Algebraic Structure Notes

Instructor: Anton Bernshteyn
Notes by: Lichen Zhang
Carnegie Mellon University
21-373 Algebraic Structure

December 18, 2019

Contents

1 Sets, Functions and Equivalence Relations 2
  1.1 Basic definitions ......................................................... 2
  1.2 Higher-order functions ............................................... 4
  1.3 Equivalence relations & quotients ..................................... 5

2 Functors 7
  2.1 Covariant functors ...................................................... 7
  2.2 Universal elements ...................................................... 9
  2.3 Contravariant functors ............................................... 11

3 Groups 12
  3.1 Concrete groups .......................................................... 12
  3.2 Abstract groups .......................................................... 16
  3.3 Abelian groups, subgroups, homomorphisms ......................... 20
  3.4 Actions, cosets, orbits ............................................... 22
1 Sets, Functions and Equivalence Relations

1.1 Basic definitions

We start this notes by reminding readers some basic definitions of sets, functions and equivalence relations, which, though fundamental, are critical in the study of various algebraic structures. Given two sets $A, B$, except for the standard notation $A \cup B, A \cap B, A \setminus B, A \subseteq B, A \subset B$, we introduce symmetric difference of two sets.

**Definition 1.1.** The *symmetric difference* of two sets $A, B$, denoted by $A \triangle B$, is defined as $(A \setminus B) \cup (B \setminus A)$.

**Definition 1.2.** The set of all functions $f : A \to B$ is denoted as $B^A$.

**Exercise 1.3.** If both $A, B$ are finite, show that $\left| B^A \right| = |B|^{|A|}$.

**Proof.** To count all functions from $A$ to $B$, it is useful to think of it in a *bucket-item* manner: each element of $A$ can be viewed as a *bucket*, while each element of $B$ is *item*, count the number of functions is just counting the number of ways to put items into buckets. For each bucket, there are $|B|$ items we can put into, moreover, these items can be put into as many buckets as we want, so there are $|B|^{|B| \ldots |B|} = |B|^{|A|}$ functions in total.

**Definition 1.4.** Let $f : A \to B$ be a function.

- $f$ is *injective*, if for $a_1, a_2 \in A, a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$.
- $f$ is *surjective*, if for any $b \in B, b \in \text{im}(f)$, or equivalently, $B = \text{im}(f)$.
- $f$ is *bijective* if it is both injective and surjective.

**Definition 1.5.** Two functions $f, g$ are *equal*, if $\text{dom}(f) = \text{dom}(g)$, and for any $x \in \text{dom}(f), f(x) = g(x)$.

**Definition 1.6.** Let $A$ be a set, $\{0\}$ be a 1-element set, what is $A^{\{0\}}$? It’s the set of all functions from $\{0\}$. It is clear that there is a bijection between $A^{\{0\}}$ and $A$ by $f \mapsto f(0)$. In such scenario, we say $A$ is *isomorphic* to $A^{\{0\}}$.

**Definition 1.7.** Given two sets $A, B$, we say $A$ is *isomorphic* to $B$, denoted by $A \cong B$, if there exists a bijection from $A$ to $B$.

1. $A^{\{0,1\}} \cong A \times A$, the bijection is given by $f \mapsto (f(0), f(1))$.
2. What is $A^0, \emptyset^A$? They are different as long as $A \neq \emptyset$.
3. $\{0,1\}^A \cong \mathcal{P}(A)$, the bijection is $f \mapsto \{a \in A : f(a) = 1\}$.

**Definition 1.8.** Given three sets $A, B, C$, two functions $f : B \to C, g : A \to B$, define *composition* of functions $f, g$, denoted by $f \circ g$, as follows:

- $\text{dom}(f \circ g) = \{x \in \text{dom}(g) : g(x) \in \text{dom}(f)\}$.
For \( x \in \text{dom} \, (f \circ g) \), define \((f \circ g)(x) = f(g(x))\).

**Exercise 1.9** (Important). Verify function composition is associative, i.e., given \(f, g, h\) three functions with well-behaved domains & codomains, verify \(f \circ (g \circ h) = (f \circ g) \circ h\).

**Example 1.10.** Applying a function to an element can be “encoded” as a composition operation: let \(f : A \to B\) be our function, consider \(f(a)\), we can replace \(a\) by function \(g : \{0\} \to A\) by \(0 \mapsto a\), then \(f \circ g : \{0\} \to B : 0 \mapsto f(a)\).

**Definition 1.11.** Given a set \(A\), the *identity functions* on \(A\), denoted by \(\text{id}_A : A \to A\), is the function \(a \mapsto a\).

**Exercise 1.12.** Let \(f : A \to B\), then \(f \circ \text{id}_A = \text{id}_B \circ f = f\).

**Definition 1.13.** Let \(f : A \to B, g : B \to A\), if \(f \circ g = \text{id}_B\), then \(f\) is a *left inverse* of \(g\) and \(g\) is a *right inverse* of \(f\). If \(f\) is both left and right inverse of \(g\), then \(f\) is a *two-sided inverse* of \(g\).

**Exercise 1.14.** Give an example such that \(f\) is a left inverse, but not a right inverse of \(g\).

**Exercise 1.15.** Let \(A \neq \emptyset, B\) be two sets and \(f : A \to B, g : B \to A\). Prove the following:

1. \(f\) has a left inverse \(g\) if and only if \(f\) is injective.
2. \(f\) has a right inverse \(g\) if and only if \(f\) is surjective.

The proof is not hard, for the first part, one simply choose \(g\) to send everything to its preimage under \(f\). For the second part, \(g\) can simply send element to one of its preimage under \(f\).

**Definition 1.16.** Given \(f : A \to B\), the followings are equivalent:

1. \(f\) is bijective.
2. \(f\) has a right and left inverse.
3. \(f\) has a two-sided inverse.

In this case, we denote (two-sided) inverse of \(f\) as \(f^{-1}\). Also, \(f^{-1}\) is a bijection from \(B\) to \(A\) and \((f^{-1})^{-1} = f\).

**Exercise 1.17.** Suppose \(f : A \to B, g : B \to A\) are both bijective, then \((g \circ f)^{-1} = f^{-1} \circ g^{-1}\).
1.2 Higher-order functions

In this section, we study *higher-order functions*, which take functions as inputs and spits out functions. This idea has been heavily exploited in functional programming and the study of programming language. We motivate with an example.

**Example 1.18.** Let $X,Y,A$ be sets, then we claim $A^{X \times Y} \cong (A^X)^Y$.
Given $f \in A^{X \times Y}$, i.e., $f : X \times Y \to A$, we associate $f$ to the function $F : Y \to A^X$ as follows: for any $y \in Y, x \in X$, $(F(y))(x) := f(x,y)$. This is called function currying.

