that $\alpha_i^k = (1)$ since all α_i is disjoint. (If $\gamma\beta = (1)$ then $\gamma = \beta^{-1}$. But then γ and β would not be disjoint, which is a contradiction.)

Recall $|\alpha_i| = l_i$, so $\alpha_i^{l_i} = (1)$.

For each i, since we have $\alpha_i^k = (1)$ and $\alpha_i^{l_i} = (1)$, by Proposition 4.1.1(i), each k is a multiple of l_i (i.e., $l_i \mid k$).

Recall the lowest common multiple of $a, b \in \mathbb{Z}^+$ is the smallest integer which is divided by a and b.

$\therefore$ Choose $|\alpha| = \operatorname{lcm}(\{l_1, l_2, \ldots, l_m\})$. □

■ **Example 5.4** We can use Theorem 5.1.3 find an element of order 10 in S_7.

Consider $\alpha \in S_7$ such that α is a product of a 2-cycle and a 5-cycle which are disjoint. For example, $\alpha = (1\,2\,3\,4\,5)(6\,7)$ ■

5.1.4 Cycle type

Definition 5.1.3 — Cycle type. Let $\alpha \in S$. Let $\alpha = \alpha_1\cdots\alpha_m$ be expressed as a product of disjoint cycles. Let l_i be the length of α_i for each i.

The *cycle type* of α is a list in decreasing order of each l_i of α.

Denote $d = (l_a, \ldots l_i, l_j, \ldots l_b)$ where $l_i \geq l_j$.

Note these are just the partitions of the set, or alternatively, the different ways you can sum to an integer.

■ **Example 5.5** The cycle types of S_4 are:

Cycle type	Example of cycle with given cycle type
(4)	(1 2 3 4)
(3,1)	(1 2 3)(4)
(2,2)	(1 2)(3 4)
(2,1,1)	(1 2)(3)(4)
(1,1,1,1)	(1)(2)(3)(4)

■

Exercise 5.2 Write out the elements of S_4 for each of its cycle types.

■ **Example 5.6** We can use cycle types to count the number of elements in S_7 of order 10 as in Example 5.4.

Only the cycles of type $(5,2)$ have order 10 since $\operatorname{lcm}(\{5,2\}) = 10$.

So we need a 5-cycle. There are $\binom{7}{5}$ cycles of length 5 of 7 elements and $\frac{5!}{5}$ ways to arrange these elements. (We divide to avoid reptition, since first number of cycle is arbitrary.)

Now we need a disjoint 2-cycle. So we have $\binom{2}{2}$ cycles of length 2 with the 2 remaining elements and $\frac{2!}{2}$ ways to arrange the 2 elements.

Then we have $\binom{7}{5}\frac{5!}{5}\binom{2}{2}\frac{2!}{2} = 504$ elements in S_7 of order 10. ■

Theorem 5.1.4 [Gal17, page 102] Every element of S_n for $n > 1$ can be expressed as a product of transpositions.

R This product need not be unique or disjoint.

Proof. Let $\alpha \in S_n, n > 1$.

For the identity, we have $(1) = (1\ 2)(1\ 2)$. (Note $(1\ 2) \in S_n$ since $n > 1$.)

WLOG, suppose $\alpha = (a_1\ \cdots\ a_r)(b_1\ \cdots\ b_s)$ is a product of 2 disjoint cycles.

Then $\alpha = (a_1\ a_r)(a_1\ a_{r-1})(a_1\ a_{r-2})\cdots(a_1\ a_2)(b_1\ b_s)(b_1\ b_{s-1})(b_1\ b_{s-2})\cdots(b_1\ b_s)$.

Notice that each individual disjoint cycle is decomposed the same way, independently. □

■ **Example 5.7** We can decompose $(1\ 2\ 3\ 4\ 5)$ as $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$. Note this isn't unique, for example, $(1\ 2\ 3\ 4\ 5) = (4\ 5\ 1\ 2\ 3) = (4\ 3)(4\ 2)(4\ 1)(4\ 5)$.

Another example is $(4\ 6\ 1\ 2)(3\ 7\ 5) = (4\ 2)(4\ 1)(4\ 6)(3\ 5)(3\ 7)$. ■

5.1.5 Parity of a permutation

Definition 5.1.4 — Parity of a permutation. [Gal17, page 104] Let $\alpha \in S_n$.

The permutation α is *even* if there are an even number of transpositions in its 2-cycle decomposition, and α is *odd* otherwise (i.e., it has an odd number of transpositions).

■ **Example 5.8** Consider the examples in Example 5.7.

We have that $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$ is even.

However, $(4\ 6\ 1\ 2)(3\ 7\ 5) = (4\ 2)(4\ 1)(4\ 6)(3\ 5)(3\ 7)$ is odd. ■

5.1.6 Alternating group

Definition 5.1.5 — Alternating group. [Gal17, page 104] The set $A_n = \{\alpha \in S_n \mid \alpha \text{ is even}\}$ is called the *alternating group* of degree n.

Theorem 5.1.5 $A_n \leqslant S_n$ for $n > 1$.

Note that the subset of odd permutations is not a subgroup. It does not satisfy closure, and it does not have the identity (since $(1) = (1\ 2)(1\ 2)$).

Exercise 5.3 Prove that A_n is a subgroup of S_n for $n > 1$, $A_n \leqslant S_n$.

We can use one of the subgroup tests for this.

Also, we can now consider the parity of not just cycles but of cycle types.

■ **Example 5.9** We want to find the parity of each cycle type in S_4.

We can do this since each cycle type has the same structure. For example, $(1\ 2\ 3\ 4)$ which is cycle type (4) is odd. All cycles with the same cycle type can be decomposed the same way.

Cycle type	Parity
(4)	Odd
(3,1)	Even
(2,2)	Even
(2,1,1)	Odd
(1,1,1,1)	Even

■

Half of the elements in S_n are even permutations.

Theorem 5.1.6 [Gal17, page 104] $A_n = \frac{n!}{2}, n > 1$

We can prove this by showing a bijection between the even and odd permutations.

Proof. Let $E = \{\text{Even permutations in } S_n\}$ (note $E = A_n$) and $O = \{\text{Odd permutations in } S_n\}$. Consider $H : E \to O$, $\alpha \mapsto \alpha(1\ 2)$.

We want to show H is a bijection.

First, we show H is injective.

Suppose $H(\alpha) = H(\beta)$ for any $\alpha, \beta \in E$. That is, $\alpha(1\ 2) = \beta(1\ 2)$. By right cancellation law, $\alpha = \beta$.

Then, we show H is surjective.

We can show this by construction. Consider $\beta \in O$. Then $\beta(1\ 2)$ is even.

So H is bijective. So $|E| = |O|$. Also $S_n = E \sqcup O$.

$|S_n| = |A_n| + |O| = |A_n| + |A_n| = 2|A_n|$.

$\therefore |A_n| = \frac{n!}{2}$. □

6. Homomorphisms and Isomorphisms

6.1 Introduction to Homomorphisms and Isomorphisms

6.1.1 Homomorphism and Isomorphism

As motivation for homomorphisms and isomorphisms, consider a matrix group

$$N = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \middle| \, b \in \mathbb{R} \right\} \tag{6.1}$$

under matrix multiplication. (We could prove this is a group by showing it is a subgroup of $GL(2,\mathbb{R})$.)

Now what happens when do the group operation? We get the following:

$$\begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{bmatrix} \in N \tag{6.2}$$

This looks just like the group $\mathbb{R}$ under addition.

We can define a map $\phi : (\mathbb{R},+) \to (N,\cdot)$ such that $b \mapsto \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Then with this map, we could show that $\phi(b_1 + b_2) = \phi(b_1)\phi(b_2)$. On the left hand side, we have addition, the operation on $\mathbb{R}$, and on the right hand side, we have matrix multiplication, the operation on N. This is an example of a homomorphism.

Definition 6.1.1 — Homomorphism. Let $G, \overline{G}$ be groups.

A map $\phi : G \to \overline{G}$ that satisfies $\phi(ab) = \phi(a)\phi(b)$, $\forall a,b \in G$ is a *homomorphism*.

R In the definition of a homomorphism, on the left hand side, we have the operation of G, and on the right hand side, we have the operation of $\overline{G}$.

Definition 6.1.2 — Isomorphism. A homomorphism that is also bijective is an *isomorphism.*

We can consider an isomorphism as a renaming of the group since the two groups have the exact same structure.

Notation 6.1. *We say that G is isomorphic to $\overline{G}$ if there is an isomorphism between them. This can be denoted as:*

- $G \approx \overline{G}$ *(This is used in [Gal17])*
- $G \simeq \overline{G}$ *(This is the most commonly used)*
- $G \cong \overline{G}$

6.1.2 Examples of Homomorphisms and Isomorphisms

■ **Example 6.1** Let $G, \overline{G}$ be groups.

The map $\phi : G \to \overline{G}$ defined by $\phi(g) = \overline{e}, \forall g \in G$ (where $\overline{e}$ is the identity in $\overline{G}$) a homomorphism called the trivial homomorphism. ■

Proof. We want to show $\forall g_1, g_2 \in G, \phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

Let $g_1, g_2 \in G$.

Since $g_1 g_2 \in G$ by closure, $\phi(g_1 g_2) = \overline{e}$ by definition of ϕ.

Then $\phi(g_1 g_2) = \overline{e} = \overline{e} \cdot \overline{e} = \phi(g_1)\phi(g_2)$. □

■ **Example 6.2** Let G be a group.

The map $\phi : G \to G$ defined by $\phi(g) = g, \forall g \in G$ is a homomorphism, called the identity homomorphism.

In fact, ϕ is bijective, so it's an isomorphism, called the trivial isomorphism. ■

Exercise 6.1 Prove Example 6.2 is a homomorphism.

■ **Example 6.3** Let G be a group and let $H \leqslant G$.

The map $\phi : H \hookrightarrow G$ defined by $\phi(h) = h, \forall h \in H$ is a homomorphism, called the inclusion homomorphism. ■

Exercise 6.2 Prove Example 6.3 is a homomorphism.

Now let's show how to disprove whether a map is a homomorphism.

■ **Example 6.4** Define $\phi\ GL(2,\mathbb{R}) \to GL(2,\mathbb{R})$ defined by $\phi(A) = A^2$.

Is this a homomorphism?

No, it is not a homomorphism. Consider $\phi(AB) = (AB)^2 = ABAB$, while $\phi(A)\phi(B) = A^2B^2$. We know that matrix multiplication is not necessarily commutative.

We just need a counterexample to show this is not a homomorphism. Consider $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. First, show membership. These are 2×2 real matrices, but we need to show they are invertible to be in $GL(2,\mathbb{R})$. They both have determinant 1 which is nonzero so they are both invertible.

After computing the matrix multiplication, we get $\phi(AB) = ABAB = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$ and $\phi(A)\phi(B) =$

$AABB = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$. So the map does not satisfy the definition of a homomorphism. ■

Definition 6.1.3 [Gal17, page 194] Let $G, \overline{G}$ be groups. Let $\phi : G \to \overline{G}$ be a homomorphism. The set $\ker \phi = \{ g \in G \mid \phi(g) = \overline{e} \}$ is the *kernel* of ϕ.

From this definition, we get that the kernel of a homomorphism is a subgroup.

Proposition 6.1.1 [Gal17, page 197] Let $G, \overline{G}$ be groups. Let $\phi : G \to \overline{G}$ be a homomorphism. Then $\ker(\phi) \leqslant G$.

Proof. We can use one-step subgroup test.

SUBSET: $\ker(\phi) \subseteq G$ by definition.

NON-EMPTINESS: $\phi(e) = \overline{e}$ so $e \in \ker(\phi)$. So $\ker(\phi) \neq \varnothing$.

We need to show why $\phi(e) = \overline{e}$.

Consider $\phi(e)$.

$$\begin{aligned} \phi(e) &= \phi(e \cdot e) && (e \text{ is identity in } G) \\ &= \phi(e)\phi(e) && (\phi \text{ is a homomorphism}) \end{aligned}$$

But also, $\phi(e) = \overline{e} \cdot \phi(e)$ since $\overline{e}$ is identity in $\overline{G}$.

Since we have $\overline{e} \cdot \phi(e) = \phi(e) = \phi(e)\phi(e)$, we can use the right cancellation law to get $\overline{e} = \phi(e)$.

CLOSURE WITH INVERSE: We want to show $g_1 g_2^{-1} \in \ker(\phi), \forall g_1, g_2 \in \ker(\phi)$.

Let $g_1, g_2 \in \ker(\phi)$.

Consider $g_1 g_2^{-1}$. Since G is a group and $g_1, g_2 \in G$, $g_1 g_2^{-1} \in G$.

