Group Theory

Contents

List of Symbols

$\forall$	For all/any
$\exists$	For some / There exists
$a \in S$	a belongs to / is an element of set S
$\cup$, $\cap$	Union and intersection (respectively) of sets
$\varnothing$	Empty set $\{\}$
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	Sets of natural numbers, integers, rational numbers, real numbers, complex numbers (respectively)
$\mathbb{N}_0$	Set of non-negative integers $\{0, 1, 2, \ldots\}$
$\mathbb{R}_{>0}$	Set of positive real numbers
$A \subseteq B$	A is a subset of set B
$\lvert S \rvert$	Cardinality (number of elements) of set S
$\mathrm{o}(G)$	Order of group G
$\mathrm{o}(x)$	Order of element x
x^{-1}	Inverse of element x in a group
$H \leq G$	H is a subgroup of G
$H \trianglelefteq G$	H is a normal subgroup of G
$G \cong H$	Group G is isomorphic to group H
$\langle x \rangle$	Cyclic subgroup generated by element x of a group
xH, Hx	Left and right cosets (respectively) of subgroup H of group G
HK	The set $\{hk \mid h \in H, k \in K\}$ with $H, K \leq G$
$\lvert G : H \rvert$	Index of subgroup H in group G
xHx^{-1}	$\{ xhx^{-1} \mid h \in H \}$
$Z(G)$	Centre of group G

$C_G(S)$	Centraliser of subset S of group G
$\langle H, K \rangle$	Join of subgroups H and K of group G
$SL(G)$	Subgroup lattice of group G
$NL(G)$	Normal subgroup lattice of group G
V_4	Klein 4-group
S_n	Symmetric group on n elements – group of all permutations of $\{1, \ldots, n\}$
$\mathbb{Z}_n$	The integers modulo n
Q_8	Quaternion group

1 Introduction

Definition 1.1. 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: $\forall x \in G$, $\exists y \in G$, $x * y = y * x = e$ (where e is the identity element defined in the previous axiom). 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., for any two elements x and y of G, the element $x * y$ also belongs to 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.

Example 1.2.
1. 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.
2. $(\mathbb{Z}, -)$ 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).
3. Similarly, the rationals, reals, and complex numbers also form groups under addition: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$. All three are infinite groups.
4. The set of non-negative integers $\mathbb{N}_0 = \{0, 1, 2, \cdots\}$ does **not** form a group under addition. (Why?)
5. 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. (Why does the empty set $\varnothing$ not form a group?)

6. 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.

7. Is $(\mathbb{Z} - \{0\}, \times)$ a group?

8. If $\mathbb{R}_{>0}$ denotes the set of all positive real numbers, $(\mathbb{R}_{>0}, \times)$ is also a group. (Verify this carefully).

9. Note that if $G = \mathbb{R}_{<0}$ (the set of negative reals), then $(\mathbb{R}_{<0}, \times)$ is **not** a group. Which axiom fails? Multiplication is associative, so Axiom 1 holds. The multiplicative identity is 1, which is not present in G. We can remedy this by redefining G to be $G = \mathbb{R}_{<0} \cup \{1\}$. Associativity still holds, and now G has an identity element as well. Axiom 3 holds as well, since the multiplicative inverse of any negative real number x is the negative real number $1/x$. Thus, all axioms hold. However, the operation $\times$ is not a binary operation on G at all! For example, -1 and -2 are elements of G, but their product $(-1)(-2) = +2$ is not an element of G.

10. 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.

11. 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, since $\det(AB) = (\det A)(\det B) \neq 0$ 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: $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

12. 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.

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

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.

1.1 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 $e_1 = e_2$.

Similarly, 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 1.1. 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 1.2 (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 1.3. 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 $x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1} \implies yx^{-1} = x^{-1}y$. 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. And every element commutes with its own inverse. This concludes the proof.

Definition 1.3. 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 be an element of a group 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 1.4. Let $x \in G$, and let m and n be integers. With the notation given in Definition 1.3, 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 that in each case, m and n may be (independently) 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.