The inverse of this operation is as follows: to each $F \in (A^X)^Y$, assign $f : X \times Y \to A$ by $f(x,y) := (F(y))(x)$.

**Definition 1.19.** Let $X,Y,A$ be sets, to each function $f : X \to Y$, corresponds a function $f^A : X^A \to Y^A$, given by $f^A(g) := f \circ g$.

**Proposition 1.20.** Let $X,Y,Z$ be sets and $f : X \to Y, g : Y \to Z$, then $(g \circ f)^A = g^A \circ f^A$.

**Proof.** First, let’s compare the domains.

- $g \circ f : X \to Z$, so $(g \circ f)^A : X^A \to Z^A$
- $g^A : Y^A \to Z^A, f^A : X^A \to Y^A$, so $g^A \circ f^A : X^A \to Z^A$

Take and $h \in X^A$, let’s do some computations.

- $(g \circ f)^A(h) = (g \circ f) \circ h$
- $g^A \circ f^A(h) = g^A(f \circ h) = g \circ (f \circ h)$

By 1.9, we know that function composition is associative, therefore, they are equal.

**Definition 1.21.** Let $X,Y,A$ be sets, to each function $f : X \to Y$, corresponds a function $A^f : A^Y \to A^X$ by $(A^f)(g) = g \circ f$.

**Exercise 1.22.** Let $X,Y,Z$ be sets and $f : X \to Y, g : Y \to Z$, then $A^{g \circ f} = A^f \circ A^g$. 

1.3 Equivalence relations & quotients

**Definition 1.23.** A (binary) relation on a set $X$ is a subset $R \subseteq X \times X$, usually, we write $xRy$ instead of $(x, y) \in R$.

**Definition 1.24.** An equivalence relation $E$ on set $X$ is a relation such that

1. $E$ is reflexive.
2. $E$ is symmetric.
3. $E$ is transitive.

**Example 1.25.** Consider the following relation on $\mathbb{Z}$:

- $xEy$ $\iff$ $x - y \in \mathbb{Z}$, this is an equivalence relation.
- $xEy$ $\iff$ $x + y \in \mathbb{Z}$, this is not an equivalence relation, transitivity does not hold.

**Definition 1.26.** Given function $f : X \to Y$, the equivalence kernel of $f$ is the relation $E_f$ on $X$, given by $xE_f y \iff f(x) = f(y)$, this $E_f$ is an equivalence relation.

Conversely, given an equivalence relation $E$ on $X$, for $x \in X$, let $[x]_E := \{y \in X : xEy\}$, defined as the equivalence class of $x$.

Let $X/E := \{[x]_E : x \in X\}$ be the quotient of $X$ by $E$, the map $p_E : X \to X/E : x \mapsto [x]_E$ is called the quotient map.

**Proposition 1.27.** Let $E$ be an equivalence relation on $X$, then $p_E : X \to X/E$ is a surjection, with equivalence kernel $E$.

**Proof.** The first part is clear, any equivalence class $[x]_E$ has at least one canonical representation, namely $x$ in it, this is given by $E$ is reflexive. To see the second part, consider the following chain of equivalence: $xEy \iff [x]_E = [y]_E \iff p_E(x) = p_E(y)$. □

**Definition 1.28.** Let $E$ be an equivalence relation on set $X$, a function $f : X \to Y$ is $E$-invariant if $xEy \Rightarrow f(x) = f(y)$, i.e., $f$ is constant on equivalence classes.

**Theorem 1.29.** Let $E$ be an equivalence relation on $X$, if $f : X \to Y$ is $E$-invariant, then there is a unique function $g : X/E \to Y$ such that $f = g \circ p_E$.

**Proof.** The theorem is equivalent to the following diagram:

$$
\begin{array}{ccc}
X & \xrightarrow{p_E} & X/E \\
\downarrow{f} & \downarrow{\exists y} \\
Y & & \\
\end{array}
$$

Define function $g$ as follows: for each $C \in X/E$, let $g(C) := f(x)$, for any $x \in C$. Since $f$ is $E$-invariant, this does not depend on the choice of $x \in C$, so $g$ is well-defined.

Moreover, $(g \circ p_E)(x) = g(p_E(x)) = g([x]_E) = f(x)$, this proves the existence of such an $g$.

To see uniqueness, if $f = g \circ p_E$, then for any $x$, $(g \circ p_E)(x) = g([x]_E) = f(x)$, therefore, it’s unique. □
Exercise 1.30. Based on the construction of $g$ above, prove the following:

1. $g$ is injective if and only if the equivalence kernel of $f$ is $E$.
2. $g$ is surjective if and only if $f$ is surjective.
3. If $E_f = E$ and $\text{im } (f) = Y$, then $g$ is a bijection.

Corollary 1.31 (Canonical decomposition theorem). Let $f : X \to Y$, then $f$ can be decomposed as follows:

\[
\begin{align*}
X & \xrightarrow{p} X/E_f & \xleftarrow{b} \text{im } (f) \\
\downarrow{f} & & \downarrow{i} \\
Y & &
\end{align*}
\]

where:

- $p$ is the quotient map $p_E$, which is surjective.
- $i$ is the inclusion map, which is injective.
- $b$ is a bijective map, which is $g$ from 1.29.
2 Functors

In this section, we study the first algebraic structure in this course, which operates on sets and functions.

2.1 Covariant functors

Definition 2.1. A functor (on sets to sets) is a rule \( F \) that assigns each set \( S \) a set \( F(S) \) and to each function \( f : S \rightarrow T \) a function \( F(f) : F(S) \rightarrow F(T) \) such that

1. For each set \( S \), \( F(id_S) := id_{F(S)} \).

2. For any \( f : S \rightarrow T \), \( g : R \rightarrow S \), we have \( F(f \circ g) = F(f) \circ F(g) \).

One can think of a functor \( F \) consists of

- an “object map”: \( \mathcal{F}_O : \text{sets} \rightarrow \text{sets} \).
- a “mapping map”: \( \mathcal{F}_M : \text{functions} \rightarrow \text{functions} \).

Let’s look at some examples of functors to form a better sense of the definition.

Example 2.2. 1. The identity functor, given by \( \text{Id} (S) = S, \text{Id} (f) = f \).

2. Fix a set \( A \), let \( F(S) := A \) for any set \( S \), and let \( F(f) := \text{id}_A \), for any \( f \).

Exercise 2.3. Are there any other functors with \( F(S) \), for any set \( S \)?

