Group Theory

Bendit Chan

February 2, 2023

Disclaimer

This is a set of handouts dedicated to cover elementary group theory. The content is heavily based on the following resources:

- Course notes of the courses M40003 – Linear Algebra & Groups, M50005 – Groups & Rings, and M60036 – Group Theory 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 $\star$)
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 $m = |\text{supp}(f)|$.

If $m = 0$ then $f = \text{id} = (1)$. Now assume $m \geq 1$, and take $i_1 \in \text{supp}(f)$, 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 $\text{supp}(g) = \text{supp}(f) \setminus \{i_1, \ldots, i_r\}$. 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 $i_1 \in \text{supp}(f)$. 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) $f^m = \text{id}$ if and only if $f_i^m = \text{id}$ for all $1 \leq i \leq k$.

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

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 $f_1^m \ldots f_k^m = \text{id}$, 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

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

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

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,

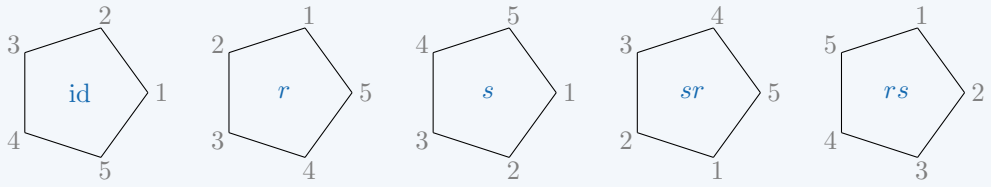
$$D_{2n} = \{\text{id}, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

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 $r^n = s^2 = \text{id}$ 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

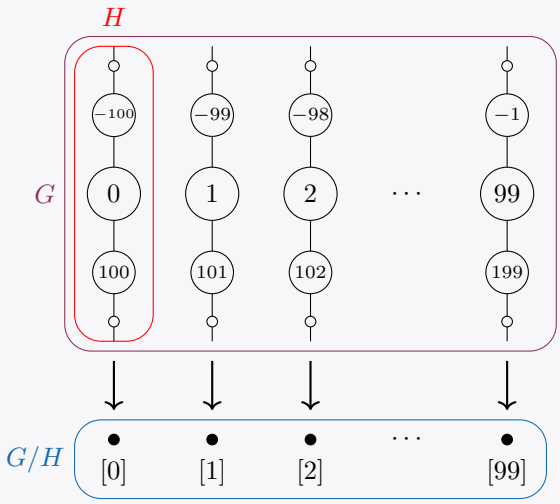
$$100\mathbb{Z} = \{\dots, -200, -100, 0, 100, 200, \dots\}.$$

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

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

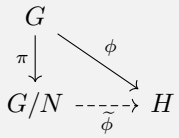
which we claim is an isomorphism. We have to check:

- 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 groups)

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



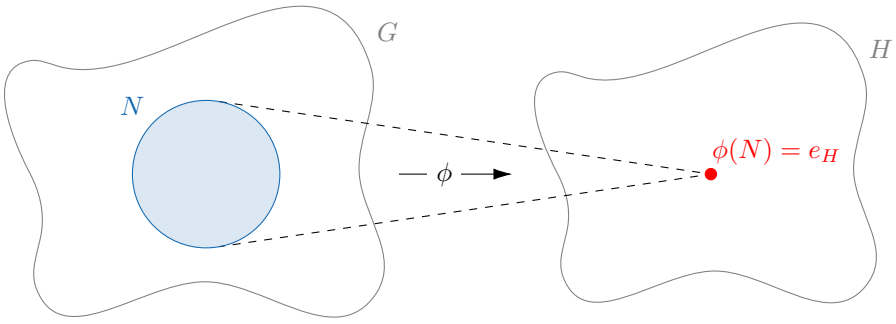
commutes, where $\pi : G \to G/N$ is the projection map $g \mapsto gN$ as in Lemma 2.3.

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 $H/H \cap N \cong HN/N$.

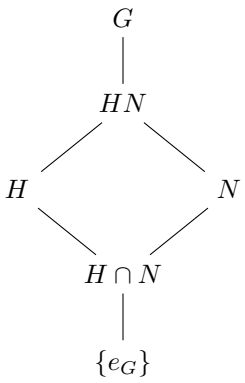
Proof. By the essence of the universal property, we define the map

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

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:



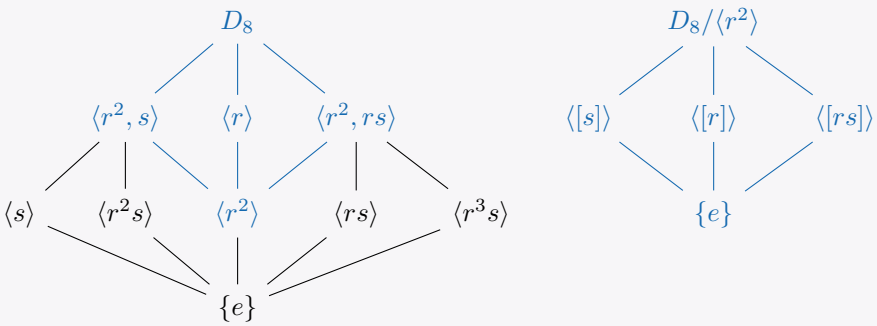
where a line means that the group below is a subgroup of the group above.

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.

3 Generators and Free Groups

Let us now revisit Definition 1.22 and develop the theory of generators and free groups.

Motivation

If G is a group and $S \subseteq G$ is a subset, an alternative definition of $\langle S \rangle$ is

$$\langle S \rangle = \text{smallest subgroup of } G \text{ containing } S.$$

However, this is informal: what is "smallest"? What if two different subgroups of the same order both contain S? Luckily, that cannot happen: if $S \subseteq H_1, H_2$ then we have $S \subseteq H_1 \cap H_2$, which is again a subgroup.

We can now give a formal definition:

Definition 3.1 (Subgroup generated by a set)

Let G be a group and $S \subseteq G$. Then

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

is the **subgroup of G generated by S**. Moreover,

- If $\langle S \rangle = G$ for some $S \subseteq G$ then we say **S generates G**.
- If $\langle S \rangle = G$ for some *finite* $S \subseteq G$ then we say **G is finitely generated**.

This definition takes care of both the existence and uniqueness of $\langle S \rangle$. Note that $\langle G \rangle = G$, so any finite group is finitely generated.

This is all good, but in practice we will almost surely use Definition 1.22 to work out the elements in a subgroup generated by a set. In addition, Definition 1.22 **doesn't rely on the structure of** G, but only the relations on the elements of S, i.e. we can create new groups without specifying what G is. For instance, D_{2n} can be described as a group with generators r, s and relations

$$r^n = s^2 = srsr = \mathrm{id}\,.$$

This motivates the following section, which is the construction of **free groups** and **presentations**.

3.1 Free groups

The goal in this section is to define a group $F(S)$ for any set S without specifying $S \subseteq G$ for some group G. The elements will be:

Definition 3.2 (Word)

A **word** w is a finite sequence $x_1, \ldots, x_m$ where $m \geq 0$ and each $x_i \in S \cup S^{-1}$. We write w as $x_1 x_2 \ldots x_m$. Note that the empty sequence, i.e. when $m = 0$, is a word, denoted $\emptyset$ (or sometimes, e).

Caution: As before, the set $S = \{x^{-1} : x \in S\}$ is the set of "inverses" of S; but that doesn't mean anything as they are just symbols at this stage, as S is not necessarily a subset of a group. By convention we require $S \cap S^{-1} = \emptyset$.

Example 3.3

Let $S = \{a, b, c\}$ be any three-element set. Then

- $ab, aabac, b$ are words of S.
- $aa^{-1}c$ and c are also words, but **they are unequal words** at this step (of course, we would want them to be equal at last).
- ab and ba are also unequal words, as usual.

To proceed, we want to identify words like $aa^{-1}c$ and c, so that they become the same word in the group $F(S)$. We define:

Definition 3.4 (Reduced words)

A word is said to be **reduced** if it contains no pairs of the form aa^{-1} or $a^{-1}a$ for any $a \in S$.

