# *Groups and Rings*

PMATH 347

William Slofstra

LaTeXed by Sibelius Peng

# Preface

**Disclaimer** Much of the information on this set of notes is transcribed directly/indirectly from the lectures of PMATH 347 during Spring 2020 as well as other related resources. I do not make any warranties about the completeness, reliability and accuracy of this set of notes. Use at your own risk.

Spring 2020 classes online only. So the grading scheme:

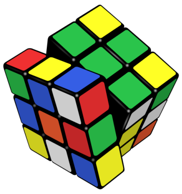
- Participation: 4%
- Quizzes: 32%
- Written homework: 32%
- Final takehome exam: 32%

For any questions, send me an email via `https://notes.sibeliusp.com/contact/`.

You can find my notes for other courses on `https://notes.sibeliusp.com/`.

Sibelius Peng

# Contents



# Part I:

# Group Theory

It is important to realize, with or without the historical context, that the reason the abstract definitions are made is because it is useful to isolate specific characteristics and consider what structure is imposed on an object having these characteristics.

*Abstract Algebra, Third Edition*

# 1 Introduction to Groups

## 1.1 Binary Operations

week 1

If we randomly ask someone on the street: *What's math about?* The answer we might get is **numbers**. It always comes with **operations**.

| Objects | Operations |
|---|---|
| Natural numbers $\mathbb{N}$ | addition $+$<br>subtraction $-$<br>multiplication $\cdot$<br>division with remainders |
| Integers $\mathbb{Z}$ | negation $x \mapsto -x$ |
| Rational number $\mathbb{Q}$ | multiplicative inversion $x \mapsto 1/x$ |
| Real numbers $\mathbb{R}$ | $k$th roots, etc |
| $\mathbb{Z}/n\mathbb{Z}$ | modular arithmetic and operations |

Then we realizd that math is not just about numbers. We later have **elementary algebra**:

| Objects | Operations |
|---|---|
| Expressions with variables | operations with variables |
| Functions | Pointwise operations $+, -, \cdot$ and Composition $\circ$ |

Then ..., and (leaving lots of stuff out), we have **linear algebra**:

| Objects | Operations |
|---|---|
| Vectors | Vector addition $+$, scalar multiplication $\cdot$ |
| Matrices | $+, -,$ scalar and matrix multiplication $\cdot$ |

Then *what's algebra about?*

Pre-university answer:

- manipulating expr involving indeterminates (variables):

If $a, b \in \mathbb{R}, ax = b$ and $a \neq 0$, then $x = \frac{b}{a}$.

- solving eqs by applying ops to both sides:
  If $A, B$ are matrices, $AX = B$ and $A$ is invertible, then $X = A^{-1}B$.

**Key idea**: algebra is about operations

Then *what operations should we study?* Polynomials in several vars; functions, pointwise ops and function composition... *Are there other operations we should study?* Then we introduce **abstract algebra**: try to answer this question by studying operations abstractly, and seeing what the possibilities are.

**binary operation**

A binary operation on a set $X$ is a function $b : X \times X \to X$.

Notation:

- Any letter $(b, m)$ or symbol $(+, \cdot)$
- function notation
$$b : X \times X \to X : (x, y) \mapsto b(x, y)$$
  or inline notation
$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (x, y) \mapsto x + y$$
  Typically use inline notation with symbols and function notation with letters.
- There are lots of symbols to choose from: $a + b, a \times b, a \cdot b, a \circ b, a \oplus b, a \otimes b, a \odot b, a \diamond b, a \lozenge b, a \blacklozenge b, a * b, a \bullet b, a \boxplus b, a \boxtimes b, a \uplus b$
- If there's no chance of confusion, can even drop symbol completely:
$$X \times X \to X : (a, b) \mapsto ab$$

Example:

- Addition $+$ is a binary op on $\mathbb{N}$, but subtraction $-$ is not, since $a - b$ is not necessarily a natural number.
- Subtraction $=$ is a binary op on $\mathbb{Z}$.
- If $(V, +, \cdot)$ is a vector space over a field $\mathbb{K}$, then $+$ is a binary op on $V$, but $\cdot$ is not, since $\cdot$ is a function $\mathbb{K} \times V \to V$.[a]

[a] We'll define fields later, now think of $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$.

**k-ary operation**

A $k$-ary operation on a set $X$ is a function

$$\underbrace{X \times X \times \cdots X}_{k \text{ times}} \to X$$

A 1-ary operation is called a unary operation.

Example:
Negation $\mathbb{Z} \to \mathbb{Z} : x \mapsto -x$ is a unary operation.

Taking the multiplicative inverse $x \mapsto 1/x$ is not a unary operation on $\mathbb{Q}$, since $1/0$ is not defined, but it is a unary operation on

$$\mathbb{Q}^\times := \{a \in \mathbb{Q} : a \neq 0\}$$

Now let's discuss some properties that binary ops might satisfy.

## 1.2 Associativity and commutativity

**associative**

A binary operation $\boxtimes : X \times X \to X$ is associative if

$$a \boxtimes (b \boxtimes c) = (a \boxtimes b) \boxtimes c$$

for all $a, b, c \in X$.

Many operations we've mentioned so far are associative:

- Addition and multiplication for $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, polynomials, and functions
- Vector addition, matrix addition and multiplication
- Modular addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$
- Function composition

Note that Subtraction and division are not associative. Subtraction is adding negative numbers, same for division. So we aren't that interested in subtraction and division, and focus on associative operations.

Here we introduce an informal definition: A **bracketing** of a sequence $a_1, \ldots, a_n \in X$ is a way of inserting brackets into $a_1 \boxtimes \ldots \boxtimes a_n$ so that the expression can be evaluated.

Example:
The bracketings of $a_1, \ldots, a_4$ are

$$a_1 \boxtimes (a_2 \boxtimes (a_3 \boxtimes a_4))$$
$$a_1 \boxtimes ((a_2 \boxtimes a_3) \boxtimes a_4)$$

$$(a_1 \boxtimes a_2) \boxtimes (a_3 \boxtimes a_4)$$
$$(a_1 \boxtimes (a_2 \boxtimes a_3)) \boxtimes a_4$$
$$((a_1 \boxtimes a_2) \boxtimes a_3) \boxtimes a_4$$

**Proposition 1.1**

A binary operation $\boxtimes : X \times X \to X$ is associative if and only if for all finite sequences $a_1, \ldots, a_n \in X, n \geq 1$, every bracketing of $a_1, \ldots, a_n$ evaluated to the same element of $X$.

**Note**
If $\boxtimes$ is associative, can use notation $a_1 \boxtimes a_2 \boxtimes \ldots \boxtimes a_n$ without choosing a bracketing.

Proof:

$\Leftarrow$ The two bracketings $a \boxtimes (b \boxtimes c)$ and $(a \boxtimes b) \boxtimes c$ of $a, b, c$ evaluate to the same element of $X$ for all sequences of length 3.

$\Rightarrow$ Proof is by induction. Base cases are $n = 1, 2, 3$.

For $n = 1, 2$, there's only one bracketing. For $n = 3$ follows from defn of associativity.

Suppose prop is true for all sequences of length $k$, $1 \leq k < n$.

Let $w$ be a bracketing of $a_1, \ldots, a_n$.

$w = w_1 \boxtimes w_2$ where $w_1$ is a bracketing of $a_1, \ldots, a_k$, $w_2$ is a bracketing of $a_{k+1}, \ldots, a_n$, for some $k < n$.

By induction,

$$w_1 = (\cdots((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \quad \text{and} \quad w_2 = (a_{k+1} \boxtimes \cdots (a_{n-1} \boxtimes a_n) \cdots)$$

Therefore

$$\begin{aligned} w &= (\cdots((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \boxtimes w_2 = (a_{k+1} \boxtimes \cdots (a_{n-1} \boxtimes a_n) \cdots) \\ &= (\cdots (a_1 \boxtimes a_2) \cdots \boxtimes a_{k-1}) \boxtimes (a_k \boxtimes (a_{k+1} \boxtimes \cdots a_n) \cdots) \\ &= \cdots \\ &= (a_1 \boxtimes (a_2 \boxtimes \cdots (a_n \boxtimes a_n) \cdots)) \end{aligned}$$

$\square$

**commutative**

A binary operation $\boxtimes : X \times X \to X$ is commutative (also known as abelian) if $a \boxtimes b = b \boxtimes a$ for all $a, b \in X$.

**Fact** The word "abelian" comes from the surname of Niels Henrik Abel (1802-1829).

Many familiar operations are commutative: addition and multiplication on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; vector and matrix addition; modular addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$. The following operation are **not** commutative: subtraction and division; function composition; matrix multiplication.

Therefore, subtraction and division are not commutative or associative. Function composition and matrix multiplication are not commutative, but are associative. We are not going to worry about the first type of operation, but we are interested in operations of the second type.

**First half of the course**: group theory – single associative operation, not necessarily commutative.

**Second half of the course**: ring theory – two associative operations (like addition and multiplication on $\mathbb{Z}$), focus on commutative case.

## 1.3 Identities and inverses

Let $\boxtimes$ be a binary operation on a set $X$.

**identity**

An element $e \in X$ is an identity for $\boxtimes$ if

$$e \boxtimes x = x \boxtimes e = x$$

for all $x \in X$.

Example:
The zero element 0 of $\mathbb{Z}$ is an identity for $+$. $1 \in \mathbb{Q}$ is identity for $\cdot$. $0 \in \mathbb{Q}$ is not identity for $\cdot$

**Lemma 1.2**

If $e, e' \in X$ are both identities for $\boxtimes$, then $e = e'$.

Proof:
$e = e \boxtimes e' = e'$ □

**inverse**

Let $\boxtimes$ be a binary operation on $X$ with identity element $e$. An element $y$ is a left inverse for $x$ (w.r.t. $\boxtimes$) if $y \boxtimes x = e$, a right inverse if $x \boxtimes y = e$, and an inverse if $x \boxtimes y = y \boxtimes x = e$.

Example:
$-n$ is an inverse for $n \in \mathbb{Z}$ w.r.t. $+$.

$n \in \mathbb{Z}$ does not have an inverse w.r.t. $\cdot$ unless $n = \pm 1$.

If $x \in \mathbb{Q}$ is non-zero, then $1/x$ is an inverse of $x$ w.r.t. $\cdot$. The element 0 does not have an inverse.

**Lemma 1.3**

Let $\boxtimes$ be an **associative** binary op with an identity $e$. If $y_L$ and $y_R$ are left and right inverse of $x$ respectively, then $y_L = y_R$.

Proof:
$y_L = y_L \boxtimes e = y_L \boxtimes (x \boxtimes y_R) = (y_L \boxtimes x) \boxtimes y_R = e \boxtimes y_R = y_R$ □

**Corollary 1.4**

- If $x$ has both a left and right inverse, then $x$ has an inverse.
- Inverses are unique.

**invertible**

An element $a$ is invertible if it has an inverse, in which case the inverse is denoted by $a^{-1}$.

Exercise
It's possible to have a left (resp. right inverse), but not be invertible. Also, left and right inverses don't have to be unique (unless an element has both).

**Lemma 1.5**

1. If $\boxtimes$ has an identity $e$, then $e$ is invertible, and $e^{-1} = e$.
2. If $a$ is invertible, then so is $a^{-1}$, and $(a^{-1})^{-1} = a$.
3. If $\boxtimes$ is associative, and $a$ and $b$ are invertible, then so is $a \boxtimes b$, and $(a \boxtimes b)^{-1} = b^{-1} \boxtimes a^{-1}$.

Proof:

1. $e \boxtimes e = e$
2. $a \boxtimes a^{-1} = a^{-1} \boxtimes a = e$, so $a$ is clearly an inverse to $a^{-1}$.
3. $(a \boxtimes b) \boxtimes (b^{-1} \boxtimes a^{-1}) = a \boxtimes (b \boxtimes b^{-1}) \boxtimes a^{-1} = a \boxtimes e \boxtimes a^{-1} = a \boxtimes a^{-1} = e$, and similarly $(b^{-1} \boxtimes a^{-1}) \boxtimes (a \boxtimes b) = e$.

□

**Proposition 1.6**

Let $\boxtimes$ be an associative binary operation on $X$ with identity $e$, and let $x$ and $y$be variables taking values in $X$.

An element $a \in X$ is invertible if and only if the equations

$$a \boxtimes x = b \text{ and } y \boxtimes a = b$$

have unique solutions for all $b \in X$.

Proof:

$\Leftarrow$ A solution to $ax = e$ is a right inverse of $a$, and a solution to $ya = e$ is a left inverse. If $a$ both have a left and right inverse, then it has an inverse.

$\Rightarrow$ Suppose $a$ is invertible. Then

$$a \boxtimes (a^{-1}b) = (a \boxtimes a^{-1}) \boxtimes b = e \boxtimes b = b$$

so $a^{-1} \boxtimes b$ is a solution to $a \boxtimes x = b$.

If $x_0$ is a solution to $a \boxtimes x = b$, then

$$a^{-1} \boxtimes b = a^{-1} \boxtimes (a \boxtimes x_0) = (a^{-1} \boxtimes a) \boxtimes x_0 = e \boxtimes x_0 = x_0$$

So $a^{-1} \boxtimes b$ is the unique solution to $a \boxtimes x = b$.

Similarly $b \boxtimes a^{-1}$ is the unique solution to $y \boxtimes a = b$.

$\square$

**Proposition 1.7: Cancellation property**

Let $\boxtimes$ be an associative binary operation, and $a \in X$. Then

1. If $a$ has a left inverse and $a \boxtimes u = a \boxtimes v$, then $u = v$.
2. If $b$ has a right inverse and $u \boxtimes a = v \boxtimes a$, then $u = v$.

Proof:

1. $u = a^{-1} \boxtimes a \boxtimes u = a^{-1} \boxtimes a \boxtimes v = v$
2. similar.

$\square$

1 and 2 also hold for $n \in \mathbb{Z}$ w.r.t. $\cdot$ if $n \geq 0$, even though $n$ is not invertible for $n \neq \pm 1$.

## 1.4 Groups

**group**

A **group** is a pair $(G, \boxtimes)$, where

1. $G$ is a set, and
2. $\boxtimes$ is an associative binary operation on $G$ such that
   (a) $\boxtimes$ has an identity $e$, and
   (b) every element $g \in G$ is invertible with respect to $\boxtimes$.

**abelian**

A group is **abelian** (or commutative) if $\boxtimes$ is abelian.

**finite**

A group is **finite** if $G$ is a finite set.

**order**

The **order** of $G$ the number of elements in $G$ if $G$ is finite, and $+\infty$ if $G$ is infinite. The order of $G$ is denoted by $|G|$.

### 1.4.1 Terminology

Usually we refer to $(G, \boxtimes)$ simply as $G$, and just assume the operation is given. (Note: we still need to clearly specify the operation for each group we work with).

It's cumbersome to write $\boxtimes$ all the time, so usually we use one of the following options:

- Use $\cdot$ as the standard symbol, write $g \cdot h$ for the product of $g, h \in G$
- Drop the symbol entirely, write $gh$ for the product of $g, h \in G$.

The identity of $G$ is denoted by $e$ (or $e_G$ when we want to make the group clear). 1 and $1_G$ are also used.

Since every element of a group $G$ is invertible, $g^{-1}$ is defined for all $g \in G$. The function $G \to G : G \mapsto g^{-1}$ can be regarded as a unary operation on $G$.

Consider $\iota : G \to G : g \mapsto g^{-1}$. Since $(g^{-1})^{-1} = g$, $\iota \circ \iota = \mathrm{Id}_G$, the identity map $G \to G$. In particular, $\iota$ is a bijection, both injective and surjective.

If $g \in G$, then

$$g^n := \underbrace{g \cdot \dots \cdot g}_{n \text{ times}} \text{ and } g^{-n} := (g^{-1})^n = (g^n)^{-1}$$

Exercise

If $m, n \in \mathbb{Z}$, then $(g^n)^m = g^{mn}$.

If $g, h \in G$, then

$$(gh)^n = ghgh \cdots gh,$$

which is not necessarily the same as $g^n h^n$ if $G$ is not abelian.

Example: Groups

$\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all groups under operation $+$. The identity is 0 and the inverse of $n$ is $-n$. These groups have infinite order. They are infinite abelian groups.

$\mathbb{Z}/n\mathbb{Z}$ is also a group under $+$. The identity is $0 = [0]$, and the inverse of $[m]$ is $-[m] = [-m]$. This group is finite, with order $|\mathbb{Z}/n\mathbb{Z}| = n$. It is a finite abelian group.

If $(V, +, \cdot)$ is a vector space, then $(V, +)$ is group. The identity element is 0, and the inverse of $v$ is $-v$.

Example: Not a group?! & Trivial group

$\mathbb{Z}$ is not a group with respect to $\cdot$, since most elements do not have an inverse.

$\mathbb{Q}$ is also not a group with respect to $\cdot$, since 0 does not have an inverse.

$\mathbb{Q}^\times$ is a group with respect to $\cdot$.

Every group has to contain at least one element, the identity. So the simplest possible group is $\{1\}$ with operation $1 \cdot 1 = 1$. This is called the **trivial group**.

## A non-abelian example

All the examples previously are abelian.

Let $\mathrm{GL}_n(\mathbb{K})$ denote the invertible $n \times n$ matrices with entries in a field $\mathbb{K}$.

**Proposition 1.8**

$\mathrm{GL}_n(\mathbb{K})$ is a group under matrix multiplication (called the **general linear group**). For $n \geq 2$, $\mathrm{GL}_n(\mathbb{K})$ is non-abelian.

Proof:

If $A$ and $B$ are invertible matrices, then $AB$ is also invertible, so matrix multiplication is an associative binary operation $\mathrm{GL}_n(\mathbb{K})$. The identity matrix is an identity, and every element has an inverse by definition, so $\mathrm{GL}_n(\mathbb{K})$ is a group.

Exercise

Find matrices $A, B$ such that $AB \neq BA$.

$\square$

### 1.4.2 Additive notation

Standard notation for operation in a group is $gh$. This is called **multiplicative notation**. For groups like $(\mathbb{Z}, +)$, it is confusion to write $mn$ instead of $m + n$, since $mn$ already has another meaning. For abelian groups $G$, there is another convention called **additive notation**. In additive notation, we write the group operation as $g + h$. The identity is denoted by 0 or $0_G$. Inverse are denoted by $-g$. Writing $g^n$ in additive notation gives

$$\underbrace{g + g + \ldots + g}_{n \text{ times}},$$

so rather than $g^n$ we use $ng$. Similarly $g^{-n}$ is $-ng$.

For nonabelian groups we always use multiplicative notation. For abelian groups, we can choose either.

Note the potential for conflict between the two conventions. We must be clear about what convention we are using!.

For groups like $(\mathbb{Z}, +)$, we could denote the operation by $mn$, but it's clearer to write $m + n$. For groups like $(Q^\times, \cdot)$, we could denote the operation by $x + y$, but it is clearer to write $x \cdot y$ or $xy$.

### 1.4.3 Multiplicative table

**multiplicative table**

The multiplicative table of a group $G$ is a table with rows and columns indexed by the elements of $G$. The cell for row $g$ and column $h$ contains the product $gh$.

The multiplication table contains the complete info of the group $G$. It is defined for finite and infinite groups, but makes the most sense for finite groups.

Example: $\mathbb{Z}/2\mathbb{Z}$

The multiplication table for $\mathbb{Z}/2\mathbb{Z}$ is

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

| Multiplicative notation | Additive notation |
|---|---|
| $g \cdot h$ or $gh$ | $g + h$ |
| $e_G$ or $1_G$ | $0_G$ |
| $g^{-1}$ | $-g$ |
| $g^n$ | $ng$ |

Table 1.1: Comparison between multiplicative and additive notation

### 1.4.4 Order of elements

**order**

If $G$ is a group, then the order $g \in G$ is

$$|G| := \min\{k \geq 1 : g^k = e_G\} \cup \{+\infty\}$$

Some easy properties:

- $|g| = 1$ if and only if $g = e_G$.
- If $g^n = 1$, then $g^{n-1}g = gg^{n-1} = g^n = 1$, so $g^{n-1} = g^{-1}$. In particular, if $|g| = n < +\infty$, then $g^{-1} = g^{n-1}$.

Example: $\mathbb{Z}/n\mathbb{Z}$

We use additive notation for $\mathbb{Z}/n\mathbb{Z}$, so $g^n$ is written as $ng$, $e = 0$. For this group, $k1 = 0$ if and only if $n$ divides $k$, so $|1| = n$.

**Lemma 1.9**

$g^n = e$ if and only if $g^{-n} = e$, so in particular $|g| = |g^{-1}|$.

Proof:

We have $g^{-n} = (g^n)^{-1}$. Since $g \mapsto g^{-1}$ is a bijection,

$$g^n = e \text{ if and only if } (g^n)^{-1} = e^{-1} = e.$$

But $g^{-n}$ also equals $(g^{-1})^n$, so

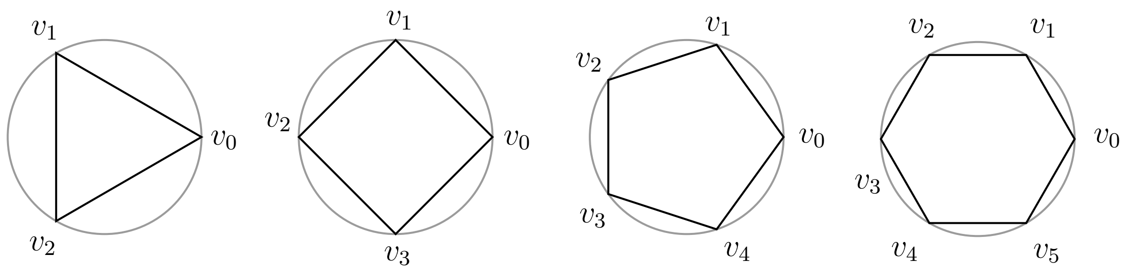
$$\{k \geq 1 : g^k = e\} = \left\{k \geq 1 : \left(g^{-1}\right)^k = e\right\}$$

and this implies $|g| = |g^{-1}|$. □

## 1.5 Dihedral groups

**n-gon**

A regular polygon $P_n$ with n vertices, $n \geq 3$, is called an $n$-gon.




3-gon 4-gon 5-gon 6-gon

To be specific: set $v_k = (\cos 2\pi k/n, \sin 2\pi k/n) = e^{2\pi i k/n}$

Get $n$-gon by drawing line segment from $v_k$ to $v_{k+1}$ for all $0 \leq k \leq n$ (where $v_n := v_0$)

**symmetry**

A symmetry of the $n$-gon $P_n$ is an invertible linear transformation $T \in \mathrm{GL}_2(\mathbb{R})$ such that $T(P_n) = P_n$.

**dihedral group**

The set of symmetries of $P_n$ is called the dihedral group, and is denoted by $D_{2n}$ (or $D_n$).

In this course, we use $D_{2n}$.

**Note**

We think of matrices and invertible linear transformations interchangeably.

Matrix multiplication = composition of transformations.

**Proposition 1.10**

$D_{2n}$ is a group under composition.

Proof:

Later. Key point: $S, T \in D_{2n} \implies ST \in D_{2n}$. □

$v_i$ and $v_j$ are **adjacent** in $P_n$ if connected by line segment.

**Lemma 1.11**

1. If $T \in D_{2n}$ then $(T(v_0), T(v_1))$ are adjacent
2. If $S, T \in D_{2n}$ and $S(v_i) = T(v_i)$, $i = 0, 1$ then $S = T$.

Proof:

1. $v_0, v_1$ are adjacent, $T$ is linear
2. $v_0$ and $v_1$ are linearly independent.

□

**Corollary 1.12**

$|D_{2n}| \leq 2n$

Proof:
Let $A$ be the set of adjacent pairs $(v_i, v_j)$[a], so $|A| = 2n$. By Lemma 1.11, $D_{2n} \to A : T \mapsto (T(v_0), T(v_1))$ is well-defined and injective. □

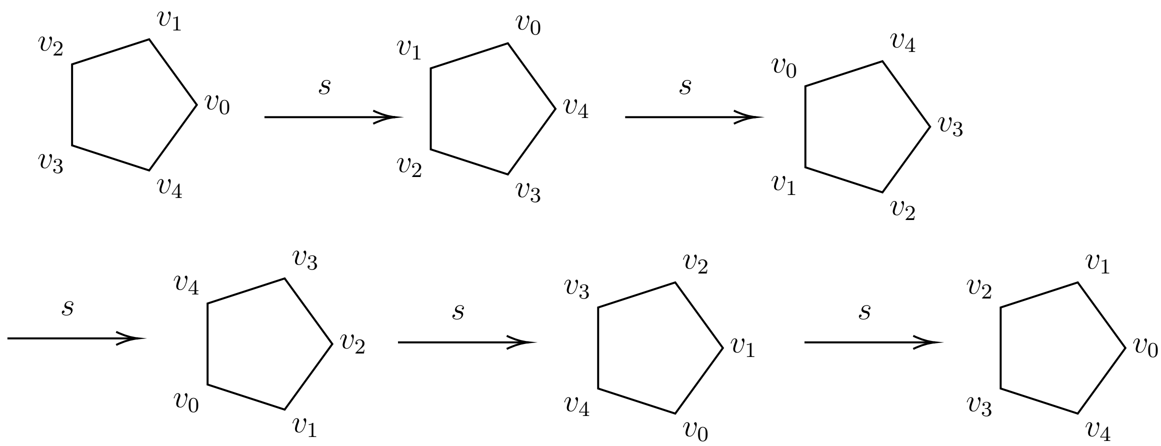
[a] ordered pairs

For every pair of adjacent vertices $(v_i, v_j)$, is there an element $T \in D_{2n}$ with $T(v_0) = v_i, T(v_1) = v_j$?

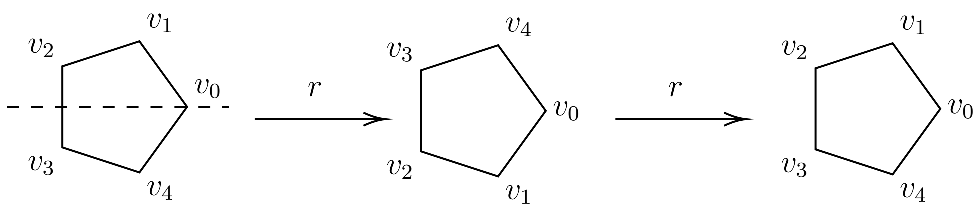
If the answer is yes, then $|D_{2n}| = 2n$.

### 1.5.1 Special elements of $D_{2n}$

Let $s \in D_{2n}$ be rotation by $2\pi/n$ radians, so $|s| = n$ (i.e., $s^n = 2, s^k \neq e$ for $1 \leq k < n$).




Let $r$ be reflection through the $x$-axis:

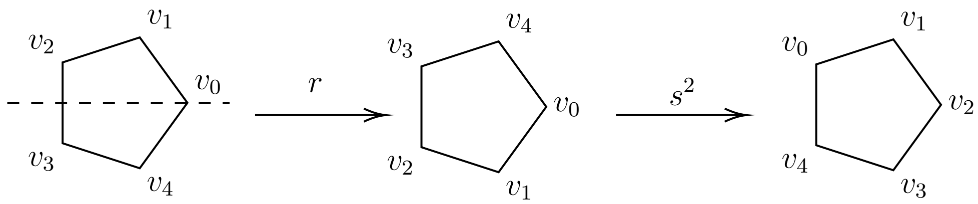



$|r| = 2$, i.e. $r^2 = e, r \neq e$.

$r(v_0) = v_0$. $r(v_1)$ is now the vertex before $v_0$, rather than the vertex after $v_0$.

If we try to put these two elements together:

1. $s^i$, $0 \leq i < n$: sends $v_0 \mapsto v_i, v_1 \mapsto v_{i+1}$ (notes: $v_n = v_0$, $s^0$ is the identity)
2. $s^i r, 0 \leq i < n$: sends $v_0 \mapsto v_i$, $v_1 \mapsto v_{i-1}$ (notes: $v_{-1} = v_{n-1}$)




**Proposition 1.13**

$D_{2n} = \{s^i r^j : 0 \leq i < n, 0 \leq j < 2\}$, so $|D_{2n}| = 2n$.

*What is $rs$?*

$rs(v_0) = r(v_1) = v_{n-1}$ and $rs(v_1) = r(v_2) = v_{n-2}$. So

$$rs = s^{n-1} r = s^{-1} r$$

**Corollary 1.14**

$D_{2n}$ is a finite nonabelian group.

Exercise

$D_{2n} = \{s^i r^j : 0 \leq i < n, 0 \leq j < 2\}$

$|D_{2n}| = 2n$

$s^n = e, r^2 = e, rs = s^{-1} r$

These relations are enough to completely determine $D_{2n}$.

*What's group theory about?*

Basic answer: study sets with one binary op. A better answer: group theory is study of symmetry. If we resize or rotate $P_n$, then symmetries are the same.

Kleinian view of geometry:

- $D_{2n}$ captures what it means to be a regular $n$-gon
- More generally, geometry is about study of symmetries

## 1.6 Permutation groups

If $X$ is a set, let $\mathrm{Fun}(X, X)$ be set of functions $X \to X$. Then

$$\circ : \mathrm{Fun}(X, X) \times \mathrm{Fun}(X, X) \to \mathrm{Fun}(X, X) : (f, g) \mapsto f \circ g$$

is an associative operation with an identity $\mathrm{Id}_X$. Let $S_X = \{f \in \mathrm{Fun}(X, X) : f \text{ is a bijection}\}$

**Proposition 1.15**

$S_X$ is a group under $\circ$.

Proof:
See homework. $\square$

**symmetric/permutation group**

Let $n \geq 1$. The symmetric group (or permutation group) $S_n$ is the group $S_X$ with $X = \{1, \ldots, n\}$.

Elements of $S_n$ are bijections $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$

*What makes a function $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ a bijection?*

Every element of $\{1, \ldots, n\}$ must appear in the list $\pi(1), \ldots, \pi(n)$, and no element can appear twice ($\Leftarrow$ redundant by pig.-hole princ.)

*How many elements in $S_n$?*

$n$ choices for $\pi(1)$, $n-1$ choices for $\pi(2)$, ..., 1 choice for $\pi(n)$. So $n(n-1)\cdots 1 = n!$ choices $\implies |S_n| = n!$.

Note $|S_1| = 1! = 1$, so $S_1$ is the trivial group.

### 1.6.1 Representations

Elements of $S_n$ are called **permutations**. There are a number of different ways to represent permutations:

1. **Two-line representation**:

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

2. **One-line representation**:

$$\pi = 651423$$

   This representation saves space than the previous one, but it is hard to do operations in group theory. The one below seems counter-intuitive, but convenient for doing operations.

3. Note $\pi(1) = 6, \pi(6) = 3, \pi(3) = 1$. Say $(163)$ is a **cycle** of $\pi$.

   **Disjoint cycle representation**: write down cycles of $\pi$

$$\pi = (163)(25)(4) = (163)(25)$$

We typically drop cycles of length 1.

Identity is empty in disjoint cycle notation, so just use $e$.

The convention is that we start from the lowest item in the cycle, and sort the cycles by their lowest items.

## Multiplication

Multiplication can be done in two-line or disjoint cycle notation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (163)(25)$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & 1 \end{pmatrix} = (126)(345)$$

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 1 & 6 \end{pmatrix} = (15)(234)$$

Note $i$ comes from the right: $\pi(\sigma(i))$.

(It's a bit of a pain in one-line notation, so we don't use one-line notation often in group theory)

## Inversion

We can also take inverse in two-line or disjoint cycle notation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (163)(25)$$

$$\pi^{-1} = \begin{pmatrix} 6 & 5 & 1 & 4 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \stackrel{*}{=} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} = (136)(25)$$

$*$: swap two rows and sort the columns by the first row. Disjoint cycle notation is even easier.

If $\pi(i) = j$, then $\pi^{-1}(j) = i$, so cycles of $\pi^{-1}$ are cycles of $\pi$ in opposite order.

**fixed points**

The fixed points of a permutation $\pi \in S_n$ are the numbers $1 \le i \le n$ such that $\pi(i) = i$.

**support set**

The support set of $\pi \in S_n$ is

$$\operatorname{supp}(\pi) = \{1 \le i \le n : \pi(i) \ne i\}$$

**disjoint**

$\pi$ and $\sigma$ are disjoint if $\mathrm{supp}(\pi) \cap \mathrm{supp}(\sigma) = \varnothing$

Example:

$\mathrm{supp}((163)(25)) = \{1, 2, 3, 5, 6\}$

Remark:

In general, $\mathrm{supp}(\pi)$ are numbers that appear in disjoint cycle representation of $\pi$ (when cycles of length one are dropped).

$\mathrm{supp}(\pi) = \varnothing$ if and only if $\pi = e$

$\mathrm{supp}(\pi^{-1}) = \mathrm{supp}(\pi)$

If $i \in \mathrm{supp}(\pi)$, then $\pi(i) \in \mathrm{supp}(\pi)$

**commute**

Two elements $g, h$ in a group $G$ commute if $gh = hg$.

**Lemma 1.16**

If $\pi, \sigma \in S_n$ are disjoint, then $\pi\sigma = \sigma\pi$.

Proof:

Suppose $1 \le i \le n$. If $i \in \mathrm{supp}(i)$, then $\pi(i) \in \mathrm{supp}(\pi)$. Since $\pi, \sigma$ disjoint, $i, \pi(i) \notin \mathrm{supp}(\sigma)$. So $\pi(\sigma(i)) = \pi(i) = \sigma(\pi(i))$.

By symmetry, $\pi(\sigma(i)) = \sigma(\pi(i))$ if $i \in \mathrm{supp}(\sigma)$.

If $i \notin \mathrm{supp}(\pi) \cup \mathrm{supp}(\sigma)$, then $\pi(\sigma(i)) = i = \sigma(\pi(i))$.

So $\pi(\sigma(i)) = \sigma(\pi(i))$ for all $i \implies \pi\sigma = \sigma\pi$. □

### 1.6.2 Cycles

**k-cycle**

A $k$-cycle is an element of $S_n$ with disjoint cycle notation $(i_1 i_2 \cdots i_k)$.

Suppose cycles of $\pi \in S_n$ are $c_1, \ldots, c_k$. We can regard $c_i$ as an element of $S_n$, $\pi = c_1 \cdot c_2 \cdot \cdots \cdot c_k$ as product in $S_n$. $c_i$ and $c_j$ are disjoint, so $c_i c_j = c_j c_i$. Note that order of cycles in disjoint cycle representation doesn't matter.

Example:

$\pi = (163)(25) = (25) \cdot (163)$

We can also get an interesting prospective on this formula for the inverse of $\pi$ in the disjoint cycle notation. If $c_1, \ldots, c_k$ are cycles of $\pi$, then $\pi = c_1 c_2 \cdots c_k$ as product in $S_n$.

$c_i$ and $c_j$ are disjoint, so $c_i c_j = c_j c_i$.
$\pi^{-1} = c_k^{-1} \cdots c_1^{-1} = c_1^{-1} \cdots c_k^{-1}$

> Example:
>
> If $c$ and $c'$ are non-disjoint cycles, then they don't necessarily commute:
> $(12)(23) = (123)$ while $(23)(12) = (123)^{-1} = (132) \neq (12)(23)$.

If $\pi$ is a permutation, then $\pi$ commutes with $\pi^i$ for all $i$ since $\pi^{i+1} = \pi\pi^i = \pi^i\pi$, so $\pi$ and $\pi^i$ commute. However, note that they don't necessarily have disjoint support sets.

# 2

# Subgroups

## 2.1 Subgroups

week 2

**subgroup**

Let $(G, \cdot)$ be a group. A subset $H \subseteq G$ is a **subgroup** if

(a) for all $g, h \in H$, $g \cdot h \in H$ ($H$ is **closed under products**),

(b) for all $g \in H$, $g^{-1} \in H$ ($H$ is **closed under inverses**), and

(c) $e_G \in H$.

Notation $H \leq G$.

Example:
$\mathbb{Z} \leq \mathbb{Q}^+ := (\mathbb{Q}, +)$

$\mathbb{Q}_{>0} := \{x \in \mathbb{Q} : x > 0\} \leq \mathbb{Q}^\times$.

To check this: if $x, y \in \mathbb{Q}$, $x, y > 0$, then $xy > 0 \implies xy \in \mathbb{Q}_{>0}$.

Also, if $x > 0$, then $1/x > 0 \implies 1/x \in \mathbb{Q}_{>0}$.

Example: More complicated
Let $G = D_{2n}$, $s$ rotation.

$H = e = s^0, s, s^2, \ldots, s^{n-1}$ is a subgroup of $D_{2n}$.

Proof:

**Claim** $s^i \in H$ for all $i \in \mathbb{Z}$.

**Proof** Let $i = nk + r, 0 \le r < n$. Then $s^i = s^{nk+r} = (s^n)^k s^r = s^r$, since $s^n = e$. ■

Now check subgroup: if $s^i, s^j \in H$, then $s^{i+j} \in H$. If $s^i \in H$, then $s^{-i} \in H$. Finally, $e \in H$ by construction. □

$H$ is the smallest subgroup containing $s$. The notation for $H$ is $\langle s \rangle$.

Example: $\mathbb{Z}$

Let $G = \mathbb{Z} = (\mathbb{Z}, +)$.

If $m \in \mathbb{Z}$, then $m\mathbb{Z} := \{km : k \in \mathbb{Z}\} = \{n \in \mathbb{Z} : m|n\}$ is a subgroup of $\mathbb{Z}$.

In particular, if $m = 0$, then $0\mathbb{Z} = \{0\}$ is a subgroup of $\mathbb{Z}$, which is called the **trivial subgroup**.

**trivial subgroup**

If $G$ is a group, $\{e\}$ is a subgroup called the **trivial subgroup**.

**proper subgroup**

Also, $G$ is a subgroup of $G$. A subgroup $H$ is **proper** if $H \neq G$. Notation: $H < G$.

$H$ is proper nontrivial subgroup if $\{e\} \neq H < G$.

Example: Not subgroups

$\mathbb{Q}_{\geq 0} := \{x \in \mathbb{Q} : x \geq 0\}$ is not a subgroup of $\mathbb{Q}^+$. We can verify as follows: If $x, y \in \mathbb{Q}_{\geq 0}$, then $x + y \in \mathbb{Q}_{\geq 0}$. Also $0 \in \mathbb{Q}_{\geq 0}$. But if $x \in \mathbb{Q}_{\geq 0}$, then $-x \notin \mathbb{Q}_{\geq 0}$ unless $x = 0$.

$\mathbb{Q}^\times$ is not a subgroup of $(\mathbb{Q}, \cdot)$ because $(\mathbb{Q}, \cdot)$ is not a group.

**Proposition 2.1**

If $H$ is a subgroup of $(G, \boxtimes)$, then $(H, \boxtimes|_{H\times H})$ is a group, such that

(a) the identity of $H$ is $e_H = e_G$, and

(b) the inverse of $g \in H$ is the same as the inverse of $g$ in $G$.

Proof:

First, why is $\boxtimes|_{H\times H}$ a binary operation on $H$?

Recall $\boxtimes$ is a function $G \boxtimes G \to G$ which implies $\boxtimes|_{H\times H}$ is a function $H \times H \to G$ if we restrict its domain. But if $g, h \in H$, then $g \boxtimes h \in H$. So we can think of $\boxtimes|_{H\times H}$ as function $H \times H \to H$. For the rest of this proof, we just denote this function by $\tilde{\boxtimes}$.

Since $\boxtimes$ is associative, $\tilde{\boxtimes}$ is also associative.

$e_H = e_G$ is identity for $\tilde{\boxtimes}$.

If $g \in H$, then inverse $g^{-1}$ with respect to $\boxtimes$ is in $H$ by the definition of subgroup.

Since $g \tilde{\boxtimes} g^{-1} = g \boxtimes g^{-1} = e_G = e_H$, and similarly $g^{-1} \boxtimes g = e_H$, $g^{-1}$ is inverse of $g$ with respect to $\tilde{\boxtimes}$.

So $(H, \tilde{\boxtimes})$ is a group. □

Call $\tilde{\boxtimes}$ the **operation induced by** $\boxtimes$ on $H$. Usually just refer to $\tilde{\boxtimes}$ as $\boxtimes$.

Example:
$\mathbb{Z}$ is subgroup $\mathbb{Q}$ with operation $+$.

If $H$ is group of $(G, \cdot)$, then $H$ is group with operation $\cdot$.

**Proposition 2.2**

$H$ is subgroup if and only if

(a) $H$ is non-empty, and

(b) $gh^{-1} \in H$ for all $g, h \in H$.

Proof:

$\Rightarrow$ If $H$ is a subgroup of $G$, then $e_G \in H$, so $H \neq \varnothing$. Also if $g, h \in H$, then $h^{-1} \in H$, so $gh^{-1} \in H$.

$\Leftarrow$ By (a), there is some element $x \in H$. In part (b), let $g = h := x$, then $xx^{-1} = e_G = e_H \in H$.

Also by (b), $e_G \cdot x^{-1} = x^{-1} \in H$ (closed under inverses).

If $x, y \in H$, then $y^{-1} \in H$, so $xy = x(y^{-1})^{-1} \in H$ (closed under inverses).

□

Example:
Let $(V, +, \cdot)$ be a vector space.

If $W$ is a subspace of $V$, then $W$ is a subgroup of $(V, +)$.

Check:

- $0 \in W$ so $W$ is non-empty.
- If $v, w \in W$, then $v - w \in W$.

Conclusion: $W$ is subgroup.

**Proposition 2.3**

Suppose $H$ is a finite subset of $G$. Then $H$ is a subgroup of $G$ if and only if

(a) $H$ is non-empty, and

(b) $gh \in H$ for all $g, h \in H$.

Proof:
Since $H$ is nonempty, suppose $g \in H$. By induction, we can show $g^n \in H$ for all $n \in \mathbb{N}$. Since $H$ is finite, sequence $g, g^2, g^3, \ldots \in H$ must eventually repeat. So $g^i = g^j$ for some $1 \leq i < j \implies g^n = e$ for $n = j - i$. Since $i < j$, then $n \geq 1$, therefore $g^n = e \in H$.

Now we need to show it is closed under inverses.

- $n = 1$, then $g = e = g^{-1}$.
- $n > 1$, then $g^{n-1} = g^{-1} \in H$.

$\square$

## 2.2 Subgroups generated by a set

**Proposition 2.4**

Suppose $\mathcal{F}$ is a non-empty set of subgroups of $G$. Then

$$L := \bigcap_{H \in \mathcal{F}} H$$

is a subgroup of $G$.

Proof:
First we check it is non-empty. Since $e_G \in H$ for all $H \in \mathcal{F}$, then $e_G \in K \implies K$ is non-empty.

Suppose $x, y \in K$, then

$$\begin{aligned} &\implies x, y \in H \quad \forall H \in \mathcal{F} \\ &\implies y^{-1} \in H \quad \forall H \in \mathcal{F} \\ &\implies xy^{-1} \in H \quad \forall H \in \mathcal{F} \\ &\implies xy^{-1} \in K \end{aligned}$$

By Proposition 2.3, $K$ is a subgroup of $G$. $\square$

**subgroup generated by $S$ in $G$**

Let $S$ be a subset of group $G$. The **subgroup generated by $S$ in $G$** is

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

# Index