3. The powerset functor, given by \( \mathcal{F}(S) = \mathcal{P}(S) \), and for function \( f : S \rightarrow T \), we need to have \( \mathcal{F}(f) : \mathcal{P}(S) \rightarrow \mathcal{P}(T) \). For any subset \( A \subseteq S \), let \( \mathcal{F}(f)(A) := \{ f(a) : a \in A \} \), i.e., the image of \( A \) under \( f \), or \( f(A) \). Let’s verify it’s a functor.

Proof. Notice \( \mathcal{F}(\text{id}_S)(A) = \text{id}_S(A) = A \), and \( \text{id}_{\mathcal{F}(S)}(A) = A \), so they are equal. For composition, we use \( f_* \) as a shorthand notation for \( \mathcal{F}(f) \), then

- \((f \circ g)_*(A) = \{(f \circ g)(a) : a \in A\} = (f \circ g)(A) = f(g(A))\)
- \(f_* \circ g_* (A) = f_*(g_*(A)) = f_*(g(A)) = f(g(A))\)

Again, the composition is preserved. \( \square \)

4. Fix a set \( A \), define the functor to raise sets and functions to the power of \( A \): \( S \mapsto S^A, f \mapsto f^A \). This defines a functor, since in 1.20, we have shown that \((f \circ g)^A = f^A \circ g^A \). Identity is easy to verify.

5. For each set \( S \), let \([S]^{< \infty}\) be the set of all finite subsets of \( S \), define a functor as follows: for each set \( S \), \( \mathcal{F}(S) := [S]^{< \infty} \), and for each function \( f : S \rightarrow T \), \( \mathcal{F}(f) : \mathcal{F}(S) \rightarrow \mathcal{F}(T) \), given by \( \mathcal{F}(f)(A) := \{ f(a) : a \in A \} \). Since input subset \( A \) is finite, output is also finite, so this functor is well-defined.

Definition 2.4. A functor \( \mathcal{G} \) is called a subfunctor of \( \mathcal{F} \) if for any set \( S \), \( \mathcal{G}(S) \subseteq \mathcal{F}(S) \), and for any \( f : S \rightarrow T \), \( \mathcal{G}(f) = (\mathcal{F}(f)) |_{\mathcal{G}(S)} \).
A quick observation: suppose $\mathcal{F}$ is a functor and let $G_0$ be a mapping that assigns each set $S$ a subset $G_0(S) \subseteq \mathcal{F}(S)$, then there is a unique subfunctor $G$ of $\mathcal{F}$ whose object map is $G_0$ if and only if $\text{im}(\mathcal{F}(f)|_{G_0(S)}) \subseteq G_0(T)$, for any $f : S \to T$.

**Example 2.5.** Fix a set $A$, let $\mathcal{F}$ be the functor given by $\mathcal{F}(S) := S^A$, and for each $f : S \to T$, define $\mathcal{F}(f) := f^A$. Let $E$ be an equivalence relation on $A$, let $G_0(S) := \{E\text{-invariant functions } f : A \to S\}$. This gives rise to a subfunctor of $\mathcal{F}$: first, it’s clear that for any set $S$, we have $G_0(S) \subseteq S^A$, our goal is to show that $f^A|_{G_0(S)} : G_0(S) \to G_0(T)$ is well-defined and well-behaved, i.e., $f^A|_{G_0(S)}(g) = f \circ g$, is this function $E$-invariant? Notice that by definition, $g$ is $E$-invariant, so if $a_1 E a_2 \Rightarrow g(a_1) = g(a_2) \Rightarrow f(g(a_1)) = f(g(a_2))$. 
2.2 Universal elements

Definition 2.6. A universal element for a functor $\mathcal{F}$ is a pair $(R, u)$, where $R$ is a set, $u \in \mathcal{F}(R)$ such that for any set $S$ and each $s \in \mathcal{F}(S)$, there exists a unique function $h : R \to S$, satisfying $(\mathcal{F}(h))(u) = s$.

Example 2.7. Fix a set $A$ and an equivalence relation $E$, we have a functor $\mathcal{F}$ that maps $S$ to $\mathcal{F}(S) = \{E$-invariant functions $g : A \to S\}$, and each $f : S \to T$ to $\mathcal{F}(f)$ by $g \mapsto f \circ g$.

What is the universal element of this functor? We need a set $R$, and $u \in \mathcal{F}(R)$, where $u$ is an $E$-invariant function from $A$ to $R$, our goal is to satisfy the universal property, i.e., for all set $S$ and $s : A \to S$ which is $E$-invariant, there is a unique function $h : R \to S$ such that $\mathcal{F}(h)(u) = h \circ u = s$.

Let’s set $R = A/E$, and $u = p_E$, set $h([x]_E) = s(x)$, given such $u$, $h$ must be unique, so $(A/E, p_E)$ is a universal element of functor $\mathcal{F}$.

Example 2.8. Fix sets $A, B$, define $\mathcal{F}(S) = S^A \times S^B$, given $f : S \to T$, define $\mathcal{F}(f)$ by $(g, h) = (f \circ g, f \circ h)$.

Exercise 2.9. Prove it’s a functor.

What is the universal element? It’s called disjoint union of $A$ and $B$. Let $R$ be our target set, $u \in \mathcal{F}(R) = R^A \times R^B = (i, j)$, for set $S$ and $s \in \mathcal{F}(s) = (g, h)$, there is a unique function $f : R \to S$ such that $\mathcal{F}(f)(i, j) = (g, h) = (f \circ i, f \circ j)$.

![](image)

If $A \cap B = \emptyset$, then we can simply set $R = A \cup B$ and $i, j$ be inclusion maps. Set

$$f(x) = \begin{cases} g(x), & \text{if } x \in A \\ h(x), & \text{if } x \in B \end{cases}$$

On the other hand, if $A \cap B \neq \emptyset$, then let $A', B'$ be $A' := A \times \{0\}, B' = B \times \{1\}$, and $i, j$ maps element with an extra bit. By this bit, $f$ has the ability to decode the input. Set

$$f(x) = \begin{cases} g(i^{-1}(x)), & \text{if } x \in A' \\ h(j^{-1}(x)), & \text{if } x \in B' \end{cases}$$

This construction is referred as the disjoint union of $A$ and $B$.

Proposition 2.10. Let $(R, u)$ be a universal element of $\mathcal{F}$, suppose $b : R \to R'$ is a bijection, then $(R', u')$ is also a universal element, where $u' = \mathcal{F}(b)(u)$.

Proof. Take any set $S$ and $s \in \mathcal{F}(S)$, we need to show that there exists a unique $h' : R' \to S$ such that $\mathcal{F}(h')(u') = s$. We separately show the existence and uniqueness.

