Group Theory

Bendit Chan

October 23, 2022

Disclaimer

This is a set of handouts dedicated to cover elementary group theory. The content is heavily based on the course notes of the courses M40003 – Linear Algebra & Groups and M50005 – Groups & Rings in Imperial College London, J. S. Milne's "*Group Theory*"[1], and Evan Chen's "*An Infinitely Large Napkin*"[2], so all credits go to them.

[2] https://www.jmilne.org/math/CourseNotes/gt.html
[2] https://venhance.github.io/napkin/Napkin.pdf

Contents

Note. Following Ravi Vakil's style, we use $\star$ to denote topics worth knowing on a second (but not first) reading.

1 Basics

A group is one of the most basic structures in higher mathematics. In this section, we will introduce some basic group theory to kickstart our journey.

1.1 Groups and Subgroups

A group consists of two data: a set G, and an associative binary operation $\star$ with some properties. Before the definition, let's first look at a motivational example:

Motivation

Lets look at one of the simplest group: the pair $(\mathbb{Z}, +)$. The set is $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and the associative operation is *addition*. Note that

- the element $0 \in \mathbb{Z}$ is an **identity**: $a + 0 = 0 + a = a$ for any a;
- every element $a \in \mathbb{Z}$ has an additive **inverse**: $a + (-a) = (-a) + a = 0$.

This makes $\mathbb{Z}$ a group under addition.

From this, you might already have a guess on what the definition of a group is:

Definition 1.1 (Group)

A **group** is a pair $G = (G, \star)$ consisting of a set of elements G and a binary operation $\star : G \times G \to G$ such that

(G1) the operation is **associative**: $(a \star b) \star c = a \star (b \star c)$ for any $a, b, c \in G$;

(G2) G has an **identity** element: there exists $e \in G$ such that

$$g \star e = e \star g = g \text{ for all } g \in G;$$

(G3) every element in G has an **inverse**: for any $g \in G$, there exists $h \in G$ such that

$$g \star h = h \star g = e.$$

Remark. Some authors like to add a "closure" axiom, i.e. to say that $g \star h \in G$ for any $g, h \in G$. This is implied already by the fact that $\star$ is a binary operation on G, but is worth keeping in mind nonetheless.

Note that associativity essentially means that brackets do not affect the result of the operation, so we usually omit the parentheses. However, this does NOT imply that $\star$ is commutative ($g \star h = h \star g$ for all $g, h \in G$). So we say a group is **abelian** if the operation is commutative and **non-abelian** otherwise.

Example 1.2 (Rationals)

You have seen one example of groups above. Here is another classic example:

- The pair $(\mathbb{Q}, \cdot)$ is NOT a group: while there is an identity element, the element 0 does not have an inverse.
- However, $(\mathbb{Q}^\times, \cdot)$ where $\mathbb{Q}^\times$ denotes the set of **non-zero** rational numbers, is a group: multiplication is obviously associative, and
  - the element $1 \in \mathbb{Q}^\times$ is an identity: for any $a \in \mathbb{Q}^\times$, $a \cdot 1 = 1 \cdot a = a$;
  - for any $a \in \mathbb{Q}^\times$, there is an inverse $a^{-1} = 1/a$ so that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

  In other words, taking out 0 from $\mathbb{Q}$ makes it a group.

Example 1.3 (Complex unit circle)

Let S^1 denote the set of complex numbers z with absolute value one; that is

$$S^1 := \{z \in \mathbb{C} : |z| = 1\}.$$

Then $(S^1, \times)$ is a group because

- the complex number $1 \in S^1$ is an identity element;
- each complex number $z \in S^1$ has an inverse $1/z$ which is also in S^1, since $|z^{-1}| = 1/|z| = 1$.

There is one more thing that has to be checked as well: that $\times$ is actually a binary operation on S^1 (the closure axiom mentioned in the remark under Definition 1.1). But this follows from $|z_1 z_2| = |z_1|\ |z_2| = 1$.

Notice that all examples above are abelian. We now introduce some non-abelian examples:

Example 1.4 (Linear groups $\star$)

If you know some linear algebra, the following examples should be familiar:

- Let n be a positive integer. We define

  $$\mathrm{GL}_n(\mathbb{R}) := \{n \times n \text{ real matrices } A : \det A \neq 0\}.$$

  The identity element is I_n. With the extra condition, any matrix has an inverse. Moreover, $\det(AB) = \det A \cdot \det B$ so $\mathrm{GL}_n(\mathbb{R})$ is closed. Thus $(\mathrm{GL}_n(\mathbb{R}), \times)$ is a group, called the **general linear group**.
- Following the example above, if we define

  $$\mathrm{SL}_n(\mathbb{R}) := \{n \times n \text{ real matrices } A : \det A = 1\},$$

  then similarly $(\mathrm{SL}_n(\mathbb{R}), \times)$ is a group, called the **special linear group**.

Before we move on to more examples, we shall first cover some crucial properties of groups.

Remark. From now on, we will often refer to a group $(G, \star)$ as simply G. Moreover, we abbreviate $a \star b$ to just ab, and similarly $g \star \cdots \star g$ to g^n where n is the number of g's.

Proposition 1.5

Let G be a group. Then

(i) the identity of G is unique (so we denote the unique identity by e or sometimes e_G);

(ii) the inverse of any $g \in G$ is unique (so we denote the unique inverse by g^{-1});

(iii) for any $g, h \in G$, $(g^{-1})^{-1} = g$ and $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. The proof of this is just some simple manipulations:

(i). If e and f are identities, then $e = e \star f = f$.

(ii). If h and h' are inverses to g, then $h = h \star (g \star h') = (h \star g) \star h' = h'$.

(iii). We have $g \star g^{-1} = g^{-1} \star g = e$, so by definition g is the inverse to g^{-1}, i.e. $(g^{-1})^{-1} = g$.

For the second part, we compute

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = e.$$

Similarly $(h^{-1}g^{-1})(gh) = e$ as well. This shows that $h^{-1}g^{-1}$ is the inverse to gh, i.e. $(gh)^{-1} = h^{-1}g^{-1}$. □

The following important lemma about groups shows why having an inverse is valuable:

Lemma 1.6 (Left multiplication is a bijection)
Let G be a group and $g \in G$. Then the map $\phi_g : x \mapsto gx$ is a bijection.

Proof. It suffices to check:

- ϕ_g is injective: Suppose $\phi_g(x) = \phi_g(y)$, i.e. $gx = gy$. "Multiplying" g^{-1} on both sides gives
$$g^{-1}gx = g^{-1}gy \implies ex = ey \implies x = y$$
as desired. (This is often called the **cancellation law**.)
- ϕ_g is surjective: Let $y \in G$. Then
$$\phi_g(g^{-1}y) = gg^{-1}y = ey = y$$
so ϕ_g maps $g^{-1}y$ to y, i.e. it is surjective. □

Finally, we will introduce a more sophistacated but important example; this acts as a fundamental example in later discussions.

Example 1.7 (Symmetric group)
The **symmetric group** S_n consists of *permutations* of $\{1, 2, \dots, n\}$, i.e. bijections $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$.

- We denote an element σ by the notation
$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$
Note that the second row is an "rearrangement" of the first row.
- The group operation is given by composition, which is also a permutation of $\{1, 2, \dots, n\}$.

This is indeed a group: the identity is given by the identity function $\mathrm{id}(x) = x$, and inverses exist because elements of S_n are bijections. Moreover, it is finite: $|S_n| = n!$ (or we also say S_n is a group of **order** $n!$).

Remark. More generally, we might define the **symmetric group** $\mathrm{Sym}(X)$ for any finite set X to be the permutations of X (again this is a group by the same argument). Then $S_n = \mathrm{Sym}(\{1, 2, \dots, n\})$.

Here's an explicit example of the group operation on S_4. Consider
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$
Then to compute $\alpha \circ \beta$, we note that
$$1 \xmapsto{\beta} 2 \xmapsto{\alpha} 4 \qquad 3 \xmapsto{\beta} 4 \xmapsto{\alpha} 3$$
$$2 \xmapsto{\beta} 1 \xmapsto{\alpha} 2 \qquad 4 \xmapsto{\beta} 3 \xmapsto{\alpha} 1$$
and thus we conclude (with a similar computation for $\beta \circ \alpha$) that
$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$
Note in particular that these two are still permutations, and $\alpha \circ \beta \neq \beta \circ \alpha$, so S_4 is non-abelian.

Caution: When calculating $\alpha \circ \beta$, β is the first permutation being applied (since $\alpha \circ \beta(x) = \alpha(\beta(x))$).

