1 Motivating Example: Dihedral and Permutation Groups

We will use dihedral and permutation groups to motivate a handful of concepts.

Consider a regular n-gon, for $n \geq 3$. For this example we will consider a **symmetry** to be a 'rigid motion in $\mathbb{R}^3$'. Rigid motions are akin to 'picking up' a shape and moving it around so that it covers the same area. These are not precise definitions.

Let D_{2n} be the set of all such symmetries. This will motivate our concept of a 'group'. It doesn't matter how the symmetries are made, just the end result. In this sense, two symmetries are the same if they have the same final position.

Let us fix a labelling of the verticies (i.e., assign each vertex a label 1, 2, 3, ...). An element of D_{2n} determines and is determined by how it permutes the verticies.

Definition 1.1: Permutation

A **permutation** of a set X is a bijection

$$\sigma : X \to X$$

We let S_X be the set of permutations of X and $S_n = S_{\{1,2,\cdots,n\}}$.

We can see without much trouble that $D_{2n} \subset S_n$. We view $\sigma \in D_{2n}$ as the permutation $\{1, \cdots, n\} \to \{1, \cdots, n\}$ where $i \mapsto$ the vertex that the symmetry σ takes i to. But not all permutations are symmetric!

Example 1.1: Permutations that aren't symmetric

Let $n = 4$ and consider the n-gon (in fact, a square). Let $\sigma : (1, 2, 3, 4) \to (2, 1, 3, 4)$. We can see that because the verticies aren't fixed in relation with each other that this is not a rigid motion (although they are valid permutations of the verticies). Thus, $\sigma \notin D_{2n}$.

In general, we should note that $D_{2n} \neq S_n$. In fact, we claim that $|S_n| = n!$ and $|D_{2n} = 2n$.

Notice that we can 'multiply' in D_{2n} by way of composition, we can reverse any permutation in D_{2n} (i.e., there is an inverse), and theres an element that does nothing. We will shortly see that D_{2n} is in fact a group.

2 Introduction to groups

Definition 2.1: Group

A **group** is a nonempty set G equipped with a binary operation $* : G \times G \to G$ satisfying three conditions:

1. Associativity: $a * (b * c) = (a * b) * c$
2. Identity: $\exists e \in G \ni a * e = e * a = a$
3. Inverse: $\exists a^{-1} \in G \ni a * a^{-1} = a^{-1} * a = e$

for any $a, b, c \in G$.

Definition 2.2: Subgroup

A **subgroup** of a group $(G, *)$ is a nonempty subseteq $H \subseteq G$ that is closed under $*$ and inverses. I.e., for $a, b \in H$:

1. $a * b \in H \subseteq G$
2. $a^{-1} \in H \subseteq G$

Remarks:

1. $H \leq G$ is the notation for H as a subgroup of G.
2. Defining $*|_{H\times H} H \times H \to H$ makes $(H, *|_{H\times H})$ a group. In fact, we call this the induced group structure on H.

Example 2.1: Examples of groups

1. The nonzero real numbers $\mathbb{R}^\times$
2. $GL_n(\mathbb{R})$, the set of $n \times n$ invertible real matricies.
3. S_n, the group of all permutations.

Definition 2.3: Abelian

A group $(G, *)$ is called **abelian** if $*$ is commutative. I.e., for any $a, b \in G$ we have that $a * b = b * a$.

Remarks:

1. (Multiplicative Notation): We often write ab for $a * b$, and we tent to write 1 for e. This is standard abuse of notation.
2. (Additive notation): If we are working with a group $(G, *)$ that we know is abelian, we will often write $a + b$ instead of $a * b$ and 0 instead of e. We also write $-a$ instead of a^{-1}. This additive notation is never used if we are unsure of the commutativity of the group.

Proposition 2.1: P1

Suppose that G is a group.

Proposition 2.2: P1a

The identity element is unique.

Suppose $e, e' \in G$ are both identity elements. Then $e = e'e = e'$ since both e, e' are identites.

Proposition 2.3: P1b

For each $a \in G$, a has a unique inverse.

Suppose $b, c \in G$ are both inverses of a. Then $ab = 1 = ac$ since b and c are both inverses. Then $b(ab) = b(ac) \implies (ba)b = (ba)c \implies b = c$

Proposition 2.4

$\left(a^{-1}\right)^{-1} = a$

Since $a^{-1}a = aa^{-1}$, we see that a is the inverse of a^{-1} by definition.

Proposition 2.5

$\left((ab)^{-1} = b^{-1}a^{-1}\right)$

$$\begin{aligned}\left(b^{-1}a^{-1}\right)(ab) &= \left(b^{-1}\right)\left(a^{-1}a\right)(b) && \text{by associativity}\\ &= \left(b^{-1}b\right)\\ &= 1\end{aligned}$$

Thus we have that $\left(b^{-1}a^{-1}\right)$ is the left inverse of (ab). Similarly, show that $\left(b^{-1}a^{-1}\right)$ is a right inverse.

Proposition 2.6: Generalized Associativity

For $a_1, \cdots, a_n \in G$ we have that $a_1a_2\cdots a_n$ is 'the same no matter how the expression is bracketed'. Proof as exercise

Proposition 2.7

In any group G, $1^{-1} = 1$

Notation: For $a \in G$ and $n > 0$ we write $a^n = a \cdot a \cdot \cdots \cdot a$. Also, $a^0 = 1$ and $a^{-n} = (a^n)^{-1}$.

Proposition 2.8: Cancellation Law

For any $a, b, u, v \in G$, the **left cancellation** is $au = av \implies u = v$. The **right cancellation** law is $ub = vb \implies u = v$.
Proof sketch: Use the property that every element in the group has an element that is both a left and right inverse.

Definition 2.4: Homomorphism

A **group homomorphism** $\phi : G \to H$ with $(G, *); (H, \cdot)$ as groups is a function with the property that for all $a, b \in G$:

$$\phi(ab) = \phi(a)\phi(b)$$

To avoid abuse of notation we may write that $\phi(a * b) = \phi(a) \cdot \phi(b)$ This is also called a **morphism of groups**.

Definition 2.5: Isomorphism

A homomorphism $\phi : G \to H$ is called an **isomorphism** if ϕ is bijective. We write $G \simeq H$ and say that G is **isomorphic** to H if there exists that bijective function ϕ.

Proposition 2.9: P3

If $\phi : G \to H$ is a group homomorphism then:

1. $\phi(1_G) = 1_H$
2. $\forall a \in G$, $\phi(a^{-1}) = (\phi(a))^{-1}$

Consider the fact that $1_H\phi(1_G) = 1_H\phi(1_G1_G)$. Since ϕ is a homomorphism, then $1_H\phi(1_G1_G) = 1_H\phi(1_G)\phi(1_G) = \phi(1_G)\phi(1_G)$. Thus we have that $\phi(1_G) = 1_H$.
Now consider that $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1_G) = 1_H$. We show this similarly for $\phi(a)\phi(a^{-1})$. Then we have that $\phi(a^{-1}) = (\phi(a))^{-1}$.

Definition 2.6: Kernel

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

$$\ker(\phi) = \{a \in G | \phi(a) = 1_H\}$$

Proposition 2.10: P4

Let $\phi : G \to H$ be a group homomorphism. Then $\ker(\phi) \leq G$.

We need to show that $\ker(\phi)$ is a subgroup. Suppose that $a, b \in \ker(\phi)$. Observe that since $a, b \in \ker(\phi)$ that $\phi(ab) = 1_H$ so that $ab \in \ker(\phi)$. Similarly, observe that $\phi(a^{-1}) = (\phi(a))^{-1} = 1_H$ so $a^{-1} \in \ker(\phi)$. The kernel must also be nonempty since $\phi(1_G) = 1_H$.
We have shown that $\ker(\phi)$ is closed under group operation, inverses and is nonempty. Thus it is a subgroup.

Definition 2.7: Inverse to the group homomorphism

If $\phi : G \to H$ is a group homomorphism, then an **inverse** to ϕ is a group homomorphism $\psi : H \to G$ such that $\psi \circ \phi = 1_G$. Similarly $\phi \circ \psi = 1_H$.

Exercise: A group homomorphism is an isomorphism if and only if it has an inverse group homomorphism.

Proposition 2.11: P5

Suppose $\phi : G \to H$ is a surjective group homomorphism. If G is abelian, then so is H.

Let $a, b \in H$ with $a = \phi(r), b = \phi(s)$ for $r, s \in G$. Then we have that

$$ab \underset{\text{surjection}}{=} \phi(r)\phi(s) \overset{homomorphism}{=} \phi(rs) \underset{G \text{ is abelian}}{=} \phi(sr) \underset{\text{homomorphism}}{=} \phi(s)\phi(r) = ba$$

Corollary: $G \simeq H \implies (G \text{ abelian} \iff H \text{ ablelian})$.