Remark. If the operation in a group G is denoted by $+$ (whether this denotes the usual addition of numbers, or the addition of vectors, or something else altogether depending on what the elements of G are), the notation used in studying this group is said to be *additive*. Additive notation is usually (not always) used when the operation of G is commutative. In additive notation, we write the identity element as 0 (again, this may denote the real number 0, or the zero vector, or something else). We also write $-x$ instead of x^{-1} to denote the inverse of x, and nx instead of x^n, to denote $\underbrace{x + x + \cdots + x}_{n}$.

Thus in this notation, $0x = 0$ and $(-n)x = n(-x) = -nx$.

1.2 Abelian groups

We have seen that the operation in a group is not necessarily commutative. Now we define a special class of groups with a commutative operation.

Definition 1.4. 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, of course, *non-Abelian*. In Example 1.2, the groups defined in 11, 12, and 13 are non-Abelian.

Exercise 1.5. 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 (in fact, 0 is the only self-inverse element of this group).

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).

2 Subgroups

In Example 1.2, 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. These are all examples of subgroups.

Definition 2.1. A *subgroup* of a group $(G, *)$ is a subset $H \subseteq G$ such that $(H, *)$ is also a group. Then we write $H \leq G$.

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. On the other hand, 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. (For example, the subset of odd integers is not a subgroup of $(\mathbb{Z}, +)$, since the sum of two odd integers is an even integer). 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 lemma below.

Lemma 2.2. *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, $\forall x \in H$, $x^{-1} \in H$.*

We can, in some sense, combine closure and existence of inverses to obtain two different conditions that characterise subgroups. In many cases, it becomes easier to check these two conditions than to check the three given above.

Theorem 2.3. *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 $H \neq \emptyset$, $\exists x \in H$. Then $x, x \in H \implies xx^{-1} \in H \implies e \in H$, which shows that H contains the identity element.

(ii) Now if $x \in H$, then $e, x \in H \implies ex^{-1} = x^{-1} \in H$, which proves that H is closed under inverses.

(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 $xy \in H$, proving closure of H under the group operation.

□

Example 2.4. Let G be the group of non-zero complex numbers under multiplication, and let $\omega = e^{\frac{2\pi i}{3}}$, the primitive complex cube root of unity. Then $H = \{1, \omega, \omega^2\}$ is a subgroup of G. Clearly, H is non-empty. Now, the elements of H are all the integer powers of ω – i.e., 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 2.3, $H \leq G$.

Can two or more subgroups be combined together to construct other subgroups? The following results show that they can, in certain ways.

Theorem 2.5. *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 $e \in K$, $e \in H \cap K \neq \emptyset$. 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 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 $h' \in H$. Observe that h' is not necessarily equal to h, and k' is not necessarily equal to k.

Theorem 2.6. *Let H and K be any two subgroups of a group G. Then $HK \leq G$ if and only if $HK = KH$.*

Proof. Suppose that $HK \leq G$. Let $x \in HK$. Then $x^{-1} \in HK \implies x^{-1} = hk$, $\exists h \in H$, $k \in K$. 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 $(kh)^{-1} = h^{-1}k^{-1} \in HK \implies ((kh)^{-1})^{-1} = kh \in HK$. Therefore, $HK = KH$.
For the converse, suppose that $HK = KH$. We must show that $HK \leq G$. Since H and K are non-empty, so is HK. Now let $x, y \in HK$. We shall show that $xy^{-1} \in HK$. Let $x = h_1k_1$, $y = h_2k_2$, where $h_1, h_2 \in H$, $k_1, k_2 \in K$. 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 2.1. Let G be a group.

1. The *centre* of G, 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 $n \in \mathbb{N}$, define $H = \{ x^n \mid x \in G \}$. Show that $H \leq G$.
5. Let G be Abelian. For $n \in \mathbb{N}$, define $H = \{ x \in G \mid x^n = e \}$. Show that $H \leq G$.

2.1 Cyclic subgroups and cyclic groups

Definition 2.7. 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: $\langle x \rangle = \langle x^{-1} \rangle$ (why?).

