PMATH 347: Groups and Rings

University of Waterloo
William Slofstra
Spring 2021

Marco Yang

Last updated: June 23, 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,

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

$\square$

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.

$e = e \boxtimes e' = e'$. $\square$

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.

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

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

$\square$

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 $y \boxtimes a = b$.

$\square$

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.

$\square$

(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 $AB \neq BA$. $\square$

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 $|g| = |g^{-1}|$. $\square$

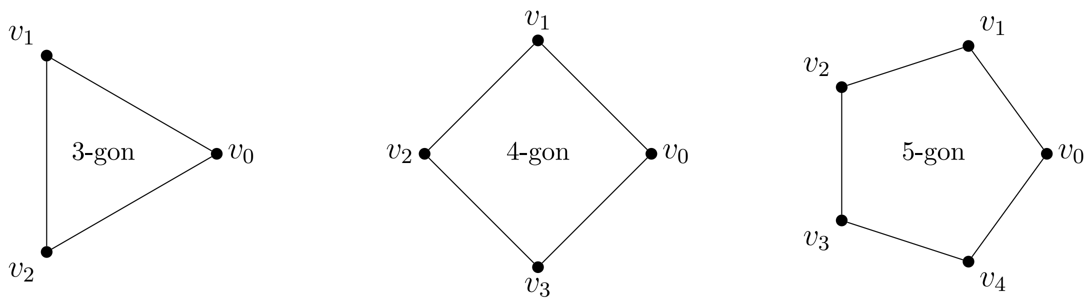
2: Dihedral and permutation groups

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 $\mathbb{R}^2$).

$\square$

Corollary

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

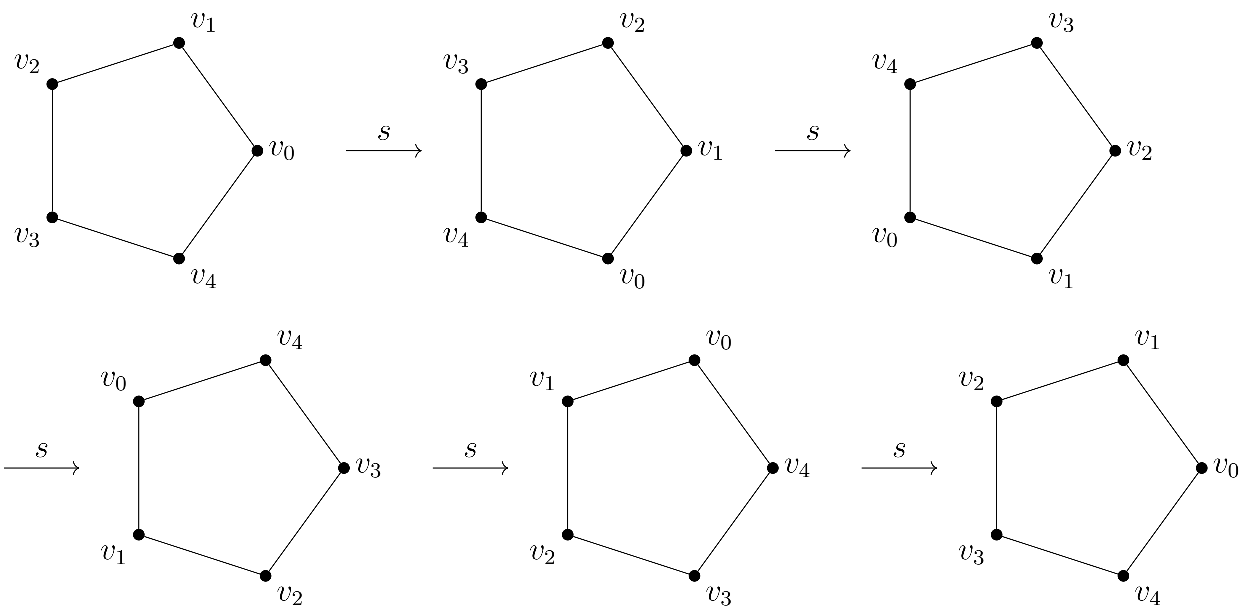
Proof.

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. $\square$

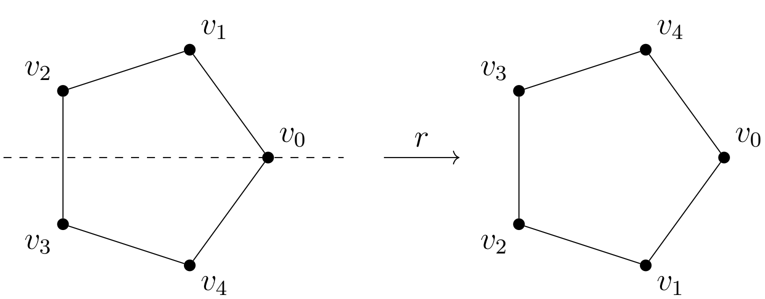
Intuitively, we can ask: for every pair of adjacent vertices (v_i, v_j), is there an element $T \in D_{2n}$ with $T(v_0) = v_i$ and $T(v_1) = v_j$? If yes, then $|D_{2n}| = 2n$.

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.



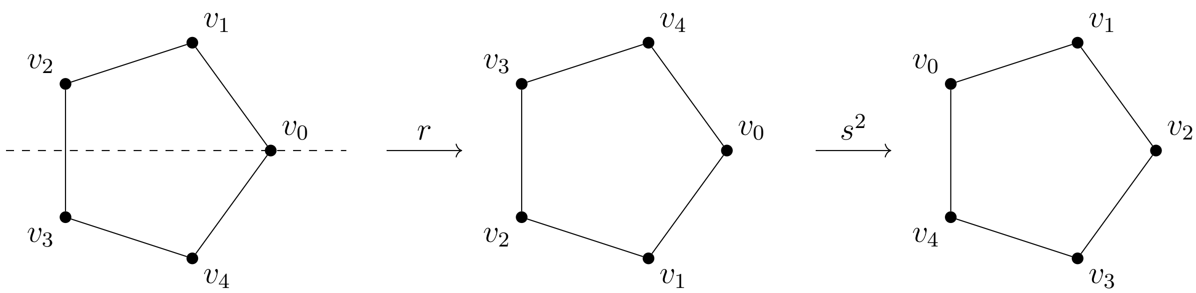
$|r| = 2$, that is, $r^2 = e$ and $r \neq e$.

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. $\square$

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

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

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

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

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 $s^{-i} \in H$.
- $e \in H$.

$\square$

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).

$\square$

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 $g^{n-1} = g^{-1} \in H$. $\square$

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. $\square$

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

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

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 $\langle S\rangle = K$. $\square$

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 $\langle H_1 \cup H_2 \rangle$.

$$\begin{tikzcd}[arrows=-]
& \mathbb{Z} \arrow[dl] \arrow[d] \arrow[dr] & \\
2\mathbb{Z} \arrow[d] \arrow[dr] & 3\mathbb{Z} \arrow[d] & \cdots \\
4\mathbb{Z} \arrow[dr] & 6\mathbb{Z} \arrow[d] & \\
& \vdots \arrow[d] & \\
& 0\mathbb{Z} &
\end{tikzcd}$$

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 $\langle a\rangle = \{a^i : 0 \le i < n\}$.

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 $|a| = |G|$. $\square$

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 $G = \langle T \rangle$ 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 $|[b]| = \frac{n}{b}$. $\square$

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 $|\langle [a] \rangle| = d$. $\square$

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 $\mathbb{Z}$.

5: Homomorphisms

Homomorphisms

Definition — homomorphism (morphism)

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

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

for all $g, h \in G$.

A homomorphism preserves the group operation from G to H.

Example

- For $\mathbb{K}$ a field, $\mathbb{K}^\times = \{a \in \mathbb{K} : a \neq 0\}$ is a group with operation $\cdot$.

  Then $\mathrm{GL}_n \mathbb{K} \to \mathbb{K}^\times : A \mapsto \det(A)$ is a homomorphism because $\det(AB) = \det(A)\det(B)$ for all A, B.
- Let $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\} \leq \mathbb{R}^\times$. Then $\mathbb{R}_{>0} \to \mathbb{R}_{>0} : x \mapsto \sqrt{x}$ is a homomorphism since $\sqrt{xy} = \sqrt{x}\sqrt{y}$.
- Additive notation: $\phi\colon (G, +) \to (H, +)$ is a homomorphism if $\phi(x+y) = \phi(x)+\phi(y)$ for all $x, y \in G$.

  $\phi\colon \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ is a homomorphism for any $m \in \mathbb{Z}$ since $\phi(x+y) = m(x+y) = mx + my = \phi(x) + \phi(y)$ for all $x, y \in \mathbb{Z}$.
- If V, W are vector spaces and $T\colon V \to W$ 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 because $e^{x+y} \neq e^x + e^y$ in general (take $x = y = 0$).

Lemma

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

1. $\phi(e_G) = e_H$.
2. $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.
3. $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$.
4. $|\phi(g)| \mid |g|$ for all $g \in G$ (say $n \mid \infty$ for all $n \in \mathbb{N}$).

Proof.

1. $\phi(e_G) = \phi(e_G^2) = \phi(e_G) \cdot \phi(e_G)$, so $e_H = \phi(e_G)^{-1} \cdot \phi(e_G) = \phi(e_G)^{-1} \cdot \phi(e_G) \cdot \phi(e_G) = \phi(e_G)$.
2. $e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ and similarly $\phi(g^{-1})\phi(g) = e_H$, so $\phi(g^{-1})$ is the unique inverse of $\phi(g)$.
3. Use induction for $n \geq 0$, additionally with part (b) for $n < 0$.
4. If $|g| = n < \infty$, then $g^n = e_G$ so $\phi(g)^n = \phi(g^n) = \phi(e_G) = e_H$. Homework: prove $|\phi(g)| \mid n$.

$\square$

Making new homomorphisms from old

Lemma

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

Proof.

$i(g \cdot h) = g \cdot h = i(g) \cdot i(h)$. □

Lemma

If $\phi\colon G \to M$ and $\psi\colon H \to K$ 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

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

Proof.

$\phi|_K = \phi \circ i$, where $i\colon K \to G$ is the inclusion $x \mapsto x$. □

Images of homomorphisms

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

Proposition

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

That is, homomorphisms send subgroups of the domain to subgroups of the codomain.

Proof.

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

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

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 $x_0 y_0^{-1} \in K$. $\square$

Definition — image

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

Example

- Let $\phi\colon \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$.

  $e^x > 0$ 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 $i\colon K \to G$ is inclusion, then $\operatorname{Im} i = K$.
- For $\phi\colon \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$ for some $m \in \mathbb{Z}$, $\phi(\mathbb{Z}) = m\mathbb{Z}$.

Properties of images

Lemma

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

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

Lemma

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

Proof.
Obvious from definition. □

Corollary

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

Proposition

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

Proof.

First, $\phi(S^{-1}) = \{\phi(s^{-1}) : s \in S\} = \{\phi(s)^{-1} : s \in S\} = \phi(S)^{-1}$. Thus

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

□

Pulling back subgroups

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

Proposition

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

That is, we can also get a subgroup of the domain from a subgroup of the codomain.

Note: the forward and backward processes are not necessarily inverses, so we don't have a bijection (just yet).

Proof.

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

If $x, y \in \phi^{-1}(K)$, then $\phi(x), \phi(y) \in K$ so $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \in K$ and hence $xy^{-1} \in \phi^{-1}(K)$. □

The kernel of a homomorphism

Definition — kernel

If $\phi\colon G \to H$ 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 $\det\colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$, we have $\ker\det = \{A \in \mathrm{GL}_n(\mathbb{K}) : \det(A) = 1\}$.

  This subgroup of $\mathrm{GL}_n(\mathbb{K})$ is called the **special linear group**, denoted by $\mathrm{SL}_n(\mathbb{K})$.
- If $\phi\colon \mathbb{Z} \to \mathbb{Z} : k \mapsto mk$, 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 $\phi\colon \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$, then $e^x = 1$ if and only if $x = 0$, so $\ker\phi = \{0\}$.

Proposition

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

Proof.

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

($\Longleftarrow$) 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 $x = y$. That is, ϕ is injective.

$\square$

Application: subgroups of cyclic groups

Proposition

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

Proof.

We need the following facts:

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

Since G is cyclic, by (2) there is a surjective homomorphism $\phi\colon \mathbb{Z} \to G$.

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

So let $\psi\colon \mathbb{Z} \to \mathbb{Z}$ be the homomorphism with $\psi(k) = mk$.

Then $\phi \circ \psi\colon \mathbb{Z} \to G$ is a homomorphism. We see that

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

by (3).

We can restrict the codomain of $\phi \circ \psi$ to get a surjective homomorphism $\mathbb{Z} \to H$. Hence H is cyclic by (2). $\square$

Review on bijections

Definition — bijection

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

- **injective** if for all $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies that $x_1 = x_2$;
- **surjective** if for all $y \in Y$, there exists $x \in X$ with $f(x) = y$; and
- **bijective** if f is both injective and surjective.

Proposition

$f\colon X \to Y$ is a bijection if and only if there is a function $g\colon Y \to X$ 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}.

Isomorphisms

Definition — isomorphism

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

Lemma

$\phi\colon G \to H$ 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 $\phi\colon G \to H$ is injective, then ϕ induces an isomorphism $G \to \operatorname{Im}\phi$.
- $\mathbb{Z} \to m\mathbb{Z} : k \mapsto mk$ is an isomorphism.

Proposition

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

Proof.

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

Let $g, h \in H$. Then $\phi(\phi^{-1}(g) \cdot \phi^{-1}(h)) = \phi(\phi^{-1}(g)) \cdot \phi(\phi^{-1}(h)) = g \cdot h$.

So $\phi^{-1}(g) \cdot \phi^{-1}(h) = \phi^{-1}(g \cdot h)$. Hence ϕ^{-1} is a homomorphism. $\square$

Corollary

A homomorphism $\phi\colon G \to H$ is an isomorphism if and only if there is a homomorphism $\psi\colon H \to G$ such that
1. $\psi \circ \phi = 1_G$, and
2. $\phi \circ \psi = 1_H$.

This shows isomorphisms are to homomorphisms as bijections are to functions.

Proof.

($\Longleftarrow$) If ψ exists, then ϕ is a bijection.

($\Longrightarrow$) If ϕ is an isomorphism, then we can take $\psi = \phi^{-1}$.

□

Definition — isomorphic

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

Notation: $G \cong H$.

Key facts:

- If $G \cong H$, then $H \cong G$ (symmetry).

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

- If $G \cong H$ and $H \cong K$, then $G \cong K$ (transitivity).

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

- $G \cong G$ (reflexivity).

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

Isomorphism as a relation

Idea: if $G \cong H$, then G and H are identical *as groups*.

If $\phi\colon G \to H$ 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.

Isomorphisms of cyclic groups

Proposition

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

Proof.

The forward implication is obvious.

Suppose $G = \langle a \rangle$ and $H = \langle b \rangle$ where $|G| = |H|$.