We need some information about the inverse g_2^{-1} in the kernel. Consider $\phi(e) = \overline{e}$. Then $\phi(e) = \phi(g_2 g_2^{-1}) = \phi(g_2)\phi(g_2^{-1}) = \overline{e}$. Since $g_2 \in \ker(g_2^{-1})$, $\phi(g_2) = \overline{e}$. So $\phi(e) = \overline{e} \cdot \phi(g_2^{-1}) = \overline{e}$. $\therefore \phi(g_2^{-1}) = \overline{e}$ $(*)$.

Consider $\phi(g_1 g_2^{-1})$.

$$\begin{aligned} \phi(g_1 g_2^{-1}) &= \phi(g_1)\phi(g_2^{-1}) && (\phi \text{ is a homomorphism}) \\ &= \overline{e}\phi(g_2^{-1}) && (g_1 \in \ker(\phi)) \\ &= \phi(g_2^{-1}) && (\text{Identity}) \\ &= \overline{e} && (\text{By } (*)) \end{aligned}$$

So $g_1 g_2^{-1} \in \ker(\phi)$.

By the one-step subgroup test, $\therefore \ker(\phi) \leqslant G$. □

6.2 Properties of Homomorphisms

Theorem 6.2.1 [Gal17, page 196]

Let $G, \overline{G}$ be groups. Let $\phi : G \to \overline{G}$ be a homomorphism.

(i) $\phi(e) = \overline{e}$;

(ii) $\phi(g^n) = (\phi(g))^n, \forall g \in G, n \in \mathbb{Z}$;

(iii) If $|g| < \infty$, then $|\phi(g)| \mid |g|$;
(iv) ϕ is injective iff $\ker(\phi) = \{e\}$.

Proof. (i) We did this in the proof of Proposition 6.1.1

(ii) Let $g \in G, n \in \mathbb{Z}$
First, consider $n > 0$.

$$\begin{aligned}\phi(g^n) &= \phi(\underbrace{g \cdot g \cdots g}_{n \text{ times}}) \\ &= \underbrace{\phi(g) \cdot \phi(g) \cdots \phi(g)}_{n \text{ times}} && \text{(Associativity, } \phi \text{ is a homomorphism)} \\ &= (\phi(g))^n\end{aligned}$$

When $n = 0$, we can use (i) to get $\phi(g^0) = \phi(e) = \overline{e} = (\phi(g))^0$.
Then, consider $n < 0$.

$$\begin{aligned}\phi(g^{-n}) &= \phi(\underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}) \\ &= \underbrace{\phi(g^{-1}) \cdot \phi(g^{-1}) \cdots \phi(g^{-1})}_{n \text{ times}} && \text{(Associativity, } \phi \text{ is a homomorphism)} \\ &= (\phi(g^{-1}))^{|n|}\end{aligned}$$

We need to simplify $\phi(g^{-1})$. We know $\phi(e) = \overline{e}$. Using the inverse axiom and the definition of ϕ, we get $\phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = \overline{e}$.

$$\begin{aligned}&\phi(g)\phi(g^{-1}) = \overline{e} \\ \Leftrightarrow\ &(\phi(g))^{-1}(\phi(g)\phi(g^{-1})) = (\phi(g))^{-1} \cdot \overline{e} \\ \Leftrightarrow\ &\overline{e} \cdot \phi(g^{-1}) = (\phi(g))^{-1} && \text{(by } \overline{G} \text{ definition)} \\ \Leftrightarrow\ &\phi(g^{-1}) = (\phi(g))^{-1},\end{aligned}$$

Then we have that $\phi(g^{-1}) = (\phi(g))^{-1}$ $(**)$ which we can use to simplify $\phi(g^{-n})$ further.

$$\begin{aligned}\phi(g^{-n}) &= (\phi(g^{-1}))^{|n|} \\ &= ((\phi(g))^{-1})^{|n|} && \text{(By } (**)) \\ &= \underbrace{(\phi(g))^{-1} \cdot (\phi(g))^{-1} \cdots (\phi(g))^{-1}}_{n \text{ times}} \\ &= (\phi(g))^{-|n|} \\ &= (\phi(g))^n && (n < 0 \text{ in this case})\end{aligned}$$

$\therefore \phi(g^n) = (\phi(g))^n$.

(iii) Let $g \in G$.
Suppose $|g| = n < \infty$ for some $n \in Z^+$.
We want to show $|\phi(g)| \mid |g|$.
Consider $(\phi(g))^n$.

$$\begin{aligned}(\phi(g))^n &= \phi(g^n) && \text{(by (ii))} \\ &= \phi(e) && (|g| = n) \\ &= \overline{e} && \text{(by (i))}\end{aligned}$$

Proposition 4.1.1(i) states if $|a| = n < \infty, a^k = e, k \in Z^+$, then $n \mid k$.
Note we have $(\phi(g))^n = e$. So using 4.1.1, we get $|\phi(g)| \mid n$.

(iv) We want to show ϕ is injective $\Leftrightarrow \ker(\phi) = \{e\}$.
First, we show ϕ is injective $\Rightarrow \ker(\phi) = \{e\}$.
Suppose ϕ is injective. We know $\overline{e} \in \overline{G}$. By (i), $\phi(e) = \overline{e}$. By injectivity, e is the only element that maps to $\overline{e}$. $\therefore \ker(\phi) = \{e\}$
Then, we show $\ker(\phi) = \{e\} \Rightarrow \phi$ is injective.
Suppose $\ker(\phi) = \{e\}$. Assume $\phi(a) = \phi(b)$ for any $a, b \in G$.

$$\begin{aligned} &\phi(a) = \phi(b) \\ \Leftrightarrow\ &(\phi(a))^{-1}\phi(a) = (\phi(a))^{-1}\phi(b) && (\overline{G} \text{ is a group}) \\ \Leftrightarrow\ &\overline{e} = \phi(a^{-1})\phi(b) && (\text{Inverse, (ii)}) \\ \Leftrightarrow\ &\overline{e} = \phi(a^{-1}b) && (\phi \text{ is a homomorphism}) \end{aligned}$$

Then by definition of $\ker(\phi)$, $a^{-1}b \in \ker(\phi) = \{e\}$. So $a^{-1}b = e$. When we multiply a on the left on both sides and simplify by properties of G, we get $b = a$. $\therefore \phi$ is injective.
$\therefore \phi$ is injective $\Leftrightarrow \ker(\phi) = \{e\}$

□

R These properties remain true for isomorphism because an isomorphism is a homomorphism.

6.3 Image of Homomorphism

Definition 6.3.1 — Image of a homomorphism. [Gal17, page 197] Let $G, \overline{G}$ be groups. Let $\phi : G \to \overline{G}$ be a homomorphism. Let $H \leqslant G$.

The set $\phi(H) = \{\,\phi(h) \mid h \in H\,\} \subseteq \overline{G}$ is called the *image of H under ϕ*.

Theorem 6.3.1 — Homomorphism image properties. [Gal17, page 197]
Let $G, \overline{G}$ be groups. Let $\phi : G \to \overline{G}$ be a homomorphism. Let $H \leqslant G$.

(i) $\phi(H) \leqslant \overline{G}$;
(ii) If H is cyclic then $\phi(H)$ is cyclic;
(iii) If H is abelian then $\phi(H)$ is abelian.

Exercise 6.3 Prove Theorem 6.3.1.

While an isomorphism is a homomorphism, it also has stronger properties that apply. For example, Theorem 6.3.1(ii) and (iii) become biconditional statements if ϕ is an isomorphism.

Theorem 6.3.2 — Isomorphism image properties. [Gal17, page 127]
Let $G, \overline{G}$ be groups. Let $\phi : G \to \overline{G}$ be an isomorphism. Let $H \leqslant G$.

(i) H is cyclic iff $\phi(H)$ is cyclic;
(ii) H is abelian iff $\phi(H)$ is abelian.

Exercise 6.4 Prove Theorem 6.3.2.

■ **Example 6.5** $\mathbb{Z}_6 \not\approx D_3$. ■

There are many ways to prove this by showing some group-theoretic property is not satisfied by both group.

Proof. $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ is cyclic because $\langle 1 \rangle = \{n1 \pmod 6 \,|\, n \in .\!\because\!. \nexists g \in D_3$ such that $D_3 = \langle g \rangle$.

$\therefore D_3$ is not cyclic.

By negation of Theorem 6.3.2(i), $\mathbb{Z}_6 \not\cong D_3$. □

We can prove this by contradiction of the definition of an isomorphism, but this is generally harder than using one of the properties. We can also use Theorem 6.3.2(ii), but we have to show Z_6 abelian, which we can show by direct computation (e.g. Cayley table).

Theorem 6.3.3 — Cayley's Theorem. [Gal17, page 124]

Let G be a group.

If $|G| < \infty$, then G is isomorphic to a subgroup of S_n for some $n \in \mathbb{Z}_{\geq 0}$.

Proof. Suppose G is a finite group, say $|G| = n$ for some $n \in \mathbb{Z}^+$.

Let X be the set in G (the finite collection of elements ignoring the binary operation). We know $\mathrm{Perm}(X) = \{f \mid f : X \to X \text{ bijective}\}$ is a group under composition. (We will use the notation $S_X = \mathrm{Perm}(X)$.)

Define $\phi : G \to S_X$ as $g \mapsto T_g$ where $T_g \in S_X$ is $T_g(x) = gx, \forall x \in X$.

We claim ϕ is an injective homomorphism.

Let $g_1, g_2 \in G$.

Consider $x \in X$. Then we have:

$$\begin{aligned}
\phi(g_1g_2) &= T_{g_1g_2} && \text{(By definition of } \phi\text{)}\\
&= (g_1g_2)x && \text{(By definition of } T_g\text{)}\\
&= g_1(g_2x) && \text{(Associativity)}\\
&= T_{g_1}(g_2x) && \text{(By definition of } T_g\text{)}\\
&= T_{g_1}(T_{g_2}(x)) && \text{(By definition of } T_g\text{)}\\
&= T_{g_1} \circ T_{g_2} && \\
&= \phi(g_1)\phi(g_2) && \text{(By definition of } \phi\text{)}
\end{aligned}$$

$\therefore \phi$ is a homomorphism.

Recall that ϕ is injective is equivalent to $\ker(\phi) = \{e\}$.

$$\begin{aligned}
\ker(\phi) &= \{g \in G \mid \phi(g) = \bar{e}\} && \text{(By definition of } \ker(\phi)\text{)}\\
&= \{g \in G \mid T_g(x) = T_e(x), \forall x \in X\} && \text{(By definition of } \phi\text{)}\\
&= \{g \in G \mid gx = ex\} && \text{(By definition of } T_g\text{)}\\
&= \{g \in G \mid g = e\} = \{e\} && \text{(Right cancellation law)}
\end{aligned}$$

$\therefore \phi$ is injective.

Relabel the elements of X to $\{1,2,3,\dots,n\}$. Notice S_X is S_n after relabeling.

To get an isomorphism, we need to show surjectivity.

Let's restrict the range ϕ such that we have $\phi : G \to \phi(G)$, that is, we only consider the codomain as the range of ϕ. Then we automatically get surjectivity.

$\therefore \phi$ is bijective.

$\therefore \phi$ is an isomorphism and $\phi(G) = S_n$. □

Proposition 6.3.4 Let $G, \overline{G}$ be groups. Suppose $|G| < \infty$. Let $\phi : G \to \overline{G}$ be an isomorphism.

Then for any $n \in \mathbb{Z}^+$, the number of elements in G of order n is equal to the number of elements in $\overline{G}$ of order n.

Proof. Let $G, \overline{G}$ be groups. Suppose $|G| < \infty$. Let $\phi : G \to \overline{G}$ be an isomorphism.

Let $n \in \mathbb{Z}^+$. Let $g \in G$ with $|g| = n$.

By Theorem 6.2.1(iii), $|\phi(g)| \mid n$.

Suppose $|\phi(g)| = k$ for some $k \in \mathbb{Z}^+$ (that is, $(\phi(g))^k = \overline{e}$).

If we show $n \mid k$ then $n = k$.

By Theorem 6.2.1(ii), $(\phi(g))^k = \phi(g^k)$. Then $\phi(g^k) = \overline{e}$. By definition of $\ker(\phi)$ and since ϕ is injective (since it is an isomorphism), $g^k \in \ker(\phi) = \{e\}$. So $g^k = e$.

Since $g^k = e$ and $|g| = n$, by Proposition 4.1.1(i), $n \mid k$.

$n \mid k$ and $k \mid n$. $\therefore |g| = |\phi(g)|$.

We can show the number of elements with the same order are the same in G and $\overline{G}$ by defining a map $F : \{g \in G \mid |g| = n\} \to \left\{\overline{g} \in \overline{G} \mid |\overline{g}| = n\right\}$ such that $g \mapsto \phi(g)$.