Definition 2.8. 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 2.9. 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 2.10. $\mathbb{Z} = \langle 1 \rangle$, since every integer n can be written as $n \times 1$. (Recall that we write $\mathbb{Z}$ in additive notation, and therefore write nx, and not 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 2.11. Let V_4 denote the group formed by $\{1, 3, 5, 7\}$ under multiplication modulo 8 (i.e., for $a, b \in V_4$, $a \cdot b = c$ where c is the remainder obtained when the integer $a \times b$ is divided by 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 (alternatively, notice that the table is symmetric, which shows that the operation is commutative). 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**.

Every group, even if it is non-cyclic, has cyclic subgroups – every element of a group generates one. But can a cyclic group have non-cyclic subgroups?

Theorem 2.12. *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,

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

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). 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 $n > r \ge 0$, therefore, $r = 0$. Thus we have $g^m = (g^n)^q$, as required. □

Definition 2.13. 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 $\mathrm{o}(x)$.

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.

Theorem 2.14. *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). □

2.2 Lagrange's theorem

Definition 2.15. 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 $h \in H$, $hH = Hh = H$. (It is obvious, due to closure of H under the operation, that hH is a subset of H – why is it *equal* to H?).

We shall show that left cosets (LCs) of a subgroup partition the whole group into equally sized parts (G: "You're tearing me apart, LCs!").

Theorem 2.16 (Lagrange)**.** *If G is a finite group and H a subgroup of G, then 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 2.17.

$$G = \bigcup_{i=1}^{k} x_iH$$

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 2.18. *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, $xH = yH$. □

Finally, we show that all left cosets of H have the same number of elements. To test whether this is true, we simply need to use the cancellation law (Coset: "I got the results of the test back! I *definitely* have left cancellation").

Lemma 2.19. *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. □

Now we can prove Lagrange's theorem.

Proof of Lagrange's theorem. From Lemma 2.17,

$$
\begin{aligned}
G = \bigcup_{i=1}^{k} x_i H \implies \\
o(G) &= \left| \bigcup_{i=1}^{k} x_i H \right| \\
&= \sum_{i=1}^{k} |x_i H| \quad \text{[Lemma 2.18]} \\
&= \sum_{i=1}^{k} |H| \quad \text{[Lemma 2.19]} \\
&= k \times o(H).
\end{aligned}
$$

Thus, $o(H) \mid o(G)$. □

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

Proof. Exercise. □

Corollary 2.21. *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 2.20, $o(g) \mid p$, which implies that $o(g) = 1$ or p. But $g \neq e \implies o(g) \neq 1$. Thus, $o(\langle g \rangle) = o(g) = p \implies G = \langle g \rangle$. □

3 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 that if $H \leq G$, then $xHx^{-1} \leq G$. (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 (which, ironically, is called a *normal* subgroup).

Definition 3.1. 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 3.2. 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 3.1.

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 3.3. *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 3.4. *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 $N \trianglelefteq G$. □

Appendices

A Cayley tables

A *Cayley table* or *multiplication table* of a group is a method of specifying a group completely by displaying the result of applying the group operation to every pair of elements – naturally, this is only feasible when the group is finite (indeed, relatively small).
The Cayley table of a finite group $(G, *)$ has all the elements of G (taken in some order) listed along both rows and columns (in the same order). The entry in any cell of the table is the product of the element in the header of the row containing that cell with the element in the header of the column containing that cell. That is,

	$\cdots$	y	$\cdots$
$\vdots$		$\vdots$	
x	$\cdots$	$x * y$	$\cdots$
$\vdots$		$\vdots$	

Some properties of the group are readily visible in its Cayley table.

1. The identity element is the element whose row (or column) is a copy of the header row (or column).

2. In the row of any element x, the header of the column in which the identity element occurs is the inverse of x (and similarly for columns).

3. A group is Abelian if and only if its Cayley table is symmetric (about the main diagonal).

4. No element is repeated in any single row or column of the table – this corresponds to the laws of left and right cancellation respectively.

5. Each row and each column contains all the elements of the group – this is because given any two elements x and y, $y = x(x^{-1}y) = (yx^{-1})x$.

B Subgroup lattices

The notation $\leq$ used for the subgroup relation is intentional – it is a partial order relation on the set of all subgroups of a group (verify). The set of all subgroups of a group G forms a poset $SL(G)$.
If H and K are any two subgroups of G, then so is $H \cap K$. This is the largest subgroup of G contained in both H and K, in the sense that if $M \leq H$ and $M \leq K$, then $M \leq H \cap K$. Thus, $H \cap K$ is the greatest lower bound of H and K in the poset $SL(G)$.
However, $H \cup K$ is not a subgroup unless $H \subseteq K$ or $K \subseteq H$. Nevertheless, H and K do have a greatest upper bound in $SL(G)$. This is $\langle H, K \rangle$, the smallest subgroup of G containing both H and K – i.e., $\langle H, K \rangle$ is the intersection of all subgroups of G that contain both H and K. This is clearly a subgroup since it is defined as the intersection of some subgroups, and it is contained in any other subgroup containing both H and K. Thus, $SL(G)$ forms a lattice with $H \vee K = \langle H, K \rangle$ and $H \wedge K = H \cap K$. This lattice is called the *subgroup lattice* of G.
Recall that $HK \leq G$ if and only if $HK = KH$. In this case, $\langle H, K \rangle = HK$. In particular, if H and K are normal subgroups of G, then $HK = KH$, and therefore $HK \leq G$. Also, $xHK = HxK = HKx$ for any $x \in G$, so that $HK \trianglelefteq G$. Similarly, $H \cap K \trianglelefteq G$ as well (verify). These observations show that the set of all normal subgroups of G also forms a lattice, called the *normal subgroup lattice* of G, denoted $NL(G)$.

Exercise B.1. Prove the normal subgroup lattice $NL(G)$ of a group G is a *modular lattice*: for any three normal subgroups $M, N, K \trianglelefteq G$, if $M \leq K$, then $M \vee (N \wedge K) = (M \vee N) \wedge K$. That is, $M(N \cap K) = MN \cap K$.

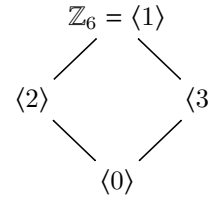
C Cyclic groups

As observed in Example 2.9, the n complex roots of unity form a cyclic group under multiplication – which is the cyclic subgroup of $\mathbb{C} - \{0\}$ generated by $\omega = \exp\left(\frac{2\pi i}{n}\right)$. Now let us construct a "different" cyclic group of order n, this time using additive notation. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Define $+_n$ on $\mathbb{Z}_n$ as addition *modulo* n. That is, for $a, b \in \mathbb{Z}_n$, let $a +_n b$ denote the remainder obtained when the (usual) sum of $a + b$ is divided by

n (and this is guaranteed to be an element of $\mathbb{Z}_n$). Equivalently, if $a + b < n$, then $a +_n b = a + b$ – otherwise, it is $a +_n b = a + b - n$.

Example C.1. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, with Cayley table and subgroup lattice given below.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4



Addition modulo n is associative and commutative, 0 is the identity element, and for each $a \in \mathbb{Z}_n$, we have $n - a \in \mathbb{Z}_n$ as well, with $a +_n (a - n) = 0$, which makes $n - a$ the inverse of a. Thus, $(\mathbb{Z}_n, +_n)$ is an Abelian group. Indeed, it is a cyclic group, as each $a \in \mathbb{Z}_n$ can be written as $a \times 1 = \underbrace{1 +_n \cdots +_n 1}_{a}$, so that $\mathbb{Z}_n = \langle 1 \rangle$.

Remark. $\mathbb{Z}_n$ is also written as $\mathbb{Z}/n\mathbb{Z}$, although then it is defined as the *quotient group* of $\mathbb{Z}$ by the normal subgroup $n\mathbb{Z}$.

While $\mathbb{Z}_n$ looks different from the group of n^{th} roots of unity, it is actually the same group (structurally). This is obvious if we look at the Cayley tables of $\mathbb{Z}_n$ and $\langle \omega_n \rangle$, where in the case of the former, the rows and columns are ordered $0, 1, \ldots, n-1$, and in that of the latter, they are ordered $1, \omega_n, \ldots, \omega_n^{n-1}$. In group theoretic language, we say that these two groups are *isomorphic*.

Definition C.2. An isomorphism from a group $(G, *)$ to a group $(H, \cdot)$ is a bijective function $f : G \to H$ such that

$$\forall x, y \in G, \quad f(x * y) = f(x) \cdot f(y).$$

That is, an isomorphism is a bijective, "structure-preserving" map – as it is in the case of any other mathematical object. For a group, its structure is simply the group operation, and therefore an isomorphism must preserve the (result of the) operation. If there is an isomorphism from G to H, we say that G and H are isomorphic, and write $G \cong H$. Exercise: Prove that the relation $\cong$ is an equivalence relation (on the collection of all groups). Thus, isomorphic groups are exactly the same groups for all purposes – the only difference is in notation. But a rose by any other name ....

All cyclic groups of the same order are isomorphic to one another. Let $G = \langle g \rangle$ be a finite cyclic group of order n. Define $f : G \to \mathbb{Z}_n$, as $f(g^k) = k$, $k = 0, 1, \ldots, n-1$.

This is a well defined function, since every element of G can be expressed uniquely in the form g^k with $0 \leq k \leq n-1$. It is clearly a bijection for the same reason. Now if $g^i, g^j \in G$, then $g^i \cdot g^j = g^{i+j}$. But since $g^n = 1$, $g^{i+j} = g^k$, where $k = i +_n j$ (e.g., if $n = 6$, then $g^3 \cdot g^5 = g^8 = g^2$). Thus, $f(g^i \cdot g^j) = i +_n j = f(g^i) + f(g^j)$, which shows that f is an isomorphism from G to $\mathbb{Z}_n$.
Now suppose $G = \langle g \rangle$ is an infinite cyclic group. Define $f : G \to \mathbb{Z}$ as $f(g^k) = k$, $k \in \mathbb{Z}$. Again, this is a well defined bijection since every element G can be expressed uniquely in the form g^k for some $k \in \mathbb{Z}$. It is also easy to see that this bijection preserves the operation, thus it is an isomorphism from G to the additive group of integers, $\mathbb{Z}$ (which, we know, is an infinite cyclic group).
Thus, all finite cyclic groups of order n are isomorphic to $\mathbb{Z}_n$, and since isomorphism is an equivalence relation, they are all isomorphic to one another. All infinite cyclic groups are isomorphic to $\mathbb{Z}$, and hence to one another as well. Therefore, we say that there is a unique cyclic group of any given (countable) order, *up to isomorphism*. However, note that there is no cyclic group of uncountably infinite order.

D The quaternion group Q_8

The *quaternion group* Q_8 of order 8 provides an accessible example of a finite non-Abelian group. It is one of the two non-Abelian groups of order 8, and the only smaller non-Abelian group is S_3 of order 6. The elements of Q_8 are denoted as given below.

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

We define an associative multiplication on Q_8 with 1 as the identity and $(-1)^2 = 1$. Further, for $x = i$, j, or k, we define $(-1)x = x(-1) = -x$. Finally, define

$$i^2 = j^2 = k^2 = -1$$
$$ij = k, \quad jk = i, \quad ki = j.$$

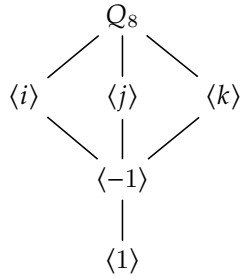
This information is sufficient to compute all other possible products. For example, since $j = ki$, we get $ji = (ki)i = ki^2 = k(-1) = -k$. Similarly, $kj = -i$ and $ik = -j$.

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

The non-trivial cyclic subgroups of Q_8 are

- $\langle -1 \rangle = \{1, -1\}$
- $\langle i \rangle = \{1, i, -1, -i\} = \langle -i \rangle$
- $\langle j \rangle = \{1, j, -1, -j\} = \langle -j \rangle$
- $\langle k \rangle = \{1, k, -1, -k\} = \langle -k \rangle$

Any subgroup that contains both i and j must contain $k = ij$, and hence all other elements. Similarly, any subgroup containing j and k, or i and k, must also be the whole of Q_8. Thus, the cyclic subgroups listed above, together with the trivial subgroup of Q_8 itself are all the subgroups of Q_8. The subgroup lattice of Q_8 is shown below. Note that $Z(Q_8) = \{1, -1\}$.



E Symmetric groups S_n

A *permutation* of a set is a bijective function from the set to itself. Given the finite set $X = \{1, 2, \ldots, n\}$, let S_n denote the set of all permutations of X. Thus, every element $\alpha \in S_n$ is a bijective function from X to X, and given any other element $\beta \in S_n$, we can

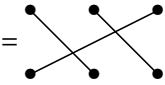
compose α and β as functions to find $\alpha \circ \beta$, defined by $(\alpha \circ \beta)(k) = \alpha(\beta(k))$, $k = 1, \ldots, n$. Since the composition of bijective functions is bijective, $\alpha \circ \beta$ is also a permutation of X, so that $\circ$ is a binary operation on S_n. Indeed, it is an associative operation (verify). The identity function, defined by $\mathrm{id}(k) = k$ is the identity element of this composition. Bijective functions are exactly the invertible functions, thus any $\alpha \in S_n$ has an inverse α^{-1}, which is also a bijective function on X, and therefore is an element of S_n. These observations show that $(S_n, \circ)$ is a group. Hereafter, we will denote $\alpha \circ \beta$ by $\alpha\beta$.

We can conveniently represent permutations in an array format (called the *two-line notation*) as given below.

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}$$

The top row consists of the elements of X in the order $1, \ldots, n$, and the bottom row contains the same elements in the order obtained after applying the permutation. That is, the element of the second row directly below the element k of the first row is $\alpha(k)$. For example, the permutation α of $\{1, 2, 3\}$ defined by $\alpha(1) = 2$, $\alpha(2) = 3$, and $\alpha(3) = 1$, is given by $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

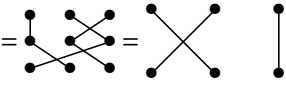
We may also graphically represent permutations by using *wiring diagrams*. The wiring diagram for the permutation α is shown below.

$\alpha =$ 

The vertices in both rows are the elements $1, 2, \ldots, n$. Each vertex k of the top row is joined to the vertex $\alpha(k)$ in the bottom row.

To find the permutation resulting from the composition of two permutations α and β, we need to compute $\alpha(\beta(k))$ for each $k \in X$. Note that we apply β first and then α to the result of that. Thus, if α is as before and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, then $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(\beta(1)) & \alpha(\beta(2)) & \alpha(\beta(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(1) & \alpha(3) & \alpha(2) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

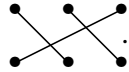
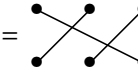
We can perform the same computation by "pasting" wiring diagrams – β on *top* of α (since β is applied before α) – and then "contracting" the wires.

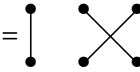
$\alpha\beta =$ 

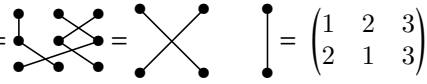
We know what all the elements of S_n are – they are all possible permutations of $1, 2, \ldots, n$. But we have not yet examined how they interact. Let us look at two small examples.

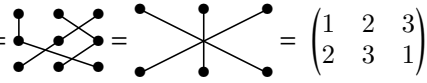
Example E.1. There are only two permutations of $\{1,2\}$, so $S_2 = \{\mathrm{id}, \alpha\}$, where $\alpha = \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$. S_2 is Abelian, and in fact cyclic: $S_2 = \langle\alpha\rangle$, since α is the only non-identity element, and therefore must be self-inverse – i.e., α is an element of order 2. Another way to see this is that $o(S_2) = 2$, which is prime, and we know that any group of prime order is cyclic.

Example E.2. S_3 provides a more interesting example of a symmetric group. Since there are $3! = 6$ permutations of $\{1,2,3\}$, $o(S_3) = 6$.

Let $\alpha = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} =$  . Then $\alpha^2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} =$  , and $\alpha^3 = \mathrm{id}$ ($\implies \alpha^{-1} = \alpha^2$). Thus, $\langle\alpha\rangle$ is an order-3 subgroup of S_3. This tells us that the remaining 3 elements of S_3 cannot be written in terms of α alone.

Let $\beta = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} =$  be the permutation that interchanges 2 and 3 (and fixes 1). Then $\beta^2 = \mathrm{id}$ ($\implies \beta^{-1} = \beta$). Again, this means that the other permutations cannot be written in terms of β alone. However, now we may compose β with α and α^2 and attempt to obtain the other elements.

$\alpha\beta =$  $= \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$

$\alpha^2\beta =$  $= \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$

These are two permutations, and now that we have a total of six, we have found all elements of S_3. Thus,

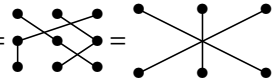
$$S_3 = \{\mathrm{id}, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

with α and β as defined above.

Now, we can compute the Cayley table of S_3. Since we have expressed all elements in terms of α and β in the form $\alpha^i\beta^j$ ($i = 0,1,2$, $j = 0,1$), we already have part of the table.

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β			id		
$\alpha\beta$	$\alpha\beta$			α		
$\alpha^2\beta$	$\alpha^2\beta$			α^2		

Like β, both $\alpha\beta$ and $\alpha^2\beta$ are *transpositions* – permutations that interchange two elements and fix all other elements. Since every transposition must be self-inverse, we have $(\alpha\beta)^2 = (\alpha^2\beta)^2 = \mathrm{id}$. That leaves ten more products to compute. But observe that if we determine how to write the product $\beta\alpha$ in the form $\alpha^i\beta^j$, we can easily compute all the other products as well.

$\beta\alpha =$  $= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha^2\beta$

Thus, $\beta\alpha = \alpha^2\beta$. Therefore, S_3 is a non-Abelian group. (As we shall see later, it is the smallest non-Abelian group). Now to compute another product, say $\beta(\alpha\beta)$, we merely need to use this repeatedly: $\beta(\alpha\beta) = (\beta\alpha)\beta = (\alpha^2\beta)\beta = \alpha^2\beta^2 = \alpha^2$. Proceeding in this way, we can complete the Cayley table of S_3.

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id

If $m > n$, then there is some sense in which S_n is a subgroup of S_m. Any permutation of $X = \{1, 2, \ldots, n\}$ can be naturally extended to a permutation of $Y = \{1, 2, \ldots, m\}$. For, given a permutation α of X, define a permutation α' of Y that permutes the elements $1, 2, \ldots, n \in Y$ according to α, and fixes the remaining elements $n+1, \ldots, m$. That is,

$$\alpha'(k) = \begin{cases} \alpha(k), & k = 1, 2, \ldots, n \\ k, & k = n+1, \ldots, m. \end{cases}$$

Thus, $\alpha' \in S_m$. Moreover, let $\alpha, \beta \in S_n$, and let $\alpha', \beta' \in S_m$ be their extensions to Y constructed as given above. If $\gamma = \alpha\beta$, then the extension of γ to Y is $\gamma' = \alpha'\beta'$. This shows that the set of permutations of Y obtained by extending the permutations of X form a subgroup of S_m isomorphic to S_n. In particular, every S_n with $n > 3$ contains a subgroup isomorphic to S_3. Since S_3 is non-Abelian, so is every S_n, $n \geq 3$.

Remark. Formally, if $S'_n = \{\, \alpha' \mid \alpha \in S_n \,\}$ (where for each α, α' denotes its extension to Y as defined above), then $S'_n \leq S_m$ and the map $f : S_n \to S'_n$ given by $f(\alpha) = \alpha'$ is an isomorphism. (An isomorphism from a group G to a subgroup $K \leq H$ of some group H is called an *embedding* of G into H. The above construction is an example of embedding – of S_n into S_m for any $m > n$).

F Classification of groups of order at most 5

Now we determine all groups with at most five elements, up to isomorphism, and note that they are all Abelian. Thus, S_3 is the smallest non-Abelian group.
Consider a group G. If $o(G) = 1$, then it is the trivial group $\{e\}$. If $o(G) = 2, 3, 5$, then it is cyclic, for any group of prime order is cyclic (and hence Abelian). That leaves groups of order 4. Let $o(G) = 4$. If G has an element of order 4, then it is cyclic (and hence Abelian). Suppose no element of G has order 4. We know that the order of an element divides the order of a group. The only divisors of 4 are 1, 2, and 4, and since G has no element of order 4, all non-identity elements of G must have order 2 – i.e., they must all be self-inverse. Therefore, G is Abelian. Let $G = \{e, a, b, c\}$. Then $a^2 = b^2 = c^2 = e$. Now, ab cannot be equal to e since $a^{-1} = a \neq b$. Also, $ab \neq a$, as that would imply $b = e$. Similarly, $ab \neq b$. Thus, $ab = c = ba$ (since G is Abelian). In a similar manner, we see that $bc = a = cb$ and $ac = b = ca$. Thus, G is the group with the Cayley table given below.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Exercise: Prove that this group is isomorphic to the group defined in Example 2.11.

G Additional exercises

1. Find two elements x and y of S_3 such that $(xy)^2 \neq x^2y^2$.
2. Prove that a group G in which $\forall x, y \in G$, $(xy)^k = x^k y^k$ for three consecutive integers k is Abelian.
3. We know that if $H, K \leq G$, then $H \cup K$ is not a subgroup unless one of H and K is contained in the other. Find an example of a group G with three subgroups H, K, N, none of which is contained in the other two, such that $H \cup K \cup N$ is a subgroup.
4. Show that any finite non-empty subset H of a group G is a subgroup if and only if it is closed under the group operation – i.e., $\forall x, y \in H$, $xy \in H$. Hint: Show that $\forall x \in H$, $xH = H$, and use this together with the finiteness of H to conclude that H contains e and x^{-1}.
5. Let $H \leq G$, and $x, y \in G$. Show that $xH = yH \iff y^{-1}x \in H \iff x^{-1}y \in H$. What is the analogous condition for $Hx = Hy$?

6. Show that $\forall x \in G$, $x^{\mathrm{o}(G)} = e$.

7. **Bézout's identity**: Using the fact that every subgroup of a cyclic group is cyclic, prove that for any two integers $a, b \in \mathbb{Z}$, $\gcd(a, b) = ma + nb$ for some integers $m, n \in \mathbb{Z}$. Hint: Show that $\{ ma + nb \mid m, n \in \mathbb{Z} \}$ is a subgroup of $\mathbb{Z}$. It must be cyclic. What is its generator?

8. Prove that any infinite group has infinitely many distinct subgroups. Hint: Observe that $\mathbb{Z}$ has infinitely many subgroups, and recall that any infinite cyclic group is isomorphic to $\mathbb{Z}$. If a group has any element of infinite order, then the cyclic subgroup generated by the element is infinite. What if the group has no element of infinite order?

9. Let A be an Abelian group, and $a, b \in A$ with $\mathrm{o}(a) = m$, $\mathrm{o}(b) = n$. Show that $\mathrm{o}(ab) \leq \mathrm{lcm}(m, n)$. Give an example where $\mathrm{o}(ab) = \mathrm{lcm}(m, n)$, and another example where $\mathrm{o}(ab) < \mathrm{lcm}(m, n)$.

10. Let A be an infinite Abelian group, and let T be the set of all elements of A having finite order. Show that $T \leq A$.

11. If G is Abelian, then all subgroups of G are normal. Is the converse true?

12. Show that every subgroup of Q_8 is normal.

13. Find all subgroups of S_3. Which of them are normal? S_3 has six subgroups of which only three are normal.