MATH222 – ALGEBRAIC METHODS I

This subject introduces the study of fundamental algebraic structures and the methods of abstract algebra which pervade much of modern mathematics. One of the important aims of the subject is to develop skills in proving theorems, finding and analyzing examples and counter examples, and in making, proving or disproving conjectures. The subject will concentrate on one particular algebraic structure, that of a group.

Group structure is present in a great many of the situations with which mathematics deals: the integers, real and complex numbers, matrices, sets of functions, and the symmetries of geometric figures to mention but a few. By studying groups abstractly, from an axiomatic point of view, basic structure and results common to all such applications are revealed. Further by identifying ideas which are common to many areas it allows us to transfer our intuition about one of the applications to all of the others. This abstract approach helps unify mathematics and has proved an effective and efficient way forward. A way which has occupied much of twentieth century mathematics.

The text for the subject, henceforth identified as **[F]**, is:

> John B. Fraleigh, *A first course in Abstract Algebra*, 5th edition, Addison-Wesley.

The notes that follow provide a **summary** of the material presented in lectures. In some cases discussions, proofs and other explanations given in lectures have been suppressed. These notes are not intended as a substitute for lectures, but rather as a guide and supplement to them.

0. PRELIMINARIES, SETS and EQUIVALENCE RELATIONS

Definition 0.1: A *set* is a 'well defined' collection of objects; that is, if S is a set and a is some object then either a is definitely in S or a is definitely not in S.

Notation, and basic operations.

$a \in S$ $\quad$ a is in S, a is an element of S, or a is a member of S.

$a \notin S$ $\quad$ a is not an element of S.

$\sharp S$, or $|S|$ $\quad$ the number of elements in S, or the cardinality of S.

$\emptyset$ $\quad$ the empty, or null, set. The set with no elements. Sometimes denoted by $\{\}$.

$A \subseteq B$ $\quad$ A is a subset of B, or B is a superset of A (sometimes denoted $B \supseteq A$); that is $a \in A \implies a \in B$.

$A \ = \ B$ $\quad$ A equals B; that is, $A \subseteq B$ and $B \subseteq A$.

$A \subset B$ $\quad$ A is a proper subset of B; that is, $A \subseteq B$ and $A \neq B$.

2^S, or $\mathcal{P}(S)$ the power set of S; that is, the set of all subsets of S. It has $2^{\sharp S}$ elements.

$A\backslash B$ A difference B; $x \in A\backslash B$ if and only if $x \in A$ and $x \notin B$.
Sometimes denoted by $A - B$, but we will reserve this to mean something different.

$\{x :\ p(x)\}$ the set consisting of elements x for which the predicate $p(x)$ is TRUE.

$A \cup B$ the union of A and B; $A \cup B := \{x :\ x \in A \text{ or } x \in B\}$.
Note, here and elsewhere 'or' is used inclusively to mean 'and or'.

$A \cap B$ the intersection of A and B; $A \cap B := \{x :\ x \in A \text{ and } x \in B\}$.

Two sets, A and B, are disjoint if $A \cap B = \emptyset$.

$\mathbf{N}$ the natural numbers $\{1, 2, 3, \cdots\}$.

$\mathbf{Z}$ the integers $\{\cdots, -3, -2, -1, 0, 1, 2, 3 \cdots\}$.

$\mathbf{Q}$ the rational numbers.

$\mathbf{R}$ the real numbers.

$\mathbf{C}$ the complex numbers.

$|\mathbf{Z}|$ the positive integers, $\{x \in \mathbf{Z} : x \geq 0\} \ = \ \{0, 1, 2, 3, \cdots\}$.
$|\mathbf{Q}|$ and $|\mathbf{R}|$ are defined similarly.

$\mathbf{R}^+$ the strictly positive real numbers, $\{x \in \mathbf{R} :\ x > 0\}$.
$\mathbf{Q}^+$ is defined similarly. Note, $\mathbf{Z}^+ = \mathbf{N}$

$\mathbf{R}^*$ the non-zero real numbers, $\mathbf{R}\backslash\{0\}$.

The next one may be new to you.

$A \times B$ the *Cartesian product* of two sets A and B, consisting of all ordered pairs whose first element is from A and whose second element is from B; that is,
$A \times B := \{(a, b) :\ a \in A \text{ and } b \in B\}$.

For finite sets A and B their Cartesian product can be conveniently presented in a table.
For example, if $A = \{a, b, c\}$ and $B = \{1, 2, 3, 4\}$ then

$$\begin{aligned} A \times B \ = \ \{&(a,1), (a,2), (a,3), (a,4), \\ &(b,1), (b,2), (b,3), (b,4), \\ &(c,1), (c,2), (c,3), (c,4)\}. \end{aligned}$$

Note, $A \times B$ has $\sharp A \times \sharp B$ elements.

We extend this inductively to the Cartesian product of more than two sets by defining $A \times B \times C$ to be

$$A \times (B \times C) \ = \ \{(a, (b, c)) : a \in A, b \in B, c \in C\},$$

which may be identified with the set of all ordered triplets $\{(a, b, c) : a \in A, b \in B, c \in C\}$. We frequently denote the Cartesian product of a set S with itself n-times, $S \times S \times S \times \cdots \times S$, by S^n. It consists of the set of all ordered n-tuples of elements of S

Partitions and equivalence relations.

Definition 0.2: A *partition* of a set S is a decomposition of S into disjoint nonempty subsets (cells) such that each element of S is in precisely one of the subsets. So, S is a union of disjoint cells.

For example, the set of fractions $\{m/n : m, n \in \mathbf{Z} \text{ with } n \neq 0\}$ decomposes into sets of the form

$$\left[\frac{2}{3}\right] := \left\{\frac{2}{3}, \frac{-2}{-3}, \frac{4}{6}, \frac{-4}{-6}, \cdots\right\} = \left\{\frac{n}{n} : 3m = 2n,\ n \neq 0\right\},$$

each of which may be identified with a distinct rational number.

Let $\sim$ be a 'relation' on S. That is, given any pair of elements a, $b \in S$ either a is related to b, $a \sim b$, or a is not related to b ($a \not\sim b$). Formally the relation $\sim$ on S may be identified with the subset $\{(a, b) : a \sim b\}$ of the Cartesian product $S \times S$.

Examples of relations are: when $\sim$ means "is a sibling of" (S a set of people), and $m/n \ \sim\ h/k$ if $mk = nh$ (S the set of fractions).

Definition 0.3: We say a relation $\sim$ on S is an *equivalence relation* if it is

Reflexive: $a \sim a$, for all $a \in S$,
Symmetric: $a \sim b$ implies that $b \sim a$, and
Transitive: if $a \sim b$ and $b \sim c$ then it follows that $a \sim c$.

Exercise: Give as many examples of relations as you can, including the two suggested above, and investigate each of them to determine whether or not it is an equivalence relation.

Definition 0.4: Let $\sim$ be an equivalence relation on the set S. For each element $a \in S$ the *equivalence class of* a, denoted by $[a]$, consists of all the elements of S which are related to a by $\sim$. That is,

$$[a] := \{x \in S : x \sim a\}.$$

Example: On the set of fractions the relation $m/n \ \sim\ h/k$ if $mk = nh$ is an equivalence relation with respect to which the equivalence class of 2/3 is the set [2/3] identified above (verify this).

This example suggests a close connection between equivalence relations and partitions. Indeed we have the following general result.

Theorem 0.5: *If $\sim$ is an equivalence relation on the set S then the equivalence classes of $\sim$ define a partition of S.*

Remark: The converse of this is also true. That is, if we have a partition of S then the relation defined on S by $a \sim b$ if a and b are in the same cell of the partition is an equivalence relation whose equivalence classes are the cells of the given partition. The proof of this is left as an **exercise**.

Proof, of theorem 0.5: For any $x \in S$ we have $x \sim x$, so $x \in [x]$. Thus the equivalence classes are nonempty and every element of S is in at least one of them. It remains to show that each $x \in S$ is in only one of them. Suppose that some x were in more than one of them. That is, $x \in [a]$ and $x \in [b]$, we will show that $[a] = [b]$ thereby establishing the result. (Note, this will also show that two equivalence classes are either identical or else disjoint.)

Now, $x \in [a]$ means $x \sim a$ and so by (S) $a \sim x$. Also $x \in [b]$ means $x \sim b$. Combining these using (T) we get $a \sim b$.

Let $z \in [a]$, this means $z \sim a$ and so, since $a \sim b$, we have by (T) that $z \sim b$. Thus $z \in [b]$, and since z was any element of $[a]$ we conclude that $[a] \subseteq [b]$. By a symmetric argument with the roles of a and b interchanged we also have $[b] \subseteq [a]$, and so $[a] = [b]$ as required.

An example: the integers modulo $m \in \mathbf{Z}^+$.

Given $m \in \mathbf{Z}^+$ define a relation on $\mathbf{Z}$ by $a \sim b$ if $a - b$ is divisible by m. That is, if $a - b = km$, or equivalently $a = b + km$, for some $k \in \mathbf{Z}$. The relation $\sim$ is an equivalence relation (verify this). In place of $a \sim b$ we will write

$$a \equiv b \pmod{m}$$

and say a is congruent to b modulo m.

The equivalence class of $a \in \mathbf{Z}$ has the form

$$[a] = \{\cdots, a-2m, a-m, a, a+m, a+2m, a+3m, \cdots\} = \{b : b = a + km, \text{ for } k \in \mathbf{Z}\}.$$

There are precisely m distinct equivalence classes: $[0], [1], [2], \cdots, [m-1]$, which form a partition of $\mathbf{Z}$.

For example: Taking $m = 4$, we have $-17 \equiv 3 \pmod 4$ and

$$\begin{aligned}
[0] &= \{\cdots, -8, -4, 0, 4, 8, \cdots\} \\
[1] &= \{\cdots, -7, -3, 1, 5, 9, \cdots\} \\
[2] &= \{\cdots, -6, -2, 2, 6, 10, \cdots\} \\
[3] &= \{\cdots, -5, -1, 3, 7, 11, \cdots\} \\
[4] &= \{\cdots, -4, 0, 4, 8, 12, \cdots\} \; = \; [0]
\end{aligned}$$

1. GROUPS

1.1 Binary operations

Definition 1.1.1: A binary operation $*$ on a set S is a rule which assigns to each ordered pair (a, b) of elements of S some unique element of S which we denote by $a * b$. That is, $*$ is a function from $S \times S$ into S.

The fact that $a * b$ is in S for all a and $b \in S$ is expressed by saying S is closed under the operation $*$.

We will frequently use $(S, *)$ to denote a set S together with a binary operation $*$ defined on it.

Some examples:

$(|\mathbf{Z}|, +)$, $(\mathbf{Z}, -)$, $(\mathbf{R}, \times)$, $(\mathbf{R}^*, \div)$.

$(\mathbf{R}^+, *)$ where $a * b := a^b$.

Matrix multiplication on the set $\mathcal{M}_n$ of all square n by n matricies.

$+$, $-$, $\times$, $\div$ and composition, $\circ$, on appropriate sets of functions (give examples of what these sets might be for each of the operations listed).

For any given $n \in \mathbf{N}$, the operation $\oplus_n$ defined on $\{0, 1, 2, \cdots, n-1\}$ by $a \oplus_n b := a + b \pmod{n}$. For instance, on $\{0, 1, 2, 3\}$ we have $2 \oplus_4 2 = 4 \pmod{4} = 0$, while $2 \oplus_4 3 = 5 \pmod{4} = 1$.

For a positive prime number p (see below for why p must be prime), the operation $\otimes_p$ defined on $\{1, 2, \cdots, p-1\}$ by $a \otimes_p b := ab \pmod{p}$. For example, on $\{1, 2, 3, 4\}$ we have $2 \otimes_5 3 = 6 \pmod{5} = 1$.

On a finite set a binary operation can be represented (or defined) by a table. For example, the operation $\otimes_5$ on $\{1, 2, 3, 4\}$ is given by

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Now, consider constructing a similar table for $\otimes_6$ on $S := \{1, 2, 3, 4, 5\}$ we get

$\otimes_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	**0**	2	4
3	3	**0**	3	**0**	3
4	4	2	**0**	4	2
5	5	4	3	2	1

The presence of 0 in the table shows that S is not closed under $\otimes_6$, so $\otimes_6$ is not a binary operation on S. We could extend to $\{0, 1, 2, 3, 4, 5\}$, but then $\otimes_6$ would not have properties that we will subsequently be interested in. It has zero divisors: non-zero elements which 'multiply' to give 0, and non-unique factorization: $3 = 3 \otimes_6 3 = 3 \otimes_6 5$.

Two properties a binary operation may have.

Definition 1.1.2: A binary operation $*$ on a set S is *associative* if $(a * b) * c = a * (b * c)$, for all $a, b, c \in S$.

When a binary operation is associative we can unambiguously write expressions such as $a * b * c$ and a^n.

Definition 1.1.3: A binary operation $*$ on a set S is *commutative* if $a * b = b * a$, for all $a, b \in S$.

Exercise: Decide which of the operations $+$, $-$, $\times$ and $\div$ defined on appropriate sets of numbers are associative and which are commutative.

1.2 Groups.

Definition 1.2.1: a *group* $(G, *)$ is a set G together with a binary operation $*$ on G which satisfies the following three 'group axioms'.

(G1) $*$ is associative; that is, $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$.

(G2) There exists an element e in G such that $e * x = x * e = x$, for all $x \in G$.

(G3) For each element $x \in G$ there exists an element $x' \in G$ such that $x * x' = x' * x = e$, where e is the element identified in (G2).

Notation: $*$ is referred to as the group operation, or 'group product'. When the operation $*$ is clearly understood we will often write G in place of $(G, *)$ and denote $a * b$ by juxtaposition as ab.

If the operation $*$ of a group $(G, *)$ is commutative ($a*b = b*a$, for all $a, b \in G$) then we say G is a *commutative group*, or *Abelian group*, named after the Norwegian mathematician Niels Henrik Abel (1802–1829), whose work on the algebraic resolution of equations helped initiate the group concept. To indicate that a group is Abelian it is common to use $+$ instead of the generic $*$ to denote the group operation.

Some simple examples of groups: $(\mathbf{R}, +)$, $(\mathbf{Z}, +)$, $(\mathbf{R}^+, \times)$, $(\mathbf{C}^*, \times)$, the set of all functions from a domain D into $\mathbf{R}$ with point-wise addition, the set of invertible $n \times n$-real matrices with matrix multiplication. The last example is an example of a non-Abelian group, known as the *general linear group* of degree n, denoted by $\mathrm{GL}(n, \mathbf{R})$.

Questions: What is e and what is $3'$ in $(\mathbf{R}^+, \times)$? Why is $(\mathbf{R}, \times)$ not a group? Why is $(\mathbf{R}, \div)$ not a group?

Further examples of groups are provided by:

For $n \in \mathbf{N}$,

U_n , the *unitary group of order* n, consisting of the n complex roots of unity under complex multiplication: $U_n := \{1, \omega, \omega^2, \cdots, \omega^{n-1}\}$, where $\omega = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$.

$\mathbf{Z}_n$ $\equiv (\mathbf{Z}_n, \oplus_n)$, where $\mathbf{Z}_n := \{0, 1, 2, \cdots, n-1\}$ and addition is modulo n. In $\mathbf{Z}_4$ what is e and what is $3'$?

For p a prime number,

$\mathbf{Z}_p^*$ $\equiv (\mathbf{Z}_p^*, \otimes_p)$, where $\mathbf{Z}_p^* := \{1, 2, \cdots, p-1\}$ and multiplication is modulo p. In $\mathbf{Z}_5^*$ what is e and what is $3'$? Explain why $\mathbf{Z}_p^*$ is not a group if p is not a prime.

1.3 Simple properties of groups.

Theorem 1.3.1: *Let $(G, *)$ be a group. The element e, whose existence is ensured by (G2), is unique.*

Proof: Suppose e_1 and e_2 are two such elements; that is, $x * e_1 = e_1 * x = x$ and $x * e_2 = e_2 * x = x$, for all $x \in G$. Then

$$\begin{aligned} e_1 &= e_1 * e_2, \quad \text{by (G2) with } x = e_1 \text{ and } e = e_2, \\ &= e_2, \quad \text{by (G2) with } x = e_2 \text{ and } e = e_1. \end{aligned}$$

Since there is precisely one element e in any group satisfying (G2) we can unambiguously refer to it by name. We call it the *identity element* of the group. In general we will denote it by e or 1, but in an Abelian group we will often use 0 in keeping with the use of + for the operation.

Theorem 1.3.2: *Let $(G, +)$ be a group. For each $x \in G$ the element x', whose existence is asserted by (G3), is unique.* We refer to it as the *inverse* of x and henceforth denote it by x^{-1}, or sometimes $-x$ in the case of an abelian group.

Proof: Suppose both x'_1 and x'_2 act as an x', then

$$x'_1 = x'_1 * e = x'_1 * (x * x'_2) = (x'_1 * x) * x'_2 = e * x'_2 = x'_2.$$

Corollary 1.3.3: *In any group $(G, *)$, $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Proof: To verify this it suffices to show that $y^{-1} * x^{-1}$ acts as an inverse for $x * y$. Do so.

In any group $(G, *)$ we have the following. Prove them.

Cancelation laws 1.3.4: If $a * b = a * c$ then $b = c$.
If $b * a = c * a$ then $b = c$.

Solvability of equations 1.3.5: For any given $a, b \in G$ the equations $a * x = b$ and $x * a = b$ both have unique solutions.

We also have:

Proposition 1.3.6: *Suppose that ℓ is a left identity for the group G. That is; $\ell x = x$, for all $x \in G$. Then $\ell = e$, the identity of the group.*

Proof:

$$\begin{aligned} \ell &= \ell e, \quad \text{as } e \text{ is the identity of } G, \\ &= e, \quad \text{as } \ell \text{ is a left identity.} \end{aligned}$$

Proposition 1.3.7: *Let G be a group and let $x \in G$. Suppose that x' is a left inverse for x. That is, $x'x = e$. Then $x' = x^{-1}$, the inverse of x.*

Proof: $x' = x'e = x'(xx^{-1}) = (x'x)x^{-1} = ex^{-1} = x^{-1}$.

Similarly, a right identity for a group is necessarily the identity, and a right inverse of a group element is necessarily its inverse.

Indeed, we have the following.

Challenging exercise: Let $*$ is a binary operation on a set G which satisfies (G1) and the following seemingly weaker axioms than (G2) and (G3):

(LG2) $(G, *)$ has a left identity. That is, there exists an element $\ell \in G$ such that $\ell * x = x$, for all $x \in G$, and

(LG3) each element of G has a left inverse. That is, for each $x \in G$ there exists an element $x' \in G$ such that $x' * x = \ell$, where ℓ is the left identity for $(G, *)$ identified in (LG2).

Show that $(G, *)$ is in fact a group.

1.4 Finite groups and group tables.

Definition 1.4.1: A group G with only a finite number of elements is termed a *finite group* and the *order of* G, denoted by $|G|$, is the number of elements in it.

For example, $\mathbf{Z}_n$ is a finite group of order n.

For relatively small orders, such a group can be conveniently presented via a *group table* (the table of its binary operation). After looking at some examples we will discuss identifying features of group tables

1.4.1 Groups of order 1: There is essentially only one such group, $G = \{e\}$, where e is the identity element $e^2 = e = e^{-1}$. Its group table is:

$*$	e
e	e

1.4.2 Groups of order 2: Suppose $(G = \{e, a\}, *)$ is a group of order 2, where e is the identity element which it must contain by (G2). Constructing its group table we have

$*$	e	a
e	e	a
a	a	?

Since G is closed under $*$ there are only two possible choices for ?, namely e,or a. If we take ? $= a$, then a has no inverse (there is no element a' such that $a' * a = e$). Thus, the only possibility is ? $= e$ and the only possible group table is

$*$	e	a
e	e	a
a	a	e

Clearly (G2) and (G3) are satisfied ($a^{-1} = a$), so it only remains to verify (G1): Using the table we have:

$$\begin{aligned}
&(e * e) * e = e * e = e \text{ and } e * (e * e) = e * e = e \text{ so } (e * e) * e = e * (e * e)\\
&(e * e) * a = e * a = a \text{ and } e * (e * a) = e * a = a \text{ so } (e * e) * a = e * (e * a)\\
&(e * a) * e = a * e = a \text{ and } e * (a * e) = e * a = a \text{ so } (e * a) * e = e * (a * e)\\
&(e * a) * a = a * a = e \text{ and } e * (a * a) = e * e = e \text{ so } (e * a) * a = e * (a * a)\\
&(a * e) * e = a * e = a \text{ and } a * (e * e) = a * e = a \text{ so } (a * e) * e = a * (e * e)\\
&(a * e) * a = a * a = e \text{ and } a * (e * a) = a * a = e \text{ so } (a * e) * a = a * (e * a)\\
&(a * a) * e = e * e = e \text{ and } a * (a * e) = a * a = e \text{ so } (a * a) * e = a * (a * e)\\
&(a * a) * a = e * a = a \text{ and } a * (a * a) = a * e = a \text{ so } (a * a) * a = a * (a * a)
\end{aligned}$$

Thus, (G1) is satisfied and there is one group, and essentially only one group, of order 2.

As this example illustrates, checking asssociativity using a case-by-case analysis can be very tedious. Allowing for the special role of e there are in general $(|G|-1)(|G|-2)(|G|-3) \sim |G|^3$ cases to examine. An alternative approach is to try and recognize the table as corresponding to that of some operation which we already know to be associative. For example, appart from the names of the elements the above table is the same as that for U_2:

$\times$	1	-1
1	1	-1
-1	-1	1

Here $G = \{1, -1\} \subset \mathbf{Z}$ and the operation is ordinary multiplication of real numbers, which we already know to be associative.

In the same way we can also recognize it as $\mathbf{Z_2}$ and $\mathbf{Z}_3^*$.

$\oplus_2$	0	1
0	0	1
1	1	0

and

$\otimes_3$	1	2
1	1	2
2	2	1

Groups which are essentially the same in this way are said to be *isomorphic*. We will shortly make this idea more precise.

1.4.3 Groups of order 3: Suppose $(G = \{e, a, b\}, *)$ is a group of order 3. Its multiplication table has the form:

$*$	e	a	b
e	e	a	b
a	a	x_1	x_2
b	b	x_3	x_4

where $\{x_1, x_2, x_3, x_4\} = \{e, a, b\}$.

Note that *no row or column of a group table can contain the same element more than once* (otherwise, either the left or right casncellation law would be violated: if the same element occured, for example, in both the y- and z-columns of the x-row of the table then we would have $x * y = x * z$ and so $y = z$, contradicting the fact that the columns of the table are labeled by distinct group elements).

Consequently, *each group element must appear precisely once in each row and column of the table.* (In any given row or column there are $|G|$ elements to be distributed into $|G|$ places, and no element is to be used more than once, so each element must be used. Alternatively, observe that $y = x * (x^{-1} * y)$, so y occurs in the x-row of the table.)

From these observations we see that $x_1 = e$ is not a valid choice, as then we would have to choose $x_2 = b$ to avoid repetitions in the a-row and b would occur twice in the b-coulmn of the table. Thus, we must have $x_1 = b$ and $x_2 = e$. Similar reasoning shows that we must choose $x_3 = e$ and $x_4 = a$, so the only possible table is:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

This table is 'isomorphic' to that for U_3, the unitary group of order 3:

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

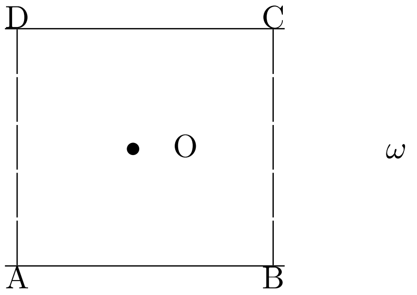
To see this, note that renaming 1 to be e, ω to be a and ω^2 to be b yields the table.

Thus, there is essentially only one group of order 3, namely U_3.

1.4.4 Groups of order 4: One such group is U_4 with group table

$\times$	1	ω	ω^2	ω^3
1	1	ω	ω^2	ω^3
ω	ω	ω^2	ω^3	1
ω^2	ω^2	ω^3	1	ω
ω^3	ω^3	1	ω	ω^2

This may be identified as the *group of rotational symmetries of a square* ABCD with ω equal to rotation about O through an angle of $\pi/2$.



It is isomorphic to $\mathbf{Z}_4 = (\{0, 1, 2, 3\}, \oplus_4)$, $\mathbf{Z}_5^* = (\{1, 2, 3, 4\}, \otimes_5)$ and to the groups with multiplication tables

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

and

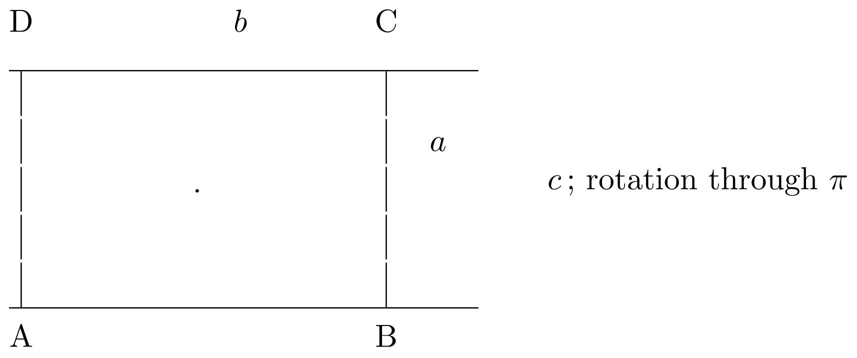
$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

To see that these last two tables are isomorphic (essentially the same) note that the second is just the first with the roles of a and b swapped and the columns and then the rows rearranged to bring the column and row labels back into the order e, a, b, c. A quick glance at these two tables serves to show that it may not always be easy to spot when two groups are isomorphic.

Using the constraints identified in 1.4.3, a systematic search for order 4 group tables distinct from (non-isomorphic to) that of U_4 (perform such a search) reveals that the only possibility is:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This is the group table of the *Klein 4-group*, which corresponds to the symmetries of a rectangle.



That this group is distinct from U_4 is easily seen by observing, for example, that in U_4 there are only two elements (e and ω^2) whose square is the identity, but in the Klein 4-group this is true of all four elements.

Thus, there are essentially only two groups of order 4: U_4 and the Klein 4-group.

We could continue our systematic study to groups of order 5, 6, $\cdots$, but we will pursue a different direction. We first ask the question:

1.4.5 When is a binary operation table a group table?

Associativity of the binary operation is not reflected by any identifiable feature of the table, thus it must be checked either using a case-by-case analysis (for groups of any size this is best left for a computer to perform), or by some other means.

Assuming that the operation is associative we have already seen that the following are two necessary conditions.

(1) There exists an element (the identity) whose table row and column match the column- and row-labels respectively.

(2) Every element must appear exactly once in each row and column of the table.

These two conditions, together with associativity, are also sufficient for the table to be that of a group. Condition (1) clearly establishes the presence of an identity element, while (1) and (2) together imply the existence of inverses.

1.5 Subgroups

Let $(G,*)$ be a group and S a subset of G. Restricting the map $*: G\times G \longrightarrow G$ to $S\times S$, we obtain a map $*: S\times S \longrightarrow G$, but S may not be closed under this operation, so $*$ may not be a binary operation on S. For example, in U_4 with $S=\{1,\omega\}$ we have $\omega=i$ and $\omega*\omega=-1\notin S$.

If it happens that S is closed under $*$: that is, $a*b\in S$ for all choices of $a,b\in S$, then $*: S\times S\longrightarrow S$ is a binary operation on S. We refer to this as the operation *induced* on S (*inherited* by S) from $(G,*)$.

Definition 1.5.1: Let $(G,*)$ be a group and $H\subseteq G$. If H is closed under the operation $*$ inherited from $(G,*)$, and with this operation $(H,*)$ is itself a group, then we say H is a *subgroup* of G, which we denote by writing $H\leq G$

For any group G we always have $G\leq G$ and $\{e\}\leq G$, where e is the identity element of G. We say $H\leq G$ is a *proper subgroup* of G, denoted $H<G$, if $H\neq G$, and we say H is a *nontrivial* subgroup of G if $H\neq\{e\}$.

Some examples of subgroups

(1) $(\{1,\omega^2\},\times)<U_4<(\mathbf{C}^*,\times)$. In fact, an inspection of the group table for U_4 shows that $(\{1,\omega^2\},\times)$ is the only proper nontrivial subgroup of U_4.

(2) $(\mathbf{Q}^+,\times)<(\mathbf{R}^+,\times)$.

(3) The even integers under addition $(\{2n:n\in\mathbf{Z}\},+)<(\mathbf{Z},+)$

(4) $(\{f:[0,1]\longrightarrow[0,1] \;:\; f \text{ is onto and strictly increasing}\},\circ)$ is a nontrivial proper subgroup of $(\{f:[0,1]\longrightarrow[0,1] \;:\; f \text{ is invertible}\},\circ)$. Here the operation $\circ$ is composition of functions.

Note: For any group G, $\leq$ (‘is a subgroup of”) is a *partial order* on the subgroups of G. That is, it is:

Reflexive; $H\leq H$, for all $H\leq G$,

Antisymmetric; if $H\leq K$ and $K\leq H$ then $H=K$, and

Transitive; if $H\leq K$ and $K\leq L$ then $H\leq L$.

(Prove these.)

This gives rise to the *lattice of subgroups* of G. For example:

(1)

$$\begin{tikzcd} U_4 \arrow[d, dash] & \\ \{1,\omega\} \arrow[d, dash] & = U_2 \\ \{1\} & \end{tikzcd}$$

(2) For the Klein 4-group, V,

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$\begin{tikzcd} & V \arrow[d, dash] & \\ \{e,a\} & \{e,b\} \arrow[d, dash] & \{e,c\} \\ & \{e\} & \end{tikzcd}$$

1.5.2 Subgroup criteria

Let $(G,*)$ be a group and $H \leq G$. Since $(H,*)$ is itself a group, for $a,b \in H$ the equation $a * x = b$ has a unique solution in H. This is also an equation in G (where it also has a unique solution). Since the solution $x \in H \subseteq G$ is also a solution in G it must be the unique solution in G. That is, the solution in H and in G must be the same.

In particular, since $(H,*)$ is a group it must have an identity element e_H which is a solution of $e_H * x = e_H$ in H and hence G, but $x = e$, the identity element of G, is also a solution in G so we must have $e_H = e$. consequently, necessarily the identity of G, e,is in any subgroup H of G.

Similarly, if a' is the inverse in H of $a \in H$, then $x = a'$ solves $a * x = e$ in H and hence in G. But, $x = a^{-1}$, the inverse of a in G is also a solution in G, so we must have $a' = a^{-1}$.

Thus, if $(G,*)$ is a group and H is a subgroup of G then

(1) H is closed under $*$,

(2) $e \in H$, where e is the identity element of G, and

(3) if $a \in H$ then $a^{-1} \in H$, where a^{-1} is the inverse of a in G. That is, H is closed under the taking of inverses.

These three *subgroup criteria* are therefore necessary conditions for H to be a subgroup of G. We now observe that they are also sufficient. Thus, they are all we need check in order to verify that a subset H of G is in fact a subgroup of G. To see this, note that (1) implies that $*$ restricted to H is a binary operation on H, which inherits its associativity from $(G,*)$, so $(H,*|_H)$ satisfies (G1). Trivialy (2) implies (G2) while (3) implies (G3) for H, and so we conclude that $(H,*|_H)$ is a subgroup of G.

Note: An even cleaner criteria for $H \subseteq G$ to be a subgroup of $(G, *)$ is given in **F** section *1.2*, exercise **40**, namely:

$H \leq G$ if and only if for all $a, b \in H$ we have that $a * b^{-1} \in H$.

(Prove this, and then be prepared to use it.)

2. CYCLIC GROUPS

Let $(G, *)$ be a group. For $a \in G$ and $n \in \mathbf{Z}$ we have

$$a^n := \underbrace{a * a * a \cdots * a}_{n \text{ factors}}$$

We will sometimes write na instead of a^n when the group is Abelian and we are using $+$ to stand for the group operation.

Similarly

$$\begin{aligned} a^{-n} := (a^{-1})^n &:= \underbrace{a^{-1} * a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ factors}} \\ &= (a^n)^{-1} \end{aligned}$$

Again, we sometimes write $-na$ in place of a^n when additive notation is being used in the case of a commutative group.

If we adopt the convention $a^0 = e$, the identity element of the group, then the normal index rule applies:

$$\text{For } n, m \in \mathbf{Z} \text{ we have} \quad a^n * a^m = a^{n+m}.$$

For $a \in G$ let

$$\langle a \rangle := \{a^n : n \in \mathbf{Z}\}.$$

That is, $\langle a \rangle = \{\cdots a^{-2}, a^{-1}, e, a, a^2, a^3, \cdots\}$.

Proposition 2.0.1: *For G a group and $a \in G$ we have that $\langle a \rangle$ is a commutative subgroup of G, the smallest subgroup of G containing a.*

The proof is immediate and so will be omitted.

We refer to a as a *generator* for $\langle a \rangle$. Any group generated in this way by a single element is called a *cyclic group.*

Examples: $U_n = \langle \omega \rangle$, where $\omega = e^{2\pi i/n}$.

$(\mathbf{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.

In $(\mathbf{Z}, +)$, for $n \in \mathbf{N}$, the set of all multiples of n,

$$n\mathbf{Z} := \langle n \rangle = \{\cdots, -2n, -n, 0, n, 2n, 3n, \cdots\},$$

is a cyclic subgroup. Note: if n divides m then $m\mathbf{Z} \leq n\mathbf{Z}$.

$(\mathbf{R}, +)$, $(\mathbf{R}^*, \times$, and the Klein 4-group are examples of non cyclic groups.

Theorem 2.0.2: *Every subgroup of a cyclic group is itself a cyclic group.*

Proof: Let G be a cyclic group with generator a. that is,

$$G = \langle a \rangle := \{\cdots, a^{-2}, a^{-1}, a^0 := e, a, a^2, a^3 \cdots\},$$

and let $H \leq G$.

If $H = \{e\} = \langle e \rangle$ then there is nothing to prove, otherwise for some n with $a^n \neq e$ we must have $a^n \in H$ and hence, since H is a subgroup, also $a^{-n} \in H$.

This shows that $m = \min\{n \in \mathbf{N} : e \neq a^n \in H\}$ exists and $m \geq 1$. Further $a^{nm} \in H$, for all $n \in \mathbf{Z}$.

Now suppose $a^k \in H$, and let $k = qm + r$, where $q \in \mathbf{Z}$ and $0 \leq r < m$ (r is the remainder of k divided by m). Then, $a^r = a^{-qm}a^{qm+r} = a^{-qm}a^k \in H$, as a^{-qm} and a^k are in H and H is a subgroup.

But, this implies $r = 0$ (definition of m), and so $k = qm$.

Thus all elements of H are of the form a^{qm}, for some $q \in \mathbf{Z}$. That is, $H = \langle a^m \rangle$ and so H is cyclic.

Application: The subgroups of $(\mathbf{Z}, +)$ are precisely the groups $(n\mathbf{Z}, +)$, for $n \in |\mathbf{Z}|$.

2.1 Infinite cyclic groups

Theorem 2.1.1: *Let G be an infinite cyclic with generator a, then*

$$G = \{\cdots, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \cdots\}$$

and all the powers of a are distinct.

Proof: The form of G follows from the definition of cyclic. Now, suppose that $a^n = a^k$, for some $n \neq k$. Without loss of generality take $k < n$. Then, $a^{n-k} = e$ with $n - k > 0$. Thus, there exists a smallest strictly positive integer m for which $a^m = e$. It follows that $e, a, a^2, a^3, \cdots, a^{m-1}$ are all distinct (why?) Further, these m elements are the only distint elements of G (which is the sought for contradiction, since G is infinite). To see that there are no other distinct elements, observe that we have:

$$\begin{aligned}
&a^m = e \\
&a^{m+1} = a \\
&a^{m+2} = a^2 \\
&\cdots \\
&a^{2m-1} = a^m a^{m-1} = a^{m-1} \\
&a^{2m} = (a^m)^2 = e \\
&a^{2m+1} = a \\
&\cdots
\end{aligned}$$

and

$$\begin{aligned}
&a^{-1} = ea^{-1} = a^m a^{-1} = a^{m-1}\\
&a^{-2} = a^{m-2}\\
&\dots
\end{aligned}$$

Corollary 2.1.2: *Any infinite cyclic group G is isomorphic to* $(\mathbf{Z}, +)$. Thus $(\mathbf{Z}, +)$ is 'essentially' the only infinite cyclic group.

Proof: If we set up a correspondence between G and $\mathbf{Z}$ by $a^n \leftrightarrow n$, then

$$\begin{aligned}
a^n * a^m &= a^{n+m}\\
&\leftrightarrow n + m.
\end{aligned}$$

Theorem 2.1.3: *Let H be the smallest subgroup of the infinite cyclic group $\langle a \rangle$ containing a^m and a^n, then $H = \langle a^d \rangle$, where $d = \gcd(m, n)$ is the greatest common divisor of m and n.*

Proof: Since H contains all elements of the form

$$a^{pm+qn} = (a^m)^P (a^n)^q, \quad \text{for } p, q \in \mathbf{Z},$$

and the set of all such elements form a subgroup (check this) we must have

$$H = \{a^{pm+qn} : p, q \in \mathbf{Z}\}.$$

As a subgroup of the cyclic group $\langle a \rangle$ we know by theorem (2.0.2) that H must be cyclic with generator a^d, say.

Now, $a^m \in H \implies a^m = (a^d)^k = a^{kd}$, for some $k \in \mathbf{Z}$. So, $m = kd$ and d divides m. Similarly, $a^n \in H$ implies d divides n.

On the other hand, $a^d \in H \implies a^d = a^{pm+qn}$, for some $p, q \in \mathbf{Z}$. So,

$$d = pm + qn. \tag{$*$}$$

Since any common divisor of m and n divides the right hand side of $(*)$ we see that any divisor of m and n divides d. Thus $d = \gcd(m, n)$.

Remark 2.1.4: From the above proof, in particular $(*)$, we see that if $d = \gcd(m, n)$ then $d = pm + qn$, for some $p, q \in \mathbf{Z}$. The ability to express the greatest common divisor of two number as such an integer linear combination of them is often very useful and should be borne in mind.

2.2 Finite cyclic groups

Let G be a finite cyclic group of order n $(< \infty)$ with generator a. That is $G = \langle a \rangle$. Then, not all the powers of a can be distinct, so there must exist distinct integers h, k with $a^h = a^k$. So, $a^{k-h} = e$ and if $m \geq 1$ is the smallest strictly positive integer with $a^m = e$ we must have

$$G = \{e, a, a^2, a^3, \cdots, a^{m-1}\},$$

so $m = n - 1$.

Under the correspondence $a \leftrightarrow \omega$, where $\omega = e^{2\pi i/n}$ we see that G is isomorphic to the unitary group U_n and hence also to $(\mathbf{Z}_n, \oplus_n)$. Thus, *there is essentially only one cyclic group of any given order.*

Theorem 2.2.1: *Let $G = \langle a \rangle$ be a cyclic group of order n and let $r \in \{1, 2, \cdots, n-1\}$, then $H := \langle a^r \rangle$ is a cyclic subgroup of order n/d, where $d = gcd(n, r)$.*

Proof: We know that H, as a subgroup of a cyclic group, must itself be cyclic, hence it only remains to establish its order. Suppose h is the order of H, then h is the smallest strictly positive integer for which $e = (a^r)^h = a^{rh}$. Since a power of a equals e if and only if the power is a multiple of n, we see that h is the smallest strictly positive integer for which n divides rh. Since n/d and r/d are integers (by the definition of d), it follows that n/d divides $(r/d)h$. Further, since n/d and r/d are relatively prime integers (again, by the definition of d), we must have that n/d divides h. That is, $h = k(n/d)$, for some $k \in \mathbf{N}$, and so the smallest possible value for h is n/d. Further n does divide $r(n/d) = (r/d)n$, and hence we conclude that $h = n/d$, as claimed.

Remark 2.2.2: Since any subgroup of the finite cyclic group $G = \langle a \rangle$ must be of the form $\langle a^r \rangle$, for some $r \in \{1, 2, \cdots, n-1\}$, the above theorem shows that the order of any subgroup of G must divide the order of G. We will shortly show that this is true, not just for cyclic groups, but for any finite group G.

Corollary 2.2.3: *If a generates a finite cyclic group of order n then the generators for G are a^r, where $gcd(r, n) = 1$.*

These results help us to determine the lattice of subgroups of any finite cyclic group.

Example 2.2.4: For $(\mathbf{Z}_{12}, \oplus_{12}) = \langle 1 \rangle$, generators are integers between 1 and 11 which are relatively prime to 12; namely, $1, 5, 7$ and 11. Other elements generate proper subgroups. Thus, the non-trivial proper (necessarily cyclic) subgroups are:

$$\langle m \rangle, \quad \text{of order } 12/\text{gcd}(m, 12),$$

where $m = 2, 3, 4, 6, 8, 9$, or 10.

These are:

$\langle 2 \rangle$, of order 6; $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$,

$\langle 3\rangle$, of order 4; $\langle 3\rangle = \{0,3,6,9\}$,

$\langle 4\rangle$, of order 3; $\langle 4\rangle = \{0,4,8\}$,

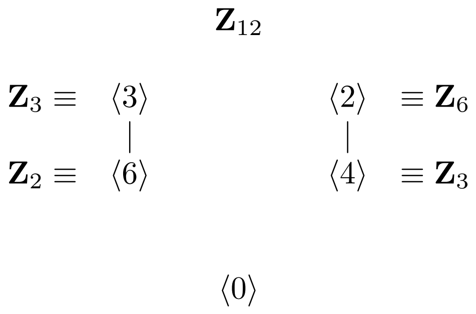
$\langle 6\rangle$, of order 2; $\langle 6\rangle = \{0,6\}$,

$\langle 8\rangle$, of order 3; $\langle 8\rangle = \{0,8,4\} \ = \ \langle 4\rangle$,

$\langle 9\rangle$, of order 4; $\langle 9\rangle = \{0,9,6,3\} \ = \ \langle 3\rangle$, and

$\langle 10\rangle$, of order 6; $\langle 10\rangle = \{0,10,8,6,4,2\} \ = \ \langle 2\rangle$.

The lattice of subgroups for $\mathbf{Z}_{12}$ is therefore:


$\mathbf{Z}_{12}$
$\mathbf{Z}_3 \equiv \ \langle 3\rangle$
$\langle 2\rangle \ \equiv \mathbf{Z}_6$
$\mathbf{Z}_2 \equiv \ \langle 6\rangle$
$\langle 4\rangle \ \equiv \mathbf{Z}_3$
$\langle 0\rangle$

2.3 Generators

Here we extend the idea of a group generated by a single element (a cyclic group) to groups generated by sets of elements.

Theorem 2.3.1: *Let G be a group and let A be a subset of G. The set of all* finite *expressions of the form*

$$a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k},$$

where $a_1, a_2, \cdots, a_k$ are not necessarily distinct elements of A, and $n_1, n_2, \cdots, n_k \in \mathbf{Z}$ are positive, or negative, powers forms a group: the subgroup of G generated by A, *which we denote by $\langle A\rangle$.*

Proof: For $a = a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ and $b = b_1^{m_1} b_2^{m_2} \cdots b_j^{m_j}$ in $\langle A\rangle$ we clearly have

$$ab^{-1} = a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} b_j^{-m_j} b_{j-1}^{-m_{j-1}} \cdots b_1^{-m_1} \ \in \ \langle A\rangle.$$

Indeed more can be said.

Theorem 2.3.2: *For G a group and $A \subseteq G$, $\langle A\rangle$ is the* smallest *subgroup of G containing A.*

Proof: Closure under the binary operation ensures that if $A \subseteq S \leq G$, then $\langle A\rangle \subseteq S$. So, any other subgroup of G containing A is larger than (contains) $\langle A\rangle$.

Recalling that any intersection of subgroups of G is itself a subgroup of G, we see that this last result implies that

$$\langle A\rangle \;=\; \bigcap\{S : A\subseteq S\leq G\}.$$

If $A\subseteq G$ is such that $\langle A\rangle = G$ we say A *generates* (or, is a *generating set* for) G, and we refer to the collection of elements of A as *generators* for G.

Note: A is always a generating set for $\langle A\rangle$. Also, our use of $\langle a\rangle$ to denote the cyclic group generated by a is a slight abuse of the notation $\langle\{a\}\rangle$, and is certainly consistent with the more general ideas developed here.

Remark: It is perhaps worth noting the close analogy between $\langle A\rangle$ and generating set with the notions of span and spanning set of vectors in linear algebra.

Example 2.3.3: For $\mathbf{Z}_6$, we have

$$\begin{aligned}\langle 1\rangle &= \mathbf{Z}_6,\\ \langle 5\rangle &= \mathbf{Z}_6 \quad\text{and}\\ \langle\{2,3\}\rangle &= \mathbf{Z}_6.\end{aligned}$$

So, 1; 5 and 2,3 are generators for $\mathbf{Z}_6$, while $\langle\{2,4\}\rangle = \langle 2\rangle = \{0,2,4\}\equiv\mathbf{Z}_2<\mathbf{Z}_6$.

Exercise 2.3.4: Verify that $\{a,b\}$, $\{a,c\}$ and $\{b,c\}$ are all generating sets for the Klein 4-group $\{e,a,b,c\}$ defined in section 1.4.3.

Note 2.3.5: In a *finite* group $a^{-1}=a^k$, for some $k\in\mathbf{N}$, so only strictly positive powers of the generators need be used to form $\langle A\rangle$.

3. PERMUTATION GROUPS

Intuitively a *permutation* of a set A is a 'rearrangement' of its elements, for example:

$$\begin{array}{cccc} a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow \\ d & a & b & c \end{array}$$

formally it is a 1-1 and onto function $\sigma : A \longrightarrow A$.

It is readily verified (do so) that the set of all permutations of a set A with composition as the binary operation forms a group, which we denote by S_A.

For example: Let $A = \{1, 2, 3, 4\}$, for the permutations

$$\sigma : \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 2 & 3 \end{array} \quad \text{which we write as} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

we have

$$\sigma\tau \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Note: 'multiplication' of permutations is from right to left; $\sigma\tau(1) = \sigma(\tau(1)) = \sigma(2) = 3$. (Caution: some authors combine permutations from left to right. They see this as more natural, but it does not conform to our usual notation for the composition of functions. It is important that you establish what convention is being used before reading any book on permutations.)

Remark: The group S_A is not concerned with what the elements of A really are. Thus if B is any set with the 'same number' of elements as A (that is, there is a 1-1 correspondence between A and B), then S_B has the same structure as S_A; they are isomorphic groups.

We will mainly be concerned with finite sets, and if A is a set with n elements then by the above remark we might as well take A to be the set $\{1, 2, \cdots, n\}$. The group of all permutations of this set is the *symmetric group on n symbols* which we will denote by S_n. It has $n!$ elements; that is, S_n has order $n!$ (why?).

For example, the permutations σ and τ given above are elements of S_4. The identity element is

$$\iota = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \text{while the inverse of } \sigma \text{ is} \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

What is τ^{-1}?

Examples:

$$\mathbf{S_1} \;=\; \{\iota\}, \quad \text{where} \quad \iota = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$\circ$	ι
ι	ι

$$\mathbf{S_2} \;=\; \left\{ \iota = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$\circ$	ι	σ
ι	ι	σ
σ	σ	ι

$\mathbf{S_3}$ has $3! = 6$ elements, namely:

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$\circ$	ι	ρ_1	ρ_2	μ_1	μ_2	μ_3
ι	ι	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ι	μ_3	μ_1	μ_2
ρ_2	ρ_2	ι	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ι	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ι	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ι

Note: $\rho_2\mu_1 = \mu_2 \neq \mu_3 = \mu_1\rho_2$, so S_3 is a non-abelian group. The notational division of its elements into ρ's and μ's is explained by the following interpretation.

S_3 is the group of symmetries of an equilateral triangle:

As the full group of symmetries of an equilateral triangle S_3 is also known as the *third dihedral group* and denoted by D_3.

Remark: The *n'th dihedral group*, D_n, is the group of symmetries of a regular n-gon. It has order $2n$ (why?) and so, except in the case $n = 3$, it is a proper subgroup of S_n. WARNING, Because it has $2n$ elements some authors choose to denote the symmetry group of a regular n-gon by D_{2n}. Thus, for these authors our D_3 would be denoted by D_6. You must establish the convention being used in any book you are working with.

3.1: The octic group, $\mathbf{D_4}$

The octic group D_4 is the full group of symmetries of a square. It is an order 8 proper subgroup of S_4 (order 24).

Besides the identity, $\iota = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, the remaining seven elements of D_4, some of whose entries have been left blank for you to fill in as an exercise, are:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \rho_2 = \rho_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & ? & ? & ? \end{pmatrix}, \quad \rho_3 = \rho_1^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ ? & ? & ? & ? \end{pmatrix},$$

representing anticlockwise rotations through $\pi/2$, π and $3\pi/2$ respectively about the centre of the square,

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ ? & ? & ? & ? \end{pmatrix},$$

representing reflections in the two lines of symmetry which pass through the midpoints of pairs of opposite sides, and

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ ? & ? & ? & ? \end{pmatrix},$$

representing reflections in the two diagonals.

The group table for D_4 is:

$\circ$	ι	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ι	ι	ρ_1	$\rho_2\rho_3$	μ_1	μ_2	$\delta\vert_1$	δ_2	
ρ_1	ρ_1	ρ_2	ρ_3	ι	?	?	?	?
ρ_2	ρ_2	ρ_3	ι	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ι	ρ_1	ρ_2	?	?	?	?
μ_1	μ_1	?	?	?	ι	ρ_2	ρ_3	?
μ_2	μ_2	?	?	?	ρ_2	ι	?	?
δ_1	δ_1	?	δ_2	?	ρ_1	?	ι	ρ_2
δ_2	δ_2	?	δ_1	?	?	?	ρ_2	ι

You should complete this table as an exercise. You may find the omitted entries by either multiplying the appropriate permutations, e.g.

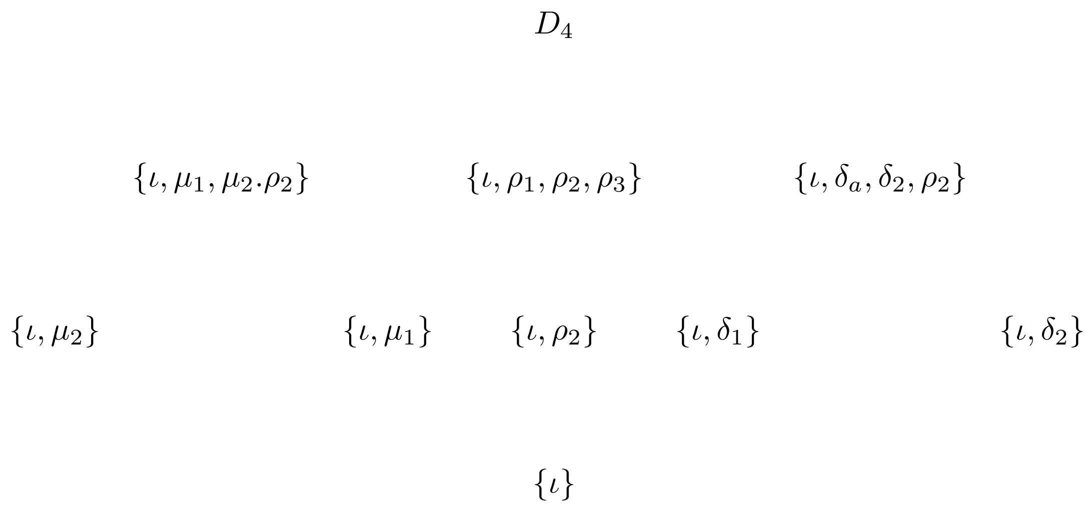
$$\delta_1\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \rho_1,$$

or by performing the operations in order on a square and noting the result, e.g.

so, $\delta_1\rho_2 = \delta_2$.

Note that D_4 is a non-commutative group, all of whose proper subgroups are commutative.

The lattice of subgroups for D_4 is :



3.2 Orbits, Cycles and Transpositions

Definition 3.2.1: Given;

a finite set A, which witout loss of generality we take to be $\{1, 2, 3, \cdots, n\}$,

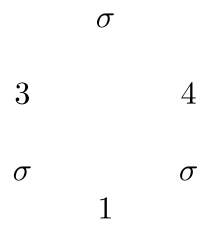
a permutation σ of A, and

an element a of A,

the *orbit of* a *under* σ is the set $\{a, \sigma(a), \sigma^2(a), \cdots, \sigma^k(a), \cdots\}$.

For example: If $A = \{1, 2, 3, 4, 5, 6\}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$ and $a = 3$

the orbit of a under σ is $\{3, 4, 1, 3, 4, 1, 3, 4, \cdots\} = \{3, 4, 1\}$.

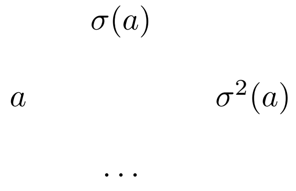


Note: the definition may suggest that orbits are infinite. However, as the example illustrates, since A is finite, only finitely many of the elements in the orbit can be distinct. If we continue listing the elements $a, \sigma(a), \sigma^2(a), \cdots, \sigma^k(a), \cdots$ while-ever they are distinct we must eventually stop, at $\sigma^m(a)$ say, and then $\sigma^{m+1}(a)$ must be one of the already listed elements. CLAIM: it can only be a. Indeed if $\sigma^{m+1}(a) \neq a$ then $\sigma^{m+1} = \sigma^k(a)$ for some $k \in \{1, 2, 3, \cdots, m\}$, then

$$\sigma(\sigma^{k-1}(a)) = \sigma^k(a) = \sigma^{m+1}(a) = \sigma(\sigma^m(a))$$

contradicting the fact that σ is a permutation and hence 1-1, as by the choice of m we have that $\sigma^{k-1}(a)$ and $\sigma^m(a)$ are distinct.

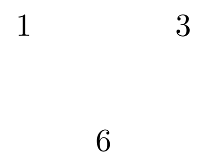
Thus orbits necessarily circle back on themselves:



The above argument also shows that if b is an element in the orbit of a under σ, then as a set the orbit of b under σ necessarily equals the orbit of a under σ. Thus the orbits of *sigma* are either disjoint or identical. [For an alternative description of the orbit of a under σ, as the equivalence class of a under the equivalence relation: $a \sim b$ if $b = \sigma^k(a)$ for some $k \in \mathbf{Z}$, see **F** pp101–102 (orbits).

Definition 3.2.2: A permutation $\sigma \in S_n$ is a *cycle* if it has at most one orbit containing more than one element. The *length of the cycle* is the number of distinct elements in its largest orbit.

Example: The cycle in S_8 containing the orbit



is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}.$$

Rather than write cycles like this we will use the abreviated *cyclic notation* $(1, 3, 6)$, think of this as $(1 \to 3 \to 6)$.

Note: $(1, 3, 6) = (6, 1, 3)$ etc.

Definition 3.2.3: Two cycles in S_n are *disjoint* if in cyclic notation they have no elements in common. NOTE: disjoint cycles commute.

Theorem 3.2.4: *Every permutation in S_n can be written as a product of disjoint cycles.*

Proof: The proof is essentially an algoritm for writing any given permutation in this way. We illustrate it on the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Choose any element a_1 of $\{1, 2, 3, \cdots, n\}$ and form its orbit: $a_1, \sigma(a_1), \sigma^2(a_1), \cdots, \sigma^{m_1}(a_1)$ equal to $1, 3, 6$ in our example with $a_1 = 1$. Use this to define a cycle $\mu_1 := (a_1, \sigma(a_1), \sigma^2(a_1), \cdots, \sigma^{m_1}(a_1))$. In our example, $\mu_1 := (1, 3, 6)$.

Now choose any element a_2 not in the orbit of a_1. Form its orbit (which is necessarily distinct from that for a_1, why?) and use this to define another (disjoint) cycle μ_2. For example, choosing $a_2 = 2$, we have $\mu_2 := (2, 8)$.

Continue this process to obtain (necessarily distinct) cycles $\mu_1, \mu_2, \mu_3, \cdots$ until the elements of $\{1, 2, 3, \cdots, n\}$ are exhausted. In our example this happens after we have formed $\mu_3 := (4, 7, 5)$.

Then, $\sigma = \mu_1\mu_2\mu_3\cdots$. For example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1, 3, 6)(2, 8)(4, 5, 7).$$

Check this by multiplying out the right hand side.

Note: In writing a permutation as a product of cycles we may ignor cycles of length 1 as these correspond to the identity permutation ι. Thus, since the orbits of σ are unique, the above decomposition of σ into cycles is unique up to the order in which the cyclic factors appear.

Definition 3.2.5: A cycle of length 2 is a *transposition*.

For example: $\mu_2; = (2, 8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 3 & 4 & 5 & 6 & 7 & 2 \end{pmatrix}$ in S_8 is a transposition.

Lemma 3.2.6: *Every permutation of* $\{1, 2, \cdots, n\}$ *can be written as a product of transpositions.*

Proof: Since every permutation can be written as a product of (disjoint) cycles it suffices to show that every cycle can be written as a product of transpositions, and a simple computation verifies that

$$(a_1, a_2, \cdots, a_k) = (a_1, a_k)(a_1, a_{k-1})(a_1, a_{k-2}) \cdots (a_1, a_3)(a_1, a_2).$$

Example:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} &= (1, 3, 6)(2, 8)(4, 5, 7) \\ &= (1, 6)(1, 3)(2, 8)(4, 5)(4, 7). \end{aligned}$$

Note: Since in general the transpositions involved in this decomposition are not disjoint (for instance the first pair, and last pair, in the example above), and so do not commute, the order in which the transposition factors appear is important. Also the decomposition into a product of transpositions is non-unique. For example; verify that,

$$\begin{aligned}\begin{pmatrix}1&2&3&4&5&6&7&8\\3&8&6&7&4&1&5&2\end{pmatrix} &= (1,6)(1,3)(2,8)(4,5)(4,7)\\ &= (2,8)(3,1)(3,6)(4,5)(4,7)\\ &= (2,8)(3,1)\underbrace{(3,7)(3,7)}_{\iota}(3,6)(4,5)(4,7) \quad \text{etc.}\end{aligned}$$

However we do have the following result concerning the number of transpositions involved.

Theorem 3.2.7: *If a permutation σ of $\{1,2,3,\cdots,n\}$ can be written as a product of k transpositions and also as a product of ℓ transpositions then $k \equiv \ell$ mod(2). That is, for a given permutation the number of transpositions involved in any decomposition of it into a product of transpositions is either always even or always odd.*

Proof: We begin by forming a special product of the integers $\{1,2,3,\cdots,n\}$.

Let

$$P_n \;:=\; \prod_{1\leq j<i\leq n} (i-j).$$

For example: $P_4 = (2-1)(3-1)(4-1)(3-2)(4-2)(4-3)$.

For any permutation β of $\{1,2,3,\cdots,n\}$ let

$$\beta P_n \;:=\; \prod_{1\leq j<i\leq n} (\beta(i)-\beta(j)).$$

In our example, $\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix} P_4 \;=\; (4-3)(2-3)(1-3)(2-4)(1-4)(1-2) \;=\; -P_4.$

The effect of β on P_n is to rearrange the factors and change the sign of some of them. So always we have $\beta P_n \;=\; \pm P_n$. Now note that if τ is a transposition, $\tau = (r,s)$ say, with $r < s$, then the only factors of P_n containing either r or s (and so affected by τ) are of the form:

Transpositions		*Effect of interchangeing* r and s
$(r-s)$		sign changed to $-$
$(t-s)$, $(t-r)$	$t > s$	sign unchanged, $(+\times+)$
$(s-t)$, $(t-r)$	$s > t > r$	sign unchanged, $(-\times-)$
$(s-t)$, $(r-t)$	$r > t$	sign unchanged, $(+\times+)$

So for any transposition τ we have $\tau P_n \;=\; -P_n$.

Thus, if σ is the product of k transpositions $\sigma P_n = (-1)^k P_n$, and if σ is also the product of ℓ transpositions $\sigma P_n = (-1)^\ell P_n$. That is, $(-1)^k = (-1)^\ell$ and so k and ℓ are either both even or both odd.

[For alternative proofs, see **F** pp106–108, or exercise 28 on p112.]

Definition 3.2.8: A permutation which can be written as the product of an even (odd) number of transpositions is termed an *even (odd) permutation*. Theorem 3.2.7 shows that these terms are well defined.

Example: Since the identity permutation $\iota = (a, b)(a, b)$ we see that ι is always an even permutation in S_n. The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1, 3, 2, 4)$$

which changes the sign of P_4 is an odd permutation. Indeed $(1, 3, 2, 4) = (1, 4)(1, 2)(1, 3)$.

3.3 Some General Group Theory

Ley G be a group, for $g \in G$ the mapping

$$\lambda_g : G \longrightarrow G : x \longmapsto gx$$

is invertible (indeed $\lambda_g^{-1} = \lambda_{g^{-1}}$: $\lambda_{g^{-1}}\lambda_g(x) = g^{-1}gx = x$ and $\lambda_g\lambda_{g^{-1}}(x) = gg^{-1}x = x$), and also $\lambda_i = Id$, the identity map from G onto G ($\lambda_i(x) = ix = x$, for all $x \in G$).

The mapping

$$g \longmapsto \lambda_g$$

is an *isomorphism* (1-1, onto and preserves the group operation: $x * y \mapsto \lambda_x \circ \lambda_y$) of G onto a subgroup of invertible functions (from G to G), known as the *left regular representation of* G.

Thus, ever group G is isomorphic to a subgroup of invertible (1-1 and onto) functions on some set (namely, G itself). Since such functions are permutations (of G), we see that *every group is isomorphis to a subgroup of the permutations of some set* – this is **Cayley's Theorem** [see, for example, **F** page 180].

Now, let A_n denote the set of all even permutations in S_n and let B_n be the set of all odd permutations in S_n. If τ is any transposition then, $\lambda_\tau : \sigma \mapsto \tau\sigma$ is an invertible (and hence 1-1 and onto) map from A_n to B_n. Thus A_n and B_n are in 1-1 correspondence and so have the same number of elements; namely $n!/2$, half the number of elements in S_n.

Further, $\iota \in A_n$, and if σ and μ are even permutaions (that is, in A_n) then so too is $\sigma\mu$. Also, if $\sigma = \tau_1\tau_2 \cdots \tau_{2k}$, where the τ_i are transpositions, then $\sigma^{-1} = \tau_{2k}^{-1} \cdots \tau_2^{-1}\tau_1^{-1}$, so

σ^{-1} is also an even permutation, and hence in A_n. Thus, A_n is an oder $n!/2$ subgroup of S_n, known as the *alternating group on n symbols*.

These groups play an important role in algebra: for example, the fact that there is no formula in terms of radicals for the roots of a general quintic (or higher order) polynomial is a consequence of the structure of A_5.

4. COSETS, LAGRANGE'S THEOREM and FACTOR GROUPS

4.1 Cosets

Given a group G and a subgroup $H \leq G$ we define a relationship between the elements of G by $a \sim_L b$ if $b^{-1}a \in H$.

'$\sim_L$' is an equivalence relation on G:

Reflexivity, $a \in G \implies a^{-1}a = e \in H \implies a \sim_L a$,

Symmetry, $a \sim_L b \implies b^{-1}a \in H \implies (b^{-1}a)^{-1} \in H \implies a^{-1}b \in H \implies b \sim_L a$, and

Transitivity, $a \sim_L b$ and $b \sim_L c \implies b^{-1}a \in H$ and $c^{-1}b \in H \implies c^{-1}a = (c^{-1}b)(b^{-1}a) \in H \implies a \sim_L c$.

The '$\sim_L$'-equivalence classes are known as the *left H-cosets of G*.

The left H-coset of $a \in G$; that is, the '$\sim_L$'-equivalence class of a is:

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

Intuitively, consider the Abelian case: $a \sim_L b \implies -b + a \in H \implies a - b = h \in H$. That is, a and b differ by an element of H. The left H-cosets are what we would see if we looked at G through 'H-coloured glasses', glasses which could not distinguish elements differing by an element of H.

Note: A similar equivalence relation '$\sim_R$' could be defined by $a \sim_R b$ if $ab^{-1} \in H$. This would lead to the right H-cosets of G where the right H-coset of $a \in G$ is $Ha := \{ha : h \in H\}$. We will work mainly with left cosets, however, some other authors choose to work with right ones.

Examples:

(1) For the symmetric group on n-symbols, S_n, and the alternating subgroup A_n, we see that $A_n = \iota A_n$ and the set of all odd permutations $B_n = \sigma A_n$, where σ is any odd permutation of $\{1, 2, \cdots, n\}$, are the two left A_n-cosets of S_n.

(2) For $G = \mathbf{Z}_6$ and H the subgroup $\{0, 3\}$ the left H-cosets are

$$\begin{aligned}0H = 0 + H = \{0, 3\} = 3H,\\ 1H = 1 + H = \{1, 4\} = 4H,\\ 2H = 2 + H = \{2, 5\} = 5H.\end{aligned}$$

If we rearrange the group table of $\mathbf{Z}_6$ with the elements along the borders collected into left $\{0, 3\}$-cosets we obtain,

$\oplus_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

and we see that it is possible to define a 'multiplication' on the cosets so that they form a group:

	$0H$	$1H$	$2H$
$0H$	$0H$	$1H$	$2H$
$1H$	$1H$	$2H$	$0H$
$2H$	$2H$	$0H$	$1H$

(3) For $n \in \mathbf{N}$ the distinct left $n\mathbf{Z}$-cosets of $\mathbf{Z}$ are:

$$\begin{aligned} 0 + n\mathbf{Z} &= \{\cdots, -n, 0, n, 2n, \cdots\} = n\mathbf{Z}, \\ 1 + n\mathbf{Z} &= \{\cdots, 1 - 2n, 1 - n, 1, n + 1, 2n + 1, \cdots\}, \\ 2 + n\mathbf{Z} &= \{\cdots, 2 - 2n, 2 - n, 2, n + 2, 2n + 2, \cdots\}, \\ &\cdots \\ (n - 1) + n\mathbf{Z} &= \{\cdots, -1, n - 1, 2n - 1, \cdots\} \\ &. \end{aligned}$$

Note, $n + n\mathbf{Z} = \{\cdots, -n, 0, n, 2n, \cdots\} = 0 + n\mathbf{Z}$ etc.

Alternatively, we can note that in this case $a \sim_L b \implies -b + a = kn$, for some $k \in \mathbf{Z}$. That is, $a \equiv b \ (\text{mod} n)$. So, the cosets can be identified with the elements of $\mathbf{Z}_n$. This shows that again in this case it would be possible to define a 'multiplication', $\oplus_n$, on the cosets so that they formed a group.

(4) In S_3,

$\circ$	ι	ρ_1	ρ_2	μ_1	μ_2	μ_3
ι	ι	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ι	μ_3	μ_1	μ_2
ρ_2	ρ_2	ι	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ι	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ι	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ι

with H equal to the subgroup $\{\iota, \mu_1\}$, the left H-cosets are:

$$\begin{aligned}\iota H &= \{\iota, \mu_1\} = \mu_1 H,\\ \rho_1 H &= \{\rho_1, \mu_3\} = \mu_3 H, \text{ and}\\ \rho_2 H &= \{\rho_2, \mu_2\} = \mu_2 H.\end{aligned}$$

Again, arranging the group table of S_3 with the elements along the borders collected into left H-cosets

$\circ$	ι	μ_1	ρ_1	μ_3	ρ_2	μ_2
ι	ι	μ_1	ρ_1	μ_3	ρ_2	μ_2
μ_1	μ_1	ι	μ_2	ρ_2	μ_3	ρ_1
ρ_1	ρ_1	μ_3	ρ_2	μ_2	ι	μ_1
μ_3	μ_3	ρ_1	μ_1	ι	μ_2	ρ_2
ρ_2	ρ_2	μ_2	ι	μ_1	ρ_1	μ_3
μ_2	μ_2	ρ_2	μ_3	ρ_1	μ_1	ι

we see that it would not be possible to define a multiplication on the cosets so that they formed a group in a way similar to what happened in the previous two examples. We will shortly investigate this situation further.

4.2 Lagrange's Theorem

For any group G we have seen (section 3.3) that multiplication by a fixed group element g of G defines a 1-1 mapping λ_g of G onto itself.

For any a, $b \in G$

$$\lambda_{ba^{-1}} : G \longrightarrow G : x \longmapsto ba^{-1}x$$

is such a map. Further, for $H \leq G$

$$\lambda_{ba^{-1}}(aH) = bH.$$

To see this, observe that $x \in aH \implies x = ah$, for some $h \in H \implies \lambda_{ba^{-1}}(x) = ba^{-1}ah = bh \in bH$, so $\lambda_{ba^{-1}}(aH) \subseteq bH$. Similarly, $y \in bH \implies y = bh$, for some $h \in H$, and so for this h we have $\lambda_{ba^{-1}}(ah) = ba^{-1}ah = bh = y$, where $ah \in aH$. Thus, $bH \subseteq \lambda_{ba^{-1}}(aH)$.

Therefore, given any two left H-cosets of G: aH and bH, the mapping $\lambda_{ba^{-1}}$ provides a 1-1 and onto correspondence between them. Thus, any two (and hence all) left H-cosets of G have the same cardinality (number of elements in the case they are finite).

As an application of this we have the following theorem.

Theorem 4.2.1 (Lagrange's Theorem): *Let G be a group of finite order and let H be a subgroup of G, then the order of H, ord(H), divides the order of G, ord(G).*

Proof: Suppose there are ℓ distinct left H-cosets of G. These are all disjoint and partition G (as $a \in aH$), further, by above, they all have the same number of elements, in particular they all have the same number of elements as $eH = H$, namely $\mathrm{ord}(H)$. Thus, $\mathrm{ord}(G) = \ell \times \mathrm{ord}(H)$, establishing the result.

Corollary 4.2.2: *Let G be a finite group, then the order of each element of G divides the order of G.*

Proof: For $a \in G$ we have $\mathrm{ord}(a) \ := \mathrm{ord}(\langle a \rangle)$ which by Lagrange's theorem divides $\mathrm{ord}(G)$, where $\langle a \rangle$ is the cyclic group generated by a.

Corallary 4.2.3: *Every group G of prime order is cyclic.* Thus, up to isomorphism, there is only one group of each prime order.

Proof: By corollary 4.2.2, if $a \neq e$ then $2 \leq \mathrm{ord}(a)$ divides $\mathrm{ord}(G)$, a prime. So, $\mathrm{ord}(a) = \mathrm{ord}(G)$ and $\langle a \rangle = G$.

Remark: Let G be a finite group. One might seek a converse to Lagrange's theorem by asking the question: *if d divides the order of G is there necessarily a subgroup of G of order d?* In general the answer is no: A_4 has order 12, but has no subgroup of order 6. It is true when G is an Abelian group, see **F** theorem 2.13. However, to understand the proof of this it would be necessary to work through section 2.4 of **F**, which falls outside the scope of our course. It is even more trivially true when G is cyclic (in this last case, if $G = \langle a \rangle$ and d divides $\mathrm{ord}(G)$, then $a^{\mathrm{ord}(G)/d}$ generates a subgroup of order d, see theorem 2.2.1).

Notation: For $H \leq G$ the number of left H-cosets of G is the *index* of H in G, denoted by $(G : H)$.

Note: (1) $(G : H)$ also equals the number of right H-cosets of G. See **F** section 2.3, exercise 30.

(2) We may have $(G : H) \ = \ \infty$. However, if $\mathrm{ord}(G) < \infty$, then

$$(G : H) \ = \ \frac{\mathrm{ord}(G)}{\mathrm{ord}(H)} \ < \ \infty.$$

Thinking of $(G : H)$ as this last quotient the following theorem is readily understood.

Theorem 4.2.4: *Let $K \leq H \leq G$ with $(H : K)$ and $(G : H)$ both finite, then*

$$(G : K) \ = \ (G : H) \times (H : K).$$

Proof: See **F** section 2.3, exercise 33.

4.3 Normal Subgroups and Factor (Quotient) Groups

Given a group G and subgroup H of G we investigate when in some natural sense the left H-cosets of G form a group. Examples (2) and (3) of section 4.1 show that in some cases this is possible, while example (4) suggests that in other cases it may not be possible.

Given $H \leq G$ it is natural to define the 'product' of two left H-cosets by

$$(aH) * (bH) = \{xy : x \in aH \text{ and } y \in bH\}.$$

This will only define a binary operation on the left H-cosets of G if the right hand side is itself a left H-coset of G, and the examples referred to above show that this may and may not be the case.

Since $a \in aH$ and $b \in bH$ we have that ab is in the right hand side, so if this right hand side is to be a left H-coset it must be $(ab)H$ (remember, cosets are equivalence classes and ab is a representative of $(ab)H$). Thus, in order to define a binary operation on the left H-cosets we must have H such that

$$\text{for all } a,\, b \in G \text{ we have } (aH) * (bH) = (ab)H. \qquad (*)$$

We aim to identify what properties the subgroup H must have in order for $(*)$ to hold.

Now, for any $a \in G$ and $x \in Ha$ we have $x = ha$, for some $h \in H$. So,

$$\begin{aligned} ax = a(ha) &= (ah)(ae) \\ &\in (aH) * (aH) \\ &= a^2H, \quad \text{if (*) is true} \end{aligned}$$

and $ax = a^2h'$, for some $h' \in H$. That is, $x = ah' \in aH$.

Therefore, $(*)$ implies that $Ha \subseteq aH$, for all $a \in G$.

But then, if $Ha \subseteq aH$, for all $a \in G$, we have for any $b \in aH$ that

$$\begin{aligned} b &= ah, \quad \text{for some } h \in H, \\ &= (ah)e \\ &= (ah)(a^{-1}a) \\ &= a(ha^{-1})a \\ &= a(a^{-1}h')a, \quad \text{as } ha^{-1} \in Ha \subseteq aH, \text{ so } ha^{-1} = a^{-1}h', \text{ for some } h' \in H. \\ &= h'a \\ &\in Ha \end{aligned}$$

and so $Ha = aH$.

Thus, a necessary condition for $(*)$ to hold is that $Ha = aH$, for all $a \in G$.

This condition is also sufficient. That is, $aH = Ha$, for all $a \in G$, implies $(*)$. To see this, note that always $(ab)H = (ae)bH \subseteq aHbH$, so we need only show that $aHbH \subseteq abH$. Let $x \in aH$ and let $y \in bH$, so $x = ah_x$ and $y = bh_y$, for some $h_x, h_y \in H$. Then,

$$\begin{aligned} xy = (ah_x)(bh_y) &= a(h_x b)h_y \\ &= abh'h_y, \quad \text{as } h_x b \in Hb = bH, \text{ so } h_x b = bh' \text{ for some } h' \in H, \\ &\in (ab)H. \end{aligned}$$

We encapsulate the property $(*)$ with the following definition.

Definition 4.3.1: A subgroup H of the group G for which $aH = Ha$, for all $a \in G$, is called a *normal subgroup* of G, denoted by $H \trianglelefteq G$.

For example: Any subgroup of an Abelian group is a normal subgroup. However, the subgroup $H = \{\iota, \mu_1\}$ of S_3 is not a normal subgroup, $\rho_2 H = \{\rho_2, \mu_2\}$, while $H\rho_2 = \{\rho_2, \mu_3\}$.

Clearly for a normal subgroup N of a group G the left N-cosets of G and the right N-cosets of G coincide. Bearing this in mind, when $N \trianglelefteq G$ we will simply refer to the N-cosets of G. The converse of this observation is also true.

Proposition 4.3.2: *$H \leq G$ is a normal subgroup of G if and only if every left H-coset of G is also a right H-coset of G and vice versa.*

Proof: We need only prove $(\Longleftarrow)$. Now, given any $a \in G$ suppose $aH = Hb$, then $a \in aH = Hb$. Thus, a is a representative of the equivalence class Hb and so we must have $Hb = Ha$. But then, $aH = Hb = Ha$ and $H \trianglelefteq G$.

Exercise: For a group G and $H \leq G$, show that $H \trianglelefteq G$ if and only if $g^{-1}hg \in H$, for all $g \in G$ and all $h \in H$.

Puting all this together, we can now state the main result of this section.

Theorem 4.3.3: *Let G be a group and let N be a normal subgroup of G, then the N-cosets of G with the binary operation*

$$(aN) * (bN) := (ab)N$$

form a group known as the quotient *(or* factor*)* group of G by N, *and denoted by G/N.*

Proof: The definition of a normal subgroup was devised to describe precisely those subgroups for which the operation $*$ is a binary operation on the cosets. Thus we need only verify that the group axioms (G1) to (G3) are satisfied.

(G1): The associativity of $*$ is inherited from G.

(G2): $eN = N$ is an identity element. Indeed, $eNaN = eaN = aN$ and $aNeN = aeN = aN$.

(G3): $a^{-1}N$ is an inverse for aN, as $a^{-1}NaN = a^{-1}aN = eN$ and $aNa^{-1}N = aa^{-1}N = eN$.

From section 4.1 we have the following.

Examples: (1) $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to $\mathbf{Z}_n = (\{0, 1, 2, \cdots, n-1\}, \oplus_n)$.

(2) $\mathbf{Z}_6/\{0, 3\}$ has as its group table

	$0H$	$1H$	$2H$
	$\{0,3\}$	$\{1,4\}$	$\{2,5\}$
$0H = \{0,3\}$	$0H$	$1H$	$2H$
$1H = \{1,4\}$	$1H$	$2H$	$0H$
$2H = \{2,5\}$	$2H$	$0H$	$1H$

which is isomorphic to $\mathbf{Z}_3$.

5. HOMOMORPHISMS and the HOMOMORPHISM THEOREM So far we have been fairly informal in our teatment groups being isomorphic we will shortly make this precise. First, however, we consider a more general notion.

5.1 Homomorphisms

Definition5.1.1: Let $G_1 = (G_1, *_1)$ and $G_2 = (G_2, *_2)$ be two groups. A function (mapping) $\phi : G_1 \longrightarrow G_2$ is a *homomorphism* if

$$\phi(a *_1 b) = \phi(a) *_2 \phi(b), \quad \text{for all } a, b \in G_1.$$

Examples 5.1.2: (1) The trivial homomorphism from any group G_1 into any other group G_2 given by $\phi(a) = e_2$, for all $a \in G_1$, where e_2 is the identity element of G_2. [$\phi(a *_1 b) = e_2 = e_2 *_2 e_2 = \phi(a) *_2 \phi(b)$.]

(2) Any linear transormation $T : \mathbf{R}^n \longrightarrow \mathbf{R}^m : \mathbf{x} \longmapsto M\mathbf{x}$, where M is an $m \times n$-matrix, and the group operation is vector addition.
[$T(\mathbf{x} + \mathbf{y}) = T(\mathbf{x}) + T(\mathbf{y})$.]

(3) The determinant $\det(A)$ defines a homomorphism $\mathrm{GL}(n, \mathbf{R}) \longrightarrow (\mathbf{R}^*, \times)$, where $\mathrm{GL}(n, \mathbf{R})$ is the general linear group of all ($n \times n$-invertible matrices with matrix multiplication as the group operation.
[$\det(AB) = \det(A)\det(B)$.]

(4) Let G be the group of functions from a domain D into $\mathbf{R}$ with addition defined pointwise. That is, $(f + g)(x) := f(x) + g(x)$. The first + (addition of functions)is being defined, the second + is ordinary addition of numbers.

For any $x_0 \in D$ the *evaluation functional* $f \longmapsto f(x_0)$ defines a homomorphism from G into $(\mathbf{R}, +)$.

(5) For the group $\mathcal{C}[0, 1]$ of real valued continuous function on the interval [0,1]

$$\phi(f) := \int_0^1 f(x)dx$$

defines a homomorphism from $\mathcal{C}[0, 1]$ into $(\mathbf{R}, +)$.
[$\int_0^1 (f + g) = \int_0^1 f \ + \ \int_0^1 g$.]

(6) Differentiation D on the additive group of differentiable real valued function of a real variable is a homomorphism into the additive group of real valued functions of a real variable. [$D(f + g) = Df + Dg$.]

(7) The mapping $(\mathbf{Z}, +) \longrightarrow (n\mathbf{Z}, +) : a \longmapsto na$ is a homomorphism (verify this).

Theorem 5.1.3: *Let G_1 and G_2 be two groups, and let $\phi : G_1 \longrightarrow G_2$ be a homomorphism, then:*

(i) $\phi(e_1) = e_2$,

(ii) *for any $a \in G_1$ we have $\phi(a^{-1}) = \phi(a)^{-1}$,*

(iii) *$H \leq G_1$ implies $\phi(H) \leq G_2$. In particular, $\phi(G_1)$, the range of ϕ, is a subgroup of G_2, and*

(iv) *$K \leq G_2$ implies $\phi^{-1}(K) := \{a \in G_1 : \phi(a) \in K\}$, the preimage of K, is a subgroup of G_1.*

Proof:

(i) $e_2 = \phi(e_1)\phi(e_1)^{-1} = \phi(e_1^2)\phi(e_1)^{-1} = \phi(e_1)\phi(e_1)\phi(e_1)^{-1} = \phi(e_1)$.

(ii) For $a \in G$ we have $\phi(a)\phi(a)^{-1} = e_2 = \phi(e_1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ and so $\phi(a)^{-1} = \phi(a^{-1})$.

(iii) Let a_2 and b_2 be any two elements of $\phi(H)$, then there exists a_1 and b_1 in H such that $a_2 = \phi(a_1)$ and $b_2 = \phi(b_1)$ and so $a_2b_2^{-1} = \phi(a_1)\phi(b_1)^{-1} = \phi(a_1)\phi(b_1^{-1}) = \phi(a_1b_1^{-1}) \in \phi(H)$, as $a_1b_1^{-1} \in H$. Thus, $\phi(H)$ is a subgroup of G_2.

(iv) If a and b are any two elements in $\phi^{-1}(K)$, then $\phi(a), \phi(b) \in K$, so $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} \in K$ and therefore $ab^{-1} \in \phi^{-1}(K)$. Thus $\phi^{-1}(K)$ is a subgroup of G_1.

5.2 Isomorphisms

Definition 5.2.1: Let G_1 and G_2 be two groups. A homomorphism $\phi : G_1 \longrightarrow G_2$ which is one-to-one and onto is an *isomorphism*.

Examples 5.1.2: (1) $\mathbf{Z} \longrightarrow n\mathbf{Z} : a \longmapsto na$.

(2) $\phi : U_4 \longrightarrow \mathbf{Z}_4 : \omega^n \longmapsto n$, where $n = 0, 1, 2, 3$ and $\omega = e^{i\pi/2} = i$.

(3) An infinite cyclic group $\langle a \rangle \longmapsto (\mathbf{Z}, +) : a^n \longmapsto n$.

Theorem 5.2.3: *If $\phi : G_1 \longrightarrow G_2$ is an isomorphism, then the inverse map $\phi^{-1} : G_2 \longrightarrow G_1$ exists and is an isomorphism of G_2 to G_1.*

Proof: Since ϕ is one-to-one and onto we know from the general theory of functions that ϕ^{-1} exists and is also one-to-one and onto, thus it only remains to show it is a homomorphism.

Now, given any a_2 and b_2 in G_2, since ϕ is onto, there exists a_1 and b_1 in G_1 with $a_2 = \phi(a_1)$ and $b_2 = \phi(b_1)$, indeed $a_1 = \phi^{-1}(a_2)$ and $b_1 = \phi^{-1}(b_2)$. Thus,

$$\phi^{-1}(a_2b_2) = \phi^{-1}(\phi(a_1)\phi(b_1)) = \phi^{-1}(\phi(a_1b_1)) = a_1b_1 = \phi^{-1}(a_2)\phi^{-1}(b_2).$$

5.3 Homomorphisms and factor groups

Let G_1 and G_2 be groups and let $\phi : G_1 \longrightarrow G_2$ be a homomorphism. From theorem 5.1.3 (iv) with K equal to the trivial group $\{e_2\}$ we know that $\phi^{-1}(e_2)$ is a subgroup of G_1, known as the *kernel* of ϕ:

$$\mathrm{Ker}\phi \;:=\; \phi^{-1}(e_2).$$

This should be compared with the notion of the kernel of a linear transformation as used in linear algebra, indeed the two notions are essentially the same. If we forget about scalar multiplication a vector space with vector addition as the operation is an Abelian group (with identity element the zero vector, $\mathbf{0}$) and a linear transformation T between two such spaces is then a homomorphism with $\mathrm{Ker}\, T = T^{-1}(\mathbf{0})$.

Proposition 5.3.1: $\mathrm{Ker}\phi \trianglelefteq G_1$.

Proof: