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:

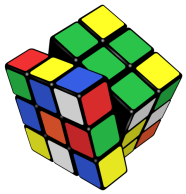
- Participation: 4%
- Quizzes: 32%
- Written homework: 32%
- Final takehome exam: 32%

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 $+$ subtraction $-$ multiplication $\cdot$ division with remainders
Integers $\mathbb{Z}$	negation $x \mapsto -x$
Rational number $\mathbb{Q}$	multiplicative inversion $x \mapsto 1/x$
Real numbers $\mathbb{R}$	kth 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: $a + b, a \times b, a \cdot b, a \circ b, a \oplus b, a \otimes b, a \odot b, a \diamond b, a \diamondsuit b, a \blacklozenge b, a * b, a \bullet b, a \boxplus b, a \boxtimes b, a \uplus b$
- 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

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

□

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 $y \boxtimes a = b$.

□

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.

□

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, ι is a bijection, both injective and surjective.

If $g \in G$, then

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

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 $AB \neq BA$.

□

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

	0	1
0	0	1
1	1	0

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

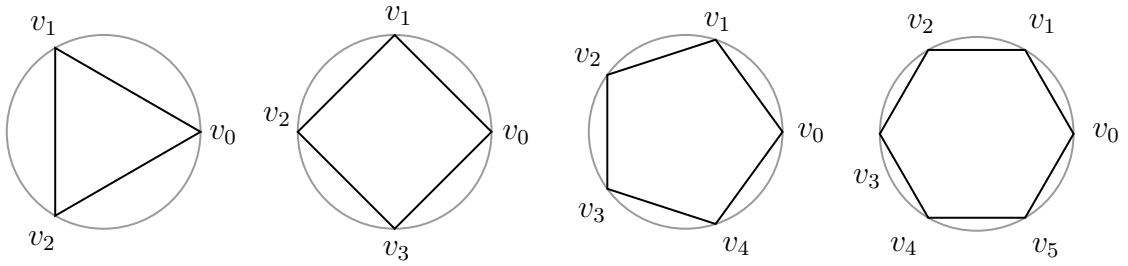
$$\left\{k \geq 1 : g^k = e\right\} = \left\{k \geq 1 : \left(g^{-1}\right)^k = e\right\}$$

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 $v_k = (\cos 2\pi k/n, \sin 2\pi k/n) = e^{2\pi ik/n}$

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. □

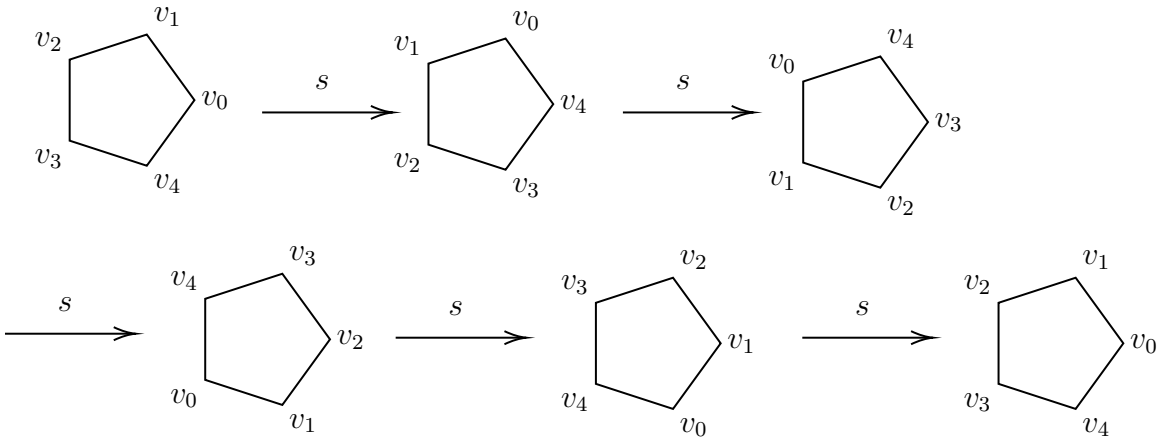
[a] ordered pairs

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

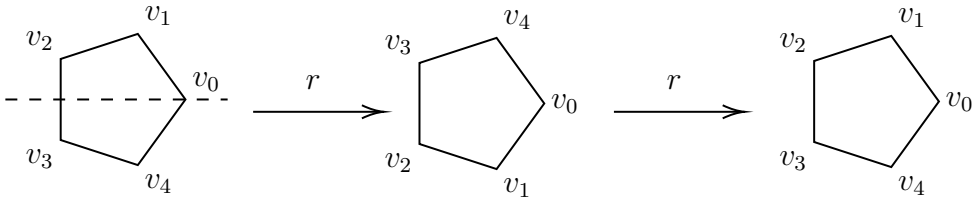
If the answer is yes, then $|D_{2n}| = 2n$.

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:

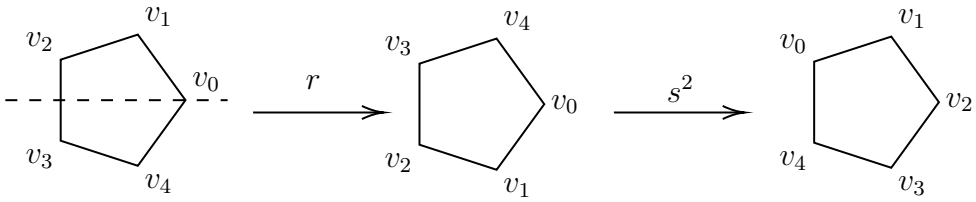


$|r| = 2$, i.e. $r^2 = e, r \neq e$.

$r(v_0) = v_0$. $r(v_1)$ 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 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. □

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 π.

Disjoint cycle representation: write down cycles of π

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

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

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

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

$*$: 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 π^{-1} are cycles of π in opposite order.

fixed points

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

support set

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

$$\text{supp}(\pi) = \{1 \leq i \leq n : \pi(i) \neq i\}$$

disjoint

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

Example:

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

Remark:

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

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

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

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

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 $1 \leq i \leq n$. If $i \in \text{supp}(i)$, then $\pi(i) \in \text{supp}(\pi)$. Since π, σ disjoint, $i, \pi(i) \notin \text{supp}(\sigma)$. So $\pi(\sigma(i)) = \pi(i) = \sigma(\pi(i))$.

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

If $i \notin \text{supp}(\pi) \cup \text{supp}(\sigma)$, 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 π in the disjoint cycle notation. If $c_1, \ldots, c_k$ are cycles of π, 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 π is a permutation, then π commutes with π^i for all i since $\pi^{i+1} = \pi\pi^i = \pi^i\pi$, so π and π^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 $i = nk + r, 0 \leq r < n$. 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 $g^{n-1} = g^{-1} \in H$.

□

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

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

By Proposition 2.3, K is a subgroup of G. □

subgroup generated by S in G

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

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

Note

Intersection is non-empty because $S \subseteq G \leq G$.

If $S \subseteq K \leq G$, then $\langle S \rangle \subseteq K$. So say that $\langle S \rangle$ is smallest subgroup of G containing S.

To simplify the notation: If $S = \{s_1, s_2, \ldots\}$, often write $\langle S \rangle = \langle s_1, s_2, \ldots \rangle$.

