Group Theory

Department of Mathematics
Manipal Institute of Technology, Manipal

Introduction

Group Axioms

Definition 1.

A group is a set G together with a binary operation $*\colon G \times G \to G$, satisfying three properties (called the *group axioms*).

1. Associativity: $\forall x, y, z \in G,\ x * (y * z) = (x * y) * z$.
2. Existence of identity: $\exists e \in G,\ \forall x \in G,\ e * x = x * e = x$. The element e is said to be an identity element of G.
3. Existence of inverses: $\forall x \in G,\ \exists y \in G,\ x * y = y * x = e$. The element y is said to be an inverse of the element x.

Then we say that $(G, *)$ is a group, or that G is a group *under the operation* $*$.

Implicit in the statement that $*$ is a binary operation on G, is the fact that G is closed under $*$ – i.e., $\forall x, y \in G,\ x * y \in G$. This property is therefore called closure.

If $(G, *)$ is a group, the number of elements in the set G is said to be the order of G, and is denoted $|G|$ or $o(G)$. A finite group is a group whose order is finite, and an infinite group is a group of infinite order.

When the group operation is clear from context, we shall write xy to mean $x * y$.

Remark.
Note that xy is different from yx, as the group operation need not be commutative. If x and y are two elements such that $xy = yx$, then we say that x and y *commute* with each other. Every element commutes with the identity element. Obviously, each element also commutes with itself. If y is an inverse of x, then $xy = yx = e$, which means that x and y commute with each other.

Example 2.

- The set $\mathbb{Z}$ of integers forms a group under the usual addition $+$. The sum of any two integers is also an integer, thus $+$ is indeed a binary operation on $\mathbb{Z}$ (in other words, $\mathbb{Z}$ is closed under $+$). The identity element of this group is 0, since $n + 0 = 0 + n = n$ for all $n \in \mathbb{Z}$. Finally, for any integer n, we know that $n + (-n) = (-n) + n = 0$, so that $-n$, which is also an integer, is the inverse of n. This a group of infinite order.
- $(\mathbb{Z}, -)$ is **not** a group, since $-$ is not associative (nor is there an identity element for subtraction, since $n - e = n$ only if $e = 0$, but then $e - n = 0 - n = -n \neq n$; and without an identity element, inverses are not defined).
- Similarly, the rationals, reals, and complex numbers also form groups under addition: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$. All three are infinite groups.
- The set of non-negative integers $\mathbb{N}_0 = \{0, 1, 2, \cdots\}$ does **not** form a group under addition.

Example 2.

- Let $G = \{0\}$, the singleton set containing only the real number 0. Then $(G, +)$ is a group. Its order is 1, and it is therefore the smallest group.
- The set of non-zero real numbers forms a group under multiplication: $(\mathbb{R} - \{0\}, \times)$. The identity element is 1 and the inverse of $x \in \mathbb{R}$, $x \neq 0$, is $1/x$ (which is also a non-zero real number). If we include 0, it is no longer a group, since 0 has no (multiplicative) inverse.
- If $\mathbb{R}_{>0}$ denotes the set of all positive real numbers, $(\mathbb{R}_{>0}, \times)$ is also a group.
- Let $G = \{1\}$, $H = \{1, -1\}$, and $K = \{1, i, -1, -i\}$, where $i = \sqrt{-1}$. Then $(G, \times)$, $(H, \times)$ and $(K, \times)$ are groups of orders 1, 2, and 4 respectively.

Example 2.

- A square matrix A is *non-singular* (or *invertible*) if its determinant is non-zero: $\det A \neq 0$. The set of all $n \times n$ non-singular real matrices forms a group under matrix multiplication, denoted $GL_n(\mathbb{R})$. Matrix multiplication is associative, the identity matrix is the identity element for this multiplication, and every non-singular matrix A has an inverse A^{-1} (which is also non-singular). Note that $GL_n(\mathbb{R})$ is certainly closed under multiplication, as $\det(AB) = (\det A)(\det B) \neq 0$ whenever $\det A, \det B \neq 0$. For $n > 1$, $GL_n(\mathbb{R})$ is an example of a group where the operation is not *commutative* – if A and B are two $n \times n$ matrices AB is generally not equal to BA. Example: $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

Example 2.

- Let X be any non-empty set, and let $S(X)$ denote the set of all bijections from X to itself. That is,

$$S(X) = \{ f : X \to X \mid f \text{ is 1-1 and onto} \}$$

  Then $S(X)$ forms a group under composition of functions. For function composition is associative, the identity function (that maps every element $x \in X$ to x itself) is the identity element, and every bijective function $f : X \to X$ has an inverse $f^{-1} : X \to X$ that is also bijective. If X has three or more elements (possibly an infinite number of elements) then $S(X)$ is not commutative.

- If $X = \{1, 2, \ldots, n\}$, then $S(X)$ is written as S_n, and is called the symmetric group.

Basic Properties of Groups

Every group has a unique identity element.

For, suppose e_1 and e_2 are both identity elements of a group G (i.e., both e_1 and e_2 satisfy the equations when written in place of e in Axiom 2).

Then $e_1 = e_1 e_2 = e_2$.

The former equality is true because e_2 is an identity element (so $xe_2 = x$ for any x), and the latter equality is true because e_1 is an identity element.

Thus, we see that $e_1 = e_2$.

Basic Properties of Groups

Every element of a group has a unique inverse.

Let x be an element of a group G.

By Axiom 3, it has an inverse, say y. Suppose z is also an inverse of x.

Then, if e denotes the identity element of G,

$$y = ye = y(xz) = (yx)z = ez = z$$

The second equality follows from z being an inverse of x; the third one from associativity; and the fourth from y being an inverse of x.

Since each element x is guaranteed to have a unique inverse, we can denote this inverse as x^{-1}. From Axiom 3, it is clear that if y is an inverse of x, then x is also an inverse of y. Thus, $(x^{-1})^{-1} = x$.

Exercise 1.
Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Exercise 1.
Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. To show that $a^{-1} = b$, we need to verify that $ab = e$ and $ba = e$.

Here, therefore, we must verify $(xy)(y^{-1}x^{-1}) = e$.

Exercise 1.
Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. To show that $a^{-1} = b$, we need to verify that $ab = e$ and $ba = e$.

Here, therefore, we must verify $(xy)(y^{-1}x^{-1}) = e$.

Indeed,

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} \quad \text{[Associativity]}$$

Exercise 1.
Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. To show that $a^{-1} = b$, we need to verify that $ab = e$ and $ba = e$.

Here, therefore, we must verify $(xy)(y^{-1}x^{-1}) = e$.

Indeed,

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} \quad \text{[Associativity]} \\ &= xex^{-1}\end{aligned}$$

Exercise 1.
Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. To show that $a^{-1} = b$, we need to verify that $ab = e$ and $ba = e$.

Here, therefore, we must verify $(xy)(y^{-1}x^{-1}) = e$.

Indeed,

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} \quad \text{[Associativity]} \\ &= xex^{-1} \\ &= xx^{-1}\end{aligned}$$

Exercise 1.
Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. To show that $a^{-1} = b$, we need to verify that $ab = e$ and $ba = e$.

Here, therefore, we must verify $(xy)(y^{-1}x^{-1}) = e$.

Indeed,

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} \quad \text{[Associativity]} \\ &= xex^{-1} \\ &= xx^{-1} \\ &= e.\end{aligned}$$

Exercise 1.
Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. To show that $a^{-1} = b$, we need to verify that $ab = e$ and $ba = e$.

Here, therefore, we must verify $(xy)(y^{-1}x^{-1}) = e$.

Indeed,

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} \quad \text{[Associativity]} \\ &= xex^{-1} \\ &= xx^{-1} \\ &= e.\end{aligned}$$

Similarly, $(y^{-1}x^{-1})(xy) = e$. Thus, $(xy)^{-1} = y^{-1}x^{-1}$.

Exercise 2 (Cancellation Laws).
Prove that the (left and right) cancellation laws hold in every group. That is, prove that if x and y are elements of a group G, then

1. If $\exists a \in G$, $ax = ay$, then $x = y$.
2. If $\exists b \in G$, $xb = yb$, then $x = y$.

Exercise 2 (Cancellation Laws).
Prove that the (left and right) cancellation laws hold in every group. That is, prove that if x and y are elements of a group G, then

1. If $\exists a \in G$, $ax = ay$, then $x = y$.
2. If $\exists b \in G$, $xb = yb$, then $x = y$.

Solution.

1. Left-multiplying by a^{-1}, we have $ax = ay$

Exercise 2 (Cancellation Laws).
Prove that the (left and right) cancellation laws hold in every group. That is, prove that if x and y are elements of a group G, then

1. If $\exists a \in G$, $ax = ay$, then $x = y$.
2. If $\exists b \in G$, $xb = yb$, then $x = y$.

Solution.

1. Left-multiplying by a^{-1}, we have $ax = ay \implies a^{-1}(ax) = a^{-1}(ay)$

Exercise 2 (Cancellation Laws).
Prove that the (left and right) cancellation laws hold in every group. That is, prove that if x and y are elements of a group G, then

1. If $\exists a \in G$, $ax = ay$, then $x = y$.
2. If $\exists b \in G$, $xb = yb$, then $x = y$.

Solution.

1. Left-multiplying by a^{-1}, we have $ax = ay \implies a^{-1}(ax) = a^{-1}(ay) \implies (a^{-1}a)x = (a^{-1}a)y$

Exercise 2 (Cancellation Laws).
Prove that the (left and right) cancellation laws hold in every group. That is, prove that if x and y are elements of a group G, then

1. If $\exists a \in G$, $ax = ay$, then $x = y$.
2. If $\exists b \in G$, $xb = yb$, then $x = y$.

Solution.

1. Left-multiplying by a^{-1}, we have $ax = ay \implies a^{-1}(ax) = a^{-1}(ay) \implies (a^{-1}a)x = (a^{-1}a)y \implies ex = ey$

Exercise 2 (Cancellation Laws).
Prove that the (left and right) cancellation laws hold in every group. That is, prove that if x and y are elements of a group G, then

1. If $\exists a \in G$, $ax = ay$, then $x = y$.
2. If $\exists b \in G$, $xb = yb$, then $x = y$.

Solution.

1. Left-multiplying by a^{-1}, we have $ax = ay \implies a^{-1}(ax) = a^{-1}(ay) \implies (a^{-1}a)x = (a^{-1}a)y \implies ex = ey \implies x = y$.

Exercise 2 (Cancellation Laws).
Prove that the (left and right) cancellation laws hold in every group. That is, prove that if x and y are elements of a group G, then

1. If $\exists a \in G$, $ax = ay$, then $x = y$.
2. If $\exists b \in G$, $xb = yb$, then $x = y$.

Solution.

1. Left-multiplying by a^{-1}, we have $ax = ay \implies a^{-1}(ax) = a^{-1}(ay) \implies (a^{-1}a)x = (a^{-1}a)y \implies ex = ey \implies x = y$.
2. Similarly, right-multiplying by b^{-1}, $xb = yb \implies x = y$.

Exercise 3.
If x and y are two elements of G that commute, then show that x, y, x^{-1}, and y^{-1} all commute with one another.

Exercise 3.
If x and y are two elements of G that commute, then show that x, y, x^{-1}, and y^{-1} all commute with one another.

Solution. Pre- and post-multiplying by x^{-1}, the equation $xy = yx$ becomes

$$x^{-1}(xy)x^{-1} = x^{-1}\underbrace{(\,yx\,)}_{x \text{ and } y \text{ commute}}x^{-1} \implies yx^{-1} = x^{-1}y.$$

Exercise 3.
If x and y are two elements of G that commute, then show that x, y, x^{-1}, and y^{-1} all commute with one another.

Solution. Pre- and post-multiplying by x^{-1}, the equation $xy = yx$ becomes

$$x^{-1}(xy)x^{-1} = x^{-1}\underbrace{(\,yx\,)}_{x \text{ and } y \text{ commute}}x^{-1} \implies yx^{-1} = x^{-1}y.$$

Thus, if x and y commute, then so do x and y^{-1}.

Exercise 3.
If x and y are two elements of G that commute, then show that x, y, x^{-1}, and y^{-1} all commute with one another.

Solution. Pre- and post-multiplying by x^{-1}, the equation $xy = yx$ becomes

$$x^{-1}(xy)x^{-1} = x^{-1}\underbrace{(\,yx\,)}_{x \text{ and } y \text{ commute}}x^{-1} \implies yx^{-1} = x^{-1}y.$$

Thus, if x and y commute, then so do x and y^{-1}.

By symmetry, x^{-1} and y commute as well.

Exercise 3.
If x and y are two elements of G that commute, then show that x, y, x^{-1}, and y^{-1} all commute with one another.

Solution. Pre- and post-multiplying by x^{-1}, the equation $xy = yx$ becomes

$$x^{-1}(xy)x^{-1} = x^{-1}\underbrace{(\,yx\,)}_{x \text{ and } y \text{ commute}}x^{-1} \implies yx^{-1} = x^{-1}y.$$

Thus, if x and y commute, then so do x and y^{-1}.

By symmetry, x^{-1} and y commute as well.

Applying this result to the commuting pair x and y^{-1}, we see that x^{-1} and y also commute.

Exercise 3.
If x and y are two elements of G that commute, then show that x, y, x^{-1}, and y^{-1} all commute with one another.

Solution. Pre- and post-multiplying by x^{-1}, the equation $xy = yx$ becomes

$$x^{-1}(xy)x^{-1} = x^{-1}\underbrace{(\,yx\,)}_{x \text{ and } y \text{ commute}}x^{-1} \implies yx^{-1} = x^{-1}y.$$

Thus, if x and y commute, then so do x and y^{-1}.

By symmetry, x^{-1} and y commute as well.

Applying this result to the commuting pair x and y^{-1}, we see that x^{-1} and y also commute.

Finally, every element commutes with its own inverse.

Definition 3.

Associativity allows us to write an expression of the form $x_1 \cdot x_2 \cdots x_n$ (where $x_1, \cdots, x_n \in G$) without ambiguity. Let $x \in G$. For any positive integer n, define

$$x^n = \underbrace{x \cdot x \cdots x}_{n \text{ times}}.$$

Then define $x^{-n} = (x^{-1})^n$ and $x^0 = e$.

Exercise 4.
Let $x \in G$, and let m and n be integers. Prove the following.

1. $x^{-n} = (x^n)^{-1}$
2. $x^m \cdot x^n = x^{m+n}$
3. $(x^m)^n = x^{mn}$

Note: In each case, m and n may (independently) be positive, negative, or zero. Since the definition of x^n is different when n is positive, negative, and zero, the proof must deal with all these cases separately.

Abelian Groups

Definition 4.
A group $(A, *)$ is said to be Abelian or commutative if $*$ is a commutative operation.
That is,

$$\forall a, b \in A, a * b = b * a.$$

A group that is not Abelian is non-Abelian.

Exercise 5.
Let G be a group.

1. Prove that if every element of G is self-inverse, then G is Abelian. Is the converse true?

   Solution. Suppose every element of G is self-inverse.
   That is, for all $x \in G$, $x^{-1} = x$.
   Let $a, b \in G$. We know that $(ab)^{-1} = b^{-1}a^{-1}$.
   But since all elements are self-inverse, this reduces to $ab = ba$.
   The converse is not true. For example, $(\mathbb{Z}, +)$ is an Abelian group in which not all elements are self inverse.

2. Prove that G is Abelian if and only if $\forall x, y \in G$, $(xy)^{-1} = x^{-1}y^{-1}$.
   Solution. If G is Abelian, then $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$.
   Conversely, suppose G satisfies the given property.
   Then for any two elements x and y,
   $(xy)^{-1} = x^{-1}y^{-1} \implies xy = (x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx$.
3. Prove that G is Abelian iff $\forall a, b \in G$, $(ab)^2 = a^2b^2$.
   Solution. If G is Abelian, then $(ab)^2 = abab = aabb = a^2b^2$.
   Conversely,
   $(ab)^2 = a^2b^2 \implies abab = aabb \implies ba = ab$ (by left and right cancellation).

Subgroups

Subgroups

Definition 5.

A subgroup of a group $(G, *)$ is a subset $H \subseteq G$ such that $(H, *)$ is also a group. Then we write $H \leq G$.

Example 6.
In Example 2, we saw that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all forms groups under addition. Observe that $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Similarly, $\mathbb{Q} - \{0\}$, $\mathbb{R}_{>0}$, and $\mathbb{R} - \{0\}$ are all groups under multiplication. The former two are subsets of the latter. All of these are examples of subgroups.

Remark.
It is very important that the operation be the same, for otherwise it is meaningless to call one the subgroup of the other. For example, $(\mathbb{Q} - \{0\}, \times)$ is *not* a subgroup of $(\mathbb{R}, +)$, even though $\mathbb{Q} - \{0\} \subseteq \mathbb{R}$.

Given a subset H of a group G, to check whether H is a subgroup, we need to verify that H satisfies the group axioms.

It is obvious that all elements of H will satisfy associativity, since they are elements of G as well.

The closure of H under the group operation of G needs to be checked carefully, since the result of applying the operation to two elements of H may be an element of G that is outside H.

To verify the existence of identity and inverses, it is enough to check if the identity element of the group G, which is already known, is present in the subset H, and similarly in the case of inverses.

These observations are summarised in the following lemma.

Lemma 7.

Let $(G, *)$ be a group and $H \subseteq G$. Then H is a subgroup of G if and only if all of the following hold.

1. *H is closed under $*$. That is, $\forall x, y \in H$, $x * y \in H$.*
2. *H contains the identity element (of G): $e \in H$.*
3. *The inverse of every element of H is also in H. That is, $\forall x \in H$, $x^{-1} \in H$.*

Theorem 8.

A subset H of a group G is a subgroup of G if and only if $H \neq \varnothing$ and $\forall x, y \in H$, $xy^{-1} \in H$.

Proof.
If $H \leq G$, then it is obviously non-empty (for $e \in H$) and for any $x, y \in H$, we have $x, y^{-1} \in H$ (since H contains the inverses of all its elements), and therefore $xy^{-1} \in H$ (by closure).

Conversely, suppose it is given that $H \neq \varnothing$ and $\forall x, y \in H$, $xy^{-1} \in H$.

(i) Since $H \neq \varnothing$, $\exists x \in H$. Then $x, x \in H \implies xx^{-1} \in H \implies e \in H$.

(ii) Now if $x \in H$, then $e, x \in H \implies ex^{-1} = x^{-1} \in H$.

(iii) Finally, if $x, y \in H$, then by what we have proved above, $y^{-1} \in H$. Thus, $x, y^{-1} \in H \implies x(y^{-1})^{-1} \in H$ (by the assumption on H), thus $xy \in H$.

□

Example 9.
Let G be the group of non-zero complex numbers under multiplication, and let $\omega = e^{\frac{2\pi i}{n}}$, where n is a positive integer, so that ω is a primitive n^{th} root of unity.

Then $H = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ is a subgroup of G.

Clearly, $H \neq \varnothing$.

The elements of H are all the complex numbers of the form ω^r for some integer r. Thus, if ω^r and ω^s are any two elements of H, then $\omega^r \cdot (\omega^s)^{-1} = \omega^{r-s}$ is also an element of H.

Then by Theorem 8, $H \leq G$.

Theorem 10.

Let H and K be any two subgroups of a group G. Then

1. $H \cap K \leq G$
2. $H \cup K$ *is not a subgroup of* G *unless* $H \subseteq K$ *or* $K \subseteq H$.

Proof.

1. Since $e \in H$ and $e \in K$, $e \in H \cap K \neq \varnothing$.
   Now if $x, y \in H \cap K$, then $x, y \in H \implies xy^{-1} \in H$ and
   $x, y \in K \implies xy^{-1} \in K$, and therefore, $xy^{-1} \in H \cap K$. Thus, $H \cap K \leq G$.
2. Suppose that neither one of H and K is contained in the other.
   Then there exists an element $h \in H$ such that $h \notin K$, and similarly, $\exists k \in K$, $k \notin H$.
   Now, hk cannot be an element of H, since $hk \in H \implies h^{-1}hk = k \in H$.
   Similarly, $hk \notin K$. Therefore, $hk \notin H \cup K$. Since $H \cup K$ is not closed under the operation, it is not a subgroup of G.
   If $H \subseteq K$, then $H \cup K = K \leq G$. The other case is similar.

□

For subgroups H and K of a group G, define

$$HK = \{\, hk \mid h \in H, k \in K \,\}.$$

Note that HK and KH are *subsets* of the group G (but not necessarily subgroups), and in general, $HK \neq KH$.

Every element of HK is of the form hk, where $h \in H$ and $k \in K$.

Therefore, $HK = KH$ if and only if for every element $hk \in HK$, $hk = k'h'$ for some $k' \in K$ and $h' \in H$[1].

[1] Here, h' is not necessarily equal to h, and k' is not necessarily equal to k.

Theorem 11.

Let G be a group and $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.

Proof.
First, suppose that $HK \leq G$.

Let $x \in HK$.

Then (since $HK \leq G$), $x^{-1} \in HK \implies x^{-1} = hk$, $\exists h \in H$, $k \in K$.

Now, $x = (hk)^{-1} = k^{-1}h^{-1}$, which is an element of KH since $k^{-1} \in K$ and $h^{-1} \in H$.

Thus, $x \in HK \implies x \in KH$, which shows that $HK \subseteq KH$.

To see that $KH \subseteq HK$ as well, consider an arbitrary element $kh \in KH$.

Now $(kh)^{-1} = h^{-1}k^{-1} \in HK \implies ((kh)^{-1})^{-1} = kh \in HK$ (since $HK \leq G$).

Therefore, $HK = KH$.

Theorem 11.

Let G be a group and $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.

Proof.
Conversely, suppose that $HK = KH$. Since H and K are non-empty, so is HK.

Now let $x, y \in HK$. We shall show that $xy^{-1} \in HK$.

We know that $x = h_1k_1$, $y = h_2k_2$, for some $h_1, h_2 \in H$, $k_1, k_2 \in K$. Then

$$\begin{aligned} xy^{-1} &= (h_1k_1)(h_2k_2)^{-1} = h_1 \underbrace{k_1k_2^{-1}}_{\in K} h_2^{-1} \\ &= h_1 \underbrace{k_3h_2^{-1}}_{\in KH=HK}, \quad k_3 = k_1k_2^{-1} \\ &= h_1h_3k_4, \quad \exists h_3 \in H, k_3 \in K \\ &= h_4k_4, \quad h_4 = h_1h_3 \in H \end{aligned}$$

$\implies xy^{-1} \in HK$. Thus, $HK \leq G$. □

Exercise 6.
Let G be a group.

1. The centre of G is defined by $Z(G) = \{ z \in G \mid zx = xz, \ \forall x \in G \}$. Prove that $Z(G) \leq G$.
2. Let $S \subseteq G$. Then the centraliser of S in G is $C_G(S) = \{ y \in G \mid yx = xy, \ \forall x \in S \}$. Prove that $C_G(S) \leq G$.
3. Show that any subgroup of an Abelian group is Abelian.
4. Let G be Abelian. For $n \in \mathbb{N}_0$, define $H = \{ x^n \mid x \in G \}$. Show that $H \leq G$.
5. Let G be Abelian. For $n \in \mathbb{N}_0$, define $H = \{ x \in G \mid x^n = e \}$. Show that $H \leq G$.

Definition 12.

Let G be a group and x any element of G. The cyclic subgroup of G generated by x is defined to be

$$\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}.$$

That is, $\langle x \rangle$ is the subset containing all powers (positive, negative, and zero) of x. Thus, every element of $\langle x \rangle$ is of the form x^k for some integer k, and vice-versa for every integer k, the element x^k is in $\langle x \rangle$.Clearly, it is a subgroup.

Remark.
In any group, the identity element generates the trivial subgroup: $\langle e \rangle = \{e\}$. It is the only one that does (since for all $x \in G$, $x \in \langle x \rangle$).

Any element generates the same subgroup as its inverse: $\langle x \rangle = \langle x^{-1} \rangle$.

Definition 13.
A group G is said to be cyclic if it is equal to the cyclic subgroup generated by one of its elements. That is, G is cyclic if there exists an element $g \in G$ such that $G = \langle g \rangle$. Then g is a generator of G.

If $a = g^i$ and $b = g^j$ are any two elements of a cyclic group $G = \langle g \rangle$, then $ab = x^i \cdot x^j = x^{i+j} = x^{j+i} = x^j \cdot x^i = ba$.

Thus, any cyclic group is Abelian. But the converse is not true.

Example 14.

Let $\omega = e^{\frac{2\pi i}{n}}$, where $i = \sqrt{-1}$, so that $\omega^n = 1$ (i.e., ω is a primitive n^{th} root of unity). Then $G = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ is a group under (complex) multiplication.

G is cyclic, since every element of G is a power of ω, so that $G = \langle \omega \rangle$.

Exercise: Prove that if n is prime, then every non-identity element of G is a generator of G.

Example 15.

$\mathbb{Z} = \langle 1 \rangle$, since every integer n can be written as $n \times 1$. (Recall that we write $\mathbb{Z}$ in additive notation, and therefore write nx instead of x^n).

Thus, the group of integers under addition is an infinite cyclic group.

Note that $\mathbb{Z} = \langle -1 \rangle$ as well, since -1 is the inverse of 1.

Exercise: Prove that 1 and -1 are the only generators of $\mathbb{Z}$.

Example 16.

Let V_4 denote the group formed by $\{1, 3, 5, 7\}$ under multiplication modulo 8. This is indeed a group – multiplication modulo n is associative for any integer n, and the other axioms are easily seen to hold from the multiplication table given below.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Every element of this group is self-inverse, and therefore the group is Abelian. However, it is *not* cyclic. Each non-identity element generates a subgroup of order 2.

$$\langle 3 \rangle = \{1, 3\} \qquad \langle 5 \rangle = \{1, 5\} \qquad \langle 7 \rangle = \{1, 7\}$$

This is so precisely because every element is self-inverse! This group V_4 is called the Klein 4-group (or Vierergruppe) and is the **smallest non-cyclic group**.

Theorem 17.
Every subgroup of a cyclic group is cyclic.

Proof.
Consider a cyclic group $G = \langle g \rangle$ with generator g.

Let H be any subgroup of G. Every element of H is of the form g^k, for some integer k.

Let n be the least positive integer such that $g^n \in H$.

Claim: $H = \langle g^n \rangle$.

To prove this, we must show that every element of H is a power of g^n.

Let g^m be an arbitrary element of H. By the division algorithm,

$$m = nq + r, \quad \exists q, r \in \mathbb{Z}, \quad 0 \leq r < n.$$

That is, we can divide m by n to obtain a quotient q and a remainder r (which must be a non-negative number less than n).

Theorem 17.
Every subgroup of a cyclic group is cyclic.

Proof.
Now,

$$\begin{aligned} g^m &= g^{nq+r} \\ &= (g^n)^q \cdot g^r \implies \\ g^r &= (g^n)^{-q} \cdot g^m. \end{aligned}$$

Since $g^n, g^m \in H$, this implies $g^r \in H$. But n is the least positive integer such that $g^n \in H$, and $n > r \geq 0$, therefore, $r = 0$.

Thus we have $g^m = (g^n)^q$, as required. □

Definition 18.

The order of an element x of a group G is defined as the least positive integer n, if any, such that $x^n = e$. If there is no such positive integer, then the element is said to have infinite order. The order of x is denoted by $|x|$ or $\mathrm{o}(x)$.

Remark.
The order of an *element* and the order of a *(sub)group* are defined differently – but the order of an element is called so because it is the order of the cyclic subgroup generated by that element (proved below).

Theorem 19.
For any element $x \in G$, $\mathrm{o}(x) = \mathrm{o}(\langle x \rangle)$.

Proof.
Exercise. (Note that on the LHS, the order is that of an element, and on the RHS, it is that of a subgroup – use the appropriate definition in each case). □

Definition 20.

Let G be a group and H a subgroup of G.

For any element $x \in G$, the left coset of H with respect to x is defined to be the set

$$xH = \{ xh \mid h \in H \}.$$

The right coset of H with respect to x is

$$Hx = \{ hx \mid h \in H \}.$$

Remark.
The subgroup H itself is a coset (of itself): $H = eH = He$. In fact, note that for any $h \in H$, $hH = Hh = H$ (for clearly, $hH, Hh \subseteq H$; prove that $H \subseteq hH, Hh$).

We shall show that left cosets of a subgroup partition the whole group into equally sized parts.

Theorem 21 (Lagrange).

If G is a finite group and H a subgroup of G, the order of H divides the order of G:

$$\mathrm{o}(H) \mid \mathrm{o}(G).$$

To prove the theorem, we first establish three lemmas describing how the cosets partition the group.

In the following, let G be a finite group, $H \leq G$, and let $x_1H, \ldots, x_kH$ be all the distinct left cosets of H in G.

Lemma 22.

$$G = \bigcup_{i=1}^{k} x_i H$$

Proof.
Every element is in the coset of H with respect to that element.

That is, $\forall x \in G$, $x \in xH = x_iH$ for some $i = 1, \ldots, k$. □

This does only half the work in showing that the left cosets *partition* the group. The other half is to show that distinct cosets are disjoint.

Lemma 23.

Distinct left cosets of H are disjoint.

Proof.
Suppose $xH \cap yH \neq \varnothing$.

Then $\exists z \in xH \cap yH$, so that $z = xh_1 = yh_2$, $\exists h_1, h_2 \in H$.

Then $y = xh_1h_2^{-1}$.

Now, for any $yh \in yH$, $yh = x \underbrace{h_1h_2^{-1}h}_{\in H} \implies yh \in xH$.

Thus, $yH \subseteq xH$.

Similarly, $xH \subseteq yH$, and therefore, $xH = yH$. □

Lemma 24.

Any two left cosets of H have the same cardinality.

Proof.
Let xH be any left coset of H.

We show that $|xH| = |H|$, by proving the existence of a bijection between H and xH.

Define $f : H \to xH$, $\forall h \in H$, $f(h) = xh$.

This mapping is injective since $f(h_1) = f(h_2) \implies xh_1 = xh_2 \implies h_1 = h_2$, by left cancellation.

It is surjective since every element of xH is of the form xh, $\exists h \in H$, but $xh = f(h)$.

Thus, f is a bijection and $|xH| = |H|$.

This also proves that all the left cosets are in bijection with one another and therefore have the same cardinality. □

Proof of Lagrange's theorem.

From Lemma 22, $G = \bigcup_{i=1}^{k} x_i H \implies$

$$\begin{aligned} \mathrm{o}(G) &= \left| \bigcup_{i=1}^{k} x_i H \right| \\ &= \sum_{i=1}^{k} |x_i H| \quad \text{[Lemma 23]} \\ &= \sum_{i=1}^{k} |H| \quad \text{[Lemma 24]} \\ &= k \times \mathrm{o}(H). \end{aligned}$$

Thus, $\mathrm{o}(H) \mid \mathrm{o}(G)$. □

Remark.

The integer $\frac{o(G)}{o(H)}$ is the number of left cosets of H in G, and is called the index of the subgroup H in G, denoted $|G : H|$. Note that all the results above could equivalently be written in terms of *right cosets*. Thus, the number of right cosets of H in G is also $|G : H|$.

Corollary 25.

The order of every element of a finite group divides the order of the group.

Proof.
Exercise. □

Corollary 26.

Any group of prime order is cyclic.

Proof.
Let G be a group of order p, where p is a prime number.

Since $p \geq 2$, G has at least one non-identity element, say g.

By Corollary 25, $\mathrm{o}(g) \mid p$, which implies that $\mathrm{o}(g) = 1$ or p.

But $g \neq e \implies \mathrm{o}(g) \neq 1$.

Thus, $\mathrm{o}(\langle g \rangle) = \mathrm{o}(g) = p \implies G = \langle g \rangle$. □

Normal Subgroups

Normal Subgroups

Given a group G, the conjugate of an element $g \in G$ by an element $x \in G$ is the element xgx^{-1}. Note that xgx^{-1} is different from g unless x commutes with g. If $S \subseteq G$ and x is any element of G, then we define

$$xSx^{-1} = \{ xSx^{-1} \mid n \in H \}$$

which is the set of all conjugates of elements of S by the (fixed) element x.

Observe $H \leq G \implies xHx^{-1} \leq G$. (Exercise: Prove this). But in general, xHx^{-1} may not be equal to H itself. Based on this, we define a special kind of subgroup.

Definition 27.

A subgroup N of a group G is said to be normal if $\forall x \in G$, $xNx^{-1} \subseteq N$. Then we write $N \trianglelefteq G$ or $N \triangleleft G$.

Note that the statement $xNx^{-1} \subseteq N$ is equivalent to the statement that for all $n \in N$, $xnx^{-1} \in N$.

Example 28.
For any group, the trivial subgroup and the whole group are always normal subgroups. A non-trivial group that has no normal subgroups other than these two is called a simple group.

Exercise 7.

1. If G is an Abelian group, which subgroups of G are normal?
2. Prove that a finite Abelian group is simple if and only if its order is a prime number. Hint: Every element generates a subgroup.
3. For any group G, prove that its centre $Z(G)$ is always a normal subgroup.
4. Let $H \leq G$ (not necessarily normal), and define $N = \bigcap_{x \in G} xHx^{-1}$. Show that $N \trianglelefteq G$.
5. Let N be a subgroup of index 2 in G (i.e., $|G : N| = 2$). Show that $N \trianglelefteq G$. Hint: If N has only two left cosets, and only two right cosets, and one of them is N in each case, what is the other?

Theorem 29.
Let $N \leq G$. Then $N \trianglelefteq G$ if and only if $\forall x \in G$, $xNx^{-1} = G$.

Proof.
If $N \trianglelefteq G$, then for any $x \in G$, $xNx^{-1} \subseteq N$. We must prove that $N \subseteq xNx^{-1}$ as well.

Let $n \in N$. Now (with x^{-1} in place of x),
$x^{-1}Nx \subseteq N \implies x^{-1}nx \in N \implies x^{-1}nx = n'$, for some $n' \in N$.

Then $n = xn'x^{-1} \in xNx^{-1}$.

Thus, $\forall n \in N$, $n \in xNx^{-1}$, which shows that $N \subseteq xNx^{-1}$.

Conversely, if $\forall x \in G$, $xNx^{-1} = N$, then *a fortiori*, $\forall x \in G$, $xNx^{-1} \subseteq N$, so that $N \trianglelefteq G$. □

Theorem 30.
Let $N \leq G$. Then $N \trianglelefteq G$ if and only if $\forall x \in G$, $xN = Nx$.

Proof.
Suppose that $N \trianglelefteq G$.

Let $x \in G$. Now for any $n \in N$, $xnx^{-1} \in n'$, $\exists n' \in N$.

Therefore, $xn = n'x \in Nx$.

Thus, $xN \subseteq Nx$.

Similarly, $x^{-1}nx = n''$, $\exists n'' \in N$ implies $nx = xn''$, and thus, $Nx \subseteq xN$.

Therefore, $xN = Nx$.

For the converse, suppose that $\forall x \in G$, $xN = Nx$.

Let $x \in G$, $n \in N$. Then $xn = n'x$, $\exists n' \in N$, which implies that $xnx^{-1} = n' \in N$.

Thus, $xNx^{-1} \subseteq N$, and we have $N \trianglelefteq G$. □