Group Theory

Patrick Oare

Groups are the simplest algebraic objects that have interesting properties, as we briefly saw in the introduction to this chapter. We'll now discuss them much more thoroughly, as they are one of the most fundamental things to learn and understand if you want to do higher-level math.

Definition 1: Group (Abelian)

A group is a pair $(G, \cdot)$ consisting of a set G and a binary operation $\cdot : G \times G \to G$, often called *multiplication*, such that

1. $\cdot$ is *associative*: $\forall g, h, i \in G$, $g \cdot (h \cdot i) = (g \cdot h) \cdot i$.
2. $\cdot$ has *identity*: There exists $e \in G$ (also often denoted $1 \in G$, or 0 if the group operation is addition[a]) such that $e \cdot g = g \cdot e = g$ for each $g \in G$.
3. $\cdot$ is *invertible*: For each $g \in G$, there is an inverse element, denoted $g^{-1} \in G$, such that $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

We will often abbreviate $gh := g \cdot h$. We call the group **abelian** if it satisfies a fourth property,

4 $\cdot$ is *commutative*: For each $g, h \in G$, $g \cdot h = h \cdot g$.

[a] The group operation is often thought of as multiplication, which is why the identity is often labeled as 1 instead of e, since 1 is the multiplicative inverse. I often prefer to use 1 instead of e, but when learning it can be detrimental because many examples of groups use addition as their group operation: for example, the integers $(\mathbb{Z}, +)$. In this case, the identity element (because the group operation is $+$) is $0 \in \mathbb{Z}$, so we denote $e = 0$. If we use $1 \in G$ to represent the identity, then we have to consider $0 \in \mathbb{Z}$ as the group identity $1 \in G$. It is often also convenient for *abelian* groups to denote the identity as 0, since the canonical example of an abelian group is addition.

While abelian groups are extremely important, much of group theory can be done with just the first 3 axioms. We will state when abelian groups have special properties and when groups are abelian, but this chapter will be focused on properties of general groups, so we will assume $\cdot$ is *not* commutative unless we specify that the group is abelian.

The group operation (which I will often call the *law* of the group at hand) can be summarized in a **multiplication table**. A multiplication table shows the result of every product that you can take in the group, and is a good way to explicitly show the structure of a small group. It only really works if the group is small, but if it is representable in a table, then the multiplication table tells you the entire structure of the group.

For the rest of this chapter, we'll let $(G, \cdot)$ be an arbitrary group. Like in the vector space case, this definition comes with a number of immediate corollaries that can be easily proved.

Proposition 1: First properties of groups

The identity element $e \in G$ is unique, and for each $g \in G$, the inverse g^{-1} is unique. Furthermore, the inverse of g^{-1} is g, i.e. $(g^{-1})^{-1} = g$. Finally, the inverse of two elements is their inverses in reverse order:

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}. \tag{1}$$

Groups revolve around the identity element e. This is the most important element, and we often want to know "how long it will take" for a group element to get back to 1. We'll see examples of this in the future.

Definition 2: Order of a group $|G|$ and an element $|g|$

The **order** of a group G is simply its cardinality, $|G|$. For $g \in G$, we use the shorthand,

$$g^n := \underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ times}}, \tag{2}$$

with $g^0 := e$ (this is well-defined because of associativity of $\cdot$). The **order** of an element $g \in G$, denoted $|g|$, is the smallest $n \in \mathbb{N}$ (here $0 \notin \mathbb{N}$) such that

$$g^n = e. \tag{3}$$

If $g^n \neq e$ for any $n \geq 1$, then we say g has infinite order, $|g| = \infty$.

We will often be interested in finite groups, $|G| < \infty$, as these have many interesting combinatorial applications and can be easily classified. Note that if $|g| = n$, then $g^{-1} = g^{n-1}$. The study of infinite groups, and in particular, uncountably infinite groups like $(\mathbb{R}, +)$, will be left to a later chapter on Lie theory.

As always, we need to define sub-objects of a group, which are called subgroups. These are subsets which are closed under the group operation.

Definition 3: Subgroup

A **subgroup** of a group G is a subset $H \subseteq G$ such that:

1. H contains the identity, $e \in H$.
2. H is closed under group multiplication: for all $h_1, h_2 \in H$, $h_1 \cdot h_2 \in H$.
3. H is closed under group inverse: for all $h \in H$, $h^{-1} \in H$.

We denote $H \leq G$ to mean that H is a subgroup of G.

Any (non-trivial) group contains two trivial subgroups: the identity subgroup $\{1\} \leq G$, and the entire group $G \leq G$. Here's a question for thought: if h is closed under group multiplication and inverses, then for $h \in H$, h^{-1} is also in H, and likewise $e = h \cdot h^{-1} \in H$. So, why do we need the first condition of Def. (3) that imposes that $e \in H$?

Like in the vector space case where there is a slightly simpler method to determine if a subset is a sub-object.

Proposition 2: Subgroup criterion

A subset $H \subseteq G$ is a subgroup of G iff H is non-empty and if, for each $h_1, h_2 \in H$, we have $h_1 h_2^{-1} \in H$.

This criterion works because we can simplify down all the necessary conditions for a subgroup by using this formula. Because $H \neq \emptyset$, I can take $h \in H$ and the criterion implies that $e = h \cdot h^{-1} \in H$. It also tells me that H is closed under inverses, because $e, h \in H$ implies $e \cdot h^{-1} = h^{-1} \in H$. Finally, H must be closed under $\cdot$, because if $h_1, h_2 \in H$, then $h_2^{-1} \in H$, hence $h_1 \cdot (h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$.

This is our second example of a sub-object: the first was the notion of a subspace of a vector space. We'll see throughout these notes that sub-objects are all very similar: they are simply subspaces which are closed with respect to whatever algebraic operation we've imposed on our space of interest. In this case, a subgroup is just a subset which is a group; in the vector space case, a subspace is just a subset which is a vector space.

Like how subgroups mirror the notion of subspaces, group homomorphisms mirror the notion of linear transformations. I often call linear transformations "vector space homomorphisms" to make the connection clear: a **homomorphism** is simply a structure-preserving map.

Definition 4: Group homomorphism and isomorphism

Let G, G' be two groups. A **group homomorphism** between G and G' is a map

$$\phi : G \longrightarrow G' \tag{4}$$

such that for each $g_1, g_2 \in G$, we have

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2). \tag{5}$$

If ϕ is also a bijection, we say ϕ is a **group isomorphism**. In this case we also say G and G' are **isomorphic**, denoted $G \cong G'$.

Group homomorphisms allow us to *translate the group structure from one group to another*: in $\phi(g_1 \cdot g_2)$, the group multiplication is in G, but for $\phi(g_1) \cdot \phi(g_2)$, the group multiplication is in G'. Because of this, group homomorphisms tell us that *the two groups involved have similar group structures*. An isomorphism makes this even stronger: like in the vector space case, isomorphism means two groups are **equivalent** as groups: there is a one-to-one correspondence between the groups that *respects their group structure*. Isomorphism is the

strongest statement you can make about groups short of saying they are equal: functionally, if two groups are isomorphic, they are the same object, they might just be labeled differently. Much of group theory is about searching for isomorphisms: if you understand G as a group and know that $G \cong G'$, then you also understand G'.

Definition 5: Kernel, Image

Let $\phi : G \to G'$ be a group homomorphism. The **kernel** of ϕ is defined as

$$\ker(\phi) := \{g \in G : \phi(g) = e \in G'\}. \tag{6}$$

The **image** of ϕ is defined as in any map,

$$\mathrm{im}(\phi) := \{g' \in G' : \exists g \in G \text{ s.t. } g' = \phi(g)\}. \tag{7}$$

The kernel and image of homomorphisms play a special role in the study of group theory because, like in the vector space case where they were always subspaces, they are *automatically* subgroups of the domain and codomain of the map, respectively. We will soon see that the kernel actually has more properties than the image: the kernel is actually called a **normal subgroup**, which is very important to the theory of quotient groups that we'll be exploring later.

Proposition 3: Kernel and image are subgroups

Let $\phi : G \to G'$ be a homomorphism between non-empty groups. Then, $\ker(\phi) \subseteq G$ is a subgroup of G, and $\mathrm{im}(\phi) \subseteq G'$ is a subgroup of G'.

Proof. This proof proceeds in much the same way as the vector space case. Clearly neither $\ker(\phi)$ nor $\mathrm{im}(\phi)$ is empty, since $e_G \in \ker(\phi)$ and $e_H = \phi(e_G) \in \mathrm{im}(\phi)$. Let $g_1, g_2 \in \ker(\phi)$. Then,

$$\phi(g_1 \cdot g_2^{-1}) = \phi(g_1) \cdot \phi(g_2)^{-1} = e \cdot e = e \implies g_1 \cdot g_2^{-1} \in \ker(\phi). \tag{8}$$

A similar equality holds for $g_1', g_2' \in \mathrm{im}(\phi)$. In this case, $g_1' = \phi(g_1)$ and $g_2' = \phi(g_2)$, so $g_1' \cdot g_2'^{-1} = \phi(g_1) \cdot \phi(g_2)^{-1} = \phi(g_1 \cdot g_2^{-1}) \in \mathrm{im}(\phi)$. □

Proposition 4

A group homomorphism $\phi : G \to G'$ is injective iff $\ker(\phi) = \{e\}$ is trivial, and surjective if $\mathrm{im}(\phi) = G'$. ϕ is an isomorphism iff $\ker(\phi) = \{e\}$ and $\mathrm{im}(\phi) = G'$.

