PMATH 347: Groups and Rings

University of Waterloo
William Slofstra
Spring 2021

Marco Yang

Last updated: May 20, 2021

Contents

Week 1: Groups

1: Binary operations and definition of a group

Binary operations

Definition — binary operation

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

Notation:

- We can use any letter (b, m) or symbol ($+$, $\cdot$).
- We can use function notation (typically for symbols)

$$b\colon X \times X \to X : (x, y) \mapsto b(x, y)$$

  or inline notation (typically for letters)

$$+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (x, y) \mapsto x + y.$$

- Some symbols: $a + b$, $a \times b$, $a \cdot b$, $a \circ b$, $a \oplus b$, $a \otimes b$, $a \odot b$, $a \diamond b$, $a * b$, $a \bullet b$, $a \boxplus b$, $a \boxtimes b$.
- If not ambiguous, can drop the symbol:

$$X \times X \to X : (a, b) \mapsto ab.$$

Example

- Addition $+$ is a binary operation on $\mathbb{N}$, but subtraction $-$ is not since $a - b$ is not necessarily in $\mathbb{N}$.
- Subtraction is a binary operation on $\mathbb{Z}$, *i.e.*, it defines a function $-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
- If $(V, +, \cdot)$ is a vector space over a field $\mathbb{K}$, then $+$ is a binary operation on V, but $\cdot$ is not since $\cdot$ is a function $\mathbb{K} \times V \to V$.

Definition — k-ary operation

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

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

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

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

Associative operations

Definition — associative

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

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

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

Many operations 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 (homework).

Subtraction and division are not associative:

$$10 - (5 - 1) = 6 \neq 4 = (10 - 5) - 1.$$

Subtraction is adding negative numbers; similarly for division. So we aren't as interested in subtraction and division, thus we can focus on associative operations.

A **bracketing** of a sequence $a_1, \ldots, a_n \in X$ is a way of inserting brackets into $a_1 \boxtimes \cdots \boxtimes a_n$ so that the expression can be evaluated (with binary steps).

Example

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

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

Meaning if $\boxtimes$ is associative, then the notation $a_1 \boxtimes \cdots \boxtimes a_n$ is unambiguous.

Proof.

($\Longleftarrow$) 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. So $\boxtimes$ is associative by definition.

($\Longrightarrow$) By induction. Base cases are $n = 1, 2, 3$. For $n = 1, 2$, there is only one bracketing. For $n = 3$, follows from the definition of associativity.

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

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

$$\begin{aligned} w_1 &= (\cdots((a_1 \boxtimes a_2) \boxtimes a_3) \cdots \boxtimes a_k) \\ w_2 &= (a_{k+1} \boxtimes \cdots (a_{n-2} \boxtimes (a_{n-1} \boxtimes a_n)) \cdots) \end{aligned}$$

So by repeatedly applying associativity,

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

□

Commutative (abelian) operations

Definition — commutative (abelian)

A binary operation $\boxtimes\colon X \times X \to X$ is **commutative** or **abelian** if $a \boxtimes b = b \boxtimes a$ for all $a, b \in X$.

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 operations are **not** commutative:

- Subtraction and division: $3 - 1 \neq 1 - 3$
- Function composition
- Matrix multiplication

Note:

1. Subtraction and division are not commutative or associative
2. Function composition and matrix multiplication are not commutative, but are associative

We won't study operations like (1), but we are interested in those like (2).

The first half of this course is group theory: single associative operation, not necessarily commutative.

The second half of this course is ring theory: two associative operations, focus on the both commutative case.

Identities

Definition — identity

Let $\boxtimes$ be a binary operation on a set X. 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 $+$, since $0 + x = x + 0 = x$ for all $x \in \mathbb{Z}$.
- $1 \in \mathbb{Q}$ is an identity for $\cdot$, since $1 \cdot x = x \cdot 1 = x$ for all $x \in \mathbb{Q}$.
- $0 \in \mathbb{Q}$ is not an identity for $\cdot$, since $0 \cdot x = 0 \neq x$ for all $x \in \mathbb{Q}$.

Lemma

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

Proof.