Starting with a word w, we can then perform a finite sequence of cancellations to arrive at a reduced word, which will be called the **reduced form** w_0 of w. For instance,

$$a^{-1}\underline{bb^{-1}}aba^{-1}a \longrightarrow a^{-1}ab\underline{a^{-1}a} \longrightarrow \underline{a^{-1}a}b \longrightarrow b.$$

Note that a reduced form always exists, as each time we delete $a^{-1}a$ or aa^{-1} the length of the word decreases by 2 and the length is always finite. In fact it is also unique:

Proposition 3.5

There is only one reduced form of a word w.

Proof. We induct on the length of the word. If w is reduced then there is nothing to prove. Otherwise, there is a pair aa^{-1} or $a^{-1}a$ in w, which we assume to be the first as the argument is the same.

If two reduced forms w_1 and w_2 of w are obtained by cancelling aa^{-1} first, then $w_1 = w_2$ by induction hypothesis. Similarly, if w_1 and w_2 are both obtained by a sequence of cancellation where aa^{-1} is cancelled at some point, then $w_1 = w_2$ as the result is the same if we cancel aa^{-1} first.

Finally, consider a reduced word w_0 obtained by a sequence in which there are no direct cancellations of aa^{-1}. As this pair does not remain in w_0, at least one of a or a^{-1} must be cancelled at some point. We only have two cases:

$$\cdots \underline{a^{-1}a}a^{-1}\cdots \quad \text{or} \quad \cdots a\underline{a^{-1}a}\cdots$$

where the underlined pair is the one being cancelled. Yet in both cases the result is the same if we have cancelled the pair aa^{-1} instead, so the result follows from the case already proven. □

Hence, from now on, we say w, w' are **equivalent**, denoted $w \sim w'$, if they have the same reduced form. It is clear that this is an equivalence relation. We can now define:

Definition 3.6 (Free groups)

The **concatenation** of two words $x_1 \dots x_m$ and $y_1 \dots y_n$ is the word

$$x_1 \dots x_m y_1 \dots y_n.$$

Given a set S, the **free group** $F(S)$ on the set S then consists of the equivalence classes of words of S with the group operation as concatenation.

Of course, we have to check:

- If $w \sim w'$ and $v \sim v'$, then $wv \sim w'v'$: We have $w \sim w_0$ and $v \sim v_0$, so the reduced form of wv can be obtained by first reducing w and v to get w_0v_0, i.e. $wv \sim w_0v_0$. Yet $w' \sim w_0$ and $v' \sim v_0$ too so we have $w'v' \sim w_0v_0$.
- Identity: Use the word $\emptyset$.
- Inverse: Let $w = x_1x_2 \dots x_n$ be a word (representing the equivalence class $[w]$), then

$$(x_1x_2 \dots x_n)(x_n^{-1} \dots x_2^{-1}x_1^{-1}) \sim \emptyset.$$

Hence $F(S)$ is indeed a group.

Example 3.7

Again take $S = \{a, b, c\}$. Then $F(S)$ is what we get by appending finitely many copies of a, b, c, a^{-1}, b^{-1} and c^{-1}, with all cancellations done. For instance,

$$aba^{-1}b^{-1}, c^{-1}, \emptyset \in F(S).$$

As usual, these are representatives of their equivalence class in $F(S)$, so we have $a = abb^{-1}$ in $F(S)$, etc.

Remark. Since each equivalence class $[w]$ has a representative $w_0 \in [w]$, some might alternatively think of $F(S)$ as the group of reduced words. Then, in this sense $abb^{-1} \notin F(S)$ since it is not reduced.

So, as a slogan to remember about free groups: **put elements of $S \cup S^{-1}$ in a box, seal it tightly, and shake vigorously**. We then get the free group $F(S)$.

To further understand free groups, let us now state the so-called universal property of free groups. Similar to that of quotient groups, this following property completely characterises what a free group is.

Theorem 3.8 (Universal property of free groups)

Given a set S, a group G, and a function $f : S \to G$, there is a *unique* homomorphism $\phi : F(S) \to G$ such that the following diagram commutes:

$$\begin{array}{ccc} S & & \\ {\scriptstyle \iota}\downarrow & \searrow^{f} & \\ F(S) & \xrightarrow[\phi]{} & G \end{array}$$

where $\iota : S \to F(S)$ is the inclusion map, i.e. it maps any $a \in S$ to $a \in F(S)$.

If you recall the way to think about universal properties after Theorem 2.8, we get a similar statement:

! Keypoint

To define a map out of a free group $F(S)$, just define a map out of S.

Proof. Define

$$\phi : F(S) \to G \quad \text{by } x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \mapsto f(x_1)^{\epsilon_1} \dots f(x_n)^{\epsilon_n}$$

where $x_i \in S$ and $\epsilon_i \in \{1, -1\}$ for each i (we need the ϵ_i's since f is only defined on S, not $S \cup S^{-1}$). We claim that ϕ is the unique, well-defined homomorphism.

- ϕ is well-defined: If $w \sim w'$, then $\phi(w) = \phi(w')$ by performing the same set of cancellations on w and w' to obtain w_0, the common reduced word of w and w'.
- ϕ is a homomorphism: Clear.
- ϕ is unique: For each $x \in S$, we have $\phi(x) = f(x)$. Hence ϕ must be the one defined above, since a homomorphism between groups is determined by what it does to a set of generators. □

Now we can finally answer why we care about free groups:

Corollary 3.9

Every group is isomorphic to a quotient of a free group.

Proof. Pick a set S of generators of G (e.g. $S = G$). By Theorem 3.8, the map $f : S \to G$ by $a \mapsto a$ define a map $\phi : F(S) \to G$. Now $\operatorname{im}\phi \leq G$ contains all elements of S, so it must be equal to G. Hence $G = \operatorname{im}\phi \cong F(S)/\ker\phi$ by first isomorphism theorem. □

3.2 Presentations

Recall from Section 1.5 that every *finite* group is isomorphic to some subgroup of S_n, which motivated our study in symmetric groups. Similarly, we now see that every group is a quotient of a free group, so it only makes sense to devote the following section to study such objects, which will be known as **presentations**.

Motivation

To motivate the definition of presentations, consider

$$\mathbb{Z} \cong F(a) \cong \langle a \rangle$$

i.e. the group $\mathbb{Z}$ which is isomorphic to the free group generated by one element.

There's one issue: **the generators usually satisfy certain properties**. For example, $\mathbb{Z}/100\mathbb{Z}$ is also generated by one element x, but this x has the property that $x^{100} = 1$. This motivates us to write

$$\mathbb{Z}/100\mathbb{Z} = \langle x \mid x^{100} = 1 \rangle = \langle x \rangle / \langle x^{100} \rangle.$$

As we can see, this group is a quotient of a free group $\mathbb{Z}$.

To make this rigorous, we need a technical definition for arbitrary groups:

Definition 3.10 (Normal subgroup generated by a set)

Let G be a group and $S \subseteq G$ be a subset. The **normal subgroup generated by S** is defined as

$$\langle\langle S \rangle\rangle := \left\langle \bigcup_{g \in G} gSg^{-1} \right\rangle.$$

Clearly this is a subgroup. We have to check that this is indeed normal:

Proof. Let us temporarily say that a subset $S \subseteq G$ is **normal** if $gSg^{-1} \subseteq S$ for all $g \in G$. The main step is:

Claim

If S is normal, then $\langle S \rangle \leq G$ is normal.

Proof. Let $a \in \langle S \rangle$, say $a = x_1 \cdots x_m$ with $x_i \in S \cup S^{-1}$. Then

$$gag^{-1} = (gx_1g^{-1}) \dots (gx_mg^{-1}).$$

As S is normal, each gx_ig^{-1} (or its inverse) lies in S, so $g\langle S \rangle g^{-1} \in \langle S \rangle$. □

Now clearly for any subset $S \subseteq G$, $\bigcup_{g \in G} gSg^{-1}$ is normal (as a set). Thus by the claim we obtain the result. □

Now we might define the aforementioned notion:

Definition 3.11 (Presentations)

Let S be a set and $R \subseteq F(S)$. The group $G = F(S)/\langle\langle R \rangle\rangle$ is said to have S as **generators** and R as **relations**. One also says that the pair (S, R) is a **presentation** for G, and denotes G by $\langle S \mid R \rangle$.

Hence, the group

$$\mathbb{Z}/100\mathbb{Z} = \langle x \mid x^{100} \rangle$$

has generator x and relation x^{100}. The above is a presentation of $\mathbb{Z}/100\mathbb{Z}$.

Remark. As an abuse of notation, we sometimes write an equal sign in the relations, since that is what happens when we quotient by $\langle\langle R \rangle\rangle$, i.e. the canonical map $F(S) \to F(S)/\langle\langle R \rangle\rangle$ maps everything in R to the identity; so for instance if $aba^{-1}b^{-1} \in R$ then we would have $ab = ba$ in $\langle S \mid R \rangle$.

This notation allows us to describe groups that we know in a compact manner, but also create new groups:

Example 3.12 (Examples of presentations)

Here is a plethora of examples:

- If $S = \{x_1, \dots, x_n\}$, then the free group $F(S)$ has presentation $\langle x_1, \dots, x_n \rangle$.
- As above, the dihedral group has presentation $D_{2n} = \langle r, s \mid r^n, s^2, srsr \rangle$.
- The Klein four group can be written as

  $$K_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle$$

  Indeed, under these relations, we have

  $$F(\{a, b\})/\langle\langle R \rangle\rangle = \{[e], [a], [b], [ab]\}$$

  and clearly $[a], [b]$ and $[ab]$ all have order 2, so we indeed have the above presentation.
- Let $G = \langle s, t \mid s^3 t, t^3, s^4 \rangle$. Then $G = \{e\}$ since

  $$\begin{aligned} s &= ss^3 t = s^4 t = t \\ e &= s^3 t t^{-3} = s^3 s s^{-3} = s. \end{aligned}$$

- The **quaternion group** is defined as

  $$\begin{aligned} Q_8 &= \langle a, b \mid a^4 = e, a^2 = b^2, ba = a^3 b \rangle \\ &= \{e, a, a^2, a^3, b, ab, a^2 b, a^3 b\}. \end{aligned}$$

  The group can also be described by the quaternion numbers, hence the name: we can write

  $$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

  with the multiplication defined by

  $$i^2 = j^2 = -1, \quad ij = -ji = k.$$

  The map by $i \mapsto a, j \mapsto b$ exhibits an isomorphism of this form to the presentation above.
- Two elements a and b in a group commute if and only if their **commutator** $[a, b] = aba^{-1}b^{-1}$ is the identity. The **free abelian group** on generators $a_1, \dots, a_n$ is then defined as

  $$\langle a_1, \dots, a_n \mid [a_i, a_j] \ \forall i \neq j \rangle$$

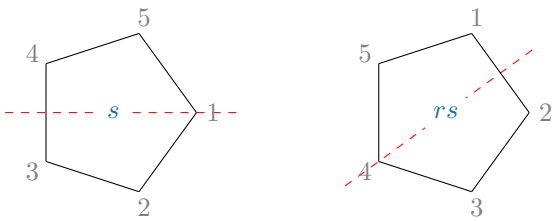
  Note that in this group we indeed have $a_i a_j = a_j a_i$ for all i, j, so it is abelian.

Caution: Note that presentations of a group is not unique; for instance, one also have

$$D_{2n} = \langle a, b \mid a^2, b^2, (ab)^n \rangle$$

which can be shown by considering the map $a \mapsto s, b \mapsto rs$.

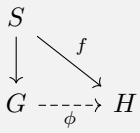
Geometrically, this means the symmetries of an n-gon can be generated by two reflections:



To end, we note that analogous to free groups, presentations also have a universal property:

Theorem 3.13 (Universal property of presentations)

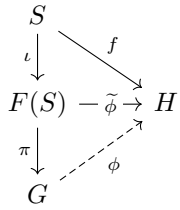
Let $G = \langle S \mid R \rangle$ be a group. For any group H and function $f : S \to H$ sending R to e_H, there exists a unique homomorphism $\phi : G \to H$ such that the following diagram commutes:



where $S \to G$ is the canonical map $a \mapsto [a]$.

This looks very similar to Theorem 2.8 (the universal property of quotient groups); but this should not be surprising: after all $\langle S \mid R \rangle$ *is* the quotient group $F(S)/\langle\langle R \rangle\rangle$. The proof follows swiftly:

Proof. The whole picture is:

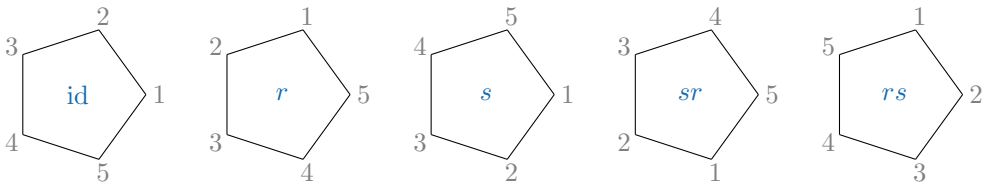


By the universal property of free groups, f extends to a homomorphism $\widetilde{\phi} : F(S) \to H$. By assumption, $\widetilde{\phi} \circ \iota(R) = f(R) = e_H$, so $\iota(R) \subseteq \ker \widetilde{\phi}$. Therefore $\langle\langle \iota(R) \rangle\rangle = \langle\langle R \rangle\rangle \trianglelefteq F(S)$ is contained in $\ker \widetilde{\phi}$.

By the universal property of quotient groups, this then gives the desired map ϕ. The uniqueness follows from the fact that we know the map on a set of generators for G. □

4 Group Actions

Historically, a group was a subgroup of a symmetric group (as we have discussed under Cayley's theorem). Hence, elements of a group can naturally be associated to an "operation": for instance in D_{10}, the elements are associated to rotations and reflections on the vertices of an n-gon;



despite the actual elements being abstract symbols r, s, rs, etc.

In a more general setting, elements of a group G might "operate" on a set X with more structure, such as a vector space. This then provides more tools to study G, which are often insightful. These operations are called **group actions**, which we shall introduce now.

4.1 Definitions and Examples

There are many ways to define a group action; but the definition we shall use is:

Definition 4.1 (Group action)

Let X be a set and G be a group. A **group action** is a binary operation

$$\cdot : G \times X \to X$$

which maps (g, x) to an element $g \cdot x$, such that

- $e_G \cdot x = x$ for all $x \in X$;
- $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $g_1, g_2 \in G$ and $x \in X$.

The conditions imply that, for each $g \in G$, we have a map:

$$g_L : X \to X, \quad x \mapsto g \cdot x,$$

which is also bijective, as it has inverse $(g^{-1})_L$. Thus $g_L \in \mathrm{Sym}(X)$, the set of all bijective functions $X \to X$.

Now the second condition says that $g \mapsto g_L$ is a homomorphism, as

$$(gh)_L(x) = (gh) \cdot x = g \cdot (h \cdot x) = g_L \circ h_L(x).$$

Thus a group action of G on X gives a map

$$G \to \mathrm{Sym}(X), \quad g \mapsto g_L$$

and conversely every such homomorphism defines a group action. Therefore:

Remark. From now on, we might use the two notations interchangeably and just denote g_L as g. So given a group action, $g \cdot x$ and $g(x)$ mean the same thing (with the latter viewing g as a map $X \to X$).

In other words,

! Keypoint

A group action views each $g \in G$ as a permutation of elements of X.

Example 4.2 (Examples of group actions)

- The dihedral group D_{2n} acts on the set of vertices of an n-gon.
- The group $(\mathbb{Z}/4\mathbb{Z}, +)$ acts on the xy-plane $\mathbb{R}^2$ by $1 \cdot (x, y) = (y, -x)$ i.e. it is a rotation by $90°$.
- The group S_n acts on $X = \{1, 2, \ldots, n\}$ by applying the permutation: $\sigma \cdot x = \sigma(x)$. More generally, any subgroup of S_n acts on X the same way.
- The group $\mathrm{GL}_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by applying the linear transformation, i.e.

$$\mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathrm{GL}_n(\mathbb{R}), \quad A \cdot \mathbf{v} \mapsto A\mathbf{v}$$

  Notice that this action can be viewed as a map $\mathrm{GL}_n(\mathbb{R}) \to \mathrm{Sym}(\mathbb{R}^n)$ as above, particularly because any $A \in \mathrm{GL}_n(\mathbb{R})$ is invertible, so $\mathbf{v} \mapsto A\mathbf{v}$ is bijective.
- Any group G acts on itself by defining

$$G \times G \to G, \quad g \cdot h = gh.$$

  Note that the two axioms follow from the group axioms of G (identity and associativity).