Existence: since $(R, u)$ is universal, there exists a unique $h : R \to S$ with $\mathcal{F}(h)(u) = s$. Define
\[ h' = h \circ b^{-1}, \] then

\[
\mathcal{F}(h') (u') = \mathcal{F}(h') (\mathcal{F}(b) (u)) \\
= \mathcal{F}(h') \circ \mathcal{F}(b) (u) \\
= \mathcal{F}(h' \circ b) (u) \\
= \mathcal{F}(h \circ b^{-1} \circ b) (u) \\
= \mathcal{F}(h) (u) \\
= s
\]

**Uniqueness:** Notice that we must have \( \mathcal{F}(h' \circ b) (u) = \mathcal{F}(h) (u) \), by uniqueness of \( h \), we must have \( h' \circ b = h \), the only choice for \( h' \) is \( h \circ b^{-1} \).

Next theorem is the converse of above proposition.

**Theorem 2.11** (Uniqueness of universal element). Let \( \mathcal{F} \) be a functor, if \( (R, u), (R', u') \) are universal for \( \mathcal{F} \), then there exists a unique \( b : R \to R' \) such that \( u' = \mathcal{F}(b) (u) \).

**Proof.** Since \( (R, u) \) is universal, there exists a unique \( b : R \to R' \) such that \( \mathcal{F}(b) (u) = u' \). Similarly, \( (R', u') \) is universal, so there exists a unique \( b' \) such that \( \mathcal{F}(b') (u') = u \). It suffices to show \( b \) is a bijection, and \( b' \) is its inverse, i.e., \( b \circ b' = \text{id}_{R'}, b' \circ b = \text{id}_R \).

\[
\mathcal{F}(b' \circ b) (u) = \mathcal{F}(b') \circ \mathcal{F}(b) (u) \\
= \mathcal{F}(b') (u') \\
= u
\]

Apply universal property on \( u \) itself, there exists a unique \( h : R \to R \) such that \( \mathcal{F}(h) (u) = u \). First observe that \( \text{id}_{\mathcal{F}(R)} (u) = u \), and \( \mathcal{F}(\text{id}_R) = \text{id}_{\mathcal{F}(R)} \), \( h \) must be \( \text{id}_R \). On the other hand, \( \mathcal{F}(b \circ b') (u) = u \), which implies \( b \circ b' = h = \text{id}_R \). The other identity is similar.
2.3 Contravariant functors

Definition 2.12. A contravariant functor \( C \) assigns to each set \( S \) a \( C(S) \) and to each \( f : S \to T \) a function \( C(f) : C(T) \to C(S) \) such that

- \( C(\text{id}_S) = \text{id}_{C(S)} \)
- If \( f : S \to T, g : R \to S \), then \( C(f \circ g) = C(g) \circ C(f) \)

Example 2.13 (Contravariant powerset functor). Define \( C \) as follows: \( S \mapsto \mathcal{P}(S), f \mapsto f^* \) by \( f^* : \mathcal{P}(T) \to \mathcal{P}(S), \) for each set \( B \subseteq T, f^*(B) = \{ a \in S : f(a) \in B \}, \) i.e., the preimage \( pf \) under \( f \).

Exercise 2.14. Check it’s a contravariant functor.

Example 2.15. Fix a set \( A \), the following is contravariant: \( S \mapsto A^S, f \mapsto A^f \), i.e., \( f : S \to T, A^f : A^T \to A^S \), and \( A^f(g) = g \circ f \).

Definition 2.16. Let \( C \) be a contravariant functor, a universal element for \( C \) is a pair \((R, u)\), where \( R \) is a set and \( u \in C(R) \), such that for any \( S \) and \( s \in C(S) \), there exists a unique \( h : S \to R \) such that \( C(h)(u) = s \).

Universal element for contravariant functors is very similar to universal element for covariant functors, except for the function \( h \), now its domain is \( S \) and codomain is \( R \).

Example 2.17. Fix sets \( A, B \), define a contravariant functor \( C \) as follows: \( C(S) := A^S \times B^S \), for \( f : S \to T \), define \( C(f) : C(T) \to C(S) \) by \( C(f)(g, h) := (g \circ f, h \circ f) \).

What is the universal element? We want \((R, u), (R', u')\), so \( u = (p, q) \in A^R \times B^R \), for any \( S \) and \( s = (g, h) \in S \), there exists a unique \( f : S \to R \) such that \( s = C(f)(p, q) = (p \circ f, q \circ f) = (g, h) \). Set \( R = A \times B, p(a, b) = a, q(a, b) = b \), and \( f(x) = (g(x), h(x)) \). It’s not hard to check this is a universal element.

Similar to covariant functor, contravariant functor also has a uniqueness theorem for universal element.

Theorem 2.18. If \((R, u), (R', u')\) are universal elements for contravariant functor \( C \), then there exists a unique bijection \( b' : R' \to R \) such that \( u' = C(b')(u) \).
3 Groups

In this section, we study group, one of the most famous algebraic structures, with a simple definition but surprisingly complicated dynamics.

3.1 Concrete groups

**Definition 3.1.** A concrete group on a set $X$ is a set $G$ of bijections $X : \rightarrow X$, such that

1. $\text{id}_X \in G$
2. if $f \in G$, then $f^{-1} \in G$
3. if $f, g \in G$, then $f \circ g \in G$

**Example 3.2.**
1. The set $\{f \in X^X : f$ is a bijection$\}$ is a concrete group on $X$, we call it symmetric group on $X$, denoted by $\text{Sym}(X)$. The elements of $\text{Sym}(X)$ are called permutations.
2. $\{\text{id}_X\}$ is a concrete group.
3. $I = \{f \in \text{Sym}(\mathbb{R}) : \forall x, y \in \mathbb{R}, x < y \Rightarrow f(x) < f(y)\}$ is a concrete group on $\mathbb{R}$.
   (a) $\text{id}_R \in I$
   (b) $f \in I \Rightarrow f^{-1} \in I$. Take $x, y \in \mathbb{R}$ with $x < y$, our goal is to show that $f^{-1}(x) < f^{-1}(y)$. Suppose not, then $f^{-1}(x) > f^{-1}(y)$, but $f$ is increasing, so $f(f^{-1}(x)) > f(f^{-1}(y)) \Rightarrow x > y$, contradicts $x < y$.
   (c) $f, g \in I \Rightarrow f \circ g \in I$, take $x, y \in \mathbb{R}$ with $x < y$, then $g(x) < g(y)$, so $f(g(x)) < f(g(y))$.
4. Let $X \subseteq \mathbb{R}^n$, a bijection $f : X \rightarrow X$ is an isometry if for all $x, y \in X$, $\|x - y\|_2 = \|f(x) - f(y)\|_2$. $\text{Iso}(X) := \{f \in \text{Sym}(X) : f$ is an isometry$\}$ is a concrete group.
5. Let $X \in \mathbb{R}^n$, a bijection $f : X \rightarrow X$ is a homeomorphism if $f$ and $f^{-1}$ are continuous. $\text{Homeo}(X) := \{f \in \text{Sym}(X) : f$ is a homeomorphism$\}$ is a concrete group on $X$.

**Exercise 3.3.** Show that $\{f \in \text{Sym}(X) : f$ is continuous$\}$ might not be a concrete group.

6. Graphs: Let $G = (V, E)$, an automorphism of $G$ is a bijection $f : V \rightarrow V$, such that for any $x, y \in V$ with $\{x, y\} \in E \iff \{f(x), f(y)\} \in E$. $\text{Aut}(G) := \{f \in \text{Sym}(V) : f$ is an automorphism$\}$ is a concrete group on $V$. Below are several graphs illustrated this idea:
The first graph is just a long path, there are only two automorphisms, namely, the identity and flip the entire path, notice no matter the length of this path, there are only these two kinds of automorphisms.

The second graph is a triangle, and $\text{Aut}(G) = \text{Sym}(\{0, 1, 2\})$. Why? No matter how we permute the three vertices, it remains an automorphism, thus, the automorphisms are exactly all permutations.

The last one is a 4-cycle, and $|\text{Aut}(G)| = 8$. To do the counting, we can first put vertex 0: 4 positions to put. Then there are 2 ways to put 1. After that, everything is fixed, so in total $4 \times 2 = 8$ automorphisms.

Two quick definitions: $C_n :=$ cycle of length $n$, and $D_{2n} := C_n$. Perhaps another name for $D_{2n}$ is much more famous: it is the dihedral group of order $2n$, and $|\text{Aut}(G)| = 2n$, we typically use $|D_{2n}|$ to denote this number.

7. Let $G$ be a concrete group on a set $X$, a function $f \in \text{Sym}(G)$ is an automorphism of $G$ if for any $g, h \in G$, $f(g \circ h) = f(g) \circ f(h)$. It is not hard to show that if $f$ is an automorphism of $G$, then $f(id_X) = id_X$, therefore, $\text{Aut}(G) := \{ f \in \text{Sym}(G) : f \text{ is an automorphism of } G \}$ is a concrete group on $G$.

8. Let $X$ be a set and $f \in \text{Sym}(X)$, for $n \in \mathbb{N}$, we write $f^n := f \circ f\cdots \circ f$, $f^0 := id_X$, $f^{n+1} := f \circ f^n$. Also, let $f^{-n} := (f^{-1})^n$.

**Exercise 3.4.** For any $n, m \in \mathbb{Z}$, show that:

(a) $f^{-n} = (f^n)^{-1}$
(b) $(f^n)^m = f^{nm}$
(c) $f^n \circ f^m = f^{n+m}$

From this, it follows that $\langle f \rangle := \{ f^n : n \in \mathbb{Z}\}$ is a concrete group on $X$, this group is called the cyclic group generated by $f$.

Now let’s dive deeper into the study of dihedral group. It is useful to keep the following picture of dihedral group $D_{2n}$ in mind:

$D_{2n}$ is just all automorphisms on the cycle of length $n$, and for $n \geq 3$, we have $|D_{2n}| = 2n$. Consider the following 2 elements of $D_{2n}$:
• \( g := \) i.e., \( g \) rotates the cycle to the left, by 1.

• \( h := \) i.e., \( h \) flips the cycle along the fixed 0 axis.

**Proposition 3.5.** Elements of \( D_{2n} \) are \( \text{id} = g^0, g^1, g^2, \ldots, g^{n-1} \), and \( h = g^0 \circ h, g^1 \circ h, g^2 \circ h, \ldots, g^{n-1} \circ h \).

**Proof.** Take any \( f \in D_{2n} \), let \( k := f (0) \), we wish to express \( f \) either as \( g^k \) or \( g^k \circ h \), let \( f' := g^{-k} \circ f \), clearly, \( f'(0) = g^{-k} \circ f (0) = g^{-k} (k) = 0 \), so \( f' \) is either \( \text{id} \) or \( h \). Moreover, we can write \( f \) as \( g^k \circ f' \), this completes the proof. \( \square \)

**Exercise 3.6.** For each \( k, \ell, \) compute \( (g^k \circ h^\ell)(0) \) and \( (g^k \circ h^\ell)(1) \), and conclude that \( 2n \) functions listed in the claim are distinct.

**Proof Sketch.** For different \( k, \ell, (g^k \circ h^\ell)(0) \) must be different. For fixed \( k, g^k (1) \neq g^k \circ h (1) \). \( \square \)

Observe that \( D_{2n} \) is the smallest group containing \( g, h \). Indeed, if \( G \) is a group containing \( g, h \), then for any \( k, \ell, g^k \circ h^\ell \in G \), so \( D_{2n} \subseteq G \). We say that \( D_{2n} \) is generated by \( g, h \).

**Lemma 3.7.** Let \( X \) be a set, \( \mathcal{G} \) be a set of concrete groups of \( G \), define \( \bigcap \mathcal{G} := \{ f \in \text{Sym}(X) : \forall G \in \mathcal{G}, f \in G \} \). Then \( \bigcap \mathcal{G} \) is also a concrete group.

**Proof.** 1. \( \text{id}_X \in \bigcap \mathcal{G} \), since for any \( G, \text{id}_X \in G \).
2. if \( f \in \bigcap G \), then \( f^{-1} \in \bigcap G \), to see this, notice that for any \( G \), \( f \in G \), and \( G \) is a concrete group, so for any \( G \), \( f^{-1} \in G \Rightarrow f^{-1} \in \bigcap G \).

3. if \( f, g \in \bigcap G \), then apply the same argument, \( f \circ g \in \bigcap G \).

**Definition 3.8.** If \( S \subseteq \text{Sym}(X) \), then \( \langle S \rangle := \bigcap \{ G : G \text{ is a concrete group on } X \text{ such that } S \subseteq G \} \) is a concrete group by 3.7, furthermore, \( S \subseteq \langle S \rangle \), so \( \langle S \rangle \) is the smallest group containing \( S \) as a subset. \( \langle S \rangle \) is called the group generated by \( S \).

For example, if \( f \in \text{Sym}(X) \), then \( \langle f \rangle = \langle \{ f \} \rangle \), and more generally, we write \( \langle \{ f_1, f_2, \ldots, f_n \} \rangle \) as \( \langle f_1, f_2, \ldots, f_n \rangle \), e.g., with \( g, h \in D_{2n} \), we have \( D_{2n} = \langle g, h \rangle \).

