Groups *

Zhiyuan Bai

Compiled on December 14, 2020

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part IA course *Groups* in Michaelmas 2019. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

*Based on the lectures under the same name taught by Dr. O. Randal-Williams in Michaelmas 2019.

0 Motivation of Group

Groups are the mathematical notion of symmetries. Indeed, if we go further into this topic, we will find that the symmetries of anything give a group, and any group is actually the symmetry of something. Then why study symmetries in this way? Why do we not just desribing the symmetries one by one instead? Consider a tetrahedron. There are 12 rotational symmetries of it: 1 doing nothing, 8 rotations on an axis joining one of the vertices and the centre of the tetrahedron, and 3 rotations on the axis joining the midpoints of opposite sides. The interesting thing is, if you composite two of the rotations that are listed above, you get another rotation. For example, if we label the vertices as $1, 2, 3, 4$, then one of the rotations on the axis passing though vertex 1 may send the vertices like

$$1 \to 1, 2 \to 4, 3 \to 2, 4 \to 3$$

and the rotation on the axis joining midpoints of opposite segments would permute them by

$$1 \to 3, 2 \to 4, 3 \to 1, 4 \to 2$$

We let R be the former rotation and S be the latter, then we could find $S \circ R$, the rotation given by doing R first then S next. Indeed, this is the permutation

$$1 \to 3, 2 \to 2, 3 \to 4, 4 \to 1$$

which is one of the rotations on the axis passing though 2. Here is an interesting thing: we can do $R \circ S$ as well, but it is, as one can check, a rotation on the axis passing though 4! So $RS \neq SR$, as in the order of the composition of two rotations matters. This is kind of the point of group theory.
Now we can look at the rotational symmetries of another soli: an isocagonal cone. This time it is quite obvious: the rotational symmetries are precisely the rotations on the central axis of degree $n\pi/6$ where $n = 0, 1, 2, \ldots, 11$. Now this set of rotations has order 12 as well. But are the two sets of rotational symmetries, one on a tetrahedron and another on a isocagonal cone, the same? No, our intuition said. But why?

Proposition 0.1. *The groups of rotational symmetries of a tetrahedron and a isocagonal cone are different.*

Proof. Note that every rotation in the tetrahedron group is the same as doing nothing after repeating itself 2 or 3 (so, 6) times. But the rotation of $\pi/6$ degrees of the isocagonal cone does not have this property. Therefore the two groups are different. □

There is another way of doing it,

Alternative proof. In our previous example, we have found two rotations S R such that they do not commute, i.e. $RS \neq SR$. However, every two rotations in the isocagonal cone group commmutes. Therefore they are different. □

Note that in the second proof, there is an important property of groups that was used: commutativity. This notion, expressed in several contexts, is essential to group theory. But to see that, you have to dive into the world of groups.

1 Definitions

Note, in our previous two examples of rotational symmetrical groups, the notion of composition is quite important: In both of our proofs that the tetrahedron group and the isocagonal cone group are different, we have harness this notion. Naturally, we should have it in our definition of group.

Definition 1.1. Let X be a set. A binary operation $\cdot$ is a function : $X \times X \to X$.

Definition 1.2. A group G is a triple $(G, \cdot, e)$, where G is a nonempty set, $\cdot$ is a binary operation on G and $e \in G$, that satisfies
G1. (Law of Associativity) $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
G2. (Identity) $\forall a \in G, a \cdot e = a$.
G3. (Inverse) $\forall a \in G, \exists b \in G, a \cdot b = e$

Most of the time we write $a \cdot b$ as ab.

Theorem 1.1. *Let $(G, \cdot, e)$ be a group, then*
1. $ab = e \implies ba = e$.
2. $ea = a$.
3. $ab = e \wedge ab' = e \implies b = b'$.
4. $\exists a, ae' = a \implies e' = e$.

Proof. 1. Choose c such that $(ba)c = e$, so $e = bac = beac = b(ab)ac = ba((ba)c) = bae = ba$.
2. By part 1, we can choose b such that $ab = ba = e$, so $ea = aba = ae = a$.
3. $b = bab' = eb'$ (due to part 1) $= b'$ (due to part 2).
4. By part 1, we choose b such that $ba = e$, so $e' = ee'$ (by part 2) $= bae' = ba = e$. □

Remark. There are a LOT of proofs to the preceding theorem. For example, the lecturer used a somewhat different proof for part 1 of the theorem. Therefore, you should try and come up with your own – it's great fun.

By part 3 and axiom G3, any a in the group has a unique b in the group such that $ab = ba = e$. Then we write $a^{-1} = b$ for this element. This is called the *inverse* of a. Note as well that $(a^{-1})^{-1} = a$. In addition, $(ab)^{-1} = b^{-1}a^{-1}$.

Definition 1.3. For any element $a \in G$, declare $a^0 = e$. Say inductively that $a^n = a(a^{n-1})$ for a positive integer n. Similarly for a negative integer n, $a^n = (a^{-1})^{-n}$

One can check that the usual laws of indices apply.

Proposition 1.2. *1.* $a^n a^m = a^{m+n}$.
2. $(a^n)^m = a^{nm}$.

Proof. Trivial. □

There are some 'fake axioms' that we do not actually have to be stated. For example, the definition of binary operation includes the axiom of closure. However, we do have to verify the closure property to show that something is a group.

2 Examples and Properties of Groups

Definition 2.1. A group G is called abelian if $ab = ba$ for any $a, b \in G$.

Definition 2.2. A group is finite if the underlying set G has finitely many element. In which case, we write $|G|$ to denote the number of elements in G. We call it the *order* of G.

Example 2.1. 1. Consider the set that contains a single element. There is an unique binary operation that can be defined on it which makes it a group.
2. The set of integers under addition $(\mathbb{Z}, +, 0)$ is a group.
3. We can replace the set $\mathbb{Z}$ by $\mathbb{R}, \mathbb{C}$ or $\mathbb{Q}$ and we still get a group. These groups are all abelian.
4. (non-example) $(\mathbb{N}, +, 0)$ is not a group since it does not have inverses.
5. (non-example) $(\mathbb{Z}, -, 0)$ is not a group since it does not have the law of associativity. $1 - (1 - 1) \neq (1 - 1) - 1$.
6. (non-example) $(\mathbb{Q}, \times, 1)$ is not a group since 0 does not have an inverse.
7. $(\mathbb{Q} \setminus \{0\}, \times, 1)$ is a group. Similarly, $(\mathbb{C} \setminus \{0\}, \times, 1)$, $(\mathbb{R} \setminus \{0\}, \times, 1)$ are also groups. And they are all abelian.
8. If $X \subset \mathbb{R}^3$ is a solid, then the set of rotational symmetries of it gives a group under composition. The identity element is "doing nothing". Note that it may or may not be abelian. It can also be infinite (e.g. sphere).
9. $(\mathbb{Q}_{>0}, \times, 1)$ is a group.
10. $(\{z \in \mathbb{C} : |z| = 1\}, \times, 1)$ is a group.
11. For any natural number n,

$$C_n = \{z \in \mathbb{C} : z^n = 1\}$$

is a group under multiplication. It is abelian and finite as well, and it has exactly n elements.
12. For any $n \in \mathbb{N}$, the set $\mathbb{Z}_n = \{0, 1, 2, \ldots n - 1\}$ is a group under $+_n$, the addition modulo n. It is also abelian and finite (order n). The groups C_n and $\mathbb{Z}_n$ are actually the same (why?).
13. Consider the set $\mathrm{Isom}(\mathbb{R})$ be the set of isometries (i.e. distance-preserving maps) within the real numbers. They constitute a group under composition, where e is the identity function. Examples of elements in this group are: the function $r : x \mapsto -x$, the function $t : x \mapsto x + 1$. So $r \circ t = -(x + 1) = -x - 1$, but $t \circ r = (-x + 1) = 1 - x \neq r \circ t$. Therefore this group is non-abelian. It is not finite as well.
14. Let $\mathrm{GL}_2(\mathbb{R})$ be the set of invertible 2×2 matrices in $\mathbb{R}$. It gives a group if we take the multiplication to be composition (matrix multiplication) and identity to be the identity matrix.

Definition 2.3. Let $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$. We say the latter is a subgroup of the former if $H \subseteq G$, $e_H = e_G$ and

$$\forall a, b \in H, a \cdot_H b = a \cdot_G b$$

In this case, we say $H \leq G$.

Proposition 2.1. *Let $(G, \cdot_G, e_G)$ be a group and $H \subseteq G$ be nonempty. If for all $a, b \in H$, $a \cdot_G b^{-1} \in \mathbb{H}$, then there is a unique $\cdot_H$ on H and a unique $e_H \in \mathbb{H}$ such that $(H, \cdot_H, e_H)$ is a group and $H \leq G$.*

Proof. As H is nonempty, it contains some element x, so by hypothesis we have $e_G = x \cdot_G x^{-1} \in H$. Now for any $a \in H$, we write $a^{-1} = e_G \cdot_G a^{-1} \in \mathbb{H}$. For any $a, b \in H$, we have $ab = a \cdot_G (b^{-1})^{-1} \in H$.
Define $e_H = e_G$ and $a \cdot_H b = a \cdot_G b$, which makes H a subgroup of G. Trivial to check. The uniqueness follows from the definition of a subgroup. □

Example 2.2. 1. $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0)$.
2. Any group is a subgroup of itself.
3. For any group $(G, \cdot, e)$, $\{e\} \leq G$. This is called the trivial subgroup.
4. $(\{1, -1\}, \times, 1) \leq (\mathbb{Q} \setminus \{0\}, \times, 1)$.
5. If $m|n$, $C_m \leq C_n$.
6. In the rotational symmetry group of the tetrahedron, the rotations by $0, \pi$ through an axis joining the midpoint of two opposite edges is a subgroup.
7. The group $\mathrm{SL}_2(\mathbb{R})$ consisting of all matrices of determinant 1 is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

In general, we cannot find the all subgroups of a group, but we can do it sometimes.

Proposition 2.2. *The subgroups of $\mathbb{Z}$ under addition are of the form $k\mathbb{Z}$ where $k \in \mathbb{Z}$.*

Proof. It is obvious that $k\mathbb{Z}$ is always a subgroup for any $k \in \mathbb{Z}$. Indeed, suppose we have $kn, km \in k\mathbb{Z}$, we have $kn - km = k(n - m) \in k\mathbb{Z}$. And $0 \in k\mathbb{Z}$, so it is not empty.
For any subgroup of $S \leq \mathbb{Z}$, either $S = \{0\} = 0\mathbb{Z}$ or we can consider the smallest positive integer k in that subgroup. Then $k\mathbb{Z} \subseteq S$. Also, if there is any element that is not a multiple of k, that is $S \ni x = kn + r$ for soem $n \in \mathbb{Z}$ and $0 < r < k$. But then $r = x - kn \in S$ contradicts the minimality of k, which is a contradiction. □

Definition 2.4 (Direct Product of Groups)**.** Consider two group $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$. Define the binary operation $\cdot$ on $G \times H$ by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$$

This makes $G \times H$ a group by taking the identity to be (e_G, e_H).