We now proceed to introduce a new concept. Recall that $\mathrm{GL}_n(\mathbb{R})$, the $n \times n$ matrices with nonzero determinant, forms a group under matrix multiplication. At the same time, the subset $\mathrm{SL}_n(\mathbb{R})$ also formed a group with the same operation. For this reason we say $\mathrm{SL}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. This generalises to the following.

Definition 1.8 (Subgroup)

Let $(G, \star)$ be a group and $H \subseteq G$. We say H is a **subgroup** of G if $(H, \star)$ is a group, and is denoted by $H \leq G$. H is a **proper subgroup** if $H \neq G$.

To specify a group G, we need to know both the set G and the operation $\star$. But to specify a subgroup H of a given group G, we only need to know the elements: the operation is inherited from the operation of G.

Example 1.9 (Examples of subgroups)

- As a trivial example, $\{e\}$ and G are both subgroups of any group G.
- $2\mathbb{Z} = \{\ldots, -2, 0, 2, \ldots\}$ is a subgroup of $\mathbb{Z}$ (with operation $+$).
- Consider again S_n, and let T be the set of permutations $\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$ for which $\tau(n) = n$. Then T is a subgroup of S_n: indeed $\mathrm{id} \in T$, and τ^{-1} also sends n to n for any $\tau \in T$, so $\tau^{-1} \in T$.

Before we move on, a subgroup has an equivalent formulation:

Proposition 1.10 (Test for a subgroup)

Let G be a group and $H \subseteq G$. Then H is a subgroup of G if and only if

- H is non-empty;
- for all $h_1, h_2 \in H$, we have $h_1 h_2 \in H$ (closed under group operation);
- for all $h \in H$, we have $h^{-1} \in H$ (closed under inverses).

Proof. ($\Leftarrow$) is simple routine. For ($\Rightarrow$), H is a group, so it has an identity e_H and it is closed, thus the first two conditions are already satisfied.

To show the third condition, we show that $e_G \in H$, i.e. H must share the identity of G. Let $h \in H$, then $he_H = h$. By the cancellation law, $e_H = e_G$. Similarly, we know h has an inverse $h' \in H$, i.e. $hh' = e_H = e_G$. But multiplying h^{-1} gives $h' = h^{-1} \in H$, as desired. □

Next is an especially important example that we'll talk about more later:

Example 1.11 (Subgroup generated by an element)

Let g be an element of a group G. Recall that $g^m = g \star \cdots \star g$ with m g's, and $g^{-m} = (g^{-1})^m$. Consider the set

$$\langle g \rangle = \{g^m : m \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}.$$

Then using the above proposition, this is a subgroup of G:

- $\langle g \rangle$ is non-empty since $e \in \langle g \rangle$.
- Let $g^n, g^m \in \langle g \rangle$. Then $g^n g^m = g^{n+m} \in \langle g \rangle$, which can be proved by induction.
- Let $g^n \in \langle g \rangle$. Then similarly one can prove $(g^n)^{-1} = g^{-n} \in \langle g \rangle$.

We call this the **(cyclic) subgroup generated by** g.

Note that $\langle g \rangle$ is abelian since $g^n g^m = g^{n+m} = g^m g^n$ for any $m, n \in \mathbb{Z}$. Also, although $\mathbb{Z}$ is infinite, $\langle g \rangle$ can be finite: this happens if $g^m = e$ for some $m \in \mathbb{Z}$.

Definition 1.12 (Cyclic groups)

We say a group G is **cyclic** if there is $g \in G$ such that $\langle g \rangle = G$. In this case, g is called a **generator** of G.

Thus a cyclic group must be abelian, but not conversely:

Example 1.13 (Klein four-group)

Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in S_4.$$

Then $K_4 = \{\mathrm{id}, \alpha, \beta, \gamma\}$ is a subgroup of S_4, called the **Klein four-group**. One can check that K_4 is abelian. However, note that $g^2 = \mathrm{id}$ for all $g \in K_4$, so

$$\langle g \rangle = \{\mathrm{id}, g\} \quad \text{for all } g \in K_4,$$

i.e. K_4 is not cyclic.

This concludes our examples of groups for now.

1.2 Orders and Cyclic groups

We now dive into more details based on the notion of cyclic groups as mentioned above. By the discussion, $\langle g \rangle$ is finite iff $g^m = e$ for some $m \in \mathbb{Z}$. Thus it makes sense to define:

Definition 1.14 (Order of an element)

The **order of an element** $g \in G$ is the smallest positive integer n such that $g^n = e$, or ∞ if no such n exists. We denote this by $\operatorname{ord} g$.

Caution: You might recall that the word order has appeared once before: the **order of a group** G is the number of elements in G, or in other words $|G|$. This is unfortunately quite confusing.

However, from another perspective this makes perfect sense, because of the following:

Theorem 1.15

Suppose G is a group and $g \in G$ has finite order n. Then

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}.$$

In particular, $\operatorname{ord} g = |\langle g \rangle| = n$, so the two notions of order coincide.

To prove this, the key step is the following lemma.

Lemma 1.16

For $a, b \in \mathbb{Z}$, we have $g^a = g^b$ if and only if $a \equiv b \pmod{n}$.

Proof. ($\Leftarrow$) is simple. For ($\Rightarrow$), if $g^a = g^b$, then $g^{a-b} = e$. By division algorithm, there are $q, r \in \mathbb{Z}$ such that $a - b = qn + r$ and $0 \le r < n$. Then

$$e = g^{a-b} = g^{qn+r} = (g^n)^q \cdot g^r = g^r.$$

Now by minimality of n (as the order of g), r must be 0. Thus $n \mid a - b$, as needed. □

Proof of Theorem 1.15. Every $m \in \mathbb{Z}$ is congruent to exactly one of $0, 1, \ldots, n-1$ modulo n, so $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$ reduces to $\{e, g, g^2, \ldots, g^{n-1}\}$ after removing duplicated elements. □

In other words, putting everything in a concise sentence:

! Keypoint

The order of $g \in G$ is the order of $\langle g \rangle$.

Example 1.17 (Examples of orders)

- The order of -1 in $\mathbb{Q}^\times$ is 2, since $(-1)^1 \neq 1$ and $(-1)^2 = 1$.
- The order of 1 in $\mathbb{Z}$ is ∞.
- Consider the group $\mathbb{Z}/6\mathbb{Z} = \{[0], [1], \ldots, [5]\}$. The operation is defined via addition modulo 6: for example, $[4] + [5] = [9] = [3]$. Then this group is cyclic since $\mathbb{Z}/6\mathbb{Z} = \langle [1] \rangle$. We can find the order of each element:

Element	[0]	[1]	[2]	[3]	[4]	[5]
Order	1	6	3	2	3	6

Can you see a pattern here?

The last example suggests a more thorough discussion on cyclic groups. Namely, how do subgroups of cyclic groups behave? Or more specifically, given a cyclic group G, how should we choose a generator g?

Motivation

Consider another group, $(\mathbb{Z}/7\mathbb{Z})^\times = \{[1], [2], \ldots, [6]\}$, the *non-zero* residues modulo 7. The operation is defined via multiplication modulo 7: for example, $[4] \cdot [5] = [20] = [6]$. Although this group is indeed cyclic, it now becomes **non-trivial to find a generator**. The only way to do this is to compute the order of each element:

Element	[1]	[2]	[3]	[4]	[5]	[6]
Order	1	3	6	3	6	2

Thus, it turns out that [3] and [5] are possible generators.

(If you know some olympiad number theory, you might recognise 3 and 5 as **primitive roots** modulo 7.)

Finding primitive roots modulo n is in general a difficult process. But, an easier question to answer is whether we can determine all primitive roots given one of them. The answer is yes (in the case that primitive roots actually exist), and more generally there is a nice result on cyclic groups telling us everything about their subgroups:

Theorem 1.18

Suppose G is a cyclic group and $G = \langle g \rangle$. We have the following:

(i) If $H \leq G$, then H is cyclic.

(ii) Suppose $|G| = n$ and $m \in \mathbb{Z}$. Let $d = \gcd(m, n)$, then

$$\langle g^m \rangle = \langle g^d \rangle \quad \text{and} \quad |\langle g^d \rangle| = n/d.$$

In particular, $\langle g^m \rangle = G = \langle g \rangle$ if and only if $\gcd(m, n) = 1$.

(iii) If $|G| = n$ and $k \leq n$, then G has a subgroup of order k if and only if $k \mid n$ (and the subgroup is $\langle g^{n/k} \rangle$).

Proof. (i). WLOG assume that $H \neq \{e\}$. Let $d := \min\{n \in \mathbb{N} : g^n \in H\}$. We claim that $H = \langle g^d \rangle$.