We won't prove the last claim because the proof is essentially the same as the vector space case.

Definition 6: Embedding

An **embedding** of a group H into a group G is an injective group homomorphism $\phi : H \hookrightarrow G$ (equivalently, ϕ has trivial kernel $\ker \phi = \{e\}$). We denote an embedding

with $\hookrightarrow$.

If $H \leq G$ is a subgroup of G, we say that the subgroup H is **embedded** into the larger group G, denoted with

$$H \hookrightarrow G. \tag{9}$$

We'll discuss this more soon, but what this really means is that although H is defined in terms of G, H can exist on its own as its own separate entity. Because subgroups are groups in their own right, we don't need to reference G to discuss the properties of H: H is closed under the group operation. Note that if $H \leq G$, then there is a canonical injective group homomorphism, called the **inclusion map**,

$$\iota : H \hookrightarrow G \qquad\qquad (h \in H) \mapsto (h \in G). \tag{10}$$

The inclusion map does nothing: H is a subset of G, so it simply sends each element of H to itself, now recognized as an element of G. This map is clearly a homomorphism, and must be injective because it has no kernel. Hence by Definition 6, ι embeds H into G.

We'll see in Section 1.3 that if we are given an embedding $\iota : G' \hookrightarrow G$ of two groups, even if G and G' are defined completely separately with nothing in common, the existence of an embedding means that there is a subgroup $H \leq G$ that is isomorphic to G', $G \cong H \leq G$. What this means in English is that such an embedding shows us that G' can be identified *as a subgroup* of G, despite not necessarily being defined as a subset of G. We'll see an example of this in the examples as $D_{2n} \hookrightarrow S_n$.

Example 1: The logarithm as a homomorphism

There are many different group structures that we can impose on subsets of the real numbers. The two examples that we will consider are the real numbers under addition, $(\mathbb{R}, +)$, and the positive real numbers under multiplication, $(\mathbb{R}_{>0}, \cdot)$. These groups appear to be quite different, but in fact they are homomorphic: the homomorphism is a function you know quite well,

$$\log : (\mathbb{R}_{>0}, \cdot) \longrightarrow (\mathbb{R}, +) \qquad\qquad x \mapsto \log x. \tag{11}$$

How do we know this is a group homomorphism? It's simply encoded in the fact that the logarithm factors[a], as you learned in 11th grade,

$$\log(a \cdot b) = \log a + \log b. \tag{12}$$

This structure is exactly that of a group homomorphism between $(\mathbb{R}_{>0}, \cdot)$ and $(\mathbb{R}, +)$! What is the kernel and image of log? The kernel is the set of elements sent to 0, the additive identity, and is clearly just the singleton

$$\ker \log = \{1\}. \tag{13}$$

Note that this is just the identity element of $(\mathbb{R}_{>0}, \cdot)$: although we are using the same base set $\mathbb{R}$ for both groups, they have different identities (0 and 1, respectively) under the corresponding group operation. The image is also the entire space $\mathbb{R}$, because for any $x \in \mathbb{R}$, we have $\log e^x = x$. Thus, log is not only a homomorphism, but is in fact

an isomorphism– The additive group $(\mathbb{R}, +)$ and the multiplicative group $(\mathbb{R}_{<0}, \cdot)$ have the exact same group structure!

[a]Whenever we use a logarithm in these notes, it will be natural log: I don't see a reason to ever really use a different base.

Before we discuss anything else, let's go into some basic examples that we'll be using.

0.1 Examples

Do any of the number systems that we have discussed $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R})$ form a group? When we ask this question, we need to think about *what operation* we are asking if they form a group under. Each of these systems has two operations: addition and multiplication. When we ask "does this set form a group", we ask that question in relation to a given operation[1]. Under the addition operation, note that $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ each form a group: they have associative addition, they each have an additive identity (0), and they each contain additive inverses (negative numbers). On the other hand, $\mathbb{N}$ *does not* contain negative numbers, hence $(\mathbb{N}, +)$ is not a group. Saying that a number system is a group over $+$ just means that it contains negative numbers.

Pivoting towards multiplication, it is clear to see that none of these sets form a group under multiplication. For $(\mathbb{N}, \cdot)$ and $(\mathbb{Z}, \cdot)$ it is clear why: they do not have multiplicative inverses. For example, $2 \in \mathbb{Z}$ has the multiplicative inverse $\frac{1}{2} \notin \mathbb{Z}$, hence $(\mathbb{Z}, \cdot)$ can clearly not be considered a group. What about $\mathbb{Q}$ and $\mathbb{R}$? They are almost groups under multiplication, but $0 \in \mathbb{Q} \subset \mathbb{R}$ *has no multiplicative inverse*, hence $(\mathbb{Q}, \cdot)$ and $(\mathbb{R}, \cdot)$ are not groups. *But*, if we remove the zero element, then both $(\mathbb{Q} \setminus \{0\}, \times)$ and $(\mathbb{R} \setminus \{0\}, \times)$ are, in fact, groups. We will see in a future chapter that abelian groups with an additional operation (called multiplication) that distributes over its group operation (called addition) are called *rings*, while if a ring also have multiplicative inverses (for all but 0) it is called a *field*. The 0 element will never be allowed to have a multiplicative inverse (division by 0), so we'll never be able to specify a set which has a group structure over $+$ and $\cdot$ that distributes correctly: so instead, fields will have a group multiplication that works on every element *except* the 0 element.

Perhaps the most important example of another group (at least for finite group theory) is the **cyclic group of order** n, denoted $\mathbb{Z}/n\mathbb{Z}$, or $\mathbb{Z}_n$ if you're a physicist (we'll see why the first notation is more precise when we discuss quotienting). This group is the set of integers *modulo* n, defined as

$$\mathbb{Z}/n\mathbb{Z} := \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\} \tag{14}$$

The bar on top means "equivalence class modulo n: two integers a and b are equivalent modulo n if they are related by a multiple of n,

$$\bar{a} = \bar{b} \iff a \cong b \mod n \iff \exists k \in \mathbb{Z}\, a = b + kn. \tag{15}$$

[1]We will later explore algebraic structures with two operations (rings, fields), and see that $(\mathbb{Z}, +, \cdot)$ is a ring, while $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$ are fields.

Every group is defined with an operation: here the group operation is addition modulo n, $\overline{a} + \overline{b} = \overline{a+b}$. The identity element is $\overline{0}$, since we are working with addition. For example, in $\mathbb{Z}/5\mathbb{Z}$, $\overline{3} + \overline{4} = \overline{7} = \overline{2}$, and in $\mathbb{Z}/8\mathbb{Z}$, $\overline{2} + \overline{6} = \overline{8} = \overline{0}$. This previous example shows that in $\mathbb{Z}/8\mathbb{Z}$, the inverse of $\overline{2}$ is $-\overline{2} = \overline{-2} = \overline{6}$. The group multiplication table for $\mathbb{Z}/5\mathbb{Z}$ is shown in Figure 1. Study the multiplication table and understand how it encodes the different properties of $\mathbb{Z}/5\mathbb{Z}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	1	ξ	ξ^2	ξ^3	ξ^4
1	1	ξ	ξ^2	ξ^3	ξ^4
ξ	ξ	ξ^2	ξ^3	ξ^4	1
ξ^2	ξ^2	ξ^3	ξ^4	1	ξ
ξ^3	ξ^3	ξ^4	1	ξ	ξ^2
ξ^4	ξ^4	1	ξ	ξ^2	ξ^3

Table 1: Group multiplication table for $\mathbb{Z}/5\mathbb{Z}$ (left) and the fifth roots of unity Ω_5 (right). The multiplication table encodes the entire structure of the group. Note that upon the relabeling $+ \to \cdot$, $\overline{0} \to 1$, $\overline{1} \to \xi$, $\overline{2} \to \xi^2$, $\overline{3} \to \xi^3$, $\overline{4} \to \xi^4$, the two multiplication tables are identical. This means the groups are the same as sets, but more importantly have the same group multiplication: they are functionally identical with respect to their group structure, up to what we name each element. This means the two groups are **isomorphic**: they are the same up to relabeling.

Exercise 1

Write out a similar group multiplication table for $\mathbb{Z}/6\mathbb{Z}$ to Table 1. The multiplication table encodes all the properties of the group that we are interested. Deduce the answers to the following questions *from the multiplication table*. What is the additive inverse $-\overline{3}$ of $\overline{3}$? Is the group abelian? What is the identity element e? Convince yourself that the order of every non-identity element in $\mathbb{Z}/5\mathbb{Z}$ is 5, but in $\mathbb{Z}/6\mathbb{Z}$, there are non-identity elements with order < 6.

The cyclic group is named as such because it is generated by a single element: if we take all powers of $\overline{1}$, we will produce the entire group. Note that "taking powers" in an additive group is equal to multiplication, since we are applying the group operation (addition) n times,

$$\overline{1}^k = \underbrace{\overline{1} + ... + \overline{1}}_{k \text{ times}}. \tag{16}$$

the order of $\overline{1}$ is n. We often denote this as:

$$\mathbb{Z}/n\mathbb{Z} = \left\{ \overline{1}^k : k \in \{0, 1, 2, ..., n-1\} \right\} \tag{17}$$

Note that $\mathbb{Z}/n\mathbb{Z}$ is abelian with order n. Another way to write the group out is called a **presentation**. A presentation tell us that we *generate* the group with the symbols we

are given, subject to the *constraints* that we impose. For $\mathbb{Z}/n\mathbb{Z}$, there is one generator ($\overline{1}$) subject to the constraint that $\overline{1}^n = e$, so we can write a presentation as follows

$$\mathbb{Z}/n\mathbb{Z} = \left\langle \overline{1} \middle| \overline{1}^n = e \right\rangle . \tag{18}$$

We then relabel $\overline{1}^2 \to \overline{2}, ..., \overline{1}^{n-1} \to \overline{n-1}$, and $e \to \overline{0}$. We will use the notation

$$\langle \text{ generators } | \text{ constraints } \rangle \tag{19}$$

to denote a group by a presentation of the group, and if there are no constraints, we leave them blank: for example, $\mathbb{Z} = \langle 1 \rangle$ (where it is generated under the group operation of addition).

Relabeling the group preserves the same group structure: two groups are equivalent if they have the same exact group structure, which can be given explicitly by a multiplication table or a presentation of the group. When two groups have the exact same structure, we call them **isomorphic**, and you can think of it as simply a renaming of the elements. To provide an example of this, for $n \in \mathbb{N}_{>0}$, we consider the n^{th} roots of unity,

$$Z_n := \{ z \in \mathbb{C} : z^n = 1 \} . \tag{20}$$

One can show that $(Z_n, \cdot)$ forms a group of order n under multiplication, and its elements are explicitly given by

$$Z_n = \left\{ 1, e^{2\pi i \frac{1}{n}}, e^{2\pi i \frac{2}{n}}, ..., e^{2\pi i \frac{n-1}{n}} \right\} = \left\{ e^{2\pi i \frac{k}{n}} : k \in \{0, 1, ..., n-1\} \right\} . \tag{21}$$

The **fundamental n^{th} root of unity** is denoted ξ_n,

$$\xi_n := e^{\frac{2\pi i}{n}} . \tag{22}$$

This root generates the group and has order n. A presentation for Z_n is thus,

$$Z_n = \left\langle \xi \middle| \xi^n = 1 \right\rangle , \tag{23}$$

with its corresponding multiplication table written out in Table 1. The presentation of Z_n is the exact same as the presentation of $\mathbb{Z}/n\mathbb{Z}$, up to relabeling ξ to $\overline{1}$ and swapping multiplication for addition. Their multiplication tables are exactly the same: this tells us the groups are **isomorphic**, and are exactly equivalent with regards to their group structure.

Another useful example of a group is the **dihedral group** of order $2n$, denoted D_{2n}. The dihedral group is the group of symmetries of the regular n-gon: there are $2n$ symmetries, hence $|D_{2n}| = 2n$, which is why we $2n$ is conventionally used as the subscript[2]. This group is generated by rotations and reflections: there are n rotations of the regular n-gon. The remaining elements are reflections about the central axis. This is illustrated for $n = 5$ (the pentagon) and $n = 8$ (the octagon) in Figure 1.

The dihedral group is generated by two elements: rotation of the n-gon by one unit, denoted r, and a flip about the central axis of the n-gon, denoted s. Clearly a rotation of

[2]Some authors prefer to denote the group as D_n, which has order $2n$, but either is OK as long as you're consistent about it and clearly specify your convention.

the n-gon by k units is given by rotating it by one unit k times, hence r^k rotates the n-gon by k. The order of r is n,

$$|r| = n \tag{24}$$

since we can do n flips to get back to our original orientation of the n-gon, and if we flip the n-gon $k < n$ times, then we do not return to the starting configuration. Likewise, the order of s is 2,

$$|s| = 2, \tag{25}$$

since after two flips about the central axis we are back to the initial configuration. In addition to $|r| = n$ and $|s| = 2$, the defining relation for the dihedral group is an equation relating r and s to one another,

$$rs = sr^{-1}. \tag{26}$$

It is worth doing out some examples to convince yourself of this: this says that flipping the n-gon then rotating it in the positive direction (rs) is equivalent to rotating in the negative direction, then flipping (sr^{-1}). Note that this is equivalent to $r^{-1} = srs = srs^{-1}$, which we say that r^{-1} is a **conjugate** of r. These relations are manifestly non-abelian: if things commuted, then this would reduce to $r = r^{-1}$, which is certainly not true.

These three relations are enough to allow us to determine a presentation of D_{2n},

$$D_{2n} = \left\langle r, s | r^n = e = s^2, rs = sr^{-1} \right\rangle. \tag{27}$$

If you want, you can try to form all the words[3] from the letters r and s. You'll find that by imposing these three relations, we can write out all the elements of D_{2n} explicitly,

$$D_{2n} = \left\{ e, r, r^2, ..., r^{n-1}, s, rs, r^2 s, ..., r^{n-1} s \right\}. \tag{28}$$

The dihedral group is interesting because it has a lot of cyclic subgroups (most groups do). The subgroup $\langle r \rangle = \{e, r, r^2, ..., r^{n-1}\}$ is cyclic and generated by r. It is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ by the map $f : \langle r \rangle \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$,

$$f : r \mapsto \overline{1}. \tag{29}$$

Note that f extends uniquely to a homomorphism, since $f(r^k) = f(r)^k = \overline{1}^k = \overline{k} \in \mathbb{Z}/n\mathbb{Z}$. We likewise have a $\mathbb{Z}/2\mathbb{Z}$ subgroup generated by s, $\langle s \rangle \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$ by $s \mapsto \overline{1} \in \mathbb{Z}/2\mathbb{Z}$. So, there are two disjoint (except for e) subgroups of D_{2n}, $\langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}$ and $\langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$, and if we take a direct product of these subgroups, the result has order $2n$. Does this mean that we can form D_{2n} by taking a direct product of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$? It does not: this construction is too complicated because of the relation $rs = sr^{-1}$. A direct product would yield a very simple group structure: we need something more complicated, which we will do by "twisting" the group structure. We'll discuss this more when we talk about **semidirect products** in Section 1.6.

[3] A word is any string of letters, where letters are the individual tokens: in this case, a word is anything like rs, $rsss$, $r^7 srs^3 rr$, etc.

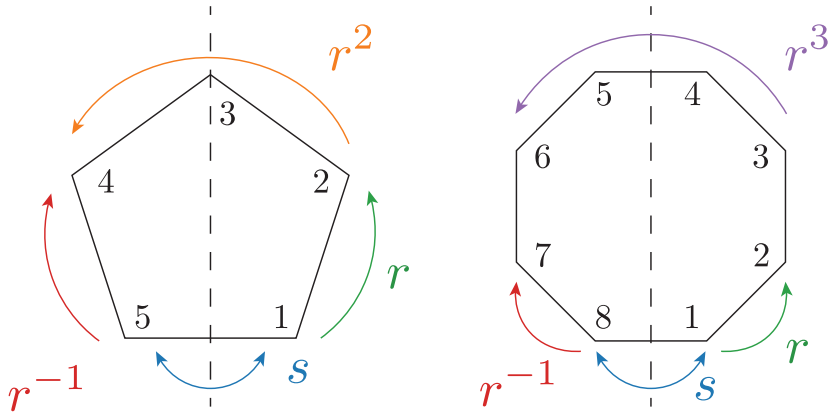

Figure 1: Some of the elements of D_{2n} for $n = 5$ (left) and $n = 8$ (right). Note that n labels the number of vertices of the polygon, and $2n$ is the number of symmetries. The element $r \in D_{2n}$ rotates each vertex in the positive direction, and r^{-1} rotates each vertex to the left. The reflection $s \in D_{2n}$ flips each polygon about its central axis. Each vertex on each polygon is labeled as $\{1, 2, ..., n\}$ in black.

0.2 The Symmetric Group: Permutations

Arguably the two most important classes of finite groups are the cyclic groups $\mathbb{Z}/n\mathbb{Z}$, which we have already discussed, and the symmetric group S_n, which will be discussed now. The **symmetric group on n letters**[4] is defined as the permutation group of n distinct objects.

Definition 7: Symmetric group S_Ω, S_n

A **permutation** of a set Ω is a bijection $\sigma : \Omega \to \Omega$. The **symmetric group on Ω** is the set of permutations on Ω under the group operation of function composition. The **symmetric group of order n**, S_n, is the set of permutations on the set of n elements $\Omega := [n] := \{1, 2, ..., n\}$,

$$S_n := \left\{\sigma : [n] \to [n] \middle| \ \sigma \text{ is a bijection}\right\}. \tag{30}$$

Why is S_n a group under function composition? The identity element is simply the permutation which leaves $[n]$ fixed,

$$\mathrm{id} : [n] \to [n] \qquad\qquad \mathrm{id}(i) = i, \ \forall i \in \{1, ..., n\}. \tag{31}$$

If we compose id with any other permutation σ, it leaves σ unchanged because id does nothing. Any permutation can also be inverted: this is just the inverse function of a bijection. Finally, function composition is associative, hence this forms a group operation. Note that the group S_n is **not abelian**, as we will soon see with examples.

[4] A "letter" is just what we call an arbitrary object: this means the symmetric group with respect to permuting n distinct elements.

Proposition 5

If $n = |\Omega|$, then $S_\Omega \cong S_n$. The order of S_n is,

$$|S_n| = n! \tag{32}$$

This corollary means that it is enough to study the symmetric group on n letters: the symmetric group of a finite group Ω is isomorphic to $S_{|\Omega|}$. Although I do not wish to prove this, if you would like to on your own, then parameterize $\Omega = \{\omega_1, ..., \omega_n\}$, define the canonical map $\iota : [n] \to \Omega$ as $\iota(i) := \omega_i$, and show that $S_n \to S_\Omega$, $\sigma \mapsto \iota \circ \sigma \circ \iota^{-1}$ is a group isomorphism. Furthermore, $|S_n| = n!$ because we have n choices of where to send the element 1, then $n-1$ choices of where to send 2, and so on until we have $n!$ possible permutations.

