Groups, Rings and Fields
Group Theory

1. Introduction to groups

A *group* is made of two ingredients:

a **set**, often called G

and

a **binary operation** on the set.

1.1. Binary operations.

Definition 1.1. Let A be a set. A *binary operation*[1] $*$ on A is a function

$$* : A \times A \to A; (a, b) \mapsto a * b$$

(i.e. we do not write $*(a, b)$ but rather $a * b$).

Notation (see What you need to know before you start)
Natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$; integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, rationals $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$, real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$.

Example 1.2. (1) $+$ is a binary operation on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
(2) $-$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
(3) $/$ (i.e. $(a, b) \mapsto a/b$) on $\mathbb{R}^*, \mathbb{Q}^*, \mathbb{C}^*$, where $U^* = U \setminus \{0\}$.
(4) $+$ on $M_n(\mathbb{R})$ ($n \times n$ matrices over $\mathbb{R}$).
(5) $\times$ on $M_n(\mathbb{R})$.

Remark 1.3.
(*i*) The fact that $a * b \in A$ is expressed as saying A is *closed* under $*$.
Notice that $-$ is closed on $\mathbb{Z}$ but not on $\mathbb{N}$ as e.g. $1 - 2 = -1 \notin \mathbb{N}$.
(*ii*) Order matters: $a * b$ is not generally the same as $b * a$, e.g. with $-$ on $\mathbb{Z}$ we have $1 - 2 \neq 2 - 1$.
(*iii*) The fact that $*$ is a function with domain $A \times A$ means that for every $a, b \in A$, $a * b$ is *defined*.
E.g. $/$ on $\mathbb{R}$ where $(a, b) \mapsto a/b$ is not a binary operation as $1/0$ is not defined.
(*iv*) The fact that $*$ is a function means that for every $a, b \in A$, $a * b$ is *uniquely* defined. This is called being **well defined**.
Warning it is not always clear that $*$ is well defined (although it usually is!).
E.g. $*$ on $\mathbb{Q}$ given by $\frac{a}{b} * \frac{c}{d} = \frac{a+c}{|b|+|d|}$ is not a binary operation as it is not well defined:

$$\frac{1}{2} * \frac{2}{3} = \frac{1+2}{2+3} = \frac{3}{5},$$

BUT ALSO

$$\frac{1}{2} * \frac{2}{3} = \frac{2}{4} * \frac{2}{3} = \frac{4}{7},$$

[1] These were called *multiplication functions* in MSI.

and

$$\frac{3}{5} \neq \frac{4}{7}.$$

i.e. there are two choices for $\frac{1}{2} * \frac{2}{3}$ so that $*$ (the function $(\frac{a}{b}, \frac{c}{d}) \mapsto \frac{a+c}{|b|+|d|}$) is not well-defined.

Other cases where 'things go wrong' are usually similar in the sense that there is more than one way of writing the elements of the set, in this case $\mathbb{Q}$.

Definition 1.4. A binary operation $*$ on A is *commutative* if for all $a, b \in A$

$$a * b = b * a.$$

e.g. $+$ on $\mathbb{Z}$ **is** commutative as $a + b = b + a$ for all $a, b \in \mathbb{Z}$; $-$ on $\mathbb{Z}$ is **not** commutative as $1 - 2 \neq 2 - 1$.

Other common symbols for binary operations are:

$$a \cdot b$$

$a + b$ particularly for commutative operations

$a \circ b$ particularly for composition of functions

and

nothing !

i.e. we just write

$$ab$$

we call this juxtaposition.

(Cayley) Tables A binary operation $*$ on a *finite* set G can be described by a table:

$*$	$\cdot$	$\cdot$	g	$\cdot$	$\cdot$	h	$\cdot$	$\cdot$
$\cdot$ $\cdot$								
g			$g * g$			$g * h$		
$\cdot$ $\cdot$								
h			$h * g$			$h * h$		
$\cdot$ $\cdot$								

Notice that $*$ is commutative if and only if the table is symmetric around the leading (north-west to south-east) diagonal, for example, $\times$ on $\{0, 1, -1\}$ is commutative, and has table

$\times$	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

but $*$ on $\{0, 1, -1\}$ given by the rule $a * b = b$ is not commutative, and has table

$*$	0	1	-1
0	0	1	-1
1	0	1	-1
-1	0	1	-1

1.2. **What is a group?**

Definition 1.5. A *group* $(G, *)$ is a set G, together with a binary operation $*$ on G, such that:

(a) for all $a, b, c \in G$,

$$a * (b * c) = (a * b) * c,$$

(b) there exists $e \in G$ such that for all $a \in G$,

$$e * a = a = a * e,$$

(c) for all $a \in G$ there exists $b \in G$ such that

$$a * b = e = b * a.$$

Remark 1.6. (i) (a) is the *associative law*;

(ii) we often drop mention of $*$ when it is clear, saying 'G' rather than '$(G, *)$' and writing 'ab' for $a * b$

(iii) being closed is built into the definition of a binary operation.

Definition 1.7. Let G be a group. The *order* of G is $|G|$ (the cardinality of the *set* G). A group is *finite/infinite* if and only if its order is finite/infinite.

Lemma 1.8. *Let G be a group. Then:*

(i) the element e such that $e * a = a = a * e$ for all $a \in G$ is unique;

(ii) given a, the element b such that $a * b = e = b * a$ is unique.

Proof. (i) Suppose $e, f \in G$ and for all $a \in G$,

$$e * a = a = a * e \text{ and } f * a = a = a * f.$$

Then

$$e * f = f \text{ and } e * f = e,$$

so that $e = f$.

We say e is **the identity** of G: we can also write $e_G, 1$ or 1_G.

(ii) Let $a \in G$ and suppose $b, c \in G$ with

$$b * a = e = a * b \text{ and } c * a = e = a * c.$$

Then

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

We say that b is **the inverse** of a and usually write $b = a^{-1}$. □

We emphasise: a^{-1} is the *unique* element of G such that

$$a^{-1} * a = e = a * a^{-1}.$$

Lemma 1.9. *Let G be a group. Then for all $a, b, c \in G$ we have:*

(1) $(a^{-1})^{-1} = a$;
(2) $(ab)^{-1} = b^{-1}a^{-1}$;
(3) $ab = ac \Rightarrow b = c$;
(4) $ba = ca \Rightarrow b = c$.

Proof. (1) Follows from uniqueness of inverses and

$$a^{-1}a = e = aa^{-1}.$$

(2) We have

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

and similarly,

$$(b^{-1}a^{-1})(ab) = e.$$

By uniqueness of inverses, $(ab)^{-1} = b^{-1}a^{-1}$.

(3) We have

$$\begin{array}{lll} ab = ac & \Rightarrow & a^{-1}(ab) = a^{-1}(ac) \\ & \Rightarrow & (a^{-1}a)b = (a^{-1}a)c \quad \text{by associativity} \\ & \Rightarrow & eb = ec \quad \text{as } a^{-1}a = e \\ & \Rightarrow & b = c \quad \text{as } e \text{ is the identity.} \end{array}$$

(4) Dual.

□

(3) and (4) above are the left and right *cancellation laws.*

Look back at the 3 theorems presented in Lecture 1!

Corollary 1.10. *Let G be a group. Then for all $a_1, \ldots, a_n \in G$,*

$$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

Proof. By Lemma 1.9 and induction. □

Corollary 1.11. The Latin Square Property *Let G be a group of finite order. Then every element of G occurs exactly once in every row and in every column of the table of G.*

Proof. Consider the row R_a labelled by $a \in G$.

	e		y
e	e		y
			$\vdots$
a	a	$\dots$	ay

Let $g \in G$. Then $a^{-1}g \in G$ and

$$a(a^{-1}g) = (aa^{-1})g = eg = g,$$

so that g appears in R_a in the column labelled by $a^{-1}g$.

	e		$a^{-1}g$
e	e		$a^{-1}g$
			$\vdots$
a	a	$\dots$	g

If g also appears in R_a in the column labelled by h,

	e		$a^{-1}g$	h
e	e		$a^{-1}g$	h
			$\vdots$	
a	a	$\dots$	g	g

then

$$g = a(a^{-1}g) = ah,$$

so that by cancellation we find

$$a^{-1}g = h.$$

Thus g appears *exactly* once in each row. Similarly for columns. □

Example 1.12. If

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

is the partial table of a group, then this must be

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

Proof. In any group, if t is the identity, then $tt = t$, so that t lies on the leading diagonal. Thus e is the identity. So, we fill in the table to get

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

We then use the Latin Square Property to fill in the remainder. For example, in the row labelled by a, we need to find ab and ac. But $ab \neq a$ or e (since they appear in row a) and $ab \neq b$ (since b already appears in column b). Thus, $ab = c$. □

Definition 1.13. A group $(G, *)$ is *commutative* or *abelian*[2] if

$$a * b = b * a$$

for all $a, b \in G$ (i.e. $*$ is *commutative*).

1.3. **First examples of groups.** *Notation* For a subset $X \subseteq \mathbb{C}$, let

$$X^* = \{x \in X : x \neq 0\} = X \setminus \{0\};$$

also

$$\mathbb{Q}^+ = \{q \in \mathbb{Q} : q > 0\} \text{ and } \mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}.$$

Example 1.14. $(\mathbb{R}^*, \times)$ is a group with identity 1 and inverse of a being $\frac{1}{a}$.
Since $a \times b = b \times a$ for all $a, b \in \mathbb{R}^*$, we have $(\mathbb{R}^*, \times)$ is commutative and infinite.
Similarly,
$(\mathbb{Q}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^+, \times)$ and $(\mathbb{R}^+, \times)$ are commutative, infinite groups.

Question: why are $(\mathbb{Z}^*, \times)$ *and* $(\mathbb{C}^+, \times)$ **not** *groups?*

Example 1.15. Let $T = \{1, -1\}$, then $(T, \times)$ is a commutative group with table

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

The order of T is 2.

[2]If we see a binary operation that is written using a symbol + then almost always we have $a+b = b+a$ for all $a, b \in G$, that is, the operation is commutative. If in a group the operation is written as + and indeed we have $a + b = b + a$ for all $a, b \in G$ then we would normally say the group is abelian. Thus, the term 'abelian group' is usually reserved for commutative groups where the binary operation is denoted by + (or by a similar symbol).

Example 1.16. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all *abelian* (commutative) groups with identity 0 and the inverse of a being $-a$.

Notation If $(G, +)$ is a group we write

$$0 \text{ or } 0_G$$

for the identity of G and

$$-a$$

for the inverse of a.

Convention $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ always denote groups under $\times$;
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ always denote groups under $+$.

Some of the most important examples of groups comes from matrices.

Definition 1.17. We let $\mathrm{GL}(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$.

Claim $(\mathrm{GL}(n, \mathbb{R}), \times)$ is a group: the ***general linear group*** over $\mathbb{R}$.

Proof Let $A, B \in \mathrm{GL}(n, \mathbb{R})$. Then

$$\det(AB) = (\det A)(\det B) \neq 0$$

so $AB \in \mathrm{GL}(n, \mathbb{R})$. Thus $\times$ is a binary operation on $\mathrm{GL}(n, \mathbb{R})$.

We know that $\times$ is associative.

We know that $\det I_n = 1 \neq 0$, so $I_n \in \mathrm{GL}(n, \mathbb{R})$ and certainly

$$I_n A = A = A I_n$$

for all $A \in \mathrm{GL}(n, \mathbb{R})$.

If $A \in \mathrm{GL}(n, \mathbb{R})$, then

$$\det A^{-1} = \frac{1}{\det A} \neq 0$$

so that $A^{-1} \in \mathrm{GL}(n, \mathbb{R})$ and certainly

$$A A^{-1} = I_n = A^{-1} A,$$

so that A^{-1} is the inverse of A in $\mathrm{GL}(n, \mathbb{R})$.

Corollary 1.18. *As* $\mathrm{GL}(n, \mathbb{R})$ *is a group, the inverse of a matrix is unique.*

Take care The group $\mathrm{GL}(n,\mathbb{R})$ is *not* commutative (see Exercises). From Lemma 1.9 that if $A, B \in \mathrm{GL}(n,\mathbb{R})$ then $(AB)^{-1} = B^{-1}A^{-1}$.

Similarly For any field F we denote the set of $n \times n$ matrices over F by $M_n(F)$. If we put

$$\mathrm{GL}(n,F) = \{A \in M_n(F) : \det A \neq 0\},$$

then $\mathrm{GL}(n,F)$ is a group in the same way as above, and is the *general linear group over* F.

Lemma 1.19. *Let* $K = \{e, a, b, c\}$ *and* $\cdot$ *be given by*

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

Then $(K, \cdot)$ *is a group, the* Klein 4-group.

Proof. From examining the table, we only need to show associativity. Consider the expressions $(xy)z$, $x(yz)$. We need to show that for any values of x, y, z from K we have $(xy)z = x(yz)$.

(1) If at least one of x, y, z is e, then the result is true.
(2) If $x, y, z \in \{a, b, c\}$ and are distinct, then $(xy)z = zz = e$ and $x(yz) = xx = e$.
(3) If $x, y, z \in \{a, b, c\}$ and $x = y \neq z$, then $(xy)z = ez = z$ and $x(yz) = xt = z$ where $t = yz \neq x$.
(4) If $x, y, z \in \{a, b, c\}$ and $x = y = z$, then $(xy)z = ez = z$ and $x(yz) = xe = x$;

the other cases similarly, using commutativity. □

Definition 1.20. If $x^{-1} = x$ for $x \in G$, then x is *self-inverse*. Note $e^{-1} = e$ so e is *always* self-inverse.

Note K is commutative and all elements are self-inverse.

1.4. **The groups** $(\mathbb{Z}_n, \oplus)$ **and** $(\mathbb{Z}_p^*, \otimes)$**,** p **a prime.** *We construct two classes of examples of groups built from integers modulo* n*; in particular we will show there is a group of any finite order.*

(See **WYNTKBYS** for further details). Let $n \in \mathbb{N}$. Recall that for $u, v \in \mathbb{Z}$

$u \equiv v \pmod{n} \Leftrightarrow n|(u - v)) \Leftrightarrow u$ and v leave the same remainder on division by n.

Then $\equiv \pmod{n}$ is an *equivalence relation*. For $a \in \mathbb{Z}$ we write

$$[a] = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\},$$

i.e. $[a]$ is the equivalence class of a.

Definition 1.21. We let $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$; we say $\mathbb{Z}_n$ *is the integers modulo* n. We define $\oplus$ and $\otimes$ on $\mathbb{Z}_n$ by:

$$[a] \oplus [b] = [a + b]$$

and

$$[a] \otimes [b] = [a \times b].$$

The next lemma is taken from Stage 1.

Lemma 1.22. *The operations* $\oplus$ *and* $\otimes$ *are associative and commutative binary operations on* $\mathbb{Z}_n$*, with identities* $[0]$ *for* $\oplus$ *and* $[1]$ *for* $\otimes$*.*

For a recap on what is required for well-definedness, here is the proof that $\oplus$ is well-defined.

Proof. Let $[a], [b] \in \mathbb{Z}_n$. We want to show that $[a] \oplus [b] := [a + b]$ takes only one value for any pair $([a], [b])$. This amounts to showing that if we take other representatives of the same equivalence class of a or b, then the sum $[a] \oplus [b]$ is unchanged.

To this end, suppose that $[a] = [a']$ and $[b] = [b']$. Then by properties of equivalence relations, $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. By definition of congruence modulo n we have that $n \mid (a - a')$ and $n \mid (b - b')$ so that $n \mid \big((a - a') + (b - b')\big) = \big((a + b) - (a' + b')\big)$. Hence $a + b \equiv a' + b' \pmod{n}$ and so

$$[a] \oplus [b] = [a + b] = [a' + b'] = [a'] \oplus [b']$$

so that $\oplus$ is well-defined as required. □

Theorem 1.23. $(\mathbb{Z}_n, \oplus)$ *is a commutative group of order* n*.*

Proof. From Lemma 1.22 we have $\oplus$ is well defined, commutative and associative with identity $[0]$. It is easy to see that

$$[0] \oplus [a] = [a], [a] \oplus [-a] = [0],$$

so that $(\mathbb{Z}_n, \oplus)$ is a commutative group with identity $[0]$ and inverse of $[a]$ being $[-a]$. □

Convention (i) When we write $\mathbb{Z}_n$ we *always* mean $\mathbb{Z}_n$ under $\oplus$.

(ii) We drop $\bigcirc$ from $\oplus$, and write $[a]$ as a, where the context is clear. So e.g. in $\mathbb{Z}_4$

$$7 = 3, -15 = 1, 7 + (-15) = -8 = 0 = 3 + 1.$$

Table for $(\mathbb{Z}_2, \oplus)$:

$+$	0	1
0	0	1
1	1	0

Note this is 'the same' as for $(T, \times)$ where $T = \{1, -1\}$.

Note We often write $[a][b]$ for $[a] \otimes [b]$.

Dropping the $[,]$ we have:

Table for $(\mathbb{Z}_3, \otimes)$

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table for $(\mathbb{Z}_4, \otimes)$

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Notice that neither of the tables above is that of a group! (Why not?)

Definition 1.24. For $n \in \mathbb{N}$ we put

$$\mathbb{Z}_n^* = \{[1], [2], \ldots, [n-1]\} = \mathbb{Z}_n \setminus \{[0]\}.$$

Notice that

$$[x] \in \mathbb{Z}_n^* \iff [x] \neq [0] \iff n \not| \, x.$$

Standard properties of prime numbers (**WYNTKBYS**) are the key to the next result.

Theorem 1.25. *Let p be a prime. Then $(\mathbb{Z}_p^*, \otimes)$ is a commutative group of order $p-1$.*

Proof. By Lemma 1.22 as an operation on $\mathbb{Z}_p$, $\otimes$ is well-defined, associative commutative and has identity $[1] \in \mathbb{Z}_p^*$.

We need to show that $\mathbb{Z}_p^*$ is closed under $\otimes$, so that $\otimes$ is a binary operation on $\mathbb{Z}_p^*$.

Let $[a], [b] \in \mathbb{Z}_p^*$. Then $p \not| \, a$ and $p \not| \, b$. As p is prime, $p \not| \, ab$ and so $[a][b] = [ab] \in \mathbb{Z}_p^*$ and $\mathbb{Z}_p^*$ is closed under $\otimes$.

Let $[a] \in \mathbb{Z}_p^*$; it only remains to show that every $[a]$ has an inverse in $\mathbb{Z}_p^*$. Since $p \not| \, a$ we have that $h.c.f.(a, p) = 1$ so that there exist $s, t \in \mathbb{Z}$ with

$$1 = as + pt.$$

Then

$$[1] = [as + pt] = [as] = [a][s],$$

so that $[a]^{-1}$ exists (and equals $[s]$). □

In practice, we do not need the Euclidean Algorithm to find s above, as just writing down the Cayley table for $\mathbb{Z}_p^*$ will yield the required inverses. For example

Table for $(\mathbb{Z}_7^*, \otimes)$

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1				
5	5					
6	6					1

so that $2^{-1} = 4, 3^{-1} = 5, 6^{-1} = 6$, etc.

Convention When we write $\mathbb{Z}_p^*$ we always mean the group $\mathbb{Z}_p^*$ under $\otimes$. We may simplify by dropping [,] and $\otimes$ by writing $\times$ or just using juxtaposition.

So far, the only non-commutative groups you have seen are infinite. Later, we will fix this, when we meet symmetric groups *and their 'subgroups'. These are used to encode the notion of symmetry, discussed in the Introduction in Lecture 1.*

2. Orders of elements, subgroups, and cyclic subgroups

2.1. Housekeeping! Routine - but important - properties of groups.

The general associative law a.k.a. 'We can leave out the brackets'

Let $(G, *)$ be a group. By the associative law, we know that

$$(a * b) * c = a * (b * c)$$

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

What can we say about products of four elements? As $*$ is a *binary* operation we can only combine two elements at once. So in expressions such as

$$a * b * c * d$$

we (ostensibly) need brackets to tell us which order to do the operations... such as

$$(a * b) * (c * d)$$

or

$$a * (b * (c * d)).$$

Fortunately we have:

Lemma 2.1. The general associative law *For any group G, and any $a_1, a_2, \ldots, a_n \in G$, the product*

$$a_1 * a_2 * \ldots * a_n$$

is unambiguous.

Proof. See Appendix □

Remark In the above result, we did not need that G was a group; we only used the fact that $*$ is a binary operation on G satisfying the associative law.

Taking powers in groups

For $g \in G$ we write

$$g^2 \text{ for } gg$$

and

$$g^3 \text{ for } ggg.$$

So, for example,

$$(ab)^2 = (ab)(ab).$$

If $ab = ba$, i.e. *a and b commute*, then **in this case**

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2.$$

However

$$\boxed{\text{In general } (ab)^2 \neq a^2b^2.}$$

Definition 2.2. For $n \in \mathbb{N}$ and $g \in G$ we define:

$$g^n = \underbrace{(g \dots g)}_{n \text{ factors}}$$

$$g^0 = e$$

and

$$g^{-n} = \underbrace{(g^{-1} \dots g^{-1})}_{n \text{ factors}} = (g^{-1})^n.$$

Proposition 2.3. The Index Laws *For any $g \in G$ and $z_1, z_2 \in \mathbb{Z}$ we have*

(1) $g^{z_1}g^{z_2} = g^{z_1+z_2}$;
(2) $(g^{z_1})^{z_2} = g^{z_1z_2}$.

Proof. See Appendix □

Note We deduce

$$g^{z_1}g^{z_2} = g^{z_1+z_2} = g^{z_2+z_1} = g^{z_2}g^{z_1},$$

so that *powers of g commute with eachother.*

Notation

	Multiplicative	Additive
$x * y$	xy	$x + y$
identity	e or 1 or e_G or 1_G	0 or 0_G
inverse	x^{-1}	$-x$
power	x^z	zx
index laws	$g^{z_1}g^{z_2} = g^{z_1+z_2}$	$z_1g + z_2g = (z_1 + z_2)g$
	$(g^{z_1})^{z_2} = g^{z_1z_2}$	$z_2(z_1g) = (z_1z_2)g$

2.2. **Orders of elements.** *We have already met the notion of the order of a group. Now we see the same word, order, used to denote a property of an element of a group. Later we see the two uses are related!*

Let G be a group. Recall that for $a \in G$ and $n \in \mathbb{N}$ we have

$$a^0 = e,\ a^n = \underbrace{a \dots a}_{n},\ a^{-n} = (a^{-1})^n = (a^n)^{-1},$$

using the index laws.

Also, as $ee = e$ so $e^{-1} = e$ we have:

$$e^0 = e,\ e^n = \underbrace{e \dots e}_{n} = e,\ e^{-n} = (e^{-1})^n = e^n = e,$$

i.e.

$$\boxed{e^z = e \text{ for all } z \in \mathbb{Z}.}$$

Consider the list

$$a(=a^1), a^2, a^3, \ldots$$

either at least one a^i is e **or** no a^i is e.

Definition 2.4. The *order* of a, written $o(a)$, is the least $n \in \mathbb{N}$ such that $a^n = e$, if such n exists. Otherwise, $o(a) = \infty$.

Beware: $o(a)$ does NOT have the same meaning as the order of G.

In + notation, $a^n = e$ is written as $na = 0$.

For any $a \in G$ we have

$$o(a) = 1 \Leftrightarrow a^1 = e \Leftrightarrow a = e$$

so

$$\boxed{e \text{ is the } \textbf{ONLY} \text{ element of order 1.}}$$

For any $a \in G$ we have

$$o(a) = 2 \Leftrightarrow a = a^1 \neq e \text{ and } a^2 = e$$

$$\Leftrightarrow a \neq e \text{ and } a^{-1} = a.$$

$$\boxed{o(a) = 1 \text{ or } 2 \text{ if and only if } a \text{ is self-inverse } (a = a^{-1}).}$$

Examples

$\underline{(\mathbb{R}^*, \times)}$ 1 has order 1 (it is the identity). For any $x \neq 1$ we have $x^n = 1 \Rightarrow x = -1$, so that $o(1) = 1, o(-1) = 2$ and $o(x) = \infty$ for all $x \in \mathbb{R}^* \setminus \{1, -1\}$.

$\underline{(\mathbb{C}^*, \times)}$ Note that i has order 4 as

$$i \neq 1, i^2 = -1 \neq 1, i^3 = -i \neq 1 \text{ but } i^4 = 1.$$

In fact, $\mathbb{C}^*$ has elements of every order *can you check this?*

$\underline{(\mathbb{R}, +)}$ $o(0) = 1$ as 0 is the identity.

For any $x \neq 0$ we have

$$nx = \underbrace{x + x + \ldots + x}_{n} \neq 0,$$

for any $n \in \mathbb{N}$. Thus $o(x) = \infty$ for all $x \neq 0$.

$\underline{(\mathrm{GL}(2, \mathbb{R}), \times)}$ The matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ has order 2.

The two notions of order (order of group and order of element) are closely related, as we will see.

Theorem 2.5. *Let G be a finite group and let $a \in G$. Then $o(a)$ is finite.*

Proof. The list

$$a, a^2, a^3, \ldots$$

must contain repeats, as G is finite. Say $a^i = a^j$ where $i < j$. Then

$$\begin{array}{rrcll} & a^i & = & a^j & \\ \Rightarrow & a^i a^{-i} & = & a^j a^{-i} & \\ \Rightarrow & a^{i-i} & = & a^{j-i} & \text{index laws} \\ \Rightarrow & a^0 & = & a^{j-i} & \\ \Rightarrow & e & = & a^{j-i} & \text{as } a^0 = e. \end{array}$$

Note $j - i \in \mathbb{N}$ and so $o(a) \leq j - i < \infty$. □

If $o(a) = 4$, then $aa^3 = e = a^3a = a^2a^2$ so a, a^3 are mutually inverse, and a^2 is self-inverse. Then

$$\begin{gathered} a^5 = aa^4 = ae = a, \\ a^6 = aa^5 = aa = a^2, \\ a^7 = aa^6 = aa^2 = a^3, \\ a^8 = aa^7 = aa^3 = a^4 = e, \end{gathered}$$

etc. and in the other direction,

$$a^{-1} = a^3, a^{-2} = (a^2)^{-1} = a^2, a^{-3} = (a^3)^{-1} = a, a^{-4} = e$$

etc. so we can rewrite the first line to the second:

$$\begin{array}{ccccccccccccccc} \ldots & a^{-4} & a^{-3} & a^{-2} & a^{-1} & a^0 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 & \ldots \\ \ldots & e & a & a^2 & a^3 & e & a & a^2 & a^3 & e & a & a^2 & a^3 & e & \ldots \end{array}$$

Lemma 2.6. The Remainder Lemma *Let G be a group and $a \in G$ with $o(a) = n < \infty$.*
Let $z, z' \in \mathbb{Z}$ with $z = nq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$.
Then:

(1) $a^z = a^r$;
(2) *if $0 \leq s < t < n$, then*
$$a^s \neq a^t;$$
(3) $a^z = e$ *if and only if* $n \mid z$;
(4) $a^z = a^{z'}$ *if and only if* $z \equiv z' \pmod{n}$.

Proof. (1) We have

$$a^z = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

(2) Now with $0 \leq s < t < n$ notice that $0 < t - s < n$, so

$$a^s = a^t \Rightarrow a^{t-s} = e,$$

contradicting $o(a) = n$.

(3) We have

$$a^z = e \Leftrightarrow a^r = e \Leftrightarrow r = 0 \Leftrightarrow n \mid z.$$

since $a^i \neq e$ for any i with $0 < i < n$, and $0 \leq r < n$.

(4) We have

$$a^z = a^{z'} \Leftrightarrow a^{z-z'} = e \Leftrightarrow n \mid (z - z') \Leftrightarrow z \equiv z' \pmod{n},$$

using (3).

□

Consequently If $o(a) = n < \infty$, then

$$\boldsymbol{e, a, a^2, \ldots, a^{n-1}}$$

is a **complete** list of **distinct** powers of a.

Example 2.7. Let $o(a) = 3$. Then the only remainders are $0, 1, 2$ so

$$\{a^z : z \in \mathbb{Z}\} = \{e, a, a^2\}.$$

Also, $a^{22} = a^1 = a$ as $22 = 3 \times 7 + 1$ and $a^{-7} = a^2$ as $-7 = 3 \times (-3) + 2$.

2.3. **Subgroups.** *A subgroup, defined below, captures the notion of one group being contained in another, with respect to the same binary operation.*

Definition 2.8. Let G be a group and $H \subseteq G$. Then H is a *subgroup of* G (written $H \leq G$) if:

(1) $e \in H$;
(2) $a, b \in H \Rightarrow ab \in H$;
(3) $a \in H \Rightarrow a^{-1} \in H$.

Notice that as $(ab)c = a(bc)$ for all $a, b, c \in G$, certainly $(ab)c = a(bc)$ for all $a, b, c \in H$. So if $H \leq G$ then H is a group *under the same operation as in* G. The converse is also true (see the Exercises), that is, for $H \subset G$ we have $H \leq G$ if and only if $(H, \circ)$ is a group, where $\circ$ is the restriction of the binary operation of G to $H \times H$.

Example 2.9. (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
$\mathbb{Q}^* \leq \mathbb{R}^*$, etc.
BUT $(\mathbb{R}^*, \times)$ is NOT a subgroup of $(\mathbb{R}, +)$.

(2) For $n \in \mathbb{N}$ let

$$n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$$

(*so that* $2\mathbb{Z}$ *is the set of even numbers*).
Then $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

(3) Let $\mathrm{SL}(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$. Then $\mathrm{SL}(n, \mathbb{R}) \leq \mathrm{GL}(n, \mathbb{R})$.

Proof. As $\det A \neq 0$ for all $A \in \mathrm{SL}(n, \mathbb{R})$ we have $\mathrm{SL}(n, \mathbb{R}) \subseteq \mathrm{GL}(n, \mathbb{R})$.
If $A, B \in \mathrm{SL}(n, \mathbb{R})$, then

$$\det AB = (\det A)(\det B) = 1 \cdot 1 = 1,$$

so that $AB \in \mathrm{SL}(n, \mathbb{R})$. We know $\det I_n = 1$ so $I_n \in \mathrm{SL}(n, \mathbb{R})$. Finally, if $A \in \mathrm{SL}(n, \mathbb{R})$ then

$$\det A^{-1} = \frac{1}{\det A} = \frac{1}{1} = 1,$$

so that $A^{-1} \in \mathrm{SL}(n, \mathbb{R})$. Hence $\mathrm{SL}(n, \mathbb{R}) \leq \mathrm{GL}(n, \mathbb{R})$. □

$\boxed{\mathrm{SL}(n,\mathbb{R}) \text{ is a } \textbf{special linear group}.}$

Similarly to the case of general linear groups, we can vary the field and obtain other special linear groups.

(4) Note that for any group G,

$$\{e\} \leq G \text{ and } G \leq G.$$

2.4. **Cyclic groups.** Let G be a group and let $a \in G$. We define

$$\langle a \rangle = \{a^z : z \in \mathbb{Z}\}.$$

In + notation,

$$\langle a \rangle = \{za : z \in \mathbb{Z}\}.$$

If $o(a) = \infty$, then if $a^i = a^j$ where $i < j$ then $a^{j-i} = e$, a contradiction. So

$$\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$$

are all distinct and $|\langle a \rangle| = \infty$. If $o(a) = n \in \mathbb{N}$ then from the Remainder Lemma, $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $e, a, a^2, \ldots, a^{n-1}$ are all distinct so $|\langle a \rangle| = n$.

Lemma 2.10. *For any $a \in G$ we have $\langle a \rangle$ is a commutative subgroup of G and $|\langle a \rangle| = o(a)$.*

Proof. We have $e = a^0 \in \langle a \rangle$. If $a^h, a^k \in \langle a \rangle$, then $a^h a^k = a^{h+k} \in \langle a \rangle$ and $(a^h)^{-1} = a^{-h} \in \langle a \rangle$, so that $\langle a \rangle \leq G$. Note, $a^h a^k = a^{h+k} = a^{k+h} = a^k a^h$ so that $\langle a \rangle$ is commutative.

The final part has been shown above. □

Remark If $o(a) = n$ then $a^{-1} = a^{n-1}, a^{-2} = a^{n-2}$, etc. If n is even, then $(a^{n/2})^{-1} = a^{n/2}$.

Definition 2.11. (i) For $a \in G$, we say $\langle a \rangle$ *is the cyclic subgroup generated by a.*

(ii) A group G is *cyclic* if $G = \langle a \rangle$ for some $a \in G$. In this case we say that *a generates G.*

$\boxed{\text{Note that cyclic groups are commutative.}}$

Proposition 2.12. *Let G be a group with finite order n. Then G is cyclic if and only if it contains an element a with $o(a) = n$. Any such a generates G.*

Proof. For any $a \in G$ we have $\langle a \rangle \leq G$ and

$$G = \langle a \rangle \Leftrightarrow |G| = |\langle a \rangle| \Leftrightarrow n = |\langle a \rangle| \Leftrightarrow n = o(a),$$

using Lemma 2.10. □

Example 2.13. (1) $\mathbb{Z}$ is cyclic as

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle.$$

(2) $\mathbb{Q}$ is not cyclic. For, if $\mathbb{Q} = \langle a \rangle$, then clearly $a \neq 0$ and

$$\mathbb{Q} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}$$

But then $\frac{a}{2} \in \mathbb{Q}$ but $\frac{a}{2} \notin \langle a \rangle$.

(3) In $\mathbb{Z}_n$ we have $o([1]) = n$ as

$$\underbrace{[1] \oplus \cdots \oplus [1]}_{u} = [u].$$

So $\mathbb{Z}_n$ is cyclic.

(4) In K (Klein 4-group) we have $o(e) = 1$ and $o(a) = o(b) = o(c) = 2$, so that K is not cyclic.

Theorem 2.14. (1) *Let $G = \langle a \rangle$ be cyclic of order $n = uv$. Then G has a subgroup of order v.*

(2) *Any subgroup of a cyclic group is cyclic.*

Proof. (1) As $o(a) = n = uv$, $o(a^u) = v$ (see Exercises).
So

$$\langle a^u \rangle = \{e, a^u, a^{2u}, \ldots, a^{u(v-1)}\}$$

is a subgroup of order v.

(2) Let $H \leq G$ where $G = \langle a \rangle$ is cyclic.
Either $H = \{e\} = \langle e \rangle$ or $\exists a^i \in H$ with $i \neq 0$.
Since also $a^{-i} = (a^i)^{-1} \in H$, we have $a^i, a^{-i} \in H$. So we can find a least $n \in \mathbb{N}$ with $a^n \in H$.
Let $a^j \in H$. Then by the Division Algorithm,

$$j = nq + r$$

where $q, r \in \mathbb{Z}$ and $0 \leq r < n$.
Now

$$a^r = a^{j-nq} = a^j (a^n)^{-q} \in H,$$

so that to avoid contradiction, $r = 0$.
We deduce that $n \mid j$. Consequently,

$$H = \langle a^n \rangle$$

and so is cyclic.

□

Example 2.15.

(1) In $\mathbb{Q}^*$ we have

$$\langle 2 \rangle = \{2^z : z \in \mathbb{Z}\} = \{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, \ldots\}.$$

In $\mathbb{Z}$ we have

$$\langle 2 \rangle = \{z2 : z \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

In $\mathbb{Z}_6$ we have

$$\langle 2 \rangle = \{0, 2, 4\}.$$

Since $|\mathbb{Z}_6| < \infty$ we know in advance that $o(2) < \infty$ by Lemma 2.5.

(2) In $(\mathbb{Z}_7^*, \otimes)$ the element 3 has order 6 as

$$3 \neq 1, 3^2 = 2 \neq 1, 3^3 = 6 \neq 1, 3^4 = 4 \neq 1, 3^5 = 5 \neq 1, 3^6 = 15 = 1.$$

So $\mathbb{Z}_7^*$ has subgroups of orders $1, 2, 3$ and 6.

$$\begin{array}{l} \{1\} = \langle 3^6 \rangle \text{ has order } 1 \\ \mathbb{Z}_7^* = \langle 3^1 \rangle \text{ has order } 6 \\ \langle 3^2 \rangle \text{ has order } 3, \langle 3^2 \rangle = \langle 2 \rangle = \{1, 2, 4\} \\ \langle 3^3 \rangle \text{ has order } 2, \langle 3^3 \rangle = \langle 6 \rangle = \{1, 6\} \end{array} .$$

3. Symmetric groups

In Calculus and Analysis, you study analytical *properties of functions from* $\mathbb{R} \to \mathbb{R}$*, such as continuity and differentiability, often referring to the graph* $G(f)$ *of a function* f *where*

$$G(f) = \{(x, f(x)) : x \in \mathbb{R}\}.$$

We are not concerned with such properties here. Rather, we will be forming groups from invertible functions, and looking at their algebraic *properties.*

3.1. **Symmetric groups.** Let X be a non-empty set. Often, X will be finite; we put $[n] := \{1, 2, \ldots, n\}$ and write I_n for $I_{[n]}$.

Definition 3.1. We denote by $\mathcal{S}_X$ the set of all bijections from X to X. If $X = [n]$ we write $\mathcal{S}_n$ for $\mathcal{S}_{[n]}$.

We have everything in place to prove the following - we make use of facts about bijections from **WYNTKBYS**.

Proposition 3.2. *The pair* $(\mathcal{S}_X, \circ)$ *is a group, the* symmetric group on X*.*

Proof. Let $\alpha, \beta \in \mathcal{S}_X$. Then $\alpha : X \to X$ and $\beta : X \to X$, so that certainly $\alpha \circ \beta : X \to X$. Also, α, β are bijections, so that as composition of bijections is a bijection, we have that $\alpha \circ \beta$ is a bijection. Thus $\circ$ is a binary operation on $\mathcal{S}_X$.

We know that $\circ$ is associative.

We know that $I_X \in \mathcal{S}_X$ and for all $\alpha \in \mathcal{S}_X$ we have

$$\alpha \circ I_X = \alpha = I_X \circ \alpha.$$

Finally, if $\alpha \in \mathcal{S}_X$, then the inverse function $\alpha^{-1} : X \to X$ exists. By definition,

$$\alpha \circ \alpha^{-1} = I_X = \alpha^{-1} \circ \alpha,$$

which shows at one and the same time that $\alpha^{-1} \in \mathcal{S}_X$ (as it has inverse function α!) and α, α^{-1} are mutually inverse in $\mathcal{S}_X$.

Thus $(\mathcal{S}_X, \circ)$ is a group. □

Note: we often drop mention of $\circ$.

Example 3.3. (1) $n = 1$; $\mathcal{S}_1 = \{I_1\}$, the table is

$\circ$	I_1
I_1	I_1

This is a trivial *group, i.e. a group with one element.*

(2) $n = 2$; $\mathcal{S}_2 = \{I_2, \alpha\}$, where

$$\alpha(1) = 2 \text{ and } \alpha(2) = 1.$$

The table is

$\circ$	I_2	α
I_2	I_2	α
α	α	I_2

(3) $n = 3$; we have $I_3, \rho \in \mathcal{S}_3$ where

$$\rho(1) = 2, \rho(2) = 3, \rho(3) = 1.$$

Clearly there are more elements - we need some 'sensible' notation.

Two-row notation We can write $\alpha \in \mathcal{S}_n$ as

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

e.g. in (3) above,

$$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Let $\beta \in \mathcal{S}_4$ be given by

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

This means

$$\beta(1) = 2, \beta(2) = 3, \beta(3) = 4 \text{ and } \beta(4) = 1.$$

With

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

we practise composition:

$$(\beta\gamma)(1) = \beta(\gamma(1)) = \beta(2) = 3, (\beta\gamma)(2) = \beta(\gamma(2)) = \beta(1) = 2,$$
$$(\beta\gamma)(3) = \beta(\gamma(3)) = \beta(4) = 1, (\beta\gamma)(4) = \beta(\gamma(4)) = \beta(3) = 4,$$

so that

$$\beta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Working out $\gamma\beta$, we have

$$\gamma\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \neq \beta\gamma.$$

Remark 3.4. In two-row notation for $\alpha \in \mathcal{S}_n$, each element of $[n] = \{1, 2, \ldots, n\}$ occurs exactly once on the second row as we have

$$\alpha = \begin{pmatrix} 1 & \ldots & x & \ldots & y & \ldots & n \\ \alpha(1) & \ldots & \alpha(x) & \ldots & \alpha(y) & \ldots & \alpha(n) \end{pmatrix}.$$

Then if $\alpha(x) = \alpha(y)$ we have

$$\alpha(x) = \alpha(y) \Rightarrow x = y$$

since α is one-one.

As α is onto, for any $z \in \{1, 2, \ldots, n\}$ we have $z = \alpha(t)$ for some $t \in \{1, 2, \ldots, n\}$ so that z appears on the second row

$$\alpha = \begin{pmatrix} 1 & \ldots & t & \ldots & n \\ \ldots & \ldots & z & \ldots & \ldots \end{pmatrix}.$$

Thus the second row is a *permutation* (re-arrangement) of $\{1, 2, \ldots, n\}$. As there are $n!$ permutations of $\{1, 2, \ldots, n\}$, we deduce

$$\boxed{|\mathcal{S}_n| = \text{ order of } \mathcal{S}_n = n!}$$

We look at our examples of small n again:

$$|\mathcal{S}_1| = 1! = 1, \ |\mathcal{S}_2| = 2! = 2, \ |\mathcal{S}_3| = 3! = 6.$$

The 6 elements of $\mathcal{S}_3$ are:

$$I_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Multiplication table for $\mathcal{S}_3$:

$\circ$	I_3	ρ	ρ^2	σ_1	σ_2	σ_3
I_3	I_3	ρ	ρ^2	σ_1	σ_2	σ_3
ρ	ρ	ρ^2	I_3	σ_3	σ_1	σ_2
ρ^2	ρ^2	I_3	ρ	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	I_3	ρ	ρ^2
σ_2	σ_2	σ_3	σ_1	ρ^2	I_3	ρ
σ_3	σ_3	σ_1	σ_2	ρ	ρ^2	I_3

You will be expected to know the labels for the elements of $\mathcal{S}_3$.

As for example $\rho\sigma_1 \neq \sigma_1\rho$, we see that $\mathcal{S}_3$ is **not** commutative.

3.2. **Cycle notation.** Some elements of $\mathcal{S}_n$ can be written as cycles.

For example, with $\rho \in \mathcal{S}_3$ we write

$$\rho = (1\,2\,3)$$

to mean

$$\rho(1) = 2, \rho(2) = 3 \text{ and } \rho(3) = 1.$$

We would get the same function ρ by writing $(2\,3\,1)$ or $(3\,1\,2)$.

Definition 3.5. A *cycle* in $\mathcal{S}_n$ (of length $m \geq 2$)

$$\alpha = (a_1\, a_2\, \ldots a_m)$$

where $a_1, a_2, \ldots, a_m \in \{1, \ldots, n\}$ and $a_i \neq a_j$ for $i \neq j$, is the bijection defined by

$$\alpha(a_1) = a_2, \alpha(a_2) = a_3, \ldots, \alpha(a_{m-1}) = a_m, \alpha(a_m) = a_1$$

and

$$\alpha(x) = x \ \ \forall x \in \{1, 2, \ldots, n\} \setminus \{a_1, \ldots, a_m\}.$$

Note that $m \leq n$.

We can write

$$a_1 \mapsto a_2 \mapsto \ldots \mapsto a_{m-1} \mapsto a_m \mapsto a_1.$$

Cycles cycle from left to right; they can have any starting point.

Example 3.6. In $\mathcal{S}_3$ we have

$$\rho = (1\,2\,3), \rho^2 = (1\,3\,2), \sigma_1 = (2\,3), \sigma_2 = (1\,3) \text{ and } \sigma_3 = (1\,2).$$

Note that $\mathcal{S}_3$ is very unusual in that every non-identity element is a cycle.

Example 3.7. Consider

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \in \mathcal{S}_5.$$

Notice β is not a cycle but

$$\beta = (1\,2)(3\,4\,5).$$

In the above we are composing two separate functions, $(1\,2)$ and $(3\,4\,5)$. We will see that this behaviour is typical.

Mixing notation,

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

So we have $\sigma(1) = 2$ and we could write

$$(1\,2)(1) = 2 \text{ or } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}(1) = 2,$$

but we tend to avoid these as they look a bit ugly!

Notice

(1) In cycle notation, the domain is understood (i.e. we assume we know what it is).
(2)

$$(a_1\, a_2 \ldots a_{m-1}\, a_m) = (a_2\, a_3 \ldots a_m\, a_1) = \ldots = (a_m\, a_1 \ldots a_{m-2}\, a_{m-1}),$$

so *cycle notation is not (quite) unique.*
(3) In $\mathcal{S}_5$ we have

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

which is **not** a cycle.

Compose cycles from **right to left** *they are functions*; cycles 'cycle' from **left to right**. I didn't make the rules!!

Inverse of a cycle The inverse of the cycle

$$a_1 \mapsto a_2 \mapsto \ldots \mapsto a_{m-1} \mapsto a_m \mapsto a_1$$

is the cycle

$$a_m \mapsto a_{m-1} \mapsto \ldots \mapsto a_2 \mapsto a_1 \mapsto a_m,$$

i.e.

$$(a_1\, a_2\, \ldots\, a_m)^{-1} = (a_m\, a_{m-1}\, \ldots\, a_1).$$

Lemma 3.8. *The* order *of a cycle of length m is m.*

Proof. Let $\alpha = (a_1\, a_2 \ldots a_m) \in \mathcal{S}_n$. Then

$$\alpha(a_1) = a_2,$$

$$\alpha^2(a_1) = \alpha(\alpha(a_1)) = \alpha(a_2) = a_3,$$

$$\vdots$$

$$\alpha^{m-1}(a_1) = a_m,$$

$$\alpha^m(a_1) = \alpha(a_m) = a_1.$$

Similarly, $\alpha^m(a_i) = a_i$ for all $1 \le i \le m$ and also $\alpha^m(x) = x$ for all $x \notin \{a_1, \ldots, a_m\}$. Thus

$$\alpha^m = I_n \text{ and } \alpha^i \neq I_n \text{ for all } 1 \le i < m,$$

so that $o(\alpha) = m$. □

Back to $\mathcal{S}_3$ The 6 elements of $\mathcal{S}_3$ are:

$$I_3 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \qquad \rho = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1\,2\,3) \qquad \rho^2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1\,3\,2)$$
$$\sigma_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2\,3) \qquad \sigma_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1\,3) \qquad \sigma_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1\,2)$$

and

$$o(I_3) = 1, o(\rho) = o(\rho^2) = 3, o(\sigma_1) = o(\sigma_2) = o(\sigma_3) = 2.$$

Notice $|\mathcal{S}_3| = 3! = 6$ and $1, 2, 3$ are all divisors of 6.

We know $\mathcal{S}_3$ is not commutative, e.g.

$$\rho\sigma_1 = (1\,2\,3)(2\,3) = (1\,2) = \sigma_3 \neq \sigma_2 = \sigma_1\rho,$$

so cycles do not in general commute. But, for example in $\mathcal{S}_5$,

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

and also

$$(1\,2)(3\,4) = (3\,4)(1\,2).$$

Definition 3.9. Two cycles are *disjoint* if they have no elements in common.

So, ρ and σ_1 are not disjoint.
$(1\,2\,4)$ and $(3\,5)$ are disjoint and
$(1\,2)$ and $(3\,4)$ are disjoint.

Proposition 3.10. *Disjoint cycles commute, i.e. if $\alpha, \beta \in \mathcal{S}_n$ are disjoint cycles, then*

$$\alpha\beta = \beta\alpha.$$

Proof. Write

$$\alpha = (a_1\, a_2 \ldots a_r), \beta = (b_1\, b_2\, \ldots b_m).$$

For any x where

$$x \notin \{a_1, \ldots a_r\} \cup \{b_1, \ldots, b_m\}$$

we have $\alpha(x) = \beta(x) = x$. Thus in this case,

$$(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$$

and similarly,

$$(\beta\alpha)(x) = x$$

so that

$$(\alpha\beta)(x) = (\beta\alpha)(x).$$

For a_i, we have that $a_i \notin \{b_1, \ldots, b_m\}$, as we are given that α and β are disjoint. Thus $\beta(a_i) = a_i$ and

$$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1},$$

with the convention that $a_{r+1} = a_1$. On the other hand $a_{i+1} \notin \{b_1, \ldots, b_m\}$ so that $\beta(a_{i+1}) = a_{i+1}$. Thus

$$(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}.$$

We have shown that

$$(\alpha\beta)(a_i) = (\beta\alpha)(a_i).$$

Similarly,

$$(\alpha\beta)(b_j) = (\beta\alpha)(b_j).$$

We have now shown that for *any* $x \in \{1, \ldots, n\}$ we have

$$(\alpha\beta)(x) = (\beta\alpha)(x).$$

This means that

$$\alpha\beta = \beta\alpha.$$

□

Proposition 3.11. *Let $\alpha \in \mathcal{S}_n$. Then*

$$\alpha = \gamma_1\gamma_2 \ldots \gamma_k$$

where $\gamma_1, \ldots, \gamma_k$ are disjoint *cycles. This expression is unique except for the order in which the cycles are written. We interpret the empty product as I_n.*

Proof. See Appendix □

Definition 3.12. The decomposition

$$\alpha = \gamma_1\gamma_2 \ldots \gamma_k$$

is called the *cycle decomposition* of α.

Example 3.13. Write the following in cycle decomposition.

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

Solution 3.13

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

Recall Disjoint cycles commute (Proposition 3.10), i.e. if γ, δ are disjoint cycles, then

$$\gamma\delta = \delta\gamma.$$

It follows that for any $z \in \mathbb{Z}$ we have

$$(\gamma\delta)^z = \gamma^z\delta^z$$

(see Exercises).

We use the above to consider the order of elements in $\mathcal{S}_n$:

Example 3.14. Let $\alpha = (1\,2\,3)(4\,5) \in \mathcal{S}_5$. Recall $o(1\,2\,3) = 3$, $o(4\,5) = 2$ and $(1\,2\,3)^2 = (1\,3\,2)$. So:

$$\begin{array}{rcll} \alpha & \neq & I_5 & \\ \alpha^2 & = & \big((1\,2\,3)(4\,5)\big)^2 & = (1\,2\,3)^2(4\,5)^2 = (1\,3\,2) \neq I_5 \\ \alpha^3 & = & \big((1\,2\,3)(4\,5)\big)^3 & = (1\,2\,3)^3(4\,5)^3 = (4\,5) \neq I_5 \\ \alpha^4 & = & \big((1\,2\,3)(4\,5)\big)^4 & = (1\,2\,3)^4(4\,5)^4 = (1\,2\,3) \neq I_5 \\ \alpha^5 & = & \big((1\,2\,3)(4\,5)\big)^5 & = (1\,2\,3)^5(4\,5)^5 = (1\,3\,2)(4\,5) \neq I_5 \\ \alpha^6 & = & \big((1\,2\,3)(4\,5)\big)^6 & = (1\,2\,3)^6(4\,5)^6 = I_5 \end{array}$$

so that $o(\alpha) = 6 = l.c.m.\{3, 2\}$.

In the above, *l.c.m.* is *least common multiple, i.e. the smallest multiple of 3 and 2, or equivalently the smallest natural number divisible by both 3 and 2.*

This leads us to:

Proposition 3.15. *Let $\alpha \in \mathcal{S}_n, \alpha \neq I_n$. Write*

$$\alpha = \gamma_1\gamma_2 \dots \gamma_m$$

where $\gamma_1, \dots, \gamma_m$ are disjoint cycles. Suppose the length of γ_i is ℓ_i for $1 \leq i \leq m$. Then

$$o(\alpha) = lcm\{\ell_1, \ell_2, \dots, \ell_m\}.$$

Proof. See Appendix. □

Example 3.16. (1) Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 1 & 6 & 5 & 2 \end{pmatrix} \in \mathcal{S}_7$. Then

$$\alpha = (1\,7\,2\,4)(5\,6)$$

so

$$o(\alpha) = lcm\{4, 2\} = 4.$$

(2) Let $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 1 & 4 & 5 & 3 & 10 & 6 & 9 & 8 & 11 & 7 \end{pmatrix} \in \mathcal{S}_{11}$. Then

$$\beta = (1\,2)(3\,4\,5)(6\,10\,11\,7)(8\,9)$$

and

$$o(\beta) = lcm\{2, 3, 4, 2\} = 12.$$

Warning Powers of cycles do not have to be cycles!! e.g.

$$(1\,2\,3\,4)^2 = (1\,3)(2\,4).$$

3.3. **Transpositions.**

Definition 3.17. A *transposition* is a cycle of length 2.

Note that if α is a transposition, then $o(\alpha) = 2$ (it is a 2-cycle!) so $\alpha = \alpha^{-1}$ (i.e. it is self-inverse). This is easily seen directly as if $\alpha = (u\, v)$, then

$$\alpha^2 = (u\, v)(u\, v) = I_n.$$

Question What are the elements of $\mathcal{S}_n$ of order 2? (See Exercises!).

Let $(1\,2\,3\,4) \in \mathcal{S}_4$. Then

$$(1\,2\,3\,4) = (4\,1)(3\,1)(2\,1)$$

and for any $(a_1\, a_2\, \ldots a_m) \in \mathcal{S}_n$ we have

$$(a_1\, a_2\, \ldots a_m) = (a_m\, a_1)(a_{m-1}\, a_1) \ldots (a_3\, a_1)(a_2\, a_1).$$

Why is this true? Well, work out where each side sends a_1, a_2 in turn. Clearly each side fixes any number that is not equal to any of the a_i's.

Careful A cycle of even/odd length is a product of an odd/even number of transpositions.

Proposition 3.18. *If $\alpha \in \mathcal{S}_n$, then α is a product of transpositions.*

Proof. We regard I_n as the product of 0 transpositions.
(If $n \geq 2$ then also $I_n = (1\,2)(1\,2)$).
Let $\alpha \neq I_n$. Then $\alpha = \gamma_1\gamma_2 \ldots \gamma_k$ for some (disjoint) cycles γ_i, $1 \leq i \leq k$. Replace each γ_i with a product of transpositions, as above. □

Example 3.19. With

$$\beta = (1\,2)(3\,4\,5)(6\,10\,11\,7)(8\,9)$$

we have

$$\beta = (1\,2)(5\,3)(4\,3)(7\,6)(11\,6)(10\,6)(8\,9).$$

These transpositions are **not** disjoint!
Also,

$$\beta = (3\,2)(1\,3)(5\,2)(4\,2)(3\,2)(7\,6)(11\,6)(10\,6)(8\,9),$$

so the expression of β as a product of transpositions is *not* unique.

Theorem 3.20. The Parity Theorem *Let $\alpha \in \mathcal{S}_n$. Then the number of transpositions whose product equals α is either always even or always odd.*

Proof. See Appendix □

Definition 3.21. Let $\alpha \in \mathcal{S}_n$. Then α is *even/odd* if α is a product of an even/odd number of transpositions.

The *sign* of α, denoted by $\mathrm{sg}(\alpha)$, is defined as follows:

$$\mathrm{sg}(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd.} \end{cases}$$

Note that I_n is always even. *By the Parity Theorem, any $\alpha \in \mathcal{S}_n$ is even or odd but* **not** *both.*

Example $\mathcal{S}_3$:

Evens: $I_3, \rho = (1\,2\,3) = (1\,3)(1\,2), \rho^2 = (1\,3\,2) = (1\,2)(1\,3)$.

Odds: $\sigma_1 = (2\,3), \sigma_2 = (1\,3)$ and $\sigma_3 = (1\,2)$.

Consider $\alpha, \beta \in \mathcal{S}_n$. Write

$$\alpha = \mu_1\mu_2 \dots \mu_r,\ \beta = \nu_1\nu_2 \dots \nu_s,$$

for some transpositions μ_i, ν_j, $1 \le i \le r, 1 \le j \le s$. So,

$$\alpha\beta = \mu_1\mu_2 \dots \mu_r\nu_1\nu_2 \dots \nu_s$$

is a product of $r + s$ transpositions. Hence

α	β	$\alpha\beta$
even	even	even
even	odd	odd
odd	even	odd
odd	odd	even

$\mathrm{sg}\,\alpha$	$\mathrm{sg}\,\beta$	$\mathrm{sg}(\alpha\beta)$
1	1	1
1	-1	-1
-1	1	-1
-1	-1	1

Definition 3.22. Let $n \in \mathbb{N}$. We define

$$\mathcal{A}_n = \{\alpha \in \mathcal{S}_n : \alpha \text{ is even}\}.$$

Proposition 3.23. *We have $\mathcal{A}_n \le \mathcal{S}_n$.*

Proof. We know I_n is even. Let $\alpha, \beta \in \mathcal{A}_n$. Then α, β are even and from the table, $\alpha\beta$ is even. Further, with

$$\alpha = \mu_1\mu_2 \dots \mu_r$$

where μ_i are transpositions, we have

$$\alpha^{-1} = (\mu_1\mu_2 \dots \mu_r)^{-1} = \mu_r^{-1}\mu_{r-1}^{-1} \dots \mu_1^{-1} = \mu_r\mu_{r-1} \dots \mu_1,$$

so that α^{-1} is even, i.e. $\alpha^{-1} \in \mathcal{A}_n$. Hence $\mathcal{A}_n \le \mathcal{S}_n$.

$\boxed{\mathcal{A}_n \text{ is the } \textbf{alternating group} \text{ on } n \text{ elements.}}$

Note we have $\mathcal{A}_3 = \{I_3, \rho, \rho^2\}$ so that

$$|\mathcal{A}_3| = 3 = \frac{6}{2} = \frac{|\mathcal{S}_3|}{2}.$$

□

We will now recap Cosets, and Lagrange's theorem. This will confirm that for $n > 1$ we always have $|\mathcal{A}_n| = \frac{|\mathcal{S}_n|}{2}$.

4. Cosets and Lagrange's Theorem

We are going to prove:

Lagrange's Theorem Let G be a finite group and let $H \leq G$. Then the order of H divides the order of G. *We will also say what $|G|/|H|$ is! See later for the full statement of the theorem.*

We will then find a number of applications.

Strategy: *We partition G into disjoint blocks, all the same size, one of which is H. These blocks will be 'cosets'. In fact, we need cosets for other constructions, so we first define and study them.*

Definition 4.1. Let G be a group, let $H \leq G$ and let $a \in G$. Then the *left coset* (with coset leader a) is

$$aH = \{ah : h \in H\}.$$

Notice that $eH = \{eh : h \in H\} = \{h : h \in H\} = H$ so H **is a left coset**.

Example 4.2. (1) Group $\mathcal{S}_3$, subgroup $H = \{I_3, \sigma_2\}$.

$$\begin{array}{rclcll} I_3H & = & \{I_3I_3, I_3\sigma_2\} & = & \{I_3, \sigma_2\} & = H \\ \rho H & = & \{\rho I_3, \rho\sigma_2\} & = & \{\rho, \sigma_1\} & \\ \rho^2 H & = & \{\rho^2 I_3, \rho^2\sigma_2\} & = & \{\rho^2, \sigma_3\} & \\ \sigma_1 H & = & \{\sigma_1 I_3, \sigma_1\sigma_2\} & = & \{\sigma_1, \rho\} & = \rho H \\ \sigma_2 H & = & \{\sigma_2 I_3, \sigma_2\sigma_2\} & = & \{\sigma_2, I_3\} & = I_3H = H \\ \sigma_3 H & = & \{\sigma_3 I_3, \sigma_3\sigma_2\} & = & \{\sigma_3, \rho^2\} & = \rho^2 H \end{array}$$

Notice:

(a) Coset leaders are **not** unique:

$$I_3H = \sigma_2H = H, \sigma_1H = \rho H, \sigma_3H = \rho^2 H.$$

(b) Distinct cosets are disjoint.

(c) Cosets have the same size: $|\mu H| = 2 = |H|$ for all $\mu \in \mathcal{S}_3$.

(d) $\mathcal{S}_3 = H \cup \rho H \cup \rho^2 H$.

(2) Group $(\mathbb{R}^*, \times)$, subgroup $(\mathbb{R}^+, \times)$.

$$r\mathbb{R}^+ = \{rs : s \in \mathbb{R}^+\} = \{rs : s > 0\} = \begin{cases} \mathbb{R}^+ & \text{if} \quad r > 0 \\ \mathbb{R}^- & \text{if} \quad r < 0 \end{cases}$$

where $\mathbb{R}^- = \{r \in \mathbb{R} : r < 0\}$.

Let $r > 0$. Then $rs > 0$ for all $s > 0$; if $h > 0$ then $h = r\frac{h}{r} \in r\mathbb{R}^+$, so $r\mathbb{R}^+ = \mathbb{R}^+$. Similarly for $r < 0$.

Notice:

(a) Coset leaders are **not** unique:

$$1\mathbb{R}^+ = 2\mathbb{R}^+, \text{ etc.}$$

(b) Distinct cosets are disjoint: $\mathbb{R}^+ \cap \mathbb{R}^- = \emptyset$;

(c) Cosets have the same size: $\exists$ bijection $\mathbb{R}^+ \to \mathbb{R}^-, x \mapsto -x$;

(d) $\mathbb{R}^* = \mathbb{R}^+ \cup \mathbb{R}^-$.

Lemma 4.3. The Coset Lemma *Let $H \leq G$ where G is a group. Define the relation $\sim_H$ on G by the rule:*

$$a \sim_H b \Leftrightarrow b^{-1}a \in H.$$

Then $\sim_H$ is an equivalence relation on G and

$$[a] = aH.$$

Proof. Let $a \in G$. Then $a^{-1}a = e \in H$, so $a \sim_H a$ and $\sim_H$ is reflexive.

Suppose that $a, b \in G$ and $a \sim_H b$. Then $b^{-1}a \in H$, so that as H is closed under taking inverses, $a^{-1}b = (b^{-1}a)^{-1} \in H$ and $b \sim_H a$, so that $\sim_H$ is symmetric.

Finally, suppose that $a, b, c \in G$ and $a \sim_H b \sim_H c$. then $b^{-1}a, c^{-1}b \in H$ and as H is closed under product, $c^{-1}a = (c^{-1}b)(b^{-1}a) \in H$. So $a \sim_H c$ and $\sim_H$ is transitive.

Thus $\sim_H$ is an equivalence relation on G. We have

$$\begin{aligned} [a] &= \{b \in G : b \sim_H a\} \\ &= \{b \in G : a^{-1}b \in H\} \\ &= \{b \in G : a^{-1}b = h \in H\} \\ &= \{b \in G : b = ah, h \in H\} \\ &= aH. \end{aligned}$$

□

Since equivalence relation partition the set in question, and since (for any equivalence) we have

$$a \sim b \Leftrightarrow [a] = [b] \Leftrightarrow b \in [a],$$

we can easily get the following:

Corollary 4.4. *Let $H \leq G$ where G is a group and let $a, b, c \in G$. Then*

(1) $a \in aH$;
(2) $c \in aH \Leftrightarrow cH = aH$;
(3) $aH = bH$ *or* $aH \cap bH = \emptyset$;
(4) $aH = bH \Leftrightarrow b^{-1}a \in H$;
(5) $aH = H \Leftrightarrow a \in H$;

Proof. (1) $a \in [a] = aH$.

(2) $c \in aH = [a]$ if and only if $cH = [c] = [a] = aH$.

(3) Equivalence classes form a partition.
(4) Definition of $\sim_H$ and note above.
(5) $aH = H = eH$ if and only if $e^{-1}a = a \in H$.

□

The equivalence relation $\sim_H$ is very special, in that all its classes have the same size:

Lemma 4.5. *Let $H \leq G$ where G is a group. Then for any $a, b \in G$, $|aH| = |bH| = |H|$.*

Proof. Define $\lambda_b : H \to bH$ by

$$\lambda_b(h) = bh.$$

Clearly λ_b is onto since

$$bH = \{bh : h \in H\} = \{\lambda_b(h) : h \in H\}.$$

Also, λ_b is one-one as for any $h, k \in H$ we have:

$$\lambda_b(h) = \lambda_b(k) \Rightarrow bh = bk \Rightarrow h = k.$$

Hence λ_b is a bijection.

Hence for any $a, b \in G$ we have $|bH| = |H| = |aH|$. □

Definition 4.6. If $H \leq G$ then we write $[G : H]$ for the number of left cosets of H in G; $[G : H]$ is the *index* of H in G.

We are now in a position to prove:

Theorem 4.7. Lagrange's Theorem *Let G be a finite group and let $H \leq G$. Then the order of H divides the order of G. Moreover,*

$$\frac{|G|}{|H|} = [G : H].$$

Proof. Let $k = [G : H]$ and let $a_1H = H, a_2H, \ldots, a_kH$ be the distinct left cosets of H in G. By Lemma 4.5,

$$|a_iH| = |H|, 1 \leq i \leq k,$$

and

$$a_iH \cap a_jH = \emptyset, 1 \leq i < j \leq k.$$

For any $g \in G$ we have $g \in gH$. Hence

$$G = H \dot{\cup} a_2H \dot{\cup} \ldots \dot{\cup} a_kH$$

and then

$$|G| = |H| + |a_2H| + \ldots |a_kH| = |H| + |H| + \ldots |H| = k|H|.$$

Hence $|H|$ divides $|G|$ and $|G|/|H| = [G : H]$. □

The above counting argument does not work for infinite sets.

Note *What is special about* left *cosets? Nothing - we could equally well use right cosets.* Let $H \leq G$ and let $a \in G$. Then the *right coset* (with coset leader a) is

$$Ha = \{ha : h \in H\}.$$

The dual argument leads us to Lagrange's Theorem. Consequently: if G is a finite group and $H \leq G$ then the number of left cosets of H in G is equal to the number of right cosets of H in G.

But be careful: with $G = \mathcal{S}_3$ and $H = \{I_3, \sigma_2\}$ we have

$$H\rho = \{I_3\rho, \sigma_2\rho\} = \{\rho, \sigma_3\} \neq \{\rho, \sigma_1\} = \rho H.$$

In fact, for any *G, there is a bijection between the set of left cosets and the set of right cosets. This does not mean that right and left cosets are the same!! See Exercises.*

4.1. **Applications of Lagrange's Theorem.** Recall that for $a \in G$ where G is a group:

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is the *cyclic subgroup generated by a*. If $o(a) = n < \infty$, then

$$n = |\langle a \rangle| \text{ and } \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Corollary 4.8. Order Corollary *Let G be a finite group and let $a \in G$. Then the order of a divides the order of G (i.e. $o(a) \,|\, |G|$.) Hence $a^{|G|} = e$.*

Proof. We have $|\langle a \rangle|$ divides $|G|$ by Lagrange, and from Lemma 2.10 we have $o(a) = |\langle a \rangle|$, so the first part follows. The second follows from the Remainder Lemma. □

Corollary 4.9. *Let G be a group of prime order. Then G is cyclic and generated by any of its non-identity elements.*

Proof. Let $|G| = p$ and let $a \in G$ with $a \neq e$. Since $o(a) \,|\, |G| = p$ we have $o(a) = p$ as p is prime and so

$$|\langle a \rangle| = p = |G|.$$

Hence $\langle a \rangle = G$. □

Corollary 4.10. *Let $n \geq 2$. Then $|\mathcal{A}_n| = \frac{n!}{2}$.*

Proof. Recall that $\mathcal{A}_n = \{\alpha \in \mathcal{S}_n : \alpha \text{ is even}\}$. Let $\mathcal{O}_n = \{\alpha \in \mathcal{S}_n : \alpha \text{ is odd}\} = \mathcal{S}_n \setminus \mathcal{A}_n$. So, $\mathcal{S}_n = \mathcal{A}_n \dot{\cup} \mathcal{O}_n$.

We claim that $\mathcal{O}_n = (1\,2)\mathcal{A}_n$.

We have

$$(1\,2)\mathcal{A}_n = \{(1\,2)\alpha : \alpha \in \mathcal{A}_n\} \subseteq \mathcal{O}_n$$

and

$$\mathcal{O}_n = \{(1\,2)\big((1\,2)\beta\big) : \beta \in \mathcal{O}_n\} \subseteq \mathcal{A}_n,$$

so that

$$(1\,2)\mathcal{A}_n = \mathcal{O}_n,$$

as required.

By Lemma 4.5,

$$|\mathcal{A}_n| = |(1\,2)\mathcal{A}_n| = |\mathcal{O}_n|,$$

so that

$$|\mathcal{S}_n| = 2|\mathcal{A}_n|,$$

giving $|\mathcal{A}_n| = \frac{n!}{2}$. □

Hence $|\mathcal{A}_3| = \frac{3!}{2} = 3, |\mathcal{A}_4| = \frac{4!}{2} = 12, |\mathcal{A}_5| = \frac{5!}{2} = 60$, etc.

Theorem 4.11. Fermat's Little Theorem *Let p be prime and let $a \in \mathbb{Z}$. Then $a \equiv a^p$ (mod p).*

Proof. If $a \equiv 0$, the result is clear.

Otherwise, $[a] \in \mathbb{Z}_p^*$. Now $|\mathbb{Z}_p^*| = p - 1$ so by the Order Corollary, $[a]^{p-1} = [1]$ in $\mathbb{Z}_p^*$. Thus $a^{p-1} \equiv 1$ and so multiplying by a we get $a^p \equiv a$. □

Warning *Let $|G| = n$ and suppose $m \,|\, n$. Then it is not always true that G has a subgroup of order m! For some well behaved groups such a subgroup is guaranteed...but not for all.*

5. Normal subgroups and conjugacy

5.1. Conjugacy.

Definition 5.1.

- Let G be a group and let $a, g \in G$. We say that
$$gag^{-1}$$
is a *conjugate* of a.
- We define a relation $\sim$ on G by $a \sim b$ if b is a conjugate of a, that is, if $b = gag^{-1}$ for some $g \in G$.

This is a familiar notion from matrix algebra where one considers matrices PAP^{-1}.

Note that $g^{-1}ag$ is also a conjugate of a (as $(g^{-1})^{-1} = g$).

Lemma 5.2. *Let G be a group. The relation $\sim$ is an equivalence relation on G.*

Proof. Let $a, b, c \in G$.

- We have $a = eae^{-1}$, so $a \sim a$ and $\sim$ is reflexive.
- Suppose that $a \sim b$ and $b = gag^{-1}$. Then $a = g^{-1}bg$, so that $b \sim a$ and $\sim$ is symmetric.
- Suppose that $a \sim b$, $b \sim c$ and $b = gag^{-1}$ and $c = hbh^{-1}$. Then $c = hbh^{-1} = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}$. Thus $a \sim c$ and $\sim$ is transitive.

□

Definition 5.3. The equivalence classes of $\sim$ are called the *conjugacy classes* of G.

The conjugacy classes are

$$[a] = \{gag^{-1} : g \in G\}$$

and they partition G.

Example 5.4. (1) Suppose that G is commutative, and $a \sim b$. Then $b = gag^{-1}$ for some $g \in G$ and so $b = a$ (as G is commutative). Thus $\sim$ is just equality.

(2) Let $A, P \in \mathrm{GL}(n, \mathbb{R})$. Then

$$\det(PAP^{-1}) = \det P \det A \det P^{-1} = \det(A).$$

This means that if $A \in \mathrm{SL}(n, \mathbb{R})$ and $A \sim B$ (in $\mathrm{GL}(n, \mathbb{R})$), then $B \in \mathrm{SL}(n, \mathbb{R})$.

(3) Working in $\mathcal{S}_6$ with $\beta = (1\,2)(3\,5\,4)$ we have $\beta^{-1} = (1\,2)(3\,4\,5)$ and

$$\beta(1\,2\,5)\beta^{-1} = (1\,2)(3\,5\,4)(1\,2\,5)(1\,2)(3\,4\,5) = (2\,1\,4) = (\beta(1)\,\beta(2)\,\beta(5)).$$

(4) Let $\alpha = (a_1 \ \dots \ a_k) \in \mathcal{S}_n$. Let $\gamma \in \mathcal{S}_n$. We claim that

$$\gamma\alpha\gamma^{-1} = (\gamma(a_1) \ \dots \ \gamma(a_k)).$$

To see this, we need to show that for any $1 \leq x \leq n$

$$\gamma\alpha\gamma^{-1}(x) = (\gamma(a_1) \ \dots \ \gamma(a_k))(x).$$

There are two cases for x. If $x \notin \{\gamma(a_1), \cdots, \gamma(a_k)\}$, that is, $\gamma^{-1}(x) \notin \{a_1, \dots, a_k\}$, then

$$\gamma\alpha\gamma^{-1}(x) = \gamma\alpha(\gamma^{-1}(x)) = \gamma\gamma^{-1}(x) = x = (\gamma(a_1) \ \dots \ \gamma(a_k))(x).$$

Otherwise, $x = \gamma(a_i)$ for some $1 \leq i \leq k$ and

$$\gamma\alpha\gamma^{-1}(x) = \gamma\alpha\gamma^{-1}\gamma(a_i) = \gamma\alpha(a_i) = \gamma(a_{i+1}),$$

with the convention that $k + 1 \equiv 1$, and

$$(\gamma(a_1) \ \dots \ \gamma(a_k))(x) = (\gamma(a_1) \ \dots \ \gamma(a_n))(\gamma(a_i)) = \gamma(a_{i+1}).$$

Thus $\gamma\alpha\gamma^{-1} = (\gamma(a_1) \ \dots \ \gamma(a_k))$ as claimed.

Definition 5.5. Let $\alpha \in \mathcal{S}_n$, $\alpha \neq I_n$. The *cycle type* of α is $[\ell_1, \dots, \ell_m]$ where we have $\ell_1 \geq \ell_2 \geq \dots \geq \ell_m$ and

$$\alpha = \gamma_1 \dots \gamma_m$$

is the cycle decomposition of α into disjoint cycles γ_i where the length of γ_i is ℓ_i.

E.g. the cycle type of $\alpha = (23)(146)$ is $[3, 2]$ and the cycle type of

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 2 & 5 & 1 & 7 & 9 & 8 & 6 \end{pmatrix}$$

is $[3, 3, 2]$, as

$$\beta = (145)(679)(23).$$

Theorem 5.6. *Let $\alpha, \beta \in \mathcal{S}_n$. Then $\alpha \sim \beta$ if and only if α and β have the same cycle type.*

Proof. Sketch of one direction
Write

$$\alpha = \gamma_1 \dots \gamma_m$$

where the length of γ_i is ℓ_i.

If $\alpha \sim \beta$, then for some $\delta \in \mathcal{S}_n$ we have

$$\begin{aligned} \beta &= \delta\alpha\delta^{-1} \\ &= \delta\gamma_1 \dots \gamma_m\delta^{-1} \\ &= \delta\gamma_1(\delta^{-1}\delta)\gamma_2(\delta^{-1}\delta)\dots(\delta^{-1}\delta)\gamma_m\delta^{-1} \\ &= (\delta\gamma_1\delta^{-1})(\delta\gamma_2\delta^{-1})\dots(\delta\gamma_m\delta^{-1}) \end{aligned} .$$

We know from Example 5.4 that $\delta\gamma_i\delta^{-1}$ is a cycle of the same length as γ_i, i.e. ℓ_i. Moreover, it is easy to check that the cycles $\delta\gamma_i\delta^{-1}$ for $1 \leq i \leq m$ are disjoint.

Hence $\beta = \delta\alpha\delta^{-1}$ has the same cycle type as α.

The full proof may be found in the Appendix □

Example 5.7. Let $\mathcal{K} = \{I_4, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Then $K \leq \mathcal{A}_4$ as every element of K is self-inverse and

$$(a\,b)(c\,d)(a\,c)(b\,d) = (a\,d)(b\,c).$$

Note that $\mathcal{K}$ is 'the same' as K. We also say $\mathcal{K}$ is the Klein 4-group. Further, for any $\gamma \in \mathcal{S}_4$ and $(a\,b)(c\,d) \in \mathcal{K}$ we have

$$\gamma(a\,b)(c\,d)\gamma^{-1} = \gamma(a\,b)\gamma^{-1}\gamma(c\,d)\gamma^{-1} = (\gamma(a)\,\gamma(b))(\gamma(c)\,\gamma(d)) \in \mathcal{K}.$$

Theorem 5.8. *The alternating group $\mathcal{A}_4$ has no order 6 subgroup.*

Proof. Recall that

$$\mathcal{A}_n = \{\alpha \in \mathcal{S}_n : \alpha \text{ is even}\}$$

and

$$|\mathcal{A}_n| = \frac{|\mathcal{S}_n|}{2} = \frac{n!}{2}.$$

Hence

$$|\mathcal{A}_4| = \frac{4!}{2} = 12.$$

The cycle types of non-identity elements of $\mathcal{S}_4$ are

$$[2],\ [2,2],[3] \text{ and } [4].$$

Elements of cycle type $[2],[4]$ are not in $\mathcal{A}_4$ as clearly $(a\,b) \notin \mathcal{A}_4$ and

$$(a\,b\,c\,d) = (a\,d)(a\,c)(a\,b) \notin \mathcal{A}_4.$$

On the other hand, elements of cycle type $[2,2]$ and $[3]$ are in $\mathcal{A}_4$ as

$$(a\,b)(c\,d) \in \mathcal{A}_4$$

and

$$(a\,b\,c) = (a\,c)(a\,b) \in \mathcal{A}_4.$$

So the elements of $\mathcal{A}_4$ are I_4,

$$(1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)$$

which are all self inverse, and

$$(1\,2\,3), (1\,3\,2); (1\,2\,4), (1\,4\,2); (1\,3\,4), (1\,4\,3); (2\,3\,4), (2\,4\,3).$$

Suppose that $\mathcal{A}_4$ has subgroup H of order 6.

- If $(a\,b\,c) \in H \leq \mathcal{A}_4$ then $(a\,b\,c)^{-1} = (a\,c\,b) \in H$.
- If H contains two elements from

$$(1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)$$

then it contains all three. Then

$$\{I_4, (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\} \leq H,$$

contradicting Lagrange's Theorem.

- If $(1\,2)(3\,4) \in H$ and $\alpha = (a\,b\,c) \in H$ then

$$\alpha(1\,2)(3\,4)\alpha^{-1} = \alpha(1\,2)\alpha^{-1}\alpha(3\,4)\alpha^{-1} = (\alpha(1)\,\alpha(2))(\alpha(3)\,\alpha(4)) \in H.$$

Thus (as $(1\,2)(3\,4)$ is the only $[2,2]$ element of H)

$$(1\,2)(3\,4) = (\alpha(1)\,\alpha(2))(\alpha(3)\,\alpha(4)).$$

As α is a 3-cycle this is impossible.

- Hence H consists entirely of 3-cycles. But these come in pairs, and $I_4 \in H$ also, which is impossible as H has even order.

So no such H exists. □

5.2. **Normal subgroups.**

Definition 5.9. Let G be a group and $H \leq G$. Then H is a *normal* subgroup of G, denoted by $H \trianglelefteq G$, if for all $g \in G$ and $h \in H$ we have

$$ghg^{-1} \in H.$$

There are other equivalent ways to define normal subgroups. One is to say, a subgroup H is normal if H is a union of conjugacy classes.

Example 5.10.

(1) Let $H \leq G$ where G is commutative. Then for any $g \in G, h \in H$ we have

$$ghg^{-1} = hgg^{-1} = he = h \in H,$$

so *every subgroup of a commutative group is normal.*

(2) We always have $\{e\} \trianglelefteq G$, $G \trianglelefteq G$, as $geg^{-1} = e$.

(3) For $\alpha \in \mathcal{S}_n$ and $\beta \in \mathcal{A}_n$ we have

$$\operatorname{sg}(\alpha\beta\alpha^{-1}) = \operatorname{sg}(\alpha)\operatorname{sg}(\beta)\operatorname{sg}(\alpha^{-1}) = \operatorname{sg}(\alpha)\operatorname{sg}(\beta)\operatorname{sg}(\alpha)^{-1} = \operatorname{sg}(\alpha)\operatorname{sg}(\alpha)^{-1} = 1,$$

so that $\alpha\beta\alpha^{-1} \in \mathcal{A}_n$ and $A_n \trianglelefteq \mathcal{S}_n$.

(4) $\rho\sigma_2\rho^{-1} = \rho\sigma_2\rho^2 = \sigma_3 \notin H = \{I_3, \sigma_2\}$, so H is *not* normal in $\mathcal{S}_3$.

(5) We know that $\mathrm{SL}(2,\mathbb{R}) \leq \mathrm{GL}(n,\mathbb{R})$. If $A \in \mathrm{SL}(2,\mathbb{R})$ and $P \in \mathrm{GL}(n,\mathbb{R})$, then we have seen that $\det(PAP^{-1}) = \det A = 1$, so that $PAP^{-1} \in \mathrm{SL}(2,\mathbb{R})$. Thus $\mathrm{SL}(2,\mathbb{R}) \trianglelefteq \mathrm{GL}(n,\mathbb{R})$.

Definition 5.11. We say that a group G is *simple* if it has no normal subgroups other than $\{e\}$ and G (that is, it has no non-trivial proper normal subgroups).

Proposition 5.12. *The group $\mathcal{A}_4$ is not simple.*

Proof. We have shown that $\mathcal{K} \trianglelefteq \mathcal{A}_4$. □

In fact, for any $n \geq 5$, we have that $\mathcal{A}_n$ is simple. The proof involves an analysis of the 3-cycles, and the fact any normal subgroup of $\mathcal{A}_n$ is closed under conjugation. See Frahleigh: A first course in abstract algebra.

6. Isomorphisms and Homomorphisms

6.1. **When are two groups 'the same' or 'alike'?** *Preliminary question: How do we determine when two sets have the same number of elements? What do we mean by this?*

Let A and B be sets. Recall that a *bijection* $\alpha : A \to B$ is a one-one, onto function.

A bijection $\alpha : A \to B$ 'pairs off' the elements of A with those of B

$$a \longleftrightarrow \alpha(a).$$

Fact There is a bijection between two finite sets if and only if they have the same number of elements.

We therefore *declare* that sets A and B (finite or infinite) 'have the same number of elements' or 'have the same **cardinality**' if and only if there is a bijection between them.

What can we say, then, about groups of the same (small) order?

Consider $\{0\} \leq \mathbb{Z}$ and $\{I_3\} \leq \mathcal{S}_3$ and $\{I_n\} \leq \mathrm{GL}(n,\mathbb{R})$. They are each groups with one element and with table

$+$	0
0	0

$\circ$	I_3
I_3	I_3

$\times$	I_n
I_n	I_n

These are 'the same' except we have varied the symbol

$$0 \leftrightarrow I_3 \leftrightarrow I_n.$$

We have $T = \{1,-1\}$ and $\langle\sigma_1\rangle = \{I_3, \sigma_1\}$ and they have tables:

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

and

$\circ$	I_3	σ_1
I_3	I_3	σ_1
σ_1	σ_1	I_3

These are 'the same' except we have varied the symbols

$$1 \leftrightarrow I_3,\ -1 \leftrightarrow \sigma_1.$$

Third,

$$K = \{e, a, b, c\} \text{ and } \mathcal{K} = \{I_4, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\},$$

and havetables

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

and

$\circ$	I_4	$(1\,2)(3\,4)$	$(1\,3)(2\,4)$	$(1\,4)(2\,3)$
I_4	I_4	$(1\,2)(3\,4)$	$(1\,3)(2\,4)$	$(1\,4)(2\,3)$
$(1\,2)(3\,4)$	$(1\,2)(3\,4)$	I_4	$(1\,4)(2\,3)$	$(1\,3)(2\,4)$
$(1\,3)(2\,4)$	$(1\,3)(2\,4)$	$(1\,4)(2\,3)$	I_4	$(1\,2)(3\,4)$
$(1\,4)(2\,3)$	$(1\,4)(2\,3)$	$(1\,3)(2\,4)$	$(1\,2)(3\,4)$	I_4

On the other hand,

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

and has table

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We can see that the tables for K and $\mathcal{K}$ are 'the same' and that for $\mathbb{Z}_5^*$ is 'different' - e.g. on the leading diagonal.

We now formalise these intuitive notions of being 'the same' and 'different' for groups.

6.2. **Homomorphisms.**

Definition 6.1. Let $(G, \circ)$ and $(H, *)$ be groups and let $\theta : G \to H$ be a map.

(1) The map θ is a (group) *homomorphism* if

$$\theta(a \circ b) = \theta(a) * \theta(b)$$

for all $a, b \in G$.

(2) The map θ is a (group) *isomorphism* if θ is a homomorphism and θ is a bijection.

Example 6.2. (1) Let $G = \{e\}$ and $H = \{f\}$ be trivial groups. Then $\theta : G \to H$ where $\theta(e) = f$ is a homomorphism, since the only products in G and H are $ee = e$ and $ff = f$, respectively, so

$$\theta(ee) = \theta(e) = f = ff = \theta(e)\theta(e).$$

Since θ is clearly a bijection, θ is an isomorphism.

(2) $\alpha : T = \{1, -1\} \to \{I_3, \sigma_1\} = \langle \sigma_1 \rangle \leq \mathcal{S}_3$ where $\alpha(1) = I_3$, $\alpha(-1) = \sigma_1$ is an isomorphism.

Proof. Clearly α is a bijection. We have

$$\alpha(1\,1) = \alpha(1) = I_3 = I_3 I_3 = \alpha(1)\alpha(1);$$

$$\alpha(1\,(-1)) = \alpha(-1) = \sigma_1 = I_3\sigma_1 = \alpha(1)\alpha(-1);$$

similarly, $\alpha((-1)1) = \alpha(-1)\alpha(1)$ and finally,

$$\alpha((-1)(-1)) = \alpha(1) = I_3 = \sigma_1\sigma_1 = \alpha(-1)\alpha(-1).$$

□

Clearly, we do not want a case-by-case analysis, so prefer homomorphisms given by 'rules', e.g.

(3) $\theta : \mathbb{R} \to \mathbb{R}^*$ given by $\theta(x) = e^x$ is a homomorphism, since for all $a, b \in \mathbb{R}$,

$$\theta(a+b) = e^{a+b} = e^a e^b = \theta(a)\theta(b).$$

Since $\operatorname{Im}\theta = \mathbb{R}^+$, clearly θ is not onto and hence not an isomorphism.

(4) $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$ is a homomorphism but not an isomorphism if $n \geq 2$.

Proof. For any $A, B \in \mathrm{GL}(n, \mathbb{R})$ we have

$$\det(AB) = \det(A)\ \det(B).$$

det is not an isomorphism for $n \geq 2$ as

$$\det \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 2 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & & & \vdots & 0 \\ 0 & & & 0 & 1 \end{pmatrix} = 2 = \det \begin{pmatrix} 2 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & & & \vdots & 0 \\ 0 & & & 0 & 1 \end{pmatrix}$$

□

(5) $\theta : K \to T = \{1, -1\}$ given by

$$\theta(e) = \theta(a) = 1,\ \theta(b) = \theta(c) = -1$$

is a homomorphism *exercise* but not an isomorphism.

We next show that taking homomorphisms commutes with taking powers.

Lemma 6.3. *Let $\theta : G \to H$ be a homomorphism. Then for all $g \in G, z \in \mathbb{Z}$:*
(i) $\theta(e_G) = e_H$;
(ii) $\theta(g^{-1}) = \theta(g)^{-1}$;
(iii) $\theta(g^z) = \theta(g)^z$.

Proof. (i) $\theta(e_G) = \theta(e_G\, e_G) = \theta(e_G)\theta(e_G)$, so cancelling in H gives $\theta(e_G) = e_H$.
(ii) $e_H = \theta(e_G) = \theta(gg^{-1}) = \theta(g)\theta(g^{-1}) = \ldots = \theta(g^{-1})\theta(g)$, so $\theta(g)^{-1} = \theta(g^{-1})$.
(iii) $\theta(g^0) = \theta(e_G) = e_H = \theta(g)^0$.
For $n \in \mathbb{N}$,

$$\theta(g^n) = \theta(gg^{n-1}) = \theta(g)\theta(g^{n-1}) = \ldots = \underbrace{\theta(g)\ldots\theta(g)}_{n \text{ times}} = \theta(g)^n,$$

$$\theta(g^{-n}) = \theta((g^{-1})^n) = (\theta(g^{-1}))^n = ((\theta(g))^{-1})^n = \theta(g)^{-n}.$$

□

For two groups to be 'the same' we would want them to have the same number of elements, that is, there is a bijection between them, and we would want the products in the tables to correspond, and this is exactly what a homomorphism gives us. This leads us to:

6.3. **Isomorphic groups.**

Definition 6.4. A group G is *isomorphic* to a group H if there is an isomorphism $\theta : G \to H$. We denote this by $G \cong H$.

Note that in the above, we are not saying that θ is unique.

Lemma 6.5. *If G, H and K are groups, then:*

(1) *$I_G : G \to G$ is an isomorphism;*
(2) *if $\theta : G \to H$ is an isomorphism, then the inverse map $\theta^{-1} : H \to G$ is also an isomorphism;*
(3) *if $\theta : G \to H, \psi : H \to K$ are isomorphisms, then $\psi\theta : G \to K$ is an isomorphism.*

Proof. (1) Clearly, I_G is a bijection, and for all $x, y \in G$,

$$I_G(xy) = xy = I_G(x)I_G(y).$$

Thus I_G is an isomorphism and so $G \cong G$.

(2) Since θ and θ^{-1} are mutually inverse, certainly $\theta^{-1} : H \to G$ is a bijection.
Let $h, k \in H$. Since θ is onto, there exist $h', k' \in G$ such that $\theta(h') = h$ and $\theta(k') = k$. Then

$$\theta(h'k') = \theta(h')\theta(k') = hk$$

so that

$$\theta^{-1}(h)\theta^{-1}(k) = h'k' = \theta^{-1}(hk),$$

giving $\theta^{-1} : H \to G$ is an isomorphism.

(3) Since composition of bijections is a bijection, $\psi\theta : G \to K$ is a bijection. Further, for any $g, h \in G$ we have

$$(\psi\theta)(gh) = \psi(\theta(gh)) = \psi(\theta(g)\theta(h))$$

as θ is a homomorphism, and then as ψ is a homomorphism

$$\psi(\theta(g)\theta(h)) = \psi(\theta(g))\psi(\theta(h)) = (\psi\theta)(g)\psi\theta(h).$$

□

Corollary 6.6. *The relation $\cong$ is an equivalence relation on the class of all groups.*

Proof. Let G, H, K be groups. By (1) of Lemma 6.5, $I_G : G \to G$ is an isomorphism, so that $G \cong G$ and $\cong$ is reflexive.

If $G \cong H$ there exists an isomorphism $\theta : G \to H$. But by (2) of Lemma 6.5, $\theta^{-1} : H \to G$ is also an isomorphism, so that $H \cong G$ and $\cong$ is symmetric.

Finally if $G \cong H$ and $H \cong G$ there exists isomorphisms $\theta : G \to H$ and $\psi : H \to K$. By (3) of Lemma 6.5, $\psi\theta : G \to K$ is an isomorphism, so that $G \cong K$ and $\cong$ is transitive.

Hence $\cong$ is an equivalence. □

6.4. **Properties shared by isomorphic groups.** *We think of isomorphic groups as being the same. But, how justified is that? Isomorphisms preserve the size (cardinality) of the group, and the multiplication table. So, any property that can be written down referring only to those terms must be preserved. We give some examples here.*

Let $G \cong H$ and let $\alpha : G \to H$ be an isomorphism.

(1) The order of G equals the order of H.

Proof. This is true since α is a bijection. □

(2) G is commutative if and only if H is commutative.

Proof. Suppose G is commutative. Let $a, b \in H$. Since α is onto, there exists $a', b' \in G$ such that $\alpha(a') = a, \alpha(b') = b$. Then

$$ab = \alpha(a')\alpha(b') = \alpha(a'b') = \alpha(b'a') = \alpha(b')\alpha(a') = ba,$$

using the fact G is commutative.

For the converse, use the fact $\alpha^{-1} : H \to G$ is an isomorphism. □

(3) Let $a \in G$. Then $o(a) = o(\alpha(a))$.

Proof. We have

$$a^n = e_G \Leftrightarrow \alpha(a^n) = \alpha(e_G) \Leftrightarrow \alpha(a)^n = e_H.$$

□

Consequently, G has an element of order u if and only if H does.

(4) G is cyclic if and only if H is cyclic.

Proof. We have

$$G = \langle a \rangle = \{a^z : z \in \mathbb{Z}\}.$$

Then

$$H = \operatorname{Im}\alpha = \{\alpha(a^z) : z \in \mathbb{Z}\} =$$
$$\{(\alpha(a))^z : z \in \mathbb{Z}\} = \{b^z : z \in \mathbb{Z}\} = \langle b \rangle$$

where $b = \alpha(a)$. Thus H is cyclic.

For the converse, use the fact $\alpha^{-1} : H \to G$ is an isomorphism.

□

6.5. **Showing groups are/are not isomorphic.** We have two kinds of problems:

To show $G \cong H$ ***we must*** **find** ***an isomorphism between them.***

Example 6.7. (1) $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ are isomorphic, since $\theta : \mathbb{R} \to \mathbb{R}^+$ given by $\theta(a) = e^a$ is an isomorphism.

Proof. We have shown it is a homomorphism, and it has inverse ln. □

(2) Let $G = \langle a \rangle$ and $H = \langle b \rangle$ be cyclic groups of order n. Then $G \cong H$.

Proof. We have

$$o(a) = |G| = n = |H| = o(b).$$

Define $\alpha : G \to H$ by

$$\alpha(a^i) = b^i.$$

Then

$$\begin{array}{rcl} a^i = a^j & \Leftrightarrow & n \,|(j-i) \\ & \Leftrightarrow & b^i = b^j \\ & \Leftrightarrow & \alpha(a^i) = \alpha(a^j) \end{array}$$

so that α is well defined and one-one. Clearly α is onto and for any a^i, a^k we have

$$\alpha(a^i a^k) = \alpha(a^{i+k}) = b^{i+k} = \alpha(a^i)\alpha(a^k),$$

so that α is an isomorphism and $G \cong H$. □

To show G ***is not isomorphic to*** H ***we must find a property, preserved by isomorphisms, which one group has but the other does not.***

Example 6.8. (1) $\mathbb{R} \ncong \mathcal{S}_n$ as $\mathbb{R}$ is infinite but $\mathcal{S}_n$ is not.
(2) $\mathcal{S}_n \ncong \mathcal{S}_m$ for $n \neq m$ as $|\mathcal{S}_n| = n! \neq m! = |\mathcal{S}_m|$.
(3) $\mathcal{S}_3 \ncong \mathbb{Z}_6$ as $\mathcal{S}_3$ is not commutative, but $\mathbb{Z}_6$ is.
(4) $K \ncong \mathbb{Z}_4$ as K is not cyclic but $\mathbb{Z}_4$ is.
(5) $\mathbb{R}^* \ncong \mathbb{R}^+$ as $\mathbb{R}^*$ has an element of order 2 but $\mathbb{R}^+$ does not.
(6) $\mathbb{R}^+ \ncong \mathbb{Q}^+$ as for all $r \in \mathbb{R}^+$ there exists $\sqrt{r} \in \mathbb{R}^+$ and $(\sqrt{r})^2 = r$, but there is no $q \in \mathbb{Q}^+$ with $q^2 = 2$. *Note: one could also use cardinality arguments here.*

6.6. **Automorphisms and inner automorphisms.**

Definition 6.9. Let G be a group. An *automorphism* of G is an isomorphism $G \to G$. We denote by $\mathrm{Aut}(G)$ the set of automorphisms of G.

Proposition 6.10. *Let* G *be a group. Then* $\mathrm{Aut}(G)$ *forms a group under* $\circ$.

Proof. We show that $\mathrm{Aut}(G) \leq \mathcal{S}_G$.

First, we have that $I_G \in \mathrm{Aut}(G)$.

If $\theta, \psi \in Aut(G)$ then $\theta, \psi : G \to G$ are isomorphisms. It follows from Lemma 6.5 that $\theta^{-1}, \psi\theta : G \to G$ are isomorphisms. So, $\theta^{-1}, \psi\theta \in \mathrm{Aut}(G)$ and $\mathrm{Aut}(G) \leq \mathcal{S}_G$. □

Let G be a group and let $a \in G$. Define $\psi_a : G \to G$ by

$$\psi_a(g) = aga^{-1}.$$

We show that $\psi_a \in \mathrm{Aut}(G)$. Notice that

$$\psi_a(gh) = agha^{-1} = ageha^{-1} = (aga^{-1})(aha^{-1}) = \psi_a(g)\psi_a(h),$$

so that ψ_a is a homomorphism. Further, for any $g, h \in G$ we have

$$\psi_a(g) = \psi_a(h) \Rightarrow aga^{-1} = aha^{-1} \Rightarrow g = h,$$

using cancellation, so that ψ_a is one-one. Finally, for any $g \in G$ we have

$$\psi_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = (aa^{-1})g(aa^{-1}) = ege = g,$$

so that ψ_a is onto. Hence $\psi_a \in \mathrm{Aut}(G)$.

Definition 6.11. The set $\mathrm{Inn}(G) = \{\psi_a : a \in G\}$ is the set of *inner automorphisms* of G.

Notice that if G is commutative, then for any ψ_a we have

$$\psi_a(g) = aga^{-1} = gaa^{-1} = ge = g = I_G(g),$$

so that $\mathrm{Inn}(G) = \{I_G\}$.

Consider $\mathcal{S}_n$ and $\alpha \in \mathcal{S}_n$. By earlier results we have

$$\psi_\alpha(a_1 \ \ldots \ a_n) = \alpha(a_1 \ \ldots \ a_n)\alpha^{-1} = (\alpha(a_1) \ \ldots \ \alpha(a_n))$$

and of course for a cycle decomposition

$$\psi_\alpha(\gamma_1 \ldots \gamma_k) = \psi_\alpha(\gamma_1) \ldots \psi_\alpha(\gamma_k).$$

Thus ψ_α preserves the cycle type.

Proposition 6.12. *Let G be a group. Then* $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Proof. We have $I_G = \psi_e \in \mathrm{Inn}(G)$.

Consider $\psi_a, \psi_b \in \mathrm{Inn}(G)$. Let $g \in G$.

$$\psi_a\psi_b(g) = \psi_a(bgb^{-1}) = a(bgb^{-1})a^{-1} = (ab)g(ab)^{-1} = \psi_{ab}(g).$$

Thus $\psi_a\psi_b = \psi_{ab} \in \mathrm{Inn}(G)$.

Also,

$$\psi_a\psi_{a^{-1}} = \psi_{aa^{-1}} = \psi_e = I_G = \psi_{a^{-1}}\psi_a$$

and so $(\psi_a)^{-1} = \psi_{a^{-1}} \in \mathrm{Inn}(G)$ and $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. □

Fun fact: for $n \neq 2, 6$ we have $\mathcal{S}_n \cong \mathrm{Aut}(\mathcal{S}_n) = \mathrm{Inn}(\mathcal{S}_n)$. One can have groups of automorphisms (suitably defined) of other algebraic structures. The groups of automorphisms of finite dimensional vector spaces are precisely the general linear groups.

6.7. **Properties preserved by homomorphisms.** *We revisit the properties preserved by isomorphisms, and see how they can be adapted to homomorphisms.*

Let G, H be groups and let $\alpha : G \to H$ be an onto homomorphism.

(1) The order of G is equal to or greater than the order of H.

Proof. This is true since $\alpha : G \to H$ is a function. □

(2) G is commutative then H is commutative.

Proof. Suppose G is commutative. Let $a, b \in H$. Since α is onto, there exists $a', b' \in G$ such that $\alpha(a') = a, \alpha(b') = b$. Then

$$ab = \alpha(a')\alpha(b') = \alpha(a'b') = \alpha(b'a') = \alpha(b')\alpha(a') = ba,$$

using the fact G is commutative.

□

(3) Let $a \in G$. If $o(a) = n$ then $o(\alpha(a)) \mid n$.

Proof. We have

$$a^n = e_G \Rightarrow \alpha(a^n) = \alpha(e_G) \Rightarrow \alpha(a)^n = e_H.$$

□

(4) If G is cyclic then H is cyclic.

Proof. We have

$$G = \langle a \rangle = \{a^z : z \in \mathbb{Z}\}.$$

Then

$$H = \operatorname{Im} \alpha = \{\alpha(a^z) : z \in \mathbb{Z}\} =$$
$$\{(\alpha(a))^z : z \in \mathbb{Z}\} = \{b^z : z \in \mathbb{Z}\} = \langle b \rangle$$

where $b = \alpha(a)$. Thus H is cyclic.

□

7. Quotient groups and the Fundamental Theorem of Homomorphisms

7.1. **Kernels and Images.**

Definition 7.1. Let G and H be groups and let $\theta : G \to H$ be a homomorphism. Then the kernel $\operatorname{Ker} \theta$ and the image $\operatorname{Im} \theta$ of θ are defined by:

$$\operatorname{Ker} \theta = \{g \in G : \theta(g) = e_H\},$$

and

$$\operatorname{Im} \theta = \{\theta(g) : g \in G\}.$$

$\operatorname{Im} \theta$ is called a *homomorphic image of* G.

Notice that by definition

$$\operatorname{Ker} \theta \subseteq G \text{ and } \operatorname{Im} \theta \subseteq H.$$

Example 7.2. Let $\theta : \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^*$ be given by $\theta(A) = \det A$. Then θ is a homomorphism with $\operatorname{Ker}\theta = \mathrm{SL}(2,\mathbb{R})$. Further, θ is onto.

Proof. Since $\det(AB) = (\det A)(\det B)$ by the multiplicative property of determinants, θ is a homomorphism.

We have

$$A \in \operatorname{Ker}\theta \Leftrightarrow \theta(A) = 1 \Leftrightarrow \det A = 1 \Leftrightarrow A \in \mathrm{SL}(2,\mathbb{R}),$$

so that $\operatorname{Ker}\theta = \mathrm{SL}(2,\mathbb{R})$.

For any $r \in \mathbb{R}^*$ we have

$$r = \det \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$$

so that θ is onto (i.e. $\operatorname{Im}\theta = \mathbb{R}^*$). □

The idea is that from G and $\theta : G \to H$ we make a new group, which will be isomorphic to $\operatorname{Im}\theta$ (and so to H in the case where θ is onto). First we show that $\operatorname{Ker}\theta$ measures 'how one-one' θ is.

Lemma 7.3. *Let G and H be groups and let $\theta : G \to H$ be a homomorphism. Then*

(1) *$\theta(a) = \theta(b)$ if and only if $a^{-1}b \in \operatorname{Ker}\theta$;*
(2) *θ is one-one if and only if $\operatorname{Ker}\theta = \{e_G\}$.*

Proof. (1) We know from Lemma 6.3 that $\theta(e_G) = e_H$, so $e_G \in \operatorname{Ker}\theta$. We have

$$\begin{array}{rcl} \theta(a) = \theta(b) & \Leftrightarrow & \theta(a^{-1})\theta(a) = \theta(a^{-1})\theta(b) \\ & \Leftrightarrow & \theta(a^{-1}a) = \theta(a^{-1}b) \\ & \Leftrightarrow & \theta(e_G) = \theta(a^{-1}b) \\ & \Leftrightarrow & e_H = \theta(a^{-1}b) \\ & \Leftrightarrow & a^{-1}b \in \operatorname{Ker}\theta. \end{array}$$

(2) We know $e_G \in \operatorname{Ker}\theta$. If θ is one-one, then for any $g \in \operatorname{Ker}\theta$ we have

$$\theta(g) = e_H = \theta(e_G),$$

so that $g = e_G$ and $\operatorname{Ker}\theta = \{e_G\}$.

Conversely, if $\operatorname{Ker}\theta = \{e_G\}$, then for any $a, b \in G$ we have

$$\theta(a) = \theta(b) \Rightarrow a^{-1}b \in \operatorname{Ker}\theta \Rightarrow a^{-1}b = e_G \Rightarrow b = a,$$

so that θ is one-one.

□

Lemma 7.4. *Let G and H be groups and let $\theta : G \to H$ be a homomorphism. Then*

$$\operatorname{Ker}\theta \trianglelefteq G$$

and

$$\operatorname{Im}\theta \leq H.$$

Proof. From Lemma 6.3 we have $\theta(e_G) = e_H$, so that $e_G \in \operatorname{Ker}\theta$ and $e_H \in \operatorname{Im}\theta$.

Ker θ Let $a, b \in \operatorname{Ker}\theta$; then

$$\theta(ab) = \theta(a)\theta(b) = e_H e_H = e_H$$

and

$$\theta(a^{-1}) = (\theta(a))^{-1} = e_H^{-1} = e_H,$$

again by Lemma 6.3. Thus $ab, a^{-1} \in \operatorname{Ker}\theta$ and $\operatorname{Ker}\theta \leq G$.

Let $g \in G, h \in \operatorname{Ker}\theta$. Then

$$\theta(ghg^{-1}) = \theta(g)\theta(h)\theta(g^{-1}) = \theta(g)e_H\theta(g^{-1}) = \theta(g)\theta(g^{-1}) = \theta(gg^{-1}) = \theta(e_G) = e_H,$$

so that $ghg^{-1} \in \operatorname{Ker}\theta$ and $\operatorname{Ker}\theta \trianglelefteq G$.

Im θ For $g, h \in \operatorname{Im}\theta$ we have $a, b \in G$ with $g = \theta(a), h = \theta(b)$. So

$$gh = \theta(a)\theta(b) = \theta(ab) \in \operatorname{Im}\theta$$

and

$$g^{-1} = (\theta(a))^{-1} = \theta(a^{-1}) \in \operatorname{Im}\theta,$$

so that $\operatorname{Im}\theta \leq H$. □

So, all kernels are normal subgroups; we must show the converse.

7.2. **Construction of quotient groups.** Let $N \trianglelefteq G$. We let

$$G/N = \{aN : a \in G\}.$$

Define a product on G/N by

$$(aN)(bN) = abN.$$

Is this well-defined? i.e. is it independent of the choice of coset leader? Yes:

Lemma 7.5. *If $aN = cN$ and $bN = dN$, then $abN = cdN$.*

Proof. We have

$$c^{-1}a \in N \text{ and } d^{-1}b \in N.$$

Now

$$(cd)^{-1}ab = d^{-1}c^{-1}ab = d^{-1}(bb^{-1})c^{-1}ab = (d^{-1}b)\big(b^{-1}(c^{-1}a)b\big) \in N,$$

as $b^{-1}(c^{-1}a)b = b^{-1}(c^{-1}a)(b^{-1})^{-1} \in N$. Hence

$$(ab)N = (cd)N.$$

□

Proposition 7.6. *Let $N \trianglelefteq G$. Then G/N is a group with*

$$I_{G/N} = N \text{ and } (aN)^{-1} = a^{-1}N,$$

for any $a \in G$.

Proof. Let $aN, bN, cN \in G/N$. Then

$$(aNbN)cN = (ab)NcN = ((ab)c)N = (a(bc))N = aNbcN = aN(bNcN),$$

so that multiplication is associative. We have $N = eN \in G/N$ and for any $aN \in G/N$

$$N(aN) = eNaN = eaN = aN = aeN = aNeN = (aN)N.$$

Finally, for $aN \in G/N$ we have $a^{-1}N \in G/N$ and then

$$(aN)(a^{-1}N) = aa^{-1}N = eN = N = eN = a^{-1}N = (a^{-1}N)(aN),$$

so that $(aN)^{-1}$ exists and equals $a^{-1}N$. □

Definition 7.7. The group G/N above is the *quotient* or *factor* group of G by N.

Continuing our running Example 7.2, let $G = \mathrm{GL}(2, \mathbb{R})$ and let $S = \mathrm{SL}(2, \mathbb{R})$. Then $\det : G \to \mathbb{R}^*$ is a homomorphism with kernel S, so that $S \trianglelefteq G$. Further, for any $A, B \in G$ we have (using the rule for two left cosets to be equal, and properties of det)

$$AS = BS \Leftrightarrow B^{-1}A \in S \Leftrightarrow \det B^{-1}A = 1 \Leftrightarrow \det A = \det B.$$

We have that

$$G/S = \{AS : A \in G\}$$

and

$$(AS)(BS) = (AB)S.$$

From the above the left coset AS is completely determined by the real number $\det A$, and similarly for BS and $(AB)S$. So you can see that G/S is isomorphic to $\mathbb{R}^*$.

Proposition 7.8. *Let $N \trianglelefteq G$. Then*

$$\nu_N : G \to G/N$$

given by

$$\nu_N(g) = gN$$

is an onto homomorphism with $\operatorname{Ker} \nu_N = N$.

Proof. For any $g, h \in G$ we have

$$\begin{aligned} \nu_N(gh) &= ghN \\ &= (gN)(hN) \\ &= \nu_N(g)\nu_N(h), \end{aligned}$$

so that ν_N is a homomorphism, which is clearly onto.

Finally,

$$\begin{aligned} n \in \operatorname{Ker} \nu_N &\Leftrightarrow \nu_N(n) = N \\ &\Leftrightarrow nN = N \\ &\Leftrightarrow n \in N, \end{aligned}$$

so that $\operatorname{Ker} \nu_N = N$. □

We have now shown that

$$\{ \text{ kernels of homomorphisms } \} = \{ \text{ normal subgroups } \}$$

and

$$\{ \text{ quotient groups } \} \subseteq \{ \text{ homomorphic images } \}.$$

We now complete the picture:

Theorem 7.9. Fundamental Theorem of Homomorphisms (FTH) for groups *Let G and H be groups and let $\theta : G \to H$ be a homomorphism. Then* $\operatorname{Ker}\theta \trianglelefteq G$, $\operatorname{Im}\theta \leq H$ *and*

$$G/\operatorname{Ker}\theta \cong \operatorname{Im}\theta.$$

Proof. From Lemma 7.4 we have that

$$\operatorname{Ker}\theta \trianglelefteq G \text{ and } \operatorname{Im}\theta \leq H.$$

Let $N = \operatorname{Ker}\theta$. Define $\overline{\theta} : G/N \to \operatorname{Im}\theta$ by

$$\overline{\theta}(aN) = \theta(a).$$

For any $aN, bN \in G/N$ we have

$$\begin{array}{rcll} aN = bN & \Leftrightarrow & b^{-1}a \in N & \text{by Corollary 4.4} \\ & \Leftrightarrow & \theta(b^{-1}a) = e_H & \text{by definition of } \operatorname{Ker}\theta \\ & \Leftrightarrow & \theta(b)^{-1}\theta(a) = e_H & \text{by Lemma 6.3} \\ & \Leftrightarrow & \theta(a) = \theta(b) & \\ & \Leftrightarrow & \overline{\theta}(aN) = \overline{\theta}(bN) & \text{definition of } \overline{\theta}. \end{array}$$

This shows that $\overline{\theta}$ is well-defined and one-one.

For any $\theta(a) \in \operatorname{Im}\theta$ we have $\theta(a) = \overline{\theta}(aN)$, so that $\overline{\theta}$ is onto, hence a bijection.

Finally, for any $aN, bN \in G/N$ we have

$$\begin{array}{rcll} \overline{\theta}(aNbN) & = & \overline{\theta}(abN) & \text{definition of multiplication in } G/N \\ & = & \theta(ab) & \text{definition of } \overline{\theta} \\ & = & \theta(a)\theta(b) & \theta \text{ is a homomorphism} \\ & = & \overline{\theta}(aN)\overline{\theta}(bN) & \text{definition of } \overline{\theta} \end{array},$$

so that $\overline{\theta}$ is an isomorphism as required. □

Continuing Example 7.2, we know that $\theta : \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^*$ given by $\theta(A) = \det A$ is an onto homomorphism with $\operatorname{Ker}\theta = \mathrm{SL}(2,\mathbb{R})$. By Theorem 7.9 we also have

$$\mathrm{GL}(2,\mathbb{R})/\mathrm{SL}(2,\mathbb{R}) \cong \mathbb{R}^*.$$

Putting $G = \mathrm{GL}(2,\mathbb{R})$ and $S = \mathrm{SL}(2,\mathbb{R})$ the group on the left is

$$\{AS : A \in G\}$$

and the isomorphism sends

$$AS \mapsto \det A.$$

7.3. **Exercises and solutions for the FTH.**

Example 7.10. (1) Show that for any $n \geq 2$, $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$ and

$$\mathcal{S}_n/\mathcal{A}_n \cong T$$

where $T = \{1, -1\}$.

In fact we have shown already that $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$, but it will also drop out below.

Proof. Recall the *sign* function, sg. For $\alpha \in \mathcal{S}_n$ we have

$$\operatorname{sg}\alpha = \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd} \end{cases}$$

We drew a table:

$\operatorname{sg}\alpha$	$\operatorname{sg}\beta$	$\operatorname{sg}(\alpha\beta)$
1	1	1
1	-1	-1
-1	1	-1
-1	-1	1

from which it is clear $\operatorname{sg}(\alpha\beta) = \operatorname{sg}(\alpha)\operatorname{sg}(\beta)$ for any $\alpha, \beta \in \mathcal{S}_n$. Thus sg is a homomorphism.

We know that

$$\mathcal{A}_n = \{\alpha : \alpha \text{ is even}\}$$

so that

$$\mathcal{A}_n = \{\alpha : \operatorname{sg}(\alpha) = 1\} = \operatorname{Ker}\operatorname{sg}.$$

From FTH, $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$. Also,

$$1 = \operatorname{sg}(I_n) \text{ and } -1 = \operatorname{sg}((1\,2)),$$

so that $\operatorname{Im}\operatorname{sg} = T$. Again FTH,

$$\mathcal{S}_n/\operatorname{Ker}\operatorname{sg} \cong \operatorname{Im}\operatorname{sg}$$

so that

$$\mathcal{S}_n/\mathcal{A}_n \cong T.$$

□

(2) Show that $\mathrm{SL}(n,\mathbb{R}) \trianglelefteq \mathrm{GL}(n,\mathbb{R})$ and

$$\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \cong \mathbb{R}^*.$$

Proof. We find an onto homomorphism $\theta : \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^*$ with $\operatorname{Ker}\theta = \mathrm{SL}(n,\mathbb{R})$.

Consider the homomorphism $\det : \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^*$. For any $r \in \mathbb{R}^*$ we have

$$r = \det \begin{pmatrix} r & 0 & \dots & & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \vdots & & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

so that det is onto and $\operatorname{Im}\det = \mathbb{R}^*$.

We have

$$A \in \operatorname{Ker}\det \Leftrightarrow \det A = 1 \Leftrightarrow A \in \mathrm{SL}(n,\mathbb{R}),$$

so that $\operatorname{Ker}\det = \mathrm{SL}(n,\mathbb{R})$. By FTH,

$$\mathrm{SL}(n,\mathbb{R}) \trianglelefteq \mathrm{GL}(n,\mathbb{R}) \text{ and } \mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \cong \mathbb{R}^*.$$

□

(3) Show that $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ and

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

Proof. Here $n\mathbb{Z}$ is defined by $n\mathbb{Z} = \{nz : z \in Z\}$.

Note: we have already shown that $n\mathbb{Z} \leq \mathbb{Z}$ and as $\mathbb{Z}$ is commutative, in fact $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. This also drops out of what follows.

Define $\alpha : \mathbb{Z} \to \mathbb{Z}_n$ by

$$\alpha(z) = [z].$$

Then for all $z, w \in \mathbb{Z}$ we have

$$\alpha(z+w) = [z+w] = [z] \oplus [w] = \alpha(z) \oplus \alpha(w),$$

so that α is a homomorphism. For $[z] \in \mathbb{Z}_n$ we have $[z] = \alpha(z)$, so that α is clearly onto. For any $z \in \mathbb{Z}$ we have

$$z \in \operatorname{Ker}\alpha \Leftrightarrow \alpha(z) = [0] \Leftrightarrow [z] = [0] \Leftrightarrow z \in n\mathbb{Z},$$

so that $n\mathbb{Z} = \operatorname{Ker}\alpha$. By FTH, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ and as

$$\mathbb{Z}/\operatorname{Ker}\alpha \cong \operatorname{Im}\alpha$$

we have

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

□

We now consider a further application of FTH, to *direct product groups*. This is a foretaste of the material that is developed in the next section.

For subsets A, B of a group G we define:

$$AB = \{ab : a \in A, b \in B\}.$$

Definition 7.11. Let G be a group, $H \leq G, K \leq G$.

We say that G is the *internal direct product* of H and K if:

(i) $H \trianglelefteq G, K \trianglelefteq G$;

(ii) $H \cap K = \{e\}$;

(iii) $G = HK$.

Proposition 7.12. *Let G be the internal direct product of subgroups H and K.*

(1) *For any $g \in G$, the expression of g as $g = hk$ for $h \in H, k \in K$, is unique.*

(2) *If $h \in H$, $k \in K$, then $hk = kh$.*

(3) *$G \cong H \times K$.*

(4) $G/H \cong K$.

Proof. (1) If $g = hk = ab$ where $h, a \in H$ and $k, b \in K$, then $a^{-1}h = bk^{-1} \in H \cap K = \{e\}$ so that $a^{-1}h = bk^{-1} = e$ and so $h = a, k = b$, as required.

(2) Notice that

$$(hk)(kh)^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{e\}$$

as $H \trianglelefteq G, K \trianglelefteq G$. So $hk = kh$.

(3) Define $\alpha : G \to H \times K$ by $\alpha(hk) = (h, k)$ where $h \in H, k \in K$. Then α is everywhere defined as $G = HK$, well defined by (1) and clearly a bijection. Further, for $h, k \in H$ and $k, b \in K$ we have using (3) that

$$\alpha((hk)(ab)) = \alpha((ha)(kb)) = (ha, kb) = (h, k)(a, b),$$

so that α is an isomorphism.

(4) Define $\theta : G \to K$ by $\theta(hk) = k$ where $h \in H, k \in K$. Then as above, θ is a function and for $hk, ab \in G$ where $h, k \in H$ and $k, b \in K$ we have

$$\theta((hk)(ab)) = \theta(hakb) = kb = \theta(hk)\theta(ab),$$

so that θ is a homomorphism. Clearly, θ is onto. Finally,

$$hk \in \operatorname{Ker}\theta \Leftrightarrow \theta(hk) = e \Leftrightarrow k = e \Leftrightarrow hk \in H,$$

so that $\operatorname{Ker}\theta = H$. By FTH we deduce that $G/H \cong K$.

□

8. Direct and semidirect products

This section is not examinable

8.1. **More on direct products, and a semidirect product.** Let G and H be groups. For clarity we denote the identity of G as e_G and the identity of H as e_H. We let $G \times H$ be the direct product group

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

with binary operation given by

$$(g, h)(g', h') = (gg', hh').$$

We recall from the Exercises that $G \times H$ is a group, with identity (e_G, e_H) and the inverse of (g, h) given by (g^{-1}, h^{-1}).

Lemma 8.1. *The direct product group $G \times H$ is commutative if and only if both G and H are commutative.*

Proof. Suppose that $G \times H$ is commutative. Then $\pi_1 : G \times H \to G$ is a homomorphism. It is onto since for any $g \in G$ we have $\pi_1(g, e_H) = g$. Thus by Subsection 6.7 we have that G is commutative. Dually, using π_2, we obtain H is commutative.

Conversely, if G and H are commutative, then for any $(g, h), (g', h') \in G \times H$ we have

$$(g, h)(g', h') = (gg', hh') = (g'g, h'h) = (g', h')(g, h),$$

so that $G \times H$ is commutative. □

Example 8.2. Let $G' = \{(g, e_H) : g \in G\}$. Use FTH to show that

$$G' \trianglelefteq G \times H$$

and

$$(G \times H)/G' \cong H.$$

Proof. Define $\pi_2 : G \times H \to H$ by $\pi_2\big((g,h)\big) = h$. Then π_2 is an onto homomorphism, as for any $(g,h),(g',h') \in G \times H$ we have

$$\pi_2((g,h)(g',h')) = \pi_2(gg', hh') = hh' = \pi_2(g,h)\pi_1(g',h').$$

Also, for any $h \in H$ we have $\pi_2(e_G, h) = h$, so that π_2 is onto and $H = \operatorname{Im}\pi_2$.
Then

$$(g,h) \in \operatorname{Ker}\pi_2 \Leftrightarrow \pi_2(g,h) = e_H \Leftrightarrow h = e_H \Leftrightarrow (g,h) \in G'.$$

So $\operatorname{Ker}\pi_2 = G'$ and $G' \trianglelefteq G \times H$. Hence by FTH,

$$(G \times H)/\operatorname{Ker}\pi_2 \cong \operatorname{Im}\pi_2,$$

gives

$$(G \times H)/G' \cong H.$$

□

Definition 8.3. Let $n \in \mathbb{N}$ and fix a symbol x. We let C_n be the group defined by

$$C_n = \{e, x, \cdots, x^{n-1}\} = \langle x \rangle$$

wher $o(x) = n$.

Note that by Example 6.7 we have $(C_n, \cdot) \cong (\mathbb{Z}_n, \oplus)$.
We think of C_n as the generic cyclic group of order n.

Example 8.4. The Klein 4-group K is isomorphic to $C_2 \times C_2$.

Proof. Define $\theta : K \to C_2 \times C_2$ by

$$e\theta = (e,e),\ a\theta = (x,e),\ b\theta = (e,x),\ c\theta = (x,x).$$

Clearly θ is a bijection - check it is an isomorphism. □

Example 8.5. Let p, q be distinct primes. Then $C_{pq} \cong C_p \times C_q$.

Proof. Let $C_p = \langle x \rangle$ and $C_q = \langle y \rangle$ where $o(x) = p$ and $o(y) = q$. We see

$$(x,y)^m = (x^m, y^m) = (e,e) \Leftrightarrow x^m = e \text{ and } y^m = e.$$

But this is equivalent to

$$p \mid m \text{ and } q \mid m$$

and so as p, q are primes, to

$$pq \mid m.$$

Thus $o(x,y) = pq$. But $\mid C_p \times C_q \mid = pq$, so we deduce $C_p \times C_q = \langle (x,y) \rangle$ and so is cyclic. Hence $C_p \times C_q \cong C_{pq}$. □

We are going to investigate when groups are isomorphic to direct product groups and more generally to semidirect products.

Example 8.6. Let $G = \mathbb{R}^* \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}, a \neq 0\}$. We define $*$ on G by the rule

$$(a, b) * (c, d) = (ac, bc + d).$$

Then $(G, *)$ is a group with identity $(1, 0)$ and the inverse of (a, b) being $(a^{-1}, -\frac{b}{a})$.

Moreover, G is infinite and is not commutative as

$$(1, 1) * (2, 0) = (2, 2) \neq (2, 1) = (2, 0) * (1, 1).$$

Moreover,

$$(1, 1)^n = (1, n)$$

for all $n \in \mathbb{N}$, so that $o(1, 1) = \infty$. On the other hand $(-1, 1)(-1, 1) = (1, 0)$, so that $o(-1, 1) = 2$.

The group $(G, *)$ is a group, an example of a *semidirect product* group.

8.2. **Internal (semi-)direct products.** Let G be a group and let $A, B \subseteq G$. Then

$$AB = \{ab : a \in A, b \in B\}.$$

For example, a left coset aH is just $\{a\}H$, but we usually drop brackets for singletons.

Lemma 8.7. *Let $H \leq G, K \trianglelefteq G$. Then $HK \leq G$.*

Proof. Recall

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

Then

$$e = ee \in HK$$

as $e \in H$ and $e \in K$.

Suppose $h, h' \in H, k, k' \in K$. Then

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

as $h^{-1} \in H (H \leq G)$ and $hk^{-1}h^{-1} \in K (K \trianglelefteq G)$.

Also

$$(hk)(h'k') = hh'(h'^{-1})kh'k' \in HK$$

as $hh' \in H$ and $(h'^{-1})kh' \in K$, so that $(h'^{-1})kh'k' \in K$. □

By duality, the same lemma holds if $H \trianglelefteq G$ and $K \leq G$.

Definition 8.8. Let G be a group, $H \leq G, K \leq G$.

We say that G is the *internal direct product* of H and K if:
(i) $H \trianglelefteq G, K \trianglelefteq G$;
(ii) $H \cap K = \{e\}$;
(iii) $G = HK$.

We say that G is the *internal semidirect product* of H and K if:
(i) $H \leq G, K \trianglelefteq G$;
(ii) $H \cap K = \{e\}$;

(iii) $G = HK$.

Lemma 8.9. *Let G be the internal semidirect product of H and K. If $g \in G$ then $g = hk$ for* unique *$h \in H, k \in K$.*

Proof. If $g = hk = h'k'$ where $h, h' \in H, k, k' \in K$, then

$$(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\}$$

so $(h')^{-1}h = k'k^{-1} = e$, giving $h' = h$ and $k' = k$. □

Theorem 8.10. *Let G be the* internal semidirect product *of H and K. Then the SET $H \times K$ is a group under*

$$(h, k)(h', k') = (hh', (h')^{-1}kh'k'),$$

denoted $H * K$. Further,

$$\theta : G \to H * K$$

given by $\theta(hk) = (h, k)$ where $h \in H, k \in K$ is an isomorphism.

Proof. Let $(h, k), (h', k'), (h'', k'') \in H \times K$. Then

$$\begin{aligned}
((h,k)(h',k'))(h'',k'') &= (hh', (h')^{-1}kh'k')(h'',k'') \\
&= (hh'h'', (h'')^{-1}((h')^{-1}kh'k')h''k'') \\
&= (hh'h'', (h'')^{-1}((h')^{-1}kh'(h''(h'')^{-1}k')h''k'') \\
&= (hh'h'', (h'h'')^{-1}kh'h''(h'')^{-1}k'h''k'') \\
&= (h,k)(h'h'', (h'')^{-1}k'h''k'') \\
&= (h,k)((h',k')(h'',k'')),
\end{aligned}$$

so the operation is associative.

For any (h, k) we have

$$(e, e)(h, k) = (eh, h^{-1}ehk) = (h, k)$$

and

$$(h, k)(e, e) = (he, e^{-1}kee) = (h, k)$$

so (e, e) is the identity.

Finally,

$$(h, k)(h^{-1}, hk^{-1}h^{-1}) = (hh^{-1}, (h^{-1})^{-1}kh^{-1}hk^{-1}h^{-1}) = (e, e)$$

and check

$$(h^{-1}, hk^{-1}h^{-1})(h, k) = (e, e).$$

So $H * K$ is a group as claimed.

By Lemma 8.9, θ is well defined; if $(h, k) \in H * K$ then

$$(h, k) = \theta(hk),$$

so θ is onto. If $\theta(hk) = \theta(h'k')$, then

$$(h, k) = (h', k')$$

so that

$$h = h' \text{ and } k = k',$$

giving $hk = h'k'$ and θ is one-one.

If $hk, h'k' \in G$, then as in Lemma 8.7 we have

$$(hk)(h'k') = (hh')((h')^{-1}kh'k'),$$

so

$$\theta((hk)(h'k')) = \theta\big((hh')((h')^{-1}kh'k')\big) =$$
$$(hh', (h')^{-1}kh'k') = (h,k)(h',k') = \theta(hk)\theta(h'k'),$$

so that θ is an isomorphism. □

The group $H * K$ above is an example of an *(external) semidirect product.*

Below, $H \times K$ is the **(external) direct product group.**

Theorem 8.11. *Let G be the* internal direct product *of H and K. Then*

$$\theta : G \to H \times K$$

given by $\theta(g) = (h,k)$ where $g = hk$, $h \in H, k \in K$ is an isomorphism.

Proof. We have

$$H \trianglelefteq G, K \trianglelefteq G.$$

Let $h \in H, k \in K$. Then

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{e\},$$

so that

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

and

$$hk = kh.$$

Then in $H * K$,

$$(h,k)(h',k') = (hh', (h')^{-1}kh'k') = (hh', k(h')^{-1}h'k') = (hh', kk'),$$

so that $H * K$ is just the direct product group $H \times K$. From Theorem 8.10

$$\theta : G \to H \times K$$

given by

$$\theta(hk) = (h,k)$$

is an isomorphism. □

For a converse:

Theorem 8.12. *Let H and K be groups. Put*

$$H' = \{(h, e_K) : h \in H\} \text{ and } K' = \{(e_H, k) : k \in K\}.$$

Then $H \times K$ is the internal direct product of H' and K'. Moreover,

$$H' \cong H \text{ and } K' \cong K.$$

Proof. We have that

$$\pi_1 : H \times K \to H,\ (h,k) \mapsto h \text{ and } \pi_2 : H \times K \to K,\ (h,k) \mapsto k$$

are onto homomorphisms, with

$$\operatorname{Ker} \pi_1 = K' \text{ and } \operatorname{Ker} \pi_2 = H',$$

so that $H' \trianglelefteq H \times K$ and $K' \trianglelefteq H \times K$.

For any $(h,k) \in H \times K$ we have

$$(h,k) = (h,e_K)(e_H,k) \in H'K'$$

and clearly

$$H' \cap K' = \{(e_H, e_K)\}.$$

Hence $H \times K$ is the internal direct product of H' and K'. Clearly

$$(h,e_k) \to h \text{ and } (e_H,k) \to k$$

are isomorphisms so that $H' \cong H$ and $K' \cong K$.

□

Let G be a group and let $H \leq G$. We know from the Exercises that for $g \in G$,

$$g^{-1}Hg \leq G.$$

Definition 8.13. Let G be a group and let $H, K \leq G$. Then H is *conjugate* to K, written $H \sim K$, if

$$K = g^{-1}Hg$$

for some $g \in G$.

Lemma 8.14. *The relation $\sim$ is an equivalence relation on the set of subgroups of G. Further, if $H \sim K$, then $H \cong K$.*

Proof. The fact that $\sim$ is an equivalence is essentially the 'same as' for Lemma 5.2. If $H \sim K$, then $K = g^{-1}Hg$ for some $g \in G$. Then $\psi_g : K \to H$ given by

$$\psi_g(k) = g^{-1}gk$$

is an isomorphism. *It is the restriction of the corresponding inner automorphism of G.* □

Remark 8.15. With the above notation, if G is the internal semidirect product of H and K, where $K \trianglelefteq G$, then in the external semidirect product $H * K$ we have

$$(h,k)(h',k') = (hh', \psi_{h'}(k)k').$$

Lemma 8.16. *Let $A \cong A', B \cong B'$. Then*

$$A \times B \cong A' \times B'.$$

Proof. If $\theta : A \to A', \phi : B \to B'$ are isomorphisms, define

$$\psi : A \times B \to A' \times B'$$

by

$$\psi(a, b) = (\theta(a), \phi(b))$$

and check ψ is an isomorphism. □

8.3. **Examples.** *We have already proven the next result using orders of elements directly. Here we use Theorem 8.11.*

Example 8.17. Let p, q be distinct primes. Then $C_{pq} \cong C_p \times C_q$.

Proof. Let $C_{pq} = \langle a \rangle$. Then $o(a) = pq$ so $o(a^q) = p$ and $o(a^p) = q$. Let

$$A = \langle a^q \rangle, \; B = \langle a^p \rangle.$$

As C_{pq} is commutative, $A \trianglelefteq C_{pq}$ and $B \trianglelefteq C_{pq}$.

Let $H = A \cap B$. Then $H \leq G$ (the intersection of subgroups is a subgroup) and so $H \leq A$ and $H \leq B$. By Lagrange, $|H|$ divides p and q, so that $|H| = 1$ and $A \cap B = \{e\}$.

To see that $C_{pq} = AB$, recall that as $\text{hcf}(p, q) = 1$, there are $s, t \in \mathbb{Z}$ with $1 = sq + tp$. Then for any $z \in \mathbb{Z}$ we have that $z = q(sz) + p(tz)$ and so

$$a^z = a^{q(sz)+p(tz)} = (a^q)^{sz}(a^p)^{tz} \in AB.$$

Thus $C_{pq} = AB$.

By Theorem 8.11

$$C_{pq} \cong A \times B$$

and so using Lemma 8.16,

$$C_{pq} \cong C_p \times C_q.$$

□

Example 8.18. Let G be the subset of $\mathcal{S}_6$ consisting of those permutations ρ which satisfy $\rho(\{1, 2, 3\}) = \{1, 2, 3\}$ (and hence also $\rho(\{4, 5, 6\}) = \{4, 5, 6\}$). Let

$$A = \{\rho \in S_6 : \rho(i) = i \text{ for } i = 4, 5, 6\}$$

and

$$B = \{\rho \in S_6 : \rho(i) = i \text{ for } i = 1, 2, 3\}.$$

You are given that G is a subgroup of $\mathcal{S}_6$, that $A \trianglelefteq G$ and $B \trianglelefteq G$. Use the theorem on direct products to show that $G \cong A \times B$.

Proof. We are given that $A, B \trianglelefteq G$.

Let $\alpha \in G$, say

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ a_1 & a_2 & a_3 & b_1 & b_2 & b_3 \end{pmatrix}.$$

Then, by definition of G, $\{a_1, a_2, a_3\} = \{1, 2, 3\}$ and $\{b_1, b_2, b_3\} = \{4, 5, 6\}$. Hence we can define permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & b_1 & b_2 & b_3 \end{pmatrix}$$

and

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ a_1 & a_2 & a_3 & 4 & 5 & 6 \end{pmatrix}.$$

Then $\sigma \in B$ and $\rho \in A$ and

$$\begin{aligned} \rho\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ a_1 & a_2 & a_3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & b_1 & b_2 & b_3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ a_1 & a_2 & a_3 & b_1 & b_2 & b_3 \end{pmatrix} \\ &= \alpha \end{aligned}$$

and hence $G = AB$.

Finally, if $\rho \in A \cap B$, then $\rho(i) = i$ for $i = 4, 5, 6$ since $\rho \in A$ and $\rho(i) = i$ for $i = 1, 2, 3$ since $\rho \in B$. So $\rho = I_6$ and $A \cap B = \{I_6\}$.

Thus by our theorem on direct products, $G \cong A \times B$. □

Example 8.19. Let $A = \langle(123)\rangle$ and $B = \langle(143)\rangle$. Is $\mathcal{S}_4$ the internal direct product of A and B?

Proof. No! If $\mathcal{S}_4$ were internal direct product of A and B, then $\mathcal{S}_4 \cong A \times B$. But A and B are cyclic, and hence commutative.

If U and V are commutative, then in $U \times V$,

$$(u, v)(u', v') = (uu', vv') = (u'u, v'v) = (u', v')(u, v),$$

so that $U \times V$ is commutative. Hence $A \times B$ and so $\mathcal{S}_4$ would be commutative. But in $\mathcal{S}_4$,

$$(123)(12) \neq (12)(123).$$

□

Appendix

The material in this section is not directly examinable

Lemma 2.1. *For any group G, and any $a_1, a_2, \ldots, a_n \in G$, the product*

$$a_1 * a_2 * \ldots * a_n$$

is unambiguous.

Proof. We show that, no matter how we bracket the product, it is equal to

$$x_1 * (x_2 * (\ldots (x_{n-1} * x_n) \ldots)).$$

We use induction. If $n = 1$ or $n = 2$ there is nothing to show. Suppose now that $n \geq 3$ and the result is true for any m with $1 \leq m < n$. Consider the expression $x_1 * x_2 * \ldots * x_n$ and suppose that the final bracket is placed as follows

$$(x_1 * \ldots * x_i) * (x_{i+1} * \ldots * x_n).$$

By the inductive hypothesis, the product

$$x_1 * \ldots * x_i$$

may be calculated as

$$x_1 * (x_2 * (\ldots * (x_{i-1} * x_i) \ldots)).$$

Thus

$$(x_1 * \ldots * x_i) * (x_{i+1} * \ldots * x_n) = (x_1 * y) * z$$

where $y = x_2 * \ldots * x_i$ and $z = x_{i+1} * \ldots * x_n$. By the inductive hypothesis, y and z are unambiguous. By associativity,

$$(x_1 * \ldots * x_i) * (x_{i+1} * \ldots * x_n) = x_1 * (y * z)$$

and again by induction,

$$y * z = x_2 * (x_3 * (\ldots * (x_{n-1} * x_n) \ldots))$$

giving that

$$(x_1 * \ldots * x_i) * (x_{i+1} * \ldots * x_n) = x_1 * (x_2 * (\ldots * (x_{n-1} * x_n) \ldots))$$

as required.

□

Proposition 2.3 *For any $g \in G$ and $z_1, z_2 \in \mathbb{Z}$ we have*

(1) $g^{z_1} g^{z_2} = g^{z_1 + z_2}$;
(2) $(g^{z_1})^{z_2} = g^{z_1 z_2}$.

Proof. It is handy in this proof to use $*$ for the binary operation in G.

(1) We split the argument into special cases.

At least one of the exponents is 0

We have

$$g^{z_1} * g^0 = g^{z_1} * e = g^{z_1} = g^{z_1 + 0}$$

and similarly,

$$g^0 * g^{z_2} = g^{0+z_2},$$

for any $z_1, z_2 \in \mathbb{Z}$.

Both exponents are natural numbers

Let $m, n \in \mathbb{N}$. Then

$$g^m * g^n = \underbrace{(g * \cdots * g)}_{m \text{ factors}} * \underbrace{(g * \cdots * g)}_{n \text{ factors}} = \underbrace{g * \cdots * g}_{m+n \text{ factors}} = g^{m+n}.$$

Both exponents are negative

Let $m, n \in \mathbb{N}$. Then

$$g^{-m} * g^{-n} = \underbrace{(g^{-1} * \cdots * g^{-1})}_{m \text{ factors}} * \underbrace{(g^{-1} * \ldots g^{-1})}_{n \text{ factors}} =$$

$$= \underbrace{g^{-1} * \cdots * g^{-1}}_{m+n \text{ factors}} = g^{-(m+n)} = g^{(-m)+(-n)},$$

as required.

Remembering now the rule for the inverse of a product, we have

$$g^{-n} = (g^{-1})^n = (g^n)^{-1}. \tag{1}$$

The first exponent is positive, the second negative

Let $m, n \in \mathbb{N}$. Suppose first that $m = n$. Then

$$g^m * g^{-n} = g^m * g^{-m} = g^m * (g^m)^{-1} = e = g^0 = g^{m+(-n)}.$$

If $m > n$, then

$$g^m * g^{-n} = g^{(m-n)+n} * g^{-n}.$$

Using the result in the case where both exponents are positive, we have

$$g^m * g^{-n} = (g^{m-n} * g^n) * g^{-n} = g^{m-n} * (g^n * g^{-n}) = g^{m-n},$$

as we know that $g^n * g^{-n} = e$. Thus

$$g^m * g^{-n} = g^{m+(-n)}.$$

Finally in this case, suppose that $m < n$. Then

$$g^m * g^{-n} = g^m * (g^{(-m)+(-(n-m)}).$$

Now use the case where both exponents are negative to obtain

$$g^m * g^{-n} = g^m * (g^{-m} * g^{m-n}) = (g^m * g^{-m}) * g^{m-n} = g^{m-n} = g^{m+(-n)}.$$

The first exponent is negative, the second positive

Similar to the previous case!

(2) Again, we have to look at special cases. If $z_1 = 0$, then

$$(g^{z_1})^{z_2} = (g^0)^{z_2} = e^{z_2} = e,$$

as $e^{-1} = e$ and e^{z_2} is therefore a product of $|z_2|$ copies of e. Thus

$$(g^{z_1})^{z_2} = g^0 = g^{0z_2} = g^{z_1 z_2}.$$

On the other hand, if $z_2 = 0$, then by definition of g^0,

$$(g^{z_1})^{z_2} = e = g^{z_1 0} = g^{z_1 z_2}.$$

Both exponents are positive
Let $m, n \in \mathbb{N}$. Then

$$(g^m)^n = \underbrace{(g * \cdots * g)}_{m \text{ factors}}^n = \underbrace{\underbrace{(g * \cdots * g)}_{m \text{ factors})} * \cdots * \underbrace{(g * \cdots * g)}_{m \text{ factors}}}_{n\text{factors}} =$$

$$= \underbrace{(g * \cdots * g)}_{mn \text{ factors}} = g^{mn}.$$

Both exponents are negative
Let $m, n \in \mathbb{N}$. Then, making use of Equation (1)

$$(g^{-m})^{-n} = (((g^m)^{-1})^n)^{-1} = (((g^m)^n)^{-1})^{-1} = (g^m)^n = g^{mn} = g^{(-m)(-n)}.$$

The first exponent is negative, the second is positive
We have

$$(g^{-m})^n = ((g^m)^{-1})^n = ((g^m)^n)^{-1} = (g^{mn})^{-1} = g^{-mn} = g^{(-m)n}.$$

The first exponent is positive, the second is negative
We have

$$(g^m)^{-n} = ((g^m)^n)^{-1} = (g^{mn})^{-1} = g^{-mn} = g^{m(-n)},$$

so completing the proof.

□

Proposition 3.11 *Let $\alpha \in \mathcal{S}_n$. Then*

$$\alpha = \gamma_1 \gamma_2 \dots \gamma_k$$

where $\gamma_1, \dots, \gamma_k$ are disjoint *cycles. This expression is unique except for the order in which the cycles are written. We interpret the empty product as I_n.*

Proof. Let $\alpha \in \mathcal{S}_n$. Consider the list of numbers

$$1, 2, \dots, n.$$

Choose the first i in the list such that $\alpha(i) \neq i$. (If no such i can be found, α would be the identity I_n, and by convention I_n is a product of 0 cycles.) Consider the list

$$i = \alpha^0(i), \alpha(i), \alpha^2(i), \alpha^3(i), \dots$$

This list must be finite (as it is contained in $\{1, \dots, n\}$) and so must contain repeats. Suppose that $\alpha^u(i)$ is the first power to be repeated and $\alpha^u(i) = \alpha^{u+v}(i)$ where $v > 0$ is the first repeat. The inverse of α^u in the group $\mathcal{S}_n$ is α^{-u}, so that

$$i = I_n(i) = \alpha^{-u}\alpha^u(i) = \alpha^{-u}\alpha^{u+v}(i) = \alpha^{(-u)+(u+v)}(i) = \alpha^v(i).$$

The conclusion of this is that α^0 is the first repeated power, that is, $u = 0$. Also, $\alpha^v(i)$ is the first repeat in the list. Thus

$$i, \alpha(i), \alpha^2(i), \ldots, \alpha^{v-1}(i)$$

are all distinct. Put $k_1 = v - 1$. Let γ_1 be the cycle

$$(i, \alpha(i), \alpha^2(i), \ldots, \alpha^{k_1}(i)).$$

Using the division algorithm, we can show that for any $z \in \mathbb{Z}$,

$$\alpha^z(i) \in \{i, \alpha(i), \alpha^2(i), \ldots, \alpha^{k_1}(i)\}.$$

If $\alpha(j) = j$ for all j not in the list

$$i, \alpha(i), \alpha^2(i), \ldots, \alpha^{k_1}(i)$$

we stop. Otherwise, pick the smallest j not in this list and consider the elements

$$j, \alpha(j), \alpha^2(j), \ldots$$

of $\{1, \ldots, n\}$. We cannot have

$$\alpha^u(i) = \alpha^v(j)$$

for any $0 \leq u \leq v$ as this would give us

$$j = \alpha^{v-u}(i),$$

contradicting the choice of j. Arguing as above, we obtain a cycle γ_2

$$(j, \alpha(j), \alpha^2(j), \ldots, \alpha^{k_2}(j))$$

for some k_2; notice that this cycle is disjoint to γ_1.

Continuing in this manner we obtain disjoint cycles $\gamma_1, \gamma_2, \ldots, \gamma_r$ until all the elements of $\{1, \ldots, n\}$ have been used up. By their very construction, α is the product of the disjoint cycles $\gamma_1, \ldots, v_r$, that is,

$$\alpha = v_1 \ldots \gamma_r.$$

We must now argue for uniqueness. If also

$$\alpha = \delta_1 \ldots \delta_s$$

for disjoint cycles $\delta_1, \ldots, \delta_s$ then notice that for any $\ell \in \{1, 2, \ldots, n\}$ we have that $\alpha(\ell) = \ell$ if and only if ℓ does not appear in any γ_i if and only if ℓ does not appear in any δ_j.

If ℓ appears in γ_h and δ_k then without loss of generality we may assume that

$$\gamma_h = (\ell, \ldots\ldots) = (\ell, \alpha(\ell), \ldots, \alpha^p(\ell))$$

where $\alpha^{p+1}(\ell) = \ell$. But, since we can also assume that δ_k 'begins' with ℓ we obtain that $\gamma_h = \delta_k$. Since disjoint cycles commute, we can also assume that $h = k = 1$ so that by cancellation

$$\gamma_2 \ldots \gamma_r = \delta_2 \ldots \delta_s.$$

An inductive argument now yields that $r = s$ and (after re-labelling) $\gamma_i = \delta_i$ for $1 \leq i \leq r$. $\square$

Proposition 3.15 *Let $\alpha \in \mathcal{S}_n, \alpha \neq I_n$. Write*

$$\alpha = \gamma_1\gamma_2 \dots \gamma_m$$

where $\gamma_1, \dots, \gamma_m$ are disjoint cycles. Suppose the length of γ_i is ℓ_i for $1 \leq i \leq m$. Then

$$o(\alpha) = lcm\{\ell_1, \ell_2, \dots, \ell_m\}.$$

Proof. Let the cycle decomposition of α be $\gamma_1\gamma_2 \dots \gamma_m$ where γ_i is a cycle of length ℓ_i. We know that the order of γ_i is its length, namely ℓ_i. Since disjoint cycles commute,

$$\alpha^x = (\gamma_1 \dots \gamma_m)^x = \gamma_1^x \dots \gamma_m^x$$

for any $x \in \mathbb{N}$. If x is a multiple of ℓ_i, then $\gamma_i^x = I_n$, so that if x is a common multiple of *all* the γ_i, then

$$\alpha^x = \gamma_1^x \dots \gamma_m^x = I_n \dots I_n = I_n.$$

Suppose that $y \in \mathbb{N}$, $\alpha^y = I_n$ and y is not a common multiple of $\ell_1, \dots, \ell_m$. Since the γ_i commute with eachother, we can assume that ℓ_1 does not divide y. Write $y = q\ell_1 + r$ where $0 < r < \ell_1$. We know that $\gamma_1^y = \gamma_1^r$. Let

$$\gamma_1 = (a_1\, a_2\, \dots\, a_{\ell_1}).$$

Since the γ_i are disjoint, a_1 does not appear in any of $\gamma_2, \dots, \gamma_m$. Thus $\gamma_j^y(a_1) = a_1$ for $2 \leq j \leq m$. Now

$$\begin{aligned} \alpha^y(a_1) &= (\gamma_1^y\gamma_2^y \dots \gamma_m^y)(a_1) \\ &= \gamma_1^y(\gamma_2^y(\dots(\gamma_m^y(a_1))\dots)) \\ &= \gamma_1^y(\gamma_2^y(\dots(\gamma_{m-1}^y(a_1))\dots)) \\ &= \dots = \gamma_1^y(a_1) = \gamma_1^r(a_1) = a_{1+r} \neq a_1. \end{aligned}$$

Thus $\alpha^y \neq I_n$, a contradiction.

We deduce that $\alpha^x = I_n$ if and only if x is a common multiple of the ℓ_i. Hence the least such x, namely the order of α, must be the lcm of $\{\ell_1, \ell_2, \dots, \ell_m\}$.

□

Theorem 3.20 *Let $\alpha \in \mathcal{S}_n$. Then the number of transpositions whose product equals α is either always even or always odd.*

Proof. Consider a real polynomial in n variables

$$x_1, \dots, x_n.$$

If f is such a polynomial and $\mu \in \mathcal{S}_n$, then

$$\mu * f$$

is the polynomial obtained by applying μ to all the subscripts in f. For example, if $n = 6$ and $f = x_1 + x_2x_3$, then

$$(1\,2\,3) * f = x_2 + x_3x_1 \neq f$$

whereas

$$(2\,3) * f = x_1 + x_3x_2 = x_1 + x_2x_3 = f.$$

Notice that for any f and any μ,

$$\mu * (-f) = -(\mu * f).$$

Also, for any $\mu_1, \mu_2, \ldots, \mu_r$,

$$(\mu_1 \ldots \mu_r) * f = \mu_1 * (\mu_2 * (\ldots (\mu_r * f) \ldots)).$$

Given that you accept all this, the rest of the proof just involves counting!

We let f_n be the polynomial

$$f_n = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

It helps to write f_n out as

$$\begin{array}{cccccc} (x_1 - x_2) & (x_1 - x_3) & (x_1 - x_4) & \ldots & (x_1 - x_n) \\ & (x_2 - x_3) & (x_2 - x_4) & \ldots & (x_2 - x_n) \\ & & & \vdots & \\ & & & & (x_{n-1} - x_n) \end{array}$$

Next, we look at the effect of a transpostion of the form $(i\, i+1)$ on f_n. It has no overall effect on the first $i-1$ rows, as is swaps over the terms $(x_j - x_i)$ and $(x_j - x_{i+1})$. It does not effect rows $i+2$ to n as these rows contain no term in x_i or x_{i+1}. Considering now rows i and $i+1$

$$\begin{array}{cccccc} (x_i - x_{i+1}) & (x_i - x_{i+2}) & (x_i - x_{i+3}) & \ldots & (x_i - x_n) \\ & (x_{i+1} - x_{i+2}) & (x_{i+1} - x_{i+3}) & \ldots & (x_{i+1} - x_n) \end{array}$$

it alters them to

$$\begin{array}{cccccc} (x_{i+1} - x_i) & (x_{i+1} - x_{i+2}) & (x_{i+1} - x_{i+3}) & \ldots & (x_{i+1} - x_n) \\ & (x_i - x_{i+2}) & (x_i - x_{i+3}) & \ldots & (x_i - x_n) \end{array}.$$

The overall effect of $(i\, i+1)$ on f_n therefore, is to change the pair $(x_i - x_{i+1})$ to $(x_{i+1} - x_i)$. Thus

$$(i\, i+1) * f_n = -f_n.$$

We use the above to show that for *any* transposition $(i\, j)$,

$$(i\, j) * f_n = -f_n.$$

To see this, notice that for $i < j$,

$$(i\, j) = (i\, i+1)(i+1\, i+2) \ldots (j-2\, j-1)(j-1\, j)(j-2\, j-1) \ldots (i+1\, i+2)(i\, i+1).$$

Counting up the number of these, we have that $(i\, j)$ is a product of $2(j-i)-1$ transpositions. For ease of notation, call these $t_{2(j-i)-1}, \ldots, t_2, t_1$. We have

$$(t_{2(j-1)-1} \ldots t_1) * f_n = t_{2(j-1)-1} * (t_{2(j-1)-2} * (\ldots (t_2 * (t_1 * f_n) \ldots))$$

As the effect of each t_i is to change the sign of $\pm f_n$, we have

$$(i\, j) * f = (-1)^{2(j-1)-1} f_n = -f_n.$$

Now for *any* $\mu \in \mathcal{S}_n$, write μ as a product of k transpositions. With a similar argument to the above we have

$$\mu * f_n = (-1)^k f_n$$

so that if k is even, $\mu * f_n = f_n$ and if k is odd, $\mu * f_n = -f_n$. We can write μ in different ways as products of transpositions, but $\mu * f_n$ cannot be both f_n and $-f_n$, so that the number of transpositions involved must be either odd or even. □

Theorem 5.6 *Let $\alpha, \beta \in \mathcal{S}_n$. Then $\alpha \sim \beta$ if and only if α and β have the same cycle type.*

Proof. Suppose that $\alpha \sim \beta$. Write

$$\alpha = \gamma_1 \dots \gamma_m$$

where the length of γ_i is ℓ_i.

If $\alpha \sim \beta$, then for some $\delta \in \mathcal{S}_n$ we have

$$\begin{aligned} \beta &= \delta\alpha\delta^{-1} \\ &= \delta\gamma_1 \dots \gamma_m\delta^{-1} \\ &= \delta\gamma_1(\delta^{-1}\delta)\gamma_2(\delta^{-1}\delta)\dots(\delta^{-1}\delta)\gamma_m\delta^{-1} \\ &= (\delta\gamma_1\delta^{-1})(\delta\gamma_2\delta^{-1})\dots(\delta\gamma_m\delta^{-1}) \end{aligned} .$$

We know from Example 5.4 that $\delta\gamma_i\delta^{-1}$ is a cycle of the same length as γ_i, i.e. ℓ_i. Moreover, if

$$\gamma_k = (x_1^k \dots x_{\ell_k}^k)$$

then

$$\delta\gamma_i\delta^{-1} = (\delta(x_1^i)\dots\delta(x_{\ell_i}^i)) \text{ and } \delta\gamma_j\delta^{-1} = (\delta(x_1^j)\dots\delta(x_{\ell_j}^j)).$$

These cycles must be disjoint, for if

$$\delta(x_u^i) = \delta(x_v^j)$$

then $x_u^i = x_v^j$, contradicting γ_i and γ_j being disjoint.

Hence $\beta = \delta\alpha\delta^{-1}$ has the same cycle type as α.

For the converse, suppose that

$$\beta = \mu_1 \dots \mu_m$$

is the cycle decomposition of some β with the same cycle type as α, so that the length of μ_i is ℓ_i for $1 \le i \le m$.

Write

$$\mu_k = (y_1^k \dots y_{\ell_k}^k).$$

Then

$$\begin{aligned} |\{x_1^1, \dots, x_{\ell_1}^1, \dots, x_1^m, \dots, x_{\ell_m}^m\}| &= |\{y_1^1, \dots, y_{\ell_1}^1, \dots, y_1^m, \dots, y_{\ell_m}^m\}| \\ &= \ell_1 + \dots + \ell_m. \end{aligned}$$

Let

$$\begin{aligned} \theta : (\{1, \dots, n\} \setminus \{x_1^1, \dots, x_{\ell_1}^1, \dots, x_1^m, \dots, x_{\ell_m}^m\}) \\ \to (\{1, \dots, n\} \setminus \{y_1^1, \dots, y_{\ell_1}^1, \dots, y_1^m, \dots, y_{\ell_m}^m\}) \end{aligned}$$

be a bijection.

Define $\delta \in \mathcal{S}_n$ by

$$\delta(x_j^i) = y_j^i$$

and for $z \notin \{x_1^1, \ldots, x_{\ell_1}^1, \ldots, x_1^m, \ldots, x_{\ell_m}^m\}$,

$$\delta(z) = \theta(z).$$

Then

$$\delta\alpha\delta^{-1} = \delta\gamma_1 \ldots \gamma_m\delta^{-1} = (\delta\gamma_1\delta^{-1}) \ldots (\delta\gamma_m\delta^{-1}) = \mu_1 \ldots \mu_m = \beta,$$

so that $\alpha \sim \beta$. □