Since ϕ is an isomorphism, it is a bijection. So F is a bijection. $\therefore |\{g \in G \mid |g| = n\}| = \left|\left\{\overline{g} \in \overline{G} \mid |\overline{g}| = n\right\}\right|$. □

■ **Example 6.6** Consider $\langle i \rangle \leqslant \mathbb{C}^x$. Then $\langle i \rangle = \mathbb{Z}_4$. ■

Since these two groups are small, we can define an isomorphism pointwise.

Definition 6.3.2 — Quaternion group. The *quaternion group* is $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\} \leqslant GL(2, \mathbb{C}^x)$ where

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

$$I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

$$K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

Consider $D_4 = \left\{ \langle r, s \rangle \mid r^4 = e, s^2 = e, srs^{-1} = r^{-1} \right\}$. This is a group presentation. The first part is the generators of the group and the second part is the relations. We can consider r is the counter-clockwise rotation by 90 degrees and s is the vertical reflection. Then we have $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$.

We can use Proposition 6.3.4 to prove the following.

■ **Example 6.7** $Q_8 \not\cong D_4$. ■

Note we can use the relations to directly compute order. For example, $|r| = 4$ because $r^4 = e$ and $|r^2| = 2$ because $(r^2)^2 = r^4 = e$.

$g \in D_4$	$\lvert g \rvert$
e	1
r	4
r^2	2
r^3	4
s	2
rs	2
r^2s	2
r^3s	2

Table 6.1: Order of elements in D_4

$g \in Q_8$	$\lvert g \rvert$
1	1
-1	2
I	4
$-I$	4
J	4
$-J$	4
K	4
$-K$	4

Table 6.2: Order of elements in Q_8

Proof. Consider elements of order 4. By Figure 6.1, D_4 has 2 and by Figure 6.2, Q_8 has 6. $\therefore$ By negation of Proposition 6.3.4, $D_4 \not\cong Q_8$. □

R Proposition 6.3.4 is not biconditional, i.e., you cannot state two groups are isomorphic because they have the same number of elements of the same order.

6.4 Automorphisms

Definition 6.4.1 — Automorphism. [Gal17, page 128] Let G be a group. An *automorphism* is an isomorphism ϕ from G to itself.

■ **Example 6.8** $\phi : GL(2, \mathbb{R}) \to GL(2, \mathbb{R})$ where $A \mapsto (A^{-1})^T$ is an automorphism. ■

Proof. Note the domain and range are both $GL(2, \mathbb{R})$. So we want to show ϕ is an isomorphism.

HOMOMORPHISM Let $A, B \in GL(2, \mathbb{R})$.

$$\begin{aligned}
\phi(AB) &= ((AB)^{-1})^T && \text{(Definition of } \phi\text{)} \\
&= (B^{-1}A^{-1})^T && \text{(Socks-shoes)} \\
&= (A^{-1})^T (B^{-1})^T && ((CD)^T = D^T C^T) \\
&= \phi(A)\phi(B) && \text{(Definition of } \phi\text{)}
\end{aligned}$$

INJECTIVE We know injectivity is equivalent to a trivial kernel.

$$\begin{aligned}
\ker(\phi) &= \{g \in G \mid \phi(g) = \bar{e}\} \\
&= \left\{A \in GL(2,\mathbb{R}) \mid (A^{-1})^T = I\right\}
\end{aligned}$$

$$\Rightarrow \ (A^{-1})^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\Rightarrow ((A^{-1})^T)^T = A^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad ((C^T)^T = C)$$

$$\Rightarrow (A^{-1})^{-1} = A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad ((g^{-1})^{-1} = g)$$

SURJECTIVE Let $B \in GL(2,\mathbb{R})$.

Choose $A = (B^T)^{-1}$. First, this is a 2×2 real matrix. Also, $\det(A) = \det((B^T)^{-1}) = \frac{1}{\det(B^T)} = \frac{1}{\det(B)} \neq 0$ since $B \in GL(2,\mathbb{R})$. So $A \in GL(2,\mathbb{R})$ (the domain).

Now $\phi(A) = \phi\left((B^T)^{-1}\right) = \left(((B^T)^{-1})^{-1}\right)^T = (B^T)^T = B$.

□

Theorem 6.4.1 — Automorphism Group. [Gal17, page 129] Let G be a group. The set of all automorphisms in G is $\text{Aut}(G) = \{\,\phi \mid \phi$ is an automorphism of $G\}$ together with composition is a group called the *automorphism group of G*.

We want to show $\text{Aut}(G), \circ$ is a group, which means it satisfies the following axioms:

NONEMPTINESS	Identity
CLOSURE	Under composition, show $fg \in \text{Aut}(G)$
ASSOCIATIVITY	$(fg)h = f(gh)$
IDENTITY	$ef = fe = f$
INVERSE	$f^{-1}f = ff^{-1} = e$

■ **Example 6.9** Consider $\mathbb{Z}_4 = \{0,1,2,3\}$. We want to find the automorphisms of $\mathbb{Z}_4$. Note that $0 \mapsto 0$ since an identity must map to an identity. Also note that $|2| = 2$ and is the only element of order 2, so $2 \mapsto 2$, while $|3| = |1| = 4$.

$$\begin{aligned}
\phi_1 : \mathbb{Z}_4 &\to \mathbb{Z}_4 \\
0 &\mapsto 0 \\
1 &\mapsto 1 \\
2 &\mapsto 2 \\
3 &\mapsto 3 \\
\phi_3 : \mathbb{Z}_4 &\to \mathbb{Z}_4 \\
0 &\mapsto 0 \\
1 &\mapsto 3 \\
2 &\mapsto 2 \\
3 &\mapsto 1
\end{aligned}$$

These are all such maps because other assignments to elements would map homomorphism properties. ■

$\circ$	ϕ_1	ϕ_3
ϕ_1	ϕ_1	ϕ_3
ϕ_3	ϕ_3	ϕ_1

Table 6.3: Cayley table for $(\mathrm{Aut}(\mathbb{Z}_4), \circ)$

$\cdot \pmod 4$	1	3
1	1	3
3	3	1

Table 6.4: Cayley table for $(U(4), \cdot \pmod 4)$

Note the structure of Table 6.3 and 6.4. We can create an isomorphism from these two groups.

Exercise 6.5 Prove $\mathrm{Aut}(\mathbb{Z}_4) \simeq U(4)$.

This generalizes to the following theorem.

Theorem 6.4.2 [Gal17, page 131] $\mathrm{Aut}(\mathbb{Z}_n) \simeq U(n)$

We will investigate how we would make the connection between the two groups. Let $\phi \in \mathrm{Aut}(\mathbb{Z}_n), \phi : \mathbb{Z}_n \to \mathbb{Z}_n$.

Consider $\phi(k), k \in \mathbb{Z}_n, k \neq 0$. We know $\phi(k) = \phi(\sum_k 1) = \sum_k \phi(1) = k\phi(1)$ since ϕ is a homomorphism. So ϕ is completely determined by $\phi(1)$. Also $\forall k \in \{1, 2, \dots, n-1\}, \phi(k) = k\phi(1) \neq 0$ because $\phi(0) = 0$ and ϕ is injective.

This implies that $\gcd(\phi(1), n) = 1$, which is exactly the elements of $U(n)$. (Assume $\gcd(\phi(1), n) > 1$. Then $\langle \phi(1) \rangle \subset \mathbb{Z}_n$.)

Proof. Define $\psi : \mathrm{Aut}(\mathbb{Z}_n) \to U(n)$ so that $\phi \mapsto \phi(1)$.

Now we show ψ is an isomorphism.

Homomorphism Let $\phi_1, \phi_2 \in \mathrm{Aut}(\mathbb{Z}_n)$.

Consider $\psi(\phi_1 \circ \phi_2)$, where all addition and multiplication is considered modulo n.

$$\begin{aligned}
\psi(\phi_1 \circ \phi_2) &= (\phi_1 \circ \phi_2)(1) && \text{(Definition of } \psi\text{)} \\
&= \phi_1(\phi_2(1)) \\
&= \phi_1\left(\sum_{i=1}^{\phi_2(1)} 1\right) && \text{(Note } \phi_2(1) \in \mathbb{Z}_n\text{)} \\
&= \sum_{i=1}^{\phi_2(1)} \phi_1(1) \\
&= \phi_2(1) \cdot \phi_1(1) \\
&= \phi_1(1) \cdot \phi_2(1) \\
& && \text{(Multiplication mod } n \text{ is commutative)} \\
&= \psi(\phi_1) \cdot \psi(\phi_2)
\end{aligned}$$

$\therefore$ ψ is a homomorphism.

Injective We know injectivity is equivalent to a trivial kernel.

$$\begin{aligned}
\ker(\psi) &= \{ g \in G \mid \psi(g) = \bar{e} \} \\
&= \{ \phi \in \mathrm{Aut}(\mathbb{Z}_n) \mid \psi(\phi) = 1 \} \\
\Rightarrow \ \psi(\phi) &= 1 \\
\Rightarrow \ \phi(1) &= 1 && \text{(Definition of } \psi\text{)} \\
\Rightarrow \ \ker(\psi) &= \{\mathrm{id}\} && (\phi(k) = k\phi(1) = k)
\end{aligned}$$

$\therefore$ ψ is injective.

SURJECTIVE Let $a \in U(n)$.

Choose $\phi_a(k) = ak \pmod{n}$ (since $\phi(1) = a$).

Exercise: Show $\phi_a(k) \in \text{Aut}(\mathbb{Z}_n)$.

Then using the definition of ψ, $\psi(\phi_a) = \phi_a(1) = a \cdot 1 \pmod{n} = a$.

$\therefore$ ψ is surjective.

$\therefore$ ψ is an isomorphism, so $\text{Aut}(\mathbb{Z}_n) \simeq U(n)$. □

7. Cosets and Lagrange's Theorem

7.1 Cosets

7.1.1 Properties of Cosets

Definition 7.1.1 — Coset. [Gal17, page 138] Let G be a group. Let $H \leqslant G$. Let $a \in G$.

The set $aH = \{\, ah \mid h \in H \,\}$ is the *left coset of H containing a*.

The set $Ha = \{\, ha \mid h \in H \,\}$ is the *right coset of H containing a*.

The element a is called the *coset representative*.

R Note that aH and Ha are not necessarily subsets of H, since $a \in G$, and closure in H isn't guaranteed. Also, aH and Ha are not necessarily subgroups of G.

Exercise 7.1 Prove if G is abelian, then $aH = Ha$ for any $a \in G$, $H \leqslant G$.

■ **Example 7.1** Let $G = U(9) = \{1,2,4,5,7,8\}$. Let $H = \langle 8 \rangle = \{1,8\}$. We want to compute all left and right cosets of H in G. Note $U(9)$ is abelian so $aH = Ha$.

$$\begin{aligned}
1H &= \{(1\cdot 1) \pmod 9, (1\cdot 8) \pmod 9\} = \{1,8\} = H1\\
2H &= \{2,7\} = H2\\
4H &= \{4,5\} = H4\\
5H &= \{5,4\} = H5\\
7H &= \{7,2\} = H7\\
8H &= \{8,1\} = H8
\end{aligned}$$

■

We observe the following:

- Not all cosets are distinct: the distinct left cosets are $1H, 2H, 4H$ (and the distinct right cosets are $H1, H2, H4$);
- The cosets have the same size;
- The cosets were either same or disjoint (i.e., they partition G).

Exercise 7.2 Let $G = S_3$. Let $H = \langle(1\ 2)\rangle$. Compute the distinct left and right cosets.

These observations help motivate the list of properties that cosets have, many of which concern equivalent definitions for equality.

Proposition 7.1.1 — Coset properties. [Gal17, page 139] Let G be a group. Let $a, b \in G$. Let $H \leqslant G$. Then:

(i) $a \in aH$;
(ii) $aH = H \Leftrightarrow a \in H$;
(iii) $aH = bH \Leftrightarrow a \in bH$;
(iv) $aH = bH \Leftrightarrow a^{-1}b \in H$;
(v) $aH = bH$ or $aH \cap bH = \varnothing$;
(vi) $|aH| = |bH|$ (where $|aH|$ denotes the cardinality of $|aH|$);
(vii) $aH = Ha \Leftrightarrow aHa^{-1} = H$;
(viii) $aH \leqslant G \Leftrightarrow a \in H$.

Note that properties (i), (v), and (vii) give us what was observed earlier: cosets partition the group into equal size subsets.

Proof. Let G be a group, $H \leqslant G$, and $a \in G$.

(i) $a = ae \in \{ah \mid h \in H\} = aH$, since $e \in H$.