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

Proof: if $a^i = a^j$ then $a^{j-i} = e$, apply the homework to finish. Conversely, if $|a| \mid j - i$, then $j - i = k|a|$. So $a^{j-i} = a^{k|a|} = e$ and hence $a^j = a^i$.

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

Now define $\phi\colon G \to H : a^i \mapsto b^i$.

Notice $|a| = |G| = |H| = |b|$. Then $a^i = a^j$ implies $|a| \mid j - i$ implies $|b| \mid j - i$ implies $b^i = b^j$, so ϕ is well-defined.

We see $\phi(a^i \cdot a^j) = \phi(a^{i+j}) = b^{i+j} = b^i \cdot b^j = \phi(a^i) \cdot \phi(a^j)$ for all $a^i, a^j \in G$, so ϕ is a homomorphism.

Similarly to above, $\psi\colon H \to G : b^i \mapsto a^i$ is well-defined and clearly an inverse to ϕ.

Thus ϕ is an isomorphism. $\square$

Corollary

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

Cyclic groups are abelian.

Exercise

Prove the previous corollary without the corollary before it.

Multiplicative notation for cyclic groups

Sometimes it is convenient to use the multiplicative form of cyclic groups.

Definition

Let a be a formal indeterminate. Let

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

Of course, we have:

- $C_\infty \cong \mathbb{Z}$ via $a^i \mapsto i$.
- $C_n \cong \mathbb{Z}/n\mathbb{Z}$ via $a^i \mapsto i$.

Week 3: Cosets, Lagrange's Theorem, and Products

6: Cosets and Lagrange's Theorem

Affine spaces

Linear subspaces motivate the definition of subgroups. Let $T\colon V \to W$ be a linear transformation (so T is a homomorphism $(V,+) \to (W,+)$). We get $\ker T = \{x \in V : T(x) = 0\}$ which are the "solutions to $Tx = 0$". What are the solutions to $Tx = b$?

Note $Tx = b$ has a solution if and only if $b \in \operatorname{Im} T$. If $b \in \operatorname{Im} T$ and $Tx = b$ has solution x_0, then all other solutions are of the form $x_0 + x_1$ for $x_1 \in \ker T$. We conclude the space of solutions has form $x_0 + \ker T$. We call this an **affine subspace** (like a linear subspace, but may not contain 0).

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

For abelian groups, $gH = Hg$. In additive notation, a coset of H in $(G,+)$ is $g + H$.

Example

- If U is a 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

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

Cosets in the dihedral group

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

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

The right cosets of H are:

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

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

Exercise 1: use $rs = s^{-1}r$ to show $s^i r = rs^{-i}$ for all $i \in \mathbb{Z}$.

Exercise 2: if $S \subseteq G$ and $g, h \in G$, then $ghS = g(hS)$.

The left cosets of H are:

- $eH = H$
- $s^i H = H$
- $s^i rH = rs^{-i}H = rH$

Notice

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

so in this case, the left and right cosets are equal.

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

Left cosets: $rK = \{r, e\} = K$ and $s^i K = \{s^i, s^i r\} = s^i rK$. We see the left cosets are $s^i K$ for $0 \le i < n$, and

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

Right cosets: $Kr = \{r, e\} = K$ and $Ks^i = \{s^i, rs^i\} = \{s^i, s^{-1}r\}$ and $Ks^i r = \{s^i r, s^{-1}\} = Ks^{-1}$. We see the right cosets are Ks^i for $0 \le i < n$, and

$$D_{2n} = \bigsqcup_{i=0}^{n-1} Ks^i.$$

In this case, the left and right cosets are not equal.

Sets of cosets

Definition — set of 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

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

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

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

Example

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

Example

Consider $n\mathbb{Z} \leq \mathbb{Z}$. Then

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

so

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

A big question for later: for which $H \leq G$ is G/H a group?

Cosets of a kernel

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

Lemma

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 $\phi(x_0^{-1}x_1) = b^{-1}b = e$, so $x_0^{-1}x_1 \in H$ and thus $x_1 = x_0(x_0^{-1}x_1) \in x_0H$.

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

A similar argument using right cosets shows the set of solutions is also Hx_0. $\square$

In this case, the left cosets are the right cosets.

Proposition

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

Proof.

$g \cdot \ker\phi$ is the set of solutions to $\phi(x) = b$ where $b = \phi(g)$.

As a result, $\phi(g \cdot \ker\phi) = \{b\}$ and $b \in \operatorname{Im}\phi$.

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

Example

Suppose $G = \mathbb{Z}$ and $K = \mathbb{Z}/n\mathbb{Z}$.

From tutorial, there is a homomorphism $\phi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : a \mapsto [a]$. We get $\ker\phi = n\mathbb{Z}$ and $\operatorname{Im}\phi = \mathbb{Z}/n\mathbb{Z}$.

Then $\mathbb{Z}/n\mathbb{Z} = \{[a] : 0 \leq a < n\} = \{a + n\mathbb{Z} : 0 \leq a < n\}$, so $a + n\mathbb{Z}$ is the set of solutions of $[x] \equiv [a]$ in $\mathbb{Z}/n\mathbb{Z}$.

Indexes and Lagrange's theorem

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

Definition — 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 — Lagrange's theorem

If $H \leq G$, then $|G| = [G:H] \cdot |H|$.

Why use left cosets in the definition?

Proposition

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

Proof.

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

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

because $H \to H : h \mapsto h^{-1}$ is a bijection. So ϕ is well-defined, and a similar argument shows $\psi\colon H\backslash G \to G/H : S \mapsto S^{-1}$ is well-defined.

Finally, ψ is an inverse to ϕ. □

Corollary

If $H \leq G$ then

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

Results from Lagrange's theorem: if $H \leq G$, then $|H|$ divides $|G|$, and if G is finite, then $[G : H] = \frac{|G|}{|H|}$.

Example

- $G = D_{2n}$, $H = \langle s \rangle$. Here, $|D_{2n}| = 2n$, $|H| = n$, so $[G : H] = 2$.
- $G = D_{2n}$, $H = \langle r \rangle$. Here, $|D_{2n}| = 2n$, $|H| = 2$, so $[G : H] = n$.
- $G = \mathbb{Z}$, $H = m\mathbb{Z}$. Here, $|G| = |H| = \infty$, but $[G : H] = |\mathbb{Z}/m\mathbb{Z}| = m$. So $|G| = [G : H]|H|$, but we don't learn anything about $[G : H]$ from Lagrange's theorem.

Consequences of Lagrange's theorem

Corollary

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

Proof.

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

Proposition

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

Proof.

Let $x \in G$ and $x \neq e$. Then $|x| \neq 1$, and $|x| \mid |G|$, so $|x| = |G|$. Then since $|\langle x \rangle| = |x| = |G|$, we have $G = \langle x \rangle$ (since G is finite). □

We can thus list out groups of small orders (up to isomorphism)...

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	$\mathbb{Z}/9\mathbb{Z}$, ??

Corollary

If $\phi\colon G \to K$ 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 $|\operatorname{Im}\phi| = [G : \ker\phi]$ by definition. Lagrange's theorem then implies $|\operatorname{Im}\phi|$ divides $|G|$ (and $|K|$). □

Exercise

If G, K are groups, then $\phi\colon G \to K : g \mapsto e_K$ is a homomorphism (called the **trivial homomorphism**). Show $\phi\colon G \to K$ is the trivial homomorphism if and only if $\operatorname{Im}\phi = \{e\}$ (the trivial subgroup).

As a result, if G and K have coprime order, then the only homomorphism $\phi\colon G \to K$ is the trivial homomorphism.

Beginning to prove Lagrange's theorem

Recall

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

Here, the cosets of H are disjoint, so we can divide G into $[G : H]$ sets of size $|H|$.

Does this work in general?

Proposition

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

1. $g^{-1}k \in H$
2. $k \in gH$
3. $gH = kH$
4. $gH \cap kH \neq \varnothing$

Example: $H = hH$ if and only if $h \in H$ (using (3) and (1)).

Proof.

(1) $\implies$ (2): If $g^{-1}k = h \in H$, then $k = gh \in gH$.

(2) $\implies$ (3): Suppose $k = gh$ for some $h \in H$. If $h' \in H$, then $kh' = g(hh') \in gH$ since $hh' \in H$. So $kh \subseteq gH$. Also $g = kh^{-1} \in kH$, so similarly $gH \subseteq kH$.

(3) $\implies$ (4): If $gH = kH$, then $gH \cap kH = gH \neq \varnothing$ (since $g \in gH$).

(4) $\implies$ (1): Suppose $x \in gH \cap kH$. Then $x = gh_1 = kh_2$ for $h_1, h_2 \in H$. So $g^{-1}k = h_1 h_2^{-1} \in H$. □

Partitions

Definition — partition

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

$$\text{(a)} \bigcup_{S\in\mathcal{Q}} S = X \quad \text{and} \quad \text{(b) } S \cap T = \varnothing \text{ for all } S \neq T \in \mathcal{Q}.$$

Equivalently, $\mathcal{Q}$ is a partition if $X = \bigsqcup_{S\in\mathcal{Q}} S$ or every element of X is contained in exactly one element of $\mathcal{Q}$.

We can show cosets partition G:

Corollary

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

Proof.

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

Suppose $S \neq T$ are in G/H. If $S \cap T \neq \varnothing$, then $S = T$ by (3) and (4) of the proposition. So $S \cap T = \varnothing$. □

We can also show cosets have the same size:

Lemma

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

Proof.

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

As a consequence, if H is finite and $g \in G$, then $|gH| = |H|$.

Proof of Lagrange's theorem

Proof (Lagrange's theorem).

If $|H| = \infty$ then $|G| = \infty$.

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

Now suppose $|H|$ and $[G : H]$ are finite. By lemma, $|gH| = |H|$ 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 $|H|$.

So $|G| = [G : H]|H|$. $\square$

Equivalence relations

Definition — relation

A **relation** $\sim$ on a set 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

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

Example

- $=$ on X
- $\equiv_m$ (congruence mod m) on $\mathbb{Z}$
- not $\leq, <, >, \geq$ on $\mathbb{N}$, $\mathbb{R}$, etc.
- isomorphism $\cong$ on the *proper class* of groups

Equivalence classes

Definition — 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

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

1. $x \sim y$
2. $y \in [x]$
3. $[x] = [y]$
4. $[x] \cap [y] \neq \varnothing$

Proof.

(1) $\implies$ (2): By definition.

(2) $\implies$ (3): If $z \in [y]$, then $x \sim y \sim z \implies z \in [x]$, so $[y] \subseteq [x]$. Also $x \sim y \implies y \sim x \implies [x] \subseteq [y]$.

(3) $\implies$ (4): $[x] \cap [y] = [x] \supseteq \{x\} \neq \varnothing$.

(4) $\implies$ (1): If $z \in [x] \cap [y]$, then $x \sim z \sim y \implies x \sim y$. $\square$

Equivalence relations yield partitions:

Corollary

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

Partitions yield equivalence relations:

Corollary

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 $x \sim y \iff S_x = S_y$. $\square$

Let's apply this to cosets:

Proposition

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 $[g] = gH$.

For example, $h \sim e$ if and only if $h \in H$.

7: Normal subgroups

When is a left coset a right coset?

From before:

Proposition

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

1. $g^{-1}k \in H$
2. $k \in gH$
3. $gH = kH$
4. $gH \cap kH \neq \varnothing$

By symmetry:

Proposition

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

1. $k^{-1}g \in H$
2. $k \in Hg$
3. $Hg = Hk$
4. $Hg \cap Hk \neq \varnothing$

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

Lemma

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

Proof.

$g \in Hg = hH$, so $gH = hH$. □

Definition — normal subgroup

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

Notation: $N \trianglelefteq G$.

Conjugation and set multiplication

Definition — conjugate

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

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

Note $gSg^{-1} = \{ghg^{-1} : h \in S\}$. We also get $gN = Ng$ if and only if $gNg^{-1} = N$.

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

Equivalent characterizations of normal subgroups

Proposition

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

1. $N \trianglelefteq G$ ($gN = Ng$ for all $g \in G$)
2. $gNg^{-1} = N$ for all $g \in G$
3. $gNg^{-1} \subseteq N$ for all $g \in G$
4. $G/N = N\backslash G$
5. $G/N \subseteq N\backslash G$
6. $N\backslash G \subseteq G/N$

Proof.

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

Clearly (2) $\implies$ (3).

For (3) $\implies$ (2), suppose $gNg^{-1} \subseteq N$ for all $g \in G$. Given $g \in G$, we know $g^{-1}Ng \subseteq N$, so $N \subseteq gNg^{-1}$. Hence $N = gNg^{-1}$.

Clearly (1) $\implies$ (4) $\implies$ (5) and (6).

For (5) $\implies$ (1), suppose $G/N \subseteq N\backslash G$. If $g \in G$, then $gN = Nh$ for some $h \in G$. By lemma, $gN = Ng$.

(6) $\implies$ (1) is similar. $\square$

Example

- $\langle s\rangle \leq D_{2n}$: we already saw $G/\langle s\rangle = \langle s\rangle\backslash G$. So $\langle s\rangle \trianglelefteq D_{2n}$. We can also check $s^i\langle s\rangle s^{-i} = \langle s\rangle$ and $r\langle s\rangle r^{-1} = \langle s\rangle$ (since $rs^ir^{-1} = s^{-i}$).
- $\langle r\rangle \leq D_{2n}$: $G/\langle r\rangle \neq \langle r\rangle\backslash G$, so $\langle r\rangle$ is not normal. Indeed, $srs^{-1} = s^2r \notin \langle r\rangle$ for $n \geq 3$.
- If G is abelian, then all subgroups are normal.
- If $\phi\colon G \to K$ is a homomorphism, then $\ker\phi$ is normal.

  Previous proof: $G/\ker\phi$ is the set of solution sets to equations $\phi(x) = b$ where $b \in \operatorname{Im}\phi$, which is $\ker\phi\backslash G$.

  Alternative: if $x \in \ker\phi$ and $g \in G$, then we have $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e$, so $gxg^{-1} \in \ker\phi \implies g(\ker\phi)g^{-1} \subseteq \ker\phi$.

Warning: normal subgroups are not transitive

The subgroup relation $\leq$ is transitive: if $H \leq G$ and $K \leq H$, then $K \leq G$. (Usually we just say $K \leq H \leq G \implies K \leq G$.)

The normal subgroup relation $\trianglelefteq$ is not transitive: consider $H = \langle r, s^2 \rangle \leq D_8$. Then $rs^2 = s^{4-2}r = s^2 r \implies rs^2r^{-1} = s^2$. Exercise: check $H \trianglelefteq D_8$. From the homework, H is abelian so $\langle r \rangle \trianglelefteq H$. But $\langle r \rangle \ntrianglelefteq D_8$.

Normalizers

Definition — normalizer

Let $S \subseteq G$. Then $N_G(S) := \{g \in G : gSg^{-1} = S\}$ is called the **normalizer** of S in G.

Lemma

$N_G(S) \leq G$.

Proof.

$eSe = S$, so $e \in N_G(S)$.