Indeed, as $g^d \in H$ and $H \leq G$, we have $\langle g^d \rangle \leq H$. For the other direction, let $h \in H$, then $h = g^m$ for some $m \in \mathbb{Z}$. Write $m = qd + r$ by division algorithm with $0 \leq r < d$, so

$$h = g^{qd+r} = (g^d)^q g^r \implies g^r = h(g^d)^{-q} \in H,$$

as $h \in H$ and $g^d \in H$. Minimality of d gives $r = 0$ and $h = (g^d)^q \in \langle g^d \rangle$.

(ii). By Bézout identity, there are $a, b \in \mathbb{Z}$ such that $d = am + bn$.

To show that $\langle g^m \rangle = \langle g^d \rangle$, it is enough to prove that $g^m \in \langle g^d \rangle$ and $g^d \in \langle g^m \rangle$. Since $d \mid m$, g^m is a power of g^d, so the former is true. For the latter, we have

$$g^d = g^{am+bn} = (g^m)^a (g^n)^b = (g^m)^a \in \langle g^m \rangle$$

since $n = \operatorname{ord} g$ and $g^n = e$.

Now let's consider $|\langle g^d \rangle|$. Since $d \mid n$ we have $n = kd$ for some $k \in \mathbb{N}$, and so $\langle g^d \rangle = \{e, g^d, \dots, g^{(k-1)d}\}$. These are all distinct since $d, \dots, (k-1)d$ are all less than n, so $|\langle g^d \rangle| = k = n/d$.

(iii). This follows from (i) and (ii). □

This is a whole lot to digest, so let's try to apply this result on the last two examples:

Example 1.19 (Properties of cyclic groups)

- Consider $(\mathbb{Z}/6\mathbb{Z}, +)$ where the addition is modulo 6. We have already seen that $\mathbb{Z}/6\mathbb{Z} = \langle [1] \rangle$, so $g = [1]$. By Theorem 1.18(ii), the generators of this group are $[1]^1$ and $[1]^5$ since $\gcd(1, 6) = \gcd(5, 6) = 1$. Indeed,
$$[1]^5 = \underbrace{[1] + \cdots + [1]}_{5 \text{ times}} = [5].$$
- Similarly, for $((\mathbb{Z}/7\mathbb{Z})^\times, \cdot)$, we may pick $g = [3]$, so Theorem 1.18(ii) tells us again that $[3]^1$ and $[3]^5$ are generators. Indeed,
$$[3]^5 = \underbrace{[3] \cdot \cdots \cdot [3]}_{5 \text{ times}} = [5].$$

We will give an application of the previous theorem to prove a result by Gauss, on the following function.

Definition 1.20 (Euler totient function)

For $n \in \mathbb{N}$, the **Euler totient function** $\phi(n)$ is the number of $k \in \mathbb{N}$ with $1 \le k \le n$ such that $\gcd(k, n) = 1$.

This function is crucial in nnumber theory, and the following corollary is one of its major feature:

Corollary 1.21

For all $n \in \mathbb{N}$ we have

$$\sum_{d \mid n} \phi(d) = n.$$

Proof. Let G be a cyclic group of order n. By Theorem 1.18(iii), if $d \mid n$ then G has a **unique** subgroup G_d of order d. But then for each element $g \in G$ with $\operatorname{ord} g = d$, we have $|\langle g \rangle| = d$, so $\langle g \rangle = G_d$. In particular $g \in G_d$, so G_d contains every element of G of order d.

Now by Theorem 1.18(i), G_d is cyclic, and so by Theorem 1.18(ii), G_d has $\phi(d)$ elements of order d. Counting elements of G based on their order gives the result. □

Naturally, one would consider groups generated by more than one element. For instance, we can define:

Definition 1.22 (Subgroup generated by a set)

Let G be a group and $S \subseteq G$ be non-empty. Write $S^{-1} = \{g^{-1} : g \in G\}$, then

$$\langle S \rangle := \{g_1 \dots g_k : k \in \mathbb{N} \text{ and } g_1, \dots, g_k \in S \cup S^{-1}\}$$

is the **subgroup generated by** S.

We will postpone the study of these subgroups to Section 3.

1.3 Lagrange's Theorem and Cosets

The main theorem we want to prove in this section is as follows:

Theorem 1.23 (Lagrange's Theorem)

Suppose G is a finite group and H is a subgroup of G. Then $|H|$ divides $|G|$.

This theorem has a plethora of applications, as we will see later. To prove this theorem, we need to introduce an essential definition:

Definition 1.24 (Cosets)

Let G be a group, $H \leq G$, and $g \in G$. The subset

$$gH := \{gh : h \in H\} \subseteq G$$

is called a **left coset** of H in G. Similarly, a **right coset** is a subset of the form Hg.

Motivation

How should one think about cosets? The fundamental example is of "modding things out": consider $G = \mathbb{Z}$ and $H = 100\mathbb{Z} = \{100n : n \in \mathbb{Z}\}$. The cosets of H are (written additively since the operation in G is $+$)

$$\begin{aligned} H &= \{\ldots, -200, -100, 0, 100, 200, \ldots\} \\ 1 + H &= \{\ldots, -199, -99, 1, 101, 201, \ldots\} \\ 2 + H &= \{\ldots, -198, -98, 2, 102, 202, \ldots\} \\ &\vdots \\ 99 + H &= \{\ldots, -101, -1, 99, 199, 299, \ldots\}. \end{aligned}$$

The elements of each set have the **same remainder when dividing by** 100, so it is natural to group them together. Moreover, any two elements in different cosets have different remainders.

Thus, from now on, we will think of the *elements* of $\mathbb{Z}/100\mathbb{Z}$ as cosets: for example $[3] = [103] = [-197]$ is the coset $3 + 100\mathbb{Z}$. We will explain this idea further in Section 2.1.

Caution: Although the notation might not suggest it, keep in mind that g_1H is often equal to g_2H even if $g_1 \neq g_2$. In the above example, $3 + H = 103 + H$. In other words, these cosets are *sets*. Or, for instance, given that

$$x + 100\mathbb{Z} = \{\ldots, -197, -97, 3, 103, 203, \ldots\},$$

there's no reason to think I picked $x = 3$. (I actually picked $x = -13597$.)

Although the above is intuitively how you should remember cosets, they can look vastly different based on what group we are in:

Example 1.25 (More examples of cosets)

- Let $G = (\mathbb{C}^\times, \cdot)$ and $H = \{z \in G : |z| = 1\}$, where $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. Note that $H \leq G$. Then

  $$2H = \{2e^{i\theta} : \theta \in \mathbb{R}\} = \{z \in G : |z| = 2\}$$

  is a left coset of H.

- Let $G = (\mathbb{R}^n, +)$ and $H = \{\mathbf{x} \in G : A\mathbf{x} = 0\}$ for some fixed $m \times n$ matrix A with real entries. Again note that $H \leq G$. Now suppose $\mathbf{b} \in \mathbb{R}^m$ and there exists $\mathbf{v} \in \mathbb{R}^n$ with $A\mathbf{v} = \mathbf{b}$. Then

  $$A\mathbf{x} = \mathbf{b} \iff A(\mathbf{x} - \mathbf{v}) = 0 \iff \mathbf{x} - \mathbf{v} \in H \iff \mathbf{x} \in \mathbf{v} + H,$$

  i.e. the set of solutions to $A\mathbf{x} = \mathbf{b}$ (if non-empty) is a coset of H.

We saw in the previous examples that, for a fixed subgroup H, the left H-cosets partition G: every element of G is in exactly one left H-coset. This is in fact a general phenomenon:

Lemma 1.26 (Cosets partition a group)

Let G be a group and $H \leq G$. Suppose $g_1, g_2 \in G$.

(i) If $g_1 \in g_2H$, then $g_1H = g_2H$.

(ii) If $g_1H \cap g_2H \neq \emptyset$, then $g_1H = g_2H$.

Proof. (i). ($\subseteq$). As $g_1 \in g_2H$, there exists $h \in H$ with $g_1 = g_2h$. Take any $g_1h' \in g_1H$, then

$$g_1h' = (g_2h)h' = g_2(hh') \in g_2H$$

where $hh' \in H$ since $H \leq G$. ($\supseteq$) follows too by noticing that $g_2 = g_1h^{-1} \in g_1H$.

(ii). Let $x \in g_1H \cap g_2H$. By (i), applied twice, we have $g_1H = xH = g_2H$. □

In addition, similar to Lemma 1.6, the map $H \to gH$ given by $h \mapsto gh$ is a bijection. Hence if H is finite, $|H| = |gH|$, or in other words, all cosets have the same cardinality. In conclusion,

! Keypoint

Cosets of a group G partition G into equal size subsets.