$e = e \boxtimes e' = e'$. □

Inverses

Definition — inverse

Let $\boxtimes$ be a binary operation on X with an identity element e. An element y is a **left inverse** for x (with respect to $\boxtimes$) 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 $n \in \mathbb{Z}$ with respect to $+$, since $n + (-n) = (-n) + n = 0$.
- $n \in \mathbb{Z}$ does not have an inverse with respect to $\cdot$ unless $n = \pm 1$.
- If $x \in \mathbb{Q}$ is non-zero, then $1/x$ is an inverse of x with respect to $\cdot$. The element 0 does not have an inverse, since there is no element y with $0 \cdot y = 1$.

Lemma

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

Proof.

$y_L = y_L \boxtimes e = y_L \boxtimes (x \boxtimes y_R) = (y_L \boxtimes x) \boxtimes y_R = e \boxtimes y_R = y_R$. □

Corollaries:

- If x has both a left and a right inverse, then x has an inverse.
- Inverses are unique: if y and y' are both inverses of x, then $y = y'$.

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

Exercise

Show it is possible to have a left (resp. right) inverse, but not be invertible. Also show left and right inverses are not necessarily unique (unless an element has both).

Properties of inverses

Lemma

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

□

Inverses and solving equations

Proposition

Let $\boxtimes$ be an associative binary operation on X with an 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 $a \boxtimes x = b$ and $y \boxtimes a = b$ have unique solutions for all $b \in X$.

Proof.

($\Longleftarrow$) A solution to $a \boxtimes x = e$ is a right inverse of a, and a solution to $y \boxtimes a = b$ is a left inverse. Since both solutions exist, a has an inverse.

($\Longrightarrow$) Suppose a is invertible. Then

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

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 $y \boxtimes a = b$.

□

Left and right cancellation property

Proposition

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

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

Proof.

1. $u = a_L \boxtimes a \boxtimes u = a_L \boxtimes a \boxtimes v = v$.
2. Similar.

□

(1) and (2) also hold for $n \in \mathbb{Z}$ with respect to $\cdot$ if $n \neq 0$, even though n is not invertible for $n \neq \pm 1$.

Groups

Definition — 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 $\boxtimes$.

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

A group is **finite** if G is a finite set. The **order** of G is the number of elements in G if G is finite, or $+\infty$ if G is infinite.

The order of G is denoted by $|G|$.

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 $\boxtimes$, so usually we use one of the following options:
  - Use $\cdot$ as the standard symbol: $g \cdot h$ is the product of $g, h \in G$.
  - Drop the symbol entirely: gh is the product of $g, h \in G$.
- The identity of G is denoted by e (or e_G for clarity). Also used are 1 and 1_G.
- 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 $\iota \colon G \to G : g \mapsto g^{-1}$. Since $(g^{-1})^{-1} = g$, $\iota \circ \iota = \mathrm{Id}_G$, the identity map $G \to G$. In particular, ι is a bijection (injective and surjective).
- If $g \in G$, then
$$g^n := \underbrace{g \cdots g}_{n \text{ times}}$$
and
$$g^{-n} := (g^{-1})^n = (g^n)^{-1}$$
where $g^0 := e$. Exercise: if $m, n \in \mathbb{Z}$, then $(g^n)^m = g^{mn}$.
- If $g, h \in G$, then
$$(gh)^n = gh \cdots gh,$$
which is not necessarily the same as $g^n h^n$ if G is not abelian.

Example

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all (abelian) groups under operation $+$. The identity is 0 and the inverse of n is $-n$. These groups have infinite order.
- $\mathbb{Z}/n\mathbb{Z}$ is also a group under $+$ (and also abelian). The identity is $0 = [0]$ and the inverse of $[m]$ is $-[m] = [-m]$. This group is finite with order $|\mathbb{Z}/n\mathbb{Z}| = n$.
- If $(V, +, \cdot)$ is a vector space, then $(V, +)$ is a group. The identity is 0 and the inverse of v is $-v$.
- $\mathbb{Z}$ 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 the **trivial group**.

A non-abelian example

All the previous examples are abelian.

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

Proposition

$\mathrm{GL}_n(\mathbb{K})$ 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 on $\mathrm{GL}_n(\mathbb{K})$. 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 $AB \neq BA$. □

Additive notation

Standard notation for a group operation is gh. This is called **multiplicative notation**.

For groups like $(\mathbb{Z}, +)$, it is confusing to write mn instead of $m + n$ since mn already has another meaning.

For abelian groups G, we can also use **additive notation**. In additive notation, we write the group operation as $g + h$. The identity is denoted by 0 or 0_G. Inverses are denoted by $-g$.

Writing g^n in additive notation gives

$$\underbrace{g + \cdots + g}_{n \text{ times}}$$

so instead of g^n we use ng. Similarly g^{-n} is $-ng$.

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

For non-abelian groups we always use multiplicative notation. For abelian groups, we can choose either. Note the conventions may conflict, so we should be clear about which we choose.

For a group like $(\mathbb{Z}, +)$, we could use mn, but it is clearer to use $m + n$.

For a group like $(\mathbb{Q}^\times, \cdot)$, we could use $x + y$, but it is clearer to use $x \cdot y$ or xy.

Multiplication table

Definition — multiplication table

The **multiplication 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 information of the group (even for infinite groups).

Example

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

	0	1
0	0	1
1	1	0

Order of elements

Definition — order of a group element

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

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

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

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

Lemma

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

But $g^{-n} = (g^{-1})^n$ also, so $\{k \geq 1 : g^k = e\} = \{k \geq 1 : (g^{-1})^k = e\}$ which implies $|g| = |g^{-1}|$. □

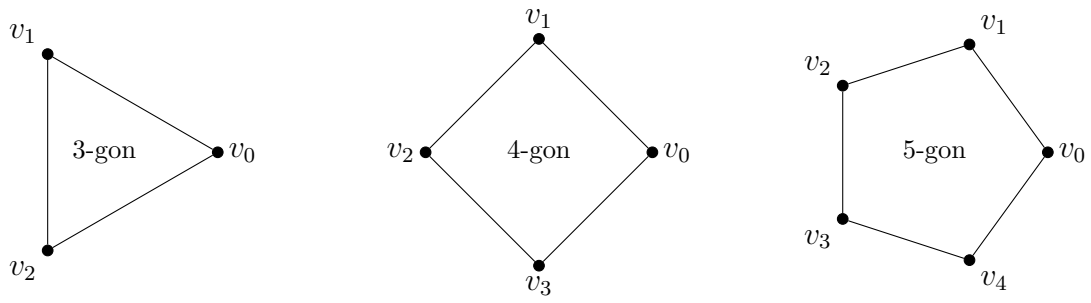
2: Dihedral and permutation groups

Dihedral groups

Definition — n-gon

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

Specifically: set $v_k = (\cos(2\pi k/n), \sin(2\pi k/n)) = e^{2\pi ik/n}$ and get an n-gon by drawing a line segment from v_k to v_{k+1} for all $0 \leq k \leq n$ (where $v_n := v_0$).



Definition — symmetry, dihedral group

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

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

(Think of matrices and linear transformations interchangeably. Matrix multiplication = composition of transformations.)

Proposition

D_{2n} is a group under composition.

Proof later (key point: $S, T \in D_{2n} \implies ST \in D_{2n}$).

Lemma

Say v_i and v_j are adjacent in P_n if they are connected by a line segment.

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

Proof.

1. v_0, v_1 are adjacent and T is linear (lines map to lines).
2. v_0, v_1 are linearly independent (and form a basis in $\mathbb{R}^2$).

□

Corollary

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

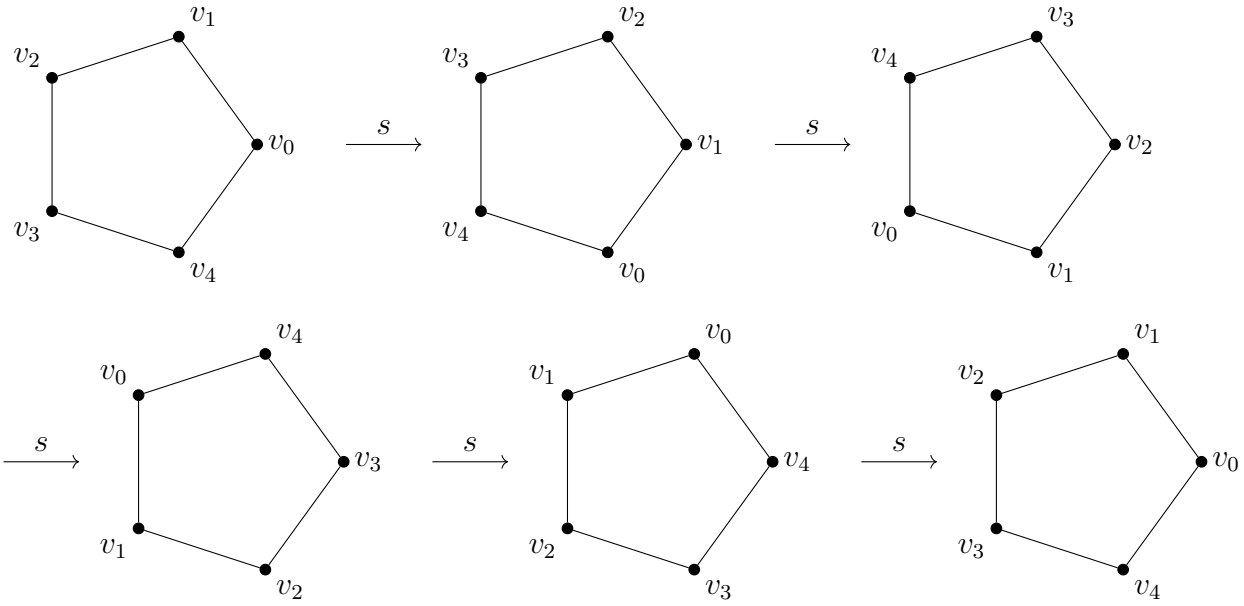
Proof.

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

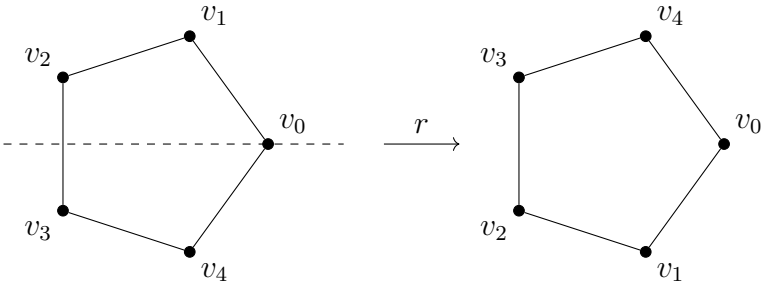
Intuitively, we can ask: for every pair of adjacent vertices (v_i, v_j), is there an element $T \in D_{2n}$ with $T(v_0) = v_i$ and $T(v_1) = v_j$? If yes, then $|D_{2n}| = 2n$.

Special elements of D_{2n}

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



Let r be reflection through the x-axis.



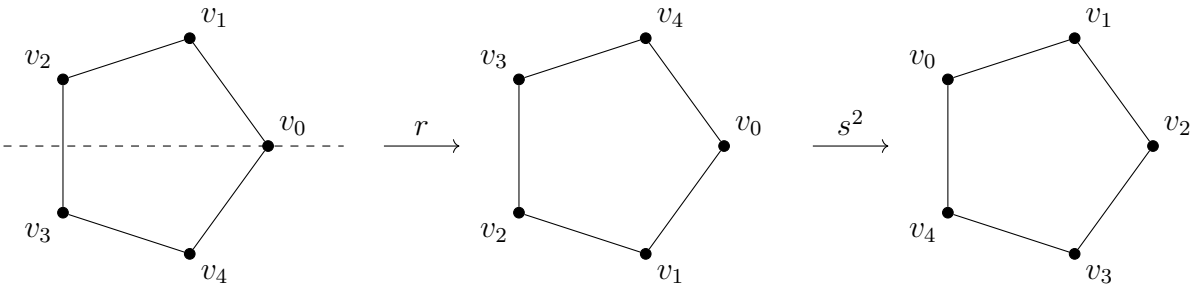
$|r| = 2$, that is, $r^2 = e$ and $r \neq e$.

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

Putting rotation and reflection together

s^i for $0 \leq i < n$ sends $v_0 \mapsto v_i$ and $v_1 \mapsto v_{i+1}$. (Say $v_n = v_0$ and $s^0 = e$.)

$s^i r$ for $0 \leq i < n$ sends $v_0 \mapsto v_i$ and $v_1 \mapsto v_{i-1}$. (Say $v_{-1} = v_{n-1}$.)



Proposition

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

So 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

D_{2n} is a finite non-abelian group.

In summary:

- $D_{2n} = \{s^i r^j : 0 \leq i < n,\ 0 \leq j < 2\}$
- $|D_{2n}| = 2n$
- $s^n = e$, $r^2 = e$, $rs = s^{-1}r$
- D_{2n} is a finite non-abelian group.

Exercise: show these relations are enough to completely determine D_{2n}.

What's group theory about?

Basic answer: sets with one binary operation.

Better answer: group theory is the study of symmetry.

If we resize or rotate P_n, then the symmetries remain the same.

Kleinian view of geometry:

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

Permutation groups

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

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

is an associative operation with an identity Id_X.

Let $S_X = \{f \in \mathrm{Fun}(X,X) : f \text{ is a bijection}\}$.

Proposition

S_X is a group under $\circ$.

Proof.

Homework. □

Definition — symmetric 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 $\pi\colon \{1,\ldots,n\} \to \{1,\ldots,n\}$.

What makes such a π a bijection? Every element of $\{1,\ldots,n\}$ must appear in the list $\pi(1),\ldots,\pi(n)$ and no element can appear twice.

We have n choices for $\pi(1)$, $n-1$ choices for $\pi(2)$, $\ldots$, 1 choice for $\pi(n)$. Thus $|S_n| = n(n-1)\cdots 1 = n!$.

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

Permutations

Elements of S_n are called **permutations**. We have several ways of representing 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: $\pi = 651423$.
3. Disjoint cycle representation: write down the **cycles** of π. Here $\pi(1) = 6$, $\pi(6) = 3$, and $\pi(3) = 1$, so (163) is a cycle of π.

   $\pi = (163)(25)(4) = (163)(25)$. We typically drop cycles of length 1, and write cycles containing the smallest unused element first.

   The identity is empty in disjoint cycle notation, so we just use e.

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

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (163)(25)$$
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & 1 \end{pmatrix} = (126)(345)$$
$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 1 & 6 \end{pmatrix} = (15)(234)$$

One-line notation is hard, so we don't use it here.

Inversion can also be done in two-line or disjoint cycle notation:

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

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

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

Fixed points and support sets

Definition — fixed point, support set

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

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

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

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

Example

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

Some notes:

- In general, $\operatorname{supp}(\pi)$ are exactly the numbers that appear in the disjoint cycle representation of π (when length-1 cycles are omitted).
- $\operatorname{supp}(\pi) = \varnothing$ if and only if $\pi = e$.
- $\operatorname{supp}(\pi^{-1}) = \operatorname{supp}(\pi)$.
- If $i \in \operatorname{supp}(\pi)$, then $\pi(i) \in \operatorname{supp}(\pi)$.

Commuting elements

Definition — commute

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

Lemma

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

Proof.

Suppose $1 \leq i \leq n$.

If $i \in \text{supp}(\pi)$, then $\pi(i) \in \text{supp}(\pi)$. Since π, σ are disjoint, we have $i, \pi(i) \notin \text{supp}(\sigma)$. 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 $\pi(\sigma(i)) = i = \sigma(\pi(i))$.

Then $\pi(\sigma(i)) = \sigma(\pi(i))$ for all i, so $\pi\sigma = \sigma\pi$. □

Cycles

Definition — cycle

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

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

Example

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

Additionally, we have $\pi^{-1} = c_k^{-1} \cdots c_1^{-1} = c_1^{-1} \cdots c_k^{-1}$.

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, so π and π^i commute. However, π and π^i don't have disjoint support sets.

Week 2: Subgroups and homomorphisms

3: Subgroups

Subgroups

Definition — subgroup

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

1. for all $g, h \in H$, $g \cdot h \in H$ (H is **closed under products**),
2. for all $g \in H$, $g^{-1} \in H$ (H is **closed under inverses**), and
3. $e_G \in H$.

Notation: $H \leq G$.

Example

- $\mathbb{Z} \leq \mathbb{Q}^+ := (\mathbb{Q}, +)$.
- $\mathbb{Q}_{>0} := \{x \in \mathbb{Q} : x > 0\} \leq \mathbb{Q}^\times$.

  Check: if $x, y \in \mathbb{Q}$ and $x, y > 0$, 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

Let $G = D_{2n}$ and s be 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 $i = nk + r$ with $0 \leq r < n$. Then $s^i = s^{nk+r} = (s^n)^k s^r = s^r$ since $s^n = e$.

Checking subgroup properties:

- If $s^i, s^j \in H$, then $s^{i+j} \in H$.
- If $s^i \in H$, then $s^{-i} \in H$.
- $e \in H$.

□

H is the smallest subgroup containing s (since subgroups are closed under products).

Notation for H is $\langle s \rangle$.

Example

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

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

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

Definition — trivial subgroup, proper subgroup

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

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

H is a proper non-trivial subgroup if $\{e\} \neq H < G$.

Example

Some non-subgroups:

- $\mathbb{Q}_{\geq 0} := \{x \in \mathbb{Q} : x \geq 0\}$ is not a subgroup of $\mathbb{Q}^+$.

  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 $x \in Q_{\geq 0}$, 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

If H is a subgroup of $(G, \boxtimes)$, then $(H, \boxtimes|_{H\times H})$ is a group, such that
1. the identity of H is $e_H = e_G$, and
2. the inverse of $g \in H$ is the same as the inverse of g in G.

Proof.

First, we show $\boxtimes|_{H\times H}$ is a binary operation on H. Note $\boxtimes$ is a function $G \times G \to G$, so $\boxtimes|_{H\times H}$ is a function $H \times H \to G$. But if $g, h \in H$, then $g \boxtimes h \in H$. Thus $\boxtimes|_{H\times H}$ is a function $H \times H \to H$.

From now on, denote this function by $\tilde{\boxtimes}$.

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

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

If $g \in H$, then g^{-1} with respect to $\boxtimes$ is in H.

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

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

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

Example

- $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ with operation $+$.
- If H is a subgroup of $(G, \cdot)$, then H is a group with operation $\cdot$.

Speeding up the subgroup check

Proposition

H is a subgroup of G if and only if
1. H is non-empty, and
2. $gh^{-1} \in H$ for all $g, h \in H$.

Proof.

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

($\impliedby$) By (1), there is some $x \in H$. By (2), $xx^{-1} = e_G \in H$.

Also by (2), $e_G \cdot x^{-1} = x^{-1} \in H$ (so H is closed under inverses).

Now if $x, y \in H$, then $y^{-1} \in H$, so $xy = x(y^{-1})^{-1} \in H$ (so H is closed under products).

□

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 $v + (-w) = v - w \in W$.

W is a subgroup by the proposition.

Finite subgroups

Proposition

Suppose H is a finite subset of G. Then H is a subgroup of G if and only if
1. H is non-empty, and
2. $gh \in H$ for all $g, h \in H$.

Proof.

The forward direction is trivial.

Suppose $g \in H$. By induction, we can show $g^n \in H$ for all $n \in \mathbb{N}$.

Since H is finite, the 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 $n = j - i$.

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

Subgroups generated by a set

Proposition

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

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

is a subgroup of G.

Proof.

Note $e_G \in H$ for all $H \in \mathcal{F}$, so $e_G \in K$ and thus K is non-empty.

Now consider $x, y \in K$. Then $x, y \in H$ for all $H \in \mathcal{F}$, so $y^{-1} \in H$ for all $H \in \mathcal{F}$, so $xy^{-1} \in H$ for all $H \in \mathcal{F}$, so $xy^{-1} \in K$.

By proposition, K is a subgroup of G. □

Definition — subgroup generated by a set

Let S be a subset of a group G.

The **subgroup generated by S in G** is

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

Notes:

- The 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 the smallest subgroup of G containing S.
- $\langle \varnothing \rangle = \langle e \rangle = \{e\}$, the trivial subgroup.
- If $S = \{s_1, s_2, \ldots\}$, we often write $\langle S \rangle = \langle s_1, s_2, \ldots \rangle$.

Example

Consider D_{2n} and its rotation generator s.

Let $K = \{e = s^0, s^1, s^2, \ldots, s^{n-1}\}$. As previously checked, K is a subgroup of D_{2n}.

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

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

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

If $S \subset G$, let $S^{-1} = \{s^{-1} : s \in S\}$.

Proposition

If $S \subset G$, let

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

Then $\langle S \rangle = K$.

Proof.

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

Proof: We know $e \in \langle S \rangle$. Prove by induction that $s_1 \cdots s_k \in \langle S \rangle$ for all $k \geq 1$ and $s_1, \ldots, s_k \in S \cup S^{-1}$.

Claim 2: K is a subgroup.

Proof: $e \in K$ by construction. Consider $x, y \in K$. Then

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

So $xy = s_1 \cdots s_k t_1 \cdots t_\ell \in K$, and $x^{-1} = s_k^{-1} \cdots s_1^{-1} \in K$ since $s_k^{-1}, \ldots, s_1^{-1} \in S \cup S^{-1}$.

So K is a subgroup.

Proof of proposition: $S \subseteq K$ and $\langle S \rangle$ is the smallest subgroup containing S, so $\langle S \rangle \subseteq K$.

Thus $\langle S \rangle = K$. □

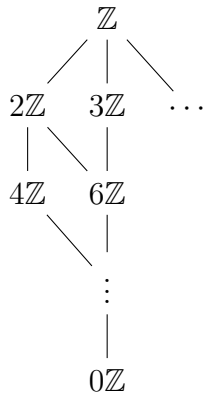
Lattice of subgroups

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 $\leq$. (Exercise.)

The set of subgroups of G with order $\leq$ is called the **lattice of subgroups of G**.

The first subgroup below $H_1, H_2 \leq G$ in the lattice is $H_1 \cup H_2$. The first subgroup above $H_1, H_2 \leq G$ in the lattice is $\langle H_1 \cup H_2 \rangle$.



4: Cyclic groups

Generators and cyclic groups

Definition — generate, cyclic

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

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 (homework)
- 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

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 previous proposition about $\langle S \rangle$.
2. See argument for $\langle s \rangle$ in D_{2n}.

□

Questions:

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

Order of cyclic groups

Proposition

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

Proof.

We've already seen that $|G| \leq |a|$.

Suppose $|G| = n < \infty$.

The sequence $a^0, a^1, a^2, \ldots, a^n \in G$ must have repetition. So there are $0 \leq i < j \leq n$ with $a^i = a^j$, which means $a^{j-i} = e$ and hence $|a| \leq n$.

So $|a| \leq |G|$, thus $|a| = |G|$. □

Examples in closer detail

Example

For $G = \mathbb{Z}$:

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

  Homework: all subgroups of $\mathbb{Z}$ are cyclic.

Example

Can we analyze $\mathbb{Z}/n\mathbb{Z}$ in the same way?

(Note: at this point we may drop the brackets. For example, in $\mathbb{Z}/5\mathbb{Z}$, $3 = 8$.)

Questions:

- What are the generators of $\mathbb{Z}/n\mathbb{Z}$?
- What are the orders of elements of $\mathbb{Z}/n\mathbb{Z}$?
- What are the subgroups?

Generators of $\mathbb{Z}/n\mathbb{Z}$

Lemma

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

So $\mathbb{Z}/n\mathbb{Z} = \langle [a] \rangle$ if and only if $[1] \in \langle [a] \rangle$ (since $[1]$ is a generator). Note then

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

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

Order of elements in $\mathbb{Z}/n\mathbb{Z}$

Lemma

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

Proof.

Homework. □

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

Lemma

Suppose $a \mid n$. 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

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

Proof.

Since $b \mid a$, there is k such that $a = kb$. Thus $[a] \in \langle [b] \rangle$, so $\langle [a] \rangle \subseteq \langle [b] \rangle$.

By properties of gcd, there are $x, y \in \mathbb{Z}$ such that $xa + yn = b$.

So $[b] = x[a] + y[n] = x[a]$, which implies $[b] \in \langle [a] \rangle$ and thus $\langle [b] \rangle \subseteq \langle [a] \rangle$.

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

Proposition

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

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

But $b \mid n$, so by lemma $|[b]| = \frac{n}{b}$. □

Subgroups of $\mathbb{Z}/n\mathbb{Z}$

Corollary

Let $n \geq 1$.

- The order d of any cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ divides n.
- For every $d \mid n$, there is a unique cyclic 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.

Also, $d = \frac{n}{\gcd(a,n)}$, and by lemma, $\langle [a] \rangle = \langle [\frac{n}{d}] \rangle$.

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

Example

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

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

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

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

Proofs later

- Every subgroup of a cyclic group is cyclic. (So the previous corollary is a complete list of subgroups of $\mathbb{Z}/n\mathbb{Z}$.)
- Every cyclic group is isomorphic to one of $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$, or $\mathbb{Z}$.