As we've seen, an element of S_n is a permutation of $[n]$, $\sigma : [n] \xrightarrow{\sim} [n]$. There are two types of common notation for permutations. The first is to explicitly specify where it sends each element in $[n]$, which is done in the following notation,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix} \tag{33}$$

This notation explicitly lays out the map σ in a compact way: it shows exactly how σ permutes each element of $[n]$.

A **cycle** is a string in $[n]$ (which represents a permutation $\sigma \in S_n$) that is closed under permutation by σ: we start with k_1, then $k_2 := \sigma(k_1)$, $k_3 := \sigma(k_2)$, and continue to apply σ until we get back to $k_1 = \sigma(k_\ell)$ for some $\ell < n$. We assume all other elements of $[n]$ are fixed by the cycle. ℓ is called the **length** of the cycle σ, and it is also the **order** of σ as a group element of S_n[5]. We can represent a cycle with **cycle notation**,

$$(k_1\, k_2\, k_3\, ...\, k_\ell) \tag{34}$$

which means that $\sigma : k_1 \mapsto k_2 \mapsto k_3 \mapsto ... \mapsto k_\ell \mapsto k_1$ and that σ fixes any element of $[n]$ not in $\{k_1, ..., k_\ell\}$. **Important**: we read cycles left to right, but we read *products of permutations or cycles* from right to left. The difference is because we've defined cycle notation lexicographically, but the product operation on permutations is function composition, which is read right to left (the closest function is applied first).

Definition 8: Disjoint cycles, transpositions

Two cycles $\sigma_1, \sigma_2 \in S_n$ are **disjoint** if they permute different elements of $[n]$. Disjoint cycles commute, i.e., $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$. A length two cycle is called a **transposition**, and typically denoted $\tau \in S_n$.

[5]This is because for $\sigma^n = 1$, clearly k_1 must map back to k_1, which can only happen after ℓ applications of σ. Likewise by tracing out the cycle, we can see that ℓ applications of σ applied to any k_j in the cycle will yield itself, hence $\sigma^\ell = \text{id}$.

Theorem 1: Cycle decomposition

Any element $\sigma \in S_n$ can be expressed as the product of disjoint cycles.

Given $\sigma \in S_n$, the basic idea behind the cycle decomposition is to first find the cycle starting with 1 by repeatedly applying σ to 1 until eventually $1 = \sigma^\ell(1)$: this gives the cycle $(1\,\sigma(1)\,\sigma^2(1)\,...\sigma^\ell(1))$ (note that if σ fixes 1, then this cycle is trivial and just (1). Then, pick the next smallest number which is not in this cycle and repeat the procedure until every element in $[n]$ appears in a cycle.

There is also another way to decompose $\sigma \in S_n$: one can decompose it into a sequence of transpositions. In contrast to the cycle decomposition, we

Theorem 2: Transposition decomposition

Any element $\sigma \in S_n$ can be expressed as the product of transpositions. Explicitly, given $(a_1\,a_2\,a_3\,...\,a_k) \in S_n$, one has

$$(a_1\,a_2\,a_3\,...\,a_k) = (a_1 a_k)...(a_1 a_3)(a_1 a_2). \tag{35}$$

Note the transpositions are **not** disjoint.

The idea here is that we can express any cycle as just repeatedly flipping two elements of $[n]$, and build up a permutation in this way. The **order** we build up the product of transpositions is important, because we *read the permutations from right to left* and apply permutations as we go. In Eq. (35), we want to send $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, and so on, until $a_k \mapsto a_1$. On the right-hand side, a_1 is mapped to a_2 in the first transposition, then never touched again (there are no more a_2 factors in the remaining string). a_2 is mapped to a_1, which then maps to a_3 in the next tranposition, hence $a_2 \mapsto a_3$ as desired. This pattern repeats until the end of the string, when a_k maps to a_1 as expected.

Let's do some examples. The permutation,

$$\sigma_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} \in S_6 \tag{36}$$

interchanges 1 and 5, leaves 3 fixed, and maps $2 \mapsto 4 \mapsto 6 \mapsto 2$. This permutation σ_1 has two cycles: it has a transposition $1 \mapsto 5 \mapsto 1$, and a length 3 cycle $2 \mapsto 4 \mapsto 6$. We can thus denote it,

$$\sigma_1 = (15)(246)(3). \tag{37}$$

The (3) by itself means that σ_1 fixes 3: we will conventionally just drop the (3) term, and write

$$\sigma_1 = (15)(246). \tag{38}$$

Since 3 is not included in a cycle, it is implied that it is fixed by σ_1. Note that we can also write $\sigma_1 = (246)(15)$.

We can also do some computations. Let

$$\sigma_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix} = (134)(56). \tag{39}$$

What is $\sigma_1 \circ \sigma_2$? **The order matters**: we first apply σ_2, then apply σ_1. We can do this by explicitly working out where $\sigma_1 \circ \sigma_2$ sends each element of $[n]$. For example, σ_2 sends 1 to 3, which is fixed by σ_1, so $1 \mapsto 3$. Likewise, $2 \xrightarrow{\sigma_2} 2 \xrightarrow{\sigma_1} 4$, $3 \xrightarrow{\sigma_2} 4 \xrightarrow{\sigma_1} 6$, and so on. We have:

$$\sigma_1 \circ \sigma_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} = (136)(245) \tag{40}$$

What if we compute $\sigma_2 \circ \sigma_1$? In this case,

$$\sigma_2 \circ \sigma_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 5 & 3 & 2 \end{pmatrix} = (162)(345). \tag{41}$$

These are different cycles: S_n **is not an abelian group** as its product does not commute. What about computing inverses? We can simply invert the column representation of the permutation and reorder it:

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 2 & 1 & 4 \end{pmatrix} = (15)(264) \tag{42}$$

It's usually easier to take an inverse directly from the cycle decomposition: one just inverts each cycle, i.e., $(134)^{-1} = (431)$. Note that we can shift cycles with impunity, i.e. $(431) = (314) = (143)$. Symmetric group algebra is very useful to know, and pretty easy once you get the hang of it: I'd suggest doing a few examples (some good exercises can be found in Dummitt and Foote Chapter 1.3).

In the previous section, we discussed the dihedral group D_{2n}. D_{2n} can actually be intimately connected to the symmetric group. For a concrete idea of what each of these elements are doing, one can label the vertices of each object as $\{1, 2, ..., n\}$ (as shown in Figure 1). Each element of D_{2n} can be represented by a specific permutation of $[n]$. For example, let's work with D_{10}, the permutations of the pentagon. The rotation r by one unit, the flip s, and the rotation sr^2 can each be denoted by a bijection on $\{1, 2, ..., 5\}$, given by,

$$r : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 5 \\ 5 \mapsto 1 \end{cases} \qquad s : \begin{cases} 1 \mapsto 5 \\ 2 \mapsto 4 \\ 3 \mapsto 3 \\ 4 \mapsto 2 \\ 5 \mapsto 1 \end{cases} \qquad sr^2 = r^3 s : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \\ 4 \mapsto 5 \\ 5 \mapsto 4 \end{cases} . \tag{43}$$

Note that for sr^2, we rotate twice by r first, then apply the flip s (we read these right to left). This element represents a flip around the axis drawn between the center of the pentagon and the vertex 2. You can write down the other 7 elements in the exact same way: this gives a more concrete way to represent elements of the dihedral group.

This implies that the dihedral group D_{2n} can be thought of permutations on the set $\{1, 2, ..., n\}$. Formally said, there is an embedding,

$$\iota : D_{2n} \hookrightarrow S_n \tag{44}$$

that sends each element of D_{2n} to its corresponding permutation. For example, Eq. (43) shows us that in D_{10}, $\iota(r) = (12345)$, $\iota(s) = (15)(24)$, and $\iota(rs^2) = (13)(45)$. This means

that **we can view D_{2n} as an order $2n$ subgroup of S_n**. We'll soon see a similar feature: it turns out that *any finite group can be embedded in the symmetric group* (although in the general case, we'll see D_{2n} embedded in S_{2n}: the embedding into S_n is special to the structure of the dihedral group).

Let's see how embeddings work concretely for $n = 4$ by explicitly writing out the multiplication tables for a few groups (here we are working with D_8 because it is quicker to write out the multiplication table). I'll write out first the multiplication tables for $\mathbb{Z}/4\mathbb{Z}$, D_8, and part of the table for S_4 (there are 24 elements, so I don't want to write the whole thing!), so that we can view them all next to one another, then explain why they are interesting.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

D_8	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

Table 2: Group multiplication table for $\mathbb{Z}/4\mathbb{Z}$ and D_8. Note the similarities in the top left of the table for D_8 with the table for $\mathbb{Z}/4\mathbb{Z}$.

S_4	e	(1234)	$(13)(24)$	(4321)	$(14)(23)$	(13)	$(12)(34)$	(24)	...
e	e	(1234)	$(13)(24)$	(4321)	$(14)(23)$	(13)	$(12)(34)$	(24)	...
(1234)	(1234)	$(13)(24)$	(4321)	e	(13)	$(12)(34)$	(24)	$(14)(23)$	...
$(13)(24)$	$(13)(24)$	(4321)	e	(1234)	$(12)(34)$	(24)	$(14)(23)$	(13)	...
(4321)	(4321)	e	(1234)	$(13)(24)$	(24)	$(14)(23)$	(13)	$(12)(34)$	...
$(14)(23)$	$(14)(23)$	(24)	$(12)(34)$	(13)	e	(4321)	$(13)(24)$	(1234)	...
(13)	(13)	$(14)(23)$	(24)	$(12)(34)$	(1234)	e	(4321)	$(13)(24)$	...
$(12)(34)$	$(12)(34)$	(13)	$(14)(23)$	(24)	$(13)(24)$	(1234)	e	(4321)	...
(24)	(24)	$(12)(34)$	(13)	$(14)(23)$	(4321)	$(13)(24)$	(1234)	e	...
$\vdots$									

Table 3: Part of the multiplication table for S_4 (specifically, the multiplication table for the subgroup $\langle (1234), (14)(23) \rangle$). Note the similarities in the first 8 elements of the table with the multiplication table for D_8 (Table 2).

Note that in Table 2, the relation $rs = sr^{-1}$ has been used frequently. We multiply the column on the left by the row on the right, so for example the column r^2s times the row r is the element sr^3. Why is it sr^3? Because

$$(r^2s)r = (sr^{-2})r = (sr^2)r = sr^3. \tag{45}$$

Note that $r^{-2} = r^{4-2} = r^2$ because $n = 4$ for D_8. Furthermore, we could move the r on the right-hand side to the left, as so,

$$r^2(sr) = r^2(r^{-1}s) = rs. \tag{46}$$

Is this the same element as sr^3? Indeed it is, because $rs = sr^{-1} = sr^3$ in D_8. There are many such equivalences: although we parameterized D_8 in Table 2 with $r^k s$, we could have equivalently parameterized it with sr^k, or with sr^{-k}: it's just a choice of convention, but it's important that you keep the convention consistent.

Consider Table 2. The multiplication table on the left ($\mathbb{Z}/4\mathbb{Z}$) can be relabeled to look like a subtable of the multiplication table on the right (D_8). Consider the map,

$$\theta : \mathbb{Z}/4\mathbb{Z} \to D_8 \qquad\qquad \theta := \begin{cases} \overline{0} \mapsto e \\ \overline{1} \mapsto r \\ \overline{2} \mapsto r^2 \\ \overline{3} \mapsto r^3 \end{cases} . \tag{47}$$

θ is clearly injective, and is also a homomorphism: it respects the group structures of $\mathbb{Z}/4\mathbb{Z}$ and D_8. Use θ to relabel the group multiplication table for $\mathbb{Z}/4\mathbb{Z}$: note that it is now the exact same group multiplication table as the upper right block of the multiplication table for D_8 (the block that corresponds to the multiplication table for the subgroup $\langle r \rangle \leq D_8$). This means that $\mathbb{Z}/4\mathbb{Z}$ and $\langle r \rangle$ have the same group structure: they are isomorphic! The map θ is an embedding (an injective homomorphism), and induces an isomorphism between $\mathbb{Z}/4\mathbb{Z}$ and the subgroup $\langle r \rangle$ of D_8. If we are given an embedding of groups, we can interpret the domain ($\mathbb{Z}/4\mathbb{Z}$) as a **subgroup** of the codomain, up to relabeling. This case is relatively simple, since both $\mathbb{Z}/4\mathbb{Z}$ and $\langle r \rangle$ are **cyclic groups**: they are each generated by 1 element of order 4. There isn't much difference that can occur in their group structure. So, let's move on to a more complicated example: the embedding of D_8 into S_4.

We have written the multiplication table for S_4 in a specific order to suggest the embedding that we were considering. We saw that the dihedral group D_{2n} can be embedded into S_n by considering it as a permutation of the vertices of the n-gon, which are labeled $\{1, 2, ..., n\}$. What permutations do the elements of D_8 correspond to? r again rotates $1 \to 2 \to 3 \to 4 \to 1$, and s maps $1 \leftrightarrow 4$ and $2 \leftrightarrow 3$. This yields,

$$r \hookrightarrow (1234) \qquad\qquad s \hookrightarrow (14)(23) \tag{48}$$

This extends uniquely into a homomorphism $\phi : D_8 \to S_4$. We can either multiply appropriate powers of (1234) and (14)(23) together to find out what each element of D_8 maps to, or we can work it out geometrically from the symmetries of the square. It is clear that r^k rotates the square k times, so r^2 maps vertex 1 to 3, vertex 2 to 4, and so on, and likewise for the other vertices,

$$r^2 \hookrightarrow (13)(24) \qquad\qquad r^3 \hookrightarrow (1432) = (4321) = (1234)^{-1}. \tag{49}$$

The elements $r^k s$ are a bit harder, but can be worked out in the same way. We have

$$rs \hookrightarrow (13) \qquad\qquad r^2 s \hookrightarrow (12)(34) \qquad\qquad r^3 s \hookrightarrow (24). \tag{50}$$

With the map ϕ in mind, we can now establish an equality (isomorphism) between D_8 and the subgroup $\langle (1234), (14)(23) \rangle$ of S_4. If we go to the multiplication tables above and use the embedding ϕ to replace the labels on the multiplication table for $\langle (1234), (14)(23) \rangle$ with the corresonding value of $\phi^{-1}(\sigma)$, then the two multiplication tables become identical! This means they have identical group structures: they are isomorphic. Indeed, this illustrates the core idea of why an embedding is so important. If $\phi : G \hookrightarrow G'$ is an embedding (injective homomorphism), then G is isomorphic to a subgroup of G'. In plain English, this means that there is an identical copy of G **inside** of G'. This copy of G will often have a different labeling, but at the level of its group structure, it is exactly the same object. As we saw, this means there is a copy of D_8 living inside of S_4: the specific copy of D_8 is the subgroup $\langle (1234), (14)(23) \rangle$, where (1234) plays the role of the element r and $(14)(23)$ plays the role of the element s.

This is the result of an injective homomorphism: it embeds a copy of the domain into the codomain. If we are given a surjective homomorphism between two groups, how can we relate their group structures then? That is the subject of the next section: we'll need to understand both of these concepts, because we'll soon be applying them with the goal of **classifying** all the groups of a given size.

Interlude 1: What group structure do homomorphisms translate?

I've been stressing that group homomorphisms can be used to translate group structure between two groups, but group isomorphisms are really what tell you that two groups have equal structure. This point can in fact be quite subtle. Consider, for example, a group homomorphism,

$$\phi : G \to G'. \tag{51}$$

What type of structure does G' inherit from G, and vice versa what type of structure does G inherit from G'? If ϕ is an isomorphism, then all group properties between G and G' must be the same, but for a general homomorphism, this is not the case.

Let's consider the case when either G or G' is an abelian group. If G is an abelian group, then $\mathrm{im}(\phi) \leq G'$ is also abelian. This is simply because for $g'_1, g'_2 \in G'$, we have $g'_i = \phi(g_i)$, so

$$g'_1 g'_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = g'_2 g'_1. \tag{52}$$

So, a homomorphism will pass on the abelian structure of a group to its image. What about the other way around, if G' is abelian? We can't say much about this case, because even though $\phi(g_1 g_2) = \phi(g_2 g_1)$, all this means is that $\phi(g_1 g_2)\phi(g_2 g_1)^{-1} = \phi(g_1 g_2 g_1^{-1} g_2^{-1}) = e$: that the **commutator** of g_1 and g_2, $[g_1, g_2] := g_1 g_2 g_1^{-1} g_2^{-1}$, lies in the kernel of ϕ.

We'll now do an example of a homomorphism between groups where G is non-abelian, but G' is abelian. Consider the map,

$$\phi : D_8 \to \mathbb{Z}/2\mathbb{Z} \qquad \phi : \begin{cases} r^k \mapsto \overline{0} \\ sr^k \mapsto \overline{1} \end{cases} . \tag{53}$$

You should convince yourself this is a homomorphism: indeed it is, as ϕ counts "powers of s" in an element of D_8, which because of the relation of $sr = r^{-1}s$ makes this map a homomorphism. There is information about the group structure contained in the fact that D_8 and $\mathbb{Z}/2\mathbb{Z}$ are homomorphic: but it is not as obvious as "they are both abelian", since D_8 is clearly non-abelian. We'll see exactly how this group structure is shared between the two groups in the next section.

As a final point to lead into the next section, the kernel of ϕ is easy to write out from this definition: it is the cyclic subgroup generated by r,

$$\ker \phi = \{e, r, r^2, r^3\} = \langle r \rangle. \tag{54}$$

The kernel has a very specific property that we will explore next: it is a **normal subgroup**. Note that under conjugation by other elements of D_8 (for example, conjugating $r \in \ker \phi$ by $s \in D_8 \setminus \ker(\phi)$), elements of the kernel are not fixed,

$$srs^{-1} = srs = r^{-1}s^2 = r^{-1} = r^3 \neq r. \tag{55}$$

However, note that $srs^{-1} = r^3 \in \ker(\phi)$. Although it is not fixed under conjugation (because r and s do not commute), the conjugate srs^{-1} is another element of $\ker \phi$. This is a property called **normality**: a subgroup $H \leq G$ is **normal** if for any $g \in G$,

$$gHg^{-1} = H, \tag{56}$$

and denoted $H \trianglelefteq G$. The kernel of any map satisfies this normality condition, which we'll soon see. For our specific case,

$$g\langle r \rangle g^{-1} = \ker(\phi) \qquad \forall g \in D_8, \tag{57}$$

hence $\ker \phi$ is a **normal subgroup**. You should work this We'll explore this idea in depth in the next section, because it is crucial to the concept of quotienting.