Example 2.2

Let G, H be the groups $G = (\mathbb{Z}_4, \oplus)$ and $H = \left(\mathbb{Z}_5^\times, \otimes\right)$ where $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$ with identity 1.
Let $\phi : G \to H$ with $\phi(0) = 1; \phi(1) = 2; \phi(2) = 3; \phi(3) = 4$.
We see that

$$\phi(1 \oplus 1) = \phi(2) = 3\phi(1) \otimes \phi(1) = 2 \otimes 2 = 4$$

Since $\phi(1 \otimes 1) \neq \phi(1 \oplus 1)$ we have that ϕ is not a group homomorphism. This doesn't imply that $G \not\simeq H$, though! Because in fact, $G \simeq H$.

$$\psi(0) = 1; \psi(1) = 2; \psi(2) = 4; \psi(3) = 3$$

as one can check for themselves, is an isomorphism.

subsectionGroup Actions

Definition 2.8: Group Action

A (left) **group action** of a group G on a set A is a function $G \times A \to A$ denoted by $\cdot$. I.e., for $g \in G, a \in A$ a mapping $(g, a) \mapsto g \cdot a \in A$ satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = \begin{pmatrix} \text{operation in } G \\ g_1 g_2 \end{pmatrix} \underset{\text{group action}}{\cdot} a$
2. $1_G \cdot a = a$

If G acts on A , for each $g \in G$ we may define the functions:

$$\begin{aligned} \sigma_g : A &\to A \\ a &\mapsto g \cdot a \end{aligned}$$

Lemma 2.1: L6

G acts on A, $g \in G$. Then $\sigma_g : A \to A$ is a bijection.

Injectivity: Let $a, b \in A$. Suppose that $\sigma_g(a) = \sigma_g(b)$. Then, we have that $g\dot{a} = g\dot{b}$. Then $g^{-1}(g \cdot a) = g^{-1}(g \cdot b)$. Then we use the compatability with multiplication property of group actions:

$$(g^{-1}g) \cdot a = \left(g^{-1}g\right) \cdot b \implies 1 \cdot a = 1 \cdot b$$

Then $a = b$ so σ_g is injective.
Surjectively: Given $b \in A$, let $a := g^{-1} \cdot b$. $\sigma_g(a) = \sigma_g(g^{-1} \cdot b) = g \cdot (g^{-1} \cdot b) = (gg^{-1}) \cdot b = b$. Thus we have that σ_g is surjective.
Thus, σ_g is bijective.

Warning: Do not confuse the action of G on A and the grou operation in G, since they use similar notation (lazy fucks like us drop $a \cdot b$ to ab.

Recall that for any set A, we define $S_A :=$ group of bijections $\sigma : A \to A$ under composition. If G acts on A we have just defined a function

$$\begin{aligned} G &\to S_A \qquad \text{by lemma 6} \\ g &\mapsto \sigma_g \end{aligned}$$

Proposition 2.12: P7: Permutation Representation

The function $G \to S_A$ given by $g \mapsto \sigma_g$ is a group homomorphism.

Exercise: Prove the converse of P7.

Definition 2.9: Trivial Homomorphism

Let G, H be groups. The **Trivial Homomorphism** $\phi : G \to H$ is $\phi(g) = 1_H$ for all $g \in G$. That is, $\ker(\phi) = G$.

Definition 2.10: Kernel of the action

Suppose that G acts on A and $\phi : G \to S_A; g \mapsto \sigma_g$ is the corresponding homomorphism. We call $\ker(\phi) \leq G$ the **kernel of the action of G on A**. It is the set of elements in G that act trivially on A.

Last time: Left cosets and Lagrange's Theorem.

Remark: We could have also considered right cosets. i.e., $a \in G, H \leq G, H_a := \{ha | h \in H\}$.

Definition 2.11: Quotient group? Set of left cosets

Let $H \leq G$. Then we have that:

$$G/H := \text{ the set of all left cosets of } H \in G \qquad := \{ah | a \in G\} \tag{1}$$

We have a natural action of G on G/H given by:

$$g \cdot aH := (ga)H$$

for $g \in G$.

The kernel of this action

$$= \{g \in G | gaH = aH \, \forall a \in G\} \tag{2}$$
$$= \{g \in G | a^{-1}ga \in H \, \forall a \in G\} \tag{3}$$
$$\tag{4}$$

What subgroup is this? We'll come back to it.

Recall the kernel of an action: If G acts on A then we have a group homomorphism $G \to S_A$. The kernel of the action is the kernel of this homomorphism. I.e., $ker = \{g \in G | ga = a \forall a \in A\}$.

Example 2.3: Left cosets generalize congruence classes

1. Let $G = (\mathbb{Z}, +)$ with $H = d\mathbb{Z} \leq \mathbb{Z}$ fix $d > 0$. Consider $\mathbb{Z}/d\mathbb{Z}$.

$$\begin{aligned}\mathbb{Z}/d\mathbb{Z} &= \{a + d\mathbb{Z} | a \in \mathbb{Z}\} \\ &= \{[a]_d | a \in \mathbb{Z}\}\end{aligned}$$

where $[a]_d = \{n \in \mathbb{Z} | n \equiv a (mod d)\} = a + d\mathbb{Z}$. So the congruence class of $a \mod d$ is just the left coset of $d\mathbb{Z}$ by a. One way we can think of this is a generalization of congruence classes to any group. This has a natural group structure. That is, $[a]_d + [b]_d = [a + b]_d$. $d\mathbb{Z}$ is all integer multiples of d (i think?).

Now, lets try to put a natural group structure on G/H. $(aH)(bH) := abH$.

But in general, given any two subsets $X \subseteq G, Y \subseteq G$ of a group G we have that $XY := \{xy | x \in X, y \in Y\} \subseteq G$.

If $X = aH, Y = bH$ then $XY = \{ah_1bh_2 | h_1, h_2 \in H\}$, and $abH = \{abh | h \in H\}$. We see that $abH \subseteq XY$, and that in general, $XY \nsubseteq abH$. Although if G is abelian, then we do have that $XY = abH$ and then $(aH)(bH) := abH$ is a good definition for a group structure on G/H.

But this is a strong assertion. In fact, for our definition to be nice, all we need is for $h_1 \in H$ that $h_1 b = bh'$ for some $h' \in H$. Then we have that $ah_1bh_2 = abh'h_2 = abh$.

Definition 2.12: Normal subgroup

A subgroup $H \leq G$ is **normal** if for every $b \in G, Hb = bH$. i.e., $\forall h \in H \exists h' \in H \ni hb = bh'$.
We denote a normal subgroup by $H \triangleleft G$. (Read: H triangle G)

Recall prop. 11 is the proposition about left cosets, and prop 12. was Lagrange's theorem.

Proposition 2.13: Normal subgroup equivalencies

Let $H \subset G$. Then the following are equivalent:
1. $H \triangleleft G$
2. $b^{-1}Hb \subseteq H \forall b \in G$
3. $b^{-1}Hb = H$

(i) $\iff$ (iii): Let $H \triangleleft G$ and $b \in G$. We have that $Hb = bH \iff b^{-1}Hb = H$.

$$\begin{aligned}Hb &= \{hb | h \in H\} \\ bH &= \{bh | h \in H\} \\ b^{-1}Hb &= \{b^{-1}hb | h \in H\}\end{aligned}$$

(iii) $\implies$ (ii): This is clear (if they are equal, then one is contained within the other).
(ii) $\implies$ (iii): Apply (ii) to b^{-1}. Then we have that $\left(b^{-1}\right)^{-1} H \left(b^{-1}\right) \subseteq H$. Then:

$$\begin{aligned}bHb^{-1} &\subseteq H \\ Hb^{-1} &\subseteq b^{-1}H \\ H &\subseteq b^{-1}Hb \\ H &= b^{-1}Hb\end{aligned}$$

Proposition 2.14: lemma

Proof as an exercise. This is what motivated the definition of normal!

Remark: Suppose $H \triangleleft H$. Let G act on G/H. The kernel of the action is H. ProoF: Let $h \in H, a \in G$. Then $haH = ah'H$ since H is normal to G. Then $haH = aH$. Thus h is in the kernel of the action. Now suppose $g \in G$ is in the kernel of the action. So $gaH - aH$ for all a. In particular, let $a = 1$. So then $gH = H$. By proposition 11a, we must have that $g \in H$. Thus H is the kernel of the action.

subsectioncyclic subgroups

Definition 2.13: Cyclic Subgroups

Let G be a group with $a \in G$. The **cyclic cubgroup of G generated by a** is $\langle a \rangle := \{a^n | n \in \mathbb{Z}\}$.

Proposition 2.15: P15

Let G be a group, $a \in G$.

1. $\langle a \rangle \leq G$.

   $$a^n a^m = a^{n+m} \in \langle a \rangle$$
   $$(a^n)^{-1} = \left(a^{-1}\right)^n = a^{-n} \in \langle a \rangle$$
   $$1 = a^0 \in \langle a \rangle$$

2. $\langle s \rangle$ is the smallest subgroup of G that contains a

   $\langle \leq G \rangle$ by part (a). $a \in \langle a \rangle$ since $a = a^{-1}$.
   If $H \leq g$ and $a \in H$ then since H is closed under group multiplication and inverses, $a^n \in H$ for all $n \in \mathbb{Z}$. So $\langle a \rangle \leq H$

3. Suppose order of a is finite, say n. Then $\langle a \rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ and $|\langle a \rangle| = n$.

   If $n = 1$ then $a = 1$. So it is clear that $\langle a \rangle = \{1\}$. Now assume $a > 1$. Let $m \in \mathbb{Z}$, where $m = qn + r$ i.e., $0 \leq r < n$ is the remainder. Then:

   $$a^m = a^{qn+r} = (a^n)^q a^r = 1^q a^r = a^r \in \{1, a, \cdots, a^{n-1}\}.$$

   Therefore for finite order n, $\langle a \rangle = \{1, a, \cdots, a^{n-1}$.
   Now suppose $0 \leq r \leq s < n$ with $a^r = a^s \implies a^{s-r} = a^s a^{-r} = 1$.
   But $0 \leq s - r < n$. By minimality of order, $s - r = 0$. So $1, a, a^2, \cdots, a^{n-1}$ are all distinct and $|\langle a \rangle| = n$.

4. If G is finite then every element of G has finite order.

   $1, a, a^2, \cdots$ cannot all be distinct as G is finite. So for some $s > r \geq 1$, it must be that $a^s = a^r$. So $a^{s-r} = 1$.

5. If G is finite, then $order(a) \mid |G|$.

   By part (a) , we have that $\langle a \rangle \leq G$. By Lagrange's theorem, $|\langle a \rangle| \mid |G|$. By part (d), a has finite order. By part (c) we have that $order(a) = |\langle a \rangle|$

6. If G is finite, $|G| = n$, then a^n.

   By part (d) and (e), the order of a is finite and $order(a) \mid n$. Let $l = order(a)$ for some $n = lk$, $k \in \mathbb{Z}$. Then
   $$a^n = a^{lk} = \left(a^l\right)^k = 1^k = 1$$

7. If $|G|$ is prime, then G is **cyclic**. I.e., $G = \langle a \rangle$ by some $a \in G$.

   Let $a \in G, a \neq 1$. The order of a is finite and $order(a) \mid |G|$. This implies that $order(a) = 1$ or $|G|$. But $order(a) = 1 \implies a = 1$ which is not possible so $order(a) = |G|$. But by part (c), $order(a) = |\langle a \rangle|$. Therefore $\langle a \rangle = G$.

8. Every subgroup of a cyclic group is cyclic.

   Generalization of HW2 Q1. Proof similar.

Now back to subgroups (in general).

Last time we defined $H \triangleleft G$ and we showed if $H \triangleleft H$ then $(aH)(bH) = (ab)H$. I.e., $H \triangleleft G$ says that $bH = Hb$.

Proposition 2.16: P16

If $H \triangleleft G$ then (G/H = the set of all left cosets) is a group under set multiplication. Moreover, $\pi : G \to G/H$ given $\pi(g) = gH$ is a group surjective homomorphism.

Definition 2.14: Quotient group, map

G/H is called the **quotient group** and $\pi : G \to G/H$ is called the **quotient map**

Associtaivity:

$$\begin{aligned}
(aHbH)cH &= (abH)(cH) && \text{by P14}\\
&= (ab)cH && \text{by 14}\\
&= a(bc)H && \text{since } G \text{ associative}\\
&= aHbcH && \text{by 14}\\
&= aH(bHcH) && \text{by 14}
\end{aligned}$$

The inverse of aH is $a^{-1}H$. We have that $aHa^{-1}H = aa^{-1}H = 1H = H_{G/H}$ by 14. Similarly, $a^{-1}HaH = H = 1_{G/H}$. So $(aH)^{-1} = a^{-1}H$.
The identity in G/H is H.

$$aHH = aHHaH = aH$$

Therefore G/H is a group under set multipication.

$$\begin{aligned}
\pi(ab) = abH = aHbH && && \text{by 14}\\
&= \pi(a)\pi(b)
\end{aligned}$$

Remark: $\ker(\pi) = H$. Proof: See that $\pi(a) = 1_{G/H} \iff aH = H \iff a \in H$ by 11a.

Last time: $H \triangleleft G$ then G/H is a group under the set ??? and $\pi : G \to G/h;\ a \mapsto aH$ is a group homomorphism with $\ker(\pi)H$.

Example 2.4: Normal subgroups and quotient maps

1. $\langle 1\rangle = \{1\} \triangleleft G$ $a1a^{-1} = 1$ for any $a \in G$. $\pi : G \to G/\langle 1\rangle$ (Quotient map) π is an ismorphism:

$$\begin{aligned} \pi(a) = \pi(b) &\iff a\langle 1\rangle = b\langle 1\rangle \\ &\iff a = b \end{aligned}$$

   Hence $G \simeq G/\langle 1\rangle$.
2. $H = G \triangleleft G$ since forany $a \in G$, $aGa^{-1} \subseteq G$ and $\pi : G \to G/G$. G/G is the trivial. Got any $a \in G$, $aG = G$.
3. If G is abelian, then every $H \leq G$ is normal i.e., $H \triangleleft G$. $\forall a \in G, h \in H$, we have $aha^{-1} = aa^{-1}h = h \in H$ therefore $aHa^{-1} \leq H$.

   Example 2.5: abelian normal ness

   $G = (\mathbb{Z}, +)$. $H = d\mathbb{Z}$ with $d \geq 0$. $d = 0$ in case (i), $d = 1$ in case (ii), and $d > 1$ $\mathbb{Z}/d\mathbb{Z}$ group of congruence classes modulo d.
4. If $\phi : G \to H$ is a group homomorphism then $\ker(\phi) \triangleleft G$.

   Let $a \in G, b \in \ker(\phi)$.

$$\begin{aligned} \phi(aba^{-1}) &= \phi(a)\phi(b)\phi(a)^{-1} \\ &= \phi(a)\phi(a)^{-1} && \text{since b in kernel} \\ &= 1_H \end{aligned}$$

   Then $a\ker(\phi)a^{-1} \subset$
   So normal subgroups of G are precisely the kernels of homomorphisms on G.
5. Let $G = D_{10}$ be the group of rigid transformations of the regular pentagon dihedral group of order 10. Let $S \in D_{10}$ be a reflection. We see order$(s) = 2$. Then $\langle s\rangle = \{1, 5\} \subseteq D_{10}$. We can see that $\langle s\rangle \not\triangleleft D_{10}$. Let $r = \frac{2\pi}{s}$ be clockwise rotation. $rsr^{-1} = rrs = r^2s \neq 1 \neq s$. Since every element of D_{10} can be written uniquely as r^is^k. So $r^2s \neq 1 \neq s$ and $rsr^{-1} \notin \langle s\rangle$. Therefore $\langle s\rangle$ is not normal to d_{10}.
   On the other hand, $\langle r\rangle = \{1, r, r^2, r^3, r^4\}$. so order $r = 5$. We claim $\langle r\rangle \triangleleft D_{10}$.

   Let $a \in D_{10}$. Let $a = r^is^k$. Let $l \in \{1, 2, 3, 4\}$. $ar^la^{-1} = r^is^kr^ls^{-k}r^{-1}$.
   If $k = 0$: $ar^la^{-1} = r^ir^lr^{-1} = r^l \in \langle r\rangle$.
   If $k = 1$: $ar^la^{-1} = r^i(sr^l)s^{-1}r^{-i} = r^ir^{-l}ss^{-1}r^{-i} = r^{-l} \in \langle r\rangle$.
   Thus $ar^la^{-1} \in \langle r\rangle$ and $a\langle r\rangle a^{-1} \subset \langle\rangle$. Thus $\langle r\rangle \triangleleft d_{10}$.

   Consider now $pi : D_{10} \to D_{10}/\langle r\rangle$ be a quotient map. What is $D_{10}/\langle r\rangle$?
   $|D_{10}| = 10, |\langle r\rangle| = 5$ by Lagrange's theorem. There are exactly two cosets:

$$\begin{aligned} \langle r\rangle &= \{1, r, r^2, r^3, r^4\} \\ s\langle r\rangle &= \{s, sr, sr^2, sr^3, sr^4\} \end{aligned}$$

   Thus $D_{10}/\langle r\rangle$ is a group of size 2.
   Up to isomorphisms, there is only one group with two elements.

   Let $G = \{1, a\}$ with $a \neq 1$.
   Look at the **Caley Graph**.

G	1	a
1	1	a
a	a	a

   We claim $a^2 = 1$ or a. $a^2 = a \implies a = 1$ which is not possible, so $a^2 = 1$.
6. $G = \mathbb{C}^\times$ multiplicative group of complex numbers $S := \{z \in \mathbb{C}^\times \mid |z| = 1\}$.
   $S \leq \mathbb{C}^\times$, $|Zn| = |z||w|$, $|frac1z| = \frac{1}{|z|}$. 11
   We see that $\mathbb{C}^\times$ abelian $\implies S \triangleleft \mathbb{C}^\times$. But what is $\mathbb{C}^\times/S$? In fact, $\mathbb{C}^\times/S \simeq (\mathbb{R}^{>0}, \cdot)$.
   $\pi : \mathbb{C}^\times \to \mathbb{C}^\times/S$.
   A typical element of $\mathbb{C}^\times/S$ is a left coset wS where $w \in \mathbb{C}^\times$.

Given $H \triangleleft G$, consider the quotient map $\pi : G \to G/H$. Given an element $aH \in G/H$, the **fibre** $\pi^{-1}(aH) = aH \subseteq G$. Note: aH is an *element* as the argument of π^{-1}, but its output aH is a *subset*. To see this consider $b \in G$. $\pi(b) = aH \iff bH = aH$.

$$\begin{aligned} &\iff a^{-1}b \in H \iff a^{-1}b = h \text{ for some } h \in H \\ &\iff b = ah \text{ for some } h \in H \\ &= b \in aH \end{aligned}$$

Reminder that $aH = bH \iff a^{-1}b \in H \iff a \in bH \iff b \in aH$.

Since $H = \ker \pi$, the fibres of π are all left cosets of the kernel.

Proposition 2.17: P17?

Let $\phi : G \to H$ be a group homomorphism, and $K = \ker \phi \triangleleft G$. The nonempty fibres of ϕ are the left cosets of K.

Consier $h \in Im(\phi) \leq H$. (h in the image of ϕ which is a subgroup of H). Fix $a \in \phi^{-1}(h) := \{g \in G | \phi(g) = a\}$. We claim that $\phi^{-1}(h) = aK$. Let $b \in G$. Then:

$$\begin{aligned} b \in \phi^{-1} &\iff \phi(b) = h \\ &\iff \phi(b) = \phi(a) \\ &\iff \phi(a)^{-1}\phi(b) = 1_H \\ &\iff \phi(a^{-1}b) = 1_H \\ &\iff a^{-1}b \in K \\ &\iff b \in aK \end{aligned}$$

Thus a fibre is a left coset.
Conversely, let aK be a left coset.

$$\begin{aligned} b \in aK &\implies b = ak \text{ for some } k \in K \\ &\implies \phi(b) = \phi(a)\phi(b) = \phi(a) \text{ since } k \in K = \ker \phi \\ &\implies b \in \phi^{-1}(\phi(a)) \end{aligned}$$

Thus $aK \subseteq \phi^{-1}(\phi(a)) = bK$. But by the previous pary, $\phi^{-1}(\phi(a)) = bK$ for some $b \in G \implies aK = bK = \phi^{-1}(\phi(a))$.

Corollary 2.1: C18

A group homomorphism $\phi : G \to H$ is injective if and only if $\ker \phi = \langle 1 \rangle$.

By the previous proposition (P17) the nonempty fibres of ϕ are cosets of $\ker \phi$.

$$\phi \text{ is injective} \iff \text{the nonempty fibres are singletons}$$

Since $\ker \phi \to a \ker \phi$ $x \mapsto ax$ is a bijection, $a \ker \phi$ is a singleton $\iff$ $\ker \phi$ is a singleton $\iff \ker \phi = \langle 1 \rangle$.

Given $\phi : G \to H$ homormorphism, we know that $\ker \phi \triangleleft G$. Consdier $\pi : G \to G/\ker \phi$ as a quotient homomorphism. We see now that $\ker \pi = \ker \phi$.

Theorem 2.1: Universal Property of Quotients

Suppose $N \triangleleft G$. Then the quotient map $\pi : G \to G/N$ is universal with respect to all group homomorphisms on G whose kernel is contains N.
That is, if $\phi : G \to H$ is any group homomorphism with $\ker \phi \leq N$ then there exists a unique group homomorphism $\bar{\phi} : G/N \to H$ such that
This means for any $a \in G$, we have that $\bar{\phi}\pi(a) = \phi(a)$. We say that $\bar{\phi}$ is **induced** by ϕ.

Define $\bar{\phi} : G/N \to H$ by $\bar{\phi}(aN) = \phi(a)$. for any $a \in G$.
Well defined: Suppose $aN = bN \implies b^{-1}a \in N \leq \ker \phi \implies \phi(b^{-1}a) = 1_H \implies \phi(b^{-1})\phi(a) = 1_H \implies \phi(a) = \phi(b)$.
Now we show $\bar{\phi}$ is a homomorphism.

$$\begin{aligned}\bar{\phi}\left((aN)(bN)\right) &= \bar{\phi}(abN) \\ &= \phi(ab) = \phi(a)\phi(b) \\ &= \bar{\phi}(aN)\bar{\phi}(bN)\end{aligned}$$

Commuting diagram: $a \in G$. Then

$$\bar{\phi}(\pi(a)) = \bar{\phi}(aN) = \phi(a)$$

Exercise: Show that $\bar{\phi}$ is the unique such homomorphism $G/N \to H$.

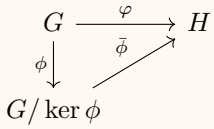
Note. So far, we've roughly covered the following sections in Dummit and Foote: 1.1, 1.2, 1.3, 1.6, 1.7, 2.1, 2.3, 3.1, 3.2. Now, we are (roughly) covering section 3.3

Last time: We covered the universal property.

Corollary 2.2: C20: First Isomorphism Theorem

This is actually a standard name for this theorem.
If $\phi : H \to H$ is a surjective group homomorphism, then $G/\ker\phi \simeq H$.

We know $\ker phi \triangleleft G$. Now we apply the Universal Property to get induced homomorphism.



$\bar{\phi}$ is surjective: If $h \in H$ since ϕ is surjactve, $h = \phi(a)$ for some $a \in G$. Then $\bar{\phi}(a\ker\phi) = \phi(a) = h$.
$\bar{\phi}$ is injective: Let $a\ker\phi \in G/\ker\phi$ such that $\bar{\phi}(a\ker\phi) = 1_H$. This implies $\phi(a) = 1_H \implies a \in \ker\phi \implies a\ker\phi = \ker\phi = 1_{G/\ker\phi}$. Therefore, $\ker\bar{\phi} = \langle 1_{G/\ker\phi}\rangle$. By 18, $\bar{\phi}$ is injective.

Example 2.6

1. $\phi : \mathbb{C}^\times \to \mathbb{R}^{>0}$ with $z \mapsto |z|$. This is a group homomorphism since $|zw| = |z||w|$. (i.e., taking modulus is a group homomorphism). This is clearly surjective.
   $\ker \phi = \{z \in \mathbb{C}^\times \mid |z| = 1\} = S$ The circle of radius 1 centred at the origin. By the first isomorphism theorem, we have $\mathbb{C}^\times / S \simeq \mathbb{R}^{>0}$.
2. $rem : (\mathbb{Z}, +) \to (\mathbb{Z}_m, \oplus)$ for $m > 1$. Where $(\mathbb{Z}_m, \oplus)$ is has modulo m addition on $\{0, 1, \cdots, m\}$. $rem(n) =$ remainder when n is divided by m.
   We have seen that this is a surjective group homomorphism $\ker rem = \{n \in \mathbb{Z} \mid rem(n) = 0\} = m\mathbb{Z}$. Then by 20, $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$.

Recall that H, K are subgroups of G where $HK = \{hk | h \in H, k \in K\} \subseteq G$ where HK is set multiplication.

Note also that $H \subseteq HK$ and $K \subseteq HK$ since $h \in H, h = h \cdot 1$ and $k \in K, k = 1 \cdot k$.

In general, HK may **not** be a subgroup of G.

Example 2.7: Set multiplication does not yield subgroups

Let $G = D_{10}$. $H = \langle s \rangle = \{1, s\}$. $K = \langle sr \rangle = \{1, sr\}$ (since $(sr)^2 = srsr = s^2 r^{-1} r = 1$. Then $HK = \{1, sr, s, r\}$. Then we may see that $HK \not\leq D_{10}$ since $s, r \in HK$ and $rs \notin HK$.

Lemma 2.2: L21

Let $H \leq G$ and $K \leq G$. If one of H or K is normal in G then $HK \leq G$.

Suppose $H \triangleleft G$. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then we have that $(h_1 k_1)(h_2 k_2) = h_1 h' k_1 k_2 \in HK$ for some $h' \in H$. Since H normal to G we have $k_1 H = H k_1$. Similar argument for K normal to G.
Now we show closed under inverses. Let $hinH$, $k \in K$.

$$\begin{aligned} (hk)^{-1} &= k^{-1} h^{-1} & \\ &= h' k^{-1} & \text{for some } h' \in H \\ &\in HK & \text{since } k^{-1} \in K \text{ as } K \leq G \end{aligned}$$

And a similar argument if K is normal to G.

Theorem 2.2: Second Isomorphism Theorem

Let G be a group with $N \triangleleft G$, $H \leq G$. Then $H \cap N \triangleleft H$ and $H/H \cap N \simeq HN/N$.

Consdier $\phi : H \to G/N$ given by (insert image)
So $\phi(h) = hN$ is a homomorphism.
We will show that $\Im \phi = HN/N$