The next proposition will show that, we can write elements of \( \langle S \rangle \) in a more structured way.

**Proposition 3.9.** Let \( X \) be a set, \( S \subseteq \text{Sym}(X) \), then
\[
\langle S \rangle = \{ g_1^{\epsilon_1} \circ g_2^{\epsilon_2} \circ \ldots \circ g_k^{\epsilon_k} : k \in \mathbb{N}, g_1, \ldots, g_k \in S, \epsilon_1, \ldots, \epsilon_k \in \{-1, 1\} \}
\]

**Proof.** Let \( H \) denote the set on RHS, clearly, \( H \subseteq \langle S \rangle \), and also, \( S \subseteq H \). So to argue for the other inclusion, it suffices to show \( H \) is a group, then we will have \( \langle S \rangle \subseteq H \) automatically.

- Take \( k = 0 \), we have \( g_0 = \text{id}_X \in H \).
- Suppose \( f \in H = g_1^{\epsilon_1} \circ \ldots \circ g_k^{\epsilon_k} \), then \( f^{-1} = g_k^{-\epsilon_k} \circ g_{k-1}^{-\epsilon_{k-1}} \circ \ldots \circ g_2^{-\epsilon_2} \circ g_1^{-\epsilon_1} \in H \).
- If \( f, g \in H \), then it’s clear \( f \circ g \in H \): we just express it by adding a \( \circ \) between the representation of \( f \) and \( g \).

Let’s look at some examples of groups generated by a set of elements.

**Example 3.10.**
1. Rubik’s cube: let \( X \) be a set of cardinality 48, and \( S := \) set of 6 individual rotations, viewed as permutations on \( X \). The Rubik’s group is \( \langle S \rangle \).

2. The lamplighter group is defined as follows: \( X = \{0, 1\}^\mathbb{Z} \times \mathbb{Z} \), and there are two functions:
   - \( g : \) move to the next light, i.e., \( g(x, n) := (x, n + 1) \).
   - \( h : \) switch the light the person is currently standing by, i.e., \( h(x, n) := (x', n) \), where
     \[
     x'_i = \begin{cases} 
     1 - x_i, & \text{if } i = n \\
     x_i, & \text{otherwise}
     \end{cases}
     \]
     We use \( \langle g, h \rangle \) to denote the lamplighter group.
3.2 Abstract groups

Definition 3.11. A binary operation on a set $S$ is a function $\star : S \times S \to S$.

Example 3.12. 1. If $G$ is a concrete group on $X$, then $\circ : G \times G \to G$ is a binary operation, where $\circ (f, g) = f \circ g$. Note: $\star$ is always written as an infix operator.

2. There are tons of binary operations on $\mathbb{Z}$: $+$ on $\mathbb{Z}$, $\ast$ on $\mathbb{Z}$, and $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$: $(n, m) \mapsto n$.

Definition 3.13. A binary operation $\star : S \times S \to S$ is associative if $\forall a, b, c \in S : (a \star b) \star c = a \star (b \star c)$.

Definition 3.14. Let $\star$ be a binary operation on $S$, then an element $e \in S$ is an identity for $\star$ if for all $a \in S$, $a \star e = e \star a = a$.

Lemma 3.15. Let $\star$ be a binary operation on $S$, then $\star$ has at most one identity.

Proof. Suppose both $e$ and $e'$ are identities for $\star$, then $e \star e' = e = e'$.

Definition 3.16. Let $\star$ be a binary operation with identity element $e$ on $S$, an inverse of an element $a$ is an element $b \in S$ such that $a \star b = b \star a = e$.

Exercise 3.17. Given an example of a binary operation $\star$ with identity such that there is an element with more than one inverse.

You can intentionally assign two elements as inverse to some element, then force those two elements to be different from each other.

Lemma 3.18. If $\star$ is associative, with identity $e$, then for any $a \in S$, if it has inverse, then it has at most one inverse.

Proof. Suppose $b, b'$ are inverses of $a$, then compute $b \ast a \ast b' = (b \ast a) \ast b' = e \ast b' = b'$, on the other hand, $b \ast a \ast b' = b \ast (a \ast b') = b \ast e = b$, by associativity, we have $b = b'$.

After setting up enough definitions, we are ready to define abstract groups.

Definition 3.19. An abstract group, or group for short, is a set $G$ with a binary operation $\star$ such that

- $\star$ is associative.
- $\star$ has an identity.
- each $a \in G$ has an inverse with respect to $\star$.

The main example: if $G$ is a concrete group on $X$, then $(G, \circ)$ is a group.

Some quick examples: $(\mathbb{N}, +)$ is not a group, but $(\mathbb{Z}, +)$ is a group. $(\mathbb{R}, \ast)$ is not a group, but $(\mathbb{R} \setminus \{0\}, \ast)$ is a group.

Exercise 3.20. Let $X$ be a set, recall $\triangle$ is the symmetric difference operation on two sets, then $(\mathcal{P}(X), \triangle)$ is a group.

Some more examples of groups:
Example 3.21. 1. \(\mathbb{Z}/n\mathbb{Z}\): let \(n \geq 2\) be an integer, and \(\mathbb{Z}_n = \{0, 1, \ldots, n-1\}\), \(+_n\) : addition modulo \(n\), i.e., for \(x, y \in \mathbb{Z}_n\), define \(x +_n y\) to be the remainder of \(x + y\) after divided by \(n\). Then, \((\mathbb{Z}_n, +_n)\) is a group. Please verify this. The nasty part is to verify that \(+_n\) is associative.

2. Elliptic curves: An elliptic curve is the set of points \((x, y) \in \mathbb{R}^2\), satisfying an equation of the form \(y^2 = x^3 + ax + b\), for example, \(y^2 = x^3 - x + 1\). We denote the set by \(E\). Let’s illustrate this with diagram:

Let \(\ast\) be an extra element not in \(E\), define an operation \(\oplus\) on \(E \cup \{\ast\}\) as follows: \(P \oplus Q \Rightarrow\) take tangent of the line \(PQ\), find its third intersection with \(E\), then flip that point with respect to \(x\) axis. What if \(PQ\) intersects \(E\) only on \(P\) and \(Q\)? For example, consider

Then define \(P \oplus Q = \ast\). For all \(P \in E\), define \(\ast \oplus P = P \oplus \ast = P\), and \(\ast \oplus \ast = \ast\), i.e., \(\ast\) is the identity element. This turns \(E \cup \{\ast\}\) into a group.