If $g, h \in N_G(S)$, then $ghS(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$ so $gh \in N_G(S)$.

If $g \in N_G(S)$, then $g^{-1}Sg = g^{-1}(gSg^{-1})g = eSe = S$, so $g^{-1} \in N_G(S)$. □

Lemma

Suppose $H \leq G$. Then $H \trianglelefteq G$ if and only if $N_G(H) = G$.

Corollary

If $G = \langle S \rangle$ and $H \leq G$, then $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for all $g \in S$.

Proof.

$H \trianglelefteq G$ if and only if $N_G(H) = G$ if and only if $S \subseteq N_G(H)$ (the normalizer is a subgroup of G, so it is equal to G iff it contains the generators of G). □

Warning: it is possible to have $gHg^{-1} \subseteq H$ and $g \notin N_G(H)$.

Lemma

If $|g| < \infty$ and $gHg^{-1} \subseteq H$, then $g \in N_G(H)$.

Proof.

Induction: if $gHg^{-1} \subseteq H$, then $g^i H g^{-i} \subseteq H$ for all $i \geq 0$.

If $|g| = n < \infty$, then $g^{-1}Hg = g^{n-1}Hg^{-(n-1)} \subseteq H$. Hence $H \subseteq gHg^{-1}$, so $gHg^{-1} = H$. $\square$

Corollary

Suppose $G = \langle S \rangle$ is finite and $H \leq G$. If $gHg^{-1} \subseteq H$ for all $g \in S$, then $H \trianglelefteq G$.

Centres

Definition — centre

If G is a group, the **centre** of G is $Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$.

That is, $Z(G)$ is the set of elements in G which commute with all elements in G.

Example

$Z(\mathrm{GL}_n \mathbb{C}) = \{\lambda I_n : \lambda \neq 0\}$.

Proposition

$Z(G) \trianglelefteq G$.

Proof (exercise).

$eh = he$ for all $h \in G$, so $e \in Z(G)$.

If $g, h \in Z(G)$ and $k \in G$, then $ghk = gkh = kgh$ so $gh \in Z(G)$.

If $g \in Z(G)$ and $k \in G$, then $gk = kg \implies k = g^{-1}kg \implies kg^{-1} = g^{-1}k$ so $g^{-1} \in Z(G)$.

Thus $Z(G) \leq G$.

By definition, we clearly have $kZ(G) = Z(G)k$ for all $k \in G$, so $Z(G) \trianglelefteq G$. $\square$

8: Product groups

Getting more groups

Proposition

Suppose $(G_1, \cdot_1)$ and $(G_2, \cdot_2)$ are groups. Then $G_1 \times G_2$ is a group under operation

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot_1 h_1, g_2 \cdot_2 h_2)$$

for $g_i, h_i \in G_i$ where $i = 1, 2$.

Proof (homework).

Since G_1 and G_2 are groups, they are closed under $\cdot_1$ and $\cdot_2$ respectively, so $\cdot$ is clearly a binary operation on $G_1 \times G_2$ by construction. Furthermore, $\cdot_1$ and $\cdot_2$ are associative, so $\cdot$ is clearly associative by construction.

Letting $e_1 = e_{G_1}$ and $e_2 = e_{G_2}$, we see

$$(e_1, e_2) \cdot (g_1, g_2) = (g_1, g_2) = (g_1, g_2) \cdot (e_1, e_2)$$

for all $g_1 \in G_1$ and $g_2 \in G_2$, so (e_1, e_2) is an identity in $G_1 \times G_2$.

For $(g_1, g_2) \in G_1 \times G_2$, we know $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$ and

$$(g_1, g_2) \cdot (g_1^{-1}, g_2^{-1}) = (e_1, e_2) = (g_1^{-1}, g_2^{-1}) \cdot (g_1, g_2)$$

so (g_1, g_2) has an inverse in $G_1 \times G_2$, namely (g_1^{-1}, g_2^{-1}). $\square$

Definition — product group

If G_1, G_2 are groups, the group $G_1 \times G_2$ with the operation from the above proposition is called the **product** of G_1 and G_2.

Example: Klein 4-group

Obviously $|G_1 \times G_2| = |G_1| \cdot |G_2|$, so the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order 4. We call this the **Klein 4-group**.

The group's multiplication table is

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

so all elements have order 2 and thus the group is not cyclic.

The identity is $(0,0)$. In general, $e_{G_1 \times G_2} = (e_{G_1}, e_{G_2})$.

Two subgroups of a product

Proposition

Suppose $G = H \times K$. Let $\tilde{H} = \{(h, e_K) : h \in H\}$ and $\tilde{K} = \{(e_H, k) : k \in K\}$. Then

1. $\tilde{H}, \tilde{K} \leq G$.
2. $H \to \tilde{H} : h \mapsto (h, e)$ and $K \to \tilde{K} : k \mapsto (e, k)$ are isomorphisms.

Proof (homework).

□

So we can think of H and K as subgroups of $H \times K$. Note $H \times K$ can have many other subgroups as well.

Compactly, we can write $\tilde{H} = H \times \{e\} \leq H \times K$ and $\tilde{K} = \{e\} \times K \leq H \times K$.

These subgroups commute.

Lemma

If $h \in \tilde{H}$ and $k \in \tilde{K}$, then $hk = kh$.

Proof (homework).

For clarity, say $\tilde{h} = (h, e) \in \tilde{H}$ and $\tilde{k} = (e, k) \in \tilde{K}$. Then

$$\tilde{h}\tilde{k} = (h, e) \cdot (e, k) = (h, k) = (e, k) \cdot (h, e) = \tilde{k}\tilde{h}.$$

□

Corollary

If $\phi \colon H \times K \to G$ is a homomorphism, then $\phi(h)\phi(k) = \phi(k)\phi(h)$ for all $h \in \tilde{H}$ and $k \in \tilde{K}$.

This is a simple result, but we can actually prove a version equivalent to the converse as well.

Homomorphisms between products

Lemma

If $\alpha\colon H \to G$ and $\beta\colon K \to G$ are homomorphisms such that $\alpha(h)\beta(k) = \beta(k)\alpha(h)$ for all $h \in H$ and $k \in K$, then $\gamma\colon H \times K \to G : (h,k) \mapsto \alpha(h)\beta(k)$ is a homomorphism.

Proof.

For all $x, z \in H$ and $y, w \in K$:

$$\begin{aligned}\gamma((x,y)\cdot(z,w)) &= \gamma((xz,yw))\\ &= \alpha(xz)\beta(yw)\\ &= \alpha(x)\alpha(z)\beta(y)\beta(w)\\ &= \alpha(x)\beta(y)\alpha(z)\beta(w)\\ &= \gamma(x,y)\gamma(z,w).\end{aligned}$$

□

Notation: the homomorphism γ is called $\alpha \cdot \beta$ (not entirely standard).

Corollary

If $\alpha\colon H \to H'$ and $\beta\colon K \to K'$ are homomorphisms, then $\gamma\colon H \times K \to H' \times K'$: $(h,k) \mapsto (\alpha(h), \beta(k))$ is a homomorphism.

Proof.

Define $\tilde{\alpha}\colon H \to H' \times K' : h \mapsto (\alpha(h), e)$ and $\tilde{\beta}\colon K \to H' \times K' : k \mapsto (e, \beta(h))$.

From the homework, $\tilde{\alpha}$ and $\tilde{\beta}$ are homomorphisms, and that $\tilde{\alpha}(x)\tilde{\beta}(y) = \tilde{\beta}(y)\tilde{\alpha(x)}$ for all $x \in H$ and $y \in K$.

Then $\gamma((x,y)) = (\alpha(x), e)\cdot(e, \beta(y)) = \tilde{\alpha}(x)\cdot\tilde{\beta(y)}$ so $\gamma = \tilde{\alpha}\cdot\tilde{\beta}$. □

Notation: the homomorphism γ is called $\alpha \times \beta$ (more standard).

Corollary

If $\alpha\colon H \to H'$ and $\beta\colon K \to K'$ are isomorphisms, then $\alpha \times \beta\colon H \times K \to H' \times K'$ is an isomorphism.

Proof.

$\alpha \times \beta$ has inverse $\alpha^{-1} \times \beta^{-1}$. □

Proposition

$G \to G \times \{e\} : g \mapsto (g, e)$ is an isomorphism.

Proof.

See homework for equivalent proof. □

Groups of small order (revised)

We can use products to complete the list of groups of order p^2.

Proposition

Suppose p is prime and $|G| = p^2$. Then either G is cyclic, or $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Proof (homework). $\square$

Order	Known groups
1	Trivial group
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
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	$\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

How do we know if a group is a product?

Recall:

Proposition

Suppose $G = H \times K$. Let $\tilde{H} = \{(h, e_K) : h \in H\}$ and $\tilde{K} = \{(e_H, k) : k \in K\}$. Then

1. $\tilde{H}, \tilde{K} \leq G$.
2. $H \to \tilde{H} : h \mapsto (h, e)$ and $K \to \tilde{K} : k \mapsto (e, k)$ are isomorphisms.

Corollary: $H \times K \to \tilde{H} \times \tilde{K} : (h, k) \mapsto ((h, e), (e, k))$ is an isomorphism.

Other properties of $\tilde{H}$ and $\tilde{K}$ (homework):

- If $h \in \tilde{H}$ and $k \in \tilde{K}$, then $hk = kh$.
- Every $g \in G$ can be written as $g = \tilde{h}\tilde{k}$ for unique $\tilde{h} \in \tilde{H}$ and $\tilde{k} \in \tilde{K}$.

Unique factorizations

Given $S, T \subseteq G$, let $ST = \{gh : g \in S,\ h \in T\}$.

Lemma

$G = ST$ if and only if every $g \in G$ can be written as $g = hk$ for some $h \in S$ and $k \in T$.

Example: $D_{2n} = \{s^i r^j\} = \langle s \rangle \langle r \rangle$.

Question: if $G = HK$ for $H, K \leq G$, when does $g = hk$ for unique $h \in H$ and $k \in K$? (Uniqueness means that if $g = hk = h'k'$ for $h, h' \in H$ and $k, k' \in K$, then $h = h'$ and $k = k'$.)

Notice if $e \neq g \in H \cap K$, then $g = ge = eg$ so the factorization is not unique. So a necessary condition for unique factorization is that $H \cap K = \{e\}$. This is actually sufficient:

Lemma

Suppose $G = HK$ for $H, K \leq G$ for $H, K \leq G$. Then every element $g \in G$ can be written as $g = hk$ for unique $h \in H$ and $k \in K$ if and only if $H \cap K = \{e\}$.

Proof.

We already proved $H \cap K = \{e\}$ is necessary.

Suppose $H \cap K = \{e\}$. If $g = hk = h'k'$, then $(h')^{-1}h = k'k^{-1} \in H \cap K$. So $(h')^{-1}h = k'k^{-1} = e$ implying $h = h'$ and $k = k'$. $\square$

Internal (direct) products

Definition — internal direct product

G is the **internal direct product** of subgroups $H, K \leq G$ if

1. $HK = G$,
2. $H \cap K = \{e\}$, and
3. $hk = kh$ for all $h \in H$ and $k \in K$.

Example

- $H \times K$ is the internal direct product of $\tilde{H} = H \times \{e\}$ and $\tilde{K} = \{e\} \times K$.
- D_{2n} is not the internal direct product of $\langle s \rangle$ and $\langle r \rangle$ because $sr \neq rs$.

Theorem

Suppose G is the internal direct product of H and K. Then $\phi\colon H \times K \to G : (h, k) \mapsto hk$ is an isomorphism.

Proof.

Let $i_H\colon H \to G : h \mapsto h$ and $i_K\colon K \to G : k \mapsto k$. By part (3) of the definition, $i_H(h)i_K(k) = i_K(k)i_H(h)$ for all $h \in H$ and $k \in K$, so $\phi = i_H \cdot i_K$ is a homomorphism.

By lemma, every element $g \in G$ can be written as $g = hk$ for unique $h \in H$ and $k \in K$. Thus ϕ is a bijection. $\square$

A weaker condition

Lemma

If G is an internal direct product of H and K, then $H, K \trianglelefteq G$.

Proof.

Suppose $g \in G$, so $g = hk$ for $h \in H$ and $k \in K$. Then $kHk^{-1} = \{khk^{-1} : h \in H\} = \{kk^{-1}h : h \in H\} = H$, so $gHg^{-1} = hkHk^{-1}h^{-1} = hHh^{-1} \subseteq H$. Then $H \trianglelefteq G$.

Similar for K. $\square$

Proposition

G is the internal direct product of $H, K \leq G$ if and only if

1. $G = HK$,
2. $H \cap K = \{e\}$, and
3. $H, K \trianglelefteq G$.

Definition — commutator

The **commutator** of $g, h \in G$ is $[g, h] := g \cdot h \cdot g^{-1} \cdot h^{-1}$.

Lemma

If $g, h \in G$, then $[g, h] = e$ if and only if $gh = hg$.

Proof (proposition).

We already saw the forward implication.

If $h \in H$ and $k \in K$, then $[h, k] = (hkh^{-1})k^{-1} \in K$ since $K \trianglelefteq G$. But $[h, k] = h(kh^{-1}k^{-1}) \in H$ since $H \trianglelefteq G$. So $[h, k] \in H \cap K = \{e\}$ which implies $[h, k] = e$. Hence $hk = kh$, which completes the definition of an internal direct product. $\square$

Week 4: Quotients and the Isomorphism Theorems

9: Quotient groups

Left cosets and functions

If $H \leq G$, then G/H is the set of left cosets.

Defining an equivalence relation $\sim_H$ by $g \sim_H k \iff g^{-1}k \in H$, the equivalence class of $g \in G$ is $[g] = gH$.

For example, $\mathbb{Z}/n\mathbb{Z} = \{[a] : 0 \leq a < n\}$. Here, $\mathbb{Z}/n\mathbb{Z}$ is a group with operation $[a] + [b] = [a + b]$.

Can we generalize this by defining a group structure on G/H by $[g] \cdot [h] = [gh]$? (Or, $gH \cdot hH = ghH$ as elements of G/H.) A big problem: this might not be well-defined.

Definition — function

A **relation** R between sets X and Y is a subset of $X \times Y$. Notation: $a\ R\ b$ if $(a, b) \in R$.

A relation R is a **function** from $X \to Y$ if

1. for all $x \in X$, there is $y \in Y$ such that $x\ R\ y$, and
2. for all $x \in X$ and $y, z \in Y$, if $x\ R\ y$ and $x\ R\ z$ then $x = z$.

We can define a relation $\to$ between $G/H \times G/H$ and G/H by $([g], [h]) \to [gh]$ for all $g, h \in G$.

Is this relation a function? For (1), if $x = ([g], [h])$ we can take $y = [gh]$. What about (2)?

Lemma

The relation $\to$ between $G/H \times G/H$ and G/H defined by $([g], [h]) \to [gh]$ is a function if and only if H is normal.
Furthermore, if H is normal, then $ghH = gh \cdot hH$ (the setwise product).

Proof.

In the forward direction, suppose $\to$ is a function.

Suppose $g \in G$ and $h \in H$. Then $([g], [g^{-1}]) \to [e]$. But $[g] = [gh]$, and $([gh], [g^{-1}]) \to [ghg^{-1}]$. Since $\to$ is a function, $[ghg^{-1}] = [e]$.

This means $ghg^{-1} \sim_H e$, or $ghg^{-1} \in H$. This holds for all $g \in G$ and $h \in H$, so $H \trianglelefteq G$.

In the reverse direction, suppose H is normal.

Then $h^{-1}Hh \subseteq H$ so $(h^{-1}Hh) \cdot H \subseteq H$. Since $e \in h^{-1}Hh$, we actually get $(h^{-1}Hh) \cdot H = H$. Hence $gH \cdot hH = gh(h^{-1}Hh) \cdot H = ghH$.

Finally, say $(S, T) \to R$ and $(S, T) \to R'$ for $S, T, R, R' \in G/H$. Then $R = S \cdot T = R'$. So $\to$ is a function. $\square$

The converse of the 'furthermore' actually holds as well, giving two new characterizations of a subgroup being normal.

Quotient groups

Theorem

Let $N \trianglelefteq G$. Then the setwise product $gN \cdot hN = ghN$ makes G/N into a group. Furthermore, the function $q\colon G \to G/N : g \mapsto gN$ is a surjective homomorphism with $\ker q = N$.

G/N is called the **quotient** of G by N, or a **quotient group**.

Elements of G/N can be written as gN or $[g]$ or $\overline{g}$.

The group operation can be stated as $gN \cdot hN = ghN$ or $[g] \cdot [h] = [gh]$ or $\overline{g} \cdot \overline{h} = \overline{gh}$.

q is called the **quotient map** or **quotient homomorphism**.

Proof.

Let $[g], [h], [k] \in G/N$.

Then
$$([g] \cdot [h]) \cdot [k] = [gh] \cdot [k] = [ghk] = [g] \cdot [hk] = [g] \cdot ([h] \cdot [k])$$
so $\cdot$ is associative. Next,

$$[e] \cdot [g] = [eg] = [g] = [ge] = [g] \cdot [e]$$

so $[e] = N$ is an identity. Finally,

$$[g] \cdot [g^{-1}] = [gg^{-1}] = [e] = [g^{-1}g] = [g^{-1}] \cdot [g]$$

so g has inverse $[g^{-1}]$.

Note q is clearly surjective, and $q(gh) = [gh] = [g] \cdot [h] = q(g)q(h)$. Also, $q(g) = [g] = [e]$ if and only if $g \in N$, so $\ker q = N$. $\square$

Normal subgroups are kernels

Previously, we proved that if $\phi\colon G \to K$ is a homomorphism then $\ker\phi \trianglelefteq G$.

Corollary

Let $N \trianglelefteq G$. Then there is a group K and homomorphism $\phi\colon G \to K$ such that $N = \ker\phi$.

Proof.

Take $K = G/N$ and $q\colon G \to G/N$ the quotient homomorphism. Then $\ker q = N$. $\square$

Examples of quotient groups

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

We can now define this using the theorem instead of relying on the pre-existing definition.

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

The cosets are $\langle s\rangle = \{s^i : 0 \le i < n\}$ and $\langle s\rangle r = \{s^i r : 0 \le i < n\}$.

Multiplication table:

	$\langle s\rangle$	$\langle s\rangle r$
$\langle s\rangle$	$\langle s\rangle$	$\langle s\rangle r$
$\langle s\rangle r$	$\langle s\rangle r$	$\langle s\rangle$

so $D_{2n}/\langle s\rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Example: N not normal

Consider $\langle r\rangle$, which has left cosets $s^i\langle r\rangle = \{s^i, s^i r\}$ for $0 \le i < n$. But $\langle r\rangle \cdot s\langle r\rangle = \{s, sr, s^{-1}r, s^{-1}\}$ which is not a left coset of $\langle r\rangle$.

Also, $es = s$ is in a different coset from $rs = s^{-1}r$, so $[g]\cdot[h] = [gh]$ is not well-defined here.

Example: $D_{2n}/Z(D_{2n})$

Homework.

Example: $\mathrm{GL}_n(\mathbb{K})/Z(\mathrm{GL}_n(\mathbb{K}))$

Recall $Z(\mathrm{GL}_n(\mathbb{K})) = \{\lambda 1 : \lambda \neq 0\}$.

If M is invertible, then $[M] = \{\lambda M : \lambda \neq 0\}$.

$[M]\cdot[N] = \{\lambda_1\lambda_2 MN : \lambda_1, \lambda_2 \neq 0\} = [MN]$.

We think of $\mathrm{GL}_n(\mathbb{K})$ as the group of invertible linear transformations on $\mathbb{K}^n$ (acting on vectors).

We can then think of $\mathrm{GL}_n(\mathbb{K})/Z(\mathrm{GL}_n(\mathbb{K}))$ as the invertible transformations of lines through the origin in $\mathbb{K}^n$.

$\mathrm{GL}_n(\mathbb{K})/Z(\mathrm{GL}_n(\mathbb{K}))$ is called the **projective general linear group**, and is denoted by $\mathrm{PGL}_n(\mathbb{K})$.

In general, we can look at:

- $G/Z(G)$ for any group G
- $G/\ker\phi$ for any homomorphism $\phi\colon G \to K$

- G/N for any group G and normal subgroup $N \trianglelefteq G$

How do we find the group structure on G/N? We will build up techniques for approaching this problem.

10: First isomorphism and correspondence theorems

Homomorphisms from quotients

Suppose $N \trianglelefteq G$. What are the homomorphisms $\psi\colon G/N \to K$?

$$\begin{tikzcd} G \arrow[rr, "\psi \circ q"] \arrow[dr, "q"'] & & K \\ & G/N \arrow[ur, "\psi"'] & \end{tikzcd}$$

Every such ψ gives a homomorphism $\psi \circ q\colon G \to K$ (called the **lift** or **pullback** of ψ). What homomorphisms $G \to K$ do we get?

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "q"'] & & K \\ & G/N \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

Given ϕ, when can we fill in ψ so that the diagram **commutes** (the paths are equivalent)?

Theorem — Universal property of quotients

Suppose $\phi\colon G \to K$ is a homomorphism and $N \trianglelefteq G$. Let $q\colon G \to G/N$ be the quotient homomorphism. Then there is a homomorphism $\psi\colon G/N \to K$ such that $\psi \circ q = \phi$ if and only if $N \subseteq \ker\phi$. Furthermore, if ψ exists then it is unique.

In other words, we can fill in ψ if and only if $N \subseteq \ker\phi$.

Definition — set of morphisms

If G, K are groups, let $\mathrm{Hom}(G, K)$ be the set of morphisms $G \to K$.

Corollary

For any groups G, K and $N \trianglelefteq G$, the function

$$q^*\colon \mathrm{Hom}(G/N, K) \to \{\phi \in \mathrm{Hom}(G, K) : N \subseteq \ker\phi\} : \psi \mapsto \psi \circ q$$

is a bijection.

Comparison to universal property of products

From before (but without the name):

Theorem — Universal property of products

Let $\alpha\colon H \to G$ and $\beta\colon K \to G$ be homomorphisms, and let $i_H\colon H \to H \times K$ and $i_K\colon K \to H \times K$ be the inclusions of H and K in $H \times K$. Then there is a homomorphism $\phi\colon H \times K \to G$ such that $\phi \circ i_H = \alpha$ and $\phi \circ i_K = \beta$ if and only if $\alpha(h)\beta(k) = \beta(k)\alpha(h)$ for all $h \in H$ and $k \in K$.

$$\begin{tikzcd}
H \arrow[dr, "i_H"'] \arrow[drr, "\alpha"] & & \\
& H \times K \arrow[r, dashed] & G \\
K \arrow[ur, "i_K"] \arrow[urr, "\beta"'] & &
\end{tikzcd}$$

Corollary

There is a bijection between $\mathrm{Hom}(H \times K, G)$ and $\{(\alpha, \beta) \in \mathrm{Hom}(H, G) \times \mathrm{Hom}(K, G) : \alpha(h)\beta(k) = \beta(k)\alpha(h) \text{ for all } h \in H \text{ and } k \in K\}$.

We need some more machinery to justify why these are "universal properties", but for now we can think of them as setting up important bijections.

Proving the universal property of quotients

Lemma

If $\alpha\colon G \to H$ is surjective and $\psi_1, \psi_2 : H \to K$ are such that $\psi_1 \circ \alpha = \psi_2 \circ \alpha$, then $\psi_1 = \psi_2$.

Proof.

If $h \in H$, then there is $g \in G$ with $\alpha(g) = h$. So $\psi_1(h) = \psi_1(\alpha(g)) = \psi_2(\alpha(g)) = \psi_2(h)$. $\square$

Restatement for reference:

Theorem — Universal property of quotients

Suppose $\phi\colon G \to K$ is a homomorphism and $N \trianglelefteq G$. Let $q\colon G \to G/N$ be the quotient homomorphism. Then there is a homomorphism $\psi\colon G/N \to K$ such that $\psi \circ q = \phi$ if and only if $N \subseteq \ker\phi$. Furthermore, if ψ exists then it is unique.

Proof.

If ψ exists and $n \in N$, then $\phi(n) = \psi(q(n)) = \psi(e) = e$ so $N \subseteq \ker\phi$.

Suppose $N \subseteq \ker\phi$. Define $\psi\colon G/N \to K : [g] \mapsto \phi(g)$. To show ψ is well-defined, note that if $[g] = [h]$ then $g^{-1}h \in N \subseteq \ker\phi$, so $\phi(g^{-1})\phi(h) = \phi(g^{-1}h) = e$, so $\phi(g) = \phi(h)$.

Clearly $\psi \circ q(g) = \psi([g]) = \phi(g)$ for all $g \in G$, so $\psi \circ q = \phi$.

If $[g], [h] \in G/N$, then

$$\psi([g] \cdot [h]) = \psi([gh]) = \phi(gh) = \phi(g)\phi(h) = \psi([g])\psi([h])$$

so ψ is a homomorphism.

If $\psi'\colon G/N \to K$ is another homomorphism with $\psi' \circ q = \phi$, then $\psi' \circ q = \psi \circ q$ which implies $\psi' = \psi$ by the lemma (q is surjective). So uniqueness holds. $\square$

Note $\phi(gN) = \phi(g)\phi(N) = \phi(g)\{e\} = \{\phi(g)\}$. So if $S \in G/N$, then $\phi(S) = \{b\}$, a singleton set. Thus an equivalent way of defining ψ is by $\psi(S) = b$ for $b \in K$ such that $\phi(S) = \{b\}$.

The first isomorphism theorem

Recall: if $\phi\colon G \to K$ is a homomorphism then $[G : \ker\phi] = |\operatorname{Im}\phi|$.

Proof: there is a bijection $\psi\colon G/\ker\phi \to \operatorname{Im}\phi$ defined by $\psi(S) = b$ where $b \in K$ is such that $\phi(S) = \{b\}$.

This looks like what we just did!

Now we also know $G/\ker\phi$ is a group, so $|G/\ker\phi| = [G : \ker\phi] = |\operatorname{Im}\phi|$. Maybe this bijection is an isomorphism?

Theorem — First isomorphism theorem

Suppose that $\phi\colon G \to K$ is a homomorphism. Then there is an isomorphism $\psi\colon G/\ker\phi \to \operatorname{Im}\phi$ such that $\phi = \psi \circ q$, where $q\colon G \to G/\ker\phi$ is the quotient homomorphism.

Proof.

First, $\ker\phi \subseteq \ker\phi$, so by the universal property there is a homomorphism $\psi\colon G/\ker\phi \to K$ with $\psi \circ q = \phi$.

Next $\psi([g]) = \phi(g)$ so clearly $\operatorname{Im}\psi = \operatorname{Im}\phi$. Thus we can regard ψ as a surjective homomorphism $G/\ker\phi \to \operatorname{Im}\phi$.

To see ψ is a bijection, note ψ agrees with the function $G/\ker\phi \to \operatorname{Im}\phi$ defined previous to the theorem.

Alternatively, notice if $\psi([g]) = e$, then $\phi(g) = e$, so $g \in \ker\phi$ and thus $[g] = [e]$. Then ψ is injective by proposition. □

Example

The first isomorphism theorem is usually the best way to determine G/N:

- Recall $\mathrm{SL}_n\,\mathbb{K} \trianglelefteq \mathrm{GL}_n\,\mathbb{K}$ is defined as the kernel of the determinant homomorphism $\det\colon \mathrm{GL}_n\,\mathbb{K} \to \mathbb{K}^\times$. The image is $\operatorname{Im}\det = \mathbb{K}^\times$.

  By first isomorphism theorem, $\mathrm{GL}_n\,\mathbb{K}/\mathrm{SL}_n\,\mathbb{K} \cong \mathbb{K}^\times$. (Here, we only use the existence of ψ.)

- Consider $\mathbb{Z} \trianglelefteq \mathbb{R}^+$. What is $\mathbb{R}/\mathbb{Z}$?

  We have a homomorphism $\exp\colon \mathbb{R} \to \mathbb{C}^\times : x \mapsto e^{2\pi i x}$ and we know $e^{2\pi i x} = 1$ if and only if $x \in \mathbb{Z}$ (so $\ker\exp = \mathbb{Z}$). Then $\operatorname{Im}\exp = \{a \in \mathbb{C} : |a| = 1\} =: S^1$ (the **circle group**).

  So $\mathbb{R}/\mathbb{Z} \cong S^1$.

In general, to find G/N we can try finding a group K and homomorphism $\phi\colon G \to K$ where $\ker\phi = N$. Then the first isomorphism theorem yields $G/N \cong \operatorname{Im}\phi$.

There are several more examples on the homework.

Sometimes, we can also turn this around and use the first isomorphism theorem to find $\operatorname{Im}\phi$.

Images and pullbacks

We want to understand subgroups of G/N using $q\colon G \to G/N$.

Recall: if $f\colon X \to Y$ is a function and $S \subseteq X$ and $T \subseteq Y$, then

- $f(S) := \{f(x) : x \in S\}$ and
- $f^{-1}(T) := \{x \in X : f(x) \in T\}$.

From week 2:

Proposition

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

The “pushforward” or image of a subgroup is a subgroup.

Proposition

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

The pullback of a subgroup is a subgroup.

Subgroup correspondence for isomorphisms

If $f\colon X \to Y$ is a bijection, then $f^{-1}(f(S)) = S$ and $f(f^{-1}(T)) = T$. Thus if $\phi\colon G \to H$ is an isomorphism, we get a bijection

$$\begin{array}{c} \text{Subgroups} \\ \text{of } G \end{array} \; \begin{array}{c} \xrightarrow{\quad K \mapsto \phi(K) \quad} \\ \xleftarrow[\quad \phi^{-1}(K') \leftarrow\!\shortmid K' \quad]{} \end{array} \; \begin{array}{c} \text{Subgroups} \\ \text{of } H \end{array}$$

Furthermore:

- $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$
- $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$
- K is normal $\iff \phi(K)$ is normal
- $\phi(\langle S \rangle) = \langle \phi(S) \rangle$
- $[G : K] = [H : \phi(K)]$

Set operation identities

Some identities for bijections don't hold for general functions.

Always hold	Don't always hold
$A \subseteq B \implies f(A) \subseteq f(B)$	$f(A \cap B) = f(A) \cap f(B)$
$A \subseteq B \implies f^{-1}(A) \subseteq f^{-1}(B)$	$f^{-1}(f(A)) = A$
$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$	$f(f^{-1}(B)) = B$
$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$	
$f(A \cup B) = f(A) \cup f(B)$	

The left column holds for all functions; the right column holds for bijections but not for general functions.

One consequence of these identities is that order is preserved:

Lemma

If $\phi\colon G \to H$ is a homomorphism, then:

1. If $K_1 \leq K_2 \leq G$, then $f(K_1) \leq f(K_2)$.
2. If $K_1 \leq K_2 \leq H$, then $f^{-1}(K_1) \leq f^{-1}(K_2)$.

Note we can't say that $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$ since $\phi^{-1}(\phi(K)) \neq K$ in general.

Another consequence is that pullbacks preserve intersection:

Lemma

If $\phi\colon G \to H$ is a homomorphism and $K_1, K_2 \leq H$, then $\phi^{-1}(K_1 \cap K_2) = \phi^{-1}(K_1) \cap \phi^{-1}(K_2)$.

Set operation identities for surjections

If we suppose $f\colon X \to Y$ is surjective, the table changes:

Always hold	Don't always hold
$A \subseteq B \implies f(A) \subseteq f(B)$	$f(A \cap B) = f(A) \cap f(B)$
$A \subseteq B \implies f^{-1}(A) \subseteq f^{-1}(B)$	$f^{-1}(f(A)) = A$
$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$	$\cancel{f(f^{-1}(B)) = B}$
$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$	
$f(A \cup B) = f(A) \cup f(B)$	
$f(f^{-1}(B)) = B$	

Lemma

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

Definition — set of subgroups

If G is a group, let $\mathrm{Sub}(G)$ denote the set of subgroups of G.

If $\phi\colon G \to H$ is a homomorphism, we get the induced functions $\phi\colon \mathrm{Sub}(G) \to \mathrm{Sub}(H)$ and $\phi^{-1}\colon \mathrm{Sub}(H) \to \mathrm{Sub}(G)$.

If ϕ is surjective, the lemma shows ϕ is a left inverse to ϕ^{-1}. So $\phi^{-1}\colon \mathrm{Sub}(H) \to \mathrm{Sub}(G)$ is injective (from homework 1).

Question: what's the image of ϕ^{-1} in $\mathrm{Sub}(G)$?

The set of pullbacks in $\mathrm{Sub}(G)$

Lemma

Let $\phi\colon G \to H$ be a homomorphism. Then:
1. If $K \leq H$, then $\ker\phi \leq \phi^{-1}(K)$.
2. If $\ker\phi \leq K \leq G$, then $\phi^{-1}(\phi(K)) = K$.

Proof.

1. $\ker\phi = \phi^{-1}(\{e\}) \subseteq \phi(H)$.
2. $K \leq \phi^{-1}(\phi(K))$ is easy. Suppose $y \in \phi^{-1}(\phi(K))$. Then $\phi(y) \in \phi(K)$, so $\phi(y) = \phi(k)$ for some $k \in K$. Since $\phi(k^{-1}y) = e$, we get $k^{-1}y \in \ker\phi \subseteq K \implies y \in K$. We conclude that $\phi^{-1}(\phi(K)) \subseteq K$.

□

Conclusion: $K = \phi^{-1}(K') \iff \ker\phi \leq K$ (K is a pullback iff K contains the kernel).

Theorem — Correspondence theorem

Let $\phi\colon G \to H$ be a surjective homomorphism. Then there is a bijection

$$\begin{array}{c}\text{Subgroups}\\ K \text{ of } G \text{ with}\\ \ker\phi \leq K\end{array} \quad \begin{array}{c} \xrightarrow{\quad K \mapsto \phi(K) \quad} \\ \xleftarrow[\quad \phi^{-1}(K') \leftarrow\!\shortmid K' \quad]{} \end{array} \quad \begin{array}{c}\text{Subgroups}\\ K' \text{ of } H\end{array}$$

Furthermore, if $\ker\phi \leq K, K_1, K_2 \leq G$ then
1. $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$,
2. $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$, and
3. K is normal $\iff \phi(K)$ is normal.

Proof.

Since ϕ is surjective, $\phi(\phi^{-1}(K')) = K'$ for all $K' \leq H$. Conversely, if $\ker\phi \leq K \leq G$ then $\phi^{-1}(\phi(K)) = K$. So ϕ and ϕ^{-1} are inverses on the specified sets.

1. Follows from the fact that ϕ and ϕ^{-1} are inverses and preserve $\leq$.
2. By lemma, $\phi^{-1}(\phi(K_1) \cap \phi(K_2)) = \phi^{-1}(\phi(K_1)) \cap \phi^{-1}(\phi(K_2)) = K_1 \cap K_2$. Applying ϕ to both sides, we see also $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$.
3. (Homework.)

□

Correspondence theorem for quotient groups

If $N \trianglelefteq G$, then $q\colon G \to G/N$ is a surjection.

Theorem — Correspondence theorem for quotient groups

Let $N \trianglelefteq G$. Then there is a bijection

$$\begin{array}{c} \text{Subgroups} \\ N \le K \le G \end{array} \underset{q^{-1}(K') \leftarrow\!\shortmid K'}{\overset{K \mapsto q(K)}{\rightleftarrows}} \begin{array}{c} \text{Subgroups} \\ K' \text{ of } G/N \end{array}$$

Furthermore, if $N \le K, K_1, K_2 \le G$ then

1. $K_1 \le K_2 \iff q(K_1) \le q(K_2)$,
2. $q(K_1 \cap K_2) = q(K_1) \cap q(K_2)$, and
3. K is normal $\iff q(K)$ is normal.

This seems like a specialization of the correspondence theorem, but they are actually equivalent (with some work).

Recall the first isomorphism theorem tells us that if $\phi\colon G \to H$ is a surjective homomorphism, then $G/\ker\phi \cong H$. So there is a bijection between $\mathrm{Sub}(H)$ and $\mathrm{Sub}(G/\ker\phi)$.

As an exercise, check that (first isomorphism theorem) + (subgroup correspondence for isomorphisms) + (correspondence theorem for quotient groups) implies (correspondence theorem for surjective homomorphisms).

Identifying $q(K)$

Suppose $N \trianglelefteq G$ and $N \leq K \leq G$. Let $q_G \colon G \to G/N$ be the quotient map. Since $N \trianglelefteq K$, we also have the quotient map $q_K \colon K \to K/N$.

$$\begin{tikzcd} K \arrow[r, "i_K"] \arrow[d, "q_K"'] \arrow[dr, "q_G \circ i"] & G \arrow[d, "q_G"] \\ K/N \arrow[r, "kN \mapsto kN"'] & G/N \end{tikzcd}$$

Since $\ker q_G \circ i = N$, the first isomorphism theorem tells us there is an isomorphism $\psi \colon K/N \to \operatorname{Im} q \circ i_K = q(K)$ such that $\psi \circ q_K = q_G \circ i$.

In other words, if $k \in K$ then $\psi(kN) = q(k) = kN$.

Proposition

Suppose $N \trianglelefteq G$ and $N \leq K \leq G$. Let $q \colon G \to G/N$ be the quotient map. Then the function $K/N \to q(K) \leq G/N \colon kN \mapsto kN$ is an isomorphism.

Because of this isomorphism, we use the following notation:

Definition — subgroup $q(K)$

If $N \trianglelefteq G$ and $N \leq K \leq G$, then the subgroup $q(K)$ corresponding to K in G/N is denoted by K/N.

Example

- Let $G = D_{2n}$ and $N = \langle s \rangle$ where s is the rotation generator.

  Subgroups of D_{2n} containing N correspond to subgroups of $D_{2n}/N = \mathbb{Z}/2\mathbb{Z}$. $\mathbb{Z}/2\mathbb{Z}$ only has two subgroups, itself and $\{e\}$. So there are only two subgroups of D_{2n} containing N.

- $\mathrm{GL}_n \mathbb{K} / \mathrm{SL}_n \mathbb{K} \cong \mathbb{K}^\times$, so subgroups of $\mathrm{GL}_n \mathbb{K}$ containing $\mathrm{SL}_n \mathbb{K}$ correspond to subgroups of $\mathbb{K}^\times$ (of which there can be many).

11: Second and third isomorphism theorems

Third isomorphism theorem

What about quotients of quotients?

Suppose $N \trianglelefteq G$ and $N \leq K \leq G$.

From the correspondence theorem (homework), $K \trianglelefteq G$ if and only if $K/N \trianglelefteq G/N$. Then suppose $K/N \trianglelefteq G/N$. What is $(G/N)/(K/N)$?

Theorem — Third isomorphism theorem (informal version)

$(G/N)/(K/N) \cong G/K$.

Example

Suppose $n \mid m$, so $m\mathbb{Z} \leq n\mathbb{Z}$ (and both are normal).

Then $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. For example, $(\mathbb{Z}/20\mathbb{Z})/(5\mathbb{Z}/20\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$.

Theorem — Third isomorphism theorem

Let $N \trianglelefteq G$ and $N \leq K \trianglelefteq G$. Let
- q_1 be the quotient map $G \to G/N$,
- q_2 be the quotient map $G/N \to (G/N)/(K/N)$, and
- q_3 be the quotient map $G \to G/K$.

Then there is an isomorphism $\psi\colon G/K \to (G/N)/(K/N)$ such that $\psi \circ q_3 = q_2 \circ q_1$.

$$\begin{tikzcd} G \arrow[r, "q_1"] \arrow[d, "q_3"'] & G/N \arrow[d, "q_2"] \\ G/K \arrow[r, "\psi"'] & (G/N)/(K/N) \end{tikzcd}$$

Proof.

Note that $\ker q_2 \circ q_1 = (q_2 \circ q_1)^{-1}(\{e\}) = q_1^{-1}(q_2^{-1}(\{e\})) = q_1^{-1}(K/N) = K$.

Since q_2 and q_1 are surjective, $\operatorname{Im} q_2 \circ q_1 = (G/N)/(K/N)$.

By the first isomorphism theorem, there is an isomorphism $\psi\colon G/K \to (G/N)/(K/N)$ such that $\psi \circ q_3 = q_2 \circ q_1$. $\square$

What if K isn't normal?

Then G/K isn't a group, and neither is $(G/N)/(K/N)$.

However, we can still talk about $[G : K]$ and $[G/N : K/N]$.

Proposition

If $N \trianglelefteq G$ and $N \leq K \leq G$, then $[G : K] = [G/N : K/N]$.

In fact, this doesn't even need quotient spaces. This holds for surjective homomorphisms.

Proposition

Let $\phi\colon G \to H$ be a surjective homomorphism and suppose $\ker \phi \leq K \leq G$. Then $[G : K] = [H : \phi(K)]$.

These are equivalent by the first isomorphism theorem.

Proof.

Define a function $f\colon G/K \to H/\phi(K) : gK \mapsto \phi(g)\phi(K)$.

Well-defined: if $gK = hK$, then $h^{-1}g \in K \implies \phi(h)^{-1}\phi(g) = \phi(h^{-1}g) \in \phi(K)$. So $\phi(g)\phi(K) = \phi(h)\phi(K)$.

Since ϕ is surjective, f is surjective.

Suppose $f(gK) = f(hK)$ so $\phi(g)\phi(K) = \phi(h)\phi(K)$. Then $\phi(h^{-1}g) = \phi(h)^{-1}\phi(g) \in \phi(K)$ which shows $h^{-1}g \in \phi^{-1}(\phi(K)) = K$ by the correspondence theorem. So $gK = hK$ and f is injective.

Then f is a bijection, so the indices must be equal. $\square$

Revisiting products

Recall this lemma:

Lemma

Suppose $G = HK$ for $H, K \leq G$ for $H, K \leq G$. Then every element $g \in G$ can be written as $g = hk$ for unique $h \in H$ and $k \in K$ if and only if $H \cap K = \{e\}$.

Which motivated this definition:

Definition — internal direct product

G is the **internal direct product** of subgroups $H, K \leq G$ if

1. $HK = G$,
2. $H \cap K = \{e\}$, and
3. $hk = kh$ for all $h \in H$ and $k \in K$.

But the proof of the lemma did not use the fact that $G = HK$, so we can generalize it.

Lemma

Suppose $H, K \leq G$. Then every element of HK can be written as hk for unique $h \in H$ and $k \in K$ if and only if $H \cap K = \{e\}$.

If $H \cap K = \{e\}$, then $|HK| = |H| \cdot |K|$.

What if $H \cap K \neq \{e\}$? Here, $HK = \bigcup_{h \in H} hK$, a union of cosets of K. Let $X = \{hK : h \in H\} \subseteq G/K$. Then X is a partition of HK, so $|HK| = |X| \cdot |K|$. But how large is X?

Lemma

Let $H, K \leq G$. If $h_1, h_2 \in H$, then $h_1 K = h_2 K$ if and only if $h_1(H \cap K) = h_2(H \cap K)$.

Proof.

$h_1 K = h_2 K \iff h_1^{-1} h_2 \in K \iff h_1^{-1} h_2 \in H \cap K$. But $h_1^{-1} h_2 \in H \cap K$ if and only if $h_1(H \cap K) = h_2(H \cap K)$. $\square$

Rephrasing, consider the equivalence relations $\sim_K$ on G and $\sim_{H \cap K}$ on H: if $h_1, h_2\, inH$, then $h_1 \sim_K h_2 \iff h_1 \sim_{H \cap K} h_2$.

Corollary

$H/(H\cap K) \to X\colon h(H\cap K) \to hK$ is a bijection.

Proof.

By the lemma, this is well-defined and injective. Surjectivity is obvious. □

Now we see $|X| = [H : H \cap K]$, so $|HK| = [H : H \cap K]|K|$. Lagrange's theorem yields $[H : H \cap K] \cdot |H \cap K| = |H|$, so we have:

Proposition

If $H, K \leq G$, then $|HK||H \cap K| = |H||K|$.

If H and K are finite, another way to think of this formula is $[H : H \cap K] = |X| = \frac{|HK|}{|K|}$. Is the fraction an index as well? Maybe–HK is not necessarily a group.

Proposition

Let $H, K \leq G$. Then $HK \leq G \iff HK = KH \iff KH \subseteq HK$.

Proof.

If $HK \leq G$ and $h \in H$ and $k \in K$, then $h, k \in HK$ so $kh \in HK$. Also, $k^{-1}h^{-1} \in HK$, so $k^{-1}h^{-1} = h_0k_0$. Hence $hk = (k^{-1}h^{-1})^{-1} = k_0^{-1}h_0^{-1} \in KH$. So $KH \subseteq HK$ and $HK \subseteq KH$, hence $HK = KH$.

Now suppose $KH \subseteq HK$, we need to show $HK \leq G$. We always have $e \in HK$. If $x, y \in HK$, then $x = h_0k_0$ and $y = h_1k_1$ for some $h_0, h_1 \in H$ and $k_0, k_1 \in K$. Since $KH \subseteq HK$, $k_0^{-1}h_0^{-1}h_1 = h_2k_2$ for some $h_2 \in H$ and $k_2 \in K$. So $x^{-1}y = k_0^{-1}h_0^{-1}h_1k_1 = h_2k_2k_1 \in HK$. □

Corollary: if $KH \subseteq HK$, then $[H : H \cap K] = [HK : K]$ (exercise: even for infinite HK or K).

When is $KH \subseteq HK$?

A sufficient condition is that for all $h \in H$, there is $h' \in H$ such that $Kh = h'K$. Recall that if $Kh = h'K$, then $h'K = Kh$. So we can rephrase this condition as $hKh^{-1} = K$ for all $h \in H$, or $H \subseteq N_G(K)$.

Corollary

If $H \subseteq N_G(K)$, then $HK \leq G$, and hence $[H : H \cap K] = [HK : K]$.

What else does $H \subseteq N_G(K)$ imply?

We know $hKh^{-1} = K$ and $kKk^{-1} = K$, so $H, K \subseteq N_{HK}(K) \implies N_{HK}(K) = HK \implies K \trianglelefteq HK$.

If $k \in H \cap K$ and $h \in H$, then $hkh^{-1} \in H \cap K$. So $H \cap K \trianglelefteq H$.

Second isomorphism theorem

Theorem — Second isomorphism theorem

Suppose $H \subseteq N_G(K)$. Then $HK \leq G$, $K \trianglelefteq HK$, and $H \cap K \trianglelefteq H$. Furthermore, if $i_H : H \to HK$ is the inclusion and $q_1 : H \to H/(H \cap K)$ and $q_2 : HK \to HK/K$ are the quotient maps, then there is an isomorphism $\psi : H/(H \cap K) \to HK/K$ such that $\psi \circ q_1 = q_2 \circ i_H$.

$$\begin{tikzcd} H \arrow[r, "i_H"] \arrow[d, "q_1"'] & HK \arrow[d, "q_2"] \\ H/H \cap K \arrow[r, "\psi"'] & HK/K \end{tikzcd}$$

Proof.

We've already shown $HK \leq G$, $K \trianglelefteq HK$, and $H \cap K \trianglelefteq H$.

If $h \in H$ and $k \in K$, then $hkK = hK$. So $HK/K = \{gK : g \in HK\} = \{hK : h \in H\}$. Hence $\operatorname{Im} q_2 \circ i_H = \{hK : h \in H\} = HK/K$.

Next, $\ker q_2 \circ i_H = i_H^{-1}(q_2^{-1}(\{e\})) = i_H^{-1}(K) = H \cap K$.

By the first isomorphism theorem, there is an isomorphism ψ as desired. $\square$

Example: $\mathrm{PGL}_n \mathbb{C}$

Recall $\mathrm{PGL}_n \mathbb{C} = \mathrm{GL}_n \mathbb{C}/Z(\mathrm{GL}_n \mathbb{C})$.

Let $K = Z(\mathrm{GL}_n \mathbb{C}) = \{\lambda 1 : \lambda \neq 0\}$.

Since $K \trianglelefteq \mathrm{GL}_n \mathbb{C}$, $N_{\mathrm{GL}_n \mathbb{C}}(K) = \mathrm{GL}_n \mathbb{C}$.

Take $H = \mathrm{SL}_n \mathbb{C} = \{M \in \mathrm{GL}_n \mathbb{C} : \det M = 1\} \trianglelefteq \mathrm{GL}_n \mathbb{C} = N_{\mathrm{GL}_n \mathbb{C}}(K)$, so $HK \leq \mathrm{GL}_n \mathbb{C}$ by the second isomorphism theorem.

Suppose $M \in \mathrm{GL}_n \mathbb{C}$ and let $\lambda = \det M$. Then $\det \lambda^{-1/n} M = \lambda^{-1} \det M = 1$, so $\lambda^{-1/n} M \in H$ (for any choice of $\lambda^{-1/n}$).

We conclude $\mathrm{GL}_n \mathbb{C} = HK$.

Now define $C_n := H \cap K = \{\lambda 1 : \lambda^n = 1\} = \{e^{2\pi i k/n} : k = 0, \dots, n-1\}$. (Note $C_n \cong \mathbb{Z}/n\mathbb{Z}$.)

By the second isomorphism theorem, $\mathrm{PGL}_n \mathbb{C} \cong \mathrm{SL}_n \mathbb{C}/C_n$.

Week 5: Group Actions

12: Group actions and Cayley's theorem

Group actions

Example

Permutations S_n of $\{1, \ldots, n\}$ form a group.

This means we can multiply permutations together: e.g. $(12)(34)(24) = (1234)$.

But we can also plug in numbers from $\{1, \ldots, n\}$: e.g. $((12)(34))(3) = 4$.

We say that S_n **acts** on $\{1, \ldots, n\}$.

Example

Similarly, for $\mathrm{GL}_n \mathbb{C}$, we can do more than multiply matrices: we can also multiply matrices and vectors.

Given $A \in \mathrm{GL}_n \mathbb{C}$ and $v \in \mathbb{C}^n$, we get $Av \in \mathbb{C}^n$.

We say that $\mathrm{GL}_n \mathbb{C}$ **acts** on $\mathbb{C}^n$.

Group actions can reveal a lot about a group.

Definition — (left) action

Let G be a group. A **(left) action** of G on a set X is a function $\cdot : G \times X \to X$ such that

1. $e \cdot x = x$ for all $x \in X$, and
2. $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$.

Example

- S_n acts on $\{1, \ldots, n\}$ for $n \geq 1$ (proof: below).
- $\mathrm{GL}_n \mathbb{K}$ acts on $\mathbb{K}^n$ (proof: exercise).
- If X is any set and G is any group, we can define an action of G on x by $g \cdot x = x$ for all $g \in G$ and $x \in X$. This is the **trivial action** of G on X. Proof: (1) clear; (2) $g \cdot (h \cdot x) = g \cdot x = x = (gh) \cdot x$.

Proposition

Let X be a set. The group S_X (of invertible functions $X \to X$ under composition $\circ$) acts on X via $f \cdot x = f(x)$.

Proof.

The identity 1 in S_X is the identity function, so $1 \cdot x = 1(x) = x$. If $f, g \in S_X$, then $(f \circ g)(x) = f(g(x)) = f \cdot (g \cdot x)$. $\square$

Note: usually we use notation $f(x)$ rather than $f \cdot x$. Also, recall $S_n = S_{\{1,\ldots,n\}}$.

Lemma

If G acts on X and $H \leq G$, then H acts on X by the restricted action $H \times X \to X : (h, x) \mapsto h \cdot x$.

Hence an alternative way to show $\mathrm{GL}_n \mathbb{K}$ acts on $\mathbb{K}^n$ is to observe $\mathrm{GL}_n \mathbb{K} \leq S_{\mathbb{K}^n}$. (Invertible $n \times n$ matrices are invertible functions $\mathbb{K}^n \to \mathbb{K}^n$.)

Invariant subsets

Groups aren't tied to a particular action.

Example

D_{2n} was defined as a subgroup of $\mathrm{GL}_2\,\mathbb{R}$, so it acts on $\mathbb{R}^2$.

However, D_{2n} also acts on the vertices $v_0, \ldots, v_{n-1}$ of the n-gon.

In fact, this action determines elements of D_{2n}:

- s^i sends $v_0 \mapsto v_i$ and $v_1 \mapsto v_{i+1}$
- $s^i r$ sends $v_0 \mapsto v_i$ and $v_1 \mapsto v_{i-1}$

This dihedral group action on the vertices of the n-gon is a special case of a pattern.

Definition — invariant under an action

If G acts on X, a subset $Y \subseteq X$ is **invariant under the action of G** if $g \cdot y \in Y$ for all $g \in G$ and $y \in Y$.

Lemma

If G acts on X and Y is an invariant subset, then G acts on Y via $G \times Y \to Y : (g, y) \mapsto g \cdot y$.

Example

$\{0\}$ is an invariant subset of $\mathbb{K}^n$ under the action of $\mathrm{GL}_n\,\mathbb{K}$. In this case, the action of $\mathrm{GL}_n\,\mathbb{K}$ on $\{0\}$ is the trivial action.

Actions on functions

Proposition

Suppose G acts on X and Y, and let $\mathrm{Fun}(X,Y)$ denote the set of functions from X to Y.
If $g \in G$ and $f \in \mathrm{Fun}(X,Y)$, let $g \cdot f$ be the function

$$g \cdot f \colon X \to Y : x \mapsto g \cdot f(g^{-1} \cdot x).$$

Then $G \times \mathrm{Fun}(X,Y) : (g,f) \mapsto g \cdot f$ is a left action of G on $\mathrm{Fun}(X,Y)$.

Proof (homework).

□

Often we apply this function with the trivial action on Y, so the action looks like $g \cdot f(x) = f(g^{-1} \cdot x)$.

Actions on subsets

Proposition

Suppose G acts on X, and let 2^X denote the set of subsets of X. Then $g \cdot S = \{g \cdot s : s \in S\}$ defines an action of G on 2^X.

Proof.

Let $S \in 2^X$.

First, $e \cdot S = \{e \cdot s : s \in S\} = \{s : s \in S\} = S$.

Next, let $g, h \in G$. Then

$$\begin{aligned} g \cdot (h \cdot S) &= g \cdot \{h \cdot s : s \in S\} \\ &= \{g \cdot (h \cdot s) : s \in S\} \\ &= \{gh \cdot s : s \in S\} \\ &= gh \cdot S. \end{aligned}$$

$\square$

Alternative proof: use 2^X as the set of functions $X \to \{0, 1\}$. Realize action of G on 2^X by taking action on functions with trivial action on $\{0, 1\}$ (homework).

Left regular actions

Does every group act on some set?

Lemma

If G is a group, then the multiplication map $\cdot : G \times G \to G$ is a left action of G on G.

Proof.

Immediate from group definition. $\square$

So every group acts on itself by left multiplication. This action is called the **left regular action** of G on G.

Lemma

If $H \leq G$, then G acts on G/H by $g \cdot (kH) = gkH$.

Proof.

G/H is an invariant subset of 2^G. $\square$

Since $G/\{e\} = G$, this generalizes the left regular action.

Right actions

Example

Let G be a group where the product of g and h is denoted gh.

For $g, k \in G$, define $g \cdot k = kg$ (right multiplication). If $g, h, k \in G$, then $g \cdot (h \cdot k) = g \cdot kh = khg$, but $gh \cdot k = kgh$, which is not equal to kgh if $hg \neq gh$.

So right multiplication does not define a left action in general.

Can we fix this?

Definition — (right) action

Let G be a group. A **(right) action** of G on a set X is a function $\cdot \colon X \times G \to X$ such that

1. $x \cdot e = x$ for all $x \in X$, and
2. $(x \cdot g) \cdot h = x \cdot (gh)$ for all $g, h \in G$ and $x \in X$.

Example

- There is a right action of G on itself by right multiplication. This is called the **right regular action** of G on G. More generally, if $H \leq G$ then G acts on $H \backslash G$.
- If G is a group and X is a set, then there is a trivial right action of G on X defined by $x \cdot g = x$ for all $g \in G$ and $x \in X$.
- If there is a right action of G on X, and Y is any set, then $(g \cdot f)(x) = f(g \cdot x)$ defines a *left* action of G on $\mathrm{Fun}(X, Y)$.

Can we reconcile right and left actions somehow?

Proposition

If $\cdot$ is a right action of G on X, then $g \cdot x = x \cdot g^{-1}$ defines a left action of G on X.

Proof.

First $e \cdot x = x \cdot e = x$, and for $g, h \in G$ and $x \in X$, we get

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot (x \cdot h^{-1}) \\ &= (x \cdot h^{-1}) \cdot g^{-1} \\ &= x \cdot h^{-1} g^{-1} \\ &= x \cdot (gh)^{-1} \\ &= gh \cdot x. \end{aligned}$$

$\square$

Combined with the last example, this proposition explains why if $\cdot$ is a left action of G on X, we can define a left action of G on $\mathrm{Fun}(X, Y)$ by setting $(g \cdot f)(x) = f(g^{-1} \cdot x)$.

Permutation representations

Lemma

If G has a left action on a set X, and $g \in G$, let $\ell_g \colon X \to X$ be defined by $\ell_g(x) = g \cdot x$. Then:

1. $\ell_g \circ \ell_h = \ell_{gh}$ for all $g, h \in G$.
2. $\ell_e = 1$, the identity function.
3. ℓ_g is a bijection for all $g \in G$.

Proof.

1. $\ell_g \circ \ell_h(x) = g \cdot (h \cdot x) = gh \cdot x = \ell_{gh}(x)$.
2. $\ell_e(x) = e \cdot x = x$.
3. $\ell_g \circ \ell_{g^{-1}} = \ell_e = 1 = \ell_{g^{-1}} \circ \ell_g$, so ℓ_g is invertible.

□

Corollary

Every left action of G on X gives a homomorphism $\phi \colon G \to S_X : g \mapsto \ell_g$ with $\phi(g)(x) = g \cdot x$.

Definition — permutation representation

If X is a set, a **permutation representation** of G on X is a homomorphism $\phi \colon G \to S_X$.

If $|X| = n$, then $S_X \cong S_n$. So an action on a finite set X with $|X| = n$ gives a homomorphism to S_n.

Example: D_{2n} acts on n vertices of the n-gon, so there is a homomorphism $D_{2n} \to S_n$.

Permutation representations of the dihedral group

Let $X = \{v_0, \dots, v_{n-1}\}$ be the vertices of the n-gon. We identify X with $\{1, \dots, n\}$ by mapping $v_i \mapsto i + 1$ so we can write elements of S_X as elements of S_n.

Let $\phi\colon D_{2n} \to S_n$ be a permutation representation given by the action of D_{2n} on X.

What is $\phi(s)$? We see $s \cdot v_0 = v_1$, $s \cdot v_1 = v_2$, …, $s \cdot v_n = v_0$, so $\phi(s) = (1\ 2\ 3\ \cdots\ n)$.

What is $\phi(r)$? We see $r \cdot v_0 = v_0$, $r \cdot v_1 = v_{n-1}$, $r \cdot v_2 = v_{n-2}$, and in general $r \cdot v_i = v_{n-i}$, so

$$\phi(r) = \begin{cases} (2\ n)(3\ n-1)\cdots(\frac{n+1}{2}\ \frac{n+3}{2}) & n \text{ odd} \\ (2\ n)(3\ n-1)\cdots(\frac{n}{2}\ \frac{n}{2}+2) & n \text{ even} \end{cases}.$$

In general, $\phi(s^i r^j) = \phi(s)^i \phi(r)^j$.

(Note a different choice of r could have yielded a different representation.)

Theorem

1. If G acts on X, then there is a homomorphism $\phi\colon G \to S_X$ defined by $\phi(g)(x) = g \cdot x$.
2. If $\phi\colon G \to S_X$ is a homomorphism, then $g \cdot x = \phi(g)(x)$ defines a group action of G on X.

In other words, group actions are equivalent to permutation representations. Because of this theorem, we treat the two as interchangeable.

Proof.

1. Already done.
2. First, $e \cdot x = \phi(e)(x) = 1(x) = x$ for all $x \in X$. Next, if $g, h \in G$ and $x \in X$, then

$$g \cdot (h \cdot x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x) = \phi(gh)(x).$$

□

Faithful actions

Definition — kernel, faithful

Let G act on a set X, and let $\phi\colon G \to S_X$ be the corresponding permutation representation. The **kernel** of the action is $\ker\phi$, and the action is **faithful** if $\ker\phi = \{e\}$.

That is, an action is faithful if the corresponding permutation representation is injective.

Lemma

An action of G on X is faithful if and only if for every $g \in G$ with $g \neq e$, there is $x \in X$ such that $g \cdot x \neq x$.

Proof.

$\ell_g \neq 1$ if and only if there is $x \in X$ such that $g \cdot x = \ell_g(x) \neq x$. □

Example

- S_X acts faithfully on X.
- If $A \cdot e_i = e_i$ for all $i = 1, \ldots, n$, then $A = 1$, so the action of $\mathrm{GL}_n \mathbb{K}$ on $\mathbb{K}^n$ is faithful.
- D_{2n} acts faithfully on vertices on the n-gon (exercise).
- The trivial action is not faithful.

Does every group act faithfully on some set?

Theorem — Cayley's theorem

The left regular action of G on G is faithful.
Consequently, G is isomorphic to a subgroup of S_G. In particular, if $|G| = n < \infty$, then G is isomorphic to a subgroup of S_n.

Proof.

If $g \in G$ with $g \neq e$, then $g \cdot e = g \neq e$. So the left regular action is faithful.

Hence the permutation representation $\phi\colon G \to S_G$ is injective, and thus G is isomorphic to $\operatorname{Im}\phi \leq S_G$ (first isomorphism theorem).

If $|G| = n < \infty$, then $S_G \cong S_n$. □

The homomorphism $G \to S_G$ given by this theorem is called the **left regular representation** of G.

Example

Let $G = \mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$.

By Cayley's theorem, G is isomorphic to a subgroup of S_2.

$[0] + [0] = [0]$ and $[0] + [1] = [1]$, so $[0] \mapsto e$ in S_2.

$[1] + [0] = [1]$ and $[1] + [1] = [0]$, so $[1] \mapsto (12)$ in S_2.

Note the left regular representation may not be the most efficient permutation representation.

Example

D_6 has order 6, so it is isomorphic to a subgroup of S_6.

But D_6 acts faithfully on the vertices of the 3-gon, so there is an injective homomorphism $D_6 \to S_3$; since $|D_6| = |S_3| = 6$, this is an isomorphism.

But $|S_6| = 6! \gg 6$, so the left regular representation may be much larger in terms of space.

13: Orbits and stabilizers

Orbits

Definition — orbit

Let G act on X. The **G-orbit** of x is $\mathcal{O}_x = \{g \cdot x : g \in G\}$. A subset $\mathcal{O} \subseteq X$ is an **orbit** if $\mathcal{O} = \mathcal{O}_x$ for some $x \in X$. A group action is **transitive** if $\mathcal{O}_x = X$ for some $x \in X$.

Example

- Let $H \leq G$ act on G by left multiplication. The orbit of $g \in G$ is $\mathcal{O}_g = Hg$, a right coset.

  Since Hg is a proper subset of G if $H < G$, we see the action is not transitive unless $H = G$.

- Consider the action of $\mathrm{GL}_n \mathbb{K}$ on $\mathbb{K}^n$. Then

$$\mathcal{O}_v = \begin{cases} \{0\} & v = 0 \\ \mathbb{K}^n \setminus \{0\} & v \neq 0 \end{cases}.$$

  So this action is not transitive, and there are two orbits.

- If $1 \leq i \neq j \leq n$, then we can find $\pi \in S_n$ where $\pi(i) = j$. So $\mathcal{O}_i = \{1, \ldots, n\}$ for all i. We conclude the action of S_n on $\{1, \ldots, n\}$ is transitive and has one orbit.

- More generally, the action of S_X on X is transitive and has one orbit.

- Suppose $\sigma \in S_n$. What are the orbits of $\langle \sigma \rangle$ on $\{1, \ldots, n\}$?

  For example, take $\sigma = (137)(26)(48) \in S_8$. Then $\mathcal{O}_1 = \mathcal{O}_3 = \mathcal{O}_7 = \{1, 3, 7\}$, $\mathcal{O}_2 = \mathcal{O}_6 = \{2, 6\}$, $\mathcal{O}_4 = \mathcal{O}_8 = \{4, 8\}$, and $\mathcal{O}_5 = \{5\}$.

  In general, if $\sigma = (i_{11} \cdots i_{1k_1})(i_{21} \cdots i_{2k_2}) \cdots (i_{m1} \cdots i_{mk_m})$ (including 1-cycles), then the orbits are $\{i_{j1}, \ldots, i_{jk_j}\}$ for $1 \leq j \leq m$.

Equivalence relation from a G-action

Note that in all the previous examples, the orbits partitioned X. Recall that partitions correspond to equivalence relations.

Definition

If G acts on X, say that $x \sim_G y$ if there is $g \in G$ such that $g \cdot x = y$.

Lemma

If G acts on X, then $\sim_G$ is an equivalence relation on X.

Proof.

Since $e \cdot x = x$, $x \sim_G x$ for all $x \in X$.

If $g \cdot x = y$, then $g^{-1} \cdot y = x$, so $x \sim_G y \implies y \sim_G x$.

Finally, if $g \cdot x = y$ and $h \cdot y = z$, then $hg \cdot x = z$, so $x \sim_G y$ and $y \sim_G z \implies x \sim_G z$. □

Then if $x \in X$, the equivalence class $[x]_{\sim_G}$ of x is $\{y \in X : x \sim_G y\} = \{y \in X : y = g \cdot x \text{ for some } g \in G\} = \mathcal{O}_x$.

Thus we conclude the equivalence classes of $\sim_G$ are the orbits of G acting on X.

Proposition

If G acts on X, then orbits of G form a partition of X. In particular, the action is transitive if and only if there is only one orbit.

Definition — set of representatives

Let $\sim$ be an equivalence relation on a set X. A subset $S \subseteq X$ is said to be a **set of representatives** for $\sim$ if each equivalence class of $\sim$ contains exactly one element of S.

A set of representatives exists for every $\sim$.

Corollary

Suppose G acts on a set X and let S be a set of representatives for $\sim_G$. Then

$$|X| = \sum_{x \in S} |\mathcal{O}_x|.$$

What is $|\mathcal{O}_x|$?

We can use the function $G \to \mathcal{O}_x : g \mapsto g \cdot x$. This is clearly surjective, but what if the function is not injective (i.e., $g \cdot x = h \cdot x$ for some $g \neq h$)?

Stabilizers

Definition — stabilizer

If G acts on X, and $x \in X$, the **stabilizer** of x is $G_x := \{g \in G : g \cdot x = x\}$.

Proposition

If G acts on X, and $x \in X$, then G_x is a subgroup of G.

Proof.

First, $e \in G_x$.

Second, if $g, h \in G_x$, then $gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x \implies gh \in G_x$.

Third, if $g \in G_x$, then $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = e \cdot x = x \implies g^{-1} \in G_x$. □

Theorem — Orbit-stabilizer theorem

If G acts on X, and $x \in X$, then there is a bijection $G/G_x \to \mathcal{O}_x : gG_x \mapsto g \cdot x$.

Proof.

Well-defined: if $gG_x = hG_x$, then $g^{-1}h \in G_x$. So $g^{-1}h \cdot x = x \implies h \cdot x = g \cdot x$.

Injective: if $g \cdot x = h \cdot x$, then $g^{-1}h \cdot x = x$, so $g^{-1}h \in G_x \implies gG_x = hG_x$.

Surjective: if $y \in \mathcal{O}_x$, then $y = g \cdot x$ by definition. □

Corollary

If G acts on X and $x \in X$, then $|\mathcal{O}_x| = [G : G_x]$.

Example: S_n

Let $G = S_n$ and $X = \{1, \ldots, n\}$.

We know the action of G on X is transitive, so $\mathcal{O}_i = X$ for any i.

Then $n = |\mathcal{O}_i| = [G : G_i] = \frac{|G|}{|G_i|} = \frac{n!}{|G_i|}$. Hence $|G_i| = (n-1)!$ for any i.

Thus the stabilizer of i is $G_i = \{\pi \in S_n : \pi(i) = i\}$.

For a concrete example, if $n = 4$, then $G_1 = \{e, (23), (24), (34), (234), (243)\}$.

In general, $G_i \cong S_{n-1}$ (add 1 to each number in S_{n-1} which is $\geq i$), so we see $|G_i| = (n-1)!$ directly.

Example: G/H

Recall that the action of G on G/H is $g \cdot kH = gkH$ (i.e. usual set multiplication).

Proposition

Suppose $H \leq G$. Then the left multiplication action of G on G/H is transitive, and $G_{eH} = H$.

Proof.

If $gH \in G/H$, then $gH = g \cdot eH$, so $\mathcal{O}_{eH} = G/H$.

Also, $g \cdot eH = eH \iff gH = H \iff g \in H$. $\square$

In this case, the orbit-stabilizer theorem states that $\mathcal{O}_{eH} = G/H$ is in bijection with G/H (tautology).

Kernel versus stabilizer

If G acts on X, then the kernel of the action is $\{g \in G : g \cdot x = x \text{ for all } x\}$.

Meanwhile, the stabilizer $G_x = \{g \in G : g \cdot x = x\}$ has x fixed.

Consequently, if H is the kernel of the action, then $H \leq G_x$ for all $x \in X$.

Proposition

If G acts on X, then the kernel of the action is $\bigcap_{x \in X} G_x$, the intersection of the stabilizers.

Proof.

g is in the kernel if and only if $g \in G_x$ for all $x \in X$. □

An application:

Theorem

If G is finite and $H \leq G$ has index $[G : H] = p$ where p is the smallest prime dividing $|G|$, then $H \trianglelefteq G$.

Proof.

Let K be the kernel of the action of G on G/H (so K is normal).

By the proposition, $K \leq H = G_{eH}$. Then let $k = [H : K] = \frac{|H|}{|K|}$.

Now $[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = pk$.

By the first isomorphism theorem, G/K is isomorphic to a subgroup of S_p. So $|G/K| = kp \mid p! = |S_p| \implies k \mid (p-1)!$.

But we also have $k \mid |G|$. Since p is the smallest prime dividing $|G|$, we must have $k = 1$. Hence $|H| = |K|$ so $H = K$. □

Conjugation actions

Recall left multiplication defines a left action of G on G. There is, however, another natural left action.

Lemma

$G \times G \to G : (g, k) \mapsto gkg^{-1}$ defines an action of G on G.

This action is called the **conjugation action** of G on G.

To avoid conjustion with the left multiplication action here, we'll denote it by $g \bullet k = gkg^{-1}$.

(In practice, there is no convention about $\cdot$ and $\bullet$; specify your choices when writing.)

Proof.

If $k \in G$, then $e \bullet k = eke = k$.

If $g, h, k \in G$, then $g \bullet (h \bullet k) = g \bullet hkh^{-1} = ghkh^{-1}g^{-1} = (gh)k(gh)^{-1} = gh \bullet k$. $\square$

Definition — conjugacy class, centralizer

The orbit of $k \in G$ under the conjugation action is called the **conjugacy class** of k, denoted by $\mathrm{Conj}_G(k)$.

The stabilizer of $k \in G$ is called the **centralizer** of k in G, denoted by $C_G(k)$.

By definition, $\mathrm{Conj}_G(k) = \{gkg^{-1} : g \in G\}$.

$C_G(k) = \{g \in G : gkg^{-1} = k\} = \{g \in G : gk = kg\}$, namely the centralizer is the set of elements in G which commute with k.

By the orbit-stabilizer theorem, $|\mathrm{Conj}_G(k)| = [G : C_G(k)]$.

For example: $\mathrm{Conj}(e) = \{geg^{-1} : g \in G\} = \{e\}$ and $C_G(e) = G$.

Note the conjugation action of G on G induces an action of G on 2^G. In particular, if $g \in G$ and $S \subseteq G$, then $g \bullet S = \{g \bullet h : h \in S\} = \{ghg^{-1} : h \in S\} = gSg^{-1} = N_G(S)$ (the normalizer of S in G).

Example: matrices

One important instance of the conjugation action is with $\mathrm{GL}_n\,\mathbb{K}$.

Actually, if A, B are $n \times n$ matrices and A is invertbile, then ABA^{-1} makes sense even if B is not invertible.

Exercise

Show $\mathrm{GL}_n\,\mathbb{K}$ acts on $M_n\mathbb{K}$ by conjugation, where $M_n\mathbb{K}$ is the set of $n \times n$ matrices over $\mathbb{K}$.

Recall matrices A and B are **similar** if there is $C \in \mathrm{GL}_n\,\mathbb{K}$ such that $CAC^{-1} = B$. This is the equivalence relation $\sim_{\mathrm{GL}_n\,\mathbb{K}}$.

The orbits of the conjugation action of $\mathrm{GL}_n\,\mathbb{K}$ on $M_n\mathbb{K}$ are called **similarity classes**.

A matrix A is **diagonalizable** if it is similar to a diagonal matrix.

When $\mathbb{K} = \mathbb{C}$, every similarity class contains exactly one matrix in Jordan normal form; matrices in Jordan normal form give a set of representatives for $\sim_{\mathrm{GL}_n\,\mathbb{K}}$.

Class equation and Cauchy's theorem

Using standard facts about orbits,

$$|G| = \sum_{g\in S} |\mathrm{Conj}(g)| = \sum_{g\in S} [G : C_G(g)]$$

where S is a set of representatives for conjugacy classes.

We could simplify this by pulling out conjugacy classes of size 1:

Lemma

$|\mathrm{Conj}(k)| = 1 \iff C_G(k) = G \iff k \in Z(G).$

Proof.

$|\mathrm{Conj}(k)| = 1$ if and only if $gkg^{-1} = k$ for all $g \in G$ (since $k \in \mathrm{Conj}(k)$ always) if and only if $C_G(k) = G$ if and only if $k \in Z(G)$. □

Theorem — Class equation

If G is a finite group, then

$$|G| = |Z(G)| + \sum_{g\in T} |\mathrm{Conj}(g)|$$

where T is a set of representatives for conjugacy classes not contained in the center.

Theorem — Cauchy's theorem

If G is a finite group and p is a prime dividing $|G|$, then G contains an element of order p.

Proof.

Let $|G| = pm$. Note the theorem is clear when G is cyclic.

First assume G is abelian; proof by induction on m.

Base case: if $m = 1$, then G is cyclic, so we are done.

Inductive step: pick $a \in G$, $a \neq e$. We can assume $|a| < |G|$ (otherwise G is cyclic). If $p \mid |a|$, then by induction we get $b \in \langle a\rangle$ with $|b| = p$. Otherwise, $N = \langle a\rangle \trianglelefteq G$ since G is abelian. Thus $|G/N| = \frac{|G|}{|N|} < |G|$. Since $p \mid |G|$ but $p \nmid |N|$, we get $p \mid |G/N|$. By induction, G/N has an element gN of order p. Let $n = |g|$. Since $g^n = 1$, $q(g)^n = 1$ where q is the quotient map, so $p \mid n$. If $G = \langle g \rangle$, we are done, otherwise apply induction to $\langle g \rangle$.

Now take a general G (possibly non-abelian); induction on $|G|$.

By the class equation, $|G| = |Z(G)| + \sum_{g \in T} |\mathrm{Conj}(g)|$.

If $p \nmid |\mathrm{Conj}(g)| = |G|/|C_G(g)|$ for some $g \in T$, then $p \mid |C_G(g)|$. Since $g \notin Z(G)$, $|\mathrm{Conj}(g)| > 1 \implies |C_G(g)| < |G|$. By induction, $C_G(g)$ contains an element of order p.

If $p \mid |\mathrm{Conj}(g)|$ for all $g \in T$, then $p \mid |Z(G)|$. $Z(G)$ is an abelian group, so by the abelian case, $Z(G)$ contains an element of order p. $\square$

Center of p-groups

Definition — p-group

Let p be prime. A group G is a **p-group** if $|G| = p^k$ for some $k \geq 1$.

Theorem

If G is a p-group, then $Z(G) \neq \{e\}$.

Proof.

$|G| = |Z(G)| + \sum_{g \in T} [G : C_G(g)]$.

Note $[G : C_G(g)] \mid |G|$.

If $g \notin Z(G)$, then $[G : C_G(g)] > 1 \implies p \mid [G : C_G(g)]$.

So $p \mid |Z(G)|$. □

As shown in the proof, the order of $Z(G)$ is a non-zero power of p. Alternatively, get this from the theorem and Lagrange's theorem.

Week 6: Classification of Groups

14: Classification of groups

Classification problem: identify all groups up to isomorphism. (We could replace groups with any algebraic structure. Classification is one of the big questions in modern mathematics.)

Order	Known groups
1	Trivial group
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
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	$\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

Groups of order p^2

Proposition

Suppose p is prime and $|G| = p^2$. Then either G is cyclic, or $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Proof.

Suppose G is not cyclic, so choose $a \in G \setminus \{e\}$.

We know $\langle a \rangle \neq G$, so $|a| = p$ and we can find $b \in G \setminus \langle a \rangle$.

Since $\langle b \rangle \neq G$, we get $|b| = p$ as well. Let $H = \langle a \rangle$ and $K = \langle b \rangle$.

Since $H \cap K < K$, we see $|H \cap K| = 1$ so $H \cap K = \{e\}$. Then $|HK| = \frac{|H||K|}{|H \cap K|} = p^2$ so $HK = G$.

Finally, $[G : H] = [G : K] = p$, the smallest prime dividing $|G|$. Hence $H, K \trianglelefteq G$ so $G \cong H \times K \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. □

Groups of order pq

Lemma

Suppose $H, K \trianglelefteq G$ where $\gcd(|H|, |K|) = 1$ and $|H||K| = |G|$. Then $G \cong H \times K$.

Proof.

Since $|H \cap K|$ divides both $|H|$ and $|K|$, we get $|H \cap K| = 1$ so $H \cap K = \{e\}$.

Also, $|HK| = \frac{|H||K|}{|H \cap K|} = |G|$ so $HK = G$.

The result follows from the characterization of products. □

Suppose $|G| = pq$ for distinct primes $p < q$. What can we say about G?

By Cauchy's theorem, G has elements a, b with $|a| = p$ and $|b| = q$. Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Note $\gcd(|H|, |K|) = 1$ and $|H||K| = |G|$. Is it true that $H, K \trianglelefteq G$?

We know $[G : K] = p$, which is the smallest prime dividing $|G|$, so $K \trianglelefteq G$. But is $H \trianglelefteq G$? Not necessarily.

Counterexample: $G = D_6$, $H = \langle r \rangle$, $K = \langle s \rangle$.

What if we suppose $H, K \leq G$, $HK = G$, $H \cap K = \{e\}$, and $K \trianglelefteq G$? Is $G \cong H \times K$ here? Again, no!

In our counterexample, that would mean $D_6 \cong H \times K \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, but D_6 is non-abelian.

However, there is a set bijection $H \times K \to G : (h, k) \mapsto hk$, and we can say that $G \cong H \ltimes K$, the **semidirect product** of H and K (later, optional).

For $p = 2$ and $q = 3$, it turns out the only groups of order $pq = 6$ are $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_6$, and $D_6 \cong S_3$.

What can we say?

The difficulty in analyzing the pq case was that $H \leq G$ might not be normal. This concern is not present if G is abelian, so we will focus on finite abelian groups this week.

There are lots of other ways to approach classification. Notice that for small orders, we are essentially describing groups as being built out of other groups.

We say a group is **simple** if it contains no (non-trivial) normal subgroups. Simple groups are the minimal building blocks for other groups.

Finally, by looking at the isomorphism problem for **finitely-presented groups** (later, optional), we will see that the classification problem for infinite groups cannot be solved.

Decomposing finite abelian groups

From the earlier lemma, we can disregard the normality constraint when considering abelian groups. Then, how can we find groups of coprime order?

Lemma

Suppose G is an abelian group. Let $G^{(m)} = \{g \in G : g^m = e\}$. Then $G^{(m)} \leq G$ for all $m \geq 1$.

Proof.

Clearly $e \in G^{(m)}$ for all $m \geq 1$. If $g, h \in G^{(m)}$, then $(g^{-1}h)^m = g^{-m}h^m = e \in G^{(m)}$. □

$G^{(m)}$ is the **m-torsion subgroup**.

Proposition

Suppose $|G| = mn$ where $\gcd(m, n) = 1$. Then
1. $\phi\colon G \to G^{(m)} \times G^{(n)} : g \mapsto (g^n, g^m)$ is an isomorphism.
2. $|G^{(m)}| = m$ and $|G^{(n)}| = n$.

Proof.

1. If $g \in G$, then $g^{mn} = e$, so $g^n \in G^{(m)}$ and $g^m \in G^{(n)}$. Hence ϕ is well-defined.

   Now find $a, b \in \mathbb{Z}$ such that $an + bm = 1$. If $\phi(g) = e$, then $g^n = g^m = e \implies g = g^{an+bm} = e$, so ϕ is injective.

   If $g \in G^{(m)}$ and $h \in G^{(n)}$, then $g = g^{an+bm} = g^{an}$ and similarly $h = h^{an+bm} = h^{bm}$, so $\phi(g^a h^b) = (g^{an}h^{bn}, g^{am}h^{bm}) = (g, h)$. Hence ϕ is also surjective.

   We also need to show ϕ is a homomorphism:

   $$\phi(gh) = ((gh)^n, (gh)^m) = (g^n h^n, g^m h^m) = (g^n, g^m) \cdot (h^n, h^m) = \phi(g)\phi(h).$$

2. Since $G \cong G^{(m)} \times G^{(n)}$, $|G| = |G^{(m)}||G^{(n)}|$.

   Suppose $|G| = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of $|G|$. Since $|G| = mn$ and $\gcd(m, n) = 1$, we have $m = p_1^{b_1} \cdots p_k^{b_k}$ and $n = p_1^{c_1} \cdots p_k^{c_k}$ where for each i, $a_i = b_i + c_i$ and only one of b_i and c_i is non-zero.

   Suppose $b_i > 0$. If $p_i \mid |G^{(n)}|$, then $G^{(n)}$ has an element a of order p_i by Cauchy's theorem. Then $p_i \mid m \implies a \in G^{(m)} \implies a \in \ker\phi \implies a = e$, which is impossible. So $p_i \nmid |G^{(n)}| \implies p_i^{a_i} \mid |G^{(m)}|$.

Conclusion: $m \mid |G^{(m)}|$ and $n \mid |G^{(n)}|$. So $|G^{(m)}| = m$ and $|G^{(n)}| = n$.

□

Example

Suppose $\gcd(m, n) = 1$ and let $G = \mathbb{Z}/mn\mathbb{Z}$.

If $m[x] = 0$ for $0 \le x < mn$, then $mn \mid mx \iff n \mid x$. So $G^{(m)} = \{[x] \in G : m[x] = 0\} = n\mathbb{Z}/mn\mathbb{Z}$.

Since $\mathbb{Z} \to n\mathbb{Z} : x \mapsto nx$ is an isomorphism sending $m\mathbb{Z} \mapsto mn\mathbb{Z}$, $n\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$. Similarly, $G^{(n)} \cong m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$.

The proposition gives $\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. (Chinese remainder theorem.)

Corollary

Let G be a finite abelian group and let $|G| = p_1^{a_1} \cdots p_k^{a_k}$ where $p_1, \ldots, p_k$ are distinct primes and $a_i > 0$ for all i. Then $G \cong G_1 \times G_2 \times \cdots \times G_k$ where $|G_i| = p_i^{a_i}$.

Proof.

Let $G_1 = G^{(p_1^{a_1})}$ and let $r = p_2^{a_2} \cdots p_k^{a_k}$.

Since $p_1^{a_1}$ and r are coprime and $p_1^{a_1} \cdot r = |G|$, the proposition implies $G \cong G_1 \times G^{(r)}$ and that $|G_1| = p_1^{a_1}$ and $|G^{(r)} = r|$.

We can continue to get $G^{(r)} = G_2 \times \cdots \times G_k$ as desired. □

We can go further, and decompose into cyclic groups.

Proposition

If G is a finite abelian group, then $G \cong C_{a_1} \times C_{a_2} \times \cdots \times C_{a_k}$ for some sequence $a_1, \ldots, a_k$ where every a_i is a prime power.

(Recall that C_n is the multiplicative form of $\mathbb{Z}/n\mathbb{Z}$.)

Proof.

By the previous corollary, we can assume G is a p-group, i.e. $|G| = p^n$ for some n. Proof by induction on n; for base case $n = 0$, take $k = 0$.

Choose an element $x \in G$ of maximal order, so say $|x| = p^r$. Since G is abelian, $N = \langle x \rangle \trianglelefteq G$.

Then $|G/N| < |G|$, so by induction, $G/N = C_{b_1} \times \cdots C_{b_\ell}$ for some sequence $b_1, \ldots, b_\ell$ of prime powers. By Lagrange's theorem, $b_i = p^{s_i}$ for all i.

For each i, let $\tilde{y}_i$ be the generator of C_{b_i}. Let $y_i N \in G/N$ be the element of G/N corresponding to $(e, \ldots, e, \tilde{y}_i, e, \ldots, e)$ (that is, $\tilde{y}_i$ in the i-th position). Say $|y_i| = p^{t_i}$; note $r \geq t_i \geq s_i$.

We know that $y_i^{b_i} \in N$, so $y_i^{b_i} = x^{c_i}$ for some c_i. Now $b_i = p^{s_i}$, so $|y_i^{b_i}| = p^{t_i}/p^{s_i} = p^{t_i - s_i}$. We conclude that $c_i = d_i p^{r-(t_i - s_i)} = d_i p^{r - t_i + s_i}$ for some d_i.

Let $z_i = y_i x^{-d_i p^{r-t_i}}$. Then $z_i N = y_i N$, and $z_i^{b_i} = y_i^{b_i} x^{-d_i p^{r-t_i+s_i}} = y_i^{b_i} x^{-c_i} = e$, so $|z_i| = b_i$.

Let $H = \langle z_1, \ldots, z_\ell \rangle \leq G$ and suppose $w \in H \cap N$. Then $w = z_1^{n_1} \cdots z_\ell^{n_\ell}$ where $0 \leq n_i < b_i$ for all i.

Let $q \colon G \to G/N$ be the quotient map. Then

$$q(w) = q(z_1)^{n_1} \cdots q(z_\ell)^{n_\ell} = (z_1 N)^{n_1} \cdots (z_\ell N)^{n_\ell} = (y_1 N)^{n_1} \cdots (y_\ell N)^{n_\ell} \cong (\tilde{y}_1^{n_1}, \ldots, \tilde{y}_\ell^{n_\ell}).$$

But since $w \in N = \ker q$, $q(w) = e$, so $n_1 = \cdots = n_\ell = 0$. We conclude $w = e$, or in other words $H \cap N = \{e\}$.

Suppose $g \in G$. Then $gN \cong (\tilde{y}_1^{n_1}, \ldots, \tilde{y}_\ell^{n_\ell})$ for some $n_1, \ldots, n_\ell$ which implies $gN = (z_1 N)^{n_1} \cdots (z_\ell N)^{n_\ell} = (z_1^{n_1} \cdots z_\ell^{n_\ell})N$. In particular, $g \in HN$. We conclude $HN = G$.

Since G is abelian, $H, N \trianglelefteq G$. So $G = N \times H$

Now $N \cong C_{p^r}$ and $|H| < |G|$, so by induction, H is also a product of prime-power cyclic groups. $\square$

Now, the main result.

Theorem — Classification of finite abelian groups

If G is a finite abelian group, then $G \cong C_{a_1} \times \cdots \times C_{a_k}$ where $a_1 \leq \cdots \leq a_k$ is a sequence of prime powers.
Furthermore, if $G \cong C_{b_1} \times \cdots \times C_{b_\ell}$ where $b_1 \leq \cdots \leq b_\ell$ is another sequence of prime powers, then $k = \ell$ and $a_i = b_i$ for all $1 \leq i \leq k = \ell$.

Example

We saw earlier that $C_2 \times C_3 \cong C_6$ (or generally $C_m \times C_n \cong C_{mn}$ for coprime m and n), so the requirement that a_i be a prime power is required for uniqueness.

Proof.

We just need to prove uniqueness.

If $G \cong C_{b_1} \times \cdots \times C_{b_\ell}$, then $G^{(m)} \cong C_{b_1}^{(m)} \times \cdots \times C_{b_\ell}^{(m)}$.

If p, q are distinct primes, then $C_{p^r}^{(q^s)} = \{e\}$. Otherwise if $p = q$, $|C_{p^r}^{(p^s)}| = p^{\min(r,s)}$.

Now

$$|G^{(p^r)}| = \prod_{s \geq 1} \prod_{i : b_i = p^s} |C_{b_i}^{(p^r)}| = \prod_{s \geq 1} \prod_{i : b_i = p^s} p^{\min(r,s)}$$

and hence

$$\frac{|G^{(p^r)}|}{|G^{(p^{r-1})}|} = \prod_{s \geq r} \prod_{i : b_i = p^s} p.$$

So $\log_p |G^{(p^r)}| - \log_p |G^{(p^{r-1})}| = |\{i : b_i = p^s \text{ for some } s \geq r\}|$.

Exercise: recover ℓ and $b_1, \ldots, b_\ell$ from these numbers. $\square$