(ii) First, suppose $aH = H$.
By (i), $a \in aH = H$.
$\therefore aH = H \Rightarrow a \in H$.
Now, suppose $a \in H$. Now we want to show $aH = H$.
Let $ah \in aH$. So $h \in H$. Then by closure ($H \leqslant G$), $ah \in H$.
$\therefore aH \subseteq H$.
Let $h \in H$. We can use group axioms since $a \in H$.

$$\begin{aligned} h &= eh && \text{(Identity)} \\ &= (aa^{-1})h && \text{(Inverse)} \\ &= a(a^{-1}h) && \text{(Associativity)} \end{aligned}$$

Then we have $h' = (a^{-1}h) \in H$ (by closure, since $a \in H$ so $a^{-1} \in H$). So $h = ah' \in aH$.
$\therefore H \subseteq aH$.
$\therefore a \in H \Rightarrow aH = H$.

(vi) We can show $|aH| = |bH|$ by showing a bijective map between both exists.
Define $f : aH \to bH$ as $ah \mapsto bh$.
Let $bh \in bH$.
Choose $ah \in aH$. Then $f(aH) = bH$.
$\therefore f$ is surjective.
Let $ah_1, ah_2 \in aH$. (So $h_1, h_2 \in H \leqslant G$.)
Suppose $f(ah_1) = f(ah_2)$. By definition of f, $bh_1 = bh_2$. By left cancellation law (in G specifically, since cosets are not necessarily groups), $h_1 = h_2$. Then, multplying both sides by a, $ah_1 = ah_2$.
$\therefore f$ is injective.

$\therefore f$ is a bijection, thus $|aH| = |bH|$.

□

Exercise 7.3 Prove Theorem 7.1.1(iii), (iv), (v), (vii), and (viii).

■ **Example 7.2** Consider the following two examples as motivation for Lagrange's theorem.

(i) We know the number and structure of subgroups of $\mathbb{Z}_6 = \{0,1,2,3,4,5\} = \langle 1 \rangle$ by the Fundamental Theorem of Cyclic Groups. That is, $\exists! H \leqslant \mathbb{Z}_6$ such that $|H| = d$ where $d \mid |\mathbb{Z}_6|$.

Note the divisors of d are $1,2,3,6$, so we must have the following subgroups: $\langle 6 \rangle, \langle 3 \rangle, \langle 2 \rangle, \langle 1 \rangle$.

(ii) Consider A_4. We know $|A_4| = \frac{4!}{2} = 12$. The divisors of 12 are $1,2,3,4,6,12$.

Note $\nexists H \leqslant A_4$ such that $|H| = 6$ even though $6 \mid 12$.

■

Lagrange's Theorem is one of the most important elementary results in group theory. It provides us a necessary condition for a subgroup using its size; not only that, but it gives a number of unique cosets of that subgroup.

Theorem 7.1.2 — Lagrange's Theorem. [Gal17, page 142] Let G be a group. Let $H \leqslant G$.

Suppose $|G| < \infty$.

(i) $|H| \mid |G|$;

(ii) $\dfrac{|G|}{|H|}$ is equal to the number of distinct left (or right) cosets of H in G.

Proof. Let G be a group. Let $H \leqslant G$.

Suppose $|G| < \infty$.

By Proposition 7.1.1(i), $\forall a \in G, a \in aH$. Then $G = \bigcup_{a \in G} aH$.

We know that all cosets are disjoint by Proposition 7.1.1(v), $aH = bH$ or $bH \cap bH = \varnothing$.

Let $a_1H, a_2H, \dots, a_rH$ be the distinct left cosets of H in G. ($a_iH \cup a_jH = \varnothing \forall i \neq j$.)

So $G = \bigsqcup_{1 \le i \le r} a_iH$, the disjoint union of all a_iH.

Then $|G| = \sum_{i=1}^{r} |a_iH|$ (whose sum we can take since each coset is disjoint).

By Proposition 7.1.1(ii), $a \in H \Leftrightarrow aH = H$. So $a_iH = eH = H$ for some i (that is, the identity must exist in one of the cosets). Also, by Proposition 7.1.1(vi), all cosets of group H in G have the same cardinality. Then $|a_iH| = |H|$ for all i.

So $|G| = |G| = \sum_{i=1}^{r} |H| = r|H|$.

$\therefore |H| \mid |G|$.

Also, $r = \dfrac{|G|}{|H|}$ is the number of distinct left cosets of H in G (and $r > 0$ since H is nonempty).

□

R The converse of Lagrange's theorem, that $|H| \mid |G|$ implies $H \leqslant G$, is false.

Again, consider Example 7.2(ii). We know $|A_4| = \frac{4!}{2} = 12$, and the divisors of 12 are $1,2,3,4,6,12$, so the following claim would be a counter-example to the converse of Lagrange's theorem.

Proposition 7.1.3 $|H| \mid |G| \not\Rightarrow H \leqslant G$

Proof. Let $G = A_4$. Then $\nexists H \leqslant G$ such that $|H| = 6$.

Assume (for contradiction), $\exists H \leqslant A_4$ such that $|H| = 6$.

We know there are 8 3-cycles in A_4. This is because 3-cycles in A_4 have cycle type $(3,1)$, and there are $\binom{4}{3}\frac{3!}{3} = \frac{4!}{3! \cdot 1!} \cdot 2! = 4 \cdot 2 = 8$ (since chosen elements multiplied by permutations without counting same arrangements).

Let $\alpha \in A_4$ be a 3-cycle. We know A_4 has exactly 2 distinct left cosets of H in A_4 by Lagrange $(\frac{|A_4|}{|H|} = \frac{12}{6} = 2)$.

Consider the following 3 cosets: αH, $\alpha^2 H$, $\alpha^3 H$. (We only care about these 3, since $\alpha^3 = e$ because $|\alpha| = 3$.) Then $\alpha^3 H = eH = H$.

We want to show none of these cosets are equal, giving us 3 distinct left cosets.

1. If $\alpha H = H$, then by Proposition 7.1.1(ii), $\alpha \in H$.
   So for $\forall \alpha, \alpha \in H$, i.e., all 8 3-cycles must be in H.
   But $|H| = 6$. Contradiction.
2. If $\alpha^2 H = H$, then $\alpha^2 \in H$.
   By closure of H, $\alpha^4 \in H$. Since $|\alpha| = 3$, $\alpha^3 = e$. Then $\alpha^4 = \alpha^3 \alpha = e\alpha = \alpha \in H$.
   Again, all 8 3-cycles must be in H, but $|H| = 6$. Contradiction.
3. If $\alpha H = \alpha^2 H$, then By Proposition 7.1.1(iv), $\alpha^{-1}\alpha^2 \in H$. So $\alpha \in H$.
   Once more, all 8 3-cycles must be in H, but $|H| = 6$. Contradiction.

$\therefore \alpha H, \alpha^2 H, \alpha^3 H = H$ are distinct left cosets in G. But there are only 2 distinct left cosets of H in A_4 by Lagrange. Contradiction.

$\therefore \nexists H \leqslant G$ such that $|H| = 6$.

$\therefore |H| \mid |G|$ holds but $H \leqslant G$ does not. □

Definition 7.1.2 [Gal17, page 143] Let G be a group. Let $H \leqslant G$. The *index of H in G*, $|G:H|$, is the number of distinct left cosets of H in G.

■ Example 7.3

- Note that we can even consider infinite order groups for cosets. Let $G = \mathbb{Z}$, $H = 2\mathbb{Z} = \langle 2 \rangle$. Then $|G:H| = 2$.
- $G = S_3$, $H = \langle (1\ 2) \rangle$. $|G:H| = \frac{G}{H} = 3$.

■

Corollary 7.1.4 [Gal17, page 143] Let G be a group. Let $H \leqslant G$. If $|G| < \infty$, then $|G:H| = \frac{G}{H}$

Proof. Suppose the hypothesis. Then the consequent follows by (ii) of Lagrange and the definition of index. □

Corollary 7.1.5 [Gal17, page 143] Suppose G is a finite group and $a \in G$. Then $|a| \mid |G|$.

Proof. Suppose G is a group such that $|G| < \infty$. Let $a \in G$.

Recall that $\langle a \rangle \leq G$ by Proposition 3.1.3 and $|\langle a \rangle| = |a|$ by Proposition 4.1.1(ii).

By Lagrange, $|\langle a \rangle| \mid |G|$. Then $|a| \mid |G|$. □

Corollary 7.1.6 [Gal17, page 143] Suppose G is a finite group. Let $a \in G$.
Then $a^{|G|} = e$.

Proof. Suppose G is a finite group. Let $a \in G$.

By Corollary 7.1.5, $|a| \mid |G|$. So $|G| = r|a|$ for some $r \in \mathbb{Z}^+$.

So $a^{|G|} = a^{r|a|} = (a^{|a|})^r = e^r = e$. □

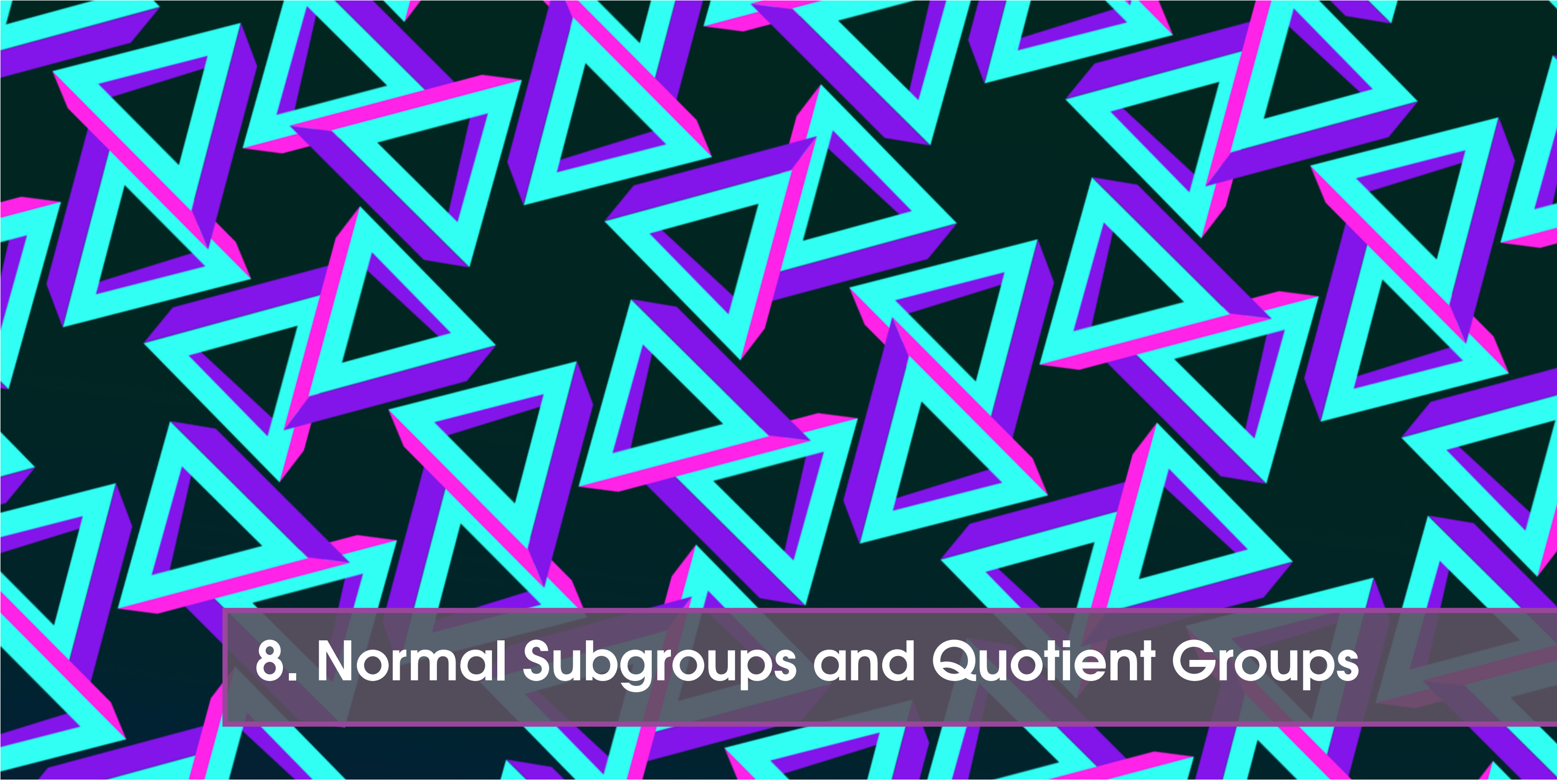
Exercise 7.4 Find the order of 7 in $U(23)$.

We know $|U(23)| = 22$. So $|7| \mid 22$. Then the possible orders of 7 are 1, 2, 11, 22, so we only have to check 7^d for those values d.

The following corollary is relevant to number theory (but not required for this course):

Corollary 7.1.7 Let G be a finite group.
If $a \in \mathbb{Z}$ and prime $p \geq 2$, then $a^{p-1} \equiv 1 \pmod{p}$. (This is Fermat's Little Theorem.)

This follows from Lagrange's Theorem.



8. Normal Subgroups and Quotient Groups

8.1 Normal Subgroups

8.1.1 Normal Subgroups

Definition 8.1.1 [Gal17, page 174] Let G be a group. Let $H \leqslant G$. Then H is a *normal subgroup*, $H \trianglelefteq G$, if $aH = Ha$ for all $a \in G$.

■ **Example 8.1** Let $V = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, the Klein four group. Then $V \trianglelefteq A_4$. ■

$\circ$	(1)	$(1\,2)(3\,4)$	$(1\,3)(2\,4)$	$(1\,4)(2\,3)$
(1)	(1)	$(1\,2)(3\,4)$	$(1\,3)(2\,4)$	$(1\,4)(2\,3)$
$(1\,2)(3\,4)$	$(1\,2)(3\,4)$	(1)	$(1\,4)(2\,3)$	$(1\,3)(2\,4)$
$(1\,3)(2\,4)$	$(1\,3)(2\,4)$	$(1\,4)(2\,3)$	(1)	$(1\,2)(3\,4)$
$(1\,4)(2\,3)$	$(1\,4)(2\,3)$	$(1\,3)(2\,4)$	$(1\,2)(3\,4)$	(1)

Table 8.1: Cayley table for V

Proof. First, we have to show $V \leqslant A_4$.

NONEMPTINESS $(1) \in V$, so $V \neq \varnothing$

SUBSET The elements of V are even (the product of an even number of 2-cycles). So $V \subseteq A_4$.

CLOSURE Note that Figure 8.1 shows that $\forall g, h \in V, gh \in V$.

INVERSE Moreover, the main diagonal of (1) tells us that each element in V is its own two-sided inverse. That is, $\forall g \in H, g^{-1} \in H$.

Then, we have to show that $\forall a \in A_4, aV = Va$. We need all the even permutations to get the elements of A_4:

$$A_4 = \{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3),\\ (1\,2\,3),(1\,2\,4),(1\,3\,2),(1\,4\,2),\\ (1\,3\,4),(1\,4\,3),(2\,3\,4)(2\,4\,3)\}$$

First, we have the left coset $(1)V = \{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$. Note that we have Proposition 7.1.1(ii), $a \in H \Leftrightarrow aH = H$. So $(1)V = (1\,2)(3\,4)V = (1\,3)(2\,4)V = (1\,4)(2\,3)V = V$.

Next, we compute $(1\ 2\ 3)V = \{(1\,2\,3),(1\,3\,4),(2\,4\,3),(1\,4\,2)\}$. By Proposition 7.1.1(iii), $aH = bH \Leftrightarrow a \in bH$. So $(1\,2\,3)V = (1\,3\,4)V = (2\,4\,3)V = (1\,4\,2)V$.

We know that $(1\,2\,4)V = (1\,3\,2)V = (1\,4\,3)V = (2\,3\,4)V$ because by Lagrange, the number of distinct left cosets of V in A_4 is $|A_4|\,/\,|V| = 12/4 = 3$.

Computing the right cosets, we will find that $(1)V = V(1)$, $(1\ 2\ 3)V = V(1\ 2\ 3)$, and $(1\,2\,4)V = V(1\,2\,4)$.

$\therefore V \trianglelefteq A_4$. □

Exercise 8.1 Compute the right cosets of V in A_4.

Theorem 8.1.1 — Normal subgroup test. [Gal17, page 175] Let G be a group. Let $H \leqslant G$. Then $H \trianglelefteq G$ iff $aHa^{-1} \subseteq G$ for all $a \in G$.

Note that $aHa^{-1} = \left\{ aha^{-1} \mid h \in H \right\}$. This is called a *conjugate subgroup* in G. In general, we multiply group elements on the left and right of sets in the same way as in the definition of cosets, which is valid since all elements belong to a group.

Proof. Suppose $H \trianglelefteq G$.

Let $a \in G$.

$$\begin{aligned} aH &= Ha \\ \Rightarrow\ aHa^{-1} &= Haa^{-1} && (a^{-1} \in G) \\ &= H(aa^{-1}) && \text{(Associativity)} \\ &= He && \text{(Inverse)} \\ &= H && \text{(Proposition 7.1.1(ii))} \end{aligned}$$

$\therefore aHa^{-1} \subseteq$ for all $a \in G$.

Suppose $aHa^{-1} \subseteq H$ for all $a \in G$.

Let $a \in G$. Then by group axioms, $(aHa^{-1})a = aH(aa^{-1}) = aHe = aH \subseteq Ha$.

Since $a'Ha'^{-1} \subseteq H$ for all $a' \in G$, it holds for $a' = a^{-1}$. This gives us $a^{-1}H(a^{-1})^{-1} \subseteq H$. We can simplify with group axioms, $a^{-1}Ha \subseteq H$. Then $a(a^{-1}Ha) = (aa^{-1})Ha = eHa = Ha \subseteq aH$.

$\therefore aH = Ha$.

$\therefore H \trianglelefteq G$. □

■ **Example 8.2** $SL(2,\mathbb{R}) \trianglelefteq GL(2,\mathbb{R})$. ■

We can use the normal subgroup test.

Proof. We have proved that $SL(2,\mathbb{R}) \leqslant GL(2,\mathbb{R})$ in Example 3.2.

We want to show $\forall A \in GL(2,\mathbb{R}), A\,SL(2,\mathbb{R})A^{-1} \subseteq SL(2,\mathbb{R})$.

Let $A \in GL(2,\mathbb{R})$.

Let $B \in SL(2,\mathbb{R})$.

Consider ABA^{-1}. This is a 2 by 2 real-entry matrix.

We need to show it is in $SL(2,\mathbb{R})$ by showing it has determinant 1. We can use the determinant properties ($\det(B) = 1, \det(A) \neq 0$), $\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\det(B)\frac{1}{A} = 1 \cdot \det(B) = \det(B) = 1$. □

Exercise 8.2 Prove $Z(G) \trianglelefteq G$.

Note that we have already proven the center of a group is a subgroup. Then we need to show $gZ(G) = Z(G)g$ for all $g \in G$.

Theorem 8.1.2 — Quotient Group. Let G be a group. Let $H \trianglelefteq G$. The set of distinct left cosets of H in G

$$G/H = \{aH \mid a \in G\}$$

together with the operation $(aH)(bH) = (ab)H$ for all $a,b \in G$ is a group. This is called the *quotient group* (or factor group).

Proof. Let G be a group. Let $H \trianglelefteq G$. Consider $G/H = \{aH \mid a \in G\}$.

Nonemptiness Since $e \in G$, $eH \in G/H$. $\therefore G/H \neq \varnothing$.

Closure Note that we have the operation $* : G/H \times G/H \to G/H$. Also, we have to ensure that our operation is well-defined, since there are multiple cosets which are equal. So for example, if we take two cosets not in the quotient, we can find cosets that are in the quotient group and show this operation outputs the equivalent coset.

Suppose $aH = a'H$, $bH = b'H$ where $a, a', b, b' \in G$. We want to show $(ab)H = (a'b')H$.

($\star$) By Proposition 7.1.1(iii), $aH = a'H \Rightarrow a \in a'H$. Then $a = a'h$ for some $h \in H$ by definition of $a'H$. Similarly, $bH = b'H \Rightarrow b \in b'H$. Then $b = b'h'$ for some $h' \in H$. (Note it does not hold that $h = h'$.)

($\star\star$) By $H \trianglelefteq G$, $xHx^{-1} \subseteq H, \forall x \in G$. So $xhx^{-1} \in H, \forall x \in G, \forall h \in H$. Take $x = (b')^{-1}$. Hence $(b')^{-1}h((b')^{-1})^{-1} = (b')^{-1}hb' \in H$. By Proposition 7.1.1(ii), this gives $(b')^{-1}hb' \in H \Rightarrow ((b')^{-1}hb')H = H$.

$$\begin{aligned}
(ab)H &= (a'hb'h')H && (\star)\\
&= (a'hb')H && \text{(Proposition 7.1.1(ii), Associativity)}\\
&= (a'ehb')H && \text{(Identity)}\\
&= (a'b'(b')^{-1}hb)H && \text{(Inverse)}\\
&= (a'b')\left((b')^{-1}hb'H\right) && \text{(Associativity)}\\
&= (a'b')H && (\star\star)
\end{aligned}$$

Then given equivalent inputs, we will get an equivalent coset output. $\therefore \forall aH, bH \in G/H, (ab)H \in G/H$.

Associativity Let $a,b,c \in G$. Let $aH, bH, cH \in G/H$.

We can use the associativity of G and the definition of G/H.

$$\begin{aligned}((aH)*(bH))*(cH) &= ((ab)H)*(cH) && \text{(Definition of } *)\\ &= ((ab)c)H && \text{(Definition of } *)\\ &= (a(bc))H && \text{(Associativity)}\\ &= (aH)*((bc)H) && \text{(Definition of } *)\\ &= (aH)*((bH)*(cH)) && \text{(Definition of } *)\end{aligned}$$

$\therefore ((aH)*(bH))*(cH) = (aH)*((bH)*(cH))$.

IDENTITY Choose $eH \in G/H$ as the identity of G/H.

Let $aH \in G/H$, so $a \in G$.

Then, since e is the identity of G, $(eH)(aH) = (ea)H = aH$ and $(ah)(eH) = (ae)H = aH$.

INVERSE Choose $a^{-1} \in G/H$ as the inverse of G/H.

Let $aH \in G/H$, so $a \in G$.

Then, since a^{-1} is the inverse of G, $(a^{-1}H)(aH) = (a^{-1}a)H = eH$ and $(aH)(a^{-1}H) = (aa^{-1})H = eH$.

□

■ **Example 8.3** Again, consider the Klein four group, $V = (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)$. We have shown that $V \trianglelefteq A_4$ in Example 8.1.

From that example, we showed that the left cosets of V in A_4 are:
- $(1)V = (1\,2)(3\,4)V = (1\,3)(2\,4)V = (1\,4)(2\,3)V = V$;
- $(1\,2\,3)V = (1\,3\,4)V = (2\,4\,3)V = (1\,4\,2)V$;
- $(1\,2\,4)V = (1\,3\,2)V = (1\,4\,3)V = (2\,3\,4)V$.

Since we only care about distinct left cosets, we choose distinct cosets.

Then $A_4/V = \{(1)V, (1\,2\,3)V, (1\,2\,4)V\}$. ■

8.1.2 First Isomorphism Theorem

The following exercise will serve as motivation.

Exercise 8.3 Let $G = D_4 = \left\{\langle r,s\rangle \mid |r| = 4, |s| = 2, sr = r^3s\right\} = \{e,r,r^2,r^3,s,rs,r^2s,r^s\}$.

(a) Prove $H = \left\langle r^2 \right\rangle \trianglelefteq G$.

(b) List the elements of G/H.

(c) Show which generator representation is equivalent to each symmetry of the square.

We have that $D_4 = \{e,r,r^2,r^3,s,rs,r^2s,r^3s\}$. Then $H = \left\langle r^2 \right\rangle = \{r^2, e\}$. It is a subgroup by Proposition 3.1.3.

We get the following cosets:

$$\begin{aligned}eH &= r^2H = \{r^2,e\} = Hr^2 = He\\ rH &= r^3H = \{r^3,r\} = Hr^3 = Hr\\ sH &= sr^2H = \{sr^2,s\} = Hs = Hr^2\\ srH &= sr^3H = \{sr^3,sr\} = Hrs = Hr^3s\end{aligned}$$

$\therefore H$ is normal. The elements of G/H are given in 8.2

To ensure that all the elements in the chart are from the distinct coset representatives, we need to refer to the cosets calculuated as well as the relations. For example, $r^2H = eH$ since they are the same coset. Also $srH = r^3sH$ by the relation, which equals rsH since they are the same coset.

$*$	eH	rH	sH	rsH
eH	eH	rH	sH	rsH
rH	rH	eH	rsH	sH
sH	sH	rsH	eH	rH
rsH	rsH	sH	rH	eH

Table 8.2: Cayley table for G/H

Note by the diagonal symmetry of Figure 8.2 (that is, $(aH)*(bH) = (bH)*(aH)$ for all $aH, bH \in G/H$), the group G/H is Abelian. Also, $|G/H| = 4$. $rH \neq eH$ and $(rH)*(rH) = r^2H = eH$

So we have $|rH| = 2$. By the Cayley table, we can see that all elements of G/H have order 2.

Now, consider the Cayley table of D_4 in Figure 8.3, ordered so that each coset gets their own columns and rows. Then, notice how each of the individual 2×2 cells

$\circ$	e	r^2	r	r^3	r^2s	s	rs	r^3s
e	e	r^2	r	r^3	r^2s	s	rs	r^3s
r^2	r^2	e	r^3	r	s	r^2s	r^3s	rs
r	r	r^3	r^2	e	r^3s	rs	r^2s	s
r^3	r^3	r	e	r^2	rs	r^3s	s	r^2s
r^2s	r^2s	s	r^3s	rs				
s	s	r^2s	rs	r^3s				
rs	rs	r^3s						
r^3s	r^3s	rs						

Table 8.3: (Partial) Cayley table for D_4

Exercise 8.4 Let $H \trianglelefteq G$

(a) If G is Abelian, is G/H Abelian?

(b) If G is cyclic, is G/H cyclic?

Theorem 8.1.3 — First isomorphism theorem. [Gal17, page 201] Let $G, \overline{G}$ be groups. Let $\phi : G \to \overline{G}$.

(i) $\ker\phi \trianglelefteq G$

(ii) $^{G}/_{\ker\phi} \simeq \phi(G)$

The kernel of ϕ is normal in G, and the quotient group of the kernel is isomorphic to the image of ϕ. Why is this useful? If we are given a homomorphism, we can create an isomorphism using this theorem by using the kernel.

We can make a commutative diagram: G to $\overline{G}$ by ϕ, G natural map to $G/\ker\phi$ by γ, $G\ker\phi$ to $\phi(G)$ by ψ, and $\phi(G) \leq \overline{G}$.

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, dashed, "\gamma"'] & \overline{G} \arrow[d, dash, "\leqslant"] \\
G/\ker(f) \arrow[r, "\psi"'] & \phi(G)
\end{tikzcd}$$

Proof. Let $G, \overline{G}$ be groups.

Let $\phi : G \to \overline{G}$ be a homomorphism.

(i) We know that $\ker\phi \leqslant G$ by Proposition 6.1.1.
Let $a \in G$. Let $g \in \ker\phi$.
We want to show $a\ker\phi a^{-1} \subseteq \ker\phi$ for all $a \in G$.
Consider $aga^{-1} \in G$ by closure.

$$\begin{aligned}
\phi(aga^{-1}) &= \phi(a)\phi(g)\phi(a^{-1}) && (\phi \text{ homomorphism}) \\
&= \phi(a)\overline{e}\phi(a^{-1}) && (g \in \ker\phi) \\
&= \phi(a)\overline{e}\phi(a)^{-1} && (\text{Theorem 6.2.1(ii)}) \\
&= \phi(a)\phi(a)^{-1} = \overline{e} && (\text{Identity, inverse})
\end{aligned}$$

$\therefore \ker\phi \trianglelefteq G$.

(ii) Define $\psi : {}^{G}\!/_{\ker\phi} \to \phi(G)$ by $a\ker\phi \mapsto \phi(a)$, i.e. $\psi(a\ker\phi) = \phi(a)$.
We need to check ψ is an isomorphism. Since we are working with coset representatives, we need to ensure it is well defined first.

WELL DEFINED Let $a\ker\phi, a'\ker\phi \in {}^{G}\!/_{\ker\phi}$, so $a, a' \in G$.
Suppose $a\ker\phi = a'\ker\phi$. By Proposition 7.1.1(iii), $a \in a'\ker\phi$, so $a = a'h$ for some $h \in \ker\phi$ by coset definition $(\star)$.

$$\begin{aligned}
\psi(a\ker\phi) &= \phi(a) && (\text{Definition of } \psi) \\
&= \phi(a'h) && (\star) \\
&= \phi(a')\phi(h) && (\phi \text{ homomorphism}) \\
&= \phi(a')\overline{e} && (h \in \ker\phi) \\
&= \phi(a') && (\text{Identity}) \\
&= \psi(a'\ker\phi) && (\text{Definition of } \psi)
\end{aligned}$$

$\therefore a\ker\phi = a'\ker\phi \Rightarrow \psi(a\ker\phi) = \psi(a'\ker\phi)$, i.e. for ψ, equivalent input cosets in ${}^{G}\!/_{\ker\phi}$ give equivalent output images in $\phi(G)$. $\therefore$ ψ is well defined.

HOMOMORPHISM Let $a\ker\phi, b\ker\phi \in {}^{G}\!/_{\ker\phi}$, so $a, b \in G$.

$$\begin{aligned}
\psi((a\ker\phi)*(b\ker\phi)) &= \psi((ab)\ker\phi) && (\text{Definition of } *) \\
&= \phi(ab) && (\text{Definition of } \psi) \\
&= \phi(a)\phi(b) && (\phi \text{ homomorphism}) \\
&= \psi(a\ker\phi)\psi(b\ker\phi) && (\text{Definition of } \psi)
\end{aligned}$$

$\therefore$ ψ is homomorphism.

INJECTIVE We know injectivity is equivalent to a trivial kernel.

$$\begin{aligned}\ker(\psi) &= \{g \in G \mid \psi(g) = \overline{e}\}\\ &= \{a\ker\phi \in G/\ker\phi \mid \psi(a\ker\phi) = \overline{e}\} && \text{(Definition of } \ker(\psi))\\ \Rightarrow\ \psi(a\ker\phi) &= \overline{e}\\ \Rightarrow\ \phi(a) &= \overline{e} && \text{(Definition of } \psi)\\ \Rightarrow\ a &\in \ker\phi && \text{(Definition of } \ker\phi)\\ \Rightarrow\ a\ker\phi &= \ker\phi && \text{(Proposition 7.1.1(ii))}\\ \Rightarrow\ \ker(\psi) &= \{\ker\phi\} = \{e\ker\phi\}\end{aligned}$$

$\therefore$ ψ is injective.

SURJECTIVE Let $\overline{a} \in \phi(G)$.

By definition of $\phi(G) = \{\phi(g) \mid g \in G\}$, $\phi(a) = \overline{a}$ for some $a \in G$. Choose $a\ker\phi \in G/\ker\phi$.

Then by definition of ψ, $\psi(a\ker\phi) = \phi(a) = \overline{a}$.

$\therefore$ ψ is surjective.

□

In the following corollary, we only look at finite groups.

Corollary 8.1.4 [Gal17, page 201] Let $G, \overline{G}$ be finite order groups.
Let $\phi : G \to \overline{G}$ be a homomorphism.
Then $|\phi(G)|$ divides both $|G|$ and $|\overline{G}|$.

Proof. Let $G, \overline{G}$ be finite order groups.

Let $\phi : G \to \overline{G}$ be a homomorphism.

We know $\phi(G) \leqslant \overline{G}$ by Theorem 6.3.1(i), so $|\phi(G)| < \infty$.

$\therefore |\phi(G)|$ divides $\overline{G}$ by Lagrange.

By First isomorphism theorem, $G/\ker\phi \simeq \phi(G)$. Then $|G/\ker\phi| = |\phi(G)|$ since we have a bijection. By Lagrange, $|G/\ker\phi| = \frac{|G|}{\ker\phi} = |\phi(G)|$.

Then $|G| = |\phi(G)|\,|\ker\phi| \in \mathbb{Z}^+$ by definition of order.

$\therefore |\phi(G)|$ divides G. □

Now, we have an application of this corollary.

■ **Example 8.4** There is no nontrivial homomorphism between $U(15)$ to $\mathbb{Z}_{15}$. ■

Proof. We have that $\mathbb{Z}_{15} = \{0,1,2,\ldots,14\}$ and $U(15) = \{g \in \mathbb{Z}_{15} \mid \gcd(g,15) = 1\} = \{1,2,4,7,8,11,13,14\}$.

Let $\phi : U_{15} \to \mathbb{Z}_{15}$ be a homomorphism.

By Corollary 8.1.4, since $\mathbb{Z}_{15}$ and $U(15)$ are finite, $|\phi(U(15))|$ must divide $|Z_{15}| = 15$ and $|U(15)| = 8$.

So $|\phi(G)| = 1$, and the only subgroup of order 1 is the trivial subgroup. $\therefore \phi(G) = \{0\}$, that is, ϕ is the trivial homomorphism.

$\therefore$ There is no nontrivial homomorphism between $U(15)$ to $\mathbb{Z}_{15}$. □

Part Two

9. Tutorial Exercises

9.1 Other Examples of Groups

Exercise 9.1 Let $G = \left\{ x \in \mathbb{R} \mid x \neq \frac{1}{2} \right\}$. Define $x * y = x + y - 2xy$. Prove that this is a group.

Proof. NON-EMPTINESS $0 \in R$ and $0 \neq \frac{1}{2}$, so $0 \in X$. $X \neq \varnothing$.

CLOSURE Let $x, y \in X$. We want to show $x * y \in X$.

Given $x * y = x + y - 2xy$, we have addition and multiplication are closed under the real numbers by axioms. Therefore we must show that $x * y \neq \frac{1}{2}$. We want to show $x \wedge y \neq \frac{1}{2} \Leftrightarrow x * y \neq \frac{1}{2}$.

We show this by contrapositive. Suppose $x * y = \frac{1}{2}$.

$$\begin{aligned} x * y = \frac{1}{2} &\Leftrightarrow x + y - 2xy = 1/2 && (9.1)\\ &\Leftrightarrow 2x + 2y - 4xy = 1 && (9.2)\\ &\Leftrightarrow 2x + 2y - 4xy - 1 = 0 && (9.3)\\ &\Leftrightarrow (2x-1) - 2y(2x-1) = 0 && (9.4)\\ &\Leftrightarrow (2x-1)(1-2y) = 0 && (9.5)\\ &\Leftrightarrow y = \frac{1}{2} \vee x = \frac{1}{2} && (9.6) \end{aligned}$$

ASSOCIATIVITY Let $x, y, z \in G$. We use the commutativity and associativity of the real numbers.

$$\begin{aligned} (x * y) * z &= (x * y) + z - 2(x * y)z && (9.7)\\ &= (x + y - 2xy) + z - 2(x + y - 2xy)z && (9.8)\\ &= x + y - 2xy + z - 2xz - 2yz + 4xyz && (9.9)\\ &= x + (y + z - 2yz) - 2x(y + z - 2yz) && (9.10)\\ &= x + (y * z) - 2x(y * z) && (9.11)\\ &= x * (y * z) && (9.12) \end{aligned}$$

Identity The identity is 0. Given $x \in X$, then $x * 0 = 0 * x = x + 0 - 2x \cdot 0 = x + 0 - 0 = x$.

Inverse Let $a \in G$. We want to find $x \in X$ such that $a * x = 0$.

$$a * x = 0 \Leftrightarrow a + x - 2xa = 0 \tag{9.13}$$

$$\Leftrightarrow x(1-2a) + a = 0 \tag{9.14}$$

$$\Leftrightarrow x = \frac{-a}{1-2a}. \tag{9.15}$$

Also note $x * a = 0 \Leftrightarrow x + a - 2ax = a + x - 2xa$ by commutativity over the reals.

□

Exercise 9.2 Suppose $(G,*)$ and $(H,\circ)$. How do we make $G \times H$ into a group?

$G \star H = \{(a,b) \mid a \in G, b \in H\}$

$(a,b) \star (a',b')$. Then we have the binary operation $(a * a', b \circ b')$, which creates a group. Prove this is a group.

Exercise 9.3 Let $G = \left\{ a + b\sqrt{2} \mid a,b \in \mathbb{Q} \right\}$ with $* = \cdot$. Prove this is a group.

Non-emptiness: $0 \in G$.

Closure: $a + b\sqrt{2} * a' + b'\sqrt{2} = aa' + bb'2 + (ab' + ba')\sqrt{2}$. The coefficients are all rational by closure of rationals.

Identity: The identity is 1.

Inverse: We want $x = \frac{1}{a+b\sqrt{2}}$ but this does not necessarily belong in G. Rationalize by conjugate to get $x = \frac{a-b\sqrt{2}}{a^2-2b^2}$.

Associativity: Show associativity.

Exercise 9.4 Suppose $G = \{x \in \mathbb{R} \mid 0 \le x < 1\}$ and $x * y = \text{frac}(x+y)$. Prove this is a group.

Note that we can use $\text{frac}(x+y) = x + y - \lfloor x+y \rfloor$.

Non-emptiness: $0 \in G$.

Closure: Let $x,y \in G$. Then $0 \le x,y < 1 \Rightarrow 0 \le x+y < 2$. We know $x * y = \text{frac}(x+y) = x + y - \lfloor x+y \rfloor$.

First consider $0 \le x+y < 1$. Then $x*y = x+y-\lfloor x+y \rfloor = x+y-0 = x+y$, and we already have $0 \le x+y < 1$ so $x*y \in G$.

Then consider $1 \le x+y < 2$. Then $x*y = x+y-\lfloor x+y \rfloor = x+y-1$. $1 \le x+y < 2 \Rightarrow 0 \le x+y-1 < 1$ so $0 \le x*y < 1$ and $x*y \in G$.

Associativity: Show this.

Identity: Identity is 0.

Inverse: Let $a \in G$.

For $a = 0$, choose $x = 0 \in G$. Then $x * a = 0 = a * x$

Let $0 < a < 1$. The inverse would be $x * a = 0$. Then we want $x + a - \lfloor x+a \rfloor = 0$. We need $x + a = \lfloor x+a \rfloor$. But this equality is only true when $x + a \in Z \Leftrightarrow x = k - a$, for some $k \in Z$. We want $x \in G \Rightarrow 0 \le x < 1$. Since $0 < a < 1$, choose $k = 1$.

For $0 < a < 1$, the inverse $x = 1 - a \in G$ because $0 < a < 1 \Rightarrow 0 > -a > -1 \Rightarrow 1 > 1 - a > 0$. x is an inverse of a because $x * a = x + a - \lfloor x+a \rfloor = 1 - a + a - \lfloor 1 - a + a \rfloor = 1 - \lfloor 1 \rfloor = 0$. Also $a * x = a + x -$

$$\lfloor a+x \rfloor = a+1-a-\lfloor a+1-a \rfloor = 1-1=0.$$

9.2 Subgroup Exercises

Exercise 9.5 Consider $U(n) = \{ m \in Z_n \mid m,n \text{ relatively prime} \}$. This forms a group under multiplication modulo n.

Let $\{ a \in \mathbb{Z} \mid \exists b \in \mathbb{Z}_n, a \cdot b \pmod{n} = 1 \}$. Show this is equivalent to $U(n)$.

For example, $U(8) = \{1,3,5,7\}$. We can use the fact from number theory that if $gcd(x,y)=1$, then $\exists s,t \in Z, sx+ty=1$.

If $(a,n)=1$, $\exists s',t' \in \mathbb{Z}, as'+nz'=1$, and $s'=kn+r, 0 \leq r < k$. Since $nk=0 \pmod{n}$, $as'=a(nk+r)=1-nt'$.

Exercise 9.6 Show that the one-step and two-step subgroup tests are equivalent.

Exercise 9.7 For each of the following, is $H \leqslant G$?

(i) Let $G=(\mathbb{C},+)$. Let $H=\{ a+ai \mid a \in \mathbb{R} \}$.

(ii) Let $G=(\mathbb{C}^{\times},\cdot)$. Let $H=(S^1,\cdot)=\{ z \in \mathbb{C} \mid |z|=1 \}$.

(iii) Let $G=(\mathbb{Q}^{\times},\cdot)$. Let $n \in \mathbb{Z}^+$, then let H be the set of all rationals whose denominator divides n under multiplication.

(iv) Let $G=(\mathbb{Q},\cdot)$. Let $H=\left\{ \frac{a}{b} \;\middle|\; a,b \in \mathbb{Z}, b \neq 0, \gcd(b,n)=1 \right\}$ under addition.

For (i), yes. This is simple to prove with two-step.

For (ii), yes. The identity is 1. Anything on the unit circle is $e^{i\theta}$, the inverse is $e^{-i\theta}$.

For (iii), no. Take $n=4$. Then $\frac{3}{4} \in H$ but $\left(\frac{3}{4}\right)^{-1} = \frac{-4}{3} \notin H$. We could make this a subgroup if we change the operation to addition.

For (iv), yes. We can do one-step, $\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}$. If $\gcd(b,n)=1$ and $\gcd(d,n)=1$, then $\gcd(bd,n)=1$ by Fundamental Theorem of Arithmetic (uniqueness of prime factorization).

Exercise 9.8 Find a subgroup of the dihedral group, D_n.

We can think of D_n as $\left\{ r,s \mid r^n = s^2 = 1,\ rs = sr^{-1} = sr^{n-1} \right\}$. Some subgroups of D_n are $H_1=\{e\}$; $H_2=\{e,s\}$, where $s^2=e$; $H_3=\{e,r^2,\dots,r^{n-1}\}$.

Say for D_4, $H_4=\{e,s,r^2,sr^2\}$.

Exercise 9.9 Suppose G is cyclic. Then G is abelian. (Thus, G is not abelian implies G is not cyclic.)

Let G be a cyclic group. We want to show $\forall x,y \in G, xy=yx$.

Since G is cyclic, $\exists g \in G \wedge m,n \in \mathbb{Z}, g^n=x, g^m=y$. Then $xy=g^ng^m$ and use associativity.

Exercise 9.10 Suppose G is abelian. Prove that $\{ g \in G \mid |g| < \infty \} \leqslant G$. Construct an explicit example which would show we need G to be abelian. (Find non-abelian G which does not have a subgroup with finite order elements.)

Consider $G=GL(2,\mathbb{R})$ and $H=\{ g \in G \mid |g| < \infty \}$. Then let $A=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B=\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$. Since $|A|=4$ and $|B|=3$, $A,B \in H$ but $|AB|=\infty$, so $AB \notin H$, so H is not a group.

Now we want to consider the center of G (the set of all elements of G which commutes with everything).

Let G be a group. Then consider $\left\{x \in G \mid g^{-1}xg = x, \forall g \in G\right\} = Z(G)$. Then $Z(G) \leqslant G$. This is nonempty since $e_G \in Z(G)$.

G is abelian $\Leftrightarrow$ $Z(G) = G$.

Exercise 9.11 Find $Z(D_n)$.

In D_n, we know that $s^2 = e$, $r^n = e$, and $\forall 0 \leq i < n, r^i s = sr^{n-i}$.

Proposition 9.2.1 If n is odd, then $Z(D_n) = \{e\}$. If n is even, then $Z(D_n) = \{e, r^k\}$ where $n = 2k$.

Proof. Let n be odd. First note that $r^i r^j = r^j r^i$, that is, reflections always commute. So it's sufficient to show its behavior with elements sr^j, that is, some reflection does not commute.

Suppose $r^i(sr^j) = (sr^j)r^i$. Then $s = sr^{2i} \Rightarrow n \mid 2i$. Since n is odd, $n \mid i \Rightarrow nk = i$. We have that $r^n = e$, so $r^i = r^{nk} = (r^n)^k = e^k = e$. Therefore $r^j \notin Z(D_n)$.

Now we show that $sr^i \notin Z(D_n)$. Choose r and suppose $r(sr^i) = (sr^i)r$. So $r(sr^i) = (sr^i)r = sr^{i+1}$. Also $rsr^i = sr^{i-1}$ by definition of D_n. These two give $sr^{i+1} = sr^{i-1}$. But this only holds if $sr^2 = s \Rightarrow r^2 = e$. But n is odd, which implies $r^2 \neq e$. Therefore $sr^i \notin Z(D_n)$.

We can use this argument to prove the even case. □

9.3 Cyclic Group Exercises

We call a group G cyclic if $\exists g \in G, \{\, g^n \mid n \in \mathbb{Z}\,\} = \langle g \rangle = G$. Note that if $\langle g \rangle = G \Leftrightarrow \left\langle g^{-1} \right\rangle = G$.

Proposition 9.3.1 Suppose that $G = \langle g \rangle$ and $|G| = \infty$. Then $\forall n \in \mathbb{Z}^{\times}, g^n \neq e$ and $g^a \neq g^b$, $\forall a, b \in \mathbb{Z}, a \neq b$.

Proof. We can prove this by contradiction.

Suppose $g^a = g^b$. WLOG, $a < b$.

$(g^a)^{-1}g^a = (g^a)^{-1}g^b \Leftrightarrow g^{b-a} = e$. But $|G| = \infty$ which is a contradiction. □

In general, if $|G| < \infty$ and $H \leqslant G$, then $|H| \bigm| |G|$.

But if G is cyclic, $G = \langle g \rangle$ and $|G| = n$, then $\forall k, k \mid n, \exists! H_k \leqslant G$ (a unique subgroup H of G) where $|H_k| = k$ and $H_k = \left\langle g^{n/k} \right\rangle$.

Note that given t where $\gcd(t, n) = 1$, then $\langle g^t \rangle = \langle g \rangle$.

9.4 More Cyclic Group Exercises

Exercise 9.12 Suppose that G is a group with finite order, $|G| < \infty$ and m divides $|G|$. Does G has an element of order m?

False. Consider the dihedral group D_3 which has order 6. But consider 6 which divides 6. There is no element with order 6, that is, D_3 is not cyclic.

Note this counter-example is not abelian. Is there an abelian counterexample?

Yes. Consider $G = \{x \in \mathbb{Z}_15 \mid \exists n \in \mathbb{Z}$ such that $nx = xn = 1 \pmod{15}\} = U(15)$ which is finite and abelian but not cyclic. Then $|G| = 8$. So consider $m = 8 \mid 8$. There is no element with that given order.

We will consider finite and infinite groups, and abelian and non-abelian groups. Recall examples and counterexamples for each of these. Remember that cyclic implies abelian.

Consider the FTOCG: If $G = \langle a \rangle$ where $a \in G$ and $|G| = n$, then $\forall m \mid n = |\langle a \rangle|$, $\exists! H \leqslant G$ with $|H| = m$, namely, $H = \left\langle a^{n/m} \right\rangle$. We call a a generator of G.

Exercise 9.13 How many generators does $\mathbb{Z}_{48}$ have?

We know $\mathbb{Z}_{48} = \langle 1 \rangle$. It is also generated by all the positive integers relatively prime to 48, $\phi(48)$.

Recall $\phi(n) = n\prod_{p|n,\, p \text{ prime}}(1-\frac{1}{p})$. Then we have:

$$\phi(48) = 2^4 \cdot 3(1-\frac{1}{2})(1-\frac{1}{3}) \qquad = 2^3(2) = 16$$

Recall that if $(m,n) = 1$ then $\phi(m,n) = \phi(m)\phi(n)$. Also $a^{\phi(n)} = 1 \pmod{n}$ if $(a,n) = 1$.

Exercise 9.14 Draw the subgroup lattice of $\mathbb{Z}_{48}$.

The divisors of 48 are 1, 2, 3, 4, 6, 8, 12, 16, 24, 48.

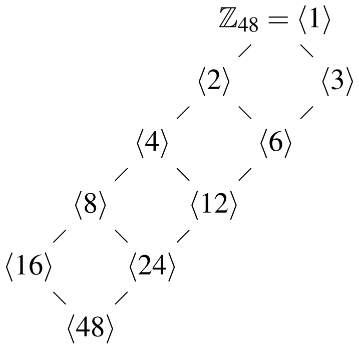


Figure 9.1: The lattice diagram of $\mathbb{Z}_{48}$

Given a group $(G,\cdot)$, how do we generate a subgroup? Take $A \subset G$, $A < \infty$. Then $\langle A \rangle \leqslant G$. Assume $\{a_1, \dots, a_m\}$. Then $\langle A \rangle = \left\{\prod_{i=1}^{m} a_i^{\alpha_i}, \alpha_i \in \mathbb{Z} \text{ and } m \in \mathbb{Z}^+\right\}$.

Exercise 9.15 Let $G = GL(2,\mathbb{R})$. Is $H = \{A \in G \mid \det(A) \in \mathbb{Q}\} \leq G$?

True, because rationals are closed, and $\det(AB) = \det(A)\det(B)$.

Exercise 9.16 Let $G = GL(2,\mathbb{R})$. Is $H = \{A \in G \mid \det(A) \in I\} \leq G$?

False, because irrationals are not closed, $\sqrt{2}\cdot\sqrt{2} = 2$.

Exercise 9.17 Let $G = (\{f : \mathbb{R} \to \mathbb{R}\}, +)$, which is pointwise addition. Give a subgroup of G.

Then $H = \mathbb{C}(\mathbb{R},\mathbb{R})$, the set of continuous functions is a subgroup of G.

Also $H' = \{f : \mathbb{R} \to \mathbb{R} \mid f(0) = 0\}$.

9.5 Homomorphism Exercises

Exercise 9.18 Prove that if G, G' are cyclic groups of the same order, then $\exists \phi : G \xrightarrow{\sim} G'$ which is an isomorphism.

$\exists x \in G, x' \in G'$ such that $G = \langle x \rangle, G' = \langle x' \rangle$. Define $\phi : x^k \mapsto x'^k, k \in \mathbb{Z}$.

Exercise 9.19 Let $|G| = |\mathbb{N}|$ and $G = \langle x \rangle$. Define an isomorphism between G and $\mathbb{Z}$.

Then we can define $\phi : k \mapsto x^k, k \in \mathbb{Z}$.

Exercise 9.20 Prove that $\mathbb{Z}\oplus\mathbb{Z}_2$ and $\mathbb{Z}$ are not isomorphic.

We have the property given a homomorphism $\phi : G \to G'$, $\forall g \in G$ such that $|G| < \infty$, then $|\phi(g)| \mid |g|$. If it's an isomorphism, then $|\phi(g)| = |g|$.

Proof. Consider $(0,1) \in \mathbb{Z}\oplus\mathbb{Z}_2$. We have $|(0,1)| = 2$.

Suppose $\exists\phi : \mathbb{Z}\oplus\mathbb{Z}_2 \xrightarrow{\sim} \mathbb{Z}$. Then $\phi((0,1)) = x$ for some x in $\mathbb{Z}$. Then $\phi((0,1)^2) = x^2 = 0 = \phi((0,0))$. But $\nexists x \in \mathbb{Z}, |x| = 2$. □

We have another proof:

Proof. Suppose $\exists\phi : \mathbb{Z}\oplus\mathbb{Z}_2 \xrightarrow{\sim} \mathbb{Z}$. Take any $(m,i) \in \mathbb{Z}\oplus\mathbb{Z}_2$.

Consider $\phi(1) = (m,i)$.

Claim that $\phi^{-1}((m,1-i)) = \varnothing$. Suppose $\exists n \in \mathbb{Z}$ such that $\phi(n) = (m,1-i)$ and build a contradiction. □

Exercise 9.21 Prove $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Proof. Suppose there is an isomorphism, $\exists\phi : \mathbb{Q} \xrightarrow{\sim} \mathbb{Z}$.

Since ϕ is surjective, $\exists q \in \mathbb{Q}$ such that $\phi(q) = 1$.

Then $\exists a,b \in \mathbb{Z}, b \neq 0, q = \frac{a}{b}$. So $\phi\left(\frac{a}{b}\right)$.

Also $\frac{a}{2b} \in \mathbb{Q}$. Say $\phi\left(\frac{a}{2b}\right) = m$.

So consider $1 = \phi\left(\frac{a}{b}\right) = \phi\left(\frac{a}{2b} + \frac{a}{2b}\right) = \phi\left(\frac{a}{2b}\right) + \phi\left(\frac{a}{2b}\right) = m + m$. But no such integer m exists. □

Exercise 9.22 Prove $\mathbb{R}^\times$ and $\mathbb{C}^\times$ are not isomorphic.

Suppose $\exists\phi : \mathbb{C}^\times \xrightarrow{\sim} \mathbb{R}^\times$.

Consider $\left|e^{\frac{2\pi i}{3}}\right| = 3$. There is no such $x \in \mathbb{R}$ such that $x^3 = 1$.

We get $\phi\left(e^{\frac{2\pi i}{3}}\right) = \phi(1)$ which gives $x^3 = 1$.

Exercise 9.23 Prove that $\mathbb{Q}$ and $\mathbb{R}$ are not isomorphic.

$|\mathbb{Q}| \neq |\mathbb{R}|$ so they are not isomorphic.

We can also prove by showing an isomorphism can't exist.

Exercise 9.24 Suppose $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ and $\phi(7) = 6$. Determine $\phi^{-1}(\{3\})$.

9.5.1 More Homomorphism Exercises

Exercise 9.25 Prove that $\mathbb{Z}\oplus\mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}$.

Proof. Consider any injective homomorphism $\phi : \mathbb{Z} \to \mathbb{Z} \hookrightarrow \mathbb{Z}_2$. Then $\ker(\phi) = \{0\}$.

Then we claim ϕ cannot be surjective.

Consider that $\phi(1) = (m,0)$ or $(m,1)$ for some $m \in \mathbb{Z}$.

If $\phi(1)=(m,0)$, then $(m,1)$ has no preimage. Assume $\exists n\in\mathbb{Z},\phi(m)=(m,1)$. We have

$$\begin{aligned}\phi(n)&=\phi(\underbrace{1+1+\cdots+1}_{n\text{ times}})\\&=\underbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}_{n\text{ times}}\\&=\underbrace{(m,0)+(m,0)+\cdots+(m,0)}_{n\text{ times}}\\&=(nm,0)\neq(m,1)\end{aligned}$$

If $\phi(1)=(m,1)$, then $(m,0)$ has no preimage either. Assume $\exists n\in\mathbb{Z},\phi(m)=(m,0)$. We have

$$\begin{aligned}\phi(n)&=\phi(\underbrace{1+1+\cdots+1}_{n\text{ times}})\\&=\underbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}_{n\text{ times}}\\&=\underbrace{(m,1)+(m,1)+\cdots+(m,1)}_{n\text{ times}}\\&=(nm,0) &&\text{(Then } n \text{ is even.)}\end{aligned}$$

So $nm=m\Rightarrow m(n-1)=0$. Either $n=1$ (contradiction) or $m=0$. If $m=0$, then $\phi(n)=(0,0)$, which can't happen because $n\notin\ker(\phi)$ (contradiction). □

Exercise 9.26 Suppose $\phi:G\xrightarrow{\sim}H$ is an isomorphism with $(G,\cdot)$ and $(H,*)$. Prove that $\phi^{-1}:H\to G$ is a homomorphism.

Proof. Consider $h,h'\in H$.

We have to show that $\phi^{-1}(h*h')=\phi^{-1}(h)\cdot\phi^{-1}(h')$.

Since ϕ is an isomorphism, $\exists!g,g'\in G$ such that $\phi(g)=h$ and $\phi(g')=h'$. Let $b=h*h'$ (which exists by closure). Then $\exists!a\in G$ such that $\phi(a)=b$.

$\therefore a=\phi^{-1}(b)=\phi^{-1}(h*h')$ and $a=g\cdot g'=\phi^{-1}(h)\cdot\phi^{-1}(h')$. (If $g\cdot g'\neq a$ then $\phi(g\cdot g')=\phi(g')*\phi(g)=h*h'=b$ which is a contradiction since $\{e\}\subset\ker(\phi)$ which means ϕ not injective). □

Exercise 9.27 Suppose $|G|<\infty$. What's the lower bound on the number of isomorphisms from G into G?

There are at least $|G|=n$ isomorphisms. $\forall x\in G$, we have $\phi_x:G\to G$ where $g\mapsto xgx^{-1}$. Show this is an isomorphism, that is, show it is a homomorphism, then show it is bijective.

9.6 Midterm Review

9.6.1 True/False Questions

Exercise 9.28 The product of disjoint cycles is even only if the number of odd cycles in the product is even.

True. S_n is the group of permutations (bijective maps $\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$). We have that $|S_n|=n!$. Given $\alpha\in S_n$, α can be written as a product of 2-cycles. Also, α is a cycle or a product of disjoint cycles.

Exercise 9.29 There is no group G of infinite order such that the order of all of its elements is finite.

False. For example, $G = \mathbb{Z}_3[x] = \left\{ p(x) = \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{Z}_3 \right\}$ which is a group under pointwise addition.

Another example, $G = \{ c \in \mathbb{C} \mid \exists n \in \mathbb{Z}, c^n = 1 \}$.

Exercise 9.30 There is a group of infinite order such that infinitely many elements have finite order and infinitely many elements have infinite order.

True. **We haven't done this yet.** Consider $\mathbb{Q}/\mathbb{Z}$. Then for any $n \in \mathbb{Z} \setminus \{0,1\}, |n| = \infty$ and for any $m \in \mathbb{Z} \setminus \{0\}, |{}^1\!/\!_m| = m$. This shows that if G is cyclic, then $\exists a \in G$ such that $\langle a \rangle = G$, then $\forall H \leqslant G$, H is cyclic and for all $m \mid |G|, \exists! H_m \leqslant G$ with $|H_m| = m$.

It only holds for cyclic groups.

Consider $U(8) = \{ n \in \mathbb{Z} \mid \exists m \in \mathbb{Z}_8, nm = 1 \} = \{ x \in \mathbb{Z}_8 \mid (8,x) = 1 \}$. It is not cyclic. $U(8) = \{1,3,5,7\}$ but none of the elements have order 4. This is only one way to show a group is not cyclic. Another way to show it is not cyclic, you can show $\forall a \in G, \langle a \rangle \neq G$, or you can just show it contradicts the FTOCG which states there is a subgroup of unique order generated by an element. For example, $\langle 3 \rangle = \{1,3\}$ and $\langle 5 \rangle = \{1,5\}$

9.6.2 Other questions

Exercise 9.31 Given that $U(100)$ is cyclic, how many elements of order 25 does $U(100)$ have?

There are 0 such elements because the order of $U(100)$ is 40. We have $|U(100)| = \phi(100) = 100\prod_{p|100}(1-\frac{1}{p}) = 100(1-\frac{1}{2})(1-\frac{1}{5}) = 40$.

Exercise 9.32 How many elements of order 20 in $U(100)$?

Recall given $\langle a \rangle = G$ and $|\langle a \rangle| = n$, $\left\langle a^d \right\rangle = G \Leftrightarrow (n,d) = 1$. Therefore, $\phi(n)$, so in this case, we consider $\phi(20)$.

Exercise 9.33 Suppose G is a group such that if $axb = cxd \Rightarrow ab = cd$ then G is abelian. Prove this.

Exercise 9.34 Prove that $\mathbb{Q}$ and $\mathbb{R}$ are isomorphic without using cardinality.

Assume on the contrary that $\exists \phi : \mathbb{Q} \to \mathbb{R}$ which is an isomorphism. Observe that $\mathbb{Z} \leqslant \mathbb{Q}$. We know that $\mathbb{Z}$ is cyclic. This implies $\phi(\mathbb{Z}) \leqslant \mathbb{R}$ must be cyclic since it is an isomorphism. Also, we know that generators are mapped to generators. We can show $\phi(1) = 1$ so $\phi(m) = m, \forall m \in \mathbb{Z}$.

Now consider $\phi^{-1}(\sqrt{2}) = \frac{m}{n} \in \mathbb{Q}$. By surjectivity, $\phi\left(\frac{m}{n}\right) = \sqrt{2}$. But then $\phi\left(n \cdot \frac{m}{n}\right) = n\sqrt{2}$. But also $\phi\left(n \cdot \frac{m}{n}\right) = \phi(m) = m$. Contradiction.

Exercise 9.35 Suppose $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ and $\phi(7) = 6$. Determine $\phi(x)$, the image of $\phi(x)$, and $\phi^{-1}(\{3\})$.

First note $|\langle 7 \rangle| = \frac{50}{(50,7)} = 50$. We know that $|\phi(7) = 6| \mid 50$. We have that $|6| = 5$. Then $\Im(\phi) = \{6,12,3,9,0\} = \langle 3 \rangle$ (which we get from $\phi(n7)$).

Note that we have that 7 is a generator of $\mathbb{Z}_{50}$. $7 \mapsto 6, 2 \cdot 7 \mapsto 12, 3 \cdot 7 \mapsto 3, 4 \cdot 7 \mapsto 9, 5 \cdot 7 \mapsto 0$.

We know $\exists n_x \in \mathbb{Z}$ such that $x = n \cdot 7 \pmod{50}$.

$$\phi(x) = \begin{cases} 6 & n_x = 1 \pmod{5} \\ 12 & n_x = 2 \pmod{5} \\ 3 & n_x = 3 \pmod{5} \\ 9 & n_x = 4 \pmod{5} \\ 0 & n_x = 0 \pmod{5} \end{cases}$$

We have that $21 \in \phi^{-1}(3)$. Note $\forall g \in \ker(\phi) \leqslant \mathbb{Z}_{50}, \phi(g+21) = \phi(g) + \phi(21) = 0 + 3 = 3$. So $\ker(\phi) = \{5n \pmod{30}\}$. So $\phi^{-1}(3) = 21 + \ker(\phi)$.

Exercise 9.36 Suppose $\phi : \mathbb{Z} \oplus \mathbb{Z} \to G$ where $\phi((3,2)) = a$ and $\phi((2,1)) = b$. Determine $\phi((4,4))$.

Use $\phi(g^k) = (\phi(g))^k, \forall n \in \mathbb{Z}$.

Exercise 9.37 Show that S_{15} does not have an element of order 50.

Exercise 9.38 Suppose $\phi : G \to H$ and $\psi : G \to H$ are homomorphisms. Let $G' = \{x \in G \mid \phi(x) = \psi(x)\}$. Prove or disprove $G' \leq G$.

Part Three

Bibliography

Books

Gal17 Gallian, J. A. *Contemporary Abstract Algebra* 9th edition (Cengage Learning, Boston, MA, 2017).

Index