MAT347: Groups, Rings & Fields

Rishibh Prakash

September 2022

Contents

1 Groups

Groups are incredibly important objects in mathematics. Despite (or maybe because of) their simple definition, groups are quite powerful.

At their core, groups are about symmetry. Consider, for example, an equilateral triangle. The symmetries of a shape are the set of rigid motions that result in the same shape in the same position. For a triangle, we can rotate it $\frac{2\pi}{3}$ radians (counter-clockwise, say) or $\frac{4\pi}{3}$ radians. In addition, we can also reflect the triangle across the perpendicular bisector of any edge. Finally, we have the identity transformation that does nothing and leaves the triangle as it is. Thus we have a total of 6 symmetries which is also the number of ways arranging the 3 vertices allowing us to conclude that we have found all the symmetries.

Suppose ρ is the rotation by $\frac{2\pi}{3}$ and σ is the reflection that swaps vertices B and C. Then $\rho\sigma$ is the reflection that swaps and A and C while $\sigma\rho$ is the reflection that swaps A and B. It should make sense that the composition of two symmetries is itself a symmetry. Performing the first action results in the same equilateral triangle so we can perform the second action which also gives the same triangle. Thus their composition is a symmetry. Importantly, however, the order in which the composition is performed is important. In the above example, we say that σ and ρ do not commute.

A similar example are the symmetries of a square. In this case, there is the identity transformation, along with 3 rotations and 4 reflections (8 in total). Note that there are in some sense 2 kinds of reflections: those with the line of reflection through the diagonal and those with the line of reflection through the edges. The first kind of reflection fixes two of the vertices while the second kind has no fixed points. One other thing to note about all the symmetries is that they can be undone to return to the original position.

Definition 1.1 (Group)**.** A group is a set G with a composition

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto gh = g \circ h \end{aligned}$$

satisfying:

1. associativity: $(gh)k = g(hk)$
2. existence of identity element: $\exists e \in G$ such that $ge = eg = g$ for all $g \in G$
3. existence of inverses: for every $g \in G$, there exists some $g^{-1} \in G$ such that $gg^{-1} = e = g^{-1}g$.

Some more examples of groups are:

- $\mathbb{Z}$ (or any field) with $+$ as the operation
- $\mathbb{Z}/n\mathbb{Z}$ with addition mod n
- $SL(n, \mathbb{F})$ which is the set of all $n \times n$ matrices over a field $\mathbb{F}$ with determinant 1

2 Examples of Groups

2.1 Fields

A field $\mathbb{F}$ consists of 2 (commutative) groups. First we have the additive group $(\mathbb{F}, +)$ with 0 as the identity and for every $x \in \mathbb{F}$ we have its 'inverse' as $-x$. We also have the multiplicative group, often denoted $\mathbb{F}^\times$, which consists of the non-zero elements of $\mathbb{F}$ with the operation of (surprise, surprise) multiplication. In this case the identity is 1 and the inverses are the usual multiplicative inverses.

Given a field, we can also construct a number of related matrix groups.

- General linear group, $GL(n, \mathbb{F})$ = set of invertible $n \times n$ matrices (with entries in $\mathbb{F}$)
- Special linear group, $SL(n, \mathbb{F})$ = set of matrices with determinant 1
- Special orthogonal group, $SO(n)$ = set of matrices A in $SL(n, \mathbb{F})$ such that $AA^T = I$. If $\mathbb{F} = \mathbb{R}$, then this is the set of rotations in $\mathbb{R}^n$.

2.2 Cyclic groups

Another important example of a group is $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. You typically think of this group as consisting of elements $\{0, 1, \ldots, n-1\}$ with the operation being addition mod n. To remind us that we are working with modular arithmetic, we often but a bar on top of the numbers, e.g. if $n = 8$, we might write $\overline{5} + \overline{7} = \overline{4}$. As one might expect, the identity is $\overline{0}$. Note that in this group $\overline{k}^{-1} = \overline{-k} = \overline{n-k}$.

There is a very natural correspondence between $\mathbb{Z}/n\mathbb{Z}$ and the n-th roots of unity. In particular, we can map $\overline{k}$ to $e^{\frac{k \cdot 2\pi i}{n}}$. The cyclic structure of the group is made particularly clear in the latter case (consider what $\overline{k+n}$ is mapped to) motivating the name *cyclic group* for $\mathbb{Z}/n\mathbb{Z}$. In general, the cyclic group of order n is denoted C_n.

2.3 Quaternion group

The quaternion group $\mathbb{H}$ is a group of 8 elements

$$\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$$

with the multiplication defined as follows

$$\begin{aligned} ij &= -ji = k \\ jk &= -kj = i \\ ki &= -ik = j \\ i^2 = j^2 = k^2 &= -1 \end{aligned}$$

The 1 is (of course) the identity and multiplication with -1 switches signs as you would expect.

Remark 2.1. Sometimes, $\mathbb{H}$ is also used to refer to the set of all linear combinations of i, j, k. This is often called the set of all quaternions or the Hamiltonian algebra.

3 Subgroups

Consider the triangle group from the previous section and consider just the rotations (including the identity element, which you can think of as a rotation by 0). It is easy to see that this set forms a group in its own right and in fact is (isomorphic to) the cyclic group of order 3.

Definition 3.1 (Subgroup)**.** A non-empty subset H of a group G is a subgroup, denoted $H \leq G$, if H is a group using the same operation as G. In other words, for all $h, k \in H$ we have $hk \in H$ and $h^{-1} \in H$.

Remark 3.2. The conditions automatically imply that $e \in H$.

Remark 3.3. If $\mathbb{F}$ is a field then we know that $(\mathbb{F}, +)$ is a group and $\mathbb{F}^\times$ is a subset of $\mathbb{F}$. But it is not a subgroup since the operations are different.

Proposition 3.4 *If $H \subset G$ is non-empty, then $H \leq G$ if and only if $hk^{-1} \in H$ for all $h, k \in H$.*

Proof. Exercise (cute) □

Consider the powers of i in $\mathbb{H}$. Since $i^2 = -1, i^3 = -i$ and $i^4 = 1$, we see that $\{1, i, -1, -i\}$ forms a (cyclic) subgroup of $\mathbb{H}$. We say that this (sub)group is generated by i and denote it $\langle i \rangle$. In general, given a group G and $g_1, \ldots, g_n \in G$, we use $\langle g_1, \ldots, g_n \rangle$ to denote the smallest subgroup of G that contains $g_1, \ldots, g_n$. The generator of a subgroup need not be unique. Looking at the above example of the subgroup of $\mathbb{H}$, we see that it is also generated by $-i$.

Suppose we are given $g \in G$ such that there exists some $m \in \mathbb{N}$ satisfying $g^m = e$. Let $n = \min\{m \in \mathbb{N} : g^n = e\}$. Then $|\langle g \rangle| = n$. We also say that the order of g is n (this is the order of an element of a group rather than the order of a group). If no such m exists, then the order of g is infinite and $\langle g \rangle = \{1, g^{\pm 1}, g^{\pm 2}, \ldots\}$ is isomorphic to $\mathbb{Z}$.

4 Cosets

As is so typical in mathematics, we begin with a definition.

Definition 4.1 ((Right) cosets)**.** Let G be a group and $H \leq G$ is a subgroup. Take some $g \in G$ and consider

$$Hg := \{hg : h \in H\}$$

This is called a *(right) coset* of H.

Remark 4.2. One can equivalently define left cosets by considering gH instead.

The remarkable thing about cosets is that they are either disjoint or equal. Let us prove this statement.

Proposition 4.3 *Let $g, g' \in G$. Then Hg and Hg' are either disjoint or equal.*

Proof. Suppose Hg and Hg' are not disjoint. Thus there lies something in the intersection. This means that

$$hg = h'g'$$

for some $h, h' \in H$. Then $g = h^{-1}h'g'$. Since H is a subgroup, $h^{-1}h' \in H$ implying that $g \in Hg'$. Similarly we can conclude that $g' \in Hg$.

Now consider an arbitrary element in Hg, call it kg where $k \in H$. Then

$$kg = kh^{-1}h'g'$$

is also an element of Hg' since $kh^{-1}h' \in H$. Therefore $Hg \subset Hg'$ and symmetrically we can conclude that $Hg' \subset Hg$ giving us the final conclusion $Hg = Hg'$. □

This means that (right) cosets of H partition G (one needs to show that the union of all the cosets is indeed G but this is clear since for every $g \in G$, we can find g in Hg). Recall that a partition of a set also defines an equivalence relation on it, where 2 elements are equivalent if and only if they are in the same set of the partition. Thus the equivalence classes correspond exactly to the cosets.