3. Let \(G\) be a connected graph, fix a vertex \(x \in V(G)\), define \(\Pi_1(G, x)\), the homotopy group of \(G\), as follows:

\[\Pi_1(G, x) := \{\text{all non-backtracking closed walks in } G, \text{ start and end at } x\}\]

Here, non-backtracking just means if you have used edge \((u, v)\), you cannot immediately take the edge \((v, u)\).
Given two walks \( u \) and \( w \), \( u \cdot w \) is the walk obtained from \( u \) and \( w \) by concatenating them and removing all backtrack edges. For example,

This defines a group.

**Theorem 3.22** (Cayley). Every abstract group is isomorphic to a concrete group, i.e., for all groups \((G, \ast)\), there exists a set \(X\), a concrete group \(H\) on \(X\), and a bijection \(\varphi : G \to H\), such that for all \(f, g \in G\), we have \(\varphi(f \ast g) = \varphi(f) \circ \varphi(g)\).

*Proof.* Take \(X = G\). For each \(g \in G\), let \(\varphi(g) : G \to G\) be the function given by \(\varphi(g)(h) := g \ast h\). We prove a sequence of propositions, to show that this \(\varphi\) gives us the desired result.

**Proposition 3.23** (Closure of \(\varphi\)). For all \(f, g \in G\), \(\varphi(f \ast g) = \varphi(f) \circ \varphi(g)\).

*Proof of Closure.* Take \(h \in G\). \(\varphi(f \ast g)(h) = (f \ast g) \ast h\), while \(\varphi(f) \circ \varphi(g)(h) = \varphi(f)(g \ast h) = f \ast (g \ast h)\). By associativity of \(\ast\), the identity holds.

The next part will focus on proving \(\varphi\) is an isomorphism, i.e., it is a bijection. By 3.23, we need to show the following:

**Proposition 3.24.** Let \(e\) be the identity of \(G\), then \(\varphi(e) = \text{id}_G\).

*Proof of identity.* Take \(h \in G\), \(\varphi(e)(h) = e \ast h = h\), for all \(h\), so \(\varphi(e) = \text{id}_G\).

The next proposition will be useful in finding our concrete group \(H\).

**Proposition 3.25.** For all \(g \in G\), \(\varphi(g)\) is a bijection.

*Proof of \(\varphi(g)\) bijectivity.* We claim that the inverse of \(\varphi(g)\) is \(\varphi(g^{-1})\).

\[
\varphi(g) \circ \varphi(g^{-1}) = \varphi(g \ast g^{-1}) = \varphi(e) = \text{id}_G
\]

\[
\varphi(g^{-1}) \circ \varphi(g) = \varphi(g^{-1} \ast g) = \varphi(e) = \text{id}_G
\]

So we can view \(\varphi\) as a function from \(G\) to \(\text{Sym}(G)\), where \(H := \text{im}(\varphi) = \{\varphi(g) : g \in G\}\).

**Proposition 3.26.** \(H\) is a concrete group on \(G\).

*Proof of \(H\) is a concrete group.*

- \(\text{id}_G \in H\), since \(e \in G\), \(\varphi(e) \in H\).
- If \(f \in H\), then \(f^{-1} \in H\): suppose \(f = \varphi(g)\) for some \(g \in G\), then \(f^{-1} = \varphi(g^{-1}) \in H\).
• If $f_1, f_2 \in H$, then $f_1 \circ f_2 \in H$: since $\varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 \ast g_2) \in H$.

Finally, we are ready to show $\varphi$ is a bijection.

**Proposition 3.27.** $\varphi : G \to H$ is a bijection.

**Proof.** Surjectivity comes from definition of $H$: it is im($\varphi$). What about injectivity? If $\varphi(g_1) = \varphi(g_2)$, then $\varphi(g_1)(e) = g_1 \ast e = g_1 = \varphi(g_2)(e) = g_2 \ast e = g_2$.

This completes the proof of Cayley’s theorem.

Let’s examine 3.22 on Dihedral group. Recall $D_{2n} = \langle g, h \rangle$, where $g$ is rotate by 1, and $h$ is flip with respect to 0 axis. What is $\varphi(g)$? If we apply it to other elements, the result will be further shifted by 1. What about $\varphi(h)$? It will flip all elements.
3.3 Abelian groups, subgroups, homomorphisms

In this section, we extend more on structures of abstract groups. We introduce three important concepts, that will be used across all later sections.

We first introduce some conventions, to simplify the notation. Often, we just say “G is a group” without mentioning the operation. In such case, the operation is called “multiplication” and denoted by $a \cdot b$ or simply $ab$. There’s a notable exception, i.e., groups with addition, such as $(\mathbb{Z}, +)$.

**Definition 3.28.** A binary operation $\star$ on set $S$ is **commutative** if order does not matter, i.e., $a \star b = b \star a$, for any $a, b \in S$.

**Definition 3.29.** If $(G, \star)$ is a group and $\star$ is commutative, we say that $(G, \star)$ is an **abelian group**. In this case, often the operation is denoted by “+”. We write $-x$ for $x^{-1}$, and 0 as identity. Also, $nx$ is used to denote $x^n$.

An exception to the above convention: $(\mathbb{Q} \setminus \{0\}, \cdot)$ is abelian.

**Definition 3.30.** Let $(G, \star)$, $(H, \cdot)$ be groups, a function $\varphi : G \rightarrow H$ is a **homomorphism** if $\varphi (g \star h) = \varphi (g) \cdot \varphi (h)$. 

**Exercise 3.31.** If $\varphi : G \rightarrow H$ is a homomorphism, where $G, H$ are groups with identities $e_G, e_H$, then $\varphi (e_G) = e_H$, and for all $g \in G$, $\varphi (g^{-1}) = (\varphi (g))^{-1}$.

It’s not hard to see that, for any $g \in G$, $\varphi (g) = \varphi (g \cdot e_G) = \varphi (g) \cdot \varphi (e_G)$, so $\varphi (e_G) = e_H$. A similar argument can be used to show the inverse part.

Given the definition of homomorphism, it is natural to ask: if we have two groups $G, H$, does there exist a homomorphism from $G$ to $H$? The answer is yes. Simply map every element of $G$ to $e_H$, then this is a valid homomorphism. Remarkably, one can show that this is the only valid homomorphism between certain groups.

**Exercise 3.32.** Consider $(\mathbb{Z}_n, +)$ as a group, show that there is no non-trivial homomorphism from $\mathbb{Z}_4$ to $\mathbb{Z}_7$.

We have seen the definition of isomorphism between two sets before, here we extend it to groups.

**Definition 3.33.** A bijective homomorphism from $G$ to $H$ is called an **isomorphism**. If an isomorphism from $G$ to $H$ exists, we say that $G$ and $H$ are **isomorphic**, denoted by $G \cong H$.