We can write the trivial subgroup as $\langle \varnothing \rangle = \langle e \rangle = \{e\}$.

Example: D_{2n}

Let s be the rotation generator of D_{2n}. Let $K = \{s^0 = e, s^1, s^2, \ldots, s^{n-1}\}$.

As previously checked, K is a subgroup of D_{2n}.

Since $s \in K, \langle s \rangle \subseteq K$.

On the other hand, can show by induction that $s^i \subseteq \langle s \rangle$ for all $i \in \mathbb{Z}$.

So $K \subseteq \langle s \rangle \implies \langle s \rangle = K$.

$\langle s \rangle$ is constructed by taking all products of s with itself. Can we generalize this example?

Here we introduce a notation: If $S \subset G$, let $S^{-1} = \{s^{-1} : s \in S\}$.

Proposition 2.5

If $S \subset G$, let

$$K = \{e\} \cup \{s_1 \cdots s_k : k \geq 1, \quad s_1, \ldots, s_k \in S \cup S^{-1}\}$$

Then $\langle S \rangle = K$.

Proof:

Claim 1 $S \subseteq K \subseteq \langle S \rangle$

Proof It is easy to show that $S \subseteq K$. We simply let $k = 1$ and s_1 to be any element of S.

To show the second part, we know $e \in \langle S \rangle$. Then we can prove by induction that $s_1 \cdots s_k \in \langle S \rangle$ for all $k \geq 1$, $s_1, \ldots, s_k \in S \cup S^{-1}$. ■

Claim 2 K is a subgroup of G.

Proof $e \in K$ by construction.

Suppose $x, y \in K$,

$$x = s_1 \cdots s_k, k \geq 0, s_1, \ldots, s_k \in S \cup S^{-1}$$
$$y = t_1 \cdots t_\ell, \ell \geq 0, t_1, \ldots, t_\ell \in S \cup S^{-1}$$

Then $xy = s_1 \cdots s_k t_1 \cdots t_\ell \in K$ by construction. Also, $x^{-1} = s_k^{-1} \cdots s_1^{-1} \in K$ since $s_k^{-1}, \cdots, s_1^{-1} \in S \cup S^{-1}$. So K is a subgroup. ■

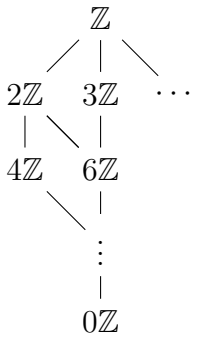
$S \subseteq K$, and $\langle S \rangle$ is smallest subgroup containing $S \implies \langle S \rangle \subseteq K$. Thus $\langle S \rangle = K$. □

2.2.1 Lattice of subgroups

Before concluding this section, it is interesting to mention one closed related subject which the lattice of subgroups of G.

Subgroups of G are ordered by set inclusion $\subseteq$. If $H_1, H_2 \leq G$, and $H_1 \subseteq H_2$, then $H_1 \leq H_2$, so we also write this order as $\leq$. Set of subgroups of G with order $\leq$ is called the **lattice of subgroups of** G. We don't need to deal with formal definitions and properties here.

The picture below shows the subgroups of $\mathbb{Z}$, where $k\mathbb{Z}$ denotes the set containing all integers that are divisible by k.



Subgroup below $H_1, H_2 \leq G$ in the lattice is $H_1 \cap H_2$. In the picture above, it is $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$. Intuitively, a number is divisible by 2 and 3, which is the same thing as being divisible by 6.

What about the subgroup above H_1 and H_2? The subgroup above H_1, H_2 is $\langle H_1 \cup H_2 \rangle$.

2.3 Cyclic groups

generate

A subset S of a group G **generates** G if $\langle S \rangle = G$.

cyclic

A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$.

Example:

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ (generators are not unique)

$\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle = \langle -[1] \rangle$

$\mathbb{Q}^+$ is not cyclic

If G is a group, then $\langle a \rangle$ is a cyclic group for any $a \in G$ (called the **cyclic subgroup generated by** a).

Lemma 2.6

1. If $a \in G$, then $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$.
2. If $|a| = n$, then $\langle a \rangle = \{a^i : 0 \leq i < n\}$.

Proof:

1. Follows from Proposition 2.5 about $\langle S \rangle$.
2. See argument for $\langle s \rangle$ in D_{2n}.

□

Remark:
In the first part of Lemma 2.6, it does not mean each element in the subgroup can be uniquely represented in the form of a^i.

Then we have two questions:

- In (2), can $|\langle a \rangle|$ be smaller than n?
- Does $|\langle a \rangle|$ determine $|a|$?

Proposition 2.7

If $G = \langle a \rangle$, then $|G| = |a|$.

This proposition also applies to infinite groups.

Proof:
From part 2 of Proposition 2.6, we know that there are at most n elements in $\langle a \rangle$, then $|G| \leq |a|$.

Suppose $|G| = n < +\infty$. Then the sequence $a^0, a^1, \ldots, a^n \in G$ must have repetition. Thus there is $0 \leq i < j \leq n$ with $a^i = a^j$. Then with the similar argument before, $a^{j-i} = e$, which implies that $|a| \leq n$.

Thus $|a| \leq |G| \implies |a| = |G|$. □

Remark:
It is worth thinking that what happens if $|G| = \infty$ and it seems the proof only works with finite order. If $|G| = \infty$, then $|G| \leq |a|$ will force $|a|$ to be infinite.

Example: $\mathbb{Z}$
$G = \mathbb{Z}$:

- Infinite cyclic group
- Generators are $+1$ and -1
- Order of $m \in \mathbb{Z}$ is
$$|m| = \begin{cases} +\infty & m \geq 0 \\ 1 & m = 0 \end{cases}$$
- Cyclic subgroups: $\langle m \rangle = m\mathbb{Z} = \{km : k \in \mathbb{Z}\}$. (Note difference in $\langle a \rangle$ in additive and multiplicative notation)

  All subgroups of $\mathbb{Z}$ are cyclic

2.3.1 $\mathbb{Z}/n\mathbb{Z}$

Can we analyze $\mathbb{Z}/n\mathbb{Z}$ in the same way? Recall $\mathbb{Z}/n\mathbb{Z}$ is the set of congruence classes mod n. We denote congruence class of $a \in \mathbb{Z}$ by $[a]$, or just a. For example, in $\mathbb{Z}/5\mathbb{Z}$, $3 = 8$.

Then we might wonder:

- What are the generators?
- What are the orders of elements?
- What are the subgroups?

Before we explore these questions, it is nice to have the following lemma which works for arbitrary group G.

Generators

Lemma 2.8

Suppose $G = \langle S \rangle$. Then $G = \langle T \rangle$ if and only if $S \subseteq \langle T \rangle$.

Proof:
It's relatively easy to prove.

$\Rightarrow$ If $G = \langle T \rangle$, and we know $S \subseteq G$, then $S \subseteq \langle T \rangle$.

$\Leftarrow$ If $S \subseteq \langle T \rangle$, and we know $\langle S \rangle$ is the smallest subgroup containing S, then $\langle T \rangle$ must contain the subgroup generated by S, which is $\langle S \rangle = G$, thus $G \subseteq \langle T \rangle$. And $\langle T \rangle$ is a subgroup as well, then $G = \langle T \rangle$.

□

What does this mean in our example? So $\mathbb{Z}/n = \langle [a] \rangle$ if and only if $[1] \in \langle [a] \rangle$.

$$\begin{aligned} [1] \in \langle [a] \rangle &\iff xa = 1 \mod n \text{ for some } x \in \mathbb{Z} \\ &\iff xa - 1 = yn \text{ for some } x, y \in \mathbb{Z} \\ &\iff xa + yn = 1 \text{ for some } x, y \in \mathbb{Z} \\ &\iff \gcd(a, n) = 1 \end{aligned}$$

So $\langle [a] \rangle = \mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$.

Order of elements

Lemma 2.9

If G is a group, $g \in G$, $g^n = e$, then $|g| \mid n$.

Proof:
Exercise. □

If $a \in \mathbb{Z}$, then $n[a] = 0$, so $|[a]| \mid n$.

Lemma 2.10

Suppose $a|n$. Then $|[a]| = \frac{n}{a}$.

Proof:
If $n = ka$, then $\ell[a] \neq 0$ for $1 \leq \ell < k$ and $k[a] = [ka] = 0$, so $|[a]| = k$. □

Lemma 2.11

Suppose $a \in \mathbb{Z}$, and let $b = \gcd(a, n)$. Then $\langle [a] \rangle = \langle [b] \rangle$.

Proof:
Since $b|a$, there is k such that $a = kb$, then $[a] \in \langle [b] \rangle \implies \langle [a] \rangle \subseteq \langle [b] \rangle$.

By properties of gcd, there is $x, y \in \mathbb{Z}$ such that $xa + yn = b$. So $[b] = x[a] \implies [b] \in \langle [a] \rangle \implies \langle [b] \rangle \subseteq \langle [a] \rangle$.

Therefore $\langle [a] \rangle = \langle [b] \rangle$. □

Using these lemmas, we can find order for a general element in $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.12

Suppose $a \in \mathbb{Z}$. Then

$$|[a]| = \frac{n}{\gcd(a, n)}$$

Proof:
Let $b = \gcd(a, n)$. Then $\langle [a] \rangle = \langle [b] \rangle$. So

$$|[a]| = |\langle [a] \rangle| = |\langle [b] \rangle| = |[b]|$$

Finally

$$|[b]| = \frac{n}{b}$$

□

Subgroups

Corollary 2.13

Let $n \geq 1$.

- The order d of any cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ divides n.
- For every $d|n$, there is a unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d. It is generated by $[a]$, where $a = \frac{n}{d}$.

Proof:
If $|\langle [a] \rangle| = d$, then $d = |[a]| \mid n$ by Lemma 2.9. Also, $d = \frac{n}{\gcd(a,n)}$, and by Lemma 2.11, $\langle [a] \rangle = \left\langle \left[\frac{n}{d}\right] \right\rangle$.

Conversely, if $d|n$ and $a = \frac{n}{d}$, then $|\langle [a] \rangle| = d$. □

Example:
Cyclic subgroups of $\mathbb{Z}/6\mathbb{Z}$ are

- $\langle 6 \rangle = \{0\}$
- $\langle 2 \rangle = \{0, 2, 4\}$
- $\langle 3 \rangle = \{0, 3\}$
- $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}/6\mathbb{Z}$.

Cyclic subgroups of $\mathbb{Z}/p\mathbb{Z}$, p prime

- $\langle p \rangle = \langle 0 \rangle$
- $\langle 1 \rangle = \mathbb{Z}/p\mathbb{Z}$

Every subgroup of a cyclic group is cyclic. So Corollary 2.13 is a complete list of subgroups of $\mathbb{Z}/n\mathbb{Z}$. Every cyclic group is isomorphic to one of $\mathbb{Z}/n\mathbb{Z}, n \geq 1$, or $\mathbb{Z}$.

3

Quotient Groups and Homomorphisms

3.1 Homomorphisms

homomorphism

Let G and H be groups. A function $\phi : G \to H$ is a **homomorphism** (or **morphism**) if

$$\phi(g \cdot h) = \phi(g) \cdot \phi(h)$$

for all $g, h \in G$.

Example:

$\mathbb{K}$ field, $\mathbb{K}^\times = \{a \in \mathbb{K}, a \neq 0\}$ with operation $\cdot$.

$\mathrm{GL}_n \mathbb{K} \to \mathbb{K}^\times : A \mapsto \det(A)$ is a homomorphism because $\det(AB) = \det(A)\det(B)$ for all invertible matrices A, B.

Let $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\} \leq \mathbb{R}^\times$. $\mathbb{R}_{>0} \to \mathbb{R}_{>0} : x \mapsto \sqrt{x}$ is a homomorphism since $\sqrt{xy} = \sqrt{x}\sqrt{y}$.

Additive notation: $\phi : (G, +) \to (H, +)$ is a homomorphism if $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in G$. For example, $\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ is a homomorphism for any $m \in \mathbb{Z}$, since

$$\phi(x + y) = m(x + y) = mx + my = \phi(x) + \phi(y) \quad \forall x, y \in \mathbb{Z}$$

If V, W are vector spaces, and $T : V \to W$ is a linear transformation, then T is a homomorphism from $(V, +)$ to $(W, +)$, since $T(v + w) = T(v) + T(w)$ for all $v, w \in V$.

Mixed notation: $\mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$ is a homomorphism since $e^{x+y} = e^x \cdot e^y$ for all $x, y \in \mathbb{R}^+$.

$\mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto e^x$ is not a homomorphism since $e^{x+y} \neq e^x + e^y$ for some $x, y \in \mathbb{R}^+$ (e.g. $x = y = 0$).

Lemma 3.1

Suppose $\phi : G \to H$ is a homomorphism. Then

(a) $\phi(e_G) = e_H$

(b) $\phi(g^{-1}) = \phi(g)^{-1}$

(c) $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$

(d) $|\phi(g)| \mid |g|$ for all $g \in G$ ($n|\infty$ for all $n \in \mathbb{N}$)

Proof:

(a) $\phi(e_G) = \phi(e_G^2) = \phi(e_G) \cdot \phi(e_G)$
so $e_H = \phi(e_G)^{-1} \cdot \phi(e_G) = \phi(e_G)^{-1} \cdot \phi(e_G) \cdot \phi(e_G) = \phi(e_G)$.

(b) $e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ and similarly $\phi(g^{-1})\phi(g) = e_H$, so $\phi(g^{-1})$ is the unique inverse of $\phi(g)$.

(c) Use induction for $n \geq 0$, use part (b) for $n < 0$.

(d) If $|g| = n < +\infty$, then $g^n = e_G$ so $\phi(g)^n = \phi(g^n) = \phi(e_G) = e_H$. This implies[a] $|\phi(g)| \mid n$.

□

[a] See homework

Lemma 3.2

If $H \leq G$, and H is considered as a group with the induced operation from G, then $i : H \to G : x \mapsto x$ is a homomorphism.

Proof:
$i(g \cdot h) = g \cdot h = i(g) \cdot i(h)$ □

Lemma 3.3

If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then $\psi \circ \phi$ is a homomorphism.

Proof:
$\psi \circ \phi(g \cdot h) = \psi(\phi(g) \cdot \phi(h)) = \psi(\phi(g)) \cdot \psi(\phi(h))$. □

Corollary 3.4

If $\phi : G \to H$ is a homomorphism, $K \leq G$, then the **restriction** $\phi|_K$ is a homomorphism.