Note that group actions are **not** unique: any group G also acts on itself by **conjugation**,

$$G \times G \to G, \quad g \cdot h = ghg^{-1}.$$

Definition 4.3 (Faithful)

An action of a group G on a set X is **faithful** if the homomorphism $G \to \mathrm{Sym}(X)$ is injective, i.e.

$$g \cdot x = x \text{ for all } x \in X \implies g = e_G.$$

Caution: The definition is not saying that the map $g(\cdot)$ is injective. Indeed, $g(\cdot) \in \mathrm{Sym}(X)$, so it is always bijective. Instead, it is asking whether $g \mapsto g(\cdot)$ is injective, i.e. if $g(\cdot)$ and $h(\cdot)$ are equal *as maps*, can we conclude that $g = h$?

All the examples above are faithful actions, except for the conjugation action: if $g \cdot h = h$ for any $h \in G$ we can only conclude that $gh = hg$, i.e. g commutes with every element in G.

In fact, the set of such elements is called the **centre** of G, on which we will disucss more later:

Definition 4.4 (Centre)

Let G be a group. The **centre** of G is defined as the set

$$Z(G) := \{g \in G : gh = hg \text{ for all } h \in G\}$$

The theory now already allows us to phrase the proof of Cayley's theorem more concisely; recall:

Theorem 1.40 (Cayley $\star$)

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

Proof. Consider G acting on itself by left multiplication, i.e.

$$g \cdot h \mapsto gh.$$

This is a faithful action, so the induced homomorphism $G \to \mathrm{Sym}(G)$ is injective. The proof follows similarly to the original proof of the theorem. □

So, when we were proving Cayley's theorem, we accidentally discovered a group action! It was exactly the map $G \to \mathrm{Sym}(G)$ via $g \mapsto \phi_g$ where $\phi_g : x \mapsto gx$.

4.2 Orbits and stabilisers

Given a group action G on X, we can define an equivalence relation $\sim$ on X as follows:

$$x \sim y \iff x = g \cdot y \text{ for some } g \in G,$$

i.e. "one can be obtained from the other by an action". Let's quickly check that it is indeed an equivalence relation:

- Reflexive: $x \sim x$ because $x = e_G \cdot x$;
- Symmetric: if $x = g \cdot y$ then $g^{-1} \cdot x = (g^{-1}g) \cdot y = y$;
- Transitive: if $y = g \cdot x, z = g' \cdot y$ then $z = g' \cdot (g \cdot x) = (g'g) \cdot x$.

We can hence define:

Definition 4.5 (Orbits)

Given a group action G on X, the **G-orbit** of an element $x \in X$ is the equivalence class of x:

$$G \cdot x = [x]_\sim = \{y \in G : x \sim y\} = \{g \cdot x : g \in G\} \subseteq X.$$

As $\sim$ is an equivalence relation, the G-orbits partition X, i.e. any $x \in X$ belongs to exactly one orbit $G \cdot x$ (but $G \cdot x$ might be equal to $G \cdot y$ for some $x \neq y$). We sometimes write X/G for the set of orbits.

It turns out that a very closely related concept is:

Definition 4.6 (Stabiliser)

Given a group action G on X, the **stabliser** of $x \in X$ is the set of $g \in G$ which fix x, i.e.

$$\mathrm{Stab}_G(x) := \{g \in G : g \cdot x = x\} \subseteq G.$$

It can be easily checked that $\mathrm{Stab}_G(x)$ is a subgroup of G for any x.

Remark. If G is clear from the context, we will simply write $\mathrm{Stab}(x)$. The notations $\mathrm{St}_G(x)$ or G_x are also seen.

Example 4.7 (Examples of orbits and stabilisers)

- Uninteresting example: consider G acting on itself by left multiplication, then for any $g \in G$,

  $$G \cdot g = G, \quad \mathrm{Stab}(g) = \{e_G\}$$

  as $g \sim h$ for any h by $g = (gh^{-1})h$, and $gh = h$ implies $h = e_G$.
- Suppose G acts on X, and let $g \in G$ be an element of order n. Then $\langle g \rangle$ also acts on X.
  The $\langle g \rangle$-orbits are the sets of the form

  $$\langle g \rangle \cdot x = \{x, g \cdot x, \ldots, g^{n-1} \cdot x\}.$$

  (Note that these elements need not be distinct, so the set might contain fewer than n elements.)
- Let S_n act on $X = \{1, 2, \ldots, n\}$. Then:
  - The only S_n-orbit is X, as $(1x)$ sends 1 to any $x \in X$, i.e. $1 \sim x$.
  - The stabiliser of $x \in X$ consists of the permutations f which fix x, i.e. the ones with $x \notin \operatorname{supp} f$.

Before we move on, let's focus on a particularly important example, which is of the action of conjugations as we've mentioned above. Recall that means the action $g \cdot h \mapsto ghg^{-1}$.

- The G-orbits are called **conjugacy classes**: for $x \in G$, the conjugacy class of x is

$$x^G = \{gxg^{-1} : g \in G\},$$

  i.e. it consists of all possible conjugations of x.

- The stabilisers and called **centralisers**: for $x \in G$, the centraliser of x is

$$C_G(x) = \{g \in G : gx = xg\},$$

  i.e. it consists of all elements of G that commute with x.

Example 4.8 (Use of conjugacy classes and centralisers)

Many concepts can be described concisely by conjugacy classes and centralisers. For instance:

- A subgroup $H \leq G$ is normal iff for all $h \in H$, $h^G \subseteq H$.
- The intersection

$$\bigcap_{h \in G} C_G(h) = \{g \in G : gh = hg \text{ for all } h \in G\} = Z(G)$$

  is the centre of G.
- If you are familiar with linear algebra, the conjugacy classes in $G = \mathrm{GL}_n(F)$ are called similarity classes, and the theory of rational canonical forms provides a set of unique representatives for the conjugacy class.

Let's now proceed to prove some results about orbits and stabilisers. The following lemma says that the stabilisers of elements in the same G-orbit are conjugate in G:

Lemma 4.9

For any $g \in G$ and $x \in X$, $\mathrm{Stab}(g \cdot x) = g\,\mathrm{Stab}(x)g^{-1}$.

Proof. Certainly, if $h \in \mathrm{Stab}(x)$, i.e. $h \cdot x = x$, then

$$(ghg^{-1}) \cdot (g \cdot x) = g \cdot (h \cdot x) = g \cdot x$$

which proves $(\supseteq)$. Conversely, if $h \cdot (g \cdot x) = g \cdot x$, then

$$(g^{-1}hg) \cdot x = g^{-1} \cdot (h \cdot (g \cdot x)) = g^{-1} \cdot (g \cdot x) = x,$$

and so $g^{-1}hg \in \mathrm{Stab}(x)$, i.e. $h \in g\,\mathrm{Stab}(x)g^{-1}$. □

We also see from the definition that

$$\bigcap_{x \in X} \mathrm{Stab}(x) = \{g \in G : g \cdot x = x \text{ for all } x \in X\} = \ker(G \to \mathrm{Sym}(X)),$$

so the action is faithful if and only if $\bigcap \mathrm{Stab}(x) = \{e_G\}$.

The main result of this section is the so-called **orbit-stabiliser theorem**, connecting the two notions:

Theorem 4.10 (Orbit-stabiliser theorem)

Suppose G acts on X. For any $x \in X$, the map (from the *set of left cosets*, not a quotient group)

$$G/\mathrm{Stab}(x) \to G \cdot x, \quad g\,\mathrm{Stab}(x) \mapsto g \cdot x$$

is a bijection. In particular, if G is finite, then $|G \cdot x| = [G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)|$.

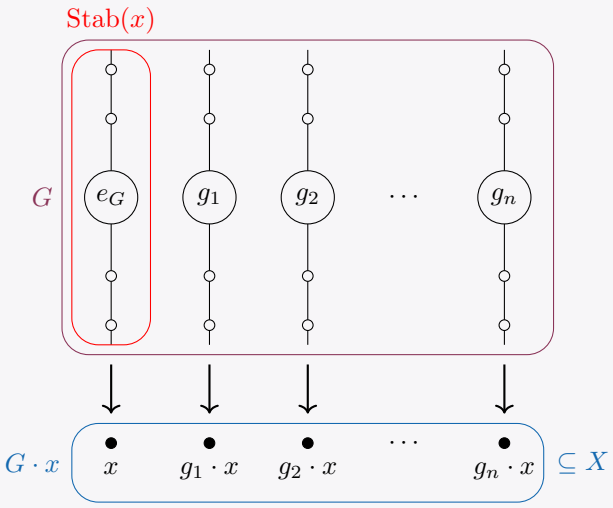
Proof. The map is well-defined for if $h \in \mathrm{Stab}(x)$, then $(gh) \cdot x = g \cdot x$. It is clearly surjective, and it is injective as

$$g \cdot x = h \cdot x \implies (g^{-1}h) \cdot x = x \implies g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x).$$

Hence the given map is a bijection. The second statement follows easily. □

Motivation

I like to remember this theorem as "telling you the size of an orbit". Pictorially:



Eah coset $g\,\mathrm{Stab}(x)$ specifies an element of $G \cdot x$, namely $g \cdot x$. The fact that $\mathrm{Stab}(x)$ is a stabiliser guarantees that it is irrelavant which representative we pick.

Note that as a consequence, when X is a finite and we write X as a disjoint union of G-orbits:

$$X = \bigcup_{i=1}^{n} G \cdot x_i,$$

then we have an equation for the size of $|X|$:

$$|X| = \sum_{i=1}^{n} |G \cdot x_i| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]. \tag{1}$$

This equation is more often used in practice.

The rest of the section will be devoted to study some applications of the orbit-stabiliser theorem. By considering the action of G on itself by conjugation, we get the following.

Proposition 4.11 (The class equation)

Let G is a finite group. Then G is a disjoint union of conjugacy classes $x_1^G, \ldots, x_n^G$, and

$$|G| = \sum_{i=1}^{n} [G : C_G(x_i)] = |Z(G)| + \sum_{|x_i^G| \neq 1} [G : C_G(x_i)].$$

Proof. The first statement and equality comes directly from (1). Observing that $|x^G| = 1$ iff $gxg^{-1} = x$ for all $g \in G$ iff $x \in Z(G)$ gives the second equality, by taking out all conjugacy classes of the form $\{x\}$ where $x \in Z(G)$. □

Remark. The number of distinct conjugacy classes, or n in the statement, is called the **class number** of the group.

Theorem 4.12 (Cauchy $\star$)

If a prime p divides $|G|$, then G contains an element of order p.

Proof. The key lemma is to first show the case when G is abelian:

Claim

If G is abelian, then the statement is true.

Proof. We induct on $|G|$. The base case $|G| = p$ is trivial. It suffices to show that G contains an element x whose order is pk for some $k \in \mathbb{N}$, because then $\operatorname{ord} x^k = p$. Let $e_G \neq g \in G$.

If $p \mid \operatorname{ord} g$ then we are done. Otherwise, $p \mid |G/\langle g\rangle|$, in which case there exists (by induction) an element $h\langle g\rangle \in G/\langle g\rangle$ with order divisible by p. But then

$$h^{\operatorname{ord} h} = e \implies (h\langle g\rangle)^{\operatorname{ord} h} = \langle g\rangle,$$

so $p \mid \operatorname{ord}(h\langle g\rangle) \mid \operatorname{ord} h$. This completes the proof. □

The general proof is also an induction on $|G|$. If there exists $x \notin Z(G)$ such that p does not divide $[G : C_G(x)] = |G|/|C_G(x)|$, then p divides $|C_G(x)| < |G|$ and we can apply induction to find an element of order p in $C_G(x)$.

Otherwise, $p \mid [G : C_G(x)]$ for any $x \notin Z(G)$, i.e. all the terms in the sum of the class equation (second form). Hence $p \mid |Z(G)|$. But $Z(G)$ is clearly abelian, so the above claim finishes the proof. □

Remark. There is also another well-known proof by considering the action of C_p, the cyclic group of order p, on G^p, the set of p-tuples of elements in G, i.e.

$$G^p := \{(g_1, \ldots, g_p) : g_i \in G \text{ for all } i\}.$$

I think the proof presented above is much more natural to think of.

Example 4.13 (Groups with order $2p$)

For a cool application, let us try to classify a family of groups, which are groups with order $2p$ where $p \neq 2$.

- From Cauchy's theorem, such a G contains elements s and r of order 2 and p respectively.
- Let $H = \langle r\rangle$. Then H is of index 2, and so is normal by Example 2.4.
- Obviously $s \neq H$, so $G = H \cup Hs$:

  $$G = \{e_G, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}.$$

  This looks familiar – it looks like the dihedral group D_{2p}! We just have to know how r and s interacts.
- As H is normal, $srs = srs^{-1} = r^i$ for some i. Since $s^2 = e$,

  $$r = s^2rs^2 = s(srs)s = r^{i^2} \implies i^2 \equiv 1 \pmod p$$

  as $\operatorname{ord} r = p$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, the only such i's are ± 1:
  - If $i = 1$, then $sr = rs$, so G is commutative (as it is generated by commuting elements). One can then see that rs has order $2p$ (as p is odd), so $G = \langle rs\rangle$.
  - If $i = -1$, then $srs = r^{-1}$ so $G = \langle r, s \mid r^p, s^2, srsr\rangle = D_{2p}$.

We conclude that the only such group is **either cyclic or dihedral**.

Cauchy's theorem also motivates the definition of a specific type of groups:

Definition 4.14 (p-groups)

Let p be a prime. A finite group G is called a **p-group** if $|G|$ is a power of p.

Alternatively, by Lagrange's and Cauchy's theorem, a finite group G is a p-group if and only if the order of every element of G is a power of p.

To end the section, arbitrary p-groups have very special properties, as showcased below.

Theorem 4.15

Every non-trivial finite p-group G has non-trivial centre, i.e. $Z(G) \neq \{e_G\}$.

Proof. By assumption, $|G|$ is a power of p, so $[G : C_G(x)] = |G|/|C_G(x)| \neq 1$ is also a power of p for all $x \notin Z(G)$. As p divides every term in the sum of the class equation (second form), it must divide $|Z(G)|$ also. □

Corollary 4.16

A group of order p^n has normal subgroups of order p^m for all $m \leq n$.

Proof. We induct on n. By Theorem 4.15 and Cauchy's theorem, $Z(G)$ contains an element g of order p, so $N := \langle g \rangle$ is a normal subgroup (as $g \in Z(G)$) of G of order p. Now the induction hypothesis allows us to assume the result for G/N, and the fourth isomorphism theorem (Theorem 2.13) implies the result. □

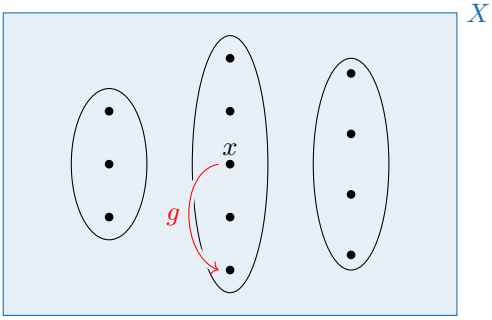
4.3 Transitivity

We now focus on a specific type of group action, called **transitive** actions. These actions can be further classified into **primitive** and **inprimitive**; they will be discussed in the next optional section. For now, transitivity allows us to "focus on one orbit only", which creates new results to, say, count the number of orbits.

Definition 4.17 (Transitive actions)

Let G act on X. We say G act **transitively** on X if there is only one orbit, i.e. $X = G \cdot x$ for some x.

As we have seen before, X is partitioned by the G-orbits:



and we can understand each orbit as "all possible points x can go to under some g". Hence:

! Keypoint

An action is transitive if there exists $x \in X$ which can "go to every point in X".

In which case we can also see any x would work, since they all live in the same orbit. So G acts transitively iff

$$X = G \cdot x \text{ for any } x \in X.$$

Example 4.18 (Examples of transitive actions)

- The action of G on itself by left multiplication is transitive, as we have seen in Example 4.7.
- However, the action of G on itself by conjugation is not transitive if $G \neq \{e\}$: suppose there is only one G-orbit (i.e. conjugacy class), then $G = e^G$, so for any $g \in G$ we must have
$$g = heh^{-1} = e \text{ for some } h \in G.$$
- The action of G on G/H where $H \leq G$ is transitive (again, G/H means just the set of left cosets, not necessarily a quotient group). The action is defined via
$$G \times (G/H) \to G/H, \quad g \cdot xH = gxH.$$
Indeed, it is clear that $G \cdot H = G/H$.

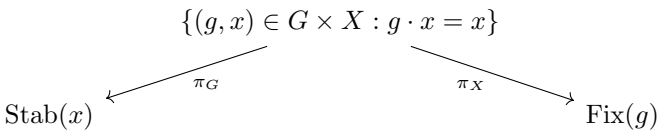
To proceed, let us define a new notion:

Definition 4.19 (Fixed points)

Let G act on X. An element $x \in X$ is called a **fixed point** of $g \in G$ if $g \cdot x = x$. We write
$$\mathrm{Fix}(g) = \{x \in X : g \cdot x = x\} \subseteq X$$
for the set of fixed points of g.

Caution: This looks dangerously similar to the definition of stabilisers, but note that $\mathrm{Fix}(g) \subseteq X$, while $\mathrm{Stab}(x) \subseteq G$.

In fact, these two notions are closely related. Consider the set of pairs (g, x) such that $g \cdot x = x$. Then:



i.e. if we project to the G component we get $\mathrm{Stab}(x)$, and vice versa for the X component and $\mathrm{Fix}(g)$.

Now under a transitive action, the orbit-stabiliser theorem simplifies to
$$|X| = [G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)| \tag{2}$$
for any $x \in X$. Using the above relation, we get the following result:

Proposition 4.20

If G acts transitively on X where both G and X are finite, then
$$|G| = \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Proof. By the diagram above, we can count the size of the top set in both ways:
$$\sum_{x \in X} |\mathrm{Stab}(x)| = |\{(g, x) \in G \times X : g \cdot x = x\}| = \sum_{g \in G} |\mathrm{Fix}(g)|.$$
Then by (2),
$$\sum_{x \in X} |\mathrm{Stab}(x)| = \sum_{x \in X} \frac{|G|}{|X|} = |X| \cdot \frac{|G|}{|X|} = |G|.$$
The result follows. □

In particular, this also implies that for $|X| \geq 2$, there is at least one $g \in G$ which has no fixed points: or else $\sum |\mathrm{Fix}(g)| \geq |G|$, and $\mathrm{Fix}(e_G) = X$ has more than one element, so $\sum |\mathrm{Fix}(g)| > |G|$, contradiction.

We can generalise the result, which gives the crux of this section: counting the number of orbits.

Corollary 4.21 (Burnside's lemma)

Let G act on X. The number of G-orbits, $|X/G|$, is equal to

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Proof. Write X as a disjoint union of G-orbits,

$$X = \bigcup_{i=1}^{n} G \cdot x_i,$$

then the number of fixed points of $g \in G$ is the sum of the number of fixed points of g in each $G \cdot x_i$. But note that G acts on each $G \cdot x_i$ transitively, so Proposition 4.20 applies and thus

$$|X/G| = \sum_{i=1}^{n} 1 = \sum_{i=1}^{n} \left(\frac{1}{|G|} \sum_{g \in G \cdot x_i} |\mathrm{Fix}(g)| \right) = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|. \qquad \square$$

Remark. As usual, this lemma was not actually proven by Burnside; Cauchy proved it first, and thus it is sometimes called *the lemma that is not Burnside's.*

The significance of Burnside's lemma is that we can calculate the number of orbits more easily, since the number of fixed points are often easy to compute.

Example 4.22

Consider when $G = \langle \sigma \rangle \leq S_5$ where $\sigma = (12)(345)$, and $X = \{1, 2, 3, 4, 5\}$. We have:

g	id	σ^1	σ^2	σ^3	σ^4	σ^5
$\mathrm{Fix}(g)$	X	$\emptyset$	$\{1,2\}$	$\{1,2,3\}$	$\{1,2\}$	$\emptyset$

Hence, the number of orbits, which is equal to the average number of fixed points by Burnside's lemma, is

$$|X/G| = \frac{5 + 0 + 2 + 3 + 2 + 0}{6} = 2.$$

Indeed, the two orbits are $G \cdot 1 = \{1, 2\}$ and $G \cdot 3 = \{3, 4, 5\}$.

Remark. By orbit-stabiliser we also have a **G-isomorphism** (a bijection which preserves the group action)

$$G/\operatorname{Stab}(x) \to G \cdot x = X$$

for any $x \in X$. Hence, we can also view a transitive action as acting on the set $G/\operatorname{Stab}(x)$. As $\operatorname{Stab}(x) \leq G$, this coincides with the third example in Example 4.18. Thus:

! Keypoint

A transitive action of a group G is equivalent to an action of G on a set of cosets G/H for some $H \leq G$.

Therefore, studying the action of G on G/H is natural and is often a useful tool.

4.4 Primitivity ⋆

We now classify transitive actions further into primitive and imprimitive actions.

Motivation

Let us start with an example. Consider $G = S_4$ acting on $X = \{1, 2, 3, 4\}$, and $\sigma = (1234)$. Then the **partition**

$$\{\{1, 3\}, \{2, 4\}\}$$

of X is "preserved" under σ, since

$$\sigma \cdot \{1, 3\} = \{2, 4\} \quad \text{and} \quad \sigma \cdot \{2, 4\} = \{1, 3\}.$$

This phenomenon plays an important role in the analysis of group actions, so we will formalise the idea below.

In what follows, we shall the extend the action of a group G on X to *subsets of* X by defining

$$g \cdot A := \{g \cdot x : x \in A\}$$

for each $A \subseteq X$. The notion used in the motivation is as follows:

Definition 4.23 (Stabilised partition)

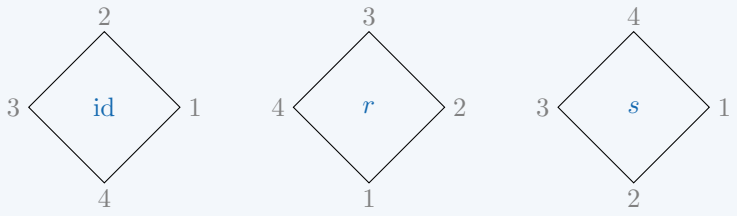
Let G act on X, and let π be a partition of X, i.e. a collection of disjoint subsets of X such that the union is X. We say that π is **stabilised** by G if for any $g \in G$,

$$A \in \pi \implies g \cdot A \in \pi.$$

It suffices to check the condition on a set of generators for G.

Example 4.24 (Examples of stabilised partitions)

- By above, the subgroup $G = \langle (1234) \rangle$ of S_4 stabilises the partition $\{\{1, 3\}, \{2, 4\}\}$ of $\{1, 2, 3, 4\}$.
- Identify $X = \{1, 2, 3, 4\}$ as the set of vertices of the square, and let D_4 acts in the usual way:



  i.e. with $r = (1234)$ and $s = (24)$, then D_4 stabilises the partition $\{\{1, 3\}, \{2, 4\}\}$ of X again (geometrically, this means opposite vertices stay opposite under both r and s).

- Recall that $G = \mathrm{GL}_2(\mathbb{R})$ act on $X = \mathbb{R} \setminus \{0\}$ by matrix multiplication, i.e. $A \cdot \mathbf{v} \mapsto A\mathbf{v}$.
  Now consider the partition $\{\ell_{\mathbf{v}}\}$ consisting of lines through origin (without the origin),

$$\ell_{\mathbf{v}} := \{\lambda \mathbf{v} : \lambda \neq 0\}.$$

  Then any $A \in G$ sends any $\ell_{\mathbf{v}}$ to another such line, namely $\ell_{A\mathbf{v}}$. So G stabilises this partition of X.

It is clear that if $|X| > 1$, the group G always stabilises two different partitions of X:

- The set of singletons: $\pi = \{\{x\} : x \in X\}$;
- The whole set: $\pi = \{X\}$.

This motivates the main definition:

Definition 4.25 (Primitive actions)

Let G act on X. If the only two partitions stabilised by G are

$$\{\{x\} : x \in X\} \quad \text{and} \quad \{X\},$$

then we say the action is **primitive**. Otherwise, it is **imprimitive**.

Remark. Some authors also say a subgroup of $\mathrm{Sym}(X)$ is primitive if it acts primitively on X.

Note that all examples in Example 4.24 are imprimitive, since there is some non-trivial stabilised partition.

Example 4.26 (S_n is primitive)

For instance, S_n acts primitively on $X = \{1, \dots, n\}$ (or we can just say S_n is primitive by the remark): Suppose there is a partition π with more than two sets, and one of the sets has more than one element, say:

$$\pi = \{\{x_1, x_2, \dots\}, \{y, \dots\}, \dots\}$$

then by setting $\sigma = (x_1 y)$,

$$\sigma \cdot \{x_1, x_2, \dots\} = \{y, x_2, \dots\} \notin \pi.$$

So π cannot be stabilised by S_n.

We promised primitive is a stronger condition than transitive; this proposition explains why:

Proposition 4.27

Let G act on X. If the action is primitive, then it is either transitive or trivial ($g \cdot x = x$).

Proof. Note that the G-orbits form a partition of X, and is stabilised by G, as for any $x \in X$,

$$g \cdot (G \cdot x) = \{g \cdot (h \cdot x) : h \in G\} = \{(gh) \cdot x : h \in G\} = G \cdot x.$$

Therefore, if the action is primitive, then the partition into orbits must be one of the trivial ones, i.e. either

- $G \cdot x = \{x\}$ for all $x \in X$, then $g \cdot x = x$ for all $g \in G$, so the action is trivial; or
- $G \cdot x = X$ for one (hence all) $x \in X$, so the action is transitive. □

We introduce a convenient notion:

Proposition 4.28

The group G acts imprimitively if and only if there exists $A \subset X$ (proper) with $|A| > 1$ such that for all $g \in G$,

$$\text{either} \quad g \cdot A = A \quad \text{or} \quad (g \cdot A) \cap A = \emptyset. \tag{3}$$

A subset A satisfying (3) will be called a **block**.

Proof. If G acts imprimitively then any set A in the partition π stabilised by G works. Conversely, given such an A we can form a partition $\{g \cdot A : g \in G\}$ of X, which is stabilised by G. □

Caution: Note that the requirement that $1 < |A| < X$ is **not** included in the definition of a block.

In other words:

! Keypoint

An action is primitive if and only if there are no non-trivial blocks.

In this case, there is also a partition of X into blocks, because $g \cdot A$ is also a block: Let $h \in G$ and suppose

$$((hg) \cdot A) \cap (g \cdot A) \neq \emptyset.$$

For any $x \in ((hg) \cdot A) \cap (g \cdot A)$, applying g^{-1} on the left gives

$$g^{-1} \cdot x \in ((g^{-1}hg) \cdot A) \cap A$$

so by A being a block, this forces $(g^{-1}hg) \cdot A = A$, thus $(hg) \cdot A = g \cdot A$, as desired.

The condition $g \cdot A = A$ should ring a bell – it looks exactly like the stabiliser. For this reason, we can extend our original definition:

Definition 4.29 (Stabiliser of a set)

Let G act on X. The **(setwise) stabiliser** of $A \subseteq X$ is the set of $g \in G$ which fix A, i.e.

$$\mathrm{Stab}_G(A) := \{g \in G : g \cdot A = A\} \subseteq G.$$

Again, one can easily check that this is a subgroup of G.

For the remainder of this section, we shall assume G to be finite, acting transitively on a set X with $|X| > 1$. The final results we will look at is a correspondence between primitive actions and the subgroups in G. We define:

Definition 4.30 (Maximal subgroup)

A subgroup $H < G$ is called a **maximal subgroup** if the only subgroups of G which contain H are H and G.

Again note that $H \neq G$ from the definition. Equivalently, there is not a chain of subgroups

$$H < K < G$$

where both of the inclusions are proper.

Lemma 4.31

Let A be a non-trivial block in X. For any $x \in A$,

$$\mathrm{Stab}(x) < \mathrm{Stab}(A) < G.$$

Proof. We have $\mathrm{Stab}(x) \subseteq \mathrm{Stab}(A)$ because

$$g \cdot x = x \implies (g \cdot A) \cap A \neq \emptyset \implies g \cdot A = A.$$

Now to show $\mathrm{Stab}(x) \neq \mathrm{Stab}(A)$, let $y \in A$ where $y \neq x$. Since G acts transitively on X, there is a $g \in G$ such that $g \cdot x = y$. Then $g \in \mathrm{Stab}(A)$ (as $y \in (g \cdot A) \cap A$) but $g \notin \mathrm{Stab}(x)$.

Finally, $\mathrm{Stab}(A) \neq G$ since for any $y \notin A$ there exists $g \in G$ such that $g \cdot x = y$, so $g \notin \mathrm{Stab}(A)$. □

This proves one direction of the following:

Theorem 4.32

The group G acts primitively on X if and only if there exists $x \in X$ such that $\mathrm{Stab}(x)$ is maximal in G.

Proof. ($\Leftarrow$) is by Proposition 4.28 and Lemma 4.31. For ($\Rightarrow$), suppose there exists $x \in X$ and a subgroup H with

$$\mathrm{Stab}(x) < H < G.$$

Then we claim that $A = H \cdot x$ is a non-trivial block. From $H \neq \mathrm{Stab}(x)$ we have $H \cdot x \neq \{x\}$, so $\{x\} \subset A \subset X$.

If $g \in H$ then $g \cdot A = A$. Otherwise $(g \cdot A) \cap A = \emptyset$: if $(gh) \cdot x = h' \cdot x$ for some $h' \in H$, then $h'^{-1}gh \in \mathrm{Stab}(x) \subset H$, say $h'^{-1}gh = h''$, and $g = h'h''h^{-1} \in H$, contradiction. Hence A is a block. □

Remark. Similar to transitive actions, if the condition in Theorem 4.32 is true for some $x \in X$, then it is also true for all $x \in X$, because $\mathrm{Stab}(x)$ and $\mathrm{Stab}(y)$ are conjugate for any $x, y \in X$ (Lemma 4.9).

Combining with the fact that a transitive action is just an action on G/H for some $H \leq G$, we can conclude:

Corollary 4.33

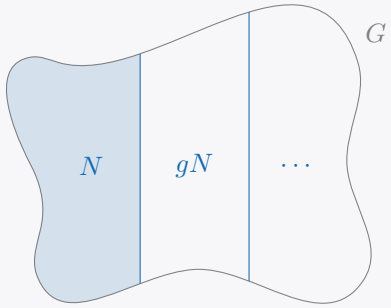
The group G acts primitively on X if and only if X is in G-isomorphism to G/H where $H \leq G$ is maximal.

One can easily check that the action of G on G/H in this case is indeed primitive, establishing ($\Leftarrow$).

Motivation

Final words: It is natural to wonder why we care about this miraculous notion at all. It turns out that primitivity is an analogue to simple groups (Definition 2.6), and thus are again building blocks to any group actions:

Recall that a group G is simple if its only normal subgroups are $\{e_G\}$ and G. Now given any group G and $N \trianglelefteq G$, we can form a partition of G, namely the set of cosets G/N:



Therefore, a (finite) group G is simple if and only if the only partitions of G into cosets of any normal subgroup N are $\{N\}$ (when $G/N \cong \{e\}$), or $\{gN : g \in G\}$ with $|N| = 1$ (when $G/N \cong G$), i.e.

$$\{G\} \quad \text{or} \quad \{\{g\} : g \in G\}.$$

As we can see, primitivity just extends this idea to general sets.

4.5 Sylow Theorems ⋆

The final part of group actions we will look at are the famous **Sylow theorems**, which tell you rich information about subgroups of any finite group.

Definition 4.34 (Sylow subgroups)

Let G be a group and let p be a prime dividing $|G|$. A subgroup of G is called a **Sylow p-subgroup** of G if its order is the highest power of p dividing $|G|$.

In other words, H is a Sylow p-subgroup if it is a p-group and $[G : H] = |G|/|H|$ is coprime to p. The Sylow theorems tell you three things:

- There exists Sylow p-subgroups of all primes $p \mid |G|$;
- The Sylow p-subgroups for a fixed p are conjugate; and
- Every p-subgroup of G is contained in such a subgroup.

Moreover, the theorems restrict the possible number of Sylow p-subgroups of G.

Remark. In this section, all groups are finite.

Before we go into the Sylow theorems, we will frequently use the following fact:

Lemma 4.35

Let G be a p-group acting on a finite set X, and X^G be the elements $x \in X$ such that $G \cdot x = \{x\}$. Then

$$|X| \equiv |X^G| \pmod{p}.$$

Proof. By orbit-stabiliser, for any $x \in X$, we have

$$|G \cdot x| = [G : \mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)|.$$

As $|G|$ is a power of p, so is $|G \cdot x|$, thus $G \cdot x$ is either a singleton ($x \in X^G$) or $|G \cdot x|$ is divisible by p. Writing X as the disjoint union of orbits give the result. □

Remark. In the special case of a p-group G acting on itself by conjugation, this translates to $|G| \equiv |Z(G)| \pmod{p}$, which implies Theorem 4.15.

Theorem 4.36 (Sylow I)

Let G be a (finite) group, and let p be a prime. If $p^r \mid |G|$, then G has a subgroup of order p^r.

Proof. By Corollary 4.16, it suffices to show that there exists a Sylow p-subgroup. Let $|G| = p^r m$ with $p \nmid m$, and

$$X = \{A \subseteq G : |A| = p^r\},$$

with the action of G defined by $g \cdot A \mapsto gA := \{ga : a \in A\}$.

Now for some $A \in X$, consider $H := \mathrm{Stab}(A) = \{g \in G : gA = A\}$. By orbit-stabiliser,

$$p^r m = |G| = [G : H] \cdot |H| = \frac{|G|}{|\mathrm{Stab}(A)|}|H| = |G \cdot A| \cdot |H|.$$

So if we can find A such that $p \nmid |G \cdot A|$, then we can conclude that $|H| = p^r$. Indeed,

$$|X| = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m - 1) \cdots (p^r m - i) \cdots (p^r m - p^r + 1)}{p^r (p^r - 1) \cdots (p^r - i) \cdots (p^r - p^r + 1)}.$$

Note that for any $i < p^r$, the power of p dividing $p^r m - i$ is the power of p dividing i. The same is true for $p^r - i$, therefore the corresponding terms on top and bottom are divisible by the same powers of p, so $p \nmid |X|$.

As the orbits form a partition of X, $|X| = \sum |G \cdot A_i|$ and thus at least one of the $|G \cdot A_i|$ is not divisible by p. □

Example 4.37 (Example of Sylow p-subgroup)

Consider $G = \mathrm{GL}_n(\mathbb{F}_p)$. The elements in G are precisely those whose columns form a basis for $\mathbb{F}_p^n$. Thus, the first column can be any nonzero vector, of which there are $p^n - 1$; the second column can be any vector not in the span of the first column, of which there are $p^n - p$; and so on. Therefore,

$$|G| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}),$$

and so the largest power of p dividing $|G|$ is $p^{1+2+\ldots+(n-1)}$. Now the upper triangular matrices of the form

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

form a subgroup U of order $p^{n-1}p^{n-2} \cdots p$, which is therefore a Sylow p-subgroup of G.

Remark. The theorem can be seen as a massive generalisation of Cauchy's theorem (Theorem 4.12). If a prime p divides $|G|$, then G has a subgroup H of order p, and any $h \neq e_G \in H$ will be an element of G of order p.

We now move on to the second theorem of Sylow, which tells you information on the Sylow p-subgroups. To do so, we need a new definition:

Definition 4.38 (Normaliser)

Let H be a subgroup of G. The **normaliser** of H in G is

$$N_G(H) = \{g \in G : gH = Hg\}.$$

Equivalently, $N_G(H)$ is the stabiliser of H under the conjugation action of G.

By Lemma 2.3(iii), H is normal in G iff $N_G(H) = G$. Moreover, one can see that $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup.

Lemma 4.39

Let P be a Sylow p-subgroup of G, and let H be a p-subgroup. If H normalises P, i.e. if $H \subseteq N_G(P)$, then $H \subseteq P$. In particular, no Sylow p-subgroup of G other than P normalises P.

Proof. Since H and P are subgroups of $N_G(P)$ with $P \trianglelefteq N_G(P)$, we may apply second isomorphism theorem and

$$H/H \cap P \cong HP/P.$$

Therefore $[HP : P]$ is a power of p (as H is a p-group), but

$$|HP| = [HP : P] \cdot |P|$$

and $|P|$ is the largest power of p dividing $|G|$, hence also $|HP|$. Thus $[HP : P] = p^0 = 1$, i.e. $H \subseteq P$. □

We are now ready to state and prove the second Sylow theorem:

Theorem 4.40 (Sylow II)

Let G be a (finite) group, and let $|G| = p^r m$ with $p \nmid m$. Then:

(a) Any two Sylow p-subgroups are conjugate.

(b) Let s_p be the number of Sylow p-subgroups in G; then $s_p \equiv 1 \pmod{p}$ and $s_p \mid m$.

(c) Every p-subgroup of G is contained in a Sylow p-subgroup.

Proof. (a) Let X be the set of Sylow p-subgroups in G, and let G act on X by conjugation, i.e.

$$G \times X \to X, \quad g \cdot P := gPg^{-1}.$$

We shall show that this action is transitive, i.e. some G-orbit $\mathcal{O}$ is all of X.

Let $P \in \mathcal{O}$, and let P act on $\mathcal{O}$ through the action of G. This single G-orbit may break up into several P-orbits, one of which will be $\{P\}$. In fact this is the only one-point orbit, because

$$\{Q\} \text{ is a } P\text{-orbit} \iff P \subseteq N_G(Q)$$

which we know (from the lemma above) happens only for $Q = P$. Again by orbit-stabiliser, the number of elements in every P-orbit other than $\{P\}$ would then be divisible by p, and so $|\mathcal{O}| \equiv 1 \pmod{p}$.

Now if there exists $P \neq \mathcal{O}$, then we again let P act on $\mathcal{O}$, but this time the same argument shows that there are no one-point orbit, so $p \mid |\mathcal{O}|$, which contradicts what we proved in the last paragraph. So $X = \mathcal{O}$.

(b) Since $s_p = |X| = |\mathcal{O}|$, we have shown that $s_p \equiv 1 \pmod{p}$.

Let P be a Sylow p-subgroup of G (so $\mathcal{O} = G \cdot P$ by (a)). By orbit-stabiliser,

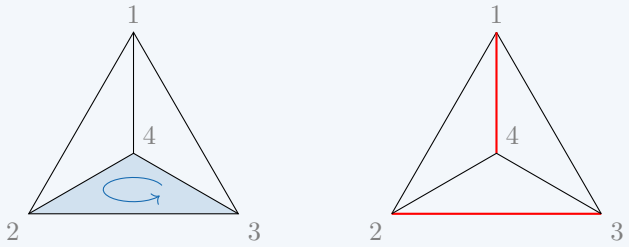
$$s_p = |G \cdot P| = [G : N_G(P)] = \frac{|G|}{|N_G(P)|} = \frac{|G|}{[N_G(P) : P] \cdot |P|} = \frac{m}{[N_G(P) : P]}$$

which implies $s_p \mid m$.

(c) Let H be a p-subgroup of H, and let H act on the set X of Sylow p-subgroups by conjugation. As $p \nmid s_p = |X|$, X^H must be nonempty (Lemma 4.35), i.e. at least one H-orbit consists of a single Sylow p-subgroup, one of which is $\{P\}$. But then H normalises P and the lemma above implies that $H \subseteq P$. □

Example 4.41 (Sylow subgroups of S_4)

Consider $G = S_4$, with order $24 = 2^3 \cdot 3$. There is a nice geometric visualisation of the Sylow subgroups by considering the action of S_4 on a tetrahedron:



- The Sylow 3-subgroups are the stabilisers of faces, generated by rotations as shown on the left, i.e.

  $$\langle(123)\rangle, \quad \langle(124)\rangle, \quad \langle(134)\rangle, \quad \text{and} \quad \langle(234)\rangle.$$

  They are conjugate because S_4 evidently acts transitively on the faces, and we see that there are indeed $4 \equiv 1 \pmod{3}$ Sylow 3-subgroups as there are 4 faces.

- The Sylow 2-subgroups are the stabilisers of pairs of opposite edges; for instance, the pair shown on the right has stabiliser

  $$\{\mathrm{id}, (14), (23), (12)(34), (13)(24), (14)(23), (1342), (1243)\}.$$

  Again they are conjugate because S_4 acts transitively on the set of pairs of disjoint edges, and there are $3 \equiv 1 \pmod{2}$ Sylow 2-subgroups as there are 3 such pairs.

Sylow theorems are extremely useful for classifying groups with only a few prime factors. We will see this in action after we develop more theory (see Section 6).

5 Normal Series

6 Extensions