Group Theory - Week 1 - Group Theory Recap: Group Properties, Subgroups and Lagrange's Theorem

Antonio León Villares

September 2022

Contents

Based on the notes by Susan J. Sierra, Chapter 1

1 Groups

1.1 Definition: Groups

Consider a set G, and let $\star$ be a ***binary function****:*

$$\star : G \times G \to G$$

$$(g, h) \mapsto g \star h \in G, \qquad \forall g, h \in G$$

A ***group*** *$(G, \star)$ satisfies 3 axioms:*

1. ***Associativity****:*

$$g \star (h \star k) = (g \star h) \star k, \qquad g, h, k \in G$$

2. ***Existence of Identity****:*

$$\exists e \in G \ : \ e \star g = g \star e = g, \qquad \forall g \in G$$

3. ***Existence of Inverse****:*

$$\forall g \in G, \exists h \in G \ : \ g \star h = h \star g = e$$

We write $h = g^{-1}$.

By letting $\star$ be a function, we ensure that $(G, \star)$ is ***closed*** *under $\star$. (Definition 1.1.1)*

- **What is the order of a group?**
  - the number of elements in G
  - we denote the order via $|G|$

1.2 Definition: Abelian Group

A group $(G, \star)$ is ***abelian*** *if:*

$$g \star h = h \star g, \qquad \forall g, h \in G$$

1.3 Theorem: Group Properties

Let $(G, \star)$ be a group. Then:

1. ***Existence and Uniqueness of Group Products**: if $g, h \in G$, then there are **unique** elements k_1, k_2 such that:*

$$k_1 \star g = h \qquad g \star k_2 = h$$

2. ***Cancellation Law**: let $g, s, t \in G$. Then:*

$$g \star s = g \star t \implies s = t$$

$$s \star g = t \star g \implies s = t$$

3. ***Uniqueness of Identity**: e is the only identity element. $\forall g, h \in G$ if $g \star h = h$, then $g = e$.*

4. ***Uniqueness of Inverse**: g^{-1} is the only inverse of $g \in G$. $\forall g, h \in G$ if $g \star h = e$, then $h = g^{-1}$.*

5. ***Inverse of Identity**: the inverse of the identity element is the identity element*

$$e^{-1} = e$$

6. ***Inverse of Inverse**: if $g \in G$, then $(g^{-1})^{-1} = g$*

(Revision Exercises 1, 2 + FPM Notes)

Proof. 1. **Existence and Uniqueness of Group Products**
We prove the first statement: if $g, h \in G$, there is a **unique** $k \in G$ such that $k \star g = h$.
Define $k := hg^{-1}$. Clearly, $k \in G$. Moreover:

$$kg = (hg^{-1})g = h(g^{-1}g) = h$$

Moreover, k is unique: assume $\exists k' \in G$ such that $k'g = h$. Then:

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

2. **Cancellation Law**
Assume $gs = gt$. By uniqueness, this is only possible if $s = t$. Alternatively:

$$gs = gt \implies g^{-1}(gs) = g^{-1}(gt) \implies s = t$$

3. **Uniqueness of Identity**

   (a) assume $\exists g, h$ such that:

$$gh = h$$

   But since $eh = h$, it follows by cancellation law/uniqueness that $g = e$, as required.

(b) assume e' is another identity. Then:

$$\begin{aligned} & e'g = eg \\ \implies & (e'g)g^{-1} = (eg)g^{-1} \\ \implies & e'(gg^{-1}) = e(gg^{-1}) \\ \implies & e' = e \end{aligned}$$

(c) assume e' is another identity. Then we must have that:

$$ee' = e \qquad ee' = e'$$

But by uniqueness of products, we must then have $e = e'$.

4. **Uniqueness of Inverse**

   (a) follows directly from existence and uniqueness, by using g, e, and the fact that by the group axioms, $gg^{-1} = e$

   (b) assume h, k are 2 inverses of g. Then:

$$gh = e \qquad gk = e \implies gk = gh$$

   so by cancellation/uniqueness, $k = h$

5. **Inverse of Identity**
   Since $ee = e$ and $ee^{-1} = e$, and inverses are unique, $e = e^{-1}$

6. **Inverse of Inverse**
   Since $g^{-1}(g^{-1})^{-1} = e$ and $g^{-1}g = e$, and inverses are unique, $g = (g^{-1})^{-1}$

□

1.4 Definition: The Product Group

*Let $(G, \star_G)$ and $(H, \star_H)$ be groups. The **direct product** $G \times H$ is a **product group** under operation $\star$, defined by:*

$$(g, h) \star (g', h') = (g \star_G g', h \star_H h')$$

(Definition 1.4.8)

1.5 Examples of Groups

1.5.1 Symmetric Group

- S_n is the symmetric group
- corresponds to the set of all **permutations** of the set $\{1, \ldots, n\}$
- $\star$ is permutation composition
- contains $n!$ elements

1.5.2 Dihedral Group

- D_n is the **dihedral groups**
- corresponds to the set of all **symmetries** of a regular n-gon
- contains $2n$ elements: n rotations and n reflections

1.5.3 Free Group

- 2 letters have a **free group** $G = \langle x, y \rangle$
- corresponds to the set of all **words** which can be generated by combining x, y, x^{-1}, y^{-1}
- $\star$ is letter concatentation:

$$xxx^{-1}y \star y^{-1}x = xxx^{-1}yy^{-1}x = xx = x^2$$

- the identity element is the **empty word** (no letters)

1.5.4 Integers Under Addition

- $(\mathbb{Z}, +)$ is a group with $e = 0$
- it is a **cyclic group** generated by 1 (so every element in $\mathbb{Z}$ can be written as a sum of 1s)
- $(\mathbb{Z}_n, +)$ (integers modulo n) are also a group

2 Subgroups

2.1 Definition: Subgroups

*Let $(G, \star)$ be a group. A **non-empty** subset $H \subseteq G$ is a **subgroup** if $(H, \star)$ is a group.*
*In particular, H is a subgroup if its **closed** under **products** and **inverses**:*

1. $hk \in H, \forall h, k \in H$
2. $h^{-1} \in H, \forall h \in H$

If H is a subgroup of G, we write:

$$H \leq G$$

(Definition 1.3.1)

Notice, the $e \in H$, since $h, h^{-1} \in H$ and there's multiplicative closure. Moreover, H will be associative, since G was. So H satisfies the properties of a group!

- **Given a finite group, how can we test for a subgroup?**
  - for **finite** subsets, it is sufficient to check that H is closed under **products**

- **What is a proper subgroup?**
  - a subgroup H which is a proper subset of G
  - we write:
$$H < G$$

2.2 Theorem: Test for Subgroup

> *Let G be a group, and $H \subseteq G$. H is a subgroup if and only if it is **non-empty** and:*
> $$hk^{-1} \in H, \qquad \forall h, k \in H$$
> *(Revision Exercise 4)*

Proof. If H is a subgroup, consider $h, k \in H$. Then, we have that $k^{-1} \in H$, and by closure, it follows that $hk^{-1} \in H$, as required.

Alternatively, let $h, k \in H$, and assume that $hk^{-1} \in H$. We need to show closure under products and inverses. Since $k \in H$, let $h = k$. Then it follows that:

$$hk^{-1} \in H \implies hh^{-1} = e \in H$$

Hence, it follows that:

$$hk^{-1} \in H \implies ek^{-1} = k^{-1} \in H$$

so H is closed under inverses.

Moreover,

$$hk^{-1} \in H \implies h(k^{-1})^{-1} = hk \in H$$

so H is closed under products. Hence, H is a subgroup.

□

2.3 Examples of Subgroups

- $\{e\}$ is the **trivial subgroup** for any group G; similarly, G is a subgroup of G
- the set of rotations of an n-gon form a subgroup of D_n
- A_n is the **alternating group**, and it's a subgroup of S_n, constructed by taking the product of an **even** number of 2-cycles
- $GL(n, F)$ is the **general linear group** over a field F, containing all the **invertible** $n \times n$ matrices. $SL(n, F)$ is the **special linear group**, the set of all invertible $n \times n$ matrices with determinant 1. $SL(n, F)$ is a subgroup of $GL(n, F)$.

2.4 Cyclic Groups

- **How can we generate subgroups by using elements of groups?**
  - we can repeatedly apply $\star$ to an element g with itself
  - this generates a subgroup:
$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$
    known as the **subgroup generated by** g

- **What is a cyclic group?**
  - a **group** which is generated by a **single** element $g \in G$:

$$G = \langle g \rangle$$

- **What is the order of a group element?**
  - the **smallest positive integer** n such that:

$$g^n = e$$

    (if it doesn't exist, $n = \infty$)
  - denoted as $o(g)$
  - we have that the order of a **cyclic subgroup** is the **order** of the subgroup's generator:

$$|\langle g \rangle| = o(g)$$

2.5 Worked Exercises

3 Cosets

3.1 Definition: Left and Right Cosets

Let $H \subseteq G$, and consider $g \in G$. Then:

- *the **left coset** of H determined by g is the set:*

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

- *the **right coset** of H determined by g is the set:*

$$Hg = \{hg \mid h \in H\} \subseteq G$$

*G/H denotes the set of all **left cosets**, whilst $H \setminus G$ denotes the set of all **right cosets**.*
(Definition 1.3.6)

- **What is the index of H in G, where $H \leq G$?**
  - the number of **left cosets** of H:

$$|G/H| = [G : H]$$

3.1.1 Worked Exercises

- (Revision Exercise 7) **Let $G = S_3$ and let $H = \{e, (12)\}$. $H \leq G$. Write down the elements of G/H and $H \setminus G$. What do you notice about these sets?**

3.2 Normal Subgroups

3.2.1 Definition: Normal Subgroups

*Let $H \leq G$. H is a **normal subgroup** if it is **invariant under conjugation**. In other words:*

$$gH = Hg, \qquad \forall g \in G$$

We write $H \triangleleft G$.

3.2.2 Theorem: Equivalent Definitions for Normal Subgroups

*The following are **equivalent**:*

1. $H \triangleleft G$
2. $gHg^{-1} = H, \qquad \forall g \in G$
3. $gHg^{-1} \subseteq H, \qquad \forall g \in G$
4. $H = \bigcap_{g \in G} gHg^{-1}$
5. $H \subseteq \bigcap_{g \in G} gHg^{-1}$

Proof.

- $H \triangleleft G \iff gHg^{-1} \subseteq H$
  ($\implies$) Let H be a normal subgroup; that is:

  $$gH = Hg, \qquad \forall g \in G$$

  For any $g \in G$, $\exists h, k \in H$ such that:

  $$gh = kg \implies ghg^{-1} = k \in H$$

  That is, if $ghg^{-1} \in gHg^{-1}$ then also $ghg^{-1} \in H$, so $gHg^{-1} \subseteq H$. (Alternatively, argue that $gH = Hg \implies gHg^{-1} = H$)
  ($\impliedby$) Assume that $gHg^{-1} \subseteq H, \forall g \in G$.
  On the one hand, we have that $\exists h, k \in H$ such that:

  $$ghg^{-1} = k \implies gh = kg \in Hg$$

  so it follows that $gH \subseteq Hg$.
  On the other hand, since $g^{-1} \in G$, $\exists h, k \in H$ such that:

  $$(g^{-1})h(g^{-1})^{-1} = k \implies g^{-1}hg = k \implies hg = gk \in gH$$

  so it follows that $Hg \subseteq gH$. Hence, we must have that $gH = Hg$, and H is a normal subgroup.

- $H \triangleleft G \iff gHg^{-1} = H$

$$\begin{aligned} H \triangleleft G &\iff gH = Hg \\ &\iff (gH)g^{-1} = (Hg)g^{-1} \\ &\iff gHg^{-1} = H \end{aligned}$$

□

3.2.3 Theorem: Another Definition for a Normal Subgroup

Let $H \leq G$, and assume that $\forall g \in G$ we have:

$$gHg^{-1} \subseteq H \qquad g^{-1}Hg \subseteq H$$

then:

$$gHg^{-1} = H$$

and so, $H \triangleleft G$.

Proof. Assume that $gHg^{-1} \neq H$. Then, $\exists h \in H$ such that $h \notin gHg^{-1}$. But then, observe:

$$\begin{aligned} H &= (gg^{-1})H(gg^{-1}) \\ &= g(g^{-1}Hg)g^{-1} \\ &\subseteq gHg^{-1} \end{aligned}$$

In other words, any element of H must be in gHg^{-1}. However, this is a contradiction, and so, no such $h \in H$ must exist. Hence, $gHg^{-1} = H$, and by the definition of a normal subgroup:

$$H \triangleleft G$$

as required.

□

4 Lagrange's Theorem

4.1 Recap: Equivalence Relations and Equivalence Classes

- **What is an equivalence relation?**
  - consider a set X
  - for $s, t \in X$, we write $s \sim t$ to say "s is related to t"
  - $\sim$ defines an **equivalence relation** if it's:
    - **reflexive**: $x \sim x, \forall x \in X$
    - **symmetric**: $x \sim y \implies y \sim x, \forall x, y \in X$
    - **transitive**: $x \sim y, y \sim z \implies x \sim z, \qquad \forall x, y, z \in X$
- **What is an equivalence class?**
  - for some $x \in X$, its **equivalence class** is the set of all elements in X which are related to x via an **equivalence relation**:

$$cl(x) = \{y \mid x \sim y, y \in X\}$$

4.1.1 Theorem: Properties of Equivalence Classes

Consider a set X with equivalence relation $\sim$. Then:

1. $cl(x) \neq \emptyset$
2. $x \sim y, x, y \in X$ ***if and only if***:

$$cl(x) = cl(y)$$

if and only if:

$$cl(x) \cap cl(y) \neq \emptyset$$

In other words, 2 equivalence classes are either the exact same, or completely disjoint.

Proof. 1. This follows from the fact that $x \in cl(x)$ by **reflexivity**

2. Assume $x \sim y$. Let $z \in cl(y)$, so that $y \sim z$. Since $x \sim y$, by transitivity it follows that $x \sim z$, so $z \in cl(x) \implies cl(y) \subseteq cl(x)$. By similar arguments, $cl(x) \subseteq cl(y)$, so:

$$cl(x) = cl(y)$$

Otherwise, if $cl(x) = cl(y)$, since $x \in cl(x)$ and $y \in cl(y)$, it follows that $x \in cl(y), y \in cl(x)$, so $x \sim y$.

Assume $x \sim y$. We know that $x \in cl(y)$ and $y \in cl(x)$, so in particular $x \in cl(x) \cap cl(y)$, so $cl(x) \cap cl(y) \neq \emptyset$.

Otherwise if $cl(x) \cap cl(y) \neq \emptyset$, then $\exists z \in cl(x) \cap cl(y)$, so $x \sim z$ and $z \sim y$. By transitivity, $x \sim y$, as required.

□

4.1.2 Theorem: Equivalence Classes Partition Sets

Let X be a set with an ***equivalence relation*** *$\sim$. Then, the* ***equivalence classes*** *generated by $\sim$* ***partition*** *X. In other words, each element of X can be put into a unique equivalence class (which is non-empty), such that the union of equivalence classes gives X.*

Proof. Any 2 equivalence classes are either the same set (if they have a common representative), or completely disjoint. Moreover, each element of x belongs to at least one equivalence class ($cl(x)$). Thus:

$$X = \bigcup_{x \in X} cl(x)$$

□

4.2 Theorem: Cosets as Equivalence Classes

Let G be a group, and $H \leq G$. The relation $\sim$, given by:

$$g_1 \sim g_2 \iff \exists g_2 \ : \ g_1 \in g_2 H, \qquad g_1, g_2 \in G$$

is an equivalence relation on G.
The equivalence classes are the cosets gH; in other words, the cosets gH partition the group, so $\exists g_1, \ldots, g_n \in G$ such that:

$$G = \bigcup_{i=1}^{n} g_i H$$

As a bonus, if $h \in H$, then we have that:

$$hH = H$$

Proof. We verify the properties of an equivalence relation:

1. **Reflexivity**
   Notice, since $e \in H$, then $g \in gH$, so it follows that $g \sim g$.

2. **Symmetry**
   Assume that $g_1 \in g_2 H$. Then, $\exists h \in H$ such that $g_1 = g_2 h$. Consider the coset $g_1 H$. We must have that:
   $$g_1 H = (g_2 h)H = g_2(hH)$$
   Now, H is closed under multiplication, so clearly $hH \subseteq H$. Suppose $t \in H$. We can write:
   $$t = h(h^{-1}t), \qquad h^{-1}t \in H$$
   Then, $t \in hH$, so $H \subseteq hH$. Thus, $hH = H$.
   This shows that if $g_1 \in g_2 H$, then $g_1 H = g_2 H$, so in particular $g_2 \in g_1 H$ (as $g_2 \in g_2 H$) so $g_1 \sim g_2 \implies g_2 \sim g_1$.

3. **Transitivity**
   Assume that $g_1 \in g_2 H$ and $g_2 \in g_3 H$. Then, $\exists h, k \in H$ such that:
   $$g_1 = g_2 h \qquad g_2 = g_3 k$$
   So:
   $$g_1 = g_2 h = (g_3 k)h = g_3(kh) \in g_3 H$$
   since $kh \in H$. Thus, $g_1 \sim g_3$, as required.

□

Notice, this then means that given 2 cosets, either:

- $g_1 H = g_2 H$
- $g_1 H \cap g_2 H = \emptyset$

4.3 Theorem: Cosets Have Same Order as Subgroup

Let $H \leq G$. Then:

$$|gH| = |H|, \qquad \forall g \in G$$

Proof. Consider the map:

$$f : H \to gH$$

defined by:

$$f(h) = gh$$

It is sufficient to show that f is a bijection. It is clearly surjective from definition:

$$gH = \{gh \mid h \in H\} = \{f(h) \mid h \in H\}$$

It is also injective, by the uniqueness of group products/cancellation law:

$$f(h_1) = f(h_2) \iff gh_1 = gh_2 \iff h_1 = h_2$$

Hence, it follows that f is a bijection, and $|gH| = |H|$.

*This is known as the **canonical map**, and we will see more next week, when defining the **Isomorphism Theorems**.*

□

4.4 Theorem: Lagrange's Theorem

*Let $H \subset G$, where G is a **finite** group. Then, the **order** of H divides the **order** of G.*
More precisely:

$$|G| = |G/H||H|$$

(Theorem 1.3.8)

Proof. We showed about that the relation $g_1 \sim g_2 \iff g_1 = g_2 H$ is an equivalence relation, with equivalence classes gH, the left cosets of H. These cosets partition the group:

$$G = \bigcup_{i=1}^{n} g_i H$$

where $g_i \in G$ are representatives of the equivalence classes.

Then, since the equivalence classes are disjoint:

$$|G| = \sum_{i=1}^{n} |g_i H| = \sum_{i=1}^{n} |H| = nH$$

where we have used the theorem above, whereby $|gH| = |H|, \forall g \in G$.
But here n is the number of distinct left cosets of H, which is $|G/H|$ so:

$$|G| = |G/H||H|$$

as required

□

4.4.1 Remark: Differences Between Left and Right Cosets

*When developing Lagrange's Theorem, we have just used **left cosets**. However, it is easy to verify that:*

$$g_1 \sim g_2 \iff g_1 \in Hg_2$$

*is an equivalence relation, with equivalence classes Hg - the **right cosets**. Thus, **Lagrange's Theorem** also applies to **right cosets**:*

$$|G| = |H \setminus G||H|$$

*and this also means that if H is a **subgroup**, it has the **same** number of left and right cosets.*

4.5 Corollaries of Lagrange's Theorem

4.5.1 Theorem: Cauchy's Theorem

*Lagrange's Theorem imposes restrictions on the possible orders of subgroups. However, it doesn't imply the **existence** of said subgroups. This changes for prime ordered subgroups.*

*If G is a **finite group** and p is **prime**, such that p divides $|G|$, then G has a subgroup of order p.*
(Theorem 1.3.9)

The proof requires the Orbit-Stabilizer Theorem, done in FPM.

4.5.2 Corollary: Order of Group Elements

Let G be a group, and $g \in G$. Then:

1. *$o(g)$ divides $|G|$*
2. *$g^{|G|} = e$*

Proof. $\langle g \rangle$ is a subgrop of order $o(g)$, so by Lagrange's Theorem:

$$|G| = |G/\langle g \rangle| o(g)$$

This places a restriction on the order of group elements!
By the above:

$$g^{|G|} = g^{|G/\langle g\rangle| o(g)} = (g^{o(g)})^{|G/\langle g\rangle|} = e^{|G/\langle g\rangle|} = e$$

□

4.5.3 Corollary: Cyclic Group if Order is Prime

> *If $|G|$ is **prime**, then G is **cyclic**.*
> *(Corollary 1.3.11)*

Proof. Let $|G|$ be prime. By Lagrange's Theorem:

$$|G| = |G/H||H|$$

Now, consider $g \in G, g \neq e$, and in particular, the subgroup $H = \langle g\rangle$. Since $o(g)$ must divide $|G|$, $g \neq e$ and $|G|$ is prime, this is only possible if $o(g) = |G|$. Hence, $H = \langle g\rangle = G$, and G is cyclic. □

4.5.4 Corollary: Groups of Order 5 or Less Are Abelian

> *Let G be a group. If $|G| < 6$, then G is **abelian**.*

4.5.5 Theorem: Fermat's Little Theorem

> *If p is prime, and $a \in \mathbb{Z}$, then:*
>
> $$a^p \equiv a \ mod \ p$$

Proof. If $a \equiv 0$, then the result follows, so assume this is not the case.
We can think of a as an element of the group $\mathbb{Z}_p^\times$ under the operation of multiplication modulo p, with identity $e = 1$.
This group has $p - 1$ elements, so by the corollary on the order of group elements:

$$g^{|\mathbb{Z}_p^\times|} = g^{p-1} = 1, \qquad \forall g \in \mathbb{Z}_p^\times$$

Moving back to a, it follows that:

$$a^{p-1} \equiv 1 \ mod \ p$$

so multiplying through by a yields the desired result. □

4.5.6 Worked Exercises

- (Revision Exercise 13) **Provide the details for the following example. Let $G = \mathbb{Z}_{10}^+$, and $H = \{0, 2, 4, 6, 8\}$. $H \leq G$ and in fact it is a normal subgroup. Show why. Verify that the left cosets of H are the same as the right cosets. Another coset is $1 + H$ (odd numbers mod 10). Verify that this is what Lagrange predicts. Finally, consider $K = \{0, 5\}$, which is also a normal subgroup. What are the 5 cosets of K?**

5 Group Homomorphisms

5.1 Definition: Group Homomorphisms and Endomorphisms

Let G, H be groups.
A function:

$$\phi : G \to H$$

such that

$$\phi(a \star_G b) = \phi(a) \star_H \phi(b), \qquad \forall a, b \in G$$

*is a **group homomorphism**.*
*If $\phi : G \to G$, then ϕ is a **group endomorphism**.*
(Definition 1.4.1)

5.2 Definition: Group Isomorphisms and Automorphisms

Let G, H be groups.
*If $\phi : G \to H$ is a **bijective group homomorphism**, then ϕ is a **group isomorphism**.*
*If $G = H$, so that $\phi : G \to G$, then ϕ is a **group automorphism**.*

- **What are isomorphic groups?**
  - groups whereby there is an **isomorphism** between them
  - if G, H are **isomorphic**, then:

$$G \cong H$$

5.2.1 Theorem: Cylic Groups are Isomorphic

*Let $n \in \mathbb{N}$. Any 2 **cyclic** groups of order n are **isomorphic**.*

Proof. Let $G = \langle g \rangle, H = \langle h \rangle$. Consider the mapping:

$$\phi : G \to H$$

$$\phi(g^t) = h^t$$

We first verify that this is a **homomorphism**. Without loss of generality, let $s, t \in \mathbb{N}$ (group composition can involve powers of inverses, but these can be expressed with positive powers, since the group is cyclic). Then:

$$\phi(g^t g^s) = \phi(g^{t+s}) = h^{t+s} = h^t h^s = \phi(g^t)\phi(g^s)$$

So ϕ is a group homomorphism.
Moreover, it is surjective, since $\forall h^t \in H$, $\phi(g^t) = h^t$. Since $|G| = |H|$ and ϕ is surjective, it follows that ϕ is also injective, and so, it's a bijection, so ϕ is an isomorphism.
Thus, any 2 cyclic groups of the same order are isomorphic.

□

5.2.2 Examples of Group Isomorphisms

- $(\mathbb{R}^+, \times)$ has an isomorphism:
$$exp : \mathbb{R} \to \mathbb{R}^+$$
$$exp(x + y) = exp(x)exp(y)$$
- the map $\phi : D_3 \to S_3$, mapping the symmetries of a triangle to the permutation of the vertices under the symmetry is an isomorphism
- if we think of $\mathbb{Z}_p$ as a field, consider the group of **units**, $\mathbb{Z}_p^\times$ (that is, the group of all elements in $\mathbb{Z}_p$ with an inverse). Then, $Z_p^\times \cong C_{p-1}$: that is, the group of units is a cyclic group of order $p - 1$

5.3 Theorem: Properties of Group Homomorphisms

Let $\phi : G \to H$ be a group homomorphism. Then:

1. $\phi(e_G) = e_H$
2. $\phi(g^{-1}) = \phi(g)^{-1}$
3. *If ϕ is a* ***group isomorphism****, then so is ϕ^{-1}.*

Proof. 1.

$$\begin{aligned}
& \phi(e_G) = \phi(e_G \star_G e_G) \\
\implies & \phi(e_G) = \phi(e_G) \star_H \phi(e_G) \\
\implies & (\phi(e_G))^{-1} \star_H \phi(e_G) = (\phi(e_G))^{-1}(\phi(e_G) \star_H \phi(e_G)) \\
\implies & e_H = \phi(e_G)
\end{aligned}$$

2.

$$\begin{aligned}
\phi(g) \star_H \phi(g^{-1}) &= \phi(g \star_G g^{-1}) \\
&= \phi(e_G) \\
&= e_H
\end{aligned}$$

$$\begin{aligned}
\phi(g^{-1}) \star_H \phi(g) &= \phi(g^{-1} \star_G g) \\
&= \phi(e_G) \\
&= e_H
\end{aligned}$$

Since inverses are unique, and $\phi(g^{-1})$ is an inverse to $\phi(g)$, it follows that:

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

3. Since ϕ is an isomorphism, $\phi^{-1} : H \to G$ is a well-defined, bijective function. Now, consider:

$$h = \phi(g) \qquad h' = \phi(g'), \qquad g, g' \in G, h, h' \in H$$

Then:

$$\begin{aligned}\phi^{-1}(h \star_H h') &= \phi^{-1}(\phi(g) \star_H \phi(g')) \\ &= \phi^{-1}(\phi(g \star_G g')) \\ &= g \star_G g' \\ &= \phi^{-1}(h) \star_G \phi^{-1}(h')\end{aligned}$$

so ϕ is a group homormorphism; since its bijective, its an isomorphism.

□

5.3.1 Theorem: Isomorphic Prime Groups

*All groups of **prime** order are **isomorphic**.*

Proof. We showed that by Lagrange's Theorem, if G is of prime order, it is cyclic. We further showed above that all cyclic groups are isomorphic, so it follows that all groups of prime order are isomorphic.

□

5.4 The Kernel of a Homomorphism

5.4.1 Definition: The Kernel

*Let $\phi : G \to H$ be a **group homormorphism**.*
*The **kernel** of ϕ is a **subgroup** of G, defined by:*

$$ker(\phi) = \{g \mid \phi(g) = 0, g \in G\}$$

5.4.2 Theorem: Properties of the Kernel

Let $\phi : G \to H$ be a group homomorphism.

1. $\ker(\phi) \leq G$ *(in fact,* $\ker(\phi) \triangleleft G$*)*
2. ϕ *is **injective if and only if**:*

$$\ker(\phi) = \{e\}$$

Proof. 1. We first show $ker(\phi)$ is a subgroup. We need to verify closure under product and inverse.
Let $g_1, g_2 \in ker(\phi)$. Then:

$$\phi(g_1) = \phi(g_2) = e_H$$

Thus:

$$e_H = e_H \star_H e_H = \phi(g_1) \star_H \phi(g_2) = \phi(g_1 \star_G g_2)$$

Hence, if $g_1, g_2 \in ker(\phi)$, then $g_1 g_2 \in ker(\phi)$.
Moreover, for $g \in ker(\phi)$:

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

Hence, by the cancellation law:

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

so if $g \in ker(\phi), g^{-1} \in ker(\phi)$.
Thus, it follows that $ker(\phi) \leq G$.
Lastly, recall, a subgroup $K \subseteq G$ is a normal subgroup **if and only if**:

$$gKg^{-1} \subseteq K$$

Let $K = ker(\phi)$. For any $g \in G, k \in K$:

$$\phi(g \star_G k \star_G g^{-1}) = \phi(g) \star_H \phi(k) \star_H \phi(g^{-1}) = \phi(g) \star_H e_H \star_H \phi(g^{-1}) = e_H$$

so it follows that $gkg^{-1} \in K$ so $gKg^{-1} \subseteq K$, and so, $ker(\phi) \triangleleft G$.

2. ($\implies$) Assume that $ker(\phi) = \{e\}$. Then, for $g_1, g_2 \in G$:

$$\begin{aligned} & \phi(g_1) = \phi(g_2) \\ \implies & \phi(g_1^{-1}) \star_H \phi(g_1) = \phi(g_1^{-1}) \star_H \phi(g_2) \\ \implies & \phi(g_1^{-1} \star_G g_1) = \phi(g_1^{-1} \star_G g_2) \\ \implies & \phi(e_G) = \phi(g_1^{-1} \star_G g_2) \\ \implies & e_H = \phi(g_1^{-1} \star_G g_2) \end{aligned}$$

Thus, it must be the case that $g_1^{-1}g_2 \in ker(\phi)$. But by assumption, $ker(\phi) = \{e_G\}$, so:

$$g_1^{-1}g_2 = e_G \iff g_1 = g_2$$

so it follows that ϕ is injective.
($\impliedby$) Assume that ϕ is injective. Since we know that $\phi(e_G) = e_H$, it can't be the case that any other $g \in G$ maps to e_H by injectivity, so:

$$ker(\phi) = \{e_G\}$$

as required.

□

5.5 The Image of a Homomorphism

5.5.1 Definition: The Image

*Let $\phi : G \to H$ be a **group homomorphism**.*
*The **image** of ϕ is a **subgroup** of H, defined by:*

$$im(\phi) = \{h \mid h = \phi(g), g \in G\}$$

5.5.2 Lemma: The Image is a Subgroup

*If $\phi : G \to H$ is a **group homomorphism**, then $im(\phi) \leq H$.*

Proof. Firstly, $im(\phi)$ is non-empty, since:

$$\phi(e_G) = e_H \in H$$

We now verify closure. If $h_1, h_2 \in im(\phi)$ then:

$$\exists g_1, g_2 \in G \ : \ \phi(g_1) = h_1 \qquad \phi(g_2) = h_2$$

So:

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$$

so $h_1 h_2 \in im(\phi)$, so $im(\phi)$ is closed.

We now verify the existence of inverse. Let $h \in im(\phi)$, so that $\exists g \in G : \phi(g) = h$. But the homomorphism maps inverses to inverses, so:

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

□

5.6 Definition: The Automorphism Group

> *Let G be a group.*
> *The **set** of all **automorphisms**, $\phi : G \to G$ forms the **automorphism group** of G, written $Aut(G)$. This is a **group** under **function composition**.*

5.6.1 Worked Example: Automorphism Group of Cyclic Group of Prime Order

Consider a cyclic group $G = C_p$, where p is prime. It can be shown that:

$$Aut(G) \cong \mathbb{Z}_p^\times \cong C_{p-1}$$

We can check this when $p = 5$. We can think of G as:

$$G = \{e, g, g^2, g^3, g^4\}$$

If $\phi \in Aut(G)$, and since G only has 5 elements, we must have one of the following cases:

$$\phi(g) = e, g, g^2, g^3, g^3$$

If $\phi(g) = e$, then ϕ won't be an automorphism, since it won't be bijective (as $\phi(e) = e$ already). Hence, we have 4 remaining possibilities:

$$\phi(g) = g, g^2, g^3, g^3$$

$\phi(g) = g$ is the identity automorphism, which works. What about $\phi(g) = g^2$. Then:

- $\phi(e) = e^2 = e$
- $\phi(g) = g^2$
- $\phi(g^2) = g^4$
- $\phi(g^3) = g^6 = g$
- $\phi(g^4) = g^8 = g^3$

Hence, this defines a bijection. Similarly, we can check that $\phi_i(g) = g^i$ defines automorphisms.
We have then found 4 automorphisms for G, which are the only possibilities, so $|Aut(G)| = 4$.
We can now look at the structure of $Aut(G)$. For instance, how it behaves under the group action:

$$\phi_i(\phi_j(g)) = \phi_i(g^j) = (\phi_i(g))^j = (g^i)^j = g^{ij} = \phi_{ij}(g)$$

Here, ij needs to be interpreted modulo 5, so we see that $Aut(G)$ has structure similar to multiplication in the field $\mathbb{Z}_5$, so indeed $Aut(G) \cong \mathbb{Z}_5^\times$ (we can't have isomorphisms from fields to groups, since fields have more structure; however, the units do form a group, with the same elements as the field).

6 Exercises for Chapter 1

1. **True or False**

   1. *Lagrange's Theorem shows that every group of order 60 has a subgroup of order 15.*
   2. *Every group of order 60 has a subgroup of order 1.*
   3. *Every group of order 60 has a normal subgroup of order 60.*
   4. *Lagrange's Theorem shows that no group of order 60 has a subgroup of order 24.*

2. **Let H, K be subgroups of G. Show that $H \cap K$ is a subgroup of G. When is $H \cup K$ a subgroup of G?**

3. **Let H, K be normal subgroups of G. Show that $H \cap K$ is a normal subgroup of G?**

4. **Suppose that $H \leq G$ and $|G/H| = [G : H] = 2$. Show that $H \triangleleft G$. You may want to use properties of cosets to show that the right coset of H is H, and the left coset of H is $G \setminus H$.**

5. **Let G be a group, and $H \leq G$. Show that $N = \bigcap_{x \in G} xHx^{-1}$ is the largest normal subgroup of G contained in H. That is, show that:**

   1. $N \triangleleft G$

   2. if $N' \triangleleft G$**, and** $N' \subseteq H$**, then** $N' \subseteq N$**.**

6. **Let G be a finite group, and let H, K be subgorups of G. Suppose that $|H|, |K|$ are coprime. Show that $H \cap K = \{e\}$.**

7. **Let G be a group, and recall tha tthe centre $Z(G)$ of G is the set:**

   $$Z(G) = \{z \mid z \in G, zg = gz \forall g \in G\}$$

   If $N \leq Z(G)$, show that $N \triangleleft G$. If in addition G/N is cyclic, show that G is abelian. You may want to show that any element of G can be written as $g^a n$ for some $a \in \mathbb{Z}$, $n \in N$.

8. **Let μ_8 be the set of eighth roots of unity in $\mathbb{C}^*$. What is $|\mu_8|$? Write down the elemnts of μ_8 as complex numbers. Show that μ_8 is a cyclic group under multiplication. Find the elemlents g in μ_8, such that $\langle g \rangle = \mu_8$; that is, which elements of μ_8 can be used as cyclic generators of μ_8?**

9. **Let $w = e^{\frac{2\pi i}{3}}$, so $w^3 = 1$, and $w \neq 1$. Since:**

   $$a := \begin{pmatrix} w^2 & 0 \\ 0 & w \end{pmatrix} \qquad b := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

   are invertible, they are in $GL(2, \mathbb{C})$. Find the orders of a and b. Calculate the conjugate bab^{-1}, and find k so that $bab^{-1} = a^k$.

10. **Let $G \leq GL(2, \mathbb{C})$, where G is generated by a, b. Show that G is a finite group, and find its order. You might want to use the fact that $ba = a^k b$, alongside Lagrange's Theorem.**

11. **Show that G from the previou problem is not isomorphic to D^6. You may want to consider the order of elements in the different groups.**

12. **Let F be a finite field with q elements. Show that $|GL(2, F)| = (q^2 - 1)(q^2 - q)$, and that:**

$$|SL(2, F)| = q(q + 1)(q - 1)$$

13. **Show that $Aut(G)$ is a group under the composition of functions.**

14. **Find $Aut(\mu_8)$.**

15. **Let L be a ring. Let $Aut(L)$ denote the set of ring isomorphisms of L to itself. Show that $Aut(L)$ forms a group.**

16. **Let K be a subfield of a field L. The set of elements of $Aut(L)$ that are equal to the identity when restricted to K is denoted by $Aut_K(L)$. Show that $Aut_K(L)$ is a subgroup of $Aut(L)$.**

17. **Interpret the preceding 2 problems for $\mathbb{R} \subseteq \mathbb{C}$. What is $Aut_{\mathbb{R}}(\mathbb{C})$**

7 Useful Exercises & Proofs from FPM

7.1 Theorem: Cyclic Groups are Abelian

*If G is **cyclic**, then G is **abelian**.*
(Exercise 2.4, FPM)

7.2 Theorem: Abelian if Square is Identity

Let G be a group. If:

$$g^2 = e, \qquad \forall g \in G$$

*then G is **abelian**.*
(Exercise 1.12, FPM)

7.3 Theorem: Product of Cyclic Groups with Coprime Order

*Let $G = C_m, H = C_n$ be **cyclic** groups of order m, n respectively.*
*Then, $G \times H$ is **cyclic if and only if** m and n are **coprime**.*
*Moreover, $C_m \times C_n \cong C_{mn}$ **if and only if** m, n are coprime.*
(Theorem 2.3.16, FPM)

7.4 Theorem: Subgroup of Cyclic Group

*If G is **cyclic**, then any subgroup $H \leq G$ is **cyclic**.*
(Theorem 2.3.15)