Now the proof of Lagrange's Theorem should be clear:

Proof of Theorem 1.23. All left cosets of H in G have size $|H|$, and any two of them are disjoint (by Lemma 1.26). Moreover, any $g \in G$ lies in some left H-coset, namely gH.

Hence $|G|$ is equal to $|H|$ times the number of distinct left cosets of H (which we define as the **index of H in G**, denoted $[G : H]$). □

Example 1.27 (Computing all cosets of a subgroup)

Consider $G = S_3$ and $H = \langle\alpha\rangle$, where $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Let's try to compute all left cosets of H:

- Note that $H = \{\mathrm{id}, \alpha\}$ so $|H| = 2$. Together with $|G| = 6$ we know that there are 3 left H-cosets. One of them must be $H = \mathrm{id}\, H = \alpha H$.
- Picking anything which is not id or α would give us a new coset, so let's take $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Thus $\beta H = \{\beta, \beta\alpha\}$ is the second coset.
- Finally, we compute that $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, so let $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \notin \alpha H \cup \beta H$ which gives the remaining left coset, $\gamma H = \{\gamma, \gamma\alpha\}$.

In this example we exploited the fact that cosets partition the group G.

Let us now use Lagrange's Theorem to prove a list of corollaries.

Corollary 1.28

Let G be a finite group of order n, and $g \in G$. Then $\operatorname{ord} g \mid n$ and $g^n = e$.

Proof. The first statement follows from Lagrange's Theorem applied on $H = \langle g\rangle$. Now if $k = \operatorname{ord} g$ then $g^n = (g^k)^{n/k} = e^{n/k} = e$ since $k \mid n$. □

As a special case, we have the well-known:

Corollary 1.29 (Fermat's little theorem)

Let p be a prime. If $x \in \mathbb{Z}$ and $p \nmid x$, then $x^{p-1} \equiv 1 \pmod{p}$.

Proof. Consider the group $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ where $(\mathbb{Z}/p\mathbb{Z})^\times$ is the set of non-zero elements of $\mathbb{Z}/p\mathbb{Z}$. Then $|G| = p-1$, and so by Corollary 1.28,

$$[x^{p-1}] = [x]^{p-1} = [1] \text{ for all } [x] \in G,$$

i.e. $x^{p-1} \equiv 1 \pmod{p}$ for all $x \not\equiv 0 \pmod{p}$. □

Finally, we can obtain a result which classifies all groups of prime order:

Corollary 1.30 (Groups of prime order are cyclic)

Suppose G is a group of prime order. Then G is cyclic, and if $e \neq g \in G$ then $G = \langle g \rangle$.

Proof. By Lagrange's Theorem, $|\langle g \rangle|$ divides p, so $|\langle g \rangle| = 1$ or p. As $e, g \in \langle g \rangle$ and $e \neq g$ we must have $|\langle g \rangle| = p$, or $\langle g \rangle = G$, as desired. □

1.4 Homomorphisms

After the discussion on groups, it is time to study functions between groups as well. In particular, we would like to study **structure-preserving** functions. This motivates the definition of homomorphisms:

Definition 1.31 (Homomorphisms)

Let $(G, \star)$ and $(H, *)$ be groups. A **homomorphism** is a function $\phi : G \to H$ such that for any $g_1, g_2 \in G$,

$$\phi(g_1 \star g_2) = \phi(g_1) * \phi(g_2).$$

If this map is a bijection, it is an **isomorphism**. We then say G and H are **isomorphic** and write $G \cong H$.

In other words, homomorphisms are functions preserving the group operation.

Motivation

Before we give examples of homomorphisms, let us focus on isomorphisms and understand them intuitively. Consider the two groups

$$\mathbb{Z} = (\{\ldots, -2, -1, 0, 1, 2, \ldots\}, +)$$
$$10\mathbb{Z} = (\{\ldots, -20, -10, 0, 10, 20, \ldots\}, +)$$

These groups are "different", but only superficially so. Specifically, the map

$$\phi : \mathbb{Z} \to 10\mathbb{Z} \text{ by } x \mapsto 10x$$

is a bijection of the underlying sets which respect the group action, i.e. $\phi(x + y) = \phi(x) + \phi(y)$.

This means that one should remember isomophisms in the following manner:

! Keypoint

Isomorphic groups are just the "same group with different names".

The isomorphism between the two groups is then explicitly saying how the names of the elements in one group should be renamed in order to get the elements in the other group.

Example 1.32 (Examples of homomorphisms)

Let G and H be groups.

- The identity map $\mathrm{id} : G \to G$ is an isomorphism, hence $G \cong G$.
- The **trivial homomorphism** $G \to H$ sends everything to e_H.
- There is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/100\mathbb{Z}$ by $x \mapsto [x]$, i.e. taking modulo 100.
- There is a homomorphism from S_n to S_{n+1} by "embedding": every permutation on $\{1, \dots, n\}$ can be thought of as a permutation on $\{1, \dots, n+1\}$ if we simply let $n+1$ be a fixed point.
- The determinant map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism since $\det(AB) = \det(A)\det(B)$.
- Specifying a homomorphism $\mathbb{Z} \to G$ is the same as specifying the image of the element $1 \in \mathbb{Z}$. Why?

Example 1.33 (Primitive roots modulo 7, revisited)

As a non-trivial example, we claim that $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/7\mathbb{Z})^\times$. The bijection is

$$\phi([a]) = [3^a]$$

where the $[a]$ on the left side is modulo 6 and the $[3^a]$ on the right is modulo 7. We need to check:

- ϕ is well-defined: If $a \equiv b \pmod 6$, then we have $a - b = 6k$ for some $k \in \mathbb{Z}$, so
$$3^a = 3^{b+6k} = 3^b \cdot (3^6)^k \equiv 3^b \pmod 7$$
since $3^6 \equiv 1 \pmod 7$ by Fermat's little theorem.
- ϕ is bijective: This follows from before that $[3]$ is a generator of $(\mathbb{Z}/7\mathbb{Z})^\times$. Explicitly,
$$(3^1, 3^2, 3^3, 3^4, 3^5, 3^6) \equiv (3, 2, 6, 4, 5, 1) \pmod 7.$$
- ϕ is a homomorphism: We want $\phi([a] + [b]) = \phi([a]) \cdot \phi([b])$; but this is just $3^{a+b} \equiv 3^a \cdot 3^b \pmod 7$.

After these examples, we have some obvious properties of homomorphisms.

Lemma 1.34

Let G, H be groups and $\phi : G \to H$ be a homomorphism. Then $\phi(e_G) = e_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.

Proof. We have $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$, and so cancellation law gives the first statement. Then

$$e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

so we also have $\phi(g^{-1}) = \phi(g)^{-1}$. □

Now comes two definitions related to a homomorphism, one of which is extremely important.

Definition 1.35 (Image and kernel)

Let $\phi : G \to H$ be a homomorphism. Then the **image** of ϕ is

$$\mathrm{im}\,\phi = \{\phi(g) : g \in G\}.$$

The **kernel** of ϕ is

$$\ker \phi = \{g : \phi(g) = e_H\}.$$

It is easy to see that they are subgroups of H and G respectively.

To start, let us first look at one particularly important property of the kernel:

Lemma 1.36
A homomorphism $\phi : G \to H$ is injective if and only if $\ker \phi = \{e_G\}$.

Proof. ($\Rightarrow$). Suppose $\phi(g) = e_H = \phi(e_G)$. Injectivity gives $g = e_G$, so $\ker \phi = \{e_G\}$.

($\Leftarrow$). Suppose $\phi(g_1) = \phi(g_2)$. Then by ϕ being a homomorphism, $\phi(g_1 g_2^{-1}) = e_H$, i.e. $g_1 g_2^{-1} \in \ker \phi$. This gives $g_1 = g_2$ as desired by assumption. □

To make this concrete, let's compute the kernel of each of our examples in Example 1.32.

Example 1.37 (Examples of kernels)

- The kernel of the identity map $\mathrm{id} : G \to G$ is $\{e_G\}$. In fact, the kernel of any isomorphism is $\{e_G\}$ since an isomorphism is injective.
- The kernel of the trivial homomorphism (by $g \mapsto e_H$) is all of G.
- The kernel of the homomorphism $\mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}$ by $x \mapsto [x]$ is precisely
$$100\mathbb{Z} = \{\ldots, -200, -100, 0, 100, 200, \ldots\}.$$
- The kernel of the embedding homomorphism $S_n \to S_{n+1}$ is trivial since it is injective.
- The kernel of the determinant map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is $\mathrm{SL}_n(\mathbb{R})$.
- Fix any $g \in G$. What is the kernel of the homomorphism $\mathbb{Z} \to G$ by $n \mapsto g^n$?

To end this section, let us give a taster of what may come afterwards. A lot of the times in group theory the goal is to classify a certain class of groups (up to isomorphism, of course); for instance, what are all the groups with order 12? As a first attempt, we can now answer two such questions:

Proposition 1.38 (There is only one cyclic group of a fixed order)
If G, H are cyclic groups of the same order, then $G \cong H$.

Proof. Let $G = \langle g \rangle$ and $H = \langle h \rangle$. Define $\phi : G \to H$ by $g^k \mapsto h^k$. We need to check:

- ϕ is well-defined: Let n be the order of G and H. We have
$$g^a = g^b \overset{(1.16)}{\Longrightarrow} n \mid a - b \overset{(1.16)}{\Longrightarrow} h^a = h^b.$$
- ϕ is bijective: Injectivity is by the implication above with arrows reversed. Surjectivity is obvious.
- ϕ is a homomorphism: We have $\phi(g^a g^b) = \phi(g^{a+b}) = h^{a+b} = h^a h^b = \phi(g^a)\phi(g^b)$. □

Proposition 1.39 (There is only one non-cyclic group of order 4)
If G is a non-cyclic group of order 4, then $G \cong K_4$.

Proof. Let $G = \{e, a, b, c\}$. As G is non-cyclic, there is no element of order 4. By Corollary 1.28, the order of a, b, c must divide 4, so this forces them to have order 2.

Now we show $ab = c$ – in fact all other possibilities are contradictory: $ab = a$ or b gives either a or b as e; and $ab = e = a^2$ gives $a = b$. Similarly we have $ba = c, \ldots, cb = a$. But now the map
$$e \mapsto \mathrm{id},\ a \mapsto \alpha,\ b \mapsto \beta,\ c \mapsto \gamma$$
is clearly an isomorphism from G to $K_4 = \{\mathrm{id}, \alpha, \beta, \gamma\}$. □

1.5 More on symmetric groups

We now devote a section to study more on symmetric groups, and alongside introduce some new examples of groups which would be useful later on. The reason why we need to care specifically about symmetric groups and their subgroups is essentially by the following (which you might skip on a first reading):

Theorem 1.40 (Cayley's theorem $\star$)

If G is a finite group, then G is isomorphic to a subgroup of S_n where $n = |G|$.

Proof. For each $g \in G$, we define $\phi_g : G \to G$ by $x \mapsto gx$. As we have seen in Lemma 1.6, this map is a bijection for any g, thus $\phi_g \in \mathrm{Sym}(G)$. Now the map

$$\phi : G \to \mathrm{Sym}(G) \text{ by } g \mapsto \phi_g$$

is an injective homomorphism:

- ϕ is a homomorphism: Let $g_1, g_2 \in G$, then
$$\phi(g_1g_2)(x) = \phi_{g_1g_2}(x) = g_1g_2x = \phi_{g_1}(g_2x) = \phi_{g_1} \circ \phi_{g_2}(x) = \phi(g_1) \circ \phi(g_2)(x).$$
- ϕ is injective: Suppose $\phi(g_1) = \phi(g_2)$ (as functions). Putting e_G into both of these functions give $g_1 = g_2$.

Hence, $G \cong \mathrm{im}\,\phi$ where $\mathrm{im}\,\phi \leq \mathrm{Sym}(G)$. Now clearly $\mathrm{Sym}(G) \cong S_n$ by relabelling the elements as $1, \ldots, n$. Thus G is isomorphic to the image of $\mathrm{im}\,\phi$ under this relabelling, which is a subgroup of S_n, as desired. □

All this is saying is that:

! Keypoint

Any finite group can be viewed as a subgroup of a symmetric group.

Remark. As a historical remark, before the definition of groups appeared, what people used to call as groups are actually "subgroups of symmetric groups". Cayley's theorem just unifies the two notions.

Now let's go back to studying symmetric groups. We will first introduce a new notation for elements in S_n: the **disjoint cycle form**. First we need a technical langauge:

Definition 1.41

Let $f, g \in S_n$ and $x \in \{1, \ldots, n\}$. We say that f **fixes** x if $f(x) = x$, and the **support** of f is

$$\mathrm{supp}(f) := \{x \in \{1, \ldots, n\} : f(x) \neq x\}.$$

We say f and g have **disjoint** support (or are disjoint) if $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \emptyset$.

Elements with disjoint supports behave nicely; more specifically, they commute:

Lemma 1.42

If $f, g \in S_n$ have disjoint supports, then $fg = gf$.

Proof. Take $x \in \{1, \ldots, n\}$. Since $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \emptyset$, x must either be fixed by f, g or both f and g. In the last case it is clear that $fg(x) = gf(x)$, so suppose x is only fixed by f.

Then from $g(x) \neq x$, we have $g(g(x)) \neq g(x)$, so $g(x) \in \mathrm{supp}(g)$ and $g(x) \notin \mathrm{supp}(f)$, or $g(x)$ is fixed by f. Thus

$$f(g(x)) = g(x) = g(f(x))$$

as desired. Similarly for the case when x is only fixed by g. □

It follows (from induction) that if $f, g \in S_n$ are disjoint, then $(fg)^n = f^n g^n$ for any $n \in \mathbb{Z}$. We are now ready to define a cycle:

Definition 1.43 (Cycles)

Let $f \in S_n$. If there exists $i_1, \ldots, i_r \in \{1, \ldots, n\}$ for some $r \leq n$ such that

$$f(i_1) = i_2,\ f(i_2) = i_3,\ \ \ldots,\ f(i_r) = i_1$$

and f fixes all other elements of $\{1, \ldots, n\}$, then f is called a **cycle of length** r, and we write f as $(i_1 i_2 \ldots i_r)$.

Example 1.44 (Examples of cycles)

- In S_6, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 2 & 6 \end{pmatrix}$ is a 3-cycle: $f = (245)$.

  Note that $f = (452) = (524)$. It is also easy to compute directly that $f^2 = (254)$ and $f^3 = \mathrm{id}$.
- $(1234) \in S_5$ is the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$.
- A 1-cycle is the identity id.

We multiply cycles in the same way for permutations (i.e. they are composition of functions). For instance, let $f = (123),\ g = (4526) \in S_6$. Then we can compute

$$\begin{aligned} 1 &\overset{g}{\longmapsto} 1 \overset{f}{\longmapsto} 2 \\ 2 &\overset{g}{\longmapsto} 6 \overset{f}{\longmapsto} 6 \\ 6 &\overset{g}{\longmapsto} 4 \overset{f}{\longmapsto} 4 \\ &\vdots \end{aligned}$$

and so $fg = (126453)$. Note that we do not always end up with a cycle: take (12) and (13425) in S_6, then

$$(12)(13425) = (134)(25)(6) = (134)(25)$$

as (6) is just the identity. Although this is not a cycle, we now have two **disjoint cycles**, and so we can compute powers easily. This is the key idea of disjoint cycle forms:

Theorem 1.45 (Disjoint cycle form)

If $f \in S_n$, then there exist cycles $f_1, \ldots, f_k \in S_n$ with disjoint supports such that $f = f_1 f_2 \cdots f_k$.

If we further assume that (i) the f_i are not 1-cycles (when $f \neq \mathrm{id}$) and (ii) $\mathrm{supp}(f_i) \subseteq \mathrm{supp}(f)$, then this representation of f is unique, up to rearrangment of f_i's. We call this the **disjoint cycle form** of f.

Before the proof, let us first look at an example of how the disjoint cycle form of an element is computed:

Example 1.46

Consider

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 1 & 6 & 9 & 3 & 8 & 7 & 2 \end{pmatrix} \in S_9.$$

The general algorithm is to start at an element of $\{1, \ldots, n\}$ and keep applying f to obtain a cycle. For instance,

$$1 \overset{f}{\longmapsto} 4 \overset{f}{\longmapsto} 6 \overset{f}{\longmapsto} 3 \overset{f}{\longmapsto} 1$$

and so (1463) is the first cycle. Similarly one could obtain $f = (1463)(259)(78)$. Note that since these cycles are disjoint, the order in which they are written doesn't matter.

Proof of Theorem 1.45. (Existence). We prove the result by strong induction on $m = |\operatorname{supp}(f)|$.

If $m = 0$ then $f = \mathrm{id} = (1)$. Now assume $m \geq 1$, and take $i_1 \in \operatorname{supp}(f)$, i.e. $f(i_1) \neq i_1$. Let $f(i_1) = i_2, f(i_2) = i_3, \ldots$, and choose r as small as possible with $f(i_r) \in \{i_1, \ldots, i_{r-1}\}$. Note that there is such an r with $r \leq n$.

We claim that $f(i_r) = i_1$. Otherwise, we have $f(i_r) = i_j$ for some $2 \leq j \leq r-1$. So

$$f(i_r) = i_j = f(i_{j-1}) \implies i_r = i_{j-1}$$

since f is bijective, contradicting minimality of r.

It follows that $f = gf_1$ where $f_1 = (i_1 \ldots i_r)$ and $\operatorname{supp}(g) = \operatorname{supp}(f) \setminus \{i_1, \ldots, i_r\}$. By induction hypothesis we can write $g = f_2 \ldots f_k$ where $f_2, \ldots, f_k$ have disjoint supports. Hence $f = f_2 \ldots f_k f_1$, a product of disjoint cycles.

(Uniqueness). Suppose we have $f = h_1 \ldots h_\ell$ as a product of disjoint cycles. We shall prove that $k = \ell$ and $\{f_1, \ldots, f_k\} = \{h_1 \ldots, h_\ell\}$. Again assume this is true for permutations with smaller support size.

Let $i_1 \in \operatorname{supp}(f)$. By rearranging the cycles if necessary we can assume that i_1 is in the cycles f_k and h_ℓ. As above let r be as small as possible with $f^r(i_1) = i_1$, then

$$f_k = (i_1, f(i_1), \ldots, f^{r-1}(i_1)) = h_\ell.$$

By cancellation law, we then have $f_1 \ldots f_{k-1} = h_1 \ldots h_{\ell-1}$, so the inductive hypothesis implies the result. □

Let us also note that the order of an element is easy to compute given its disjoint cycle form:

Theorem 1.47

Suppose $f \in S_n$ is written in disjoint cycle form as $f = f_1 \ldots f_k$ where f_i is an r_i-cycle for $1 \leq i \leq k$. Then

(i) $f^m = \mathrm{id}$ if and only if $f_i^m = \mathrm{id}$ for all $1 \leq i \leq k$.

(ii) $\operatorname{ord}(g) = \operatorname{lcm}(r_1, \ldots, r_k)$.

Proof. (i). ($\Leftarrow$) is by the fact that $f^m = f_1^m \ldots f_k^m$ (since $f_1, \ldots, f_k$ are pairwise disjoint).

For ($\Rightarrow$), we have $f_1^m \ldots f_k^m = \mathrm{id}$, but also that the f_i^m's have pairwise disjoint supports (although they are not necessarily cycles). Thus each f_i^m is the identity.

(ii). As f_i is an r_i-cycle, its order is r_i. Thus

$$f^m = \mathrm{id} \iff f_i^m = \mathrm{id} \iff r_i \mid m,$$

so the smallest m with $f^m = \mathrm{id}$ is $\operatorname{lcm}(r_1, \ldots, r_k)$. □

To end, we will introduce a type of subgroups of symmetric groups, which will be a useful example.

Definition 1.48 (Dihedral groups)

The **dihedral group of order $2n$**, denoted D_{2n}, is the group of symmetries of a regular n-gon $A_1A_2 \ldots A_n$, which includes rotations and reflections. Explicitly,

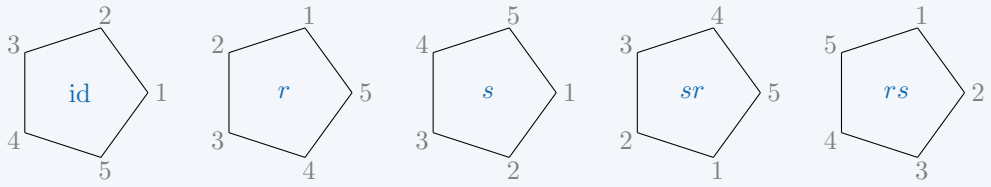
$$D_{2n} = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

where r corresponds to rotation by $\frac{2\pi}{n}$ and s corresponds to reflection across OA_1 (where O is the center of the polygon). Note that $r^n = s^2 = \mathrm{id}$ and $r^k s = sr^{-k}$.

Hence, rs means "reflect then rotate", just like function composition.

Example 1.49

Here is a picture of some elements of D_{10}:



In particular, $sr \neq rs$ so D_{10} is not abelian.

The reason why this is a subgroup of S_n should be clear: after all, r and s are both permutations on $\{1, \ldots, n\}$! Namely, we have

$$r = (12 \ldots n) \quad \text{and} \quad s = (1)(2, n)(3, n-1) \ldots$$

and $D_{2n} = \langle r, s \rangle \leq S_n$, as in Definition 1.22.

Remark. The commas in s is to avoid confusion; they are just the cycles we have seen before. The precise formula for s will also depend on whether n is odd or even.

2 Quotient Groups

We proceed to introducing an important construction of groups in this section.

2.1 Normal subgroups

Recall the motivation from before:

Motivation

Again, consider $G = \mathbb{Z}$ and $H = 100\mathbb{Z} = \{100n : n \in \mathbb{Z}\}$. The cosets of H are

$$\begin{aligned} H &= \{\dots, -200, -100, 0, 100, 200, \dots\} \\ 1 + H &= \{\dots, -199, -99, 1, 101, 201, \dots\} \\ 2 + H &= \{\dots, -198, -98, 2, 102, 202, \dots\} \\ &\vdots \\ 99 + H &= \{\dots, -101, -1, 99, 199, 299, \dots\}. \end{aligned}$$

With our understanding on homomorphisms, this can be understood as follows: we have a map $\phi : \mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}$ by "modulo 100", i.e. $x \mapsto [x]$, which has kernel

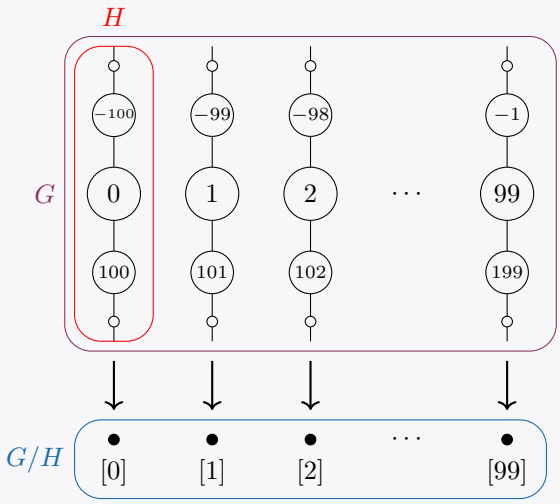
$$100\mathbb{Z} = \{\dots, -200, -100, 0, 100, 200, \dots\}.$$

What this means is that ϕ **is indifferent to the subgroup** $100\mathbb{Z}$ **of** $\mathbb{Z}$:

$$\phi(15) = \phi(2000 + 15) = \phi(-300 + 15) = \phi(700 + 15) = \cdots$$

So $\mathbb{Z}/100\mathbb{Z}$ is what we get by modding 100.

We claim that $\mathbb{Z}/100\mathbb{Z}$ should in fact be thought as the quotient of G by H. Indeed, the cosets of H divide G into equal pieces corresponding to different outputs of ϕ:



These pieces will then form a group, which is precisely $\mathbb{Z}/100\mathbb{Z}$.

Naturally we want to generalise this to a notion of a **quotient group** G/H whose elements are cosets of H. This is indeed the definition, but we have to require H to be the kernel of *some* homomorphism. Based on the naming of such subgroups we will also start to use N to notate them.

Definition 2.1 (Normal subgroups)

A subgroup N of G is called **normal** if it is the kernel of some homomorphism. We write this as $N \trianglelefteq G$.

Definition 2.2 (Quotient groups)

Let $N \trianglelefteq G$. Then the **quotient group** G/N is the group with elements as left cosets of N and the operation

$$(g_1N) \cdot (g_2N) = (g_1g_2)N.$$

Remark. It should be mentioned that by the proof of Lagrange's theorem, if G is a finite group and $N \trianglelefteq G$ then $|G/N| = |G|/|N| = [G : N]$ (the second equality holds even if N is not normal).

Clearly the identity element is $e_GN = N$ and the inverse of gN is $g^{-1}N$. We still have to check that this operation is well-defined; but let us first try to find better conditions for normal subgroups, instead of abstractly being kernels.

Lemma 2.3

Let G be a group and $N \leq G$. The following are equivalent:

(i) N is a normal subgroup of G.

(ii) For all $g \in G$ and $n \in N$, $gng^{-1} \in N$.

(iii) For all $g \in G$, $gN = Ng$.

Proof. (i $\Rightarrow$ ii). There is a homomorphism $\phi : G \to H$ with $N = \ker \phi$. Now for any $g \in G$ and $n \in N$,

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e_H,$$

so $gng^{-1} \in \ker \phi = N$.

(ii $\Rightarrow$ iii). For any $g \in G$ and $n \in N$ we have $gn \in Ng$, so $gN \subseteq Ng$. Replacing g by g^{-1} gives the other direction.

(iii $\Rightarrow$ i). Consider the homomorphism $\phi : G \to G/N$ by $g \mapsto gN$. The kernel is N since

$$n \in \ker \phi \iff \phi(n) = nN = N \iff n \in N$$

and thus N is normal. □

Lemma 2.3(iii) explains the asymmetry in the definition: although we only considered left cosets, it turns out that they coincide with right cosets if N is normal.

Example 2.4 (Examples and non-examples of normal subgroups)

- Clearly G and $\{e\}$ are normal in G.
- Every subgroup of an abelian group is normal, since $gng^{-1} = n \in N$ for any $g \in G$ and $n \in N$.
  In particular, all subgroups of $\mathbb{Z}$ are normal, and hence you can finally understand why $\mathbb{Z}/n\mathbb{Z}$ has its name!
- The subgroup $N = \{\mathrm{id}, (123), (132)\} = \langle (123) \rangle \leq S_3$ is normal, since one can check that

  $$gN = Ng = \{(12), (23), (13)\} \text{ for all } g \notin N.$$

  More generally, any subgroup N of index 2 in G is normal: let $g \in G \setminus N$, then $G = N \cup gN = N \cup Ng$, and so $gN = Ng = G \setminus N$.
- The cyclic group $\langle r \rangle$ in D_{2n} has index 2, so is normal. However, for $n \geq 3$ the subgroup $\{\mathrm{id}, s\} \leq D_{2n}$ is not normal because

  $$r^{-1}sr = r^{n-2}s \neq \{e, s\}.$$

Now we can also check that the operation in G/N is well-defined: If for $i = 1, 2$ we have $g_iN = h_iN$ for some $g_i, h_i \in G$, then $g_i \in h_iN$ gives $g_i = h_in_i$ for some $n_i \in N$. Thus

$$(g_1g_2)N = (h_1n_1h_2n_2)N = (h_1h_2(h_2^{-1}n_1h_2)n_2)N = (h_1h_2)N$$

as $h_2^{-1}n_1h_2 \in N$ by Lemma 2.3(ii).

Remark. This also showcases another understanding of quotient groups: we can view G/N as "setting all elements in N to be $e_{G/N}$", so for instance in the equation above $(h_2^{-1}n_1h_2)n_2$ just gets absorbed into N.

Example 2.5 (Product group)

Let G, H be groups. We can define a **product group** $G \times H$ where the elements are ordered pairs $(g, h) \in G \times H$ and the operation is defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2) \in G \times H.$$

One could check that this indeed form a group (with identity (e_G, e_H)). Now consider

$$G' = \{(g, e_H) : g \in G\} \cong G.$$

Then

- G' is a subgroup of $G \times H$: This is clear by using the subgroup test in Proposition 1.10.
- G' is normal in $G \times H$: Pick $(n, e_H) \in G'$ and any $(g, h) \in G \times H$. Then

  $$(g, h) \cdot (n, e_H) \cdot (g, h)^{-1} = (gng^{-1}, hh^{-1}) = (gng^{-1}, e_H) \in G'$$

  so by Lemma 2.3 we have $G' \trianglelefteq G \times H$.

Moreover, just as the notation would imply, one can check that

$$(G \times H)/G' \cong H,$$

by using the map $(e_G, h)G' \mapsto h$ (note that $(g, h)G' = (e_G, h) \cdot (g, e_H)G' = (e_G, h)G'$ for any $(g, h) \in G \times H$).

Finally, just for the sake of having a language:

Definition 2.6 (Simple groups)

A group G is called **simple** if G has no normal subgroups other than $\{e\}$ and G.

For instance, $\mathbb{Z}/p\mathbb{Z}$ for a prime p is simple: since it is cyclic any subgroup must have order dividing p, so the only possible subgroups are $\{e\}$ and G.

Remark. Simple groups turn out to be the basic building blocks for any finite group. Amazingly, we actually *have* a full list of simple groups, but the list is really bizarre; this is one of the biggest proofs in mathematics. Every finite simple group falls in one of the following:

- $\mathbb{Z}/p\mathbb{Z}$ for prime p;
- the subgroup A_n of S_n consisting of "even" permutations for $n \geq 5$;
- a simple group of Lie type;
- twenty-six "sporadic" groups which do not fit into any nice family.

Again, we will not explain the groups here, but it is worth noting that the two largest sporadic groups have cute names: the **baby monster group** has order

$$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4 \cdot 10^{33}$$

and the **monster group** (also "friendly giant") has order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}.$$

It contains twenty of the sporadic groups (by quotienting), and these twenty groups are called the **happy family**.

Math is weird.

2.2 Isomorphism theorems ⋆

Serving as a good practice and for historical reasons, we will now cover four "isomorphism theorems", which are related to certain quotient groups. However, in practice I have only seen the first one being used often, so really these theorems are just put here for completeness.

Theorem 2.7 (First Isomorphism Theorem)

If $\phi : G \to H$ is a homomorphism, then $G/\ker\phi \cong \operatorname{im}\phi$.

Remark. Note that $\ker\phi$ is a normal subgroup of G by definition, so the quotient group makes sense.

Proof. Define the map

$$f : G/\ker\phi \to \operatorname{im}\phi \quad \text{by } g\ker\phi \mapsto \phi(g)$$

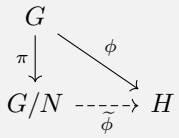
which we claim is an isomorphism. We have to check:

- f is well-defined: Suppose $g\ker\phi = h\ker\phi$. Then $gh^{-1}\ker\phi = \ker\phi$, or $gh^{-1} \in \ker\phi$. Thus
$$\phi(g) = \phi(gh^{-1}h) = \phi(gh^{-1})\phi(h) = \phi(h).$$
- f is a homomorphism: Again take $g\ker\phi, h\ker\phi \in G/\ker\phi$. Then
$$f((g\ker\phi)\cdot(h\ker\phi)) = f(gh\ker\phi) = \phi(gh) = \phi(g)\phi(h) = f(g\ker\phi)f(h\ker\phi).$$
- f is bijective: Surjectivity is visibly clear. If $f(g\ker\phi) = e_H$, then $\phi(g) = e_H$, or $g \in \ker\phi$. Thus $\ker f = \{\ker\phi\} = \{e_{G/\ker\phi}\}$. Hence by Lemma 1.36, f is injective. □

In fact, the construction of such maps out of a quotient group is extremely common in group theory; in its full generality every such map can be constructed from the following "**universal property**" of quotient groups:

Theorem 2.8 (Universal property of quotient subgroups)

Let $N \trianglelefteq G$ and $\phi : G \to H$ be a homomorphism such that $N \subseteq \ker\phi$. Then there is a *unique* homomorphism $\widetilde{\phi} : G/N \to H$ such that the diagram



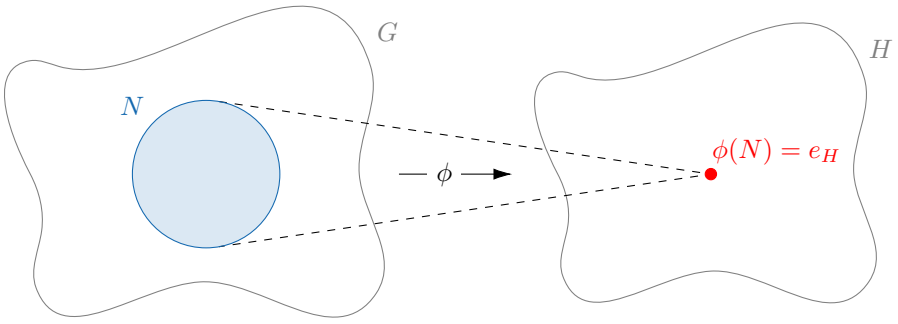
commutes, where $\pi : G \to G/N$ is the projection map $g \mapsto gN$ as in Lemma 2.3.

The proof goes exactly like above, by using $\widetilde{\phi} : gN \mapsto \phi(g)$. In other words:

! Keypoint

To define a map out of a quotient group G/N, define a map out of G which maps N to e.

Pictorially, this means that we only have to give a map of the form:



Moving on to second isomorphism theorem, the question in consideration is as follows:

Motivation

Consider again a group $G, N \trianglelefteq G$ and $H \leq G$. We know that

$$G/N = \{\text{cosets of the form } gN\}$$

but how about the set of cosets of the form hN where $h \in H$? Well, a naive guess might be H/N, but N might not be a normal subgroup of H; in fact, N might not even be a subgroup of H! To fix this, one could either:

- consider $H \cap N$ instead, which would be a normal subgroup of H;
- consider "the smallest subgroup of G containing H and N", then quotienting N.

The second isomorphism theorem assures that these two approaches give "the same answer".

Let us now make this precise. Firstly, we have to define what is the smallest subgroup containing both H and N:

Definition 2.9 (Frobenius product)

Let S and T be subsets of a group G. We define

$$ST := \{st : s \in S, t \in T\}$$

to be the **(Frobenius) product** of S and T.

Caution: This is unfortunately very confusing with the product of groups $G \times H$. We will hence always use $\times$ if this is the case, and will refer to the above product as the Frobenius product if needed.

Example 2.10

- If $S = \{g\}$ and $T = N \trianglelefteq G$ where $g \in G$, then $ST = gN$.
- When $G = S_3, S = \{\mathrm{id}, (12)\}$ and $T = \{\mathrm{id}, (23)\}$, we have

  $$ST = \{\mathrm{id}, (12), (23), (123)\}.$$

  Note that ST is **not** a subgroup of G, since $(123)^{-1} = (321) \notin ST$.

If you have seen some linear algebra before, this is exactly the analogy of the sum of two subspaces. However, what's different here is that **the product of two subgroups are not necessarily a subgroup**, as we have seen in the above example. Luckily, this is the case in most of our considerations:

Proposition 2.11

Suppose H and N are subgroups of a group G.

(i) If N is normal then $HN \leq G$.

(ii) If both H and N are normal then $HN \trianglelefteq G$.

Proof. (i). HN is non-empty, and we have

$$(h_1n_1)(h_2n_2) = h_1h_2n_1'n_2 \in HN$$

for some $n_1' \in N$ by Lemma 2.3, since $n_1h_2 \in Nh_2 = h_2N$. Thus HN is closed under the operation. Similarly,

$$(hn)^{-1} = n^{-1}h^{-1} \in Nh^{-1} = h^{-1}N \subseteq HN.$$

(ii). We further have $gHNg^{-1} = gHg^{-1} \cdot gNg^{-1} = HN$, so HN is normal. □

We are ready to state the second isomorphism theorem now. Clearly, $H, N \subseteq HN$ and it is the smallest subgroup of G to contain both H and N (by the operation being closed). Hence, our motivation translates to:

Theorem 2.12 (Second Isomorphism Theorem)
If $H \leq G$ and $N \trianglelefteq G$, then $H/H \cap N \cong HN/N$.

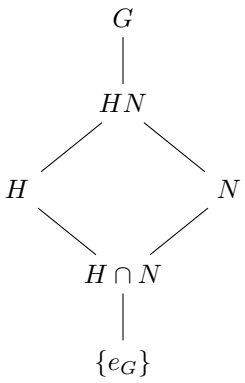
Proof. By the essence of the universal property, we define the map

$$\phi : H \to G/N \quad \text{by } h \mapsto hN$$

with $\ker \phi = H \cap N$ since $hN = N$ if and only if $h \in N$. Thus $H \cap N \trianglelefteq H$.

But $\operatorname{im} \phi = \{hN : h \in H\}$, which is exactly equal to HN/N since $(\subseteq)$ $hN = heN \in HN/N$ and $(\supseteq)$ $hnN = hN$ for any $h \in H$ and $n \in N$. The first isomorphism theorem then implies the result. □

Remark. This theorem is sometimes called the *diamond theorem* due to the shape of the lattice of subgroups:



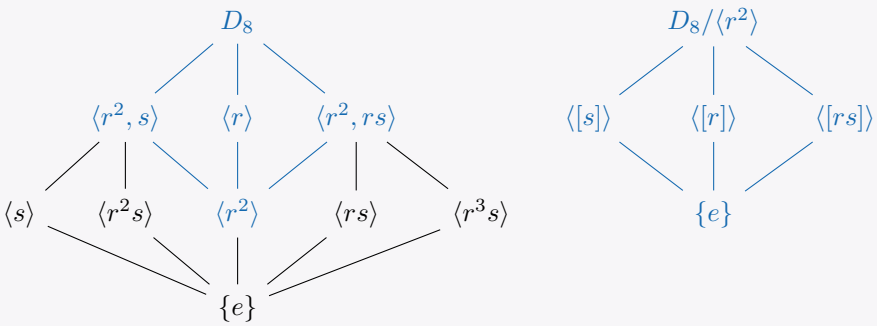
where a line means that the group below is a subgroup of the group above.

To continue, the third isomorphism theorem will be skipped since we will soon see that it is a corollary of the fourth. The motivation of it again comes from a simple consideration:

Motivation
Let G be a group and $N \trianglelefteq G$. The main question is:

$$\boxed{\text{What are the subgroups of } G/N?}$$

Taking the example of $G = D_8$ and $N = \langle r^2 \rangle$ (and noticing that $sr^2s^{-1} = (srs^{-1})^2 = (r^3)^2 = r^2 \in N$, so $N \trianglelefteq G$), one can compute their respective lattice of subgroups:



which can be computed by using Lagrange's theorem, that $D_8/\langle r^2 \rangle$ has order 4, and Proposition 1.39.

From the above example, one can probably spot a pattern; the precise statement is as follows:

Theorem 2.13 (Fourth Isomorphism Theorem)

Let G be a group and $N \trianglelefteq G$. Write $\overline{G} := G/N$ and $\phi : G \to \overline{G}$ be the canonical map. Then there is a one-to-one correspondence

$$\{\text{subgroups of } G \text{ containing } N\} \overset{1:1}{\longleftrightarrow} \{\text{subgroups of } \overline{G}\}$$

under which a subgroup H of G corresponds to $\overline{H} := \phi(H) \leq \overline{G}$. Moreover,

(i) $H_1 \subseteq H_2$ if and only if $\overline{H_1} \subseteq \overline{H_2}$, in which case $[H_2 : H_1] = [\overline{H_1} : \overline{H_2}]$.

(ii) $H \trianglelefteq G$ if and only if $\overline{H} \trianglelefteq \overline{G}$, in which case there is an isomorphism $G/H \cong \overline{G}/\overline{H}$.

Proof. Note that the correspondence makes sense, because pre-images of subgroups of $\overline{G}$ are subgroups of G containing N; indeed, if $\overline{H} \leq \overline{G}$ then $\phi(n) = N \in \overline{H}$ for any $n \in N$ and so $n \in \phi^{-1}(H)$. Now:

(i). ($\Rightarrow$). If $H_1 \subseteq H_2$ then

$$\overline{H_1} = \{hN : h \in H_1\} \subseteq \{hN : h \in H_2\} = \overline{H_2}.$$

as H_1 and H_2 both contains N.

($\Leftarrow$). Suppose $\overline{H_1} \subseteq \overline{H_2}$, then for every $h_1 \in H_1$ there exists $h_2 \in H_2$ such that $h_1 N = h_2 N$, and thus $h_1 = h_2 n$ for some $n \in N \subseteq H_2$. But then $h_1 \in H_2$ and so $H_1 \subseteq H_2$.

Now the final statement comes from

$$[H_2 : H_1] = \frac{|H_2|}{|H_1|} = \frac{|H_2|/|N|}{|H_1|/|N|} = \frac{|\overline{H_2}|}{|\overline{H_1}|} = [\overline{H_2} : \overline{H_1}].$$

(ii). ($\Rightarrow$). If $H \trianglelefteq G$ then $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. Thus

$$(gN)^{-1}(hN)(gN) = g^{-1}hgN \in \overline{H}.$$

($\Leftarrow$). We have $(gN)^{-1}(hN)(gN) = h'N$ for any $g \in G, h \in H$ and for some $h' \in H$, so $g^{-1}hg = h'n$ for some $n \in N$. But $N \subseteq H$ and hence $h'n \in H$ and $H \trianglelefteq G$.

The isomorphism is defined by $gH \mapsto \phi(g)\overline{H}$, which is well-defined by the universal property. It is easy to check that this map is bijective, which completes the proof. □

Remark. This theorem is sometimes known as the *correspondence theorem*. If we rewrite part (ii) as $G/H \cong (G/N)/(H/N)$, then we get the third isomorphism theorem.

Example 2.14

To end the section, let us give some examples of this theorem in use:

- If $N \trianglelefteq G$ has order 5 and $G/N \cong S_4$, then
  - $|G| = 120$ by Lagrange's theorem.
  - G/N has four subgroups of order 3 (in S_4 they are $\langle(123)\rangle, \ldots, \langle(234)\rangle$) which are **not** normal in G/N, so G has four non-normal subgroups of order 15 containing N.
  - G has a normal subgroup of order 20 corresponding to $\{\text{id}, (12)(34), (13)(24), (14)(23)\} \trianglelefteq S_4 \cong G/N$.
- One can show that $N \trianglelefteq G$ is maximal (i.e. $N \leq H < G$ implies $N = H$) iff G/N is simple.