Additionally, note that if $hg = h'g$ then $h = h'$ (we multiply by g^{-1} on the right on both sides). Hence each $h \in H$ gives a difference element hg in Hg. This means that

$$|Hg| = |H|$$

Thus we find that

$$|G| = (\#\text{ of distinct cosets}) \cdot |H|$$

We have just proven Lagrange's theorem.

Theorem 4.4 (Lagrange's Theorem) *If $|G| < \infty$ and $H \leq G$ then $|H|$ divides $|G|$.*

We often write $\frac{|G|}{|H|} = [G : H]$ and called it the *index* of H in G. Thus we could equivalently write

$$|G| = [G : H] \cdot |H|$$

a statement which also holds for infinite groups since if $|G| = \infty$ then (at least) one of the terms on the right will be infinite.

Let us consider some consequences of Lagrange's theorem. For example let G be a group of order p where p is a prime number. Then we know that G cannot have non-trivial subgroups. In other words, the only subgroups of G are $\{e\}$ and G itself. We know a G of order p exists of course, take $\mathbb{Z}/p\mathbb{Z}$, and we will see later that this is the only group of this order.

4.1 Example

Let $G = \mathbb{Z}$ be the integers and consider $\mathbb{H} = 2\mathbb{Z}$ the even integers. Then $H + 0 = H$ (the set of all even integers) is one coset and $H + 1$ (the set of all odd integers) is the other coset. We know there can't be any more cosets since these two cover the whole group. Thus

$$\mathbb{Z} = 2\mathbb{Z} \dot{\cup} 2\mathbb{Z} + 1$$

which is to say

$$[\mathbb{Z} : 2\mathbb{Z}] = 2$$

4.2 Interaction of cosets

Everything so far also holds for left cosets, by flipping the order and words when necessary. The more interesting thing to consider is the interaction between left and right cosets.

Consider for example the triangle group we have been working with so far. We have the three rotations e, ρ, ρ^2 and the reflections $\sigma_A, \sigma_B, \sigma_C$ where σ_K is the reflection that fixes vertex K. Therefore $G = \{e, \rho, \rho^2, \sigma_A, \sigma_B, \sigma_C\}$. We will take our subgroup to be $H = \{e, \sigma_A\}$. Then the right cosets are

$$\begin{aligned} He &= H = \{e, \sigma_A\} \\ H\rho &= \{\rho, \sigma_A\rho\} = \{\rho, \sigma_B\} \\ H\rho^2 &= \{\rho^2, \sigma_A\rho^2\} = \{\rho^2, \sigma_C\} \end{aligned}$$

On the other hand left cosets are

$$\begin{aligned} eH &= H = \{e, \sigma_A\} \\ \rho H &= \{\rho, \rho\sigma_A\} = \{\rho, \sigma_C\} \\ \rho^2 H &= \{\rho^2, \rho^2\sigma_A\} = \{\rho^2, \sigma_B\} \end{aligned}$$

Note how different these are. The right coset containing ρ contains σ_B while the left coset containing ρ contains σ_C. This illustrates that in general, left and right cosets can be completely different. The exception of course is if G is commutative since in that case the order of multiplication does not matter. The one that remains constant, regardless of whether or not G is commutative, is the number of cosets.

5 Action

Definition 5.1 (Group action)**.** An action of a group on a set X is a map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x = gx \end{aligned}$$

such that for any $x \in X$ we have

1. $e \cdot x = x$
2. $(gh) \cdot x = g(h \cdot x)$

5.1 Groups acting on themselves

If G is a group, then it can act on itself. The most obvious manner of defining $g \cdot x$ is to use the group operation itself so that $(g, x) \mapsto gx$. This is called *left translation* or the *left regular action*.

One might wonder whether we could define (g, x) to map to xg. In this case note that (gh, x) maps to xgh where $(g, (h, x))$ is sent to xhg. Since in general $hg \neq gh$, we see that this is not action.

However we can 'fix' this by using the inverse. Namely the map $(g, x) \mapsto xg^{-1}$ is indeed an action. This is what we call a *right translation* or *right regular action*. Finally we have conjugation which can be thought of as a combination of the previous two actions and is arguably the most important one. In this case, we have $(g, x) \mapsto gxg^{-1}$.

5.2 Example

Let G be $SO(3) = \{A \in \mathbb{R}^{3\times 3} : \det(A) = 1 \text{ and } AA^T = I\}$. This is of course the set of all rotations in $\mathbb{R}^3$. It is easy to see that G acts on S^2 exactly by rotating it. Note we can embed $SO(2)$ in $SO(3)$ by fixing the z-axis. To be precise, we define

$$H := \left\{ \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} : \theta \in [0, 2\pi) \right\}$$

We see that H only rotates the $x - y$ plane thus it maps a point to some other point at the same altitude (fixing the north and south poles).

5.3 Orbits

Definition 5.2. If G acts on X and $x \in X$ the the *orbit* of x (under G) is the set of all points x take to by elements of G and is often denoted

$$G \cdot x := \{gx : g \in G\}$$

Remark 5.3. The orbits of H on the sphere are the lines of latitude and the north and south poles.

We see that given a pair of points on the sphere there is a rotation that takes the first point to the second point. Thus Gx for any $x \in S^2$ is simply S^2 again.

Let us instead consider H then. The orbit of N, the north pole, under H is simply $\{N\}$. This means that for any $g \in G$, we have $gHN = gN$ since $ghN = gN$ for every $h \in H$. Thus every element of gH maps N to the same point or in other words, every coset maps N to a unique point. We may wonder whether this mapping is 1-1. In other words, can two different cosets maps N to the same point. Suppose this is the case. In other words, we have $gHN = g'HN$ which is to say $gN = g'N$. Recall that N is an element of the set S^2 and not the group. So we cannot conclude that $g = g'$. On the other hand what we do have is that $g^{-1}g'N = N$. Since $g^{-1}g'$ fixes N it must be an element of H (we have not shown that H contains all elements that fix N but hopefully this is easy to see intuitively). But if $g^{-1}g' \in H$ then $gH = g'H$. Thus not only do individual cosets map N to a single point, distinct cosets map N to distinct points. Since we know that N can be mapped to any point on the sphere by choosing an appropriate g we conclude that points on the sphere are in 1-1 correspondence with the (left) cosets of H.

6 Stabilizers and Centralizers

Definition 6.1 (Stabilizer)**.** Suppose G is a group that acts on a set X. Then given any $x \in X$ we can define

$$Stab_G(x) = \{g \in G : gx = x\}$$

and call it the *stabilizer* of x in G

Example 6.1. By looking at the previous example with $SO(3)$, we see that the stabilizer of the north pole N are the rotations in the $x - y$ plane. ■

It is easy to verify that the stabilizer of an element forms a subgroup of G. The example of the sphere generalises almost immediately to allow us to conclude that points in the orbit of x are in $1-1$ correspondence with the (left) cosets of $Stab_G(x)$. This gives us the Orbit-Stabilizer theorem.

Theorem 6.2 (Orbit-Stabilizer Theorem) *If G acts on a set X. Then for each $x \in X$ we have*

$$|Gx| = [G : Stab_G(x)]$$

Definition 6.3 (Centralizer)**.** Suppose $A \subset G$ is a subset (not necessarily subgroup). Then the *centralizer* of A in G is

$$C_G(A) = \{g \in G : ga = ag \text{ for every } a \in A\}$$

If $A = G$ then we call $C_G(G)$ the *center* of G. The centralizer is also sometimes denoted $Z(A)$.

Example 6.2. The centralizer of ρ in the triangle group (the group of rigid motions on an equilateral triangle) is $\{1, \rho, \rho^2\}$. The center of the triangle group is simply $\{e\}$. ■

Clearly G is abelian if and only if its center is G itself. We will return to these subgroups (and their cousins) later but first let us discuss the group of rigid motions of an n-gon a bit more.

7 Dihedral group

Consider the regular n-gon with $n \geq 3$ and consider how many rigid motion symmetries it has. Clear there are n rotations since we can rotate by $\frac{2pik}{n}$ for $k = 0, \ldots, n-1$ in the clockwise direction, say. There are also n reflections. If n is odd then each reflection is through the line from a vertex to the midpoint of the opposite edge (this passes through the center of the polygon). This results in n reflections. If n is even then there are $\frac{n}{2}$ reflections that are through opposing vertices and $\frac{n}{2}$ reflections that are through midpoints of opposing sides. We still have n reflections. Thus the order of such a group is always $2n$ (one can check that there can not be any more than $2n$ symmetries since any rigid motion is determined by where a pair of adjacent vertices is sent).

Suppose ρ is a clockwise rotation through $\frac{2\pi}{n}$ and σ is a reflection that fixes vertex v. Then one can check that $\rho\sigma = \sigma\rho^{-1}$. This means we can describe every reflection by composing a rotation with some fixed reflection. In particular then, we get the following proposition.

Proposition 7.1 *Suppose ρ The symmetries of the n-gon are*

$$\{1, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}$$

where ρ is a rotation by $\frac{2\pi}{n}$ and σ is a reflection through the symmetry line passing through some fixed vertex.

Definition 7.2 (Dihedral group)**.** The group of symmetries of the regular n-gon (for $n \geq 3$) is called the *dihedral group* and is often denoted D_{2n}.

8 Quotient Groups

Let G be a group and $H \leq G$ a subgroup. Then let G/H (read "G mod H") denote the set of left cosets $\{gH : g \in G\}$ and $H\backslash G$ (also read "G mod H") denote the set of right cosets. The question we want to ask is whether we can make (either of) these sets of coset a group in some natural manner. For this of course, we would need to define a group operation. The most natural multiplication

would be to simply multiply representatives of each coset (i.e define $Hg \cdot Hg' := Hgg'$). As usual though, we need to check whether or not this is well-defined (as we will see it is only well-define in some cases).

Suppose we have that for $h, h' \in H$ and $g, g' \in G$ we can find some $h'' \in H$ so that

$$hg \cdot h'g' = h''gg'$$

Then

$$hgh'g' = hgh(g^{-1}g)g' = (hgh'g^{-1})gg'$$

We want to say that $h'' = hgh'g^{-1}$ but don't know that it is an element of H. It would be in the subgroup if $gh'g^{-1}$ were an element of H. Sometimes this is the case and sometimes it is not. This motivates the following definition.

Definition 8.1 (Normal Subgroup)**.** A subgroup $H \leq G$ is *normal* if ghg^{-1} is an element of H for any $g \in G$ and $h \in H$. We often write this as $gHg^{-1} = H$. If H is a normal subgroup of G, we write $H \trianglelefteq G$. Moreover we call the group G/H, the *quotient group* (of G by H).

Remark 8.2. Note that if $gHg^{-1} = H$ then $gH = Hg$. Thus if H is a normal subgroup then the left and right cosets are the same.

9 Group Homomorphisms

Definition 9.1 (Homomorphism)**.** Suppose G, K are groups. Then a map $\phi : G \to K$ is a homomorphism if

$$\phi(gg') = \phi(g)\phi(g')$$

for every $g, g' \in G$.

Remark 9.2. Note the multiplication of gg' is in G while the multiplication of $\phi(g)\phi(g')$ is in K.

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

$$\phi(g) = \phi(eg) = \phi(e)\phi(g)$$

implying that $\phi(e)$ is the identity element (in K). Moreover

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

which means that $\phi(g^{-1}) = \phi(g)^{-1}$. Thus by requiring a map to respect the binary operation in a group, we see this automatically means it respects the identity element(s) and inversion.

Example 9.1. The map $\phi : \mathbb{Z} \to \mathbb{Z}, \phi(n) = 2n$ is a homomorphism. ■

Example 9.2. The map $\phi : \mathbb{Z} \to \mathbb{R}, \phi(n) = n$ is a homomorphism. ■

Example 9.3. If V, W are vector spaces then a linear transformation from V to W is a homomorphism (the operation being addition of vectors). ■

There are some homomorphisms that can be defined for general groups. If G is a group then we can choose some $g_0 \in G$ and define

$$\begin{aligned} C_{g_0} : G &\to G \\ g &\mapsto g_0 g g_0^{-1} \end{aligned}$$

In this case C_{g_0} is a homomorphism since

$$C_{g_0}(gh) = g_0(gh)g_0^{-1} = g_0g(g_0^{-1}g_0)hg_0^{-1} = C_{g_0}(g)C_{g_0}(h)$$

The inversion map $\phi : G \to G, \phi(g) = g^{-1}$ is a homomorphism if and only if G is abelian. The same is true for the map $\phi(g) = g^2$.

Given a homomorphism between groups we can define special subsets as we do in the linear algebra case.

Definition 9.3 (Kernel & Image)**.** Suppose $\phi : G \to K$ is a homomorphism. Then the *kernel* of ϕ is

$$\ker(\phi) := \{g \in G : \phi(g) = e\}$$

and the *image* of ϕ is

$$\mathrm{Im}(\phi) := \{\phi(g) : g \in G\}$$

Example 9.4. If $\phi : \mathbb{Z} \to \mathbb{Z}$ with $\phi(n) = 2n$ then $\ker(\phi) = \{0\}$ and $\mathrm{Im}(\phi) = 2\mathbb{Z}$. ■

Example 9.5. If $\phi : \mathbb{Z} \to \mathbb{R}$ with $\phi(n) = n$ then $\ker(\phi) = \{0\}$ and $\mathrm{Im}(\phi) = \mathbb{Z}$ (as a subset of $\mathbb{R}$). ■

Example 9.6. If G is a group, then C_{g_0} has trivial kernel is onto for every g_0. ■

Theorem 9.4 *If $\phi : G \to K$ is a homomorphism, then $\ker(\phi)$ and $\mathrm{Im}(\phi)$ are subgroups.*

Proof. We know that the identity element is always in the kernel and image so both subsets are always non-empty. Suppose $g, h \in \ker(\phi)$. Then

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

Therefore $gh \in \ker(\phi)$. Moreover since $\phi(g^{-1}) = \phi(g)^{-1}$ we see that the kernel is closed under inversion. Therefore the kernel is a subgroup. Similar calculations hold for the image. □

In fact we can make a slightly stronger statement about the kernel of a homomorphism.

Proposition 9.5 *Suppose $\phi : G \to K$ is a homomorphism. Then $\ker(\phi)$ is a normal subgroup of G.*

Proof. Suppose $k \in \ker(\phi)$ and g is any element of G. Then

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e$$

Therefore $gkg^{-1} \in \ker(\phi)$ as desired. □

Speaking of normal subgroups, we should revisit them briefly to describe a homomorphism we can create from them.

Proposition 9.6 *Suppose $N \trianglelefteq G$. Then the map $\phi : G \to G/N, \phi(g) = Ng$ is a homomorphism.*

Proof. We see that

$$\phi(g)\phi(g') = Ng \cdot Ng' = Ngg' = \phi(gg')$$

where the second last equality holds by definition of the operation on the quotient group. □

Definition 9.7. The map $g \mapsto Ng$ where N is a normal subgroup of a group G is called the *(natural) projection* (of G onto G/N). It is often denoted $\mathrm{proj}_{G/N}$ or $\pi_{G/N}$

Since the projection map is onto, its image is G/N. Its kernel is N. In order to see this, we need to find what elements in G are mapped to N (which is of course the identity element in G/N) by the projection map. But since cosets are either equal or disjoint, it can only be elements in N that are mapped to the coset N.

10 Group Isomorphisms

Suppose $\phi : G \to H$ is a homomorphism and $\ker(\phi)$ is trivial (in other words is just the identity). Then it is easy to that ϕ is injective. Suppose $\phi(g) = \phi(g')$. Then $\phi(g^{-1}g') = e$. By triviality of the kernel we conclude that $g^{-1}g' = e$ so $g^{-1} = g'$. If $\mathrm{Im}(\phi) = H$, then ϕ is onto or surjective. If ϕ is both injective and surjective then we know from basic set theory that ϕ is bijective and hence has an inverse ϕ^{-1}. It is easy to see that if ϕ is a homomorphism then so is ϕ^{-1}. Suppose $x = \phi(a)$ and $y = \phi(b)$. Then

$$\phi^{-1}(xy) = ab = \phi^{-1}(x)\phi^{-1}(y)$$

In this case, we call ϕ an isomorphism.

Definition 10.1 (Isomorphism)**.** A bijective group homomorphism is called an isomorphism.

From a group theoretic perspective, isomorphic groups are basically 'the same' and a large part of the subject is classify groups up to isomorphism. One of the greatest mathematical achievements of the last century, involving hundreds of mathematicians, was the classification of all simple groups (groups which only have trivial normal subgroups).

Suppose we have an injective homomorphism ϕ. We can 'force' it to be surjective by considering it as a map onto the image of ϕ (which recall is a subgroup of the co-domain). Here we say that $\phi : G \to H$ is an isomorphism *into* H.

Definition 10.2 (Automorphism)**.** Given a group G, an *automorphism* of G is an isomorphism ϕ from G to itself. The set of all automorphisms on a group forms a group in its own right with the operation of composition. This group is denoted $\mathrm{Aut}(G)$ is called the *automorphism group* of G.

Example 10.1. If $G = \mathbb{Z}$ then the map $n \to -n$ is an automorphism (in fact it is the only one besides the identity). More generally, given any abelian group G, the inversion map $g \mapsto g^{-1}$ is an automorphism. ■

Example 10.2. Suppose $\mathbb{F}$ is a field. Then taking $G = GL(n, \mathbb{F})$ the *transpose inverse* map $g \mapsto (g^{-1})^T$ is an automorphism (switching the order of inversion and transpose produces the same map). ■

Example 10.3. Given some element g_0 in a group G, the conjugation map C_{g_0} is an automorphism of G. ■

In fact the last example forms an important class of automorphisms, important enough to be given a name.

Definition 10.3 (Inner automorphism)**.** The so-called *inner automorphisms* of G are automorphisms that are given by conjugation. In other words,

$$\mathrm{Inn}(G) := \{\phi \in \mathrm{Aut}(G) : \phi = C_g \text{ for some } g \in G\}$$

An element of $\mathrm{Aut}(G)$ that is not an inner automorphism is called an *outer automorphism.*

If G is abeliean then $\mathrm{Inn}(G)$ is clearly trivial. In general, we have the following chain

$$\{\mathrm{id}_G\} \leq \mathrm{Inn}(G) \leq \mathrm{Aut}(G)$$

The containment can be strict or not anywhere.

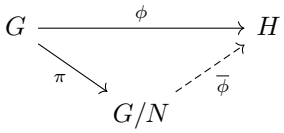
The map $G \to \mathrm{Aut}(G)$ given by $g \mapsto C_g$ is (perhaps unsurprisingly) a homomorphism. Its image is $\mathrm{Inn}(G)$ and its kernel is $Z(G)$.

10.1 Isomorphism Theorems

When given a surjective map, we often call the preimage of a single point its *fibre*. This terminology is common in differential geometry and such.

Suppose G is a group and N is a normal subgroup. Then we know the projection map $\pi : G \to G/N$ is a homomorphism. Its fibres are the cosets of N. In this case the fibres are all the same size (in terms of cardinality) although in general this need not be the case.

Let $\phi : G \to H$ be a homomorphism. Take $N = \ker(\phi)$ which we know is a normal subgroup. Note in this case the fibres of ϕ are the cosets G/N (if $\phi(g) = \phi(g')$ then $\phi(g^{-1}g') = e$ thus $g^{-1}g' \in N$ implying that $g' \in gN$). Note that each coset in G/N is mapped to a unique point in H (this is because elements in a coset only different by a point in the kernel). Thus we get the following diagram



The map $\overline{\phi}$ is the induced map which is given by evaluating ϕ at any point in a given coset (since they all map to the same point this is well-defined). In fact, this map is even a homomorphism:

$$\overline{\phi}(gN \cdot hN) = \overline{\phi}(ghN) = \phi(gh) = \phi(g)\phi(h) = \overline{\phi}(gN)\overline{\phi}(hN)$$

In fact, this map is even injective since the kernel of $\overline{\phi}$ is just $\{gN \in G/N : \phi(g) = e\} = \ker(\phi) = N$.

Theorem 10.4 (First Isomorphism Theorem) *Suppose $\phi : G \to H$ is a homomorphism. Take $N = \ker(\phi)$. Then there is an induced homomorphism $\overline{\phi} : G/N \to H$ such that $\overline{\phi} \circ \pi = \phi$ (we say 'ϕ factors through the quotient'). Moreover, $\overline{\phi} : G/N \to Im(\phi)$ is an isomorphism.*

Although quite simple, the first isomorphism theorem is quite powerful and useful. In fact we can use it to prove the other isomorphism theorems.

Before stating (and proving) the second isomorphism theorem. There are a few facts we need to be aware of.

Definition 10.5. Suppose H is a subgroup of G. Then

$$Norm_G(H) = \{g \in G : gHg^{-1} \subset H\}$$

is called the *normalizer* of H.

Although we require that $gHg^{-1} \subset H$ we in fact have equality since $g^{-1}Hg$ acts as an inverse implying that the map is a bijection. It is also easy to check that the $Norm_G(H)$ is a subgroup of G. Closure under products is clear and we see that if $ghg^{-1} = h' \in H$ then $g^{-1}h'g = g$ for all $g \in Norm_G(H)$ and $h \in H$. Also note that $H \leq Norm_G(H)$ (since H is a subgroup). Hence we may think of the normalizer of H as the largest subgroup of G in which H is normal. Then we have the following fact.

Lemma 10.6 *Let H, N be subgroups of G such that $H \leq Norm_G(N)$. Then $HN := \{hn : h \in H, n \in N\}$ is a subgroup of G and $N \trianglelefteq HN$.*

Proof. PS3, Q2 □

With this we can state the second isomorphism theorem.

Theorem 10.7 (Second Isomorphism Theorem) *Let H, N be subgroups of G such that $H \leq Norm_G(N)$. Then*

$$HN/N \cong H/(H \cap N)$$

Proof. We will use the first isomorphism theorem to prove the statement. In other words, we need to construct a map $\phi : H \to HN/N$ with a kernel $H \cap N$. We will use the obvious map by defining $\phi(h) = hN$ and hope it works.

First we want to check that ϕ is indeed a homomorphism. Note that

$$\phi(h)\phi(h') = hN \cdot h'N = hh'N = \phi(hh')$$

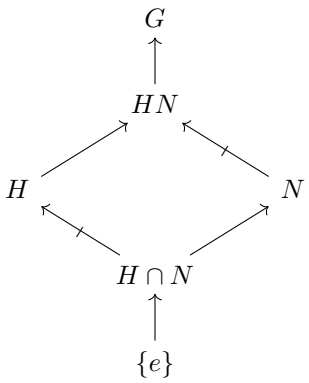
where the penultimate equality holds by definition of multiplication of cosets (see Section 8). Next we find its kernel. Suppose $\phi(h) = e_{HN/N} = N$ for some h. This means that $hN = N$. But this can only occur if $h \in N$. Obviously $h \in H$ implying that $h \in H \cap N$. This means that $\ker(\phi) \subset H \cap N$. The reverse inclusion is clear since anything in N is sent to the trivial coset N by ϕ. Thus we conclude that $\ker(\phi) = H \cap N$ (note this also immediately shows that $H \cap N$ is normal).

Let us now find the image of ϕ. An element of HN/N is of then form hnN but this is the same as hN. Therefore by the first isomorphism theorem, we can conclude that

$$H/(H \cap N) \cong HN/N$$

□

A nice way of visualising this theorem is by thinking about the following diagram



Each arrow represents a subgroup relation and the marked arrows are normal subgroup relations. The second isomorphism theorem then says that the two possible quotients in this diagram are isomorphic.

There is, of course, a third isomorphism theorem (they always say that good things come in threes).

Theorem 10.8 (Third Isomorphism Theorem) *Suppose H, N are normal subgroups of G such that $N \leq H$. Then*

$$G/H \cong G/N \Big/ H/N$$

Proof. If N is a normal subgroup of G and a subgroup of H, then it must be a normal subgroup of H as well (elements of H are elements of G so N remains invariant under conjugation by elements of H). Moreover, if H is normal in G then H/N is normal in G/N. Let us check this quickly.

$$(gN)(hN)(gN)^{-1} = gN \cdot hN \cdot g^{-1}N = (ghg^{-1})N$$

So, at the very least objects in the statement make sense.

In order to prove the statement we will, as before, use the first isomorphism theorem. Once again then, we need a homomorphism from G to $G/N \Big/ H/N$. We will (again) use the 'obvious' map although it looks a bit more complicated this time. We define $\phi(g) = gN \cdot H/N$. One can think of ϕ as the composition of the projection onto G/N with the projection onto $G/N \Big/ H/N$. This immediately tells us that ϕ is a surjective homomorphism. All that remains to do is find the kernel of ϕ.

Suppose $\phi(g) = gN(H/N) = H/N$ for some $g \in G$. This means that $gN \in H/N$. But H/N is just the group of cosets of N in H. So if the coset gN is in H/N then g must be an element of H. Therefore $\ker(\phi) = H$ as desired. Hence by the first isomorphism theorem, we conclude that

$$G/H \cong G/N \Big/ H/N$$

□

Before we move on to the fourth isomorphism theorem (of course there is a fourth isomorphism theorem), let's look at a few examples of applying the previous theorems.

First consider $G = \mathbb{Z}$, $H = 3\mathbb{Z}$ and $K = 4\mathbb{Z}$. Note that $H \cap K = 12\mathbb{Z}$. Note that all subgroups are normal since the group is abelian. Then by the second isomorphism theorem, we can conclude that

$$\mathbb{Z}/3\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$$

or

$$\mathbb{Z}/4\mathbb{Z} \cong 3\mathbb{Z}/12\mathbb{Z}$$

As a slightly more interesting example, consider $G = \mathbb{R}/\mathbb{Z}$. In this $[0, 1)$ forms a set of representatives for G (given a real number r we add or subtract integers until it lies in the above interval). Thinking visually (and topologically), we see that points close to 1 are also close to 0. We can show this by gluing the endpoints of the interval together and forming a circle. So we would like to say that $\mathbb{R}/\mathbb{Z} \cong S^1$. Unfortunately we are using topological arguments which don't quite work in the correct setting of abstract groups. Luckily in this case, we can use the first isomorphism theorem to do the work for us.

We define the homomorphism $\phi : \mathbb{R} \to \mathbb{C}^\times, \phi(t) = e^{2\pi i t}$. It's clear that this is indeed a homomorphism by property of exponentials. Moreover, the image of the map is the unit circle S^1 and its kernel is $\mathbb{Z}$. Thus we can use our beloved theorem to conclude that

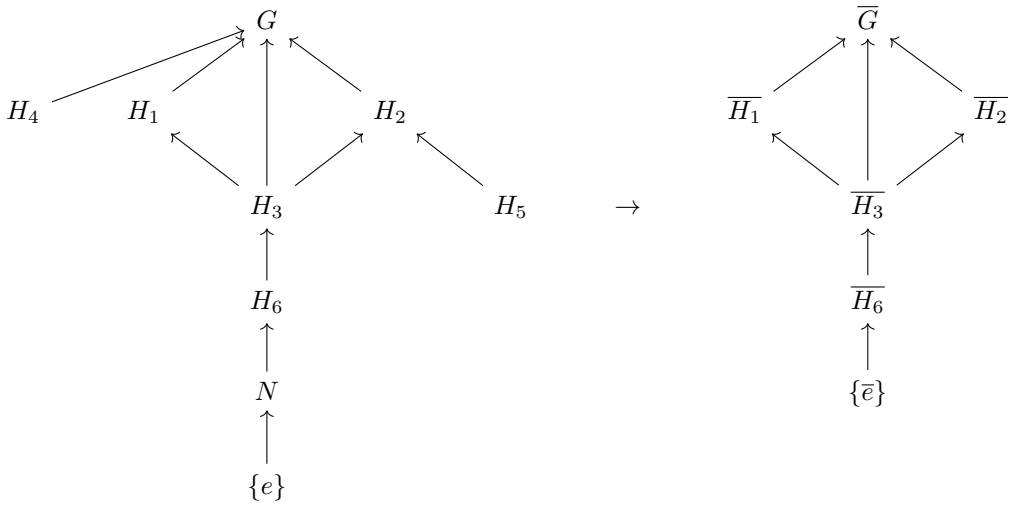
$$\mathbb{R}/\mathbb{Z} \cong S^1$$

Remark 10.9. Topological groups are a (very important) thing. These are groups where the underlying set has a topology in which the binary operation and inversion map are continuous.

We can further extend the previous example by considering $\mathbb{R}^2/\mathbb{Z}^2$. In this case the set of repesentatives is given by the square $[0, 1) \times [0, 1)$ where opposite edges are glued together. Gluing the pair of edges together forms a cylinder and gluing the ends of the cylinder gets us the torus. Therefore we conclude that $\mathbb{R}^2/\mathbb{Z}^2$ is isomorphic to the torus. We will see a purely group-theoretic proof of this fact (without using topological arguments) later.

The above diagrams showing the relationships between subgroups is an example of a subgroup lattice. The fourth isomorphism theorem, also known as the lattice isomorphism theorem, tells us that that the lattice of subgroups of group G is the same as the lattice of subgroups of G/N (ignoring all the subgroups of G that don't contain N). Below we see an example of a lattice diagram and its

result after modding out N where we use the notation $\overline{H} := H/N$



We state the theorem precisely here.

Theorem 10.10 (Fourth Isomorphism Theorem or Lattice Isomorphism Theorem) *Let G be a group and N a normal subgroup of G. Then the subgroup lattice of $G/N := \overline{G}$ has the same structure as the part of the subgroup lattice of G that contains N. In particular any subgroup $\overline{H}$ of $\overline{G}$ is of the form H/N for some $H \leq G$. Moreover, if H, K are any subgroups of G containing N then*

$$H \leq K \Leftrightarrow \overline{H} \leq \overline{K}$$
$$H \trianglelefteq K \Leftrightarrow \overline{H} \trianglelefteq \overline{K}$$
$$[H : K] = [\overline{H} : \overline{K}]$$
$$\overline{H \cap K} = \overline{H} \cap \overline{K}$$
$$\langle H, K \rangle = \langle \overline{H}, \overline{K} \rangle$$

Proof. It is clear that if $N \leq H \leq G$ then $H/N \leq G/N$ since $hN \cdot h'N = hh'N \in H/N$. Similarly $(hN)^{-1} = h^{-1}N \in H/N$.

Conversely suppose $\overline{H} \leq \overline{G}$. We want to show that $\overline{H} = H/N$ for some $H \leq G$. We want to say then $H := \pi_{G/N}^{-1}(\overline{H})$ (in other words the preimage of the projection map). We only need show that this is indeed a subgroup. The non-emptiness of H is clear (projections are always onto). Let $h, h' \in H$. Note that $\overline{H} = \{hN : h \in H\}$. Since $\overline{H}$ is a subgroup, we have $hN \cdot h'N = hh'N \in \overline{H}$. Therefore $hh' \in H$. Similarly since $(hN)^{-1} = h^{-1}N \in \overline{H}$ we must have $h^{-1} \in H$. □

11 Products

Suppose G, G' are groups. Then we can define

$$G \times G' = \{(g, g') : g \in G, g' \in G'\}$$

as usual. Moreover, we can define a group operation on it

$$(g, g') \cdot (h, h') := (gh, g'h')$$

The identity in this case is $\{(e_G, e_{G'}\}$ and $(g, g')^{-1}) = (g^{-1}, (g')^{-1})$.

Given $G \times G'$, consider the subset $G_0 := \{(g, e) : g \in G\}$. It is clear that this is a subgroup of $G \times G'$ that is isomorphic to G. Similarly we could define $G_0' := \{(e, g') : g' \in G'\}$ which is isomorphic to G'. It is easy to see that G_0 and G_0' are normal subgroups of the product and that

$$(G \times G')/G_0 \cong G'$$

We can show this concretely by using (as usual) the first isomorphism theorem on the homomorphism $\phi : G \times G' \to G'$ with $\phi(g, g') = g'$.

12 Symmetric Groups

The initial study of groups began by studying only subgroups of symmetric groups. In fact this is not quite as restricitive as it seems since we will find that any finite subgroup is isomorphic to a subgroup of a symmetric group. Before we see this, we need to know what symmetric groups are.

Definition 12.1 (Symmetric Groups)**.** The symmetric group of n objects, denoted S_n, is the set of all permutations on $\{1, \ldots, n\}$. In other words,

$$S_n := \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} | \sigma \text{ is a bijection}\}$$

Elements of S_n are called permutations.

It is easy to see that $|S_n| = n!$ (this include the trivial permutation or the identity map). The group operation is composition (of functions).

A *cycle* is a permutation that 'cycles through' some subset of $\{1, \ldots, n\}$. To be precise, for a k-cycle, or a cycle of length k, you have distinct elements $a_1, \ldots, a_k \in \{1, \ldots, n\}$ where $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{k-1} \mapsto a_k, a_k \mapsto a_1$. We often write this as

$$(a_1\, a_2\, \ldots\, a_k)$$

In principle, you can start the cycle anywhere so we could have written the above cycle as $(a_2\, a_3\, \ldots\, a_k\, a_1)$. In order to remove this ambiguity we almost always choose the first element in the cycle to be the smallest one. Consider the following permutation in S_6

$$\begin{aligned} 1 &\mapsto 3 \quad 4 \mapsto 5 \\ 2 &\mapsto 2 \quad 5 \mapsto 4 \\ 3 &\mapsto 6 \quad 6 \mapsto 1 \end{aligned}$$

We could write this permutation in cycle notation as

$$(1\ 3\ 6)(2)(4\ 5)$$

Actually by convention 1-cycles are often omitted so more typically one would see this as

$$(1\ 3\ 6)(4\ 5)$$

You can think of this as the product or composition of 2 permutations. The first one permutes $1, 3, 6$ and leaves the rest alone while the second one simply permutes 4 and 5 and fixes everything else. Thus it is easy to see that disjoint cycles commute (the above is equal to $(4\ 5)(1\ 3\ 6)$). In order to still have a unique decomposition, another common convention is to order disjoint cycles by the first element of the cycles.

It is easy to find the inverse of permutations when written as the product of disjoint cycles. Using the above permutation again we see that

$$((1\ 3\ 6)(4\ 5))^{-1} = (4\ 5)^{-1}(1\ 3\ 6)^{-1} = (4\ 5)(1\ 6\ 3) = (1\ 6\ 3)(4\ 5)$$

Even given a product of non-disjoint cycles, we can decompose it to disjoint cycles.

$$(1\ 4\ 2)(2\ 3\ 5)(3\ 4\ 7) = (1\ 4\ 7\ 5)(2\ 3)$$

We compute this by thinking of the three cycles as permutations/functions (any numbers that don't appear in the cycle are fixed). Below we see some examples

$$\begin{aligned}
1 &\overset{(3\,4\,7)}{\mapsto} 1 \overset{(2\,3\,5)}{\mapsto} 1 \overset{(1\,4\,2)}{\mapsto} 4\\
4 &\overset{(3\,4\,7)}{\mapsto} 7 \overset{(2\,3\,5)}{\mapsto} 7 \overset{(1\,4\,2)}{\mapsto} 7\\
7 &\overset{(3\,4\,7)}{\mapsto} 3 \overset{(2\,3\,5)}{\mapsto} 5 \overset{(1\,4\,2)}{\mapsto} 5\\
5 &\overset{(3\,4\,7)}{\mapsto} 5 \overset{(2\,3\,5)}{\mapsto} 2 \overset{(1\,4\,2)}{\mapsto} 1
\end{aligned}$$

We can also kind of go in reverse. Namely, given a k-cycle we can write it as the product of $k-1$ 2-cycles. For example

$$(a\ b\ c\ d) = (a\ d)(a\ c)(a\ b)$$

Obviously these 2-cycles, also called transpositions, will very rarely be disjoint. Since any cycle can be written as the product of 2-cycles and any permutation can be written as a product of cycles, we conclude that any element of S_n can be written as the product of 2-cycles. Another way of saying this is that the 2-cycles generate S_n.

12.1 Sign of a permutation

A natural question whether there is a unique decomposition of cycles into 2-cycles. We can immediately see that this is not true since we could, for example, write the above cycle as

$$(a\ d)(a\ c)(a\ b)(a\ c)(a\ c)$$

We might instead then ask about the minimum number of transpositions required but as it turns the more useful quantity will be the parity (whether a number is even or odd) of the number of transpositions in the decomposition.

Lemma 12.2 *The parity of the number of transpositions in the decomposition of a permutation is invariant.*

Proof. First we define the quantity

$$\Delta := \prod_{1\le i<j\le n} (j-i)$$

Given $\tau \in S_n$, it acts on Δ by

$$\tau\cdot\Delta = \prod_{1\le i<j\le n} (\tau(i)-\tau(j))$$

Note that since τ is a bijection the two products are equal, up to possibly a change of sign. In particular you multiply by -1 for each pair $i<j$ for which we have $\tau(i)>\tau(j)$.

Let us now consider the case of $\tau = (a\ b)$ for some $1\le a<b\le n$. In particular we are looking for pair $i<j$ where $\tau(i)>\tau(j)$. If neither i nor j is in $\{a,b\}$ then $\tau(i)=i$ and $\tau(j)=j$ so these certainly aren't the pairs we are looking for. This leaves the pairs where at least one of i,j is a or b. Suppose $i<a$. Then $\tau(i)=i<a<b=\tau(a)$. Similarly $\tau(i)<a=\tau(b)$. Therefore pairs of the form (i,a) and (i,b) don't contribute to the sign change. We have the same situation for pairs (a,j) and (b,j) for $j>b$. This only leaves pairs in $\{a,a+1,\dots,b-1,b\}$. Suppose i is strictly between a and b. Then $a<i<b$ while $\tau(i)=i<b=\tau(a)$. Therefore the pair (a,i) contributes a sign flip to $\tau\cdot\Delta$. However the same is true for the pair (i,b). Thus these sign flips come in pairs. The *only* unpaired sign flip comes from (a,b). Since we have an odd number of sign flips we get $\tau\Delta=-\Delta$.

Now let σ be an arbitrary element of S_n. Suppose we write it as the product of k transpositions. Then $\sigma\Delta = (-1)^k\Delta$. Since the left hand side is independent of the transposition decomposition, we see that two transpositions can only differ in length by a multiple of 2 and hence must have the same parity. □

The above lemma tells us the following is well-define.

Definition 12.3. The sign of $\sigma \in S_n$, denoted $\text{sgn}(\sigma)$, is $(-1)^k$ where σ can be written as the product of k transpositions.

Remark 12.4. If σ can be written as the product of an even number of permutations (i.e. $\text{sgn}(\sigma) = 1$) we say σ is even. Otherwise we say σ is odd. Note this has the strange effect that a k-cycle is even if and only if k is odd.

The map sgn in fact has a very important property. Suppose σ can be written as the product of k transpositions and τ can be written as the product of l transpositions. Then $\sigma\tau$ can be written as the product of $k + l$ transpositions. This means that

$$\text{sgn}(\sigma\tau) = (-1)^{k+l} = (-1)^k(-1)^l = \text{sgn}(\sigma)\text{sgn}(\tau)$$

which is to say that $\text{sgn} : S_n \to \{-1, 1\}$ is homomorphism. The kernel of sgn is all the even permutations and is called the alternating group and is denoted A_n. Note that by the first isomorphism theorem $S_n/A_n \cong \{-1, 1\}$ so $[S_n : A_n] = 2$ which means that

$$|A_n| = \frac{n!}{2}$$

One remarkable fact about alternating groups is that for $n \geq 5$, A_n has no (non-trivial) normal subgroup, which is to A_n is simple.

Now, for a brief comment about conjugation. Let σ be a permutation such that $\sigma(a) = b, \sigma(b) = c, \ldots$. Let τ also be a permutation where $\tau(a) = a', \tau(b) = b', \tau(c) = c', \ldots$ and now consider $\tau\sigma\tau^{-1}$.

$$(\tau\sigma\tau^{-1})(a') = \tau\sigma(a) = \tau(b) = b'$$
$$(\tau\sigma\tau^{-1})(b') = \tau\sigma(b) = \tau(c) = c'$$

Therefore conjugation by τ simply has the effect of relabelling σ (it replaces a with a', b with b', c with c' and so on).

13 Composition Series

We often try understand objects in mathematics by looking at the subobjects within it and seeing how they combine. The 'simplest' objects in the context of groups are the simple groups. These are groups that have no subobjects.

Definition 13.1 (Simple Groups)**.** A group G is called *simple* if the only normal subgroups it has are $\{e\}$ and G itself.

The composition series is one way, then, of breaking down a group into these simpler objects and seeing how they are combined.

Definition 13.2 (Composition Series)**.** Let G be a group and $G_1, \ldots, G_{r-1}, G_r := G$ be a chain of subgroups such that each G_i is normal in G_{i+1}. In other words we have

$$G_0 := \{e\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r := G$$

If all the G_{i+1}/G_i are simple for $i = 0, \ldots, r-1$ then this chain is called a *composition series* or *Jordan-Hölder* series. Moreover the quotients G_i/G_{i+1} are called the composition factors.

Unfortunately the decomposition is not entirely unique. The same group may have different composition series. However, the following theorem gives us a strong restriction for how much the decompositions can vary.

Theorem 13.3 (Jordan-Hölder) *Any two composition series for G have the same length. Moreover the set of composition factors are the same (but perhaps in different orders).*

TBD. □

Let us consider an example which illustrates how one may be inspired to conjecture the above result. Let H, K be normal subgroups of G. Then we may have the following composition series

$$\{e\} \triangleleft H \cap K \triangleleft H \triangleleft HK \triangleleft G$$
$$\{e\} \triangleleft H \cap K \triangleleft K \triangleleft HK \triangleleft G$$

Note that $H \subset Norm_G(K) = G$ and $K \subset Norm_G(H) = G$. Therefore by the second isomorphism theorem, we have $HK/K \cong H/(H \cap K)$ and $HK/H \cong K/(H \cap K)$. Therefore even if the terms of the series are different, the composition factors are the same.

Every group has a Jordan-Hölder series but in general G is not determined by this series. One exception to is are the simply groups since there composition series is simply $\{e\} \triangleleft G$. As we will prove later, A_5 is the smallest non-abelian simple group.

Definition 13.4 (Solvable Groups)**.** If the composition factors of a group G are all abelian then G is said to be *solvable*.

14 More on Actions

Suppose G acts on a set X. Then each $g \in G$ permutes the elements of X. To be precise, the map given by $x \mapsto gx$ is bijection on X. This is easily seen by noting that its inverse is $x \mapsto g^{-1}x$. Therefore there is a map $G \to S_X$ where we use S_X to denote the set of bijections on X. In fact the properties of group actions ensure that this map is a homomorphism.

Suppose G is a group and H is any subgroup of it (not necessarily). Then although $X := G/H$ may not be a group, it certainly does form a set, namely the set of left cosets of H. Then G acts on X by $g(xH) = (gx)H$. If $n = [G : H] = |X|$, then we have a homomorphism $\phi : G \to S_n$.

Remark 14.1. Note G acts transitively, which is to say any xH can be mapped to any yH by choosing an appropriate g (in this case that would yx^{-1}).

Then we may ask what is the kernel of ϕ. In other words we are looking for $g \in G$ so that

$$gxH = xH$$

for all $x \in G$. We see

$$gxh = xh' \Leftrightarrow g = xh'h^{-1}x^{-1}$$

Therefore g must be in xHx^{-1}. Since this needs to hold for all x we see that the kernel is

$$\ker(\phi) = \bigcap_{x \in G} xHx^{-1}$$

We know this must be a normal subgroup of G since it is the kernel of a homomorphism but let us verify this directly.

We could equivalently describe $\ker(\phi)$ as the set of all $g \in G$ such that $xgx^{-1} \in H$ for all $x \in G$. Suppose $g, h \in \ker(\phi)$ and $x \in G$ arbitrary. Note that $xg^{-1}x^{-1} = (xgx^{-1})^{-1}$. Since we know $xgx^{-1} \in H$ and H is a subgroup then $xg^{-1}x^{-1} \in H$ as well. Therefore $g^{-1} \in \ker(\phi)$. Similarly we wish to show that $gh \in \ker(\phi)$. Note that $xghx^{-1} = (xgx^{-1})(xhx^{-1})$. We know that xgx^{-1} and xhx^{-1} are in H so their product must be in H as well. Finally in order to show $\ker(\phi)$ is normal we verify that $xgx^{-1} \in \ker(\phi)$. Let y be any element of G. Then $y(xgx^{-1})y^{-1} = (yx)g(yx)^{-1}$. Since we know that $g \in \ker(\phi)$ this means that $xgx^{-1} \in \ker(\phi)$.

In fact $\ker(\phi)$ is the largest normal subgroup contained in H. In order to see that $\ker(\phi)$ is in H recall that it consists of g that can be written in the form xhx^{-1} for all $x \in G$ and some $h \in H$. Since this holds for all x we can in particular consider what happens when $x \in H$; it forces $g = xhx^{-1}$ to also be in H. Therefore $\ker(\phi) \leq H$. Now suppose N is any normal subgroup in H. Then we know that $xNx^{-1} \leq xHx^{-1}$ for all x. Therefore $xNx^{-1} = N \leq \ker(\phi)$.

Theorem 14.2 (Cayley's Theorem) *Every group G is isomorphic to some subgroup of a symmetric group.*

Proof. Let G be a group and take $H = \{e\}$. Consider the homomorphism from G to $S_{G/H} = S_G$ (since H is trivial $G/H \cong G$). Then we know the kernel of this homomorphism is contained in H and is therefore trivial. By the first isomorphism theorem then, G is isomorphic to $\phi(G) \leq S_G$.

The above can be thought of equivalently as G acting on itself by left multiplication. The conditions for being a group guarantee that this action is a bijection on G and hence is an element of S_G. □

15 Conjugacy Classes

For the previous theorem, we used that G acts on itself by left multiplication. This is of course not the only way that a group can act on itself. Another, arguably more important action, is conjugation. Namely, we map $g \mapsto C_g$ where we define $C_g(h) = ghg^{-1}$ for $h \in G$. Note that this action is *not* transitive. Therefore there may be more than one orbit leading to a more interesting decomposition.

Definition 15.1 (Conjugacy classes)**.** The orbits of an element $x \in G$ under the action of conjugation are called *conjugacy classes.*

By definition we know that the orbit of x is $\{C_g(x) : g \in G\}$ which we can write more simply as $\{gxg^{-1} : g \in G\}$. Therefore conjugacy classes of x can also be thought of as the set of elements conjugate to x. This makes it particularly easy to see that conjugacy classes form an equivalence relation and hence the conjugacy classes partition G.

Remark 15.2. The partitions are no longer cosets and therefore need not be of the same size.

15.1 Class Equation

Suppose z is an element of the center $Z(G)$. Then $gzg^{-1} = gg^{-1}z = z$ for all $g \in G$. Therefore each element in the center forms its own conjugacy class. Let $g_1, \ldots, g_m$ be representatives of the non-central conjugacy classes. Then, because conjugacy classes partition G, we can write

$$G = Z(G) \dot{\cup} \dot{\bigcup}_{i=1}^{m} C(g_i)$$

where $C(g_i)$ is the conjugacy class of g_i. Note we are using the fact that each element of the center has a conjugacy class which is a singleton. Therefore the union of all such classes simply produces the center $Z(G)$ again. Since all the unions are disjoint we can write

$$|G| = |Z(G)| + \sum_{i=1}^{m} |C(g_i)|$$

This is known as the *class equation*. By recalling the Orbit-Stabilizer theorem (see Theorem 6.2), we know that $|C(g_i)| = [G : Stab_G(g_i)]$. Consider what the stabiliser of g_i is in the context of conjugation. This would be set of elements $g \in G$ such that $gg_ig^{-1} = g_i$. This is simply the centralizer of g_i. Therefore we can rewrite the class equation as

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(g_i)]$$

which is often easier to compute.

Let us try an example. Suppose we take $G = S_3$. In this case there 3 conjugacy classes: $\{e\}$, 2-cycles and 3-cycles. Within the symmetric groups, the conjugacy classes are easy to identify since they simply correspond to different cycle types (the end of Section 12 demonstrates that given two cycles σ, σ' of the same cycle type we can construct τ so that $\tau\sigma\tau^{-1} = \sigma'$ since conjugation in this case is simply a relabeling of the elements. Moreover, it clear that permutations of different cycles types cannot be conjugate).

Remark 15.3. Cycle type is more or less what the permutation looks like after its been decomposed into disjoint cycles. Therefore $(a\ b), (a\ b)(c\ d)$ and $(a\ b\ c\ d)$ are all of different types.

15.2 Application of Class Equation

In order to use the class equation, we first find the center of S_3. It is easy to see that this is just the identity. Next we need a representative from each of the remaining conjugacy classes. From the 2 cycles we can choose $(1\ 2)$. Then we compute that $C_G((1\ 2)) = \{e, (1\ 2)\}$. Therefore $[G : C_G((1\ 2))] = 3$ which is exactly the number of 2-cycles. Similarly we compute $C_G((1\ 2\ 3)) = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ and hence $[G : C_G((1\ 2\ 3))] = 2$ as expected. Therefore by the class equation we find that the order of S_3 is $1 + 2 = 3 = 6$.

This example didn't exactly enlighten us with new information so let us use the class equation to prove a more interesting result.

Definition 15.4 (p-group)**.** Suppose p is a prime number. Then a group G is a *p-group* if $|G| = p^k$ for some natural number k.

Theorem 15.5 *If G is a non-trivial p-group, then it has a non-trivial center.*

Proof. We know that

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(g_i)] \tag{15.1}$$

Suppose $|Z(G)| = 1$. We first claim that $Z(g_i)$ must be a proper subgroup of G. If $Z(g_i) = G$ then g_i would commute with every element of G and hence would be in the center. By Lagrange's theorem we know that $|Z(g_i)|$ divides $|G| = p^k$. Therefore $|Z(g_i)| = p^l$ for some $l < k$ (the l may be different for different g_i. Therefore $[G : Z(g_i)] = p^{k-l}$ is a positive power of p. Therefore each number in the summation on the right hand side of (15.1) is a power of p but since $|Z(G)| = 1$ by assumption we know that the right hand side cannot be divisible by p leading to a contradition (since we know the left hand side definitely *is* divisible by p). □

Corollary 15.6 *Suppose p is prime. If $|G| = p^2$ then G is abelian.*

Proof. We know that $Z(G)$ is not trivial. Since it's a subgroup of G we know that $|Z(G)| = p$ or $|Z(G)| = p^2$. If it is the latter case, we are done. So suppose $|Z(g)| = p$. Since $Z(G)$ is normal we know that $|G/Z(G)| = p$. Note there is only one group (up to isomorphism) of order p, namely the cyclic group (in order to see this take any non-trivial element in the group consider the subgroup generated by the element). Therefore $G/Z(G) \cong C_p$ allowing us to write

$$G/Z(G) = \{e, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{p-1}\}$$

for some $x \notin Z(G)$ where we use the usual convention $\overline{x}$ denotes the coset of $\{x\}$ or $x \cdot Z(G)$ in this case. Note that $\overline{x}^p$ is the identity in $G/Z(G)$ which means that $x^p \in Z(G)$. An important remark here is that the order of $\overline{x}$ being p does not imply that the order of x is also p. In this case we know that the order of x must be p or p^2 (since $\langle x \rangle$ forms a subgroup of G). If the order of x is p^2 then the group is generated by x and is therefore abelian. So suppose the order of x is p. Then

$$G = \bigcup_{k=0}^{p-1} x^k Z(G)$$

(each of $x, \ldots, x^{p-1}$ forms a different representative of the cosets of $Z(G)$). Since $Z(G)$ has prime order it must also be cyclic so we can say $Z(G) = \{e, z, \ldots, z^{p-1}\}$. Therefore we can write

$$G = \{x^i z^j : 0 \leq i, j \leq p-1\}$$

It is clear that this is abelian since the z^j commute with everything. □

To head in a different direction, we will consider rotations of the tetrahedron. We can count them in 2 different ways. First mark one of the vertices of the tetrahedron as the 'top vertex'. Then there are 4 different options for which vertex can be on top. For each of these choices we have 3 rotations that we can do about the vertical axis going through the top vertex. This gives us a total of 12 rotations (including the identity). This makes sense since we can view this group as a subgroup of S_4 where elements of S_4 act on the tetrahedron by rearranging the vertices according to the given permutation (of course many of these won't be rotations, or even rigid motions). Since 12 divides $|S_4| = 24$ the above at least seems reasonable.

A second way of counting the rotations is to consider what a particular rotation must fix. For example, apart from the identity there are 2 rotations that fix any particular vertex. Adding back the identity this gives us $1 + 8 = 9$ of the rotations. This can be a subgroup of S_4 since 9 does not divide 24. The remaining rotations are those that fix, not a vertex, but a pair of them. In cycle notation these would be permutations of the form $(a\ b)(c\ d)$ (notice that if this permutation fixes the pair $\{a, b\}$. There are 3 such rotations (we know a must be 1 by convention so these rotations are entirely determined by the value of b) which results in a total of 12 rotations as expected. Notice that all these rotations are even which shows that rotations of a tetrahedron are exactly A_4. If we consider all rigid motions (i.e. we allow reflections), we obtain all of S_4.

Proposition 15.7 *The group A_5 is simple.*

Proof. We know that A_5 is a subgroup of S_5. Since $|S_5| = 120$ and A_5 has index 2, we know that $|A_5| = 60$.

Let us enumerate the conjugacy classes of S_5.

$(a\ b\ c\ d\ e)$	$(a\ b\ c\ d)$
$(a\ b\ c)$	$(a\ b\ c)(d\ e)$
$(a\ b)(c\ d)$	$(a\ b)$
$\{e\}$	

These are all the conjugacy classes (i.e. cycle types) in S_5. All the cycles in the right column are odd and therefore are not in A_5. An important thing to note here is that conjugacy classes in S_5

might not be the same as conjugacy classes in A_5. In particular, there might be permutations that we can conjugate using elements of S_5 by not by elements of A_5.

We will use count out the conjugacy classes. For example, let us start with the 5-cycles. There are $4! = 24$ 5-cycles. We know by the Orbit-stabilizer theorem (see Theorem 6.2) that the size of a conjugacy class must always divide the order of the group). Since 24 does not divide 60 we can be confident that all the 5-cycles are conjugate to one another in A_5. We see that $\langle(a\ b\ c\ d\ e)\rangle \leq C_{A_5}((a\ b\ c\ d\ e)) \leq C_{S_5}((a\ b\ c\ d\ e))$. It is clear that the last group must simply be powers of the permutation and no more (any other conjugation would produce a different cycle since some elements would necessarily be relabelled). Since the left and right hand side of the chain above are equal, we conclude that $|C_{A_5}((a\ b\ c\ d\ e))| = 5$. Hence $[A_5 : C_{A_5}((a\ b\ c\ d\ e))] = 12$. The remaining 12 5-cycles must form their own conjugacy class. Hence we have 2 conjugacy classes of size 12.

Now we consider the 3-cycles. Notice that there are $\binom{5}{3} \cdot 2 = 20$ of these (we choose 3 elements of the 5 and there are 2 ways of order them in a cycle). And in fact these are conjugate in A_5 since if $(a\ b\ c)$ is conjugate to $(x\ y\ z)$ by σ then it is also conjugate by $\sigma' := \sigma(d\ e)$. One of σ and σ' is in A_5 so we know the cycles are conjugate in A_5.

Finally we count the number of dual transpositions $(a\ b)(c\ d)$. There are $5 \cdot 3 = 15$ of these (we have 5 choices for which element to fix, a is simply the smallest element amount the remaining numbers so the permutation completely determined by the choice of b). Once if there is a conjugation by σ we can multiply σ by a transposition (which uses the fixed point) to form a permutation that produces the same conjugation on the given permutation.

A normal subgroup must be some union of conjugacy classes (otherwise it could not be invariant under conjugation). Therefore the order of a normal subgroup, if it were to exist, would have to be one more than some combination of $12, 12, 20, 15$ (the $1 +$ comes from adding the identity) but none of these combinations produce a factor of 60. □

16 Sylow's Theorems

The Norwegian mathematician Peter Sylow produced a number of remarkable theorems about p-groups that revolutionised the study of finite groups.

Definition 16.1 (Sylow p-subgroups)**.** Suppose $|G| = p^\alpha n$ where p is a prime number that does not divide n and α is a positive integer. Then a subgroup $P \leq G$ is a Sylow p-subgroup if $|P| = p^\alpha$. In other words, a Sylow p-subgroup is a maximal p-subgroup. We will denote the set of Sylow p-subgroups by $\mathrm{Syl}_p(G)$ and define $n_p(G) = \left|\mathrm{Syl}_p(G)\right|$.

Theorem 16.2 (Sylow's Theorems) *Let G be a finite group and p a prime number such that p divides $|G|$. Then*

1. *Sylow p-subgroups exist, i.e. $n_p(G) \neq 0$*
2. *If P is a Sylow p-subgroup and $Q \leq G$ such that $|Q| = p^r$ for some $r > 0$ then there exists some $g \in G$ such that $gQg^{-1} \leq P$. In other words all other p-subgroups are conjugate to subgroups of Sylow p-subgroups and in particular all Sylow p-subgroups are conjugate to one another.*
3. *$n_p(G) \equiv 1 \bmod p$. Moreover, $n_p(G) = [G : Norm_G(P)]$ for any Sylow p-subgroup P. Hence $n_p(G)$ divides $|G|$ and hence must also divide $n := \frac{|G|}{|P|}$.*

It will take considerable effort to prove the above statements. So let us very quickly verify it on a small example. Consider the symmetric group S_3. We know that $|S_3| = 6 = 2 \cdot 3$. Therefore the theorem above tells us that there should be Sylow 2-subgroups and Sylow 3-subgroups. We see that

$$\mathrm{Syl}_2(S_3) = \{e, (1\ 2)\}, \{e, (1\ 3)\}, \{e, (3\ 3)\}$$

Therefore $n_2(S_3) = 3$ which is indeed equivalent to $1 \bmod 2$.

In order to prove the theorem we will first need a few preliminary results.

Lemma 16.3 *If G is abelian and p is a prime number dividing $|G|$ then G contains an element of order p.*

Proof. If $|G| = p$ then we know G is cyclic and hence any non-trivial element has order p. So we can assume $|G| > p$. Suppose there is an element x in G where p divides the order of x. In other words we can write $|x| = p^r m$ where $r > 0$ and $p \nmid m$. Then $x^{p^{r-1}m}$ has order p. Therefore the only remaining case is where p does not divide the order of any element in G.

Suppose this is the case. We inductively assume that the result is true for groups smaller than G (in terms of base case we already know it works if the order of G is exactly a prime number). Since p does not $|x|$ we know that $N := \langle x \rangle$ must be a proper subgroup of G. Moreover since G is abelian, we know it is a normal subgroup. Hence G/N is a smaller group than G and we know that p divides its order. Hence by our inductive hypothesis we know there is some $y := y_0 N \in G/N$ of order p. This means that $y^p = N$ and therefore $y_0^p \in N$. Consider the group generated by y_0^p. This group must be contained in N. Therefore if $\langle y_0 \rangle = \langle y_0^p \rangle$ this would imply that $y_0 \in N$ but we are assuming this is not the case (otherwise $y_0 N = N$ which certainly cannot have order p in G/N). Therefore $\langle y_0^p \rangle$ is a proper subgroup of $\langle y_0 \rangle$. But since y_0^p generates a proper subgroup, it follows that p divides the order of y_0. This contradicts our assumption that p does not divide the order of any element in G. □