From now on, we omit the explicit statement of the binary operation and the identity element.

2.1 Symmetries of Regular Polygons

let D_{2n} be the set of isometries of the regular n-gon. We can think of the n-gon as the group generated by the n^{th} root of unity. Then D_{2n} consists of isometries of the complex numbers which send the n-gon to itself.

Theorem 2.3. *If we take the set of such isometries, and composition as multiplication and the identity to be the identity function, then it is a group of order $2n$.*

Proof. The first two axioms are trivial.
We now exhaust the elements in this group. Let $r : \mathbb{C} \to \mathbb{C}$ be the map $z \mapsto ze^{2\pi i/n}$. One can show that it is an isometry. Also, $r(e^{2\pi ik/n}) = e^{2\pi i(k+1)/n}$, so it does send the n-gon to itself. Note as well that $r^n = e$ where e is the identity function, which we have defined as the identity. So r has an inverse, so have all r^k.
Consider the map $s : \mathbb{C} \to \mathbb{C}$ by the map $z \mapsto \bar{z}$. One can also check that it is an isometry satisfying our conditions. Note this time that $s^2 = 1$, so s has an inverse which is itself.
Let f be an element of D_{2n}. $f(1) = e^{2\pi ik/n} = r^k(1)$ for some k as f preserves that n-gon. So let $g(x) = r^{-k} \circ f$, then $g(1) = 1$.
Now consider $g(e^{2\pi i/n})$, this is either $e^{2\pi i/n}$ or $e^{2\pi i(n-1)/n}$ as g is an isometry.
If it is the former case, then g fixes $0, 1$ and $e^{2\pi i/n}$. One can show that an isometry that fixes three points actually fixes any point. So $f = r^k$.
If it is the latter case, then $s \circ g$ would fix $0, 1$ and $e^{2\pi i/n}$, so it is the identity again. Therefore $f = r^k g = r^k s$.
So $D_{2n} = \{r^k s^\delta : k \in \{0, 1, \ldots, n-1\}, \delta \in \{0, 1\}\}$, one can show that none of which equals to any other and all of them have inverses. This set has $2n$ elements. □

Note that in D_{2n}, sr maps 1 to $e^{2\pi i(n-1)/n}$, and rsr fixes 1 and $rsr(e^{2\pi i/n}) = e^{2\pi i(n-1)/n}$, so $srsr = e \implies rsr = s \implies sr = r^{-1}s$. [1]

2.2 Symmetries of Sets

For a set X, the permutation of X is a bijective function $f : X \to X$.
Let $\mathrm{Sym}(X)$ be the set of all permutations of X.

Theorem 2.4. *For any set X, the set of permutations of X under composition, where the identity is the identity function, is a group called the symmetric group on X.*

Proof. Obvious. □

When $X = \{1, 2, \ldots n\}$, then we denote $\mathrm{Sym}(X)$ by S_n. Immediately $|S_n| = n!$.

3 Homomorphisms

Definition 3.1. For groups G, H, a map $\phi : H \to G$ is called a homomorphism $H \to G$ if

$$\phi(h_1 h_2) = \phi(h_1)\phi(h_2)$$

for any $h_1, h_2 \in H$.
If ϕ is a bijection as well, then it is called an isomorphism. In this case, we say G, H are isomorphic.

Example 3.1. 1. For any H, G, the function f defined by $f(h) = e$ for any $h \in H$ is a homomorphism.
2. If $H \leq G$, the inclusion map is a homomorphism.

[1] The group D_{2n} can be written otherwise as $D_{2n} = \langle s, r | srsr, r^n, s^2 \rangle$.

3. Let $n|m$, the map $z \mapsto z^{m/n}$ is a homomorphism between $C_n \to C_m$.
4. The exponential function $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ is a homomorphism $(\mathbb{R}, +, 0) \to (\mathbb{R}_{>0}, \times, 1)$.
5. The determinant function $\det : \mathrm{Gl}_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ under multiplication.

Lemma 3.1. *If $\phi : H \to G$ is a homomorphism, then*
1. $\phi(e_H) = e_G$ where e_H is the identity of H and e_G the identity of G.
2. $\forall a \in G, \phi(a^{-1}) = \phi(a)^{-1}$

Proof. 1. Consider $e^2 = e$ where e is the identity of any group, so

$$\phi(e_H)^2 = \phi(e_H^2) = \phi(e_H) \implies \phi(e_H) = e_G$$

2. we have

$$e_G = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) \implies \phi(a^{-1}) = \phi(a)^{-1}$$

as desired. □

It also follows easily from definitions that compositions of homomorphisms is a homomorphism.

Definition 3.2. Let $\phi : H \to G$ be a homomorphism, then the image of ϕ is defined as

$$\operatorname{Im}\phi = \{g \in G : \exists h \in H, \phi(h) = g\}$$

The kernel of ϕ is defined as

$$\ker\phi = \{h \in H : \phi(h) = e_G\}$$

where e_G is the identity of G.

Proposition 3.2. $\operatorname{Im}\phi \leq G, \ker\phi \leq H$.

Proof. For the first part, suppose that $a, b \in \operatorname{Im}\phi$, then suppose that $\phi(h_1) = a, \phi(h_2) = b$, we have $ab^{-1} = \phi(h_1 h_2^{-1}) \in \operatorname{Im}\phi$.
For the second part, suppose $a, b \in \ker\phi$, then $\phi(ab^{-1}) = e_G e_G^{-1} = e_G$ where e_G is the identity of G. So $ab^{-1} \in \ker\phi$.
It is also immediate that both of them are nonempty, as $e_H \in \ker\phi, e_G \in \operatorname{Im}\phi$. □

Proposition 3.3. *A homomorphism is an isomorphism if and only if its kernel is the subgroup consisting of only the idenity of the domain and that its image is the entire codomain.*

Proof. Take a homomorphism $\phi : H \to G$. If it is an isomorphism then the condition is immediate.
Conversely, since $\operatorname{Im}\phi = G$, ϕ is surjective. At the same time, if $\phi(h_1) = \phi(h_2)$ for some $h_1, h_2 \in H$, then

$$\phi(h_1 h_2^{-1}) \in \ker\phi \implies h_1 h_2^{-1} = e_H \implies h_1 = h_2$$

where e_H is the identity of H. So it is also injective, it follows that it is a bijection, therefore it is an isomorphism. [2] □

Note as well that an inverse of an isomorphism is again an isomorphism. The proof to this is trivial.

[2] Alternatively, like the lecturer did, we can construct an explicit inverse, which is not as clean as this approach in the author's opinion.

4 Cyclic Groups

Recall that C_n is the set of n^{th} roots of unity. If we write $\xi = e^{2\pi i/n}$, the group is actually generated by ξ, that is, every element is of the form ξ^k for some k. Note that $\xi^n = \xi^0 = 1$.

Definition 4.1. A group G is called cyclic if there is an $a \in G$ such that every element is of the form a^k for some k.
The element a is called the generator of G.

Example 4.1. 1. The integers under addition is cyclic with generator 1.
2. The group $\mathbb{Z}_n$ under addition modulo n is cyclic with generator 1. But in fact, if we take the function $\phi(k) \to \xi^k$, this is an isomorphism and hence $C_n \cong \mathbb{Z}_n$.

Theorem 4.1 (Classification of Cyclic Groups)**.** *A cyclic group is isomorphic to either C_n for some $n \to \mathbb{N}$ or $\mathbb{Z}$.*

Proof. Let G be a cyclic group and a be its generator. Consider $S = \{k \in \mathbb{N}\backslash\{0\} : a^k = e\}$. If $S \neq \varnothing$, then let n be the smallest element of S. Consider the function $\phi : C_n \to G$ by $\phi(\xi^k) = a^k$. We want to show that its an isomorphism. Now if $k, l < n$ are such that $k+l < n$, then $\phi(\xi^k\xi^l) = a^{k+l} = a^k a^l = \phi(\xi^k)\phi(\xi^l)$. On the other hand, if $k+l = n+r, 0 \leq r < n$, then $\phi(\xi^k\xi^l) = a^{k+l} = a^{n+r} = a^r = \phi(\xi^r) = \phi(\xi^{n+r}) = \phi(\xi^k)\phi(\xi^l)$. As G is generated by a and $a^n = e$, every element of G is of the form a^k for some $0 \leq k < n$, so $\phi(\xi^k) = a^k$, So ϕ is injective, consider the kernel of ϕ. Note that if $\phi(\xi^k) = e$ then $a^k = e \implies k = 0$, so $\ker\phi = \{1\}$, hence it is injective. So $G \cong C_n$.
Now if $S = \varnothing$, then we shall show that $G \cong \mathbb{Z}$. Consider the map $\phi(k) = a^k$, then $\phi(k+l) = a^k a^l = \phi(k)\phi(l)$. This is surjective by the same argument as above. Its kernel consists of integers k with $a^k = e$ but since S is empty, $k = 0$, so it is injective. Therefore $G \cong \mathbb{Z}$. □

Because of this theorem, it is convenient to write $\mathbb{Z} = C_\infty$.

Definition 4.2. Let G be a group and $g \in \mathbb{G}$, then the order of g is the smallest positive integer n such that $g^n = e$ if it exists. If there isn't such an n, then we say that g has infinite order.
We write $\text{ord}(g)$ to denote the order of g.

Consider the set generated by the powers of g. It follows easily that this set is a subgroup of G, we denote this by $\langle g\rangle$, the subgroup generated by g. It is cyclic, so it is isomorphic to C_n where $n = \text{ord}\, g$.

5 Group Actions

Definition 5.1. Let $(G, \cdot, e)$ be a group and S be a set. The action of G on S is a function $\star : G \times S \to S$ satisfying
A1. $\forall x \in S, e \star x = x$.
A2. $\forall g_1, g_2 \in G, \forall x \in S, (g_1 \cdot g_2) \star x = g_1 \star (g_2 \star x)$.

Example 5.1. 1. $\forall g \in G, x \in S, g \star x = x$ always defines a group action.
2. A group G acts on the set $S = G$ by left multiplication. That is, via

$g \star g' = g \cdot g'$. This is called the *left regular action.*
3. Consider $\operatorname{Sym} S$, it acts on S by applying the permutation.
4. The symmetries of a solid X acts on the set of points of X (or a special subset like the set of vertices). Note that the dihedral group D_{2n} acts on an n-gon in this way.

Definition 5.2. The orbit of $x \in S$ is the set

$$G \star x = \{y \in X : \exists g \in G, y = g \star x\}$$

If this set is equal to X, then this action is called transitive. The stabiliser of $x \in S$ is the set

$$G_x = \{g \in G : g \star x = x\}$$

The kernel is defined as

$$\{g \in G : \forall x \in S, g \star x = x\} = \bigcap_{x \in S} G_x$$

An action is faithful if its kernel is $\{e\}$.