Proof:
$\phi_K = \phi \circ i$, where $i : K \to G$ is the inclusion $x \mapsto x$. □

3.2 Homomorphisms and subgroups

If $f : X \to Y$ is a function, $S \subseteq X$, then $f(S) := \{f(x) : x \in S\}$

Proposition 3.5

If $\phi : G \to H$ is a homomorphism, and $K \leq G$, then $\phi(K) \leq H$.

Proof:
Since K is non-empty, $\phi(K)$ is non-empty.

If $x, y \in \phi(K)$, then $x = \phi(x_0), y = \phi(y_0)$ for $x_0, y_0 \in K$.

So $xy^{-1} = \phi(x_0)\phi(y_0)^{-1} = \phi(x_0)\phi(y_0^{-1}) = \phi(x_0 y_0^{-1}) \in \phi(K)$, since $x_0 y_0^{-1} \in K$. □

image

If $\phi : G \to H$ is a homomorphism, the **image** of ϕ is the subgroup $\operatorname{Im}\phi = \phi(G) \leq H$.

Example:
Let $\phi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$. $e^x > 0$ for all $x \in \mathbb{R}$, so $\operatorname{Im}\phi \subseteq \mathbb{R}_{>0}$. If $y \in \mathbb{R}_{>0}$, then $y = \phi(\log y)$, so $\operatorname{Im}\phi = \mathbb{R}_{>0}$.

If $K \leq G$ and $i : K \to G$ is inclusion, then $\operatorname{Im} i = K$.

$\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ for some $m \in \mathbb{Z}$. $\phi(\mathbb{Z}) = m\mathbb{Z}$.

Lemma 3.6

If $\phi : G \to H$ is a homomorphism with $\operatorname{Im}\phi \leq K \leq H$, then the function $\tilde{\phi} : G \to K : x \to \phi(x)$ is also a homomorphism with $\operatorname{Im}\tilde{\phi} = \operatorname{Im}\phi \leq K$.

Proof:

$$\begin{aligned}\tilde{\phi}(x \cdot y) &= \phi(x \cdot y) \\ &= \phi(x) \cdot \phi(y) \text{ in } H \\ &= \tilde{\phi}(x) \cdot \tilde{\phi}(y) \text{ in } K\end{aligned}$$

Also $\tilde{\phi}(G) = \phi(G)$, regarded as a subset of K. □

Usually just refer to $\tilde{\phi}$ as ϕ.

Lemma 3.7

A homomorphism $\phi : G \to H$ is surjective if and only if $\operatorname{Im}\phi = H$.

Proof:
Obvious from definition. □

Corollary 3.8

ϕ induces a surjective homomorphism $\tilde{\phi} : G \to K$, where $K = \operatorname{Im}\phi$.

Remark:
From Lemma 3.7, if ϕ is not surjective, then $\operatorname{Im}\phi < H$, then we can let $K = \operatorname{Im}\phi$, and then construct a surjective homomorphism by Lemma 3.6.

Because this is a bit abstract, it is helpful to go through some examples.

Recall the previous example: Let $\phi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$. $e^x > 0$ for all $x \in \mathbb{R}$. This is not surjective, because $\operatorname{Im}\phi = \mathbb{R}_{>0}$. If we restrict the codomain to be $\mathbb{R}_{>0}$, then it is surjective.

Similarly for $\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ for some $m \in \mathbb{Z}$, but it induced surjective homomorphism $\mathbb{Z} \to m\mathbb{Z}$.

Proposition 3.9

Let $\phi : G \to H$ be a homomorphism. If $S \subseteq G$, then $\phi(\langle S\rangle) = \langle\phi(S)\rangle$.

Proof:
$\phi(S^{-1}) = \{\phi(s^{-1}) : s \in S\} = \{\phi(s)^{-1} : s \in S\} = \phi(S)^{-1}$. So

$$\begin{aligned}\phi(\langle S\rangle) &= \phi\left(\left\{s_1 \cdots s_k : k \geq 0, s_1, \ldots, s_k \in S \cup S^{-1}\right\}\right)\\ &= \left\{\phi(s_1)\cdots\phi(s_k) : k \geq 0, s_1, \ldots, s_k \in S \cup S^{-1}\right\}\\ &= \left\{t_1 \cdots t_k : k \geq 0, t_1, \ldots, t_k \in \phi(S) \cup \phi(S)^{-1}\right\}\\ &= \langle\phi(S)\rangle\end{aligned}$$

□

Remark:
We used the fact that $\phi(S \cup S^{-1}) = \phi(S) \cup \phi(S^{-1})$, but it doesn't work for intersection.

If $f : X \to Y$ is a function, and $S \subseteq Y$, then $f^{-1}(S) := \{x \in X : f(x) \in S\}$.

Proposition 3.10

If $\phi : G \to H$ is a homomorphism, $K \leq H$, then $\phi^{-1}(K) \leq G$.

Proof:
$\phi(e_G) = e_H \in K$, so $e_G \in \phi^{-1}(K)$.

If $x, y \in \phi^{-1}(K)$, then $\phi(x), \phi(y) \in K$. Thus $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in K$. Hence $xy^{-1} \in \phi^{-1}(K)$. Thus it is a subgroup of G. □

kernel

If $\phi : G \to H$ is a homomorphism, then the **kernel** of ϕ is the subgroup $\ker \phi := \phi^{-1}(e_H) = \{g \in G : \phi(g) = e_H\} \leq G$.

Example:

For $\det : \mathrm{GL}_n \mathbb{K} \to \mathbb{K}^\times$, $\ker \det = \{A \in \mathrm{GL}_n : \det(A) = 1\}$.
This subgroup of $\mathrm{GL}_n \mathbb{K}$ is called the **special linear group**, and is denoted by $\mathrm{SL}_n \mathbb{K}$.

If $\phi : \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$, then $\phi(k) = 0$ if and only if $mk = 0$, so

$$\ker \phi = \begin{cases} \{0\} & m \neq 0 \\ \mathbb{Z} & m = 0 \end{cases}$$

If $\phi : \mathbb{R} \to \mathbb{R}^\times : x \mapsto e^x$, then $e^x = 1$ if and only if $x = 0$, so $\ker \phi = \{0\}$.

We can generalize the last example into the following proposition.

Proposition 3.11

A homomorphism $\phi : G \to H$ is injective if and only if $\ker \phi = \{e_G\}$.

Proof:

$\Rightarrow$ If ϕ is injective, then $\phi(x) = \phi(e_H) = \phi(e_G)$ if and only if $x = e_G$, so $\ker \phi = \{e_G\}$.

$\Leftarrow$ Suppose $\ker \phi = \{e_G\}$, and $\phi(x) = \phi(y)$. Then $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e_H$, so $xy^{-1} \in \ker \phi$.

But then $xy^{-1} = e_G$, so $x = y$ which implies that ϕ is injective.

□

3.2.1 Application: subgroups of cyclic groups

Proposition 3.12

If H is a subgroup of a cyclic group G, then H is cyclic.

Proof:

We need following facts:

1. All subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z} = \langle m \rangle$, hence cyclic.
2. G is cyclic if and only if there is surjective homomorphism $\mathbb{Z} \to G$.
3. If $f : X \to Y$ is a surjective function, and $S \subseteq Y$, then $f(f^{-1}(S)) = S$.

The first two are in the homework. The last one is not hard to see.

Since G is cyclic, there is a surjective homomorphism $\phi : \mathbb{Z} \to G$.

Since all subgroups of $\mathbb{Z}$ are cyclic, there is $m \in \mathbb{Z}$ such that $\phi^{-1}(H) = \langle m \rangle$.

Let $\psi : \mathbb{Z} \to \mathbb{Z}$ be homomorphism with $\psi(k) = mk$.

Then $\phi \circ \psi : \mathbb{Z} \to G$ is homomorphism.

$\phi \circ \psi(\mathbb{Z}) = \phi(m\mathbb{Z}) = \phi(\phi^{-1}(H)) = H$.

Then we can restrict codomain of $\phi \circ \psi$ to get surjective homomorphism $\mathbb{Z} \to H$.

Hence H is cyclic. □

3.3 Isomorphisms

in/sur/bi-jective

Let $f : X \to Y$ be a function. Then f is:

1. **injective** if for all $x, y \in X$, $f(x) = f(y) \implies x = y$,
2. **surjective** if for all $y \in Y$, $\exists x \in X$ with $f(x) = y$, and
3. **bijective** if f is both injective and surjective.

Proposition 3.13

$f : X \to Y$ is a bijection if and only if there is a function $g : Y \to X$ such that $f \circ g = 1_Y$ and $g \circ f = 1_X$.

If g exists, then it is unique, and we denote it by f^{-1}.

isomorphism

A homomorphism $\phi : G \to H$ is an **isomorphism** if ϕ is a bijection.

Lemma 3.14

$\phi : G \to H$ is an isomorphism if and only if $\ker \phi = \{e_G\}$ and $\operatorname{Im} \phi = H$.

Example:

$\mathbb{R}^+ \to \mathbb{R}_{>0} : x \mapsto e^x$ is an isomorphism.

If $\phi : G \to H$ is injective, then ϕ induces an isomorphism $G \to \operatorname{Im} \phi$.

Proposition 3.15

Suppose $\phi : G \to H$ is an isomorphism. Then $\phi^{-1} : H \to G$ is also an isomorphism.

Proof:
ϕ^{-1} is also a bijection, so just need to show that it is a homomorphism.

If $g, h \in H$, then

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

So ϕ^{-1} is a homomorphism, hence isomorphism. □

Corollary 3.16

A homomorphism $\phi : G \to H$ is an isomorphism if and only if there is a homomorphism $\psi : H \to G$ such that

- $\psi \circ \phi = 1_G$, and
- $\phi \circ \psi = 1_H$.

Proof:
$\Rightarrow$ If ϕ is an isomorphism, then can take $\psi = \phi^{-1}$.

$\Leftarrow$ If ψ exists, then ϕ is a bijection.

□

isomorphic

We say that G and H are **isomorphic** if there is an isomorphism $\phi : G \to H$.

Notation: $G \cong H$.

Key facts:

- If $G \cong H$ then $H \cong G$.

  Proof:
  If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is an isomorphism. □

- If $G \cong H$ and $H \cong K$ then $G \cong K$.

  Proof:
  If $\phi : G \to H$ is an isomorphism and $\psi : H \to K$ is an isomorphism, then $\psi \circ \phi$ is an isomorphism. □

- $G \cong G$.

  Proof:
  $1_G : G \to G$ is an isomorphism. □

Idea If $G \cong H$, then G and H are identical as groups.

If $\phi : G \to H$ is an isomorphism, then

- $|G| = |H|$

- G is abelian if and only if H is abelian
- $|g| = |\phi(g)|$ for all $g \in G$
- $K \subseteq G$ is a subgroup of G if and only if $\phi(K)$ is a subgroup of H

Proposition 3.17

If G and H are cyclic groups, then $G \cong H$ if and only if $|G| = |H|$.

Proof:
Suppose $|G| = \langle a \rangle$, $H = \langle b \rangle$.

$\Leftarrow$ Assume that $|G| = |H|$.

Claim $a^i = a^j$ for $i < j$ if and only if $|a| \mid j - i$.

Proof

$\Leftarrow$ If $a^i = a^j$ then $a^{j-i} = e$.

$\Rightarrow$ If $|a| \mid j - i$, then $j - i = k|a|$. So $a^{j-i} = a^{k|a|} = e \implies a^j = a^i$. ■

Note: if $|a| = +\infty$, $a^i \neq a^j$ for all $i \neq j \in \mathbb{Z}$.

Then we define a function $\phi : G \to H : a^i \mapsto b^i$.

Well-defined? $|a| = |G| = |H| = |b|$.
$a^i = a^h \implies |a| \mid j - i \implies |b| \mid j - i \implies b^i = b^j$

Homomorphism? $\phi(a^i \cdot a^j) = \phi(a^{i+j}) = b^{i+j} = b^i \cdot b^j = \phi(a^i) \cdot \phi(a^j)$ for all $a^i, a^j \in G$.

Inverse? $\psi : H \to G : b^i \mapsto a^i$ is well-defined. Clearly ψ is inverse to ϕ.

Thus ϕ is isomorphism $\implies G \cong H$.

$\Rightarrow$ If $G \cong H$, then $|G| = |H|$ which holds for all groups. Same cardinality thus same order.

□

Corollary 3.18

Suppose G is a cyclic group.

- If $|G| = +\infty$, then $G \cong \mathbb{Z}$.
- If $|G| = n < +\infty$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.

Corollary 3.19

Cyclic groups are abelian.

multiplicative form of cyclic groups

Let a be formal indeterminate (can use any letter). Let

- $C_\infty = \{a^i : i \in \mathbb{Z}\}$, $a^i \cdot a^j = a^{i+j}$
- $C_n = \{a^i : i \in \mathbb{Z}/n\mathbb{Z}\}$, $a^i \cdot a^j = a^{i+j}$

Of course we have $C_\infty \cong \mathbb{Z}$ via $a^i \mapsto i$, and $C_n \cong \mathbb{Z}/n\mathbb{Z}$ via $a^i \mapsto i$.

3.4 Cosets

week 3

Recall linear subspaces are motivation for definition of subgroups. Let $T : V \to W$ be a linear transformation. (so T is also a group homomorphism $(V, +) \to (W, +)$). $\ker T = \{x \in V : T(x) = 0\}$ = "solutions to $Tx = 0$".

What are solutions to $Tx = b$?

They can be empty: $Tx = b$ has a solution if and only if $b \in \operatorname{Im} T$. If $b \in \operatorname{Im} T$, and $Tx = b$ has a solution x_0, then all other solutions are of the form $x_0 + x_1$, for $x_1 \in \ker T$.

Conclusion: space of solutions has form $x_i + \ker T$. $x_0 + \ker T$ is called an **affine** subspace. (it's like a linear subspace, but doesn't have to contain 0). We can still talk about the dimension.

coset

If $S \subseteq G$, and $g \in G$, we let

$$gS = \{gh : h \in S\} \quad \text{and} \quad Sg = \{hg : h \in S\}$$

If $H \leq G$, gH is called a **left coset** of H in G and Hg is called a **right coset** of H in G.

Remark:
We also refer these sets: left/right translate of S by g.

For abelian groups, $gH = Hg$.

Additive notation: coset of H in $(G, +)$ is $g + H$.

Example:
U subspace of vector space $(V, +, \cdot)$, cosets of U are affine subspaces $v + U$ for $v \in V$.

Given $m \in \mathbb{Z}$, cosets of $m\mathbb{Z}$ are sets

$$a + m\mathbb{Z} = \{a + km : k \in \mathbb{Z}\} = \{x \in \mathbb{Z} : x \equiv a \mod m\}$$

We can think of the cosets as the sets of solutions to system of equations.

Example: Dihedral group $\langle s \rangle$

Recall $D_{2n} = \{s^i r^j : 0 \leq i < n, j \in \{0, 1\}\}$.

Let $H = \langle s \rangle = \{e = s^0, s^1, \ldots, s^{n-1}\}$

What are the right cosets of H?

$$\begin{aligned} H &= He \\ Hr &= \{r, sr, \ldots, s^{n-1}r\} \\ Hs^i &= \{s^i, s^{i+1}, \ldots, s^{n-1}, e, s^1, \ldots, s^{i-1}\} = H \\ Hs^ir &= \{s^ir, s^{i+1}r, \ldots, s^{n-1}r, r, sr, \ldots, s^{i-1}r\} = Hr \end{aligned}$$

Conclusion: right cosets are H and Hr.

Also $D_{2n} = H \sqcup Hr$, where $\sqcup$ is disjoint union.

What about the left cosets of $H = \langle s \rangle$?

Exercise

- use $rs = s^{-1}r$ to show $s^i = rs^{-i}$ for all $i \in \mathbb{Z}$.
- if $S \subseteq G$, $g, h \in G$, then $ghS = g(hS)$. This follows from the associativity of the group.

With these facts,

$$\begin{aligned} s^iH &= H \\ s^irH &= rs^{-i}H = rH \end{aligned}$$

Conclusion: left cosets of H are H, rH

$$\begin{aligned} rH &= \{r, rs, rs^2, \ldots, rs^{n-1}\} \\ &= \{r, s^{-1}r, s^{-2}r, \ldots, s^{1-n}r\} \\ &= \{r, s^{-1}r, s^{-2}r, \ldots, sr\} \\ &= \{r, s^{n-1}r, s^{n-2}r, \ldots, sr\} \\ &= Hr \end{aligned}$$

Example: Dihedral group $\langle r \rangle$

What about $H = \langle r \rangle = \{e, r\}$?

Left cosets: $rH = \{r, e\} = H$ and $s^iH = \{s^i, s^ir\} = s^irH$.

Conclusion: Left cosets are $s^iH, 0 \leq i < n$, and

$$D_{2n} = \bigsqcup_{i=0}^{n-1} s^iH$$

Right cosets: $Hr = \{r, e\} = H$ and $Hs^i = \{s^i, rs^i\} = \{s^i, s^{-i}r\}$
$Hs^ir = \{s^ir, s^{-i}\} = Hs^{-i}$

Conclusion: Right cosets are $Hs^i, 0 \leq i < n$, and $D_{2n} = \bigsqcup_{i=0}^{n-1} Hs^i$.

In this case, left cosets and right cosets are different.

set of left/right cosets

If $H \leq G$, let

$$G/H = \{gH : g \in G\} = \{S \subseteq G : S = gH \text{ for some } g \in G\}$$

be the **set of left cosets** of H in G, and

$$H \setminus G = \{Hg : g \in G\} = \{S \subseteq G : S = Hg \text{ for some } g \in G\}$$

be the **set of right cosets** of H in G.

Remark:
It is read as $G \mod H$. We count each subset once.

We are very interested in trying to understand G/H and $H \setminus G$.

Example: D_{2n}
$D_{2n}/\langle s\rangle = \{\langle s\rangle, r\langle s\rangle\}$

$D_{2n}/\langle r\rangle = \{s^i\langle r\rangle, 0 \leq i < n\}$

Example: $\mathbb{Z}/n\mathbb{Z}$
Consider $n\mathbb{Z} \leq \mathbb{Z}$.

$a + n\mathbb{Z} = \{x \in \mathbb{Z} : x \equiv a \mod n\} =: [a]$. Thus

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &= \{a + n\mathbb{Z} : a\mathbb{Z}\} \\ &= \{a + n\mathbb{Z} : 0 \leq a < n\} \\ &= \{[a] : 0 \leq a < n\}\end{aligned}$$

Big question for next week: for $H \leq G$, is G/H always a group? spoiler: no...

Suppose $\phi : G \to K$ is a homomorphism, let $H = \ker\phi$. Note that $\phi(x) = b$ has a solution x for $b \in K$ if and only if $b \in \operatorname{Im}\phi$.

Lemma 3.20

Suppose $\phi(x_0) = b$. The set of solutions $\phi^{-1}(\{b\})$ to $\phi(x) = b$ is $x_0H = Hx_0$.

Proof:
Suppose $\phi(x_1) = b$. Then $\phi(x_0^{-1}x_1) = \phi(x_0)^{-1}\phi(x_1) = b^{-1}b = e$. Thus $x_0^{-1}x_1 \in H$. Therefore $x_1 = x_0(x_0^{-1}x_1) \in H$.

Conversely, if $x_1 = x_0h$ for $h \in H$, then $\phi(x_1) = \phi(x_0h) = \phi(x_0)\phi(h) = be = b$. Therefore, every element of x_0H is a solution.

Same argument for right cosets shows set of solutions is Hx_0. □

In this case, left cosets are right cosets.

Lemma 3.21

Suppose $\phi(x_0) = b$. Then set of solutions to $\phi(x) = b$ is $x_0 \cdot \ker \phi$.

Proposition 3.22

If $\phi : G \to K$ is a homomorphism, then there is a bijection between $G/\ker\phi$ and $\operatorname{Im}\phi$.

Proof:
$g \cdot \ker\phi \in G/\ker\phi$ is the set of solutions to $\phi(x) = b$ where $b = \phi(g)$. As a result, $\phi(g \cdot \ker\phi) = \{b\}$, $b \in \operatorname{Im}\phi$.

In the other direction, given $b \in \operatorname{Im}\phi$, $g\ker\phi = \phi^{-1}(\{b\})$.

From Lemma 3.21, we see these two mappings are inverses of each other, thus bijection. □

Example:
Suppose $G = \mathbb{Z}$, $K = \mathbb{Z}/n\mathbb{Z}$.

From tutorial: there is a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : a \mapsto [a]$.

$\ker\phi = \mathbb{Z}$, $\operatorname{Im}\phi = \mathbb{Z}/n\mathbb{Z}$.

Elements of $\mathbb{Z}/n\mathbb{Z} = \{[a] : 0 \le a < n\} = \{a + n\mathbb{Z} : 0 \le a < n\}$

$a + n\mathbb{Z}$ is the set of solutions of $[x] \equiv [a]$ in $\mathbb{Z}/n\mathbb{Z}$.

3.5 The index and Lagrange's theorem

Given $H \le G$, how many left cosets does H have in G?

index

The **index** of H in G is

$$[G : H] := \begin{cases} |G/H| & G/H \text{ is finite} \\ +\infty & G/H \text{ is infinite} \end{cases}$$

Theorem 3.23: Lagrange's theorem

If $H \leq G$, then

$$|G| = [G : H] \cdot |H|$$

Remark:
Why are we use left cosets here for index? Why not right cosets? Anything holds for left cosets should also be expected hold for right cosets with the order of product reversed. Lagrange's theorem didn't mention the order of product. Thus we should expect it holds for right cosets as well. Thus when G is finite, Lagrange's theorem should imply the number of left cosets is equal to the number of right cosets.

Proposition 3.24

The function $\phi : G/H \to H \setminus G : S \mapsto S^{-1}$ is a bijection.

Proof:
First we check ϕ is will defined: if we are given left coset S, then S^{-1} is a right coset.

Suppose $S \in G/H$, so $S = gH$ for some $g \in G$. Then

$$\begin{aligned} S^{-1} &= \{(gh)^{-1} : h \in H\} \\ &= \{h^{-1}g^{-1} : h \in H\} \\ &\overset{*}{=} \{hg^{-1} : h \in H\} \\ &= Hg^{-1} \end{aligned}$$

$*$: because $H \to H : h \mapsto h^{-1}$ is a bijection.

So ϕ is well-defined, and same argument shows $\psi : H \setminus G \to G/H : S \mapsto S^{-1}$ is well-defined.

Finally, ψ is an inverse to ϕ. □

Thus can use either left or right cosets to define index:

Corollary 3.25

If $H \leq G$ then

$$[G : H] = \begin{cases} |H \setminus G| & H \setminus G \text{ is finite} \\ +\infty & H \setminus G \text{ is infinite} \end{cases}$$

Theorem 3.26: Lagrange's theorem (detailed)

If $H \leq G$, then $|G| = [G : H] \cdot |H|$. (In particular, $|H|$ divides $|G|$.) Furthermore, if G is finite, then $[G : H] = \dfrac{|G|}{|H|}$.

Remark:
We don't want to use the second formula if $|G|$ and $|H|$ both are infinite. See proof in the next section.

Example:
$G = D_{2n}$, $H = \langle s \rangle$, $|D_{2n}| = 2n$, $|H| = n$, so $[G : H] = 2$.

$G = D_{2n}$, $H = \langle r \rangle$, $|D_{2n}| = 2n$, $|H| = 2$, so $[G : H] = n$.

$G = \mathbb{Z}$, $H = m\mathbb{Z}$. $|G| = |H| = +\infty$, $[G : H] = |\mathbb{Z}/m\mathbb{Z}| = m$. So $|G| = [G : H] \cdot |H|$, but we don't get any info about $[G : H]$ from Lagrange's theorem. However, it still gives us some info in many cases.

Corollary 3.27

If $x \in G$, then $|x|$ divides $|G|$.

Proof:
$|x| = |\langle x \rangle|$ and $|\langle x \rangle|$ divides $|G|$. □

Proposition 3.28

If $|G|$ is prime, then G is cyclic.

Proof:
Here we don't treat $+\infty$ as a prime number, and 1 is not a prime number.

Let $x \in G$, $x \neq e$. Then $|x| \neq 1$, and $|x| \mid |G|$, so $|x| = |G|$. Since $|\langle x \rangle| = |x| = |G|$, $G = \langle x \rangle$. □

Order	Known groups
1	Trivial group
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, ??
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, $D_6 = S_3$, ??
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, D_8, ??
9	$\mathbb{Z}/9\mathbb{Z}$, ??

Table 3.1: Groups of small order

?? = could be more groups.

Corollary 3.29

If $\phi : G \to K$ is a homomorphism, then $|\operatorname{Im} \phi| = [G : \ker \phi]$, and hence divides $|G|$.

Proof:
There is a bijection $G/\ker\phi \to \operatorname{Im}\phi$, so $|\operatorname{Im}\phi| = [G : \ker\phi]$. Then Lagrange's theorem implies $[G : H]$ divides $|G|$ for any $H \leq G$. □

Note
Lagrange's theorem also implies that $|\operatorname{Im}\phi|$ divides $|K|$.

Exercise
If G, K are groups, then $\phi : G \to K : g \mapsto e_K$ is a homomorphism (called the **trivial homomorphism**).

$\phi : G \to K$ is the trivial homomorphism if and only if $\operatorname{Im}\phi = \{e\}$, the trivial subgroup.

Corollary 3.30

If G and K have coprime order, then the only homomorphism $\phi : G \to K$ is the trivial homomorphism.

3.6 Proof of Lagrange's theorem

How to prove this theorem?

Recall

$$\begin{aligned} D_{2n} &= \{s^i r^j : 0 \leq i < n, j \in \{0,1\}\} \\ &= \langle s\rangle \sqcup r\langle s\rangle \quad (|s| = n) \\ &= \bigsqcup_{i=0}^{n-1} s^i \langle r\rangle \quad (|r| = 2) \end{aligned}$$

In example, cosets of H are disjoint, we can divide G into $[G : H]$ sets of size $|H|$. Does this work in general? Need to better understand cosets.

Proposition 3.31

Let $H \leq G$, and suppose $g, k \in G$. Then the following are equivalent:

(a) $g^{-1}k \in H$

(b) $k \in gH$

(c) $gH = kH$

(d) $gH \cap kH \neq \varnothing$

Example:
$hH = H$ if and only if $h \in H$. (This is from (c) and (a))

Proof:
(a) ⇒ (b) If $g^{-1}k = h \in H$, then $k = gh \in gH$.

(b) ⇒ (c) Suppose $k = gh$ for $h \in H$. If $h' \in H$, then $kh' = g(hh') \in gH$, since

$hh' \in H$. So $kU \subseteq gH$.

For the reverse inclusion, notice that $g = kh^{-1} \in kH$. If $h' \in H$, then $gh' = k(h^{-1}h') \in kH$, so $gH \subseteq kH$.

(c) $\Rightarrow$ (d) Since $e \in H$, then $g \in gH$, so $gH \neq \varnothing$. If $gH = kH$, then $gH \cap kH = gH \neq \varnothing$.

(d) $\Rightarrow$ (a) Suppose $x \in gH \cap kH$. Then $x = gh_1 = kh_2$ for $h_1, h_2 \in H$. Multiply on the left by g^{-1}, right by h_2^{-1}. So $g^{-1}k = h_1h_2^{-1} \in H$.

□

partition

Let X be a set. A **partition** of X is a subset $\mathcal{Q}$ of 2^X such that

(a) $\bigcup_{S\in\mathcal{Q}} S = X$, and

(b) $S \cap T = \varnothing$ for all $S \neq T \in \mathcal{Q}$.

Here 2^X denotes set of subsets of X.

Exercise

If $\mathcal{Q} \subseteq 2^X$, then the following are equivalent:

- $\mathcal{Q}$ is a partition
- $X = \bigsqcup_{S\in\mathcal{Q}} S$
- Every element of X is contained in exactly one element of $\mathcal{Q}$.

Corollary 3.32

If $H \leq G$, then G/H is a partition of G.

Proof:

Let $g \in G$, then $g \in gH$, so every element of G belongs to some element of G/H. Consequently, $\bigcup_{S\in G/H} S = G$.

Suppose $S \neq T \in G/H$ (so $S = gH$, $T = kH$ for some $g, k \in G$). If $S \cap T \neq \varnothing$, then $S = T$ by parts (c) and (d) of Proposition 3.31. So $S \cap T = \varnothing$. □

Lemma 3.33

If $S \subseteq G$, $g \in G$, then $S \to gS : h \mapsto gh$ is a bijection.

Proof:

Inverse is $gS \to S : h \mapsto g^{-1}h$. □

Consequence: If H is finite, and $g \in G$, then $|gH| = |H|$.

Now we can prove the Lagrange's theorem.

Proof:
If $|H| = +\infty$ then $|G| = +\infty$. Since cosets are disjoint, if $[G : H] = +\infty$ then $|G| = +\infty$.

Suppose $|H|, [G : H]$ are finite.

By Lemma 3.33, $|gH| = |H|$ for all $g \in G$.

Since G/H is a partition of G, G is a disjoint union of $[G : H]$ subsets, all of size $|H|$.

Conclude that $|G| = [G : H] \cdot |H|$. □

3.6.1 Equivalence relations

relation $\sim$

Let X be a set. A **relation** $\sim$ on X is a subset of $X \times X$.

Notation: $a \sim b$ if $(a, b) \in \sim$.

Example:
$=$ on X. $\leq, <, >, \geq$ on $\mathbb{N}$ (or any ordered set). $\subseteq$ on 2^X.

equivalence relation

A relation $\sim$ on X is an **equivalence relation** if

- $x \sim x$ for all $x \in X$ (reflexivity)
- $x \sim y \implies y \sim x$ for all $x, y \in X$ (symmetry), and
- $x \sim y$ and $y \sim x$ for all $x, y, z \in X$ (transitivity).

Example:
$=$ on X. $\equiv_m$, congruence mod m, is an equivalence relation on $\mathbb{Z}$.

$\leq, <$ on $\mathbb{N}, \mathbb{R}$, etc. are not equivalence relations.

Isomorphism $\cong$ is an equivalence relation on the *proper class* of groups. Note that there is no set of all sets, or set of all groups.

equivalence class

If $\sim$ is an equivalence relation on X, the **equivalence class** of $x \in X$ is $[x] = [x]_\sim := \{y \in X : x \sim y\}$.

Proposition 3.34

Let $\sim$ be an equivalence relation on X. If $x, y \in X$ then the following are equivalent:

(a) $x \sim y$

(b) $y \in [x]$

(c) $[x] = [y]$

(d) $[x] \cap [y] \neq \varnothing$

Proof:

(a) $\Rightarrow$ (b) Follows immediately from definition of equivalent classes.

(b) $\Rightarrow$ (c) Assume $y \in [x]$. If $z \in [y]$, then $x \sim y \sim z$, and by transitivity, $z \in [x]$. Thus $[y] \subseteq [x]$. Also $x \sim y \implies y \sim x$, which implies $[x] \subseteq [y]$.

(c) $\Rightarrow$ (d) Assume $[x] = [y]$, $[x] \cap [y] = [x] \supset \{x\} \neq \varnothing$.

(d) $\Rightarrow$ (a) If $x \in [x] \cap [y]$, then $x \sim z \sim y \implies x \sim y$.

□

Corollary 3.35

If $\sim$ is an equivalence relation on X, then $\{[x]_\sim : x \in X\}$ is a partition of X.

Proof:

Since $x \sim x$, $x \in [x]$. Therefore, every element x belongs to some equivalent class. If two equivalent class intersect, they must be equal. Thus X is a disjoint union of its equivalent classes. □

Thus equivalence relation $\implies$ partition. It turns out we can go the opposite direction:

Lemma 3.36

If $\mathcal{Q}$ is a partition of X, then there is an equivalence relation $\sim$ on X such that $\{[x]_\sim : x \in X\} = \mathcal{Q}$.

Proof:

Every element $x \in X$ is contained in a unique set $S_x \in \mathcal{Q}$. Define $\sim$ by saying $x \sim y$ if and only if $S_x = S_y$. This defines an equivalence relation. □

Proposition 3.37

If $H \leq G$, define a relation $\sim_H$ on G by $g \sim_H k$ if $g^{-1}k \in H$. Then $\sim_H$ is an equivalence relation, and the equivalence class of $g \in G$ is $[g] = gH$.

Remark:
From the proposition, we would say $h \sim e$ if and only if $h \in H$.

Proposition 3.37 follows from that cosets partition G. Proposition 3.31 is a special case of Proposition 3.34. Thus we can prove that $\sim_H$ is equivalence class directly, and use Proposition 3.37 to prove Proposition 3.31.

3.7 Normal subgroups

Recall Proposition 3.31, by symmetry:

Proposition 3.38

Let $H \leq G$, and suppose $g, k \in G$. Then the following are equivalent:

(a) $kg^{-1} \in H$

(b) $k \in Hg$

(c) $Hg = Hk$

(d) $Hg \cap Hk \neq \varnothing$

Caution: $g^{-1}k \in H$ does not necessarily imply $kg^{-1} \in H$.

Lemma 3.39

If $H \leq G$ and $Hg = hH$ for $g, h \in G$, then $gH = Hg$.

Proof:
$g \in Hg = hH$, so $gH = hH$. □

normal subgroup

A subgroup $N \leq G$ is a **normal subgroup** if $gN = Ng$ for all $g \in G$.

Notation: $N \trianglelefteq G$.

conjugate of h by g

If $g, h \in G$, the **conjugate of h by g** is ghg^{-1}.

Conjugates come up in linear algebra in change of basis and diagonalization.

Recall: $gS = \{gh : h \in S\}$, $Sg = \{hg : h \in S\}$. So $gSg^{-1} = \{ghg^{-1} : h \in S\}$.

As previously mentioned, $g(hS) = (gh)S$, $(Sg)h = S(gh)$, $g(Sh) = (gS)h$, $eS = S = Se$.

So $gN = Ng$ if and only if $gNg^{-1} = N$. Here we

Also: $S \subseteq T$ if and only if $gS \subseteq gT$ if and only if $Sg \subseteq Tg$.

Proposition 3.40

Let $N \leq G$. Then the following are equivalent:

(1) $N \trianglelefteq G$ $(gN = Ng \ \forall g \in G)$

(2) $gNg^{-1} = N$ for all $g \in G$

(3) $gNg^{-1} \subseteq N$ for all $g \in G$

(4) $G/N = N \setminus G$

(5) $G/N \subseteq N \setminus G$

(6) $N \setminus G \subseteq G/N$

Proof:

We've already done (1) $\iff$ (2). Clearly (2) $\implies$ (3).

To see (3) $\implies$ (2), suppose $gNg^{-1} \subseteq N$ for all $g \in G$. Given $g \in G$, we know $g^{-1}Ng \subseteq N$ by apply assumption to g^{-1}. Thus $N \subseteq gNg^{-1}$. Hence $N = gNg^{-1}$, so (2) holds.

By definition, (1) $\implies$ (4) $\implies$ (5), (6).

(5) $\implies$ (1): Suppose $G/N \subseteq N \setminus G$. If $g \in G$, then $gN = Nh$ for some $h \in G$. By Lemma 3.39, $gN = Ng$.

(6) $\implies$ (1): Similar. $\square$

Index

N

O

P

R

S

T