0.3 The Subgroup Calculus

We'll next move onto quotients. These have a very similar intuition to the vector space case, but are a bit harder to work with. We will also see that if we want the quotient of a group to have a group structure, we cannot quotient by an arbitrary subgroup: the subgroup has to have a specific property called **normality**. We'll begin by trying to understand more about the structure of a general subgroup. We'll begin with **cosets**, which are shifted subgroups.

Definition 9: Coset

Let $H \leq G$ be a subgroup, and $g \in G$. The **left coset** of g by H is,

$$gH := \{gh : h \in H\}. \tag{58}$$

Likewise, the **right coset** of g by H is $Hg = \{hg : h \in H\}$.

We will often work with left cosets because of convenience, but our results will also apply to right cosets unless otherwise stated. Note that gH is typically **not** a subgroup of G, unless in the special case when $g \in H$.

Proposition 6

gH is a subgroup of G if and only if $g \in H$. In this case, $gH = H$.

Proof. Suppose gH is a subgroup of G. Then $e \in gH$, so $e = gh$ for some $h \in H$. This implies that $g = h^{-1}$, and since H is closed under inversion, this implies that $g \in H$, proving $\implies$. For the backwards direction, suppose $g \in H$. Clearly $gH \neq \emptyset$ since $g = ge \in gH$ □

Given an arbitrary subgroup $H \leq G$, we want to understand what the cosets of H look like in G. The first idea, which everything will eventually follow from, is that **each coset has the same size**, which is also the size of H.

Proposition 7

For any subgroup $H \leq G$ and any $g \in G$,

$$|gH| = |H|. \tag{59}$$

Proof. We want to show that the map,

$$f_g : H \longrightarrow gH \qquad\qquad h \mapsto gh \tag{60}$$

is a bijection between H and gH. By the definition of gH, it is surjective: any element of gH can be represented by $f_g(h) = gh$ for some h. The map is also injective because of the left-cancellation law; suppose that $f_g(h) = f_g(h')$. Then,

$$f_g(h) = f_g(h') \implies g \cdot h = g \cdot h' \implies h = h' \tag{61}$$

by multiplying on the left with g^{-1}. This shows f_g is a bijection, hence $|gH| = |H|$ if H is finite. Note that this map is not a homomorphism, as gH is not a subgroup of G. □

So, each coset of G is the same size. We can write

Proposition 8: Left coset equivalence

Let $g_1, g_2 \in G$. Then, $g_1H = g_2H$ if and only if $g_2^{-1} \cdot g_1 \in H$. Additionally, if $g_1H \neq g_2H$, then in fact $g_1H \cap g_2H = \emptyset$, i.e., in this case the cosets are disjoint.

As a corollary, $g_2 \in g_1H$ if and only if $g_1H = g_2H$.

Proof. For the forward direction, if $g_1H = g_2H$, then since $e \in H$, we know that $g_1 \in g_1H = g_2H \implies g_1 = g_2h$ for some $h \in H$. Inverting g_2 gives us that $g_2^{-1} \cdot g_1 = h \in H$ as desired. For the converse, suppose $g_2^{-1} \cdot g_1 \in H$, so $g_1 = g_2 \cdot h$ for some $h \in H$, and let $g_1h' \in g_1H$.

Then $g_1 h' = (g_2 h)h' = g_2 hh' \in g_2 H$, hence $g_1 H \subseteq g_2 H$. Likewise, we have $g_2 H \subseteq g_1 H$ as well, because for any $g_2 h' \in g_2 H$, we have $g_2 h' = (g_1 h^{-1})h' = g_1(h^{-1}h') \in g_1 H$ because $h^{-1}h' \in H$. This proves the first statement.

For the second statement, suppose that $g_1 H \neq g_2 H$. The first statement tells us that then $g_2^{-1} g_1 \notin H$. Suppose that $g_1 H \cap g_2 H \neq \emptyset$, so let $x \in g_1 H \cap g_2 H$. This implies that $x = g_1 h$ and that $x = g_2 h'$ for $h, h' \in H$, which yields

$$g_2^{-1} \cdot g_1 = h' \cdot h^{-1} \in H, \tag{62}$$

a contradiction. Hence $g_1 H \cap g_2 H = \emptyset$. □

There is a corresponding statement about the right cosets of G, which says that $Hg_1 = Hg_2$ if and only if $g_1 g_2^{-1} \in H$. We will typically

Definition 10: Quotient of G by H, index of G in H

Given a subgroup $H \leq G$, the set of left cosets of G by H is called the **quotient space**, denoted

$$G/H := \{gH : g \in G\}. \tag{63}$$

The corresponding set of right cosets is denoted,

$$H \setminus G := \{Hg : g \in G\}. \tag{64}$$

The number of left cosets in G is called its **index**, denoted $[G : H]$,

$$[G : H] := |G/H| = \text{Number of left cosets of } H \text{ in } G. \tag{65}$$

We will typically use the left cosets G/H, although everything we are working with follows the same logic. The reason we are focused on understanding the set of cosets G/H is because they are very well-behaved. First, we consider decomposing G into cosets. Note that we always have

$$G = \bigcup_{g \in G} gH \tag{66}$$

because for each $g \in G$, $g \in gH$ since $e \in H$. The remarkable thing about this decomposition is that by using the previous propositions, each distinct coset contains no repeats. We can thus instead write this decomposition as a *disjoint union* of cosets,

$$G = \bigsqcup_{gH \in G/H} gH. \tag{67}$$

The first equation (Eq. (66)) and this new equation (Eq. (67)) differ an important way: the disjoint union. When writing Eq. (66), we are not taking into account the fact that different elements can be in the same coset, i.e. that $g' \in gH$ for some $g' \neq g$. Eq. (67) makes it clear that the cosets G/H **partition** G, in that they form a set of subsets of G that are mutually disjoint and cover the space when joined. A cartoon of this is depicted in Figure 2 (ignore the arrows for now). In that example, there are 7 distinct cosets of H,

i.e., $G/H = \{H, g_1H, g_2H, ..., g_6H\}$. Each coset is disjoint and the union of all these cosets forms G, and each coset is also the same exact size, $|H| = |g_iH|$. This should sound familiar: it says that the cosets G/H **form a partition** of G (cf. Section **??**, Definition **??**). This means that the cosets can also be viewed as the **equivalence classes** from an equivalence relation. What is that equivalence relation?

Theorem 3: Equivalence class of left cosets

Let $H \leq G$ be a subgroup. The relation,

$$g_1 \sim_H g_2 \text{ iff } g_2^{-1} \cdot g_1 \in H, \tag{68}$$

is an equivalence relation on G. The equivalence classes of $\sim_H$ are exactly the left cosets G/H.

Proof. We need to show 3 things:

1. Equality. For $g \in G$, we have $g \sim_H g$, since $g^{-1} \cdot g = e \in H$.
2. Symmetry. Suppose $g_1 \sim_H g_2$, so $g_2^{-1} \cdot g_1 = h \in H$. Then $h^{-1} \in H$ because H is a subgroup, hence $g_1^{-1} \cdot g_2 = (g_2^{-1} \cdot g_1)^{-1} = h^{-1} \in H$, so $g_2 \sim_H g_1$.
3. Transitivity. Suppose $g_1 \sim_H g_2$ and $g_2 \sim_H g_3$, so $g_2^{-1}g_1 = h \in H$ and $g_3^{-1}g_2 = h' \in H$. We need to show that $g_1 \sim_H g_3$, i.e. that $g_3^{-1}g_1 \in H$. This is immediate because,

$$g_3^{-1}g_1 = g_3^{-1}(g_2g_2^{-1})g_1 = (g_3^{-1}g_2)(g_2^{-1}g_1) = h'h \in H. \tag{69}$$

Hence $\sim_H$ is an equivalence relation. What are the equivalence classes of $\sim_H$? We show that for $g \in G$,

$$g/\sim_H = gH. \tag{70}$$

On the left is the equivalence class of g under $\sim_H$, which we defined as $g/\sim_H = \{x \in G : g \sim_H x\}$; on the right is the coset gH. To prove $\subseteq$, suppose $x \in g/\sim_H$. Then $g \sim_H x$, so $x^{-1}g \in H$, which we have already shown (Prop 8) implies $gH = xH \implies x \in gH$. For $\supseteq$, suppose $x \in gH$. Then Prop 8 implies $xH = gH$, which implies $g^{-1}x \in H$, hence $x \sim_H g$ and thus $x \in g/\sim_H$. This proves the theorem. □

This gives us an additional way to view the cosets G/H: we can view them either as the set of cosets $\{gH : g \in G\}$, or we can view them as the equivalence classes of G under the relation $\sim_H$. Both are equivalent and give complementary intuition about the problem. The most important thing for us is that the cosets G/H form a partition of G, as depicted in Figure 2. The next result to understand is **Lagrange's theorem**, which states that the number of elements in a subgroup always cleanly divides the number of elements in a group.

Theorem 4: Lagrange

Let $H \leq G$ be a subgroup of a finite group G. Then the order of H divides the order of G,

$$|H| \,\big|\, |G|. \tag{71}$$

Furthermore, the number of cosets $[G : H]$ is explicitly,

$$[G : H] = \frac{|G|}{|H|}. \tag{72}$$

Proof. The idea here is to cut up the group G into cosets. Because G/H partitions G we can write,

$$G = \bigsqcup_{gH \in G/H} gH, \tag{73}$$

as we did above. Because the union is disjoint, this implies,

$$|G| = \sum_{gH \in G/H} |gH|. \tag{74}$$

But, we have also showed (Prop 7) that $|gH| = |H|$, hence this sum reduces,

$$|G| = \sum_{gH \in G/H} |H| = |H| \times |G/H| \tag{75}$$

which proves the claim. □

Note that $[G : H] = |G|/|H|$ looks deceptively simple, since the index $[G : H]$ is defined to be the size of G/H, i.e., by definition $[G : H] = |G/H|$. It is tempting to just move the $|\cdot|$ symbol around the / symbol, and indeed for finite groups we can do this! That is, we can explicitly say $|G/H| = |G|/|H|$, which is where the notation G/H comes from in the first place. However, it should be noted that this formula is much more simple than the underlying proof that this is true, as we've just gone through.

Lagrange's theorem allows us to start making our first non-trivial observations about the structure of arbitrary groups. The immediate corollary of this theorem is that every group which has a prime number of elements is cyclic. This is actually a remarkable result, because it lets us classify **all the groups of prime order**: each one is isomorphic to $\mathbb{Z}/p\mathbb{Z}$!

Corollary 1: Every prime order group is cyclic

If G is a finite group with $|G| = p$ for p prime, then G is a cyclic group.

Proof. Let G be a finite group with $|G| = p > 1$ (if $|G| = 1$, then $G = \{e\}$ is trivial), with p prime. Let $g \in G \setminus \{e\}$, and consider $\langle g \rangle \leq G$. This is a subgroup of G that is strictly larger than $\{e\}$, as it must contain g and e, which are distinct elements of G. But, the size of $\langle g \rangle$ must divide $p = |G|$, and the only divisors of p are 1 and p, because p is prime. Hence $|\langle g \rangle| = p = |G|$, which shows $\langle g \rangle = G$, and that G is cyclic. It follows that $G \cong \mathbb{Z}/p\mathbb{Z}$ via the isomorphism $g \mapsto \overline{1}$. □

Interlude 2: Automorphisms of $\mathbb{Z}/p\mathbb{Z}$

An isomorphism of a group with itself is called an **automorphism**. We denote the set of automorphisms of a group G as $\mathrm{Aut}(G)$. Automorphisms play a very important role in group theory, in particular in Galois theory (which we will soon study), because the

set of automorphisms $\mathrm{Aut}(G)$ forms a group under function composition.

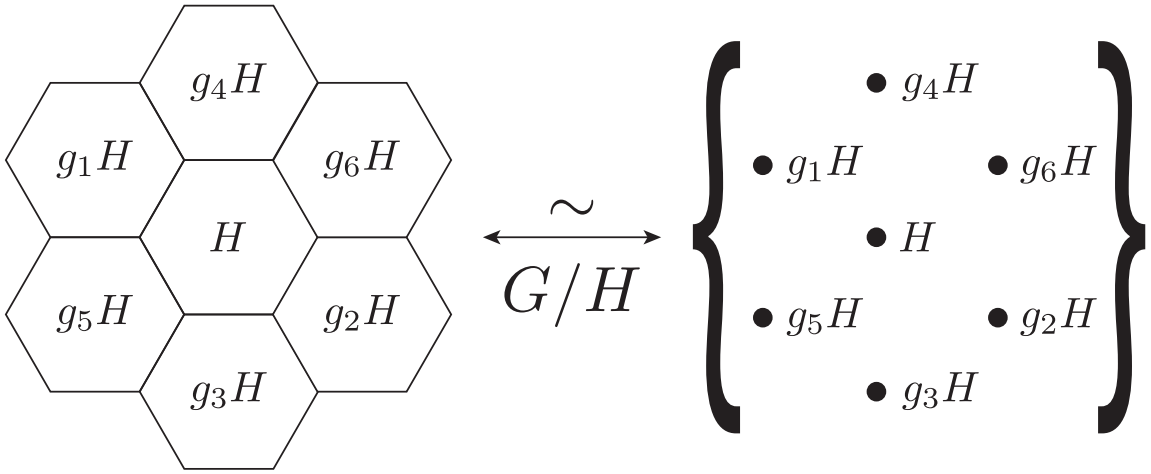

Figure 2: Illustration of a cartoon example used to visualize how a group splits up into cosets. On the left, the entire honeycomb pattern represents the group, and each coset is represented by a single hexagon, labeled either H or g_iH. Note that the subgroup H itself contains the element $e \in H$, and each coset contains $g_i \in g_iH$. Lagrange's theorem implies that each coset has the same size, $|g_iH| = |H|$, and this implies that the index $[G : H] = |G/H| = |G|/|H|$ is an integer. In this example, $[G : H] = 7$ because there are 7 cosets (including the original subgroup H). The right side shows the same picture, but viewing G/H as a 7-element set, rather than a collection of cosets. Although G/H arose from examining the cosets of H in G, we can equally well view G/H as simply a set labeled by the elements $\{H, g_1H, g_2H, ..., g_6H\}$. In this way of thinking, the internal structure of each coset does not matter, only the number of elements that we have.

Let's do a few examples. The first example will be a subgroup of $\mathbb{Z}$: note that because $|\mathbb{Z}| = \infty$, Lagrange's theorem will not hold. However, this will help us get a feel for what it means to be a coset. The next example we'll do will be in D_8, as we've already studied it quite extensively.

Example 2: Cosets of $\mathbb{Z}$ by $7\mathbb{Z}$

Consider the group $(\mathbb{Z}, +)$ and the subgroup

$$H := 7\mathbb{Z} = \{7n : n \in \mathbb{Z}\} = \{..., -14, -7, 0, 7, 14, ...\} = \langle 7 \rangle_+. \tag{76}$$

We've written this out lots of different notation to emphasize how the different notations work. $\mathbb{Z}$ is infinite, so we cannot explicitly apply Lagrange's theorem: however, we can count the number of cosets of $7\mathbb{Z}$. Because $(\mathbb{Z}, +)$ is an additive group, cosets (abstractly written gH) are of the form $n + 7\mathbb{Z} = \{n + k : k \in 7\mathbb{Z}\}$. There are exactly 7 cosets,

which are the following:

$$\begin{aligned} 7\mathbb{Z} = 0 + 7\mathbb{Z} &= \{..., -14, -7, 0, 7, 14, ..., \} \\ 1 + 7\mathbb{Z} &= \{..., -13, -6, 1, 8, 15, ..., \} \\ 2 + 7\mathbb{Z} &= \{..., -12, -5, 2, 9, 16, ..., \} \\ 3 + 7\mathbb{Z} &= \{..., -11, -4, 3, 10, 17, ..., \} \\ 4 + 7\mathbb{Z} &= \{..., -10, -3, 4, 11, 18, ..., \} \\ 5 + 7\mathbb{Z} &= \{..., -9, -2, 5, 12, 19, ..., \} \\ 6 + 7\mathbb{Z} &= \{..., -8, -1, 6, 13, 20, ..., \}. \end{aligned} \tag{77}$$

Notice that each element of $\mathbb{Z}$ falls into exactly one of the cosets. Furthermore, the cosets **are not uniquely labeled**. We could have labeled the coset $2 + 7\mathbb{Z}$ as $16 + 7\mathbb{Z}$, or as $-12 + 7\mathbb{Z}$. We call 2 a **representative** of this coset, but we can equally well choose any other representative of the coset that we wish.

The

Example 3: Cosets of S_4 by two subgroups

Consider the group D_8 and the subgroup V_4 (called the **4-group**):

$$H := V_4 := \{e, (12)(34), (13)(24), (14)(23)\}. \tag{78}$$

Note that every element of the 4-group squares to e, i.e., each non-identity element of V_4 is order 2. The 4-group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 = \{(0,0), (0,1), (1,0), (1,1)\}$, which is a group under $+ \mod 2$. Lagrange's theorem implies that there are

$$[S_4 : V_4] = |S_4|/|V_4| = 24/4 = 6 \tag{79}$$

cosets. What do these cosets look like? We can choose representative permutations and compute the cosets,

$$\begin{aligned} H &= \{e, (12)(34), (13)(24), (14)(23)\} \\ (12)H &= \{(12), (34), (1324), (1423)\} \\ (13)H &= \{(13), (1234), (24), (1432)\} \\ (14)H &= \{(14), (1243), (1342), (23)\} \\ (123)H &= \{(123), (134), (243), (142)\} \\ (321)H &= \{(321), (234), (124), (143)\}. \end{aligned} \tag{80}$$

We see by observaton that indeed these cosets partition S_4: every permutation $\sigma \in S_4$ is in a unique coset. I would advise you to work this out yourself and play with the cosets a bit. Use the abstract information we've discussed in this concrete session. For example, how can we tell that $g := (14)$ and $g' := (1342)$ live in the same coset? We

can check that $gh^{-1} \in H$, and indeed,

$$gh^{-1} = (14)(1342)^{-1} = (14)(2431) = (12)(34) \in H \tag{81}$$

as claimed, which means that $gH = g'H$: they are two representatives of the same coset.

To summarize, we now know that G/H is composed of $[G : H] = |G|/|H|$ distinct cosets of the form gH, each of the same size $|gH| = |H|$. Given a coset gH, it has many equivalent names: indeed, this coset gH can be labeled as $g'H$ as long as $g'g^{-1} \in H$. For any subgroup H, we can partition G into cosets as in Eq. (67). This is illustrated in Figure 2, where in the cartoon G splits up into 7 disjoint cosets $G/H = \{H, g_1H, g_2H, ..., g_6H\}$. Note that we can equally well view G/H as a 7-element set, rather than viewing solely as a collection of cosets. This is shown on the right in Figure 2, as we simply view each g_iH as a point in the set G/H, rather than as a full coset that contains group elements. The question that naturally arises is this: **is there additional structure that we can impose on the set G/H? Can we, in fact, turn it into a group if we properly define a group multiplication law?**

0.4 Quotient Groups

Let's study the example of the subgroup V_4 of S_4 in more detail.

Although G/H arises from partitioning the cosets of a group by a subgroup, we can think of it as a more abstract quantity in its own right: it itself is also a set with $[G : H]$ elements.

The cosets of H by G inherit a multiplication law from the group multiplication regardless of the structure of H. The main question to ask: does this induce a group multiplication law on the quotient G/H?

In the example above, suppose that $g_1 \cdot g_3 = g_4$ (this is multiplication on the level of the group). In the case that H is normal, **any element in the corresponding cosets** will inherit this group multiplication on a coset-level scale. What does this mean in English? Take an arbitrary element of g_1H, which we denote by $g_1h \in g_1H$, and an arbitrary element $g_3h' \in g_3H$. Then,

$$(g_1h)(g_3h') = g_1(g_3g_3^{-1})hg_3h' = (g_1g_3)\underbrace{(g_3^{-1}hg_3)}_{=:\tilde{h}\in H}h = g_4\underbrace{\tilde{h}h}_{=:h''\in H} = g_4h'' \in g_4H. \tag{82}$$

The key here is that because H is normal, $gHg^{-1} = H$ for any g, so using $g = g_3^{-1}$ shows us that $g_3^{-1}hg_3 \in H$ for any $g_3 \in G$ or $h \in H$.

We'll now discuss normality in a bit more detail.

Definition 11: Normal Subgroup

Let $H \leq G$. We say H is a **normal** subgroup of G if for each $g \in G$,

$$gHg^{-1} = H. \tag{83}$$

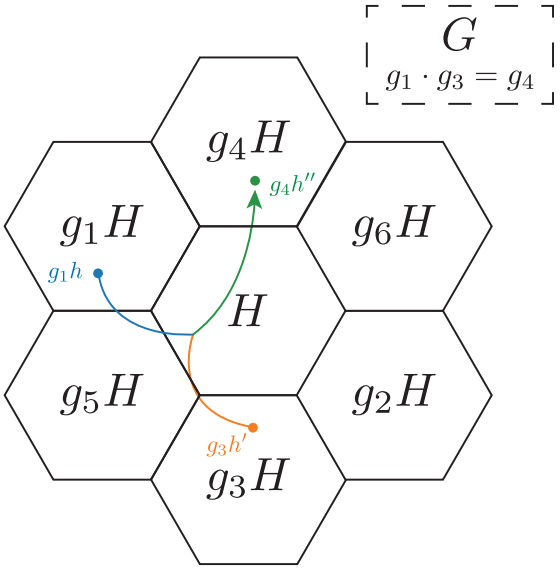

Figure 3: Illustration of a cartoon example used to visualize how a group splits up into cosets. The entire honeycomb pattern represents the group, and each coset is represented by a single hexagon, labeled either H or g_iH. Note that the subgroup H itself contains the element $e \in H$, and each coset contains $g_i \in g_iH$. TODO multiplication

Equivalently, $N_G(H) = G$. If H is a normal subgroup of G, we write[a]

$$H \trianglelefteq G. \tag{84}$$

[a]Our usual notation applies where we will use $H \trianglelefteq G$ to denote H is a normal subgroup of G (and can still be G): if we want to emphasize that H is a proper normal subgroup of G, we will write $H \triangleleft G$.

At its essence, normality is a "lighter" version of commutativity: it is commutativity on the order of a subgroup. The reason that normality shows up

Theorem 5: First isomorphism theorem

Let $\phi : G \to G'$ be a group homomorphism. Then we have the isomorphism,

$$\mathrm{im}(\phi) \cong G/\ker(\phi). \tag{85}$$

TODO figures to make

- Cosets partitioning a group
- Elements in different cosets having the group law given by the quotient
- Color-code a multiplication table according to cosets: probably do the D_8 one modded out by $\langle r \rangle$, but also might want to do a more interesting one

Example 4: Abelianization

Quotienting a group out by a subgroup is a good way to impose relations on the original group and get back the "best" copy of the original group consistent with those relations. What does this mean? Suppose we have a group G and two distinct elements g, g', and we want to see what happens to the structure of the group if we impose that $g = g'$.

0.5 Group Actions

It's often stated that groups are the set of symmetries of an object– in fact, when I took an algebra class with Richard Borcherds, he used this as the definition of a group. I'm not sure it was a rigorous mathematical definition, but it was an interesting perspective nonetheless. Given a group, your first question is often "what is this the set of symmetries of?" This is often a set or object that the group is defined *externally* from. Note that even if a group is defined as a symmetry group (i.e., the dihedral group D_{2n}), it can be abstractly defined *independently* of the object that it is the symmetries of: for example, D_{2n} exists regardless of the notion of a polygon, which is clear because we can write it down as its presentation $\langle r, s | rs = sr^{-1}, r^n = 1 \rangle$. Even if we didn't know what a n-gon was, this version of D_{2n} would still exist and could be studied.

We defined D_{2n} implicitly in terms of an *group action* it had on the regular n-gon Δ_n. Group actions are the study of this section: they provide us a way to **act** our group G on a different set, which we will call X. This allows us to actually **realize** what a group does on another set, and interpret a group as the set of symmetries of something. Group actions will later be extended with **representation theory**, which is a specific flavor of action that has lots of interesting properties.

Definition 12: Group action

A (left) **group action** is a map $\cdot : G \times X \to X$ which satisfies the following properties:

1. Identity: For any $x \in X$, $e \cdot x = x$.
2. Associativity: For $g, h \in G$ and $x \in X$, $g \cdot (h \cdot x) = (g \cdot h) \cdot x$, where $g \cdot h$ denotes group multiplication.

We can likewise define a **right group action** as a map $X \times G \to X$ satisfying comparable axioms.

A group action allows us to permute the elements of X in a way that is *consistent* with the group multiplication law. We often want to emphasize that for each g, we get a permutation of the set X: we will thus often denote the action as parameterized maps $\sigma_g : X \to X$ given by $\sigma_g(x) := g \cdot x$ for each $x \in X$.

Indeed, for a fixed $g \in G$, we have two actions on G. First, the **left action** $h \mapsto g \cdot h$, and second, the **right action** $h \mapsto h \cdot g$. Note these are equivalent if G is abelian.

Theorem 6: Cayley

Let G be a finite group of order $n = |G|$. Then, G can be embedded into S_n.

This is one of my favorite theorems in group theory, and it's relatively easy to prove. This is such an interesting result because it tells you that **any finite group** can be interpreted as a permutation group. Recall that an embedding $\sigma : G \hookrightarrow S_n$ means that G is isomorphic onto its image $\sigma(G)$, which is a subgroup of S_n. Since isomorphism is how we determine if two groups are "equal", this means that G can be interepreted as a **subgroup of** S_n. So, this theorem implies that any finite group can be interpreted as a subgroup of a permutation group. Let's prove it.

Proof. This is a construction proof: note that $S_G \cong S_n$, so WLOG we need to explicitly construct the embedding $\sigma : G \to S_G$. For $g \in G$, consider the **left translation**[6] **representation of** g **on** G,

$$\ell_g : G \to G \qquad\qquad h \mapsto g \cdot h. \tag{86}$$

ℓ_g is simply the function on G that multiplies each element of G by g on the left. We want to show that $g \mapsto \ell_g$ is the desired embedding of G into S_G. So, we need to show three things:

1. $\ell_g \in S_G$, i.e. that ℓ_g is indeed a permutation of G. This tells us that the map $G \to S_G, g \mapsto \ell_g$ is indeed well-defined.
2. $g \mapsto \ell_g$ is a group homomorphism.
3. $g \mapsto \ell_g$ is injective.

Let's prove these one-by-one.

1. We must show that ℓ_g is a permutation (bijection) of G. Indeed, ℓ_g is injective because $\ell_g(h) = \ell_g(h') \implies g \cdot h = g \cdot h' \implies h = h'$. Furthermore, it is surjective because for each $h \in G$, note that $g^{-1} \cdot h \in G$, and $\ell_g(g^{-1} \cdot h) = g \cdot (g^{-1} \cdot h) = h$. Hence $\ell_g \in S_G$.
2. $g \mapsto \ell_g$ is a group homomorphism. Let $g, h \in G$, and we need to show that $\ell_{g \cdot h} = \ell_g \circ \ell_h$. This is the equality of maps: so, let $x \in G$. Then $\ell_{g \cdot h}(x) = (g \cdot h) \cdot x = g \cdot (h \cdot x) = g \cdot \ell_h(x) = (\ell_g \circ \ell_h)(x)$. Since this holds for each $x \in G$, we have equality $\ell_{g \cdot h} = \ell_g \circ \ell_h$.
3. $g \mapsto \ell_g$ is injective. This is immediate: the kernel of a homomorphism always contains the identity, but for $g \neq e$, then $\ell_g(e) = g$, hence $\ell_g \neq \mathrm{id}$. Thus we are done!

□

I like to think about the Cayley theorem when discussing group actions because this is another way to think about how a group acts on itself.

TODO discuss the permutation representation of a group action: have $\sigma_g(x) := g \cdot x$, and $\sigma_g \in S_X$. So we get a homomorphism $g \mapsto \sigma_g$ which

TODO conjugacy classes

TODO class equation

[6] There is also a corresponding right translation representation $r_g : G \to G$, $h \mapsto h \cdot g$, which agrees with ℓ_g only when $g \in Z(G)$.

0.6 Semidirect and Wreath Products

0.7 The Sylow Theorems