Theorem 5.1. *An action is the same as a homomorphism $\rho : G \to \operatorname{Sym} S$.*

Proof. The function $t_g : x \mapsto g \star x$ is a permutation of X for any $g \in G$. Indeed, we can find an inverse of it which is exactly $t_{g^{-1}}$. Now we shall show that the map $\rho : g \mapsto t_g$ is an homomorphism. We can evaluate $\rho(gh) = t_{gh}$, but $t_{gh}(x) = (gh) \star x = g \star (h \star x) = t_g \circ t_h(x)$, therefore

$$\rho(gh) = t_g \circ t_h = \rho(g)\rho(h)$$

Conversely, let ρ be an homomorphism, then consider the function $\star$ defined by $g \star x = (\rho(g))(x)$ is an action. □

Note that the same actions are corrsponded to the same homomorphism.

Theorem 5.2 (Cayley's Theorem)**.** *Any group is isomorphic to a subgroup of some symmetric group.*

Proof. Consider the left regular action of the group G on the set G. There is then a homomorphism $\rho : G \to \operatorname{Sym} G$. Now this action is faithful. Indeed, $\rho(g) = e \iff \forall x \in G, gx = x \iff g = e$ (Or simply we can write $g = ge = e$). Therefore this homomorphism is injective, hence $G \cong \operatorname{Im} \rho \leq \operatorname{Sym} G$. □

We now want to dive deeper into orbits and stabiliser. Let G act on X.

Theorem 5.3. *For each $x \in X$, $G_x \leq G$, and the collection of all orbits $G \star x$ for every $x \in X$ partitions X.*

Proof. Note that $e \in G_x$ for each x so G_x is nonempty. If $a, b \in G_x$, then $x = e \star x = (b^{-1}b) \star x = b^{-1} \star (b \star x) = b^{-1} \star x \implies b^{-1} \in G_x$. Therefore $(ab^{-1}) \star x = a \star (b^{-1} \star x) = a \star x = x \implies ab^{-1} \in G_x$, so $G_x \leq G$.
Now the union of orbits contains each $x \in X$ since $x \in G \star x$. Now if $G \star x \cap G \star y \neq \varnothing$, there is some $g, h \in G$ such that $g \star x = h \star y$. Therefore for any $z \in G \star x$, then $z = k \star x$ for some $k \in G$, then $z = k \star ((g^{-1}) \star (h \star y)) = (kg^{-1}h) \star y \implies z \in G \star y$. So $G \star x \subseteq G \star y$ and $G \star y \subseteq G \star x$, so $G \star x = G \star y$. Hence the orbits form a parition of X. □

What we have discussed so far is called the left action. The right action $\diamond : X \times G \to X$ is defined analogously. So $x \diamond e = x$ and $(x \diamond g) \diamond h = x \diamond (gh)$.

Proposition 5.4. *If $\diamond$ is a right action, then we can define a left action $\star$ by $g \star x = x \diamond g^{-1}$. We can also have the other way around.*

Proof. Trivial. □

So we can only use left actions during the scope of our study.

Definition 5.3. If G has a left action on X, the set of orbits is called $G\backslash X = \{G \star x : x \in X\}$. If G has a right action on X, the set of orbits is called $X/G = \{x \diamond G : x \in X\}$

Example 5.2. The dihedral group D_{2n} acts on the regular n-gon X in the obvious way.
The orbit of a vertex is then all vertices. The stabiliser of a vertex is the identity and the reflection across the axis which is the diagonal through the vertex. Note here that the size of the orbit times the size of stabiliser is the size of the dihedral group.
Now consider a point in the interior of a side of the square. Then the orbit of this point would consist of 8 points, and nothing stabilises it, so we also get that the product of the sizes of the orbit and the stabiliser is 8, the size of the dihedral group.
Let us now look at the symmetries of the tetrahedron with vertices $1, 2, 3, 4$. Suppose the rotation across midpoints of opposite sides be S and the rotation across the central axis through a vertex R.
Let V be the set of vertices and let this group act on it. Then it is obvious that this action is transitive, and the stabiliser of a vertex are the rotations with respect to the axis through that vertex.
So again the sizes of the orbit and stabiliser give a product of 12, the size of the group.
Now we act on the set of edges E. Pick one of the edge X, then the action of the group on it is yet again transitive, and the stabilisers are the identity and the rotation R on the midpoint of E and its opposite edge. Again they give a product of $6 \times 2 = 12$, the size of the group.

The preceding observation triggers the following theorem.

Theorem 5.5 (Orbit-Stabiliser Theorem on finite groups)**.** $|G_x||G \star x| = |G|$

To prove it, we need some preparation.

Proposition 5.6. *If $H \leq G$, the left regular action of H on G is the left multiplication of element in H on G, i.e. $h \star g = hg$. The right regular action then is $g \diamond h = gh$*

Definition 5.4. A left coset of H in G is an orbit of the right regular action. Write G/H to denote the collection of these cosets.
We can define the right coset the other way around which are collected as $H\backslash G$.

So each left coset is in the form $gH = \{gh : h \in H\}$, and the right coset in the form $Hg = \{hg : h \in H\}$. Note that it is not always true that a left coset is equal to the right coset.

Also $G/H = \{S \subseteq G : \exists g \in G, S = gH\}$ and we can find $H\backslash G$ similarly. [3]
Note that $gH = g'H \iff g'^{-1}g \in H$, and for right cosets $Hg = Hg' \iff g'g^{-1} \in H$ but again these two conditions may or may not be equivalent.

Example 5.3. The (left and right) cosets of $2\mathbb{Z}$ are $2\mathbb{Z}$ and $2\mathbb{Z} + 1 = 1 + 2\mathbb{Z}$.
The (left and right) cosets of $n\mathbb{Z}$ are $k + n\mathbb{Z}, k \in \{0, 1, \dots n-1\}$.
Consider D_6, $R = \{e, r, r^2\}, S = \{e, s\}$ are subgroups. The (left and right) coset of R are R and $sR = Rs$ And the left cosets of S are S, rS and r^2S and the right ones are S, Sr, Sr^2, but in this case the left and right cosets are not equal.

Theorem 5.7. *If $H \subset G$ and $g \in G$, then there is a bijection $H \to gH$.*

Proof. $h \mapsto gh$ is the bijection. □

Corollary 5.8 (Lagrange's Theorem)**.** *If G is finite and $H \leq G$, then we have $|H||G/H| = G$. In particular $|H|$ divides $|G|$.*

Proof. The cosets are orbits thus parition G and they are of the same cardinality due to the preceding theorem. □

We can repeat the same argument to see that the same also applies to right cosets.

Definition 5.5. Let G be a group, and $H \leq G$, then the index of H is the order of G/H given that it is finite, otherwise we say the index is infinite.

Equivalently, the index is $|G|/|H|$ (given that H is finite).

Corollary 5.9. *If G is finite and $g \in G$, then $g^{|G|} = e$, that is,* $\operatorname{ord} g || G|$.

Proof. Consider the subgroup $\langle g \rangle \leq G$. □

Corollary 5.10. *If G is finite $|G|$ is prime, then $G \cong C_p$ and it is generated by any identity element.*

Proof. G contains some non-identity element since $|G| = p > 1$. Choose any $g \in G$ such that $g \neq e$. Then $1 < \operatorname{ord} g || G| = p$, so since p is prime, then $\operatorname{ord} g = p$. Thus since $\langle g \rangle \leq G$ and they are both finite and of the same order, $C_p \cong \langle g \rangle = G$. □

There is a corollary of this in number theory. We consider the collection of all (equivalent classes) of integers $k \in \mathbb{Z}_n$ such that $(k, n) = 1$. Since $(k, n) = 1$, k is invertible in $\mathbb{Z}_n$ for any such k in the collection. Conversely, if k cannot be invertible in $\mathbb{Z}_n$ if $(k, n) \neq 1$.
So this collection is a group $\mathbb{Z}_n^\times$ under multiplication modulo n. Also, this group has order $\phi(n)$ which is the number of positive integers less than n that are coprime to it.

Corollary 5.11 (Fermat-Euler Theorem)**.** *If $(k, n) = 1$, then*

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Proof. Apply the preceding corollary to $\mathbb{Z}_n^\times$. □

[3] Some authors use $G : H$ for the collection of left cosets.

After these warm-ups, we shall prove the Orbit-Stabiliser Theorem (in a stronger form).

Theorem 5.12 (Orbit-Stabiliser Theorem)**.** *Suppose a group G acts on a set X and $x \in X$, then there is a bijection $G/G_x \to G \star x$ by $\phi : gG_x \mapsto g \star x$.*

Proof. To see ϕ is well defined, observe that $\forall h \in G_x, g \star x = g \star (h \star x) = (gh) \star x$. It is obviously surjective by the definition of orbit. It is injective since if $\phi(gH) = \phi(g'H)$, then $(g^{-1}g') \star x = x \implies g^{-1}g' \in H \implies gH = g'H$. □

Corollary 5.13. *Theorem 5.5.*

Proof. Due to the existence of this bijection, if G is finite, then $|G|/|G_x| = |G/G_x| = |G \star x| \implies |G \star x||G_x| = |G|$. □

One of the most important application of this theorem is to work out the order of some finite group.

Example 5.4. We look at the rotational symmetries of a cube. Collect the symmetries as the group G and consider its action on the eight vertices X. Now this action is transitive, obviously, so fixing any $x \in X$, $|G \star x| = 8$. Also, any member of the stabiliser of x must be rotations though the axis through x and the centre of the centre of the group since it fixes that. There are three rotations of this form, so $|G| = |G_x||G \star x| = 24$.

Theorem 5.14 (Cauchy's Theorem)**.** *Let G be a finite group and suppose p is a prime dividing its order, then G contains an element of order p.*

Proof. Consider a subset $X \subseteq G^p$ defined by $X = \{(g_1, g_2, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\}$. Since $|G^p| = |G|^p$, and $|X| = |G|^{p-1}$. Let $H = C_p = \langle \xi \rangle$, consider the action of H on X by

$$\xi \star (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$$

This is an action, indeed, if $g_1 g_2 \cdots g_p = e$, then $g_2 g_3 \cdots g_p g_1 = g_1^{-1} e g_1 = e$. For any element $x \in X$, by Theorem 5.5, $p = |H| = |H_x||H \star x|$. But p is prime, so every orbit has to have either size 1 or size p, also the ordrs of the orbits sum to $|X| = |G|^{p-1}$ which is divisible by p. So the number of size 1 orbits must be divisible by p, thus at least 2. But all such orbits must be in the form $(g, g, \ldots, p)$, but since there are 2 of them, there is some $g \neq e$ such that this tuple is in X, thus $g^p = e$ and $g \neq e$, therefore g has order p. □

In fact, we have shown that the number of elements of order p is congruent to $p - 1 \pmod{p}$.

Definition 5.6. Fix a group G. $a, b \in G$ are conjugates of each other if $\exists g \in G, a = gbg^{-1}$.
The conjugation action is an action of a group g on itself by $g \star h = ghg^{-1}$.

One can check that the conjugation is indeed an action.

Definition 5.7. The orbits of the conjugation are called the conjugacy classes of G. The stabiliser of the conjugation of an element h is called the centraliser $C_G(h)$ of h. The kernel of the conjugation action is called the centre $Z(G)$ of G.

We can extend the conjugation action to the subgroups of G.

Definition 5.8. If $H \leq G$, then the conjugate of H by g is the subgroup $\{ghg^{-1} : h \in H\}$.

It is trivial that the conjugate of a subgroup is indeed a subgroup.

6 The Möbius Group

We want to study $f : \mathbb{C} \to \mathbb{C}$ in the form

$$f(x) = \frac{ax+b}{cx+d}, a, b, c, d \in \mathbb{C}$$

This function has a pole at $x = -d/c$, so we need an element at infinity. We can take $\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\}$ by the stereographic projection $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\} \cong S^2$. Now we define the Mobius map properly

Definition 6.1. The Mobius map $f : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is defined by

$$f(z) = \begin{cases} \frac{az+b}{cz+d}, \text{ if } z \neq \infty \text{ and } z \neq -d/c \\ \infty, \text{ if } z = -d/c \\ \frac{a}{c}, \text{ if } z = \infty \end{cases}$$

where $ad - bc \neq 0$.

The reason why we impose the last condition is that we want the Mobius map to be a bijection from $\mathbb{C}_\infty$ to $\mathbb{C}_\infty$.

Proposition 6.1. *Let $\mathcal{M} = \{f : \mathbb{C}_\infty \to \mathbb{C}_\infty : f$ is a Mobius function$\}$. Then $(\mathcal{M}, \circ, \mathrm{id})$ is a group.*

Proof. Obviously $\mathrm{id} \in \mathcal{M}$. Note also that if $g(z) = (az+b)/(cz+d), g'(z) = (a'z+b')/(c'z+d')$, then $g'(g(z)) = (a''z+b'')/(c''z+d'')$ where

$$\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then it immediately tells us that $\mathcal{M}$ is closed under $\circ$ since the determinant function is multiplicative. It gives us the inverse immediately by just finding some a', b', c', d' (which exists due to our criterion on determinant) such that

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

which works due to the discussion we just had. □

With its elements as functions $\mathbb{C}_\infty \to \mathbb{C}_\infty$, $\mathcal{M}$ acts on $\mathbb{C}^\infty$ faithfully (i.e. with trivial kernel), so $\mathcal{M}$ can be regarded as a subgroup of $\operatorname{Sym} \mathbb{C}_\infty$. Also, there is nothing special with ∞ in $\mathbb{C}_\infty$, just as there is no special point on S^2. To justify it, just fix some $a \in \mathbb{C}$ and conjugate everything that happened on $\mathbb{C}_\infty$ by the Mobius transformation $z \mapsto 1/(z-a)$.

Proposition 6.2. *Every Mobius tranformation is a composition of $z \mapsto az, a \neq 0$, $z \mapsto z + b$ and $z \mapsto 1/z$.*

Proof. Let $z \mapsto (az + b)/(cz + d)$ be a mobius transformation, then if $c = 0$ the proposition is trivial. Otherwise $c \neq 0$, then we have

$$\frac{az + b}{cz + d} = \frac{a}{c} - \frac{ad - bc}{c(cz + d)}$$

which can obviously be obtained from the said functions. □

How about fixed point of a Mobius transformation? We know that a Mobius transformation fixes at least 1 point, but how about more?

Proposition 6.3. *A Mobius transformation fixes 3 points is the identity.*

Proof. Suppose

$$f : z \mapsto \frac{az + b}{cz + d}$$

If ∞ is a fixed point, then $c = 0$, so f is a linear function. But then a linear function that fixes 2 (non-infinity) points is the identity (since $f(x) - x$ is linear and a linear function has exactly 1 root unless it is constantly 0), f is the identity.
Now if ∞ is not a fixed point, then

$$f(z) = z \iff \frac{az + b}{cz + d} - z = 0 \iff az + b - z(cz + d) = 0$$

which has at most 2 roots (hence fixed point) since it is quadratic, unless it is the zero function, which essentially means that $c = b = 0, d = a \neq 0 \implies f = \text{id}$. □

Proposition 6.4. *Given distinct $z_1, z_2, z_3 \in \mathbb{C}_\infty$ and $w_1, w_2, w_3 \in \mathbb{C}$, then there is an unique Mobius transformation f such that $f(z_i) = w_i$ for $i \in \{1, 2, 3\}$.*

Note that since every Mobius transformation is bijective (hence invertible), w_i's are distinct as well.

Proof. For existence, it suffices to deal with the case where w_1, w_2, w_3 are $0, 1, \infty$, since once we've found maps f, g such that $f : z_1, z_2, z_3 \mapsto 0, 1, \infty, g : w_1, w_2, w_3 \mapsto 0, 1, \infty$, then $g^{-1} \circ f$ will send z_1, z_2, z_3 to w_1, w_2, w_3.
Now if none of z_i's is ∞, we can use the interpolation

$$f(z) = \frac{(z - z_2)(z - z_3)}{(z_1 - z_2)(z_2 - z_3)} + \frac{(z - z_1)(z - z_2)}{z - z_3}$$

Otherwise, suppose $z_i = \infty$, then the map f_i suffices where

$$f_1(z) = \frac{z - z_2}{z - z_3}, f_2(z) = \frac{z_1 - z_3}{z - z_3}, f_3(z) = \frac{z - z_2}{z_1 - z_2}$$

For uniqueness, suppose f, f' send z_1, z_2, z_3 to w_1, w_2, w_3 respectly, then $f^{-1} \circ f'$ fixes z_1, z_2, z_3, hence $f^{-1} \circ f' = \text{id} \implies f = f'$. □

If $f, g \in \mathcal{M}$ and f fixes z_0, then gfg^{-1} fixes $g(z_0)$, which gives rise to the following observation

Theorem 6.5. *Every member of a conjugacy class of $\mathcal{M}$ has the same number of fixed point(s).*

Proof. Obviously the identity itself is itself a conjugacy class. Now for any nonidentity f, f has either 1 or 2 fixed points.
If f has 1 fixed point $z_0 \neq \infty$, then suppose $g(z) = 1/(z - z_0)$, we know that gfg^{-1} fixes ∞, and it cannot fix any other points because if so then applying g^{-1} to that point would produce another fixed point of f. So it has to be the map $z \mapsto z + b, b \neq 0$.
If f has 2 fixed point, then we consider a Mobius transformation g which sends the fixed points to $0, \infty$, then gfg^{-1} fixed 0 to ∞ and sends 1 to $a \in \mathbb{C} \neq 0, \infty$, so there is exactly one Mobius transformation $z \mapsto az, a \neq 1$. □

Note that $(g^{-1}fg)^n = g^{-1}f^ng$. This allows us to compute the arbitrary (integral) power of a Mobius transformation.

Definition 6.2. The circle in the extended complex numbers is the equation $Az\bar{z} + \bar{B}z + B\bar{z} + C = 0$ with $A, C \in \mathbb{R}, B \in \mathbb{C}$. Consider ∞ is a point on this circle if and only if $A = 0$.

Note that circles in $\mathbb{C}$ are also circles in $\mathbb{C}_\infty$, and all other $\mathbb{C}_\infty$ circles are lines in $\mathbb{C}$.

Proposition 6.6. *Circles in $\mathbb{C}_\infty$ are mapped to circles in $\mathbb{C}_\infty$ under any Mobius transformations.*

Proof. It is sufficient to verify this for $z \mapsto az, z \mapsto z + b, z \mapsto z^{-1}$ due to Proposition 6.2. It is then trivial. □

Note that every circle gets to mapped to any other circle since three points determine the circle and Proposition 6.4

Definition 6.3. For extended complex numbers z_1, z_2, z_3, z_4, the cross ratio is defined by

$$[z_1, z_2, z_3, z_4] = \frac{(z_4 - z_1)(z_2 - z_3)}{(z_2 - z_1)(z_4 - z_3)}$$

We need to examine carefully when one of these numbers is infinity. For example, if we have $z_1 = \infty$, then the cross ratio is $(z_2 - z_3)/(z_4 - z_3)$.

Corollary 6.7. *For extended complex numbers z_1, z_2, z_3, z_4, the cross ratio is equal to $f(z_4)$ where f is the unique Mobius transformation sending z_1, z_2, z_3 to $0, 1, \infty$ respectively.*

Theorem 6.8. *Mobius transformations preserve the cross-ratio.*

Proof. Suppose $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$, and $g \in \mathcal{M}$. Let f be the Mobius transformation sending z_1, z_2, z_3 to $0, 1, \infty$, so the cross ratio is $f(z_4)$, so $f \circ g^{-1}$ sends $g(z_1), g(z_2), g(z_3)$ to $0, 1, \infty$, so the cross ratio of the $g(z_i)$'s is $f \circ g^{-1}(g(z_4)) = f(z_4)$. □

The converse is also true (and proved in example sheet): If a map preserves cross-ratio, then it is a Mobius transformation.

Corollary 6.9. *Four points $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ are on a circle (in the sense of $\mathbb{C}_\infty$) if and only if $[z_1, z_2, z_3, z_4]$ is real.*

Proof. Let f be the unique Mobius transformation sending z_1, z_2, z_3 to $0, 1, \infty$, so $[z_1, z_2, z_3, z_4] = f(z_4)$. Let c be the unique circle passing through z_1, z_2, z_3, then $z_4 \in c \iff f(z_4) \in f(c)$, but $f(c) = \mathbb{R} \cup \{\infty\}$. □

7 Classification of Some Small Finite Groups

Consider

$$\underline{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \underline{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \underline{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \underline{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

One can check that $Q_8 = \{\pm\underline{1}, \pm\underline{i}, \pm\underline{j}, \pm\underline{k}\}$ is a group under matrix multiplication, we also have $\underline{i}^2 = \underline{j}^2 = \underline{k}^2 = \underline{1}, \underline{ij} = \underline{k} = -\underline{ji}, \underline{jk} = \underline{i} = -\underline{kj}, \underline{ki} = \underline{j} = -\underline{ik}$

Definition 7.1. If G, H are groups, then we can have the product group $G \times H$ under the group operation

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

One can check that $(G \times H) \times K \cong G \times (H \times K)$.

Theorem 7.1 (Chinese Remainder Theorem)**.** *If $m, n \in \mathbb{N}$ such that $m, n \geq 2$ and $(m, n) = 1$, then the following function $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ defined by*

$$a \mapsto (a \bmod m, a \bmod n)$$

is an isomorphism.

Proof. It is trivial that ϕ is well-defined and is a homomorphism. Both groups has the same size, so it suffices to show that injectivity. To see it, consider $\ker \phi$. If $a \in \ker \phi$, then $a \equiv 0 \pmod m$ and $a \equiv 0 \pmod n$, so $a \equiv 0 \pmod{mn}$. So the kernel of ϕ is trivial, hence it is injective. □

Theorem 7.2. *Let $H_1, H_2 \leq G$, then if*
1. $H_1 \cap H_2 = \{e\}$
2. $h_1 h_2 = h_2 h_1$ for any $h_1 \in H_1, h_2 \in H_2$.
3. $\forall g \in G, \exists h_1 \in H_1, h_2 \in H_2, h_1 h_2 = g$.
Then $G \cong H_1 \times H_2$.

Proof. Consider the map $\phi : H_1 \times H_2 \to G$ such that $\phi : (h_1, h_2) \mapsto h_1 h_2$. It is a homomorphism by 2, indeed, if $h_1, h_1' \in H_1, h_2, h_2' = H_2$, then

$$\begin{aligned} \phi(h_1, h_2)\phi(h_1', h_2') &= h_1 h_2 h_1' h_2' = h_1 h_1' h_2 h_2' \\ &= \phi(h_1 h_1', h_2 h_2') = \phi((h_1, h_2)(h_1', h_2')) \end{aligned}$$

Its surjectivity is implied by 3. If $\phi(h_1, h_2) = e$, then $h_1 h_2 = e \implies H_1 \ni h_1 = h_2^{-1} \in H_2$, so $h_1 = h_2 = e$, so $\ker \phi = \{e\}$, thus it is injective. Therefore it is a isomorphism. □

we now wish to classify finite groups of order at most 8. For $|G| = 1, 2, 3, 5, 7$, we already know that G would be cyclic, so it remains to find those in $4, 6, 8$.

Theorem 7.3. *For a finite group G such that each element is with order 2, then we know that $|G|$ is even, also it is isomorphic to the direct product of C_2's.*

Proof. We know that G is abelian. [4] So it is done by Theorem 7.2 and the associativity of group direct products (up to isomorphism). □

Thus, for $|G| = 4$, either there is an element of order 4, in which case $G \cong C_4$, or every element has order 2, where we have $G \cong K_4 := (C_2)^2 = C_2 \times C_2$. For $|G| = 6$, then if there is an element of order 6, then $G \cong C_6$, otherwise there is an element r of order 3 and s of order 2 (by Theorem 5.14) such that $sr \neq rs$ (since if so them $G \cong C_2 \times C_3 \cong C_6$ by Theorem 7.2 and Theorem 7.1). But the elements $\{e, s, r, r^2, rs, r^2s\}$ are distinct, by inspection we must have $sr = r^2s$, but this would give the full definition of the group operation which is identical to that of the Dihedral group on a 3-gon (aka equilateral triangle), so $G \cong D_6 \cong S_3$. Groups of order 8 is a little bit more complicated.

Claim. *There are only* 5 *groups of order* 8*, and they are*

$$C_8, C_4 \times C_2, (C_2)^3, D_8, Q_8$$

up to isomorphism.

Proof. $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ are Abelian, and D_8, Q_8 are not. Furthermore, by looking at the order of elements, $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ are all distinct. And by essentially the same method, D_8, Q_8 are distinct as well, as Q_8 has only one element of order 2 but D_8 has more.
So it remains to show that every group of order 8 is one of them.
Let G be the group. Since $|G| = 8$, any element of G must have orders $1, 2, 4, 8$. If it has element of order 8, then $G \cong C_8$; if all its elements are of order 2, then $G \cong (C_2)^3$. Assume henceforth that G has at least one element f of order 4 but none of order 8. Let $g \notin \langle f \rangle$, so $G = \langle f \rangle \cup g\langle f \rangle$, in order words

$$G = \{e, f, f^2, f^3, g, gf, gf^2, gf^3\}$$

Note that $g^2 \notin g\langle f \rangle$, thus $g^2 = e$ or $g^2 = f^2$ since g does not have order 8.
If $g^2 = e$, then $fg = gf \implies G \cong C_4 \times C_2$ by Theorem 7.2, otherwise we have $fg = g^3 f$, which means that $G \cong D_8$
Otherwise $g^2 = f^2$, then $fg \neq e, f, f^2, f^3$ by inspection. Now if g is abelian then $g^2 f^{-2} = e \implies (gf^{-1})^2 = e$, $gf^{-1} \notin \langle f \rangle \implies G \cong C_4 \times C_2$. Otherwise, by inspection $fg = gf^3$, therefore we have defined the group action completely, so it can only be isomorphic to Q_8, which is not in any of the preceding cases. [5] So the claim is proved. □

8 The Isomorphism Theorems

Definition 8.1. A subgroup $H \leq G$ is called normal if $\forall h \in H, \forall g \in G, ghg^{-1} \in H$, in which occasion $H \trianglelefteq G$

Example 8.1. 1. $\{e\} \trianglelefteq G, G \trianglelefteq G$.
2. The subgroup of the dihedral group D_{2n} generated by the rotations is normal. but that generated by the reflection generator is not normal (given $n \geq 3$).
3. If G is abelian, then for every $H \leq G, H \trianglelefteq G$.

[4] Proved a long time ago in example sheet.
[5] Alternatively we can easily construct an explicit isomorphism.

Lemma 8.1. *A subgroup $H \leq G$ is normal if and only if $\forall a \in G, aH = Ha$.*

Proof. Trivial but let us write it down.
If H is normal, then for any $ah \in aH, \exists h' \in H, aha^{-1} = h' \implies ah = h'a \in Ha$, so $aH \subset Ha$. Similarly $Ha \subset aH$, so $Ha = aH$.
Conversely, if $\forall a \in G, Ha = aH$, we can choose any $h \in H, \exists h' \in H, ah = h'a \implies aha^{-1} = h' \in H$, so H is normal. □

Corollary 8.2. *Let $H \leq G$. If $|G/H| = 2$, then H is normal.*

Proof. If $a \in H$, then obviously $aH = Ha$, otherwise, since H has index 2, $aH = G \setminus H = Ha$, thus $H \trianglelefteq G$. □

Proposition 8.3. *Let $\phi : G \to K$ be a homomorphism, then* $\ker \phi \trianglelefteq G$.

Proof. Suppose $h \in \ker \phi$, then $\forall g \in G$, then $\phi(ghg^{-1}) = \phi(g)e_K\phi(g)^{-1} = e_K \implies ghg^{-1} \in \ker \phi$. □

So we know that every kernel is a normal subgroup, but how about the converse? Must every normal subgroup the kernel of some homomorphism?

Definition 8.2. Let G be a group and $H \trianglelefteq G$, then we can define the operation

$$(aH) \cdot (bH) = (ab)H$$

And G/H is a group under this operation. This is called the quotient group.

Given that it is well defined, which we will prove later, then we know that whenever H is normal, then it is the kernel of the homomorphism $\pi : G \to G/H$ by $\pi(a) = aH$. This is called the caconical projection.
If we do not have H being normal, then if we want to define the operation

$$aH \times bH = abH$$

But is it well defined? Note that to do so, if $aH = a'H, bH = b'H$, then $a^{-1}a', b^{-1}b' \in H$, but to make the operation well-defined, we must have

$$a'b'H = abH \iff a^{-1}b^{-1}a'b' \in H$$

But this is not always true. But if H is normal, then it is however true. In fact, this is true if and only if H is normal.

Theorem 8.4. *Our operation on quotient group is well-defined and G/H is a group under it.*

Proof. If $aH = a'H, bH = b'H$, then

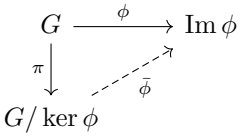
$$a'b'H = a'bH = a'Hb = aHb = abH$$

Due to normality of H.
To see that G/H is thus a group, we observe that $(aH \cdot bH) \cdot cH = abcH = aH \cdot (bH \cdot cH)$. Also $H = eH$ is the identity and $gH \cdot g^{-1}H = H$. □

Example 8.2. 1. Note that $n\mathbb{Z} \leq \mathbb{Z}$, and it is normal since $\mathbb{Z}$ is abelian. Now $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ by the isomorphism $k \mapsto k + n\mathbb{Z}$.
2. Let $R = \langle r | r^n \rangle \leq D_{2n}$, then $|D_{2n}/R| = 2$, so $D_{2n}/R \cong C_2$.
3. Let K be the group consisting of $\{e, r^2\}$ in D_8. One can check that this is normal, and that $D_8/K \cong K_4 = C_2 \times C_2$ since (by inspection) every element in the quotient group has order 2.
4. Let K be the subgroup of Q_8 consisting of $\{\pm \underline{1}\}$, and $Q_8/K \cong K_4$ since every element has order 2 again. From this example and the last one, we can see that if $H_1 \leq G_1, H_2 \leq G_2$ and $H_1 \cong H_2, G_1/H_1 \cong G_2/H_2$, we do not necessarily have $G_1 \cong G_2$. Hence, when we dissolve a group into normal subgroup and quotient, there might not be an unique way to rebuild the group from them.

Theorem 8.5 (First Isomorphism Theorem)**.** *Suppose $\phi : G \to H$ is a homomorphism, then $G/\ker\phi \cong \operatorname{Im}\phi$. Indeed, the map $\bar{\phi} : G/\ker\phi \to \operatorname{Im}\phi$ by $g\ker\phi \mapsto \phi(g)$ is well defined and is an isomorphism.*

The theorem gives the following commutative diagram, where π is the canonical projection:



Proof. We know that $\ker\phi$ is normal, thus we can form the quotient $G/\ker\phi$. If $g\ker\phi = h\ker\phi$, then $h^{-1}g \in \ker\phi$, hence

$$e_H = \phi(h^{-1}g) = \phi(h)^{-1}\phi(g) \implies \phi(g) = \phi(h)$$

thus $\bar{\phi}$ is well-defined. Note also that

$$\bar{\phi}((g\ker\phi)(h\ker\phi)) = \bar{\phi}(gh\ker\phi) = \phi(gh) = \phi(g)\phi(h) = \bar{\phi}(g\ker\phi)\bar{\phi}(h\ker\phi)$$

so it is a homomorphism. Furthermore, if $\bar{\phi}(g\ker\phi) = \bar{\phi}(h\ker\phi)$, then

$$\phi(g) = \phi(h) \implies \phi(h^{-1}g) = e_H \implies h^{-1}g \in \ker\phi \implies h\ker\phi = g\ker\phi$$

So it is injective. It is also surjective by definition, so it is bijective, hence it is an isomorphism. □

Example 8.3. 1. Consider $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Now an easy proof of that is to recognize the homomorphism $\mathbb{Z} \to \mathbb{Z}_n$ sending an integer to the remainder it left when divided by n. And the result follows by Theorem 8.5.
2. The function $\phi : (\mathbb{R}, +, 0) \to (\mathbb{C} \setminus \{0\}, \times, 1)$ by $t \mapsto e^{2\pi i t}$, so the image of ϕ is $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ and $\ker\phi = \mathbb{Z}$, so $\mathbb{R}/\mathbb{Z} \cong S^1$.
3. If H and G are groups, we have $G \times H$ and $\{e\} \times H \trianglelefteq G \times H$, but $G \times H/\{e\} \times H \cong G$.
4. Let G be the group of all symmetries (isometries) of the tetrahedron, then consider the map $\phi : G \to \operatorname{Sym} V$ where V is the set of vertices by action. But this is injective and $\operatorname{Sym} V \cong S_4$ has 24 elements, and the rotational symmetries forms an order-12 proper subgroup of G, thus we must have $G \cong G/\{e\} \cong \operatorname{Im}\phi \leq S_4$, but $12 < |\operatorname{Im}\phi||24 = |S_4|$ by Theorem 8.5, so by Corollary 5.8, $\operatorname{Im}\phi \cong S_4$. 5. G also acts on the opposite pairs of edges, which has order 3,

so it gives a homomorphism $\phi : G \to S_3$. Since its image has an element of order 2 and an element of order 3, this homomorphism is surjective, therefore $S_4/\ker\phi = G/\ker\phi \cong S_3$, so $|\ker\phi| = 4$. Interestingly, there is never again a surjective homomorphism from S_n to S_{n-1} for $n > 4$.

Definition 8.3. A group G is simple if it has no proper normal subgroup.

Example 8.4. C_p is simple for p prime, since it does not even have any proper subgroup by Corollary 5.8.

9 Cycles and Permutations

Definition 9.1. Given a list $a_1, a_2, \ldots, a_k$ of distinct elements of $\{1, 2, \ldots, n\}$, the k-cycle, written as $(a_1\ a_2\ \ldots\ a_k)$ is the permutation $\pi \in S_n$ defined by $\pi(a_i) = a_{i+1}$ for $1 \le i \le k-1$, $\pi(a_k) = a_1$, and $\pi(j) = j$ if $j \notin \{a_i : 1 \le i \le k\}$.

It is obvious that it is indeed a permutation, and we know that

$$(a_1\ a_2\ \ldots\ a_k)^{-1} = (a_k\ a_{k-1}\ \ldots\ a_1)$$

In particular, there is a set of special cycles.

Definition 9.2. A 2-cycle is called a transposition.

Two different cycles $(a_1\ a_2\ \ldots\ a_k), (b_1\ b_2\ \ldots\ b_l)$ are called disjoint if $\{a_i : 1 \le i \le k\} \cap \{b_j : 1 \le j \le l\} = \varnothing$.
We can compose the permutations since they are in fact functions

Example 9.1. $((1\ 2\ 3\ 4) \circ (3\ 2\ 4))(1) = 2$, and $((1\ 2\ 3\ 4) \circ (3\ 2\ 4))(2) = (1\ 2\ 3\ 4)(4) = 1$, similarly $((1\ 2\ 3\ 4) \circ (3\ 2\ 4))(3) = 3, ((1\ 2\ 3\ 4) \circ (3\ 2\ 4))(4) = 4$, so it is a transposition $(1\ 2)$.
By the same way, we have $(3\ 2\ 4) \circ (1\ 2\ 3\ 4) = (1\ 4)$, so $(3\ 2\ 4)$ and $(1\ 2\ 3\ 4)$ do not commute.
So S_4 is not abelian. In fact, S_n is not abelian for all $n \ge 3$ since S_n can be embedded into S_{n+1} by fixing the last element.

Lemma 9.1. *1.* $(a_1\ a_2\ \ldots\ a_k) = (a_k\ a_1\ a_2\ \ldots\ a_{k-1})$.
2. Disjoint cycles commute.

Proof. Trivial. □

Theorem 9.2. *Every permutation is a product of disjoint cycles (including* 1*-cycles for convenience) and it is unique to write it as such a product up to the ambiguity stated in the preceding lemma.*

Proof. Trivial but let us write this down. We do strong induction on n. The base case is trivial. Now we consider the sequence $1, \sigma(1), \sigma^2(1), \ldots$. Since there is only finitely many numbers, at some point the sequence goes back to 1. Indeed, there must be some $p > q$ such that $\sigma^p(1) = \sigma^q(1)$, thus $\sigma^{p-q}(1) = 1$. So we take the smallest $k \ge 1$ such that $\sigma^k(1) = 1$, so $\sigma^i(1) \ne \sigma^j(1)$ for $i \ne j$ because if so then $\sigma^{i-j}(1) = 1$ (WLOG $i > j$) which contradicts the minimality of k.
Hence σ maps $S = \{1, \sigma(1), \sigma^2(1), \ldots\}$ to itself, so it is a permutation on

$T\{1, 2, \ldots, n\} \setminus S$, thus $\sigma|_T$ is a product of disjoint cycles by induction hypothesis, thus we must have $\sigma = (1\ \sigma(1)\ \sigma^2(1)\ \ldots\ \sigma^{k-1}(1))\sigma|_T$, which proves the existence.
The uniqueness is obvious since if σ is written as two cycles, then we can pick an element and by enumerating it we can show that the cycles containing that element are the same. Hence the theorem is proved. □

Lemma 9.3. *For any permutation σ, write it as the product of disjoint cycles, that is,*

$$\sigma = (a_1^1\ a_2^1\ \ldots\ a_{k_1}^1)(a_1^2\ a_2^2\ \ldots\ a_{k_2}^2)\cdots(a_1^r\ a_2^r\ \ldots\ a_{k_r}^r)$$

Then the order of σ is the LCM of $k_1, k_2, \ldots, k_r$.

Proof. Note that

$$\sigma^j = (a_1^1\ a_2^1\ \ldots\ a_{k_1}^1)^j(a_1^2\ a_2^2\ \ldots\ a_{k_2}^2)^j\cdots(a_1^r\ a_2^r\ \ldots\ a_{k_r}^r)^j$$

since disjoint cycles commute. Now the order of a cycle $(a_1^i\ a_2^i\ \ldots\ a_{k_i}^i)$ has order k_i. So if we let ℓ be the LCM of $k_1, k_2, \ldots, k_r$, we immediately have $\sigma^\ell = e$. Suppose $\sigma^m = e$ for some m, then we would have

$$(a_1^1\ a_2^1\ \ldots\ a_{k_1}^1)^m = ((a_1^2\ a_2^2\ \ldots\ a_{k_2}^2)^m\cdots(a_1^r\ a_2^r\ \ldots\ a_{k_r}^r)^m)^{-1}$$

But the LHS fixes a_s^1 for any $1 \le s \le k_1$ due to disjointness, thus the LHS must equal to the identity, i.e. $k_1|m$. Similarly $k_i|m$ for any $1 \le i \le r$, thus $\ell|m \implies \ell \le m$, hence ℓ is the order of σ. □

9.1 The Sign of Permutation

Proposition 9.4. *Every permutation is a product of transpositions.*

Proof. By Theorem 9.2, it suffices to show that every cycle is a product of transpositions, but

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2)$$

As desired. □

Alternative proof. We proceed by induction on n such that the permutation is in S_n. In $n = 0$, there is nothing to show. More generally, for $\sigma \in S_n$ for $n > 1$. Choose an $a \in \{1, 2, \ldots, n\}$, then $(a\ \sigma(a))\sigma$ fixes a, hence is a permutation on at most $n - 1$ elements, so the proof is done by induction. □

Definition 9.3. Define the sign of a permutation σ by

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, \text{ if } \sigma \text{ has an even number of transpositions} \\ -1, \text{ otherwise} \end{cases}$$

Proposition 9.5. *The sign of the permutation is well-defined.*

Proof. Let σ be written as the product of disjoint cycles (including 1-cycles). Suppose there is $\ell(\sigma)$ many such cycles. It is well-defined by Theorem 9.2.
Consider a transposition $(c\ d)$. $\ell(\sigma \circ (c\ d)) = \ell(\sigma) + 1$ if c, d are in the same cycle in σ. Otherwise, it is $\ell(\sigma) - 1$. So in either case, $\ell(\sigma \circ (c\ d)) \equiv \ell(\sigma) + 1$

(mod 2).
Note then that $\ell(\sigma) = \ell(t_1 t_2 \cdots t_k)$ where t_i are transpositions. Thus $\ell(\sigma) \equiv \ell(e) + k \equiv n + k \pmod 2$, so if a permutation has both signs k, l, then $k \equiv l \pmod 2$. Therefore the sign is well-defined. Indeed, $\operatorname{sgn}(\sigma) = (-1)^{\ell(\sigma)-n}$. □

Immediately $\operatorname{sgn}((a_1\ a_2\ \ldots\ a_r)) = (-1)^{r-1}$.

Corollary 9.6. *The function* sgn *is a homomorphism* $S_n \to (\{1, -1\}, \times, 1)$.

Proof. Trivial. □

Definition 9.4. A permutation σ is even if $\operatorname{sgn}(\sigma) = 1$ and it is odd otherwise.

Definition 9.5. The alternating group $A_n \leq S_n$ is defined as $A_n = \ker \operatorname{sgn}$. That is, A_n consists of all even permutations.

Note that any transposition has sign -1 and the identity has sign 1, thus sgn is surjective, therefore the index of A_n is 2, hence it is normal.

9.2 Conjugation in the Permutation Group

Proposition 9.7. *If we have a permutation* σ*, then* $\sigma(a_1\ a_2\ \ldots\ a_r)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_r))$.

Proof. Trivial. □

Corollary 9.8. $\tau, \tau' \in S_n$ *are conjugates if and only if, when written as a composition of disjoint cycles (in which every number appears, i.e. counting* 1*-cycles), they have the same number of cycles of each length.*

Proof. Follows directly from the formula in the preceding proposition and Theorem 9.2. □

For a permutation, we can produce an (unique) string $1^{a_1} 2^{a_2} \cdots n^{a_n}$ where a_i is the number of cycles of length i. We call such a string the "cycles type" of a permutation. So the above corollary means that two permutations are in the same conjugacy class if and only if they have the same cycle type. It is then curious to consider the size of each conjugacy class.

Definition 9.6. The stabiliser of an element g under the conjugacy action is the centraliser, written as $C_G(g)$.

Lemma 9.9. *If* $\tau \in S_n$ *has cycle type* $1^{a_1} 2^{a_2} \cdots n^{a_n}$*, then*

$$|C_G(\tau)| = 1^{a_1}(a_1)!2^{a_2}(a_2)! \cdots n^{a_n}(a_n)!$$

Proof. Obvious. □

Corollary 9.10. *The size of the conjugacy class containing* τ *is*

$$\frac{n!}{1^{a_1}(a_1)!2^{a_2}(a_2)! \cdots n^{a_n}(a_n)!}$$

where a_i *are defined as before.*

Proof. Orbit-Stabiliser. □

Example 9.2. Consider S_4, then the conjugacy classes are of sizes 1 (consisting of e only and have cycle type 1^4), 6 (of type $1^2 2^1$), 3 (of type 2^2), 8 (of type $1^1 3^1$), and 6 (of type 4^1) by the formula. We do have $1+6+3+8+6 = 24 = 4! = |S_4|$. Note that given the number of conjugacy classes that we expect, it is trivial to work out what are the elements.

Corollary 9.11. *Any normal subgroup of a finite group G is an union of conjugacy classes of G.*

Proof. If $h \in H$ is in one of the conjugacy class, then by normality $ghg^{-1} \in H$ for any g, so the entire conjugacy class is in H. □

Example 9.3. We try to find the normal subgroups of S_4. Let $H \trianglelefteq S_4$, then H must contain the conjugacy class $\{e\}$. If H contains the conjugacy class $1^2 2^1$, then since transpositions generates S_4, H is the entire group S_4.
If H contains the conjugacy class 2^2, then it contains the normal subgroup K consisting of the conjugacy classes $1^4, 2^2$ only. We the case $H > K$ means that H contains more than 2 conjugacy classes, so we can discuss this case later by considering other conjugacy classes.
If H contains the conjugacy class 3^1, then it contains all 3-cycles, which there are 8 of them, so $|H| \geq 9$, so we must have $|H| = 12$ or 24. Note that 3-cycles are even, so $H \cap A_4$ contains all 3-cycles, which have at least 9 elements, thus $H \cap A_4 = A_4$, so $H = A_4$ or $H = S_4$.
If H contains the conjugacy class 4^1, but then it contains at least one 3-cycles (e.g. $(1\ 2\ 3\ 4)(1\ 4\ 2\ 3) = (2\ 4\ 3)$), but since H is normal it in fact contains all 3-cycles, then it is just the same as the previous case (where, since $(1\ 2\ 3\ 4)$ is odd, we have $H = S_4$).
So H is one of K, A_4, S_4.
We have $S_4/S_4 \cong \{e\}, S_4/A_4 \cong C_2, S_4/K \cong S_3$.

As $A_n \trianglelefteq S_n$, for $\sigma \in A_n$, $\operatorname{ccl}_{A_n}(\sigma) \subseteq \operatorname{ccl}_{S_n}(\sigma)$, but the equality may not hold. For example, $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are even and conjugates of each other in S_3, but they are not in A_3 which is abelian. On the other hand, in S_5, we have, however, $[(2\ 3)(4\ 5)](1\ 2\ 3)[(2\ 3)(4\ 5)]^{-1} = (1\ 3\ 2)$, and $(2\ 3)(4\ 5)$ is even, so they are conjugate in A_5 in this case.
For $\sigma \in A_n$, we have

$$|A_n|/|\operatorname{ccl}_{A_n}(\sigma)| = |C_{A_n}(\sigma)|, |S_n|/|\operatorname{ccl}_{S_n}(\sigma)| = |C_{S_n}(\sigma)|$$

But we also have $|S_n| = 2|A_n|$, so either the conjugacy classes are the same, which implies $|C_{A_n}(\sigma)| = |C_{S_n}(\sigma)|/2$. Otherwise, $|\operatorname{ccl}_{A_n}(\sigma)| = |\operatorname{ccl}_{S_n}(\sigma)|/2$ and $C_{A_n}(\sigma) = C_{S_n}(\sigma)$.
Thus either the centraliser of σ contains an odd element and the conjugacy classes are the same or the centralisers of σ is contained in A_n and the conjugacy class in A_n is half the size of that in S_n.

Example 9.4. Consider S_4 and A_4. We look at the conjugacy classes in S_4 and study whether they split in A_4. $\{e\}$ itself constitutes a conjugacy class, so there is nothing to show. The conjugacy class $1^2 2^1$ of transpositions is all odd, thus does not lie in A_4. 2^2 in S_4 are double transpositions, which are even, so it do lie in A_4, but there are only 3 elements, so it cannot split. On the other hand, $(1\ 2)$ centralises $(1\ 2)(3\ 4)$, so the centraliser does contain an odd element.

The conjugacy class $1^1 3^1$ are even so do lie in A_4. And the centraliser of it is contained in A_4, i.e. all even elements, so the conjugacy class splits into two. Indeed, they splits to give $\{(1\ 2\ 3), (1\ 4\ 2), (1\ 3\ 4), (2\ 4\ 3)\}$ and $\{(1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\}$.
The 4-cycles in S_4 are odd, so do not lie in A_4, hence again there is nothing to show.

We can also use it to search for normal subgroups of A_4.

Example 9.5. By definition a normal subgroup of A_4 must be the union of conjugacy classes. Then we could either have $\{e\}$, or K, constituting of $\{e\}$ with all the double transpositions. Note that if the normal subgroup contains one of the $1^1 3^1$ conjugacy classes, it must contain the other one which constitutes the inverses of it. Hence it must contain at least 9 elements, but $|A_4| = 12$, so it can only be A_4. Therefore the normal subgroups are $\{e\}, K, A_4$.

In particular, A_4 is not simple.

Theorem 9.12. *A_5 is simple.*

In fact, A_n is simple for any $n \neq 4$.

Proof. S_5 has 120 elements, and its conjugacy classes can be summarized as $1^5, 1^3 2^1, 1^1 2^2, 1^2 3^1, 2^1 3^1, 1^1 4^1, 5^1$, we can have the following table

Cycle type	1^5	$1^3 2^1$	$1^1 2^2$	$1^2 3^1$	$2^1 3^1$	$1^1 4^1$	5^1
Size	1	10	15	20	20	30	24
Sign	+	-	+	+	-	-	+

By looking at whether the conjugacy class split for a typical even permutation of each cycle type, we conclude the following sizes of conjugacy classes in A_5.

Cycle type	1^5	2^2	3^1	5^1	5^1
Size	1	15	20	12	12

Thus there is no way to sum them up (where we must of course add the first cycle type that is the identity) to produce a factor of $|A_5| = 60$. Therefore A_5 is simple. □

10 Linear Groups

In this section, let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. Let $M_{n\times n}(\mathbb{F})$ be the set of $n \times n$ matrices with entries in $\mathbb{F}$. Matrix multiplication then gives us a binary operation on $M_{n\times n}(\mathbb{F})$. I_n is certainly an identiy element of this operation, so $M_{n\times n}(\mathbb{F})$ is a monoid under this operation.

Proposition 10.1. *An $n \times n$ matrix is invertible iff its determinant is nonzero.*

Proof. In Vectors & Matrices. □

Definition 10.1. The set of $n \times n$ matrix with entries in $\mathbb{F}$ which has inverses, written as $\mathrm{GL}_n(\mathbb{F})$, is a group under matrix multiplication. Equivalently, by the preceding proposition, $\mathrm{GL}_n(\mathbb{F})$ consists of all $n \times n$ matrices with nonzero determinant.

The map $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^\times = (\mathbb{F} \setminus \{0\}, \times, 1)$ is a (surjective) group homomorphism since $\det(AB) = \det(A)\det(B)$.

Definition 10.2. The kernel of det is called the special linear group $\mathrm{SL}_n(\mathbb{F})$, which consists of all $n \times n$ matrices M with $\det M = 1$.

So $\mathrm{SL}_n(\mathbb{F}) \trianglelefteq \mathrm{GL}_n(\mathbb{F})$. By Theorem 8.5, we have $\mathrm{GL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F}) \cong \mathbb{F}^\times$. The group $\mathrm{GL}_n(\mathbb{F})$ acts on $\mathbb{F}^n$ by $M \star x = Mx$ (here x is written as column vector). This corresponds to a homomorphism $\rho : \mathrm{GL}_n(\mathbb{F}) \to \mathrm{Sym}(\mathbb{F}^n)$. Note that ρ is injective by considering the action of a matrix on the standard basis. Also, the image of ρ, which is isomorphic to $\mathrm{GL}_n(\mathbb{F})$ by Theorem 8.5, is precisely the set of invertible linear maps $\mathbb{F}^n \to \mathbb{F}^n$.

Proposition 10.2. *If A is a $n \times n$ matrix represents a linear transformaton $\alpha : \mathbb{F}^n \to \mathbb{F}^n$ in the standard basis $\{e_i\}$. If we have another basis $\{f_i\}$, then in the new basis, α is represented by $P^{-1}AP$ where P is the (invertible) matrix with entries determined by the linear combination of f_j by $\{e_i\}$. That is*

$$f_j = \sum_{i=1}^{n} P_{ij} e_i$$

Group theoretically, the group $\mathrm{GL}_n(\mathbb{F})$ can act on the set of all $n \times n$ matrices, so the orbit of A under this action is all matrices in the form $P^{-1}AP$, that is, the matrices that actually represents the "same" linear transformation but in different basis.

Proof. It is easy to check that conjugating by invertible matrix is indeed an action, and the formula is just verification. □

Example 10.1. 1. Every complex matrix is conjugate to a matrix in the Jordan normal form. For 2-dimensional matrices, any complex 2×2 matrix is conjugate to one of

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \lambda_1 \neq \lambda_2; \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}; \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

One can see easily by looking at eigenvalues that no two of them are conjugate to each other. Also, for different value of λ, in the latter two cases, any two matrices of the same type are not conjugate to each other either. In the first, case, $\mathrm{diag}(\lambda_1, \lambda_2), \mathrm{diag}(\mu_1, \mu_2) \iff \{\lambda_1, \lambda_2\} = \{\mu_1, \mu_2\}$.
Now we consider the stabilisers of them. Consider an invertible matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then a matrix of the first type is stabilised by it iff $b = c = 0$, and every invertible matrix stabilises a matrix of the second type. For the third type, if this matrix does stabilise a matrix of that kind, then we need $c = 0, a = d$, so the stabilisers are the matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$.
2. Consider Mobius transformations $f(z) = \frac{az+b}{cz+d}, f'(z) = \frac{a'z+b'}{c'z+d'}$, then $f \circ f' = \frac{a''z+b''}{c''z+d''}$ where we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

which implies a homomorphism $\phi : \mathrm{SL}_2(\mathbb{C}) \to \mathcal{M}$. This homorphism is surjective since multiplying all of a, b, c, d by a nonzero complex number does not

change the Mobius transformation. How about the kernel of ϕ? Suppose

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \mathrm{id}$$

So $az+b = (cz+d)z$ which has to be true for all $z \in \mathbb{C}$, hence $c = 0, d = a, b = 0$. This implies that the matrix is either I or $-I$. By Theorem 8.5,

$$\mathrm{PSL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})/\{\pm I\} \cong \mathcal{M}$$

Definition 10.3. The n^{th} orthogonal group is defined by

$$\mathrm{O}(n) = \{P \in \mathrm{GL}_n(\mathbb{R}) : PP^\top = I\}$$

Note that $PP^\top = I \iff P^\top P = I$. This is a group since

$$\forall P, Q \in \mathrm{O}(n), (PQ^{-1})(PQ^{-1})^\top = (PQ^\top)(PQ^\top)^\top = PQ^\top QP^\top = I$$

therefore $PQ^{-1} \in \mathrm{O}(n)$. Also $I \in \mathrm{O}(n)$, hence $\mathrm{O}(n) \neq \varnothing$, so indeed $\mathrm{O}(n) \leq \mathrm{GL}_n(\mathbb{R})$.
In addition, the columns of an orthogonal matrix forms an orthonormal basis for $\mathbb{R}^n$, and the converse is also true.

Lemma 10.3. *Let $P \in \mathrm{GL}_n(\mathbb{R})$, then $P \in \mathrm{O}(n) \iff \forall v, w \in \mathbb{R}^n, (Pv) \cdot (Pw) \iff v \cdot w$.*

Proof. Trivial. □

Corollary 10.4. *Any orthogonal matrix preserves lengths and angles.*

Proof. Immediate. □

Note that $\det(A^\top) = \det(A)$, so $\forall P \in \mathrm{O}(n), \det P = \pm 1$.

Definition 10.4. The n^{th} special orthorgonal group $\mathrm{SO}(n)$ consists of orthogonal matrices with determinant 1.

Or equivalently, $\mathrm{SO}(n) = \ker(\det|_{\mathrm{O}(n)})$, so immediately we have $\mathrm{SO}(n) \trianglelefteq \mathrm{O}(n)$.
Typical examples of non-special orthogonal matrices are refections. For an unit vector $a \in \mathbb{R}^n$, we can consider the reflection $R_a : v \mapsto v - 2(v \cdot a)a$. This is obviously linear and can be geometrically interpreted as reflection. So if we choose a basis for $\mathbb{R}^n$ which consists of a and an orthonormal basis for the subspace $a^\perp = \{v \in \mathbb{R}^n : v \perp a\}$, then the union of them gives an orthonormal basis for $\mathbb{R}^n$, which induces the orthogonal matrix representing the reflection. Alternatively we can evaluate to get $R_a(v) \cdot R_a(w) = v \cdot w$ for every $v, w \in \mathbb{R}^n$. But by its form in our specially chosen basis, we have $\det R_a = -1$, so $R_a \in \mathrm{O}(n) \setminus \mathrm{SO}(n)$.

Lemma 10.5.

$$\mathrm{SO}(2) = \left\{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R}\right\}$$

Proof. Consider any $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SO}(2)$, then since we have $AA^\top = I$, $a = d, b = -c$. Then $1 = ad - bc = a^2 + b^2$, so $a, b \in [-1, 1]$, so we can write $a = \cos\theta$, consequently $b = -\sin\theta$ (the sign does not matter since we can always do $\theta \mapsto -\theta$). The lemma follows. □

Note that for $A \in \mathrm{O}(2) \setminus \mathrm{SO}(2)$, we have $a = -d, b = c$ and $a^2 + c^2 = 1$, therefore

$$\mathrm{O}(2) \setminus \mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix} : \phi \in \mathbb{R} \right\} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mathrm{SO}(2)$$

One immediately have the following corollaries.

Corollary 10.6. $\mathrm{O}(2) \setminus \mathrm{SO}(2)$ *consists of reflections.*

Corollary 10.7. *Everything in* $\mathrm{O}(2)$ *is a product of at most* 2 *reflections.*

Remark. Corollary 10.7 can be generalized to $\mathbb{R}^n$ by induction (with, of course, the replacement of 2 by n).

We proceed to analyze the rotations and reflections in $\mathbb{R}^3$.

Theorem 10.8. *Let* $A \in \mathrm{SO}(3)$*, then there is an unit vector* $v \in \mathbb{R}^3$ *such that* $Av = v$*.*

Proof. Suffice to show that A has eigenvalue 1. Indeed, $\det(A - I) = \det(A^\top - I) = \det A \det(A^\top - I) = \det(I - A) = (-1)^3 \det(A - I) = -\det(A - I)$, hence $\det(A - I) = 0$. □

In fact, we can generalize 3 to any $2n + 1$ for $n \in \mathbb{N}$ using exactly the same way.

Corollary 10.9. *Every* $A \in \mathrm{SO}(3)$ *is conjugate to a matrix in the form*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

Proof. By the theorem there is some unit vector $f_1 \in \mathbb{R}^3$ such that $Af_1 = f_1$. And choose an orthonormal basis f_2, f_3 of $f_1^\perp$, so that f_1, f_2, f_3 is an orthonormal basis of $\mathbb{R}^3$. Then for $i = 2, 3$, we have $(Af_i) \cdot f_1 = (Af_i) \cdot (Af_1) = f_i \cdot f_1 = 0$. So Af_i is a linear combination of f_2, f_3 only. Hence in this new basis, the matrix will look like

$$A' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

By computing $A'A'^\top = I$, we find

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

for some θ. The result follows. □

Note that we can manipulate the change-of-basis matrix to make it special orthogonal.

Corollary 10.10. *Every element in* $\mathrm{O}(3)$ *is the composition of at most* 3 *reflections.*

Proof. Every element in SO(3) is the composition of two reflections by observing

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(-\theta) & \sin(-\theta) \\ 0 & \sin(-\theta) & -\cos(-\theta) \end{pmatrix}$$

and using Corollary 10.9. Now choose any reflection R, then $\mathrm{O}(3) \setminus \mathrm{SO}(3) = R\,\mathrm{SO}(3)$, therefore every other element in O(3) is a composition of at most 3 reflections. □

11 Bonus Lecture: Simple Groups of Order 60

Consider $\mathrm{GL}_2(\mathbb{Z}_5)$. We first want to find the size of this group. It is easy to see that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_5)$$

is invertible if annd only if $ad-bc$ has a multiplicative inverse, that is, is nonzero. Take $U_5 \subset \mathbb{Z}_5$ to be the set of elements in $\mathbb{Z}_5$ having multiplicative inverse, that is, $U_5 = \mathbb{Z}_5^\times = \mathbb{Z}_5 \setminus \{0\}$. There are $5^4 = 625$ 2×2 matrices in total. Amongst them, the number of non-invertible ones satisfies $ad \equiv bc \pmod 5$.
Case 1: $a = 0$, then $bc = 0$, so either $b = 0$ (which gives 25 choices) or $c = 0$ (which gives, again, 25 choices). There are double-counted cases where $b = c = 0$ and there are 5 cases, so there is a total of 45 choices.
Case 2: $a \neq 0$, then we can solve for d given b, c. Indeed, for any b, c, we can have an unique corresponding d, hence there are $4 \times 5^2 = 100$ choices.
So there are a total of 145 non-invertible matrices and thus 480 invertible matrices. There are still a lot of elements, so we want to think about $\mathrm{SL}_2(\mathbb{Z}_5)$. But since $\det : \mathrm{GL}_2(\mathbb{Z}_5) \to \mathbb{Z}_5^\times$ is a surjective homomorphism with kernel $\mathrm{SL}_2(\mathbb{Z}_5)$, so $|\,\mathrm{SL}_2(\mathbb{Z}_5)| = 120$. Also note that $\mathrm{PSL}_2(\mathbb{Z}_5) \cong \mathrm{SL}_2(\mathbb{Z}_5)/\{\pm I\}$, then $|\,\mathrm{PSL}_2(\mathbb{Z}_5)| = 60$. We can analyze the conjugacy classes in $\mathrm{PSL}_2(\mathbb{Z}_5)$ to find out that they look exactly like that in A_5. In fact they are isomorphic.

Theorem 11.1. $\mathrm{PSL}_2(\mathbb{Z}_5) \cong A_5$.

Proof. Let $G = \mathrm{PSL}_2(\mathbb{Z}_5)$. Take the subgroup

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix} \right\} \leq G$$

so the three non-identity elements in H has order 2 and since there is only one conjugation class of element of order 2, so the conjugates of H contains all element of order 2. Since there are 15 elements of order 2 and H contains 3 elements of order 2, there must be at least 5 conjugates of H. We want to show there are precisely 5 of them. Consider the action G on the set X of the subgroups of G by conjugation, then the stabiliser G_H (the normalizer) satisfies $|G_H| \times |G \star H| = |G| = 60$. Note that $H \leq G_H$, hence $4||G_H|$, therefore $|G \star H||15$. If $|G \star H| = 15$, we know that there are only 15 elements of order 2, some pair of conjugates have 3 elements in common (counting identity), but then they must be the same, contradiction. So $|G \star H| = 5$ as claimed. The action of G on $G \star H$ then gives a homomorphism $\rho : G \to S_5$.
Now G is simple by the same argument we used to show the simplicity of A_5

since they have the same table of sizes of conjugacy classes. Hence ρ is injective (since ρ is obviously not constant), so $G \cong \operatorname{Im}\rho$ which has index 2 in S_5, hence is normal in S_5.
Suppose $\operatorname{Im}\rho \neq A_5$, then $\operatorname{Im}\rho \cap A_5 \leq A_5$ has index 2, so $\{e\} \neq \operatorname{Im}\rho \cap A_5 \lhd A_5$, contradiction. Therefore $G \cong \operatorname{Im}\rho \cong A_5$. □

In fact, there is only one simple group of order 60 up to isomorphism.
Now we turn to the symmetry of platonic solids. Note that dual solids have isomorphic symmetries. Let G be the group of all isometries of a platonic solid and and SG the group of all rotational isometries of it. It is fact that $\mathrm{O}(3) \cong \mathrm{SO}(3) \times C_2$. Note $S_4 \ncong A_4 \times C_2$, since $x \mapsto -x$ is no longer a symmetry of the tetrahedron. Otherwise, we have $G \cong SG \times C_2$.
For cube, we have seen that SG has 24 elements. In fact, $SG \cong S_4$ since it permutes the set of long diagonals (pairs of opposite vertices).
Now symmetries of a regular isocahedron. Let SG act (transitively) on its 12 vertices. The stabiliser of the vertex are the rotations though the axis through the vertex, so it is isomorphic to C_5. So $|SG| = 5 \times 12 = 60$. In fact, again we have $SG \cong A_5$.

Proposition 11.2. *SG is simple.*

Proof. SG contains rotations of order 5 through a vertex and of order 3 through the centre of a face or order 2 through the centre of an edge. So if $H \trianglelefteq SG$ contains a rotation of order 5 around some vertex, then by conjugating we can contain all rotations of order 5 around any vertex. But then H acts transitively on the vertices, and on any pair of vertices, but then one must get all rotations, so $H = SG$. Similar arguments hold if H contains an element of order 2 or 3, hence SG is simple. □

In fact, there are five inscribed tetrahedra in an isocahedra that are permuted by the action of SG, so by the same argument used in showing $\mathrm{PSL}_2(\mathbb{Z}_5) \cong A_5$, we have $SG \cong A_5$.