**Exercise 3.34.** Show that the inverse of an isomorphism from $G$ to $H$ is an isomorphism from $H$ to $G$.

Recall that in 3.22, our argument has showed that the map from $G$ to Sym $(G)$ by $g \mapsto (h \mapsto gh)$ is an injective homomorphism. We abstract this intuition further.

**Definition 3.35.** Let $(G, \star)$ be a group. Given a subset $S \subseteq G$, define $\star_S : S \times S \rightarrow G$ by $a \star_S b = a \star b$. If $\star_S$ is a binary operation on $S$, i.e., $\text{im} (\star_S) \subseteq S$, and $(S, \star_S)$ is a group, then $(S, \star_S)$ or $S$ is called a **subgroup** of $G$, denoted by $S \leq G$.

**Lemma 3.36.** Let $G$ be a group, $S \subseteq G$, then $S \leq G$ if and only if the following conditions hold:

1. $e \in S$
2. If \( g \in S \), then \( g^{-1} \in S \).
3. If \( g, h \in S \), then \( gh \in S \).

In particular, a concrete group on set \( X \) is the same as a subgroup of \( \text{Sym}(X) \).

**Proof.** (\( \Leftarrow \)) : By the three conditions, \( S \) is a group, and \( S \) is closed under group operation, so \( S \leq G \).

(\( \Rightarrow \)) : Suppose \( S \leq G \), condition 3 holds by definition, it suffices to show the other two conditions.

1. We need to show \( e_S = e \). The first observation is, for any element \( g \in G \), if \( g^2 = g \), then \( g = e \). Why? Given \( g^2 = g \), we can multiply both sides by \( g^{-1} \), get \( g = e \). Indeed, \( e^2_S = e_S \), so \( e_S = e \).

2. We need to show that, if \( g \in S \) and \( h \) is the inverse of \( g \) in \( S \), then \( h = g^{-1} \). Indeed, \( gh = hg = e_S = e \), and \( h = g^{-1} \), as desired.

**Proposition 3.37.** Suppose \( \varphi : G \to H \) is a homomorphism, then \( \text{im}(\varphi) \leq H \).

**Proof.** It suffices to check three conditions in 3.36.

- Since \( \varphi(e_G) = e_H \), we have \( e_H \in \text{im}(\varphi) \).
- Suppose \( h \in \text{im}(\varphi) \), then there exists some \( g \in G \) such that \( \varphi(g) = h \). Since \( (\varphi(g))^{-1} = \varphi(g^{-1}) \), \( h^{-1} \in \text{im}(\varphi) \).
- Suppose \( h_1, h_2 \in \text{im}(\varphi) \), then there exists \( g_1, g_2 \in G \) being mapped to them by \( \varphi \). Since \( \varphi \) is a homomorphism, we have \( h_1 h_2 = \varphi(g_1 g_2) \), so \( h_1 h_2 \in \text{im}(\varphi) \).

Observe that if \( \varphi \) is injective, then trivially, we have \( G \cong \text{im}(\varphi) \).
3.4 Actions, cosets, orbits

Groups are interesting structures with nice property we can leverage. Can we extend it to arbitrary set? We do so by defining action.

Definition 3.38. Let $G$ be a group, an action on a set $X$ is a homomorphism $\alpha : G \to \text{Sym}(X)$.

For notations, we usually denote domain and codomain of $\alpha$ as $\alpha : G \acts X$, and often, instead of $\alpha(g)(x)$, we write $g \cdot x$ or $g \cdot x$ if $\alpha$ is clear from context.

Example 3.39. 1. Consider $\alpha : G \acts G$ given by $g \cdot h = gh$, this is called the left multiplication action.

2. $\alpha : G \acts G$ given by $g \cdot h = hg^{-1}$, this is called the right multiplication action. Let’s verify it is an action. Suppose $g_1, g_2, h \in G$, then $(g_1g_2) \cdot h = h(g_1g_2)^{-1} = hg_2^{-1}g_1^{-1} = g_1 \cdot (hg_2^{-1}) = g_1 \cdot g_2 \cdot h$.

Moreover, the map $G \to G : h \mapsto hg^{-1}$ is a bijection, we left to reader to check this.

3. The trivial action: $G \acts X : g \cdot x = x$, for all $g \in G, x \in X$.

Definition 3.40. A right action of $G$ on $X$ is a function $\beta : G \to \text{Sym}(X)$, such that for all $g_1, g_2 \in G$, $\beta(g_1g_2) = \beta(g_2) \circ \beta(g_1)$. We usually write it as $\beta : X \acts G$, and $x \cdot \beta g$ or $x \cdot g$ for $\beta(g)(x)$. With this notation, the requirement of $\beta$ can be written as $(x \cdot g_1) \cdot g_2 = x \cdot (g_1g_2)$.

So we can define right multiplication action via $h \cdot g = hg$, also, $h \cdot g = g^{-1}h$.

Definition 3.41. The shift action $\sigma : G \acts \mathcal{P}(G)$, defined as $g \cdot S := gS := \{gh : h \in S\}$.

Notice that $\mathcal{P}(G) \cong \{0, 1\}^G$, so we can view this action as $G \acts \{0, 1\}^G$. More generally, there is a shift action $G \acts X^G$ for any set $G$: take $g \in G, f \in X^G$, then $g \cdot f \in X^G$ is a function $G \to X$, given by $(g \cdot f)(h) := f(g^{-1}h)$, for all $h \in G$. It is instrumental for the reader to verify this is in fact an action.

Even more generally, given any action $G \acts Y$, we can “lift” it to an action $G \acts X^Y$: for $f \in X^Y$, define $g \cdot f : y \mapsto f(g^{-1} \cdot y)$.

An important type of action to study is actions of $(\mathbb{Z}, +)$. What does this kind of actions look like? Let $\alpha : \mathbb{Z} \acts X$, then $\alpha(0) = \text{id}_X$, suppose $\alpha(1) := f \in \text{Sym}(X)$, then $\alpha(n) = f^n$, for all $n \in \mathbb{Z}$. This is true, since we can view $\mathbb{Z}$ as generated by 1, since $\alpha$ is a homomorphism, it must preserve such a structure. Thus, there is a natural bijection between $\{\text{actions of } \mathbb{Z} \acts X\}$ and $\text{Sym}(X)$, given by $\alpha \mapsto \alpha(1)$.

Example 3.42. Consider $\alpha : \mathbb{Z} \acts [6]$, given by $\alpha(1) = \begin{bmatrix} 3 \\ 1 \\ 5 \\ 2 \\ 4 \\ 6 \end{bmatrix}$. We write in a vector form, since essentially, $\text{Sym}([6])$ are permutations, so we just need to specify where does each number go. The
